PRINCIPALLY POLARIZED SQUARES OF ELLIPTIC CURVES WITH FIELD OF MODULI EQUAL TO $\mathbb{Q}$

ALEXANDRE GÉLIN, EVERETT W. HOWE, AND CHRISTOPHE RITZENTHALER

Abstract. We give equations for 13 genus-2 curves over $\overline{\mathbb{Q}}$, with models over $\mathbb{Q}$, whose unpolarized Jacobians are isomorphic to the square of an elliptic curve with complex multiplication by a maximal order. If the Generalized Riemann Hypothesis is true, there are no further examples of such curves. More generally, we prove under the Generalized Riemann Hypothesis that there exist exactly 46 genus-2 curves over $\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to the square of an elliptic curve with complex multiplication by a maximal order.

1. Introduction

For $g > 1$, let $\mathfrak{M}_g$ (resp. $\mathfrak{A}_g$) be the moduli space classifying absolutely irreducible projective smooth curves of genus g (resp. principally polarized abelian varieties of dimension g) over $\overline{\mathbb{Q}}$. These spaces are quasi-projective varieties defined over $\mathbb{Q}$, linked by the Torelli map, which associates to a curve its Jacobian. To explain the modular interpretation of rational points on these spaces, we must define the terms *field of definition* and *field of moduli*. If X is a curve or polarized abelian variety over $\overline{\mathbb{Q}}$, we say that a field $F \subseteq \overline{\mathbb{Q}}$ is a *field of definition* of X if there exists a variety X_0/F — called a *model* of X over F — such that $X_0 \simeq_{\overline{\mathbb{Q}}} X$. Since $\overline{\mathbb{Q}}$ is a field of characteristic 0, by [Koi72, Corollary 3.2.2, p. 54] we can define the *field of moduli* of X to be either

- the field fixed by the subgroup $\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid X \simeq X^\sigma\}$, or
- the intersection of the fields of definition of X.

With these terms defined, we can say that the rational points on $\mathfrak{M}_g$ (resp. $\mathfrak{A}_g$) correspond to the isomorphism classes of curves (resp. principally polarized abelian varieties) over $\overline{\mathbb{Q}}$ that have field of moduli $\mathbb{Q}$ [Bai62].

There are a number of interesting sets of rational points on $\mathfrak{A}_g$, but the complex multiplication (CM) abelian varieties — that is, the principally polarized abelian varieties having endomorphism rings containing an order in a number field of degree $2g$ over $\mathbb{Q}$ — have attracted the most interest. When such a point on $\mathfrak{A}_g$ lies in the image of $\mathfrak{M}_g$, the corresponding curve is called a *CM-curve*. For $g = 2$, the set of *simple* CM-abelian varieties with field of moduli $\mathbb{Q}$ is known, and for those varieties that are Jacobians explicit equations have been computed for the corresponding curves [Spa94, vW99, MU01, KS15, BS17]; for $g = 3$ the similar set of possible CM maximal orders is determined in [Kıl16] and conjectural equations for the curves are given in [Wen01, KW05, BILV16, LS16, KLL+17]. (And while

2010 *Mathematics Subject Classification.* Primary 11G15; Secondary 14H25, 14H45.

This work was supported in part by a public grant as part of the *Investissement d'avenir* project, reference ANR-11-LABX-0056-LMH, LabEx LMH.

we have avoided the case $g = 1$ in the discussion above for technical reasons, it is still of course true that the CM-elliptic curves with rational j-invariants are known as well [Sil94, Appendix A.3].)

In this article we consider genus-2 curves whose Jacobians are non-simple CM-abelian surfaces. Every such surface is isogenous to the square of a CM-elliptic curve, but we restrict our attention in two ways: first, we look only at surfaces that are *isomorphic* (and not just isogenous) to E^2 for a CM-elliptic curve E, and second, we only consider E that have CM by a maximal order. The second restriction is not essential to our methods, and we impose it here in order to simplify some of our calculations. Note that if the elliptic curve E has no CM — *i.e.*, $\mathrm{End}(E) \simeq \mathbb{Z}$, then E^2 cannot be isomorphic to the Jacobian of a genus-2 curve, because E^2 has no indecomposable principal polarizations [Lan06, Corollary 4.2, p. 159].

Main Contributions. We prove under the Generalized Riemann Hypothesis that there exist exactly 46 genus-2 curves over $\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to the square of an elliptic curve with CM by a maximal order. We show that among these 46 curves exactly 13 can be defined over $\mathbb{Q}$, and we give explicit equations for them. In order to accomplish this, we develop an algorithm to compute, for an imaginary quadratic maximal order $\mathcal{O}$, canonical forms for all positive definite unimodular Hermitian forms on $\mathcal{O} \times \mathcal{O}$. Such Hermitian forms correspond to principal polarizations φ on E^2, and our algorithm computes the automorphism group of the polarized variety (E^2, φ) and identifies the polarizations that come from genus-2 curves.

Related work. Hayashida and Nishi [HN65] consider in particular when a product of two elliptic curves, with CM by the same maximal order $\mathcal{O}$, is the Jacobian of a curve over $\mathbb{C}$, and they find that this happens if and only if the discriminant of $\mathcal{O}$ is different from -1, -3, -7, and -15. Hayashida [Hay68] gives the number of indecomposable principal polarizations on E^2 where $E/\mathbb{C}$ is an elliptic curve with CM by a maximal order. More recently, Kani [Kan14, Kan16] gives existence results on Jacobians isomorphic to the product of two elliptic curves with control on the polarization, and Schuster [Sch90] and Lange [Lan06] study generalizations to higher dimensions. Rodriguez-Villegas [Rod00] considers the same situation as Hayashida and Nishi, and in the case where $\mathcal{O}$ has class number 1 and odd discriminant, he gives an algorithm (relying on quaternion algebras) for producing curves with field of moduli $\mathbb{Q}$. Note finally that Fité and Guitart [FG18] determine when there exists an abelian surface $A/\mathbb{Q}$ that is $\overline{\mathbb{Q}}$-isogenous to E^2, with $E/\overline{\mathbb{Q}}$ a CM-curve.

Outline. Our article proceeds as follows. Torelli's theorem (see [Lau01, Appendix]) implies that our genus-2 curve C has field of moduli $\mathbb{Q}$ if and only if its principally polarized Jacobian (E^2, φ) has field of moduli $\mathbb{Q}$. We therefore need to find all elliptic curves E with CM by a maximal order $\mathcal{O}$ and all polarizations φ of E^2 such that (E^2, φ) is isomorphic to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. Proposition 2.1 shows that if E^2 is isomorphic to all of its Galois conjugates — even just as an abelian variety without polarization — then the class group of $\mathcal{O}$ has exponent at most 2. Under the Generalized Riemann Hypothesis, this gives us an explicit finite list of possible orders (Table 1). For each of these orders $\mathcal{O}$, one can identify the indecomposable principal polarizations φ on E^2 and describe them as certain 2-by-2 matrices M with coefficients in $\mathcal{O}$ (Proposition 3.1). Tables of such matrices were

10 Jun 2018 23:17:48 PDT
Version 2 - Submitted to Open Book Series

computed by Hoffmann [Hof91] and Schiemann [Sch98] and were published online,[1] but they only include a fraction of the discriminants that we must consider. We therefore describe an algorithm, using a method different from that of Hoffmann and Schiemann, that we use to recompute these tables of matrices (Section 3.2). Given such a matrix M, we find explicit algebraic conditions on M for the principally polarized abelian surface (E^2, φ) to have field of moduli $\mathbb{Q}$ (Section 3.3). We check whether these conditions are satisfied for each M on our list.

We conclude the article with three more results: we heuristically compute the Cardona–Quer invariants [CQ05] of the associated curves C and see that the factorization of their denominators reveals interesting patterns; we show that the field of moduli is a field of definition if and only if C has a non-trivial group of automorphisms (*i.e.*, of order greater than 2, see Section 4.1); and for the curves C defined over $\mathbb{Q}$, we compute equations and prove that they are correct.

Notation. In the following, E is an elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication by a maximal order $\mathcal{O}$ of discriminant Δ and with fraction field K, which we sometimes call the *CM-field*.

2. Condition on E^2

We are interested in the field of moduli $\mathbf{M}$ of a principally polarized abelian surface (E^2, φ). As outlined above, we first consider the abelian surface E^2 alone and we give a necessary condition for $\mathbf{M}$ to be contained in the CM-field K. If $\mathbf{M} \subseteq K$ then in particular we have $E^2 \simeq (E^\sigma)^2$ for all $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$. The class group $\mathrm{Cl}(\mathcal{O})$ acts simply transitively on the set of elliptic curves with CM by $\mathcal{O}$ [Sil94, Proposition 1.2, p. 99]. Since $\mathrm{End}(E^\sigma) = \mathrm{End}(E) = \mathcal{O}$, for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, there exists a unique class of ideals $I_\sigma \in \mathrm{Cl}(\mathcal{O})$ such that $E^\sigma \simeq E/I_\sigma$.

Using a result of Kani [Kan11, Proposition 65, p. 335], we get that, for E, σ and I_σ defined as above,

$$E^2 \simeq (E/I_\sigma)^2 \quad \Longleftrightarrow \quad I_\sigma^2 = [\mathcal{O}]\,,$$

where the last equality is in $\mathrm{Cl}(\mathcal{O})$. Note that since we only work with maximal orders, the conditions on the conductors in Kani's result are trivially satisfied. Moreover by [Sil94, Theorem 4.3, p. 122], since for any $I \in \mathrm{Cl}(\mathcal{O})$ there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ (actually even in $\mathrm{Gal}\left(K\big(j(E)\big)/K\right)$) such that $E/I = E^\sigma$, we get the following proposition.

Proposition 2.1. *A necessary condition for $\mathbf{M} \subseteq K$ is that the class group of $\mathcal{O}$ has exponent at most 2.*

Louboutin [Lou90] shows that under the assumption of the Generalized Riemann Hypothesis, the discriminant Δ of an imaginary quadratic field whose class group is of exponent at most 2 satisfies $|\Delta| \leq 2 \cdot 10^7$. In Table 1 we list the 65 fundamental discriminants satisfying this bound that give class groups of exponent at most 2.

3. Polarized abelian surfaces

3.1. **Polarizations on the square of an elliptic curve.** We now consider the principal polarizations on the product surface $A = E^2$. A principal polarization on A is, in particular, an isogeny of degree 1 from A to the dual $\widehat{A}$ of A, but

[1] Available at https://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/.

10 Jun 2018 23:17:48 PDT
Version 2 - Submitted to Open Book Series

$\#\operatorname{Cl}(\mathcal{O})$	Discriminants Δ
2^0	-3, -4, -7, -8, -11, -19, -43, -67, -163
2^1	-15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, -427
2^2	-84, -120, -132, -168, -195, -228, -280, -312, -340, -372, -408, -435, -483, -520, -532, -555, -595, -627, -708, -715, -760, -795, -1012, -1435
2^3	-420, -660, -840, -1092, -1155, -1320, -1380, -1428, -1540, -1848, -1995, -3003, -3315
2^4	-5460

TABLE 1. Discriminants Δ of the imaginary quadratic maximal orders $\mathcal{O}$ of exponent at most 2, conditional on the Generalized Riemann Hypothesis.

not every isomorphism $A \to \widehat{A}$ is a principal polarization; other properties must be satisfied as well (see [BL04, § 4.1]). One such polarization is the product polarization $\varphi_0 = \varphi_E \times \varphi_E$. Given any other principal polarization φ, we can consider the automorphism $M = \varphi_0^{-1}\varphi$ of A, which (in light of the isomorphism $A = E^2$) we view as a matrix[2] in $\mathrm{GL}_2(\mathcal{O})$. Our first result characterizes the matrices that arise in this way; the statement is not new, but we provide a proof here because it introduces some of the ideas used in the sequel. (Recall [Hal74, Exercise 7, p. 134] that two matrices M_1 and M_2 in $\mathrm{GL}_2(\mathcal{O})$ are said to be *congruent* if there exists a matrix $P \in \mathrm{GL}_2(\mathcal{O})$ such that $P^* M_1 P = M_2$, where P^* is the conjugate transpose of P.)

Proposition 3.1. *The map $M \mapsto \varphi_0 \cdot M$ defines a bijection between the positive definite unimodular Hermitian matrices with coefficients in $\mathcal{O}$ and the principal polarizations on A. Two principal polarizations are isomorphic to one another if and only if their associated matrices are congruent to one another.*

Proof. By [BL04, Theorem 5.2.4, p. 121], the matrices M corresponding to principal polarizations are totally positive symmetric endomorphisms of norm 1. Here the symmetry is with respect to the Rosati involution of $\mathrm{End}(A)$ associated to the polarization φ_0, which is the conjugate-transpose involution under the identification $\mathrm{End}(A) = M_2(\mathcal{O})$. Thus, the matrices M corresponding to principal polarizations are exactly the positive definite unimodular Hermitian matrices.

Let φ_1 and φ_2 be two principal polarizations on A, corresponding to matrices M_1 and M_2. The polarizations φ_1 and φ_2 are isomorphic to one another if and only if there exists an automorphism $\alpha\colon A \to A$ such that $\widehat{\alpha}\varphi_1\alpha = \varphi_2$, where $\widehat{\alpha}\colon \widehat{A} \to \widehat{A}$ is the dual of α. This last condition is equivalent to $(\varphi_0^{-1}\widehat{\alpha}\varphi_0)(\varphi_0^{-1}\varphi_1\alpha) = \varphi_0^{-1}\varphi_2$. Now, $\varphi_0^{-1}\widehat{\alpha}\varphi_0$ is nothing other than the Rosati involute of α, so if we write α as a matrix $P \in \mathrm{GL}_2(\mathcal{O})$, the condition that determines whether φ_1 and φ_2 are isomorphic is simply $P^* M_1 P = M_2$. □

The principal polarizations on A come in two essentially different types.

Definition 3.2. A polarization φ on an abelian variety A over a field k is said to be *geometrically decomposable* if there exist two abelian varieties A_1 and A_2 over $\overline{k}$

[2]All matrices in this paper act on the left.

of positive dimension, together with polarizations φ_1 and φ_2, such that (A, φ) and $(A_1 \times A_2, \varphi_1 \times \varphi_2)$ are isomorphic over $\overline{k}$. A polarization that is not geometrically decomposable is *geometrically indecomposable*. For brevity's sake, in this paper we drop the adjective *geometrically* and simply use the terms *decomposable* and *indecomposable* for these concepts.

Results in [Wei57, Hoy63, OU73] show that a principally polarized abelian surface is the Jacobian of a curve if and only if the polarization is indecomposable. In the remainder of this section we show how we can easily compute representatives for the congruence classes of matrices representing the decomposable polarizations on E^2; we focus on the indecomposable polarizations in later sections.

Proposition 3.3. *If φ is a decomposable polarization on E^2, then there exist elliptic curves F and F' that have CM by $\mathcal{O}$ such that φ is the pullback to E^2 of the product polarization on $F \times F'$ via some isomorphism $E^2 \simeq F \times F'$. The pair (F, F') giving rise to a given decomposable polarization is unique up to interchanging F and F' and up to isomorphism for each elliptic curve. Moreover, for every F with CM by $\mathcal{O}$ there exists an F' with CM by $\mathcal{O}$ such that $E^2 \simeq F \times F'$.*

Proof. First we note that by definition, if φ is a decomposable polarization on E^2 there must exist elliptic curves F and F', isogenous to E, such that φ is the pullback of the product polarization on $F \times F'$ under some isomorphism $E^2 \simeq F \times F'$. Now, the center of $\mathrm{End}(E^2)$ is $\mathrm{End}(E) = \mathcal{O}$, while the center of $\mathrm{End}(F \times F')$ is $\mathrm{End}(F) \cap \mathrm{End}(F')$; since $\mathcal{O}$ is a maximal order, F and F' both have CM by $\mathcal{O}$.

If $(\alpha, \beta)\colon G \to F \times F'$ is an embedding of an elliptic curve G into $F \times F'$, then the pullback of the product polarization to G is the morphism

$$\begin{bmatrix} \widehat{\alpha} & \widehat{\beta} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \widehat{\alpha}\alpha + \widehat{\beta}\beta = \deg(\alpha) + \deg(\beta);$$

that is, the pullback is the multiplication-by-d map, with $d = \deg(\alpha) + \deg(\beta)$. It follows that if φ is the pullback to E^2 of the product polarization on $F \times F'$ via some isomorphism $E^2 \simeq F \times F'$, then the set of elliptic curves G for which there exists an embedding $\epsilon\colon G \to E^2$ such that $\epsilon^*\varphi$ is a principal polarization is simply $\{F, F'\}$. Thus, for a given decomposable principal polarization, the pair (F, F') is unique up to order and isomorphism.

As we noted at the beginning of Section 2, the set of elliptic curves with CM by $\mathcal{O}$ is a principal homogenous space for the class group of $\mathcal{O}$. Given an F with CM by $\mathcal{O}$, let $I \in \mathrm{Cl}(\mathcal{O})$ be the ideal class that takes E to F. If F' is an elliptic curve with CM by $\mathcal{O}$, say corresponding to an ideal class $I' \in \mathrm{Cl}(\mathcal{O})$, then $E^2 \simeq F \times F'$ if and only if I' is the inverse of I (see [Kan11, Proposition 65, p. 335]). This proves the final statement of the proposition. □

Corollary 3.4. *Let h denote the class number of $\mathcal{O}$, and let t denote the size of the 2-torsion subgroup of the class group. The number of decomposable polarizations on E^2 is equal to $(h + t)/2$.*

Proof. The proof of Proposition 3.3 shows that the unordered pairs (F, F') with $E^2 \simeq F \times F'$ correspond to unordered pairs (I, I^{-1}), where $I \in \mathrm{Cl}(\mathcal{O})$. The number of such pairs is $(h + t)/2$. □

Let F be an elliptic curve with CM by $\mathcal{O}$ and let I be the ideal class that takes E to F. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ representing I, such that $\mathfrak{a}$ is not divisible

by any nontrivial ideal of $\mathbb{Z}$. We may write $\mathfrak{a} = (n, \alpha)$, where $n = \mathrm{Norm}(\mathfrak{a}) \in \mathbb{Z}$ and where $\alpha \in \mathfrak{a}$ is chosen so that the ideal $\alpha\mathfrak{a}^{-1}$ is coprime to $n\mathcal{O}$; then there exist $x, y \in \mathbb{Z}$ such that $xn^2 - y\,\mathrm{Norm}(\alpha) = n$. Let F' be the elliptic curve such that $E^2 \simeq F \times F'$. We prove the following corollary in Section 3.3.

Corollary 3.5. *In the notation of the paragraph above, the isomorphism class of the decomposable polarization on E^2 obtained from pulling back the product polarization on $F \times F'$ is represented by the congruence class of the matrix*

$$\begin{pmatrix} n + \frac{\mathrm{Norm}(\alpha)}{n} & (x+y)\alpha \\ (x+y)\overline{\alpha} & x^2 n + y^2 \frac{\mathrm{Norm}(\alpha)}{n} \end{pmatrix}.$$

3.2. **How to find the polarizations?** In Section 2, we identified 65 orders $\mathcal{O}$ for which we need to compute the set of indecomposable principal polarizations, or equivalently, representatives of the congruence classes of indecomposable positive definite unimodular Hermitian matrices with coefficients in $\mathcal{O}$. In this section we describe how we computed these representatives.

Fix an embedding ϵ_0 of K into the complex numbers. For any $\alpha \in \mathcal{O}$, we write $\alpha > 0$ if either the trace of α is positive, or the trace of α is 0 and $\epsilon_0(\alpha)$ has positive imaginary part. Then for $\alpha, \beta \in \mathcal{O}$ we write $\alpha > \beta$ if $\alpha - \beta > 0$. Clearly this gives us a total ordering on $\mathcal{O}$.

Let $\mathcal{H}$ denote the set of positive definite unimodular Hermitian matrices with coefficients in $\mathcal{O}$. Let $\chi\colon \mathcal{H} \to \mathbb{N}\times\mathbb{N}\times\mathcal{O}$ be the map that sends a matrix $M = \left(\begin{smallmatrix} a & b \\ \overline{b} & d \end{smallmatrix}\right)$ to the triple (a, d, b). We define a total ordering on $\mathcal{H}$ by saying that $M_1 < M_2$ if $\chi(M_1) < \chi(M_2)$ in the lexicographic ordering on $\mathbb{N} \times \mathbb{N} \times \mathcal{O}$.

Given any $M \in \mathcal{H}$, we say that M is *reduced* if $M \le M'$ for all M' congruent to M. Clearly every $M \in \mathcal{H}$ is congruent to a unique reduced matrix. The following algorithm produces the reduced matrix that is congruent to a given M.

Algorithm 3.6.

Input: *A positive definite unimodular Hermitian matrix M with coefficients in $\mathcal{O}$, specified by $a, d \in \mathbb{Z}$ and $b \in \mathcal{O}$ such that $M = \left(\begin{smallmatrix} a & b \\ \overline{b} & d \end{smallmatrix}\right)$.*

Output: *The reduced matrix congruent to M.*

1. *Set $a' = 1$.*
2. *Compute the set A' of vectors $\mathbf{x} = (x_1, x_2) \in \mathcal{O}^2$ such that $\mathbf{x}^* M \mathbf{x} = a'$ and such that x_1 and x_2 generate the unit ideal of $\mathcal{O}$. If $A' = \emptyset$, increment a' and repeat.*
3. *Set $d' = a'$.*
4. *Compute the set D' of vectors $\mathbf{y} = (y_1, y_2) \in \mathcal{O}^2$ such that $\mathbf{y}^* M \mathbf{y} = d'$ and such that y_1 and y_2 generate the unit ideal of $\mathcal{O}$. If $D' = \emptyset$, increment d' and repeat.*
5. *Initialize $\mathcal{M}$ to be the empty set.*
6. *For each $\mathbf{x} \in A'$ and $\mathbf{y} \in D'$ such that $\mathbf{x}$ and $\mathbf{y}$ generate $\mathcal{O}^2$ as an $\mathcal{O}$-module, let M' be the matrix representing the Hermitian form M written on the basis $\mathbf{x}$, $\mathbf{y}$ of $\mathcal{O}^2$, and add M' to the set $\mathcal{M}$.*
7. *If $\mathcal{M}$ is empty, increment d' and return to Step (4).*
8. *Find the smallest element M' of $\mathcal{M}$ under the ordering of $\mathcal{H}$ defined above.*
9. *Output M'.*

Remark 3.7. In Steps (2) and (4) of Algorithm 3.6, we need to find vectors in $\mathcal{O}^2$ of a given length under the quadratic form specified by M. We note that this is a finite computation: if $\mathbf{x} = (x_1, x_2)$ satisfies $\mathbf{x}^* M \mathbf{x} = n$, with $M = \left(\begin{smallmatrix} a & b \\ \overline{b} & d \end{smallmatrix}\right)$, then

$$\mathrm{Norm}(ax_1 + bx_2) + \mathrm{Norm}(x_2) = an.$$

Thus, to solve $\mathbf{x}^* M \mathbf{x} = n$, we can simply enumerate all pairs $(u, v) \in \mathcal{O}^2$ with $\mathrm{Norm}(u) + \mathrm{Norm}(v) = an$, and keep those pairs for which $u - bv$ is divisible by a.

Note that solving $\mathbf{x}^* M \mathbf{x} = n$ can be done more quickly when the value of a is small. Thus, in Algorithm 3.6, once one finds a short vector $\mathbf{x} = (x_1, x_2)$ with x_1 and x_2 coprime, it is worthwhile to compute *any* vector $\mathbf{y}$ such that $\mathbf{x}$ and $\mathbf{y}$ generate $\mathcal{O}$, and to replace M with the congruent form obtained by rewriting M on the basis $\mathbf{x}, \mathbf{y}$.

Theorem 3.8. *Algorithm 3.6 terminates with the correct result.*

Proof. Let $M' = \left(\begin{smallmatrix} a' & b' \\ \overline{b'} & d' \end{smallmatrix}\right)$ be the reduced matrix congruent to M. If $P = \left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right)$ is an element of $\mathrm{GL}_2(\mathcal{O})$ such that $P^* M P = M'$, and if we set $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$, then $a' = \mathbf{x}^* M \mathbf{x}$ and $d' = \mathbf{y}^* M \mathbf{y}$. By the very definition of the ordering on $\mathcal{H}$, then, we want to find vectors $\mathbf{x}$ and $\mathbf{y}$, each with coordinates that are coprime to one another, such that $\mathbf{x}^* M \mathbf{x}$ is as small as possible and $\mathbf{y}^* M \mathbf{y}$ is as small as possible, given that $\mathbf{x}$ and $\mathbf{y}$ generate $\mathcal{O}^2$ as an $\mathcal{O}$-module. This is what the algorithm does. Finally, among all possible such pairs $(\mathbf{x}, \mathbf{y})$, we simply need to choose the one that gives the smallest matrix. □

Hayashida [Hay68] gives a formula for the number of isomorphism classes of indecomposable principal polarizations on E^2 in the case where E has CM by a maximal order.[3] Hayashida's proof does not immediately lead to a constructive method of finding polarizations representing the isomorphism classes, but simply knowing the number of isomorphism classes is the key to a straightforward algorithm for producing such representatives.

Algorithm 3.9.

Input: *A fundamental discriminant* $\Delta < 0$.

Output: *A list of reduced matrices representing the distinct congruence classes of positive definite unimodular Hermitian matrices with entries in the order* $\mathcal{O}$ *of discriminant* Δ*, separated into the decomposable and indecomposable classes.*

1. *Compute the number* N *of indecomposable polarizations on* E^2 *using Hayashida's formula.*
2. *Compute the set* $\mathcal{D}$ *of reduced matrices representing decomposable polarizations, using Corollary 3.5 and Algorithm 3.6.*
3. *Initialize* $\mathcal{I}$ *to be the empty set and set* $P = 0$.
4. *Increment* P*, and compute the set* S *of elements of* $\mathcal{O}$ *of norm* $P - 1$.
5. *For every divisor* a *of* P *with* $a \leq P/a$*, and for every* $b \in S$:
   (a) *Compute the reduced form* M *of the matrix* $\left(\begin{smallmatrix} a & b \\ \overline{b} & P/a \end{smallmatrix}\right)$.

[3] There is a typographical error in Hayashida's paper. In the second line of page 43, the term $(1/4)(1 - (-1))^{(m^2-1)/8}$ should be $(1/4)(1 - (-1)^{(m^2-1)/8})h$. Note that the correction involves both moving a parenthesis and adding an instance of the variable h.

(b) *If M is not contained in $\mathcal{D} \cup \mathcal{I}$, then add M to the set $\mathcal{I}$.*

6. *If $\#\mathcal{I} < N$, then return to Step (4).*
7. *Return $\mathcal{D}$ and $\mathcal{I}$.*

Of course, for our goal of producing genus-2 curves over $\mathbb{Q}$ with Jacobians isomorphic to E^2, we only need the indecomposable polarizations.

Theorem 3.10. *Algorithm 3.9 terminates with the correct result.*

Proof. The algorithm is very straightforward. Every isomorphism class of principal polarization appears somewhere on the countable list that we are considering, and we simply enumerate the polarizations and compute their reduced forms until we have found the right number of isomorphism classes. □

Remark 3.11. In our applications, when the class group of $\mathcal{O}$ has exponent at most 2, we can speed up our algorithm as follows: once we have a principal polarization M on E^2, we can view the same matrix as giving a polarization on F^2 for any elliptic curve F with CM by $\mathcal{O}$. Since the class group has exponent at most 2, there exists an isomorphism $E^2 \to F^2$, and pulling M back to E^2 via such an isomorphism gives a new positive definite unimodular Hermitian matrix M'. Each time we find a new reduced polarization M, we compute the reduced forms of the polarizations M' associated to all the curves F isogenous to E, and add these reduced forms to the set $\mathcal{D}$ if they are new.

If φ is a principal polarization on E^2 and M is the corresponding Hermitian matrix, then the automorphism group of the polarized abelian variety (E^2, φ), denoted by $\mathrm{Aut}(E^2, \varphi)$, is isomorphic to the group $\{P \in \mathrm{GL}_2(\mathcal{O}) \mid P^* M P = M\}$. Note that if φ is indecomposable, so that (E^2, φ) is the polarized Jacobian of a curve C, then Torelli's theorem [Lau01, Appendix] shows that this group is also isomorphic to $\mathrm{Aut}(C)$. In any case, computing $\mathrm{Aut}(E^2, \varphi)$ is straightforward:

Algorithm 3.12.

Input: *A positive definite unimodular Hermitian matrix $M = \left(\begin{smallmatrix} a & b \\ \overline{b} & d \end{smallmatrix}\right)$ with entries in an imaginary quadratic maximal order $\mathcal{O}$.*

Output: *A list of all matrices $P \in \mathrm{GL}_2(\mathcal{O})$ such that $P^* M P = M$.*

1. *Compute the set A of vectors $\mathbf{x} = (x_1, x_2) \in \mathcal{O}^2$ such that $\mathbf{x}^* M \mathbf{x} = a$ and such that x_1 and x_2 generate the unit ideal of $\mathcal{O}$.*
2. *Compute the set D of vectors $\mathbf{y} = (y_1, y_2) \in \mathcal{O}^2$ such that $\mathbf{y}^* M \mathbf{y} = d$ and such that y_1 and y_2 generate the unit ideal of $\mathcal{O}$.*
3. *Initialize $\mathcal{A}$ to be the empty set.*
4. *For each $\mathbf{x} \in A$ and $\mathbf{y} \in D$ such that $\mathbf{x}$ and $\mathbf{y}$ generate $\mathcal{O}^2$ as an $\mathcal{O}$-module:*
   (a) *Compute $b' = \mathbf{x}^* M \mathbf{y}$.*
   (b) *If $b' = b$ then add the matrix $\left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right)$ to the set $\mathcal{A}$.*
5. *Output $\mathcal{A}$.*

(See Remark 3.7 for an explanation of how to implement the two first steps.)

Theorem 3.13. *Algorithm 3.12 terminates with the correct result.*

Proof. If $P = \left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathcal{O})$ satisfies $P^* M P = M$, then $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$ are vectors in $\mathcal{O}^2$ such that $\mathbf{x}^* M \mathbf{x} = a$ and $\mathbf{y}^* M \mathbf{y} = d$ and $\mathbf{x}^* M \mathbf{y} = b$. The algorithm simply enumerates all $\mathbf{x}$ and $\mathbf{y}$ that meet the first two conditions, and checks to see whether they meet the third. □

3.3. **Conditions on the polarization.** Throughout this section, E is an elliptic curve with CM by a maximal order $\mathcal{O}$ of an imaginary quadratic field K whose class group has exponent at most 2. Also φ is a principal polarization on E^2 corresponding (as in Proposition 3.1) to a positive definite unimodular Hermitian matrix M with entries in $\mathcal{O}$ and $\mathbf{M}$ is the field of moduli of the polarized abelian variety (E^2, φ). We resume our analysis of the condition that $\mathbf{M} = \mathbb{Q}$.

Proposition 3.14. *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be ideals of $\mathcal{O}$ representing all of the elements of the class group of $\mathcal{O}$, and for each i let $n_i \in \mathbb{Z}_{>0}$ generate $\mathrm{Norm}(\mathfrak{a}_i)$. Then $\mathbf{M} = \mathbb{Q}$ if and only if for every i there exists a matrix $P_i \in \mathrm{GL}_2(K)$, with entries in $\mathfrak{a}_i$, such that $n_i M = P_i^* M P_i$.*

Proof. Lemma 3.15 below shows that $\mathbf{M} = \mathbb{Q}$ if and only if $\mathbf{M} \subseteq K$, and this is the case if and only if for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ there exists an isomorphism $\alpha_\sigma \colon (E^2, \varphi) \to \big((E^\sigma)^2, \varphi^\sigma\big)$. To understand this condition, we use the classical theory of complex multiplication of abelian varieties; the book of Shimura and Taniyama [ST61] is one possible reference, especially Chapter II.

Under the embedding $\epsilon_0 \colon K \to \mathbb{C}$ we chose earlier, the isomorphism classes of elliptic curves over $\overline{\mathbb{Q}} \subset \mathbb{C}$ with CM by $\mathcal{O}$ correspond to the lattices $\epsilon_0(\mathfrak{a})$ up to scaling, for fractional ideals $\mathfrak{a}$ of $\mathcal{O}$. Since the class group of the order $\mathcal{O}$ is 2-torsion, we have $E^2 \simeq F^2$ for every E and F with CM by $\mathcal{O}$, so we may as well choose our E so that it corresponds to the trivial ideal $\mathcal{O}$.

Let Δ be the discriminant of $\mathcal{O}$ and let $\delta \in \mathcal{O}$ be a square root of Δ, chosen so that $\epsilon_0(\delta)$ is positive imaginary. Note that the trace dual $\mathfrak{a}^\dagger$ of an arbitrary fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is $(1/\delta)\mathfrak{a}^{-1}$. If F is the elliptic curve corresponding to $\mathfrak{a}$, then the dual of F is the elliptic curve corresponding to the complex conjugate of $\mathfrak{a}^\dagger$, and the canonical principal polarization of F is the isomorphism $\mathfrak{a} \to (1/\delta)\overline{\mathfrak{a}}^{-1}$ given by $x \mapsto x/(n\delta)$, where $n \in \mathbb{Q}$ is the positive generator of $\mathrm{Norm}(\mathfrak{a})$. (See [ST61, § 6.3] for more details.)

Let φ_0 be the product polarization on E^2. For $\alpha_\sigma \colon E^2 \to (E^\sigma)^2$ to give an isomorphism between (E^2, φ) and $\big((E^\sigma)^2, \varphi^\sigma\big)$, the following diagram must be commutative:

$$\begin{array}{ccccc} E^2 & \xrightarrow{M} & E^2 & \xrightarrow{\varphi_0} & \widehat{E}^2 \\ \downarrow{\scriptstyle \alpha_\sigma} & & & & \uparrow{\scriptstyle \widehat{\alpha}_\sigma} \\ (E^\sigma)^2 & \xrightarrow{M} & (E^\sigma)^2 & \xrightarrow{\varphi_0^\sigma} & (\widehat{E}^\sigma)^2. \end{array}$$

To express this diagram in terms of lattices, we let $\mathfrak{a}$ be an ideal corresponding to E^σ, we let $n = \mathrm{Norm}(\mathfrak{a})$, and we let P_σ be the matrix in $\mathrm{GL}_2(K)$ corresponding to α_σ. Then the preceding diagram becomes

$$\begin{array}{ccccc} \mathcal{O} \times \mathcal{O} & \xrightarrow{M} & \mathcal{O} \times \mathcal{O} & \xrightarrow{1/\delta} & (1/\delta)(\mathcal{O} \times \mathcal{O}) \\ \downarrow{\scriptstyle P_\sigma} & & & & \uparrow{\scriptstyle P_\sigma^*} \\ \mathfrak{a} \times \mathfrak{a} & \xrightarrow{M} & \mathfrak{a} \times \mathfrak{a} & \xrightarrow{1/(n\delta)} & (1/\delta)(\overline{\mathfrak{a}}^{-1} \times \overline{\mathfrak{a}}^{-1}). \end{array}$$

Thus, there exists an isomorphism $(E^2, \varphi) \to \big((E^\sigma)^2, \varphi^\sigma\big)$ of polarized varieties if and only if there exists a matrix P, with entries in $\mathfrak{a}$, such that $nM = P^* M P$. Since the Galois group of $\overline{\mathbb{Q}}/K$ acts transitively on the set of elliptic curves with CM

by $\mathcal{O}$, the field of moduli of (E^2, φ) is contained in K if and only if we can find such a matrix P for each of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$. □

Lemma 3.15. *Let E, φ, and $\mathbf{M}$ be as mentioned at the beginning of this section. Then $\mathbf{M} = \mathbb{Q}$ if and only if $\mathbf{M} \subseteq K$.*

Proof. Let us assume that $\mathbf{M} \subseteq K$; we must show that $\mathbf{M} = \mathbb{Q}$. Since $\mathcal{O}$ has a class group of exponent at most 2, [Shi71, Exercise 5.8, p. 124] implies that $\mathbb{Q}\big(j(E)\big)$ is totally real. Let ι be any complex conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so that ι acts trivially on $\mathbb{Q}(j(E))$ and nontrivially on K. Given any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we want to show that $(E^2, \varphi) \simeq ((E^\sigma)^2, \varphi^\sigma)$.

If σ acts trivially on K, then such an isomorphism exists, because $\mathbf{M} \subseteq K$. Otherwise, $\sigma\iota$ acts trivially on K, and we have $(E^2, \varphi) \simeq ((E^{\sigma\iota})^2, \varphi^{\sigma\iota})$, and therefore $((E^\iota)^2, \varphi^\iota) \simeq ((E^\sigma)^2, \varphi^\sigma)$. So it is enough for us to show that $(E^2, \varphi) \simeq ((E^\iota)^2, \varphi^\iota)$. If we choose our model of E to be defined over $\mathbb{Q}(j(E))$, then $E^\iota = E$, and we simply need to show that there exists an element P of $\mathrm{GL}_2(\mathcal{O})$ such that $\overline{M} = P^* M P$. If $M = \left(\begin{smallmatrix} a & b \\ b & d \end{smallmatrix}\right)$, we can simply take $P = \left(\begin{smallmatrix} b & d \\ -a & -b \end{smallmatrix}\right)$. □

At this point, we have reviewed enough CM theory to prove Corollary 3.5.

Proof of Corollary 3.5. We are given an ideal $\mathfrak{a} = (n, \alpha)$ of $\mathcal{O}$, where $n \in \mathbb{Z}$ is the norm of $\mathfrak{a}$ and where $\alpha \in \mathcal{O}$, and we have $x, y \in \mathbb{Z}$ such that $xn^2 - y\,\mathrm{Norm}(\alpha) = n$. The complex conjugate $\overline{\mathfrak{a}}$ of $\mathfrak{a}$ represents the inverse of the class of $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$, and the matrix $P = \left(\begin{smallmatrix} n & y\alpha \\ \overline{\alpha} & xn \end{smallmatrix}\right)$ takes the lattice $\mathcal{O} \times \mathcal{O} \subset K^2$ onto the lattice $\mathfrak{a} \times \overline{\mathfrak{a}}$. The dual lattice for $\mathfrak{a} \times \overline{\mathfrak{a}}$ is $(n\delta)^{-1} \cdot (\mathfrak{a} \times \overline{\mathfrak{a}})$ (where δ is the positive imaginary square root of Δ as in the proof of Proposition 3.14) and the product polarization from $\mathfrak{a} \times \overline{\mathfrak{a}}$ to its dual is simply multiplication by $1/(n\delta)$. Pulling this polarization back to $\mathcal{O} \times \mathcal{O}$ via P gives us the polarization $(n\delta)^{-1} P^* P$. Since the product polarization on $\mathcal{O} \times \mathcal{O}$ is $1/\delta$, the pullback polarization is represented by the endomorphism $(1/n) P^* P$ of $\mathcal{O} \times \mathcal{O}$, and we compute that $(1/n) P^* P$ is the matrix given in the statement of the corollary. □

We close this section by indicating how we can check the criterion given in Proposition 3.14: namely, given the polarization matrix M and an ideal $\mathfrak{a}$ with $\mathrm{Norm}(\mathfrak{a}) = n\mathbb{Z}$, how can we determine whether there exists a matrix $P \in M_2(\mathfrak{a})$ that satisfies $nM = P^* M P$?

Suppose there exists such a matrix P. If $M = \left(\begin{smallmatrix} a & b \\ b & d \end{smallmatrix}\right)$ let us take $L = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, so that $L^* L = aM$. Let $Q = LPL^{-1}$. Then the condition $nM = P^* M P$ becomes the condition $n\,\mathrm{Id} = Q^* Q$. This equality can only hold if Q is of the form

$$Q = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in GL_2(K)$$

where $x, y, z, t \in K$ satisfy $\mathrm{Norm}(x) + \mathrm{Norm}(z) = \mathrm{Norm}(y) + \mathrm{Norm}(t) = n$ and $\overline{x}y + \overline{z}t = 0$. Since we have

$$P = L^{-1} Q L = \begin{pmatrix} x - bz & \frac{bx + y - b^2 z - bt}{a} \\ az & bz + t \end{pmatrix} \in M_2(\mathfrak{a}),$$

we see that we must have $x = X/a$, $y = Y/a$, $z = Z/a$, and $t = T/a$ with $X, Y, Z, T \in \mathfrak{a}$.

Therefore, to check whether a matrix P with the desired properties exists, it suffices to compute and store all solutions $(X, Z) \in \mathfrak{a} \times \mathfrak{a}$ to the norm equation $\mathrm{Norm}(X) + \mathrm{Norm}(Z) = a^2 n$ (which can be done efficiently). Then, for every two

solutions (X, Z) and (Y, T) satisfying $\overline{X}Y + \overline{Z}T = 0$, we can check whether the corresponding matrix P lies in $M_2(\mathfrak{a})$. If we obtain such a P for each of the ideals $\mathfrak{a}_i$ from Proposition 3.14, then the field of moduli for (E^2, φ) is $\mathbb{Q}$. In fact, we need only find a P for each $\mathfrak{a}_i$ in a set that generates the class group of $\mathcal{O}$.

3.4. **Results.** We have implemented the algorithms described in the previous sections. We were able to test all polarizations on the 65 possible orders identified in Section 2. The results are presented in Table 2.

h	Δ	$\#\varphi$	$\#C$	h	Δ	$\#\varphi$	$\#C$	h	Δ	$\#\varphi$	$\#C$
1	−3	0	0	4	−84	2	0	8	−420	10	0
	−4	0	0		−120	5	3		−660	16	0
	−7	0	0		−132	3	1		−840	22	0
	−8	1	1		−168	4	0		−1092	22	0
	−11	1	1		−195	8	0		−1155	32	0
	−19	1	1		−228	5	1		−1320	36	0
	−43	2	2		−280	14	0		−1380	34	0
	−67	3	3		−312	11	1		−1428	28	0
	−163	7	7		−340	14	0		−1540	46	0
					−372	8	0		−1848	46	0
2	−15	0	0		−408	14	0		−1995	56	0
	−20	1	1		−435	16	0		−3003	72	0
	−24	1	1		−483	12	0		−3315	128	0
	−35	2	0		−520	25	3				
	−40	2	2		−532	14	0	16	−5460	128	0
	−51	2	0		−555	20	0				
	−52	2	2		−595	28	2				
	−88	4	2		−627	16	0				
	−91	4	0		−708	15	1				
	−115	6	0		−715	36	0				
	−123	4	0		−760	41	1				
	−148	5	3		−795	28	2				
	−187	8	0		−1012	28	0				
	−232	9	5		−1435	64	0				
	−235	12	0								
	−267	8	0								
	−403	18	0								
	−427	16	0								

TABLE 2. The number of indecomposable principal polarizations φ and the number of isomorphism classes of curves C with field of moduli $\mathbb{Q}$ for each discriminant Δ, grouped by class number h.

There exist 1226 indecomposable polarizations, in total. Our algorithms, implemented in `Magma` on a laptop with a 2.50 GHz Intel Core i7-4710MQ processor, took less than 21 minutes to compute all of the polarizations; about 10 minutes of that time was spent on the largest discriminant. The computation required about 2.8 GB of memory.

Once we computed the polarizations, it took about 26 minutes (on the same laptop) to check the conditions of Proposition 3.14. For this calculation, the largest discriminant represented more than two-thirds of the computation time.

In the end, we obtained exactly 46 polarizations φ such that the principally polarized abelian surface (E^2, φ) is isomorphic to the Jacobian of a curve C with field of moduli $\mathbb{Q}$. These 46 curves are obtained only from orders whose class groups have order 1, 2, or 4.

4. Computation of invariants and final remarks

4.1. **Invariants of the genus-2 curves C.** A genus-2 curve C has field of moduli $\mathbb{Q}$ if and only if all of its absolute invariants are defined over $\mathbb{Q}$ (see for example [LRS12, § 3]). This is in particular true for the triplet (g_1, g_2, g_3) of invariants defined by Cardona and Quer in [CQ05], which characterizes a genus-2 curve up to $\overline{\mathbb{Q}}$-isomorphism and enables one to find an equation $y^2 = f(x)$ for the curve. We quickly review here a strategy for obtaining the Cardona–Quer invariants for the 46 curves whose invariants are $\mathbb{Q}$-rational.

The first quantity we are able to derive is a Riemann matrix τ, using the same method as [Rit10, § 3.3]. Starting with the positive definite unimodular Hermitian matrix M corresponding to the polarization $\varphi = \varphi_0 \cdot M$, we obtain the Riemann matrix τ associated to φ and the CM-elliptic curve $E \simeq \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\omega)$ where $\omega = (1 + \sqrt{\Delta})/2$ if Δ is odd and $\omega = \sqrt{\Delta}$ otherwise.

This matrix we get is defined up to the action of the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$. One then works out a matrix τ_0 in the orbit of τ for which the computation of the theta constants $(\theta_i)_{0\le i\le 9}$ at τ_0 is fast (see [Lab16] for instance).

A complex model of a curve $C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ with Riemann matrix τ_0 can then be classically approximated using Rosenhain's formulas [Ros51, p. 417]

$$\lambda_1 = \frac{\theta_0^2\theta_2^2}{\theta_1^2\theta_3^2}, \qquad \lambda_2 = \frac{\theta_2^2\theta_7^2}{\theta_3^2\theta_9^2}, \qquad \text{and} \qquad \lambda_3 = \frac{\theta_0^2\theta_7^2}{\theta_1^2\theta_9^2}.$$

By computing the theta constants to higher and higher precision, we are able to get a sufficiently good approximation of the Cardona–Quer invariants to recognize them as rationals. The numbers we get are *a priori* only heuristic as there is no bound known for the denominators of these rationals; however, we can sometimes prove that these heuristic values are correct, as follows.

Given a set of Cardona–Quer invariants that we suspect are equal to the invariants of a curve whose Jacobian is isomorphic to E^2 for an E with complex multiplication, we can easily produce a curve C having those invariants. Then we can use the techniques of [CMSV17] to provably compute the endomorphism ring of the Jacobian of C. If this endomorphism ring is isomorphic to the ring $M_2(\mathrm{End}\, E)$, then we have provably found a curve of the type we are looking for.

We computed heuristic values for the Cardona–Quer invariants of our 46 principally polarized abelian surfaces, and the list of these invariants is available on authors' web pages, together with all the programs to compute them. We are grateful to J. Sijsling for computing the endomorphism rings for the Jacobians of 13 of our 46 curves; he is currently developing a faster and more robust algorithm which should be able to handle the remaining cases. For each of these 13 curves, the

endomorphism ring was $M_2(\operatorname{End} E)$, so the heuristic values of the Cardona–Quer invariants of these curves are provably correct.

We observe for that the 13 provably-correct sets of invariants, all the denominators are smooth integers. It would be very interesting, in the same spirit as [GL07, LV15] for the CM genus-2 case, to find formulas to explain the prime powers dividing these denominators. An example of such a closed formula appears in the introduction of [Rod00] without any details. The denominators of the 33 sets of invariants that we have not proven to be correct also are smooth, which provides some further heuristic evidence that the values are correct.

We present in Table 3 the invariants for a few of the curves we could provably compute.

Δ	M	Cardona–Quer invariants $[g_1, g_2, g_3]$
-8	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 2 \end{pmatrix}$	$[2^4\cdot 5^5, 2\cdot 3\cdot 5^4, -5^3]$
-11	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 2 \end{pmatrix}$	$\left[\frac{19^5}{2^2}, \frac{3^2\cdot 11\cdot 19^3}{2^5}, -\frac{19^2\cdot 47}{2^6}\right]$
-19	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 3 \end{pmatrix}$	$\left[\frac{5^5\cdot 29^5}{2^2\cdot 3^7}, \frac{5^3\cdot 7\cdot 29^3\cdot 31\cdot 73}{2^5\cdot 3^8}, -\frac{5^2\cdot 17\cdot 29^2\cdot 2719}{2^6\cdot 3^{10}}\right]$
-20	$\begin{pmatrix} 2 & \omega \\ -\omega & 3 \end{pmatrix}$	$\left[\frac{5^5\cdot 7^5}{2^2}, \frac{5^5\cdot 7^3\cdot 11}{2^5}, -\frac{3\cdot 5^3\cdot 7^2}{2^6}\right]$
-24	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 4 \end{pmatrix}$	$\left[\frac{2^4\cdot 23^5}{3}, \frac{2\cdot 23^3\cdot 421}{3^2}, -\frac{23^2\cdot 37}{3^4}\right]$
-40	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 6 \end{pmatrix}$	$\left[\frac{2^4\cdot 5^5\cdot 43^5}{3^7}, \frac{2\cdot 5^4\cdot 43^3\cdot 6977}{3^8}, -\frac{5^4\cdot 13\cdot 43^2}{3^{10}}\right]$
-52	$\begin{pmatrix} 2 & \omega \\ -\omega & 7 \end{pmatrix}$	$\left[\frac{5^5\cdot 173^5}{2^2\cdot 3^7}, \frac{5^4\cdot 173^3\cdot 112061}{2^5\cdot 3^8}, -\frac{5^3\cdot 7\cdot 37\cdot 173^2}{2^6\cdot 3^{10}}\right]$

TABLE 3. Cardona–Quer invariants for seven of the 46 genus-2 curves with field of moduli $\mathbb{Q}$ whose Jacobians are isomorphic to E^2, where E has CM by a maximal order $\mathcal{O}$. The discriminant of $\mathcal{O}$ is Δ, the corresponding principal polarization on E^2 is $\varphi_0 \cdot M$, and ω denotes either $\sqrt{\Delta}/2$ or $(1+\sqrt{\Delta})/2$, depending on whether Δ is even or odd.

4.2. **When is $\mathbb{Q}$ also a field of definition for C?** To conclude let us consider any of the 46 previous pairs (A, φ). We know that there exists a genus-2 curve $C/\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ such that $(\operatorname{Jac}(C), j) \simeq_{\overline{\mathbb{Q}}} (A, \varphi)$, where j is the canonical polarization on $\operatorname{Jac}(C)$. If the order of $\operatorname{Aut}(A, \varphi) \simeq \operatorname{Aut}(C)$ is larger than 2, then it is known [CQ05] that the field of moduli of C is a field of definition and that there exists a genus-2 curve $C_0 \colon y^2 = f(x)$ with $f \in \mathbb{Q}[x]$ such that $(\operatorname{Jac}(C_0), j_0) \simeq_{\overline{\mathbb{Q}}} (A, \varphi)$. In particular $\mathbb{Q}$ is also a field of definition for (A, φ).

Proposition 4.1 (Compare to [Rod00, § 4]). *The field $\mathbb{Q}$ is a field of definition of C — and therefore of (A,φ) — if and only if the order of $\mathrm{Aut}(A,\varphi) \simeq \mathrm{Aut}(C)$ is larger than 2.*

Proof. It remains to prove that when $\mathrm{Aut}(A,\varphi) = \{\pm 1\}$, there is no model of (A,φ) over $\mathbb{Q}$. Actually we show there is even no model (B,μ) over $\mathbb{R}$. Indeed, an isomorphism $\psi : (A,\varphi)/\mathbb{C} \to (B,\mu)/\mathbb{R}$, defined over $\mathbb{C}$, would induce an isomorphism

$$\alpha_\iota = (\psi^{-1})^\iota \circ \psi : (A,\varphi) \to (A,\varphi)^\iota,$$

for the complex conjugation ι, such that ${\alpha_\iota}^\iota \circ \alpha_\iota = \big((\psi^{-1}) \circ \psi^\iota\big) \circ \big((\psi^{-1})^\iota \circ \psi\big) = \mathrm{Id}$.

Since we have seen that $E^\iota = E$, the isomorphism α_ι can be represented as a matrix $P \in \mathrm{GL}_2(\mathcal{O})$ such that $\overline{P}P = \mathrm{Id}$. Moreover the commutativity of the diagram

$$\begin{array}{ccc} E^2 & \xrightarrow{\varphi} & \widehat{E}^2 \\ {\scriptstyle \alpha_\iota}\downarrow & & \uparrow{\scriptstyle \widehat{\alpha}_\iota} \\ E^2 & \xrightarrow{\varphi^\iota} & \widehat{E}^2. \end{array}$$

translates into the equality $P^*\overline{M}P = M$. If we denote $M = \left(\begin{smallmatrix} a & b \\ b & d \end{smallmatrix}\right)$, then it is easy to see that the matrix $P_0 = \left(\begin{smallmatrix} \overline{b} & d \\ -a & -b \end{smallmatrix}\right)$ satisfies the last equality. Any other $P = P_0 R$ differs from P_0 by an automorphism R of (A,φ) since $R^*P^*\overline{M}PR = R^*MR = M$. Because the automorphism group of (A,φ) is $\{\pm 1\}$, this means that the only possible P are $\pm P_0$. It is easy to check that $P_0\overline{P_0} = (-P_0)(-\overline{P_0}) = -\mathrm{Id}$, so the condition $\overline{P}P = \mathrm{Id}$ cannot be satisfied. □

4.3. **Provably correct equations for the curves defined over $\mathbb{Q}$.** Using Proposition 4.1 we found that exactly 13 of our curves can be defined over $\mathbb{Q}$, and these 13 are precisely the curves for which we could provably compute the invariants. This is no coincidence, as having an equation over $\mathbb{Q}$ definitely simplifies the computation. We present these curves in Table 4.

References

[Bai62] Walter L. Baily. On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves. *Annals of Mathematics*, 75(2):342–381, 1962.

[BILV16] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS Journal of Computation and Mathematics*, 19(A):283–300, 2016.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2004.

[BS17] Gaetan Bisson and Marco Streng. On polarised class groups of orders in quartic CM-fields. *Mathematical Research Letters*, 24(2):247–270, 2017.

[CMSV17] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. arXiv:1705.09248, 2017.

[CQ05] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In Tanush Shaska, editor, *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Series on Computing*, pages 71–83. World Scientific Publishers, Hackensack, NJ, 2005.

[FG18] Francesc Fité and Xavier Guitart. Fields of definition of elliptic k-curves and the realizability of all genus 2 Sato-Tate groups over a number field. *Transactions of the American Mathematical Society*, 370(7):4623–4659, 2018.

[GL07] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic CM fields. *Annales de l'Institut Fourier (Grenoble)*, 57(2):457–480, 2007.

Δ	M	d	Equation for C
-8	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 2 \end{pmatrix}$	1	$y^2 = x^5 + x$
-11	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 2 \end{pmatrix}$	$(-11)^{1/3}$	$y^2 = 2x^6 + 11x^3 - 2 \cdot 11$
-19	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 3 \end{pmatrix}$	-19	$y^2 = x^6 + 1026x^5 + 627x^4 + 38988x^3 - 627 \cdot 19x^2 + 1026 \cdot 19^2 x - 19^3$
-43	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 6 \end{pmatrix}$	-43	$y^2 = x^6 + 48762x^5 + 1419x^4 + 4193532x^3 - 1419 \cdot 43x^2 + 48762 \cdot 43^2 x - 43^3$
-67	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 9 \end{pmatrix}$	-67	$y^2 = x^6 + 785106x^5 + 2211x^4 + 105204204x^3 - 2211 \cdot 67x^2 + 785106 \cdot 67^2 x - 67^3$
-163	$\begin{pmatrix} 2 & \omega \\ -\omega+1 & 21 \end{pmatrix}$	-163	$y^2 = x^6 + 1635420402x^5 + 5379x^4 + 533147051052x^3 - 5379 \cdot 163x^2 + 1635420402 \cdot 163^2 x - 163^3$
-20	$\begin{pmatrix} 2 & \omega \\ -\omega & 3 \end{pmatrix}$	$\sqrt{5}$	$y^2 = x^5 + 5x^3 + 5x$
-24	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 4 \end{pmatrix}$	$\sqrt{2}$	$y^2 = 3x^5 + 8x^3 + 3 \cdot 2x$
-40	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 6 \end{pmatrix}$	$\sqrt{5}$	$y^2 = 9x^5 + 40x^3 + 9 \cdot 5x$
-52	$\begin{pmatrix} 2 & \omega \\ -\omega & 7 \end{pmatrix}$	$\sqrt{13}$	$y^2 = 9x^5 + 65x^3 + 9 \cdot 13x$
-88	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 12 \end{pmatrix}$	$\sqrt{2}$	$y^2 = 99x^5 + 280x^3 + 99 \cdot 2x$
-148	$\begin{pmatrix} 2 & \omega \\ -\omega & 19 \end{pmatrix}$	$\sqrt{37}$	$y^2 = 441x^5 + 5365x^3 + 441 \cdot 37x$
-232	$\begin{pmatrix} 2 & \omega+1 \\ -\omega+1 & 30 \end{pmatrix}$	$\sqrt{29}$	$y^2 = 9801x^5 + 105560x^3 + 9801 \cdot 29x$

TABLE 4. Genus-2 curves defined over $\mathbb{Q}$ with Jacobian isomorphic over $\overline{\mathbb{Q}}$ to E^2, where E has CM by a maximal order $\mathcal{O}$. The discriminant of $\mathcal{O}$ is Δ, the corresponding principal polarization on E^2 is $\varphi_0 \cdot M$, and ω denotes either $\sqrt{\Delta}/2$ or $(1+\sqrt{\Delta})/2$, depending on whether Δ is even or odd. This list is complete if the Generalized Riemann Hypothesis holds. Each curve is a double cover of its corresponding E (as can be seen by the fact that the upper-left entry of each polarization matrix is 2), and the associated involution of C is given by $(x, y) \mapsto (d/x, d^{3/2}y/x^3)$ for the value of d given in the third column.

[Hal74] Paul R. Halmos. *Finite-dimensional vector spaces*. Springer-Verlag, New York–Heidelberg, second edition, 1974. Undergraduate Texts in Mathematics.

[Hay68] Tsuyoshi Hayashida. A class number associated with the product of an elliptic curve with itself. *Journal of the Mathematical Society of Japan*, 20(1-2):26–43, 1968.

[HN65] Tsuyoshi Hayashida and Mieao Nishi. Existence of curves of genus two on a product of two elliptic curves. *Journal of the Mathematical Society of Japan*, 17(1):1–16, 1965.

[Hof91] Detlev W. Hoffmann. On positive definite Hermitian forms. *Manuscripta Mathematica*, 71(4):399–429, 1991.

[Hoy63] William L. Hoyt. On products and algebraic families of Jacobian varieties. *Annals of Mathematics*, 77(3):415–423, 1963.

[Kan11] Ernst Kani. Products of CM elliptic curves. *Collectanea mathematica*, 62(3):297–339, 2011.

[Kan14] Ernst Kani. Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *Journal of Number Theory*, 139:138–174, 2014.

[Kan16] Ernst Kani. The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collectanea mathematica*, 67(1):21–54, 2016.

[Kıl16] Pınar Kılıçer. *The CM class number one problem for curves*. PhD thesis, Leiden University, Netherlands, 2016.

[KLL+17] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbf{Q}$ with complex multiplication. arXiv:1701.06489, 2017.

[Koi72] Shoji Koizumi. The fields of moduli for polarized abelian varieties and for curves. *Nagoya Mathematical Journal*, 48:37–55, 1972.

[KS15] Pınar Kılıçer and Marco Streng. The CM class number one problem for curves of genus 2. arXiv:1511.04869, 2015.

[KW05] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Mathematics of Computation*, 74(249):499–518, 2005.

[Lab16] Hugo Labrande. *Explicit computation of the Abel-Jacobi map and its inverse*. PhD thesis, Université de Lorraine, Nancy, France, 2016.

[Lan06] Herbert Lange. Principal polarizations on products of elliptic curves. In José M. Mu noz Porras, Sorin Popescu, and Rubí E. Rodríguez, editors, *The geometry of Riemann surfaces and abelian varieties*, volume 397 of *Contemporary Mathematics*, pages 153–162. American Mathematical Society, Providence, RI, 2006.

[Lau01] Kristin Lauter. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *Journal of Algebraic Geometry*, 10(1):19–36, 2001. With an appendix by Jean-Pierre Serre.

[Lou90] Stephane Louboutin. Minorations (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratiques imaginaires. Application. *Comptes Rendus de l'Académie des Sciences de Paris. Série I. Mathématique*, 310(12):795–800, 1990.

[LRS12] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent. In Everett W. Howe and Kiran S. Kedlaya, editors, *Proceedings of the Tenth Algorithmic Number Theory Symposium — ANTS-X*, volume 1 of *Open Book Series*, pages 463–486. Mathematical Sciences Publishers, Berkeley, CA, 2012.

[LS16] Joan-Carlos Lario and Anna Somoza. A note on Picard curves of CM-type. arXiv:1611.02582, 2016.

[LV15] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *American Journal of Mathematics*, 137(2):497–533, 2015.

[MU01] Naoki Murabayashi and Atsuki Umegaki. Determination of all $\mathbf{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces. *Journal of Algebra*, 235(1):267–274, 2001.

[OU73] Frans Oort and Kenji Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *Journal of the Faculty of Science, University of Tokyo. Section 1A. Mathematics*, 20:377–381, 1973.

[Rit10] Christophe Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS Journal of Computation and Mathematics*, 13:192–207, 2010.

[Rod00] Fernando Rodriguez-Villegas. Explicit models of genus 2 curves with split CM. In Wieb Bosma, editor, *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, 2000, Proceedings*, pages 505–514, 2000.

[Ros51] Georg Rosenhain. Mémoire sur les fonctions de deux variables et à quatre périodes, qui sont les inverses des intégrales ultra-elliptiques de la première classe. *Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut National de France. Sciences mathématiques et physiques*, 11:361–468, 1851.

[Sch90] Peter Schuster. *Produkte elliptischer Kurven der Dimension 2 und 3*. PhD thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany, 1990.

[Sch98] Alexander Schiemann. Classification of Hermitian forms with the neighbour method. *Journal of Symbolic Computation*, 26(4):487–508, 1998.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1 of *Kanô memorial lectures*. Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Spa94] Anne-Monika Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Universität Duisburg-Essen, Germany, 1994.

[ST61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[vW99] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.

[Wei57] André Weil. *Zum Beweis des Torellischen Satzes*, volume 2 of *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse*. Vandenhoeck & Ruprecht, 1957.

[Wen01] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *Journal of the Ramanujan Mathematical Society*, 16(4):339–372, 2001.

Laboratoire de Mathématiques de Versailles, UVSQ, CNRS, Université Paris-Saclay, 45 avenue des États-Unis, 78035 Versailles, France.
E-mail address: alexandre.gelin@uvsq.fr
URL: https://alexgelin.github.io/

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92129-1967 U.S.A.
E-mail address: however@alumni.caltech.edu
URL: http://alumnus.caltech.edu/~however

IRMAR, Université de Rennes 1, Campus de Beaulieu, 263 avenue du Général Leclerc, 35042 Rennes Cedex, France.
E-mail address: christophe.ritzenthaler@univ-rennes1.fr
URL: https://perso.univ-rennes1.fr/christophe.ritzenthaler/

RANKS, 2-SELMER GROUPS, AND TAMAGAWA NUMBERS OF ELLIPTIC CURVES WITH $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$-TORSION

STEPHANIE CHAN, JEROEN HANSELMAN, AND WANLIN LI

Abstract. In 2016, Balakrishnan–Ho–Kaplan–Spicer–Stein–Weigandt [1] produced a database of elliptic curves over $\mathbb{Q}$ ordered by height in which they computed the rank, the size of the 2-Selmer group, and other arithmetic invariants. They observed that after a certain point, the average rank seemed to decrease as the height increased. Here we consider the family of elliptic curves over $\mathbb{Q}$ whose rational torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Conditional on GRH and BSD, we compute the rank of 92% of the 202,461 curves with parameter height less than 10^3. We also compute the size of the 2-Selmer group and the Tamagawa product, and prove that their averages tend to infinity for this family.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. After a suitable choice of isomorphism, we can always express such a curve in its short Weierstrass form:

$$E : y^2 = x^3 + a_4x + a_6$$

with $a_4, a_6 \in \mathbb{Z}$. Using this description, we define the naive height of the curve E as $h(E) := \max\{4|a_4|^3, 27a_6^2\}$.

In [1], the authors created an exhaustive database of isomorphism classes of elliptic curves with naive height up to $2.7 \cdot 10^{10}$, which contained a total of 238,764,310 curves. For each elliptic curve in this database, they computed the minimal model, the torsion subgroup, the conductor, the Tamagawa product, the rank, and the size of the 2-Selmer group. They plotted the average rank of the curves up to a certain height. Initially the average rank seemed to be an increasing function, but around a naive height of 10^9, they observed a turnaround point, where the average rank seemed to start decreasing as the height was increasing.

In this database however, there were no elliptic curves recorded with rational torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, which is the largest possible torsion subgroup for elliptic curves over $\mathbb{Q}$. The curve with minimal naive height that has such a torsion group has Weierstrass form $y^2 = x^3 - 1386747x + 368636886$ and its naive height is $10667230914617018892 \approx 1.07 \cdot 10^{19}$.

In this paper, we describe a similar database for the family of elliptic curves over $\mathbb{Q}$ whose rational torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. We can parametrize this family in the following way:

$$\mathcal{F} := \left\{ E : y^2 = x(x+1)(x+u^4) \;\middle|\; u = \frac{2t}{t^2-1}, \quad t \in \mathbb{Q} \setminus \{0, 1\} \right\}.$$

We call t the parameter of the curve and write $t = a/b$ for coprime integers a, b. This particular parametrization was provided by Bartosz Naskręcki, resulting from ideas in [16]. The family inherits a height function from its parametrization.

26 Jun 2018 15:28:28 PDT
Version 3 - Submitted to Open Book Series

For any $E \in \mathcal{F}$, we define the parameter height $H(E) := \max\{|a|, |b|\}$. For each isomorphism class of curves in this family, we will only consider the model in $\mathcal{F}$ for which H is minimal. From now on, we will call the family of curves represented by elements of $\mathcal{F}$ the $(2, 8)$-torsion family.

We use the parameter height, as it makes it easier to enumerate and compare curves in our family. The naive height of the curves in our family is very large, as could already be seen in the example mentioned above. We prove in Section 2 that

$$0.559 \cdot h(E)^{1/48} < H(E) < 0.672 \cdot h(E)^{1/48}.$$

We also show that the parameter height controls the size of the conductor $N(E)$:

$$N(E) < 1.161 \cdot H(E)^{10}.$$

From now on, we will use the term *height* to refer to the parameter height.

There are several reasons to consider the $(2, 8)$-torsion family. First, based on the relation between the parameter height and the naive height, restricting to this family allows us to quickly see curves of large naive height. Another advantage is that the existence of the rational torsion structure makes it easier to carry out 2-descent.

To provide an example, the 2000th curve in our database has parameter $t = 98/99$, naive height $6.39 \cdot 10^{107}$ and conductor $6.65 \cdot 10^{17}$. It would be more difficult to determine the rank for a curve of similar size without any special structure, and currently it would not be feasible to carry out such calculations in bulk.

In our family, we enumerated all 202,461 isomorphism classes of curves with height less than 1000. The average rank function seems to achieve its maximum at height 24, at the 121st curve, where the average rank peaks at 0.744. Among these, we determined the rank for 186,719 classes, conditional on GRH and BSD.

This particular family of elliptic curves was also studied in [7] and [12]. In [7], the authors were in search of rank 4 curves, but were unable to find any. To date, no rank 4 curve has yet been found in this family. In [12], the authors obtained statistical results on the 2-Selmer group, similar to our data in Section 5.2.

Main Results. We found that curves with height up to 100 in the $(2, 8)$-torsion family has average rank 0.626 (Figure 2 in Section 5.1) and with height up to 1000 have average rank between 0.508 and 0.663 (Figure 3 in Section 5.1). The first curves in the $(2, 8)$-torsion family with given rank r are

$$\begin{aligned}
r = 0 &: y^2 = x^3 - 1386747x + 368636886 && (t = 1/2),\\
r = 1 &: y^2 = x^3 - 64052311707x + 6090910426477494 && (t = 1/4),\\
r = 2 &: y^2 = x^3 - 4288450677931298 7x + 337937756079527 4084396534 && (t = 5/8),\\
r = 3 &: y^2 = x^3 - 204067285599545004845 07x \\
&\qquad + 1121060630379489735235148874483894 && (t = 12/17).
\end{aligned}$$

We found that no rank 4 curves can exist with height below 1000.

The curve with rank 3 with the greatest height found in our database has parameter $t = 841/1018$; its global minimal model is as follows:

$$\begin{aligned}
y^2 + xy = x^3 &- 153729452329750732156924947255990241355929710255 0x\\
&+ 7336366246333132846308148525227910550151380147382941246791656800601001 32.
\end{aligned}$$

This curve was found when we tried to compute the 2-Selmer rank of curves beyond height 1000. Currently, the curve with maximal height on the list of elliptic curves with high rank maintained by Dujella [10] has parameter $352/1017$.

The average size of the 2-Selmer group seems to be increasing rather slowly, but steadily. We prove the following theorem, which is an analogue of a result by Lemke-Oliver and Klagsbrun for the family of elliptic curves with 2-torsion [15].

Theorem 6.3. *The average size of the 2-Selmer group tends to infinity in the $(2,8)$-torsion family.*

Similarly, observing the data on the average Tamagawa product suggested the following theorem that we prove in Section 6.1:

Theorem 6.1. *The average Tamagawa product in the $(2,8)$-torsion family up to height N has order of magnitude $(\log N)^{33}$.*

Outline of the paper. In Section 2, we provide some properties of the $(2,8)$-torsion family related to our parametrization. In Section 3, we recall general results and conjectures related to ranks of elliptic curves. In Section 4, we discuss the computational methods we use. Section 5 contains the data we obtained and our analysis of the data. In Section 6, we prove that the average Tamagawa product and the average size of the 2-Selmer group tends to infinity for this family.

Acknowledgements. The authors would like to thank Jennifer Balakrishnan for suggesting the topic and the guidance through the work. We would like to thank Andrew Booker, Jordan Ellenberg, Tom Fisher, Andrew Granville, Wei Ho, Bartosz Naskręcki, Harald Schilly, Jeroen Sijsling, William Stein, Gonzalo Tornaría and John Voight for their advice and help. The authors are indebted to Zev Klagsbrun for the rank computation of the curve with parameter $t = 66/97$. The authors thank the organizers of the "Curves and L-functions" summer school held at ICTP in 2017, where this project began: Tim Dokchitser, Vladimir Dokchitser, and Fernando Rodriguez Villegas. We used the open-source software SageMath and CoCalc extensively throughout this project. Chan was supported by the European Research Council grant agreement No. 670239. Hanselman was supported by the research grant 7635.521(16) of the Science Ministry of Baden-Württemberg.

2. Some preliminary properties of the $(2,8)$-torsion family

In this section, we discuss the parametrization for the $(2,8)$-torsion family. We also show how the parameter height is related to the naive height and the conductor.

2.1. **The parametrization.** By expressing the torsion points explicitly, one can check that any curve with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$-torsion can be described as an element of $\mathcal{F}$. Conversely, given a curve in $\mathcal{F}$, it is a straightforward calculation to verify that

$$\left(\frac{2u}{(t+1)^2}, \frac{4t(t^2+2t-1)(t^2+1)}{(t+1)^5(t-1)^3}\right)$$

is a point of order 8. Hence the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

In each isomorphism class in $\mathcal{F}$, there are exactly 8 different choices of t. We get these representatives using the transformations $t \mapsto -t$, $t \mapsto 1/t$ and $t \mapsto (1-t)/(1+t)$. We choose the t corresponding to a curve with minimal height. The maps $t \mapsto -t$, $t \mapsto 1/t$ allow us to restrict $t = a/b$ to the range $(0,1)$. Assuming $a < b$, if $a \equiv b \equiv 1 \bmod 2$, the map $t \mapsto (1-t)/(1+t)$ allows us to take parameter

$t' = a'/b'$, where $a' = (b-a)/2$ and $b' = (a+b)/2$. Then t' would have a smaller height, since $a' < b' < b$. Thus, choosing $t = a/b \in (0,1)$ with a and b coprime with different parity, we get a unique representative for each isomorphism class.

With this choice of parameter, we see that the number of curves with height n is $\phi(n)$ if n is even and $\phi(n)/2$ if n is odd, where $\phi(n)$ is the Euler totient function. By [20], we have for any $\epsilon > 0$, the estimate

$$\sum_{n \leq N} \phi(n) = \frac{3}{\pi^2} N^2 + O(N(\log N)^{2/3}(\log\log N)^{4/3}).$$

Using the fact that $\phi(2n)$ is $\phi(n)$ if n is odd and $2\phi(n)$ if n is even, one can show that the total number of curves up to height N is

$$\frac{2}{\pi^2} N^2 + O(N(\log N)^{2/3}(\log\log N)^{4/3}).$$

2.2. **Naive height and parameter height.** Let E be a curve given by the equation $y^2 = x(x+1)(x+u^4)$ in $\mathcal{F}$ where $u = 2t/(t^2-1)$ and $t = a/b$ are chosen as above. We show how the naive height and parameter height are related.

Proposition 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve in $\mathcal{F}$, with naive height h and parameter height H. We have*

$$0.559 \cdot h^{1/48} < H < 0.672 \cdot h^{1/48}.$$

Proof. We start by giving a minimal Weierstrass model for our curve. Write $S = 2ab$ and $T = b^2 - a^2$, so $u = -S/T$. It follows that S and T are coprime where S is even and T is odd. We write E in short Weierstrass form $y^2 = x^3 - Ax + B$, by putting $A = 27(S^8 - S^4T^4 + T^8)$ and $B = 27(S^4 - 2T^4)(2S^4 - T^4)(S^4 + T^4)$.

One can check that there exists no prime p such that $p^4 \mid A$ and $p^6 \mid B$, therefore this Weierstrass form is minimal. With this, the naive height of E is given by:

$$h = 3^9 T^{24} \max\{4|1 - u^4 + u^8|^3, (1-2u^4)^2(2-u^4)^2(1+u^4)^2\}.$$

Since this expression is symmetric in S and T, first assume $S < T$, so that $u \in (0,1)$. Bounding the polynomials in u, we get $3^{12} \cdot T^{24}/16 \leq h \leq 4 \cdot 3^9 \cdot T^{24}$. Note also, $\max(S,T) = \max(2ab, b^2 - a^2) \in [2(\sqrt{2}-1)H^2, 2H(H-1)]$. Therefore $(\sqrt{2}-1)^{24} \cdot 3^{12} \cdot 2^{20} \cdot H^{48} < h < 3^9 \cdot 2^{26} \cdot H^{48}$, which gives the result. □

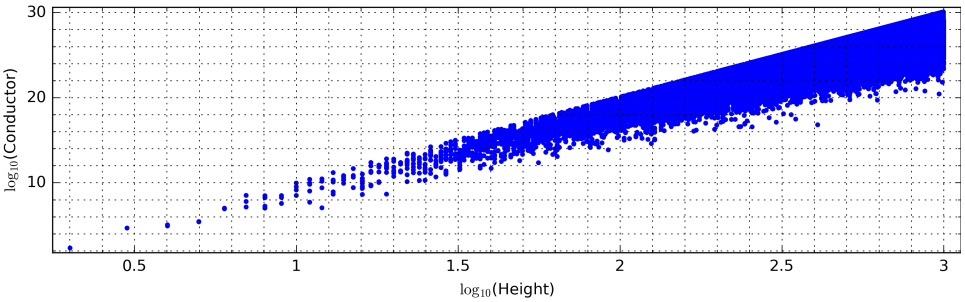


FIGURE 1. Conductor of isomorphism classes in the $(2,8)$-torsion family.

2.3. **Size of the conductor.** Consider a curve in $\mathcal{F}$ with parameter $t = a/b$, where a and b are coprime and of different parity. This curve is isomorphic to

$$E : y^2 = x(x+S^4)(x+T^4),$$

where $S = 2ab$ and $T = b^2 - a^2$ are coprime. The discriminant of E is $\Delta_E = 16S^8T^8(T^4 - S^4)^2$. By Tate's algorithm [18], this curve has bad reduction precisely at the primes dividing Δ_E, and the exponent of the conductor is always 1. Therefore the conductor of E is the product of primes dividing

$$ab(b^2-a^2)(a^2+b^2)(a^2-2ab-b^2)(a^2+2ab-b^2) = b^{10}t(1-t^2)(1+t^2)(t^2-2t-1)(t^2+2t-1).$$

The absolute value of the polynomial in t is bounded from above in the interval $(0, 1)$ by approximately 1.160. Hence $N(E) < 1.161 \cdot H(E)^{10}$.

3. Background

Computing the rank of an elliptic curve over a number field is a difficult problem, and while there are a number of techniques that work well in practice, there is no known algorithm to carry this out in general. Here we review the main theorems and conjectures and discuss how they can be used to give conditional results.

3.1. **The BSD Conjecture.** The most famous conjecture on ranks of elliptic curves is the Birch and Swinnerton-Dyer Conjecture (BSD) [4]. Let E be an elliptic curve defined over a number field with L-function $L(s, E)$. The BSD Conjecture states that the rank of E equals the order of vanishing of $L(s, E)$ at $s = 1$, which is called the *analytic rank* of E. Assuming this conjecture allows us to obtain an upper bound of the rank from the L-function.

3.2. **The Minimalist Conjecture and Current Results.** It is believed that the root number, i.e. the sign of the functional equation of $L(s, E)$, is 1 for half of all elliptic curves and -1 for the other half. The Minimalist Conjecture, initially formulated by Goldfeld [13] for the quadratic twists families, states that with respect to any reasonable ordering, half of the elliptic curves have rank 0 and half have rank 1. This would mean the average rank should tend to $1/2$, and 0% of elliptic curves have rank at least 2. One of our main goals is to provide numerical evidence for this conjecture for the $(2, 8)$-torsion family.

The following result of Bhargava and Shankar [2] on the upper bound of the average rank of elliptic curves provides strong evidence for the Minimalist Conjecture.

Theorem 3.1 (Bhargava–Shankar, [2])**.** *The average rank of all elliptic curves over* $\mathbb{Q}$ *ordered by naive height is at most* 0.885*.*

3.3. **The Selmer Group and Descent.** For each integer $n \geq 2$, the n-Selmer group $\mathrm{Sel}_n(E)$ of E over $\mathbb{Q}$ fits into an exact sequence of abelian groups

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \mathrm{Sel}_n(E) \to Ш(E)[n] \to 0, \tag{1}$$

where $Ш(E)[n]$ denotes the n-torsion subgroup of the Tate-Shafarevich group $Ш(E)$ of E over $\mathbb{Q}$. If p is a prime, then $\mathrm{Sel}_p(E)$ is an elementary abelian p-group, whose dimension as an $\mathbb{F}_p$-vector space is called the p-Selmer rank of E, which is effectively computable and provides an upper bound on the rank via (1).

Explicitly, an element in the n-Selmer group of E can be represented by a pair (C, π), where C is a genus 1 curve which is locally soluble and π is a map defined over $\mathbb{Q}$ that makes the following diagram commute:

$$\begin{array}{ccc} C & & \\ {\scriptstyle\simeq}\downarrow & \searrow^{\pi} & \\ E & \xrightarrow[[n]]{} & E \end{array}$$

In this diagram, the vertical map $C \to E$ is an isomorphism defined over $\overline{\mathbb{Q}}$. Determining (a lower bound for) the rank of E is equivalent to finding rational points on C. If no rational point of C can be found by a search by height, we apply the method of descent repeatedly. More generally, given a rational isogeny $\phi : E \to E'$, there is a Selmer group associated to it, denoted as $\mathrm{Sel}_\phi(E)$. For the dual isogeny $\hat{\phi} : E' \to E$ of ϕ, we denote the corresponding Selmer group as $\mathrm{Sel}_{\hat{\phi}}(E')$. The following is a standard result, see for example [17, Lemma 6.1].

Theorem 3.2. *Let E and E' be elliptic curves over $\mathbb{Q}$. Suppose there exists $\phi : E \to E'$ an isogeny of degree 2. Then the following sequence is exact:*

$$0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to \mathrm{Sel}_\phi(E/\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to \mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q}).$$

For $E \in \mathcal{F}$, we have $|E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2])| = 1$, which implies that

$$|\mathrm{Sel}_\phi(E/\mathbb{Q})| \leq |\mathrm{Sel}_2(E/\mathbb{Q})|.$$

Fisher [11] gives an efficient way to apply descent 6 times on elliptic curves with full 2-torsion structure. Moreover, since the $(2,8)$-torsion family has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ torsion, there are two isogenous curves with full 2-torsion structure. Applying Fisher's method to all three isogenous curves allowed us to determine the rank of more curves. Below is a picture of the isogenous curves and their torsion structures.

$$\begin{array}{ccc} E & & E_{\mathrm{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \\ \downarrow & & \downarrow \\ E' & & E'_{\mathrm{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ \downarrow & & \downarrow \\ E'' & & E''_{\mathrm{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{array}$$

There are also a number of recent results on the size of Selmer groups:

Theorem 3.3 (Bhargava–Shankar, [3])**.** *For $n \leq 5$, the average size of $\mathrm{Sel}_n(E)$ for all elliptic curves $E/\mathbb{Q}$ ordered by naive height is $\sigma(n)$, the sum of divisors of n.*

The theorem implies that the average size of the 2-Selmer group converges to $\sigma(2) = 3$. However, this no longer holds for the family with nontrivial 2-torsion.

Theorem 3.4 (Klagsbrun–Lemke Oliver, [15])**.** *The average size of $\mathrm{Sel}_2(E)$ is unbounded for the family of elliptic curves over $\mathbb{Q}$ with a torsion point of order 2 ordered by a parameter height* [1].

Our data suggests that the average size of the 2-Selmer group is also unbounded in the $(2,8)$-torsion family. In Section 6.2, we give a proof of this fact.

3.4. **The Tamagawa Number.** Let E be an elliptic curve over $\mathbb{Q}$. The *Tamagawa number* is the finite index $c_p(E) := \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$, where $E_0(\mathbb{Q}_p)$ is the subgroup of points in $E(\mathbb{Q}_p)$ which have good reduction. Each $c_p(E)$ can be easily computed from the coefficients of E using Tate's algorithm [18]. The *Tamagawa product* of E is

$$\mathcal{T}(E) = \prod_{p \leq \infty} c_p(E).$$

[1]The parameter height used here for an elliptic curve with a 2-torsion point $E_{A,B} : y^2 = x^3 + Ax^2 + Bx$, is $\max\{|A|, B^2\}$.

If there exists an isogeny $\phi : E \to E'$ of degree 2, then the *Tamagawa ratio* of E is

$$\mathcal{T}(E/E') = \frac{|\mathrm{Sel}_\phi(E)|}{|\mathrm{Sel}_{\hat{\phi}}(E')|}.$$

Consider the exact sequence induced by the isogeny ϕ:

$$0 \longrightarrow \ker(\phi) \longrightarrow E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, \ker(\phi)) \longrightarrow H^1(\mathbb{Q}, E) \longrightarrow \cdots.$$

Passing to a completion at a place p, we define

$$H^1_\phi(\mathbb{Q}_p, \ker\phi) := \delta_p(E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \subset H^1(\mathbb{Q}_p, \ker(\phi)).$$

Then the Tamagawa ratio can be related to the Tamagawa numbers as follows.

Theorem 3.5 (Cassels, [8], Lemma 3.1)**.** *The Tamagawa ratio decomposes into a product of local factors as follows:*

$$\mathcal{T}(E/E') = \prod_{p \le \infty} \mathcal{T}_p(E/E'), \quad \textit{where} \quad \mathcal{T}_p(E/E') = \frac{1}{2}\big|H^1_\phi(\mathbb{Q}_p, \ker\phi)\big|.$$

Theorem 3.6 (Dokchitser–Dokchitser, [9], Lemma 4.2 and 4.3)**.** *For $p \neq 2$ finite,*

$$\frac{1}{2}\big|H^1_\phi(\mathbb{Q}_p, \ker\phi)\big| = \frac{c_p(E')}{c_p(E)}.$$

4. Computing ranks

4.1. **Enumerating curves.** We produce a list of all isomorphism classes in $\mathcal{F}$ up to height N by computing the Farey sequence of order N to get a list of (a, b), where a and b are coprime and have opposite parities. Each pair (a, b) gives a curve in $\mathcal{F}$ of minimal height in its isomorphism class. This gives us 202,462 ordered isomorphism classes of $(2, 8)$-torsion curves with height less than 1000.

4.2. **Procedure.** To make our rank computations feasible, we assume two standard conjectures: the Birch and Swinnerton-Dyer Conjecture (BSD) and the generalized Riemann hypothesis (GRH). BSD allows us to obtain an upper bound of the rank by computing the analytic rank numerically. GRH provides the conjecturally best bound for the error term of the L-function attached to an elliptic curve, which improves the efficiency of the analytic rank computation. An immediate consequence of the BSD Conjecture is the Parity Conjecture, which states that the root number agrees with the parity of the rank. This allows us to determine the rank when the upper bound and lower bound we calculated for the rank differ by 1.

We computed the rank using a combination of Sage [19] and Magma [6]. We first ran Cremona's `mwrank` in Sage, which carries out 2-descent and searches for rational points with low height. This function gave us an upper bound and a lower bound for the rank of each curve in our database. If the bounds agreed, this determined the rank. If the bounds differed by 1, the rank is obtained conditional on the Parity Conjecture. This process determined the rank of 52.1% of the curves.

If the rank was not determined at this stage, we ran the `Sage` function `analytic_rank_upper_bound`, which computes an upper bound on the analytic rank conditional on GRH and takes a parameter Δ, using Bober's method in [5]. The runtime is exponential in Δ, but a higher Δ potentially gives a better bound. We ran the function repeatedly with increasing values of Δ up to at most 2.0, or

until the rank's upper bound differed from the lower bound by at most 1. After this stage, we still had 44.2% curves with unknown rank.

Because of the large number of curves remaining, it was computationally unfeasible to run with higher Δ for all of them. Restricting to curves with $H < 100$, only 153 remained at this stage, and we were able to continue the process up to $\Delta = 3.8$. After this, only 15 curves were left with $H < 100$. Computing the analytic rank becomes more difficult as the conductor increases. Since the parameter height appears to be positively correlated with the conductor, as is seen in Figure 1, it became more and more difficult to determine the rank the further we got along.

Since our curves have full rational 2-torsion, a recent implementation of Fisher's `TwoPowerIsogenyDescentRankBound` [11] in Magma is faster and a better fit for our purposes. Using this, we were able to determine the ranks of more than 90% of the curves up to $H < 1000$.

For the remaining curves, we returned to Sage. We ran analytic rank with higher values of Δ, up to at least 3.2, and do a further point search using a higher bound in the `mwrank` function `two_descent`. Altogether, the rank of 42.1% of the curves in our database was determined purely via descent, hence unconditionally.

Initially there was one curve left with $H < 100$: this is the curve with parameter $t = 66/97$. Thanks to Klagsbrun for suggesting the use of `AnalyticRank` in Magma, we are able to show that this curve has rank 0. The rank of all curves with $H < 100$ are determined conditional on GRH and BSD.

The list of high rank curves maintained by Dujella [10] contains 28 rank 3 curves, of which 26 has $H < 1000$. Our computations recovered the rank of 17 of them. The rank of the remaining 9 curves, which were all discovered by Fisher, were included in our database for completeness. In addition to the list, we found an extra rank 3 curve at $t = 9/296$.

5. Results and analysis of computed data

5.1. **Rank.** In the $(2, 8)$-torsion family, we very quickly observe a possible turnaround point in average rank. The average rank seems to peak at $H = 24$ with value 0.744, after 121 curves are computed, then steadily decreases to 0.626 at $H = 99$.

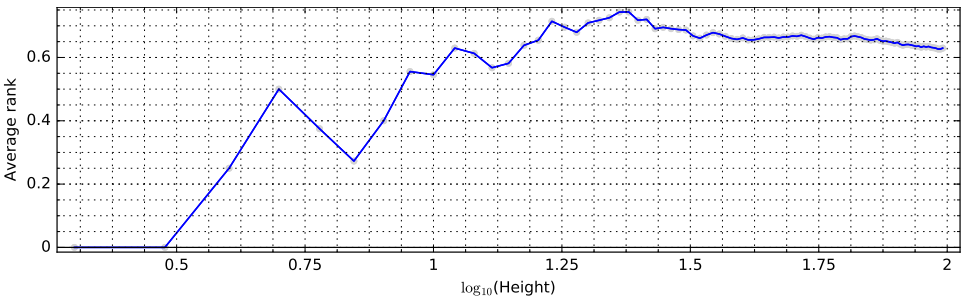


Figure 2. Average rank up to height 100 in the $(2, 8)$-torsion family.

Looking at all curves with $H < 1000$, the behaviour is less certain because of the number of curves with undetermined ranks: we are only able to compute the rank of 186,718 curves which is 92.2%. For the remaining curves, we have upper bounds and lower bounds from our computations. None of these upper bounds is greater than 3, so no rank 4 curve can exist with $H < 1000$. In Figure 3, we plot the computed upper and lower bounds for the average rank.

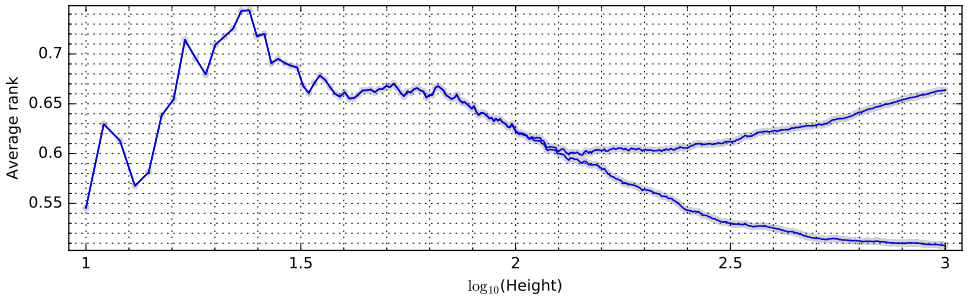


FIGURE 3. Average rank up to height 1000 in the $(2, 8)$-torsion family.

Rank	$H < 100$ (%)	$H < 250$ (%)	$H < 500$ (%)	$H < 1000$ (%)
0	865 (43.3)	5672 (45.0)	22143 (43.8)	84724 (41.8)
1	1021 (51.1)	6243 (49.5)	25108 (49.7)	101354 (50.1)
2	111 (5.6)	298 (2.4)	445 (0.9)	613 (0.3)
3	3 (0.2)	10 (0.1)	24 (0.0)	27 (0.0)
≥ 4	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Unknown	0 (0.0)	384 (3.0)	2845 (5.6)	15743 (7.8)
Total	2000(100.0)	12607(100.0)	50565(100.0)	202461(100.0)
Average	0.626	[0.545, 0.606]	[0.516, 0.628]	[0.508, 0.663]

TABLE 1. Rank distribution up to different heights.

5.2. **Size of the 2-Selmer group.** To get a clearer picture of the behaviour of the average size of the 2-Selmer group, we computed data beyond height 1000, and it seems to be divergent. In Section 6.2, we prove that this is indeed the case.

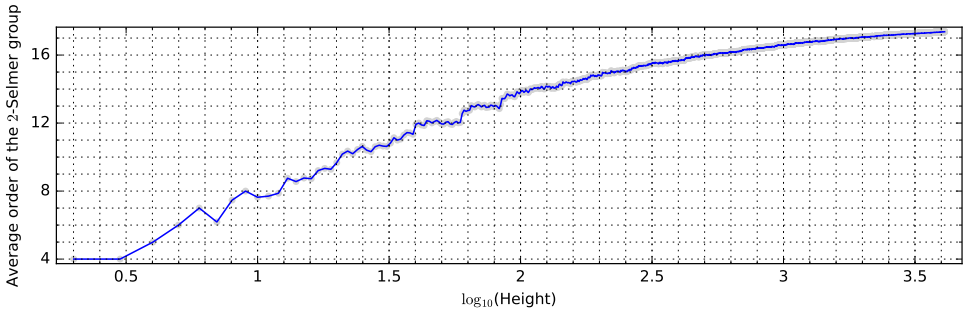


FIGURE 4. Average size of the 2-Selmer group in the $(2, 8)$-torsion family.

5.3. **Tamagawa product.** The average Tamagawa product in the $(2, 8)$-torsion family also behaves differently from the one in [1]. In their data, the average Tamagawa product peaks at 1.84 at naive height $6.3 \cdot 10^5$, then decreases with respect to the naive height. However in Figure 5, we see that it is increasing in the $(2, 8)$-torsion family, and that its value is much larger than 1.84. In Section 6.1, we show that the average Tamagawa product is unbounded for this family.

rank $\mathrm{Sel}_2(E)$	$H < 100$ (%)	$H < 1000$ (%)	$H < 2000$ (%)	$H < 4000$ (%)
2	346 (17.3)	29943 (14.8)	117397 (14.5)	462688 (14.3)
3	799 (40.0)	70856 (35.0)	278930 (34.4)	1107482 (34.2)
4	586 (29.3)	62903 (31.1)	252357 (31.1)	1009839 (31.2)
5	222 (11.1)	29287 (14.5)	120373 (14.9)	487277 (15.0)
6	44 (2.2)	7934 (3.9)	34104 (4.2)	142043 (4.4)
7	3 (0.2)	1386 (0.7)	6329 (0.8)	27823 (0.9)
8	0 (0.0)	147 (0.1)	811 (0.1)	3743 (0.1)
9	0 (0.0)	5 (0.0)	51 (0.0)	333 (0.0)
10	0 (0.0)	0 (0.0)	3 (0.0)	28 (0.0)
≥ 11	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Total	2000 (100)	202461 (100)	810352 (100)	3241228 (100)
Average $\lvert\mathrm{Sel}_2(E)\rvert$	13.728	16.574	17.055	17.361

TABLE 2. 2-Selmer rank distribution up to different heights.

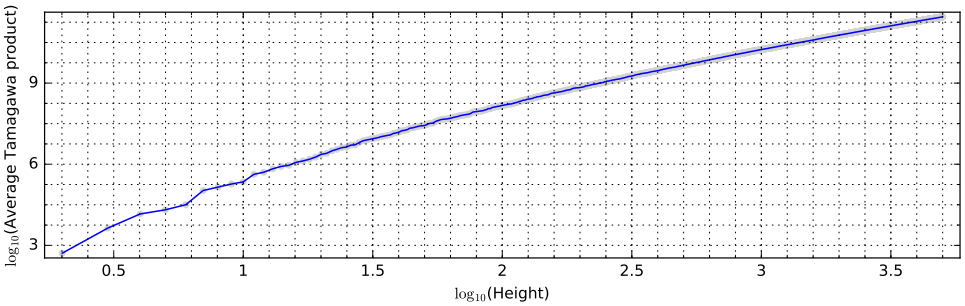


FIGURE 5. Average Tamagawa product in $\log_{10}$ scale in the $(2,8)$-torsion family.

5.4. **Root number.** The average root number appears to converge to 0, as shown in Figure 6.

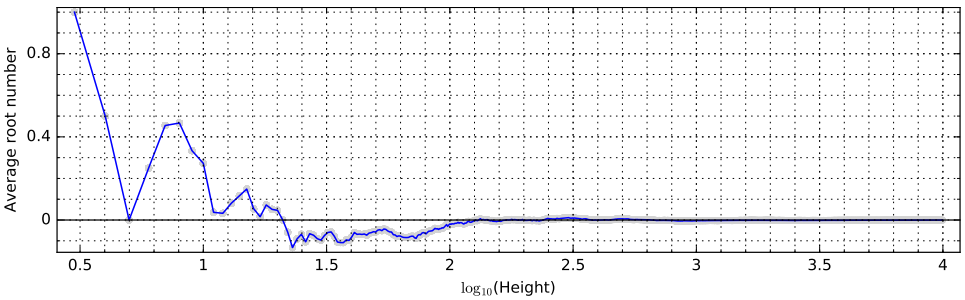


FIGURE 6. Average root number in the $(2,8)$-torsion family.

Root number	$H < 100$ (%)	$H < 1000$ (%)	$H < 10000$ (%)
1	976 (48.8)	100927 (49.9)	10125245 (50.0)
-1	1024 (51.2)	101534 (50.1)	10136574 (50.0)
Total	2000 (100)	202461 (100)	20261819 (100)
Average	-0.024000	-0.002998	-0.000559

TABLE 3. Root number distribution up to different heights.

6. Proofs

6.1. **The average Tamagawa product is unbounded.** To find the numbers $c_p(E)$, we apply Tate's algorithm [18]. We look at the model

$$E : y^2 - xy = x^3 + \frac{1}{4}\big(S^4 + T^4 - 1\big)x^2 + \frac{1}{16}S^4T^4x,$$

where $S = 2ab$ and $T = b^2 - a^2$. Again a and b are coprime and have opposite parities. The discriminant of E is $\Delta_E = \frac{1}{2^8}S^8T^8(T^4 - S^4)^2$. Note that S, T and $(T^4 - S^4)^2$ are pairwise coprime. By Tate's algorithm [18], we get

$$c_p = \begin{cases} v_p(\Delta_E) & \text{if } p \mid ST \text{ or } \Big(p \mid T^4 - S^4 \text{ and } \Big(\frac{-1}{p}\Big) = 1\Big), \\ 2 & \text{if } p \mid T^4 - S^4 \text{ and } \Big(\frac{-1}{p}\Big) = -1, \\ 1 & \text{otherwise.} \end{cases}$$

Combining the local factors $c_p(E)$, we get

$$\mathcal{T}(E) = \prod_p c_p(E) = \prod_{\substack{p \mid T^4 - S^4 \\ (\frac{-1}{p}) = -1}} 2 \prod_{\substack{p^k \| (T^4 - S^4)^2 \\ (\frac{-1}{p}) = 1}} k \prod_{p^l \| \frac{1}{2^8}S^8T^8} l.$$

Theorem 6.1. *The average Tamagawa product in the $(2, 8)$-torsion family up to height N has order of magnitude $(\log N)^{33}$.*

Proof. We estimate the sum

$$S(N) := \sum_{\substack{a,b \le N, 2 \mid a \\ (a,b)=1}} \prod_{\substack{p \mid T^4 - S^4 \\ (\frac{-1}{p}) = -1}} 2 \prod_{\substack{p^k \| (T^4 - S^4)^2 \\ (\frac{-1}{p}) = 1}} k \prod_{p^l \| \frac{1}{2^8}S^8T^8} l.$$

Let $H_1(a, b) = (a^2 - b^2 - 2ab)(a^2 - b^2 + 2ab)$, $H_2(a, b) = a^2 + b^2$ and $H_3(a, b) = ab(b-a)(b+a)$. Note that the factors $a^2-b^2-2ab, a^2-b^2+2ab, a^2+b^2, a, b, b-a, b+a$ are pairwise coprime. Let

$$f(H) = \prod_{\substack{p \mid H \\ (\frac{-1}{p}) = -1}} 2 \prod_{\substack{p^k \| H \\ (\frac{-1}{p}) = 1}} k \qquad \text{and} \qquad g(H) = \prod_{p^l \| H} l.$$

Let $P^+(x)$ and $P^-(x)$ denote the largest and smallest prime divisor of x respectively. Fix $\epsilon > 0$. Factorise $H_i(a, b)$ into d_i and $H_i(a, b)/d_i$, so that $P^-(d_i) < N^\epsilon$, and $P^+(H_i(a, b)/d_i) \ge N^\epsilon$. Then $\max_{a,b \le N}\{H_1(a, b)^2H_2(a, b)^4, H_3(a, b)^8\} \le N^{32}$, so $H_1(a, b)^2H_2(a, b)^4$ and $H_3(a, b)^8$ each has at most $32/\epsilon$ prime factors greater than N^ϵ. Therefore $f(d_1^2d_2^4) \le f(H_1(a, b)^2H_2(a, b)^4) \ll_\epsilon f(d_1^2d_2^4)$. Similarly $g(d_3^8) \le g(H_3(a, b)^8) \ll_\epsilon g(d_3^8)$. We have

$$\begin{aligned} S(N) &= \sum_{\substack{a,b \le N, 2 \mid a \\ (a,b)=1}} f(H_1(a, b)^2H_2(a, b)^4)g(H_3(a, b)^8) \\ &\asymp \sum_{\substack{d_1,d_2,d_3 \\ P^+(d_i) < N^\epsilon}} f(d_1^2d_2^4)g(d_3^8) \sum_{\substack{a,b \le N,\ 2 \mid a,\ (a,b)=1 \\ d_i \mid H_i(a,b) \\ P^-(\frac{H_i(a,b)}{d_i}) \ge N^\epsilon}} 1. \end{aligned}$$

Write $a = \alpha + ud_1d_2d_3$ and $b = \beta + vd_1d_2d_3$. Since H_1, H_2 and H_3 are pairwise coprime, we only need to look at coprime d_1, d_2 and d_3. Since H_1, H_2 are odd and

H_3 is even, we consider only odd d_1, d_2 and even d_3. Note that $a, b \mid H_3(a,b)$ by construction. Suppose $p \mid (a,b)$, then $p \mid d_2$ or $p > N^\epsilon$. We have

$$\sum_{\substack{a,b\le N\\ \exists p\ge N^\epsilon:\ p\mid(a,b)}} 1 = O\left(\sum_{p\ge N^\epsilon}\left(\frac{N}{p}\right)^2\right) = O(N^{2-\epsilon}).$$

We can exclude pairs of a and b with $P^-((a,b)) > N^\epsilon$ with a cost of $O(N^{2-\epsilon})$.

$$\sum_{\substack{a,b\le N,\ 2\mid a,\ (a,b)=1\\ d_i\mid H_i(a,b)\\ P^-(\frac{H_i(a,b)}{d_i})\ge N^\epsilon}} 1 = \sum_{\substack{\alpha,\beta<d_1d_2d_3\\ 2\mid\alpha,\ d_i\mid H_i(\alpha,\beta)\\ p\mid d_1d_2d_3\Rightarrow(p\nmid\beta \text{ or } p\nmid\alpha)}} \sum_{\substack{u,v<\frac{N}{d_1d_2d_3}\\ P^-(\frac{H_i(a,b)}{d_i})\ge N^\epsilon}} 1 + O(N^{2-\epsilon}).$$

By the small sieve [14, Theorem 2.6, p.85] we have

$$\sum_{\substack{u,v<\frac{N}{d_1d_2d_3}\\ P^-(\frac{H_i(a,b)}{d_i})\ge N^\epsilon}} 1 \asymp \frac{N^2}{d_1^2d_2^2d_3^2}\prod_{p<N^\epsilon}\left(1-\frac{7+\left(\frac{-1}{p}\right)+2\cdot\left(\frac{2}{p}\right)}{p}\right) \asymp \frac{N^2}{d_1^2d_2^2d_3^2(\log N)^7}.$$

It remains to compute

$$\sum_{\substack{\alpha,\beta<d_1d_2d_3\\ 2\mid\alpha,\ d_i\mid H_i(\alpha,\beta)\\ p\mid d_1d_2d_3\Rightarrow(p\nmid\beta \text{ or } p\nmid\alpha)}} 1 = \sum_{\substack{\alpha,\beta<d_1\\ d_1\mid H_1(\alpha,\beta)\\ p\mid d_1\Rightarrow(p\nmid\beta \text{ or } p\nmid\alpha)}} 1 \sum_{\substack{\alpha,\beta<d_2\\ d_2\mid H_2(\alpha,\beta)\\ p\mid d_2\Rightarrow(p\nmid\beta \text{ or } p\nmid\alpha)}} 1 \sum_{\substack{\alpha,\beta<d_3\\ 2\mid\alpha,\ d_3\mid H_3(\alpha,\beta)\\ p\mid d_3\Rightarrow(p\nmid\beta \text{ or } p\nmid\alpha)}} 1.$$

By the Chinese remainder theorem, it suffices to count the number of solutions of H_i modulo $p^v \| d_i$ for each prime p dividing d_i. We have

$$h_1(p^v) := \sum_{\substack{\alpha,\beta<p^v\\ p^v\mid H_1(\alpha,\beta)\\ p\nmid\beta \text{ or } p\nmid\alpha}} 1 = \begin{cases} 4\phi(p^v) & \text{if 2 is a square modulo } p^v,\\ 0 & \text{otherwise;}\end{cases}$$

$$h_2(p^v) := \sum_{\substack{\alpha,\beta<p^v\\ p^v\mid H_2(\alpha,\beta)\\ p\nmid\beta \text{ or } p\nmid\alpha}} 1 = \begin{cases} 2\phi(p^v) & \text{if } -1 \text{ is a square modulo } p^v,\\ 0 & \text{otherwise;}\end{cases}$$

$$h_3(p^v) := \sum_{\substack{\alpha,\beta<p^v\\ p^v\mid H_3(\alpha,\beta)\\ p\nmid\beta \text{ or } p\nmid\alpha}} 1 = \begin{cases} 4\phi(p^v) & \text{if } p\ne 2,\\ \phi(p^v) & \text{if } p = 2.\end{cases}$$

We extend h_1, h_2 and h_3 to multiplicative functions. Then the sum becomes

$$\begin{aligned} S(N) &\asymp \frac{N^2}{(\log N)^7}\sum_{\substack{d_1,d_2,d_3\\ P^+(d_i)<N^\epsilon}} \frac{f(d_1^2d_2^4)g(d_3^8)h_1(d_1)h_2(d_2)h_3(d_3)}{d_1^2d_2^2d_3^2}\\ &\asymp \frac{N^2}{(\log N)^7}\prod_{p<N^\epsilon}\left(1+\frac{f(p^2)h_1(p)}{p^2}\right)\left(1+\frac{f(p^4)h_2(p)}{p^2}\right)\left(1+\frac{g(p^8)h_3(p)}{p^2}\right)\\ &\asymp \frac{N^2}{(\log N)^7}\prod_{p<N^\epsilon}\left(1+\frac{1}{p}\right)^4\left(1+\frac{1}{p}\right)^4\left(1+\frac{1}{p}\right)^{32} \asymp N^2(\log N)^{33}. \end{aligned}$$

The total number of curves up to height N has order of magnitude N^2 as discussed in Section 2.1. Therefore the average Tamagawa product is of the size $(\log N)^{33}$. □

6.2. **The average size of the 2-Selmer group is unbounded.** We follow the approach in [15] to show the average Tamagawa ratio diverges in the $(2,8)$-torsion family, which implies that the average size of the 2-Selmer group is unbounded.

The curve obtained by the degree 2 isogeny $\phi : E \to E'$ corresponding to the rational subgroup generated by the point $(0,0)$ is

$$E' : y^2 - xy = x^3 + \frac{1}{4}\Big(\big(S^2+T^2\big)^2 + 4S^2T^2 - 1\Big)x^2 + \frac{1}{4}\Big(S^2T^2\big(S^2+T^2\big)^2\Big)x,$$

which has discriminant $\Delta_{E'} = \frac{1}{2^4}S^4T^4(T^4-S^4)^4$. Using Tate's algorithm and looking at Table 1 in [9], we find that the Tamagawa ratio for any finite prime p is

$$\mathcal{T}_p(E/E') = \frac{c_p(E')}{c_p(E)} = \begin{cases} 2 & \text{if } p \mid S^4 - T^4 \text{ and } \left(\frac{-1}{p}\right) = 1, \\ \frac{1}{2} & \text{if } p \mid ST, \\ 1 & \text{otherwise.} \end{cases}$$

Since the discriminants Δ_E and Δ'_E are both positive, we have $\mathcal{T}_\infty(E/E') = 1$.

Theorem 6.2. *The logarithmic Tamagawa ratio $t(a,b) := \log_2 \mathcal{T}(E/E')$ tends to a normal distribution with mean $-2\log\log N + O(1)$ and variance $6\log\log N + O(1)$.*

Before we turn to the proof, let us look at the application of Theorem 6.2. We find that $t(a,b)\log 2$ tends to a normal distribution with mean $\mu := -2(\log 2)(\log\log N) + O(1)$ and variance $\sigma^2 := 6(\log 2)^2 \log\log N + O(1)$.

Hence $\mathcal{T}(E/E') = \exp(t(a,b)\log 2)$ tends to a log-normal distribution which has mean $\exp(\mu + \frac{\sigma^2}{2}) = e^{O(1)}(\log N)^{(3\log 2 - 2)\log 2}$. Since $3\log 2 - 2 > 0$, the mean increases as N increases. From the discussion in Section 3.3, we know that $|\operatorname{Sel}_2(E)| \geq |\operatorname{Sel}_\phi(E)| \geq \mathcal{T}(E/E')$, so the following theorem is a corollary of Theorem 6.2.

Theorem 6.3. *The average size of the 2-Selmer group tends to infinity in the $(2,8)$-torsion family.*

Proof of Theorem 6.2. Let $H_1 = (a^2-b^2-2ab)(a^2-b^2+2ab)(a^2+b^2)$ and $H_2 = ab(b-a)(b+a)$. Throughout this proof, we will assume p is an odd prime as the contribution of the prime 2 can be taken into the error term. Define

$$f_p(H) := \mathbb{1}_{p|H} \cdot \mathbb{1}_{\left(\frac{-1}{p}\right)=1} \quad \text{and} \quad g_p(H) := \mathbb{1}_{p|H},$$

where $\mathbb{1}$ denotes the indicator function. Then

$$t(a,b) = f(H_1(a,b)) - g(H_2(a,b)), \text{ where } f(H) := \sum_p f_p(H) \text{ and } g(H) := \sum_p g_p(H).$$

For any function F and any property $\mathcal{P}$ defined on the set $\mathcal{A}_N := \{(a,b) : a,b \leq N,\ a \text{ and } b \text{ coprime and have opposite parities}\}$, define

$$\mathbb{P}_N(\mathcal{P}) = \frac{\sum_{(a,b)\in\mathcal{A}_N} \mathbb{1}_{\mathcal{P}(a,b)}}{|\mathcal{A}_N|} \quad \text{and} \quad \mathbb{E}_N(F) = \frac{\sum_{(a,b)\in\mathcal{A}_N} F(a,b)}{|\mathcal{A}_N|}.$$

Fix $\epsilon > 0$. For $p \leq N^\epsilon$, by counting the number of solutions of H_1, H_2 modulo p,

$$\mathbb{E}_N(f_p(H_1)) = \mathbb{P}_N(H_1 \equiv 0 \bmod p) = \begin{cases} \frac{6}{p+1} + O\left(\frac{1}{N^{2(1-\epsilon)}}\right) & \text{if } \left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1, \\ \frac{2}{p+1} + O\left(\frac{1}{N^{2(1-\epsilon)}}\right) & \text{if } \left(\frac{2}{p}\right) = -1,\ \left(\frac{-1}{p}\right) = 1; \end{cases}$$

$$\mathbb{E}_N(g_p(H_2)) = \mathbb{P}_N(H_2 \equiv 0 \bmod p) = \frac{4}{p+1} + O\left(\frac{1}{N^{2(1-\epsilon)}}\right).$$

Since $\max_{a,b\leq N}\{|H_1(a,b)|, |H_2(a,b)|\} \leq N^6$, each of H_1 and H_2 can only be divisible by at most $6/\epsilon$ prime factors larger than N^ϵ, so $\sum_{p>N^\epsilon} f_p(H_1)$ and $\sum_{p>N^\epsilon} g_p(H_2)$ are bounded above by $6/\epsilon$. Let $F(N) := \sum_{p\leq N^\epsilon} f_p(H_1)$ and $G(N) := \sum_{p\leq N^\epsilon} g_p(H_2)$. Then $F(N) = f(H) + O(1)$ and $G(N) = g(H) + O(1)$ for $(a,b) \in \mathcal{A}_N$.

We define the following random variables to model $f_p(H_1)$ and $g_p(H_2)$,

$$X_p = \begin{cases} 1 & \text{with probability } \frac{2}{p+1}\left(2 + \left(\frac{2}{p}\right)\right) \\ 0 & \text{with probability } 1 - \frac{2}{p+1}\left(2 + \left(\frac{2}{p}\right)\right) \end{cases} \text{ if } \left(\frac{-1}{p}\right) = 1;$$

$$Y_p = \begin{cases} 1 & \text{with probability } \frac{4}{p+1}, \\ 0 & \text{with probability } 1 - \frac{4}{p+1}, \end{cases}$$

and so that $\{X_p\}_p \cup \{Y_p\}_p$ are independent except $\mathbb{P}(X_p = 1 \text{ and } Y_p = 1) = 0$. If $\left(\frac{-1}{p}\right) \neq 1$, $X_p = 0$ with probability 1. Let $X(N) = \sum_{p\leq N^\epsilon} X_p$ and $Y(N) = \sum_{p\leq N^\epsilon} Y_p$. By the multidimensional central limit theorem, $X(N)$ and $Y(N)$ converge to independent normal distributions as $N \to \infty$. Note that $X(N)$ has mean and variance $2\log\log N + O(1)$; $Y(N)$ has mean and variance $4\log\log N + O(1)$.

Since mixed moments determine the multinomial distribution, we want to show that the mixed moments of $F(N)$ and $G(N)$ converge to those of $X(N)$ and $Y(N)$. We have by construction

$$\begin{aligned} \mathbb{E}_N\big(F(N)^k G(N)^l\big) &= \sum_{\substack{p_1,\dots,p_k \leq N^\epsilon \\ q_1,\dots,q_l \leq N^\epsilon}} \mathbb{P}_N(H_1 \equiv 0 \bmod p_i \text{ and } H_2 \equiv 0 \bmod q_j) \\ &= \mathbb{E}(X(N)^k Y(N)^l) + O\left(\frac{(4\log\log N)^{k+l-1}}{N^{2(1-\epsilon)}}\right). \end{aligned}$$

From this we compute

$$\begin{aligned} &\mathbb{E}_N\Big((F(N) - \mathbb{E}_N(F(N)))^k (G(N) - \mathbb{E}_N(G(N)))^l\Big) \\ &= \mathbb{E}\Big((X(N) - \mathbb{E}(X(N)))^k (Y(N) - \mathbb{E}(Y(N)))^l\Big) + O\left(\frac{(4\log\log N)^{k+l-1}}{N^{2(1-\epsilon)}}\right). \end{aligned}$$

This shows that the distributions of $F(N)$ and $G(N)$ tend to those of $X(N)$ and $Y(N)$ respectively. The difference of two normal distribution is a normal distribution, hence $f(H_1) - g(H_2) = F(N) - G(N) + O(1)$ tends to a normal distribution with mean and variance as claimed. □

References

[1] J. S. Balakrishnan, W. Ho, N. Kaplan, S. Spicer, W. Stein, and J. Weigandt. Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks. *LMS J. Comput. Math.*, 19(suppl. A):351–370, 2016.

[2] M. Bhargava and A. Shankar. The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, 2013.
[3] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015.
[4] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.
[5] J. W. Bober. Conditionally bounding analytic ranks of elliptic curves. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 135–144. Math. Sci. Publ., Berkeley, CA, 2013.
[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[7] T. D. Brooks, E. A. Fowler, K. C. Hastings, D. L. Hiance, and M. A. Zimmerman. Elliptic curves with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$? Does a rank 4 curve exist? *The Journal of the SUMSRI*, 2006. https://calico.mth.miamioh.edu/sumsri/sumj/2006/NTpaper06.pdf.
[8] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.
[9] T. Dokchitser and V. Dokchitser. Local invariants of isogenous elliptic curves. *Trans. Amer. Math. Soc.*, 367(6):4339–4358, 2015.
[10] A. Dujella. High rank elliptic curves with prescribed torsion. https://web.math.pmf.unizg.hr/ duje/tors/tors.html.
[11] T. Fisher. Higher descents on an elliptic curve with a rational 2-torsion point. *Math. Comp.*, 86(307):2493–2518, 2017.
[12] J. Flores, K. Jones, A. Rollick, and J. Weigandt. A statistical analysis of 2-Selmer groups for elliptic curves with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$. *The Journal of the SUMSRI*, 2007. http://www.units.miamioh.edu/sumsri/sumj/2007/SelmerStats07.pdf.
[13] D. Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math.*, pages 108–118. Springer, Berlin, 1979.
[14] H. Halberstam and H.-E. Richert. *Sieve methods*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4.
[15] Z. Klagsbrun and R. J. Lemke Oliver. The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point. *Res. Math. Sci.*, 1:Art. 15, 10, 2014.
[16] B. Naskręcki. Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples. *Acta Arith.*, 160(2):159–183, 2013.
[17] E. F. Schaefer and M. Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231, 2004.
[18] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. pages 33–52. Lecture Notes in Math., Vol. 476, 1975.
[19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.0)*, 2017. http://www.sagemath.org.
[20] A. Walfisz. *Weylsche Exponentialsummen in der neueren Zahlentheorie*. Mathematische Forschungsberichte, XV. VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

Department of Mathematics, University College London, Gower Street, London, WC1E 6BT, United Kingdom
Email address: stephanie.chan.16@ucl.ac.uk

Institute of Pure Mathematics, Ulm University, Helmholtzstrasse 18, 89081 Ulm, Germany
Email address: jeroen.hanselman@uni-ulm.de

Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA
Email address: wanlin@math.wisc.edu

A DATABASE OF BELYĬ MAPS

MICHAEL MUSTY, SAM SCHIAVONE, JEROEN SIJSLING, AND JOHN VOIGHT

Abstract. We use a numerical method to compute a database of three-point branched covers of the complex projective line of small degree. We report on some interesting features of this data set, including issues of descent.

1. Introduction

1.1. **Motivation.** Let X be a smooth, projective curve over $\mathbb{C}$. A *Belyĭ map* on X is a nonconstant map $\phi\colon X \to \mathbb{P}^1$ that is unramified away from $\{0, 1, \infty\}$. By a theorem of Belyĭ [2] and Weil's descent theory [15], X can be defined over the algebraic closure $\mathbb{Q}^{\mathrm{al}}$ of $\mathbb{Q}$ if and only if X admits a Belyĭ map. This remarkable observation has led to a spurt of activity, with many deep questions still open after forty years. In his study of covers of the projective line minus three points [8], Deligne writes pessimistically:

> A. Grothendieck and his students developed a combinatorial description ("maps") of finite coverings... It has not aided in understanding the Galois action. We have only a few examples of non-solvable coverings whose Galois conjugates have been computed.

Indeed, although significant mathematical effort has been expended in computing Belyĭ maps [14], there have been few systematic computations undertaken.

1.2. **Main result.** In this article we seek to remedy this state of affairs. We address Deligne's second objection by describing the uniform computation of a large catalogue of Belyĭ maps of small degree. We utilize the numerical method of Klug–Musty–Schiavone–Voight [10] and follow the combinatorial description of Grothendieck. We make some preliminary observations about our data, but leave to future work a more detailed analysis of the Galois action on the maps in our catalogue.

A *passport* is the data (g, G, λ) consisting of a nonnegative integer $g \in \mathbb{Z}_{\geq 0}$, a transitive permutation group $G \leq S_d$, and three partitions $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ of d. The *passport* of a Belyĭ map is given by its genus, its monodromy group, and the ramification degrees of the points above $0, 1, \infty$. There is a natural permutation action of S_3 on passports, so (without loss of generality) we choose exactly one passport up to this S_3-action. (For more on passports, see section 2.)

A summary of the scope of our computation is given in (1.3.1): we list the number of passports of Belyĭ maps for each degree d and genus g as well as the number of them that we have computed (green number). Our data is available at `https://github.com/michaelmusty/BelyiDB` and will hopefully also be available at `lmfdb.org` in the near future.

Date: June 13, 2018.

13 Jun 2018 18:19:42 PDT
Version 4 - Submitted to Open Book Series

1.3. **Comparison.** Our database compares to the existing catalogues of Belyĭ maps that are currently available as follows.

- Birch [4] computed a sampling of Belyĭ maps of low degree and genus, for a total of 50 passports.
- A *Shabat polynomial* is a Belyĭ map of genus 0 that is totally ramified at ∞. Bétréma–Péré–Zvonkin [3] computed all *Shabat polynomials* up to degree 8: there are 78 such passports.
- A Belyĭ map is *clean* if every point above 1 has ramification index 2. (A clean Belyĭ map has even degree, and if ϕ is an arbitrary Belyĭ map of degree d then $4\phi(1-\phi)$ is a clean Belyĭ map of degree $2d$.) Adrianov et al. [1] computed all clean Belyĭ maps up to degree 8: there are 67 such passports.
- Malle [11] computed fields of definition of some genus zero passports whose permutation group is primitive, subject to some other restrictions, up to degree 13: there are hundreds of passports.

There are many other papers that compute certain classes of Belyĭ maps: for further reference, see Sijsling–Voight [14].

(1.3.1)

d \ g	0	1	2	3	≥ 4	total
1	1/1	0	0	0	0	1/1
2	1/1	0	0	0	0	1/1
3	2/2	1/1	0	0	0	3/3
4	6/6	2/2	0	0	0	8/8
5	12/12	6/6	2/2	0	0	20/20
6	38/38	29/29	7/7	0	0	74/74
7	89/89	50/50	7/13	2/3	0	148/155
8	81/261	83/217	0/84	0/11	0	164/573
9	97/583	33/427	0/163	0/28	0/6	130/1207

1.4. **Outline.** The paper is organized as follows. We begin in section 2 by defining passports and exhibiting an algorithm to enumerate their representative permutation triples up to simultaneous conjugation. In section 3, we briefly recall the numerical method employed. In section 4, we treat the descent issues that arise. In sections 5–6, we detail steps that are specific to elliptic and hyperelliptic curves, and provide examples of these computations. We conclude in section 7 with a description of the database, some statistics, and some final observations.

1.5. **Acknowledgements.** The authors would like to thank Hartmut Monien and Greg Warrington for useful conversations; Mauricio Esquivel Rogel for his implementation of some numerical linear algebra routines, supported by a James O. Freedman Presidential Scholarship; and Joshua Perlmutter for help in verification. Thanks also to Maarten Derickx and David P. Roberts for comments. Our calculations are performed in the computer algebra system Magma [5]. Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

2. Passports

We begin by explaining the combinatorial (or topological) description of Belyĭ maps and exhibit an efficient method for their enumeration. For general background reading, see Sijsling–Voight [14, §1] and the references therein.

2.1. **Preliminaries.** Throughout, let $K \subseteq \mathbb{C}$ be a field. A *(nice) curve* over K is a smooth, projective, geometrically connected (irreducible) scheme of finite type over K that is pure of dimension 1. After extension to $\mathbb{C}$, a curve may be thought of as a compact, connected Riemann surface. A *Belyĭ map* over K is a finite morphism $\phi\colon X \to \mathbb{P}^1$ over K that is unramified outside $\{0, 1, \infty\}$; we will sometimes write (X, ϕ) when we want to pay special attention to the source curve X. Two Belyĭ maps ϕ, ϕ' are *isomorphic* if there is an isomorphism $\iota\colon X \xrightarrow{\sim} X'$ of curves such that $\phi'\iota = \phi$.

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyĭ map over $\mathbb{Q}^{\mathrm{al}}$ of degree $d \in \mathbb{Z}_{\geq 1}$. The *monodromy group* of ϕ is the Galois group $\mathrm{Mon}(\phi) := \mathrm{Gal}(\mathbb{C}(X) \,|\, \mathbb{C}(\mathbb{P}^1)) \leq S_d$ of the corresponding extension of function fields (understood as the action of the automorphism group of the normal closure); the group $\mathrm{Mon}(\phi)$ may also be obtained by lifting paths around $0, 1, \infty$ to X.

A *permutation triple* of degree $d \in \mathbb{Z}_{\geq 1}$ is a tuple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ such that $\sigma_\infty\sigma_1\sigma_0 = 1$. A permutation triple is *transitive* if the subgroup $\langle\sigma\rangle \leq S_d$ generated by σ is transitive. We say that two permutation triples σ, σ' are *simultaneously conjugate* if there exists $\tau \in S_d$ such that

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma'_0, \sigma'_1, \sigma'_\infty) = \sigma'. \tag{2.1.1}$$

An automorphism of a permutation triple σ is an element of S_d that simultaneously conjugates σ to itself, i.e., $\mathrm{Aut}(\sigma) = Z_{S_d}(\langle\sigma\rangle)$, the centralizer inside S_d.

Lemma 2.1.2. *The set of transitive permutation triples of degree d up to simultaneous conjugation is in bijection with the set of Belyĭ maps of degree d up to isomorphism.*

Proof. The correspondence is via monodromy [10, Lemma 1.1]; in particular, the monodromy group of a Belyĭ map is (conjugate in S_d to) the group generated by σ. □

The group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ acts on Belyĭ maps by acting on the coefficients of a set of defining equations; under the bijection of Lemma 2.1.2, it thereby acts on the set of transitive permutation triples, but this action is rather mysterious.

We can cut this action down to size by identifying some basic invariants, as follows. A *passport* consists of the data $\mathcal{P} = (g, G, \lambda)$ where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a tuple of partitions λ_s of d for $s = 0, 1, \infty$. These partitions will be also be thought of as a tuple of conjugacy classes $C = (C_0, C_1, C_\infty)$ by cycle type, so we will also write passports as (g, G, C). The *passport* of a Belyĭ map $\phi\colon X \to \mathbb{P}^1$ is $(g(X), \mathrm{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$, where $g(X)$ is the genus of X and λ_s is the partition of d obtained by the ramification degrees above $s = 0, 1, \infty$, respectively. Accordingly, the *passport* of a transitive permutation triple σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$, where (by Riemann–Hurwitz)

$$g(\sigma) := 1 - d + (e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty))/2 \tag{2.1.3}$$

and e is the index of a permutation (d minus the number of orbits), and $\lambda(\sigma)$ is the cycle type of σ_s for $s = 0, 1, \infty$. The *size* of a passport $\mathcal{P}$ is the number of

simultaneous conjugacy classes (as in 2.1.1) of (necessarily transitive) permutation triples σ with passport $\mathcal{P}$.

The action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ on Belyĭ maps preserves passports. Therefore, after computing equations for all Belyĭ maps with a given passport, we can try to identify the Galois orbits of this action. We say a passport is *irreducible* if it has one $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$-orbit and *reducible* otherwise.

2.2. **Passport lemma.** To enumerate passports, we will use the following lemma.

Lemma 2.2.1. *Let S be a group, let $G \leq S$ be a subgroup, let $N := N_S(G)$ be the normalizer of G in S, and let C_0, C_1 be conjugacy classes in N represented by $\tau_0, \tau_1 \in G$. Let $Z_N(g)$ denote the centralizer of g in N. Let*

$$U := \{(\sigma_0, \sigma_1) \in C_0 \times C_1 : \langle \sigma_0, \sigma_1 \rangle \subseteq G\}/\sim \tag{2.2.2}$$

where $\sim$ indicates simultaneous conjugation by elements in S. Then the map

$$\begin{aligned} u\colon Z_N(\tau_0)\backslash N/Z_N(\tau_1) &\to U \\ Z_N(\tau_0)\nu Z_N(\tau_1) &\mapsto [(\tau_0, \nu\tau_1\nu^{-1})] \end{aligned} \tag{2.2.3}$$

is surjective, and for all $[(\sigma_0, \sigma_1)] \in U$ such that $\langle \sigma_0, \sigma_1 \rangle = G$, there is a unique preimage under u.

Proof. The map (2.2.3) is well-defined, as $\nu \in N$ so $\nu\tau_1\nu^{-1} \in G$ and conjugacy classes are taken in N.

We first show that (2.2.3) is surjective. Let $[(\sigma_0, \sigma_1)] \in U$. Then $g\sigma_0 g^{-1} = \tau_0$ for some $g \in N$, and so $[(\sigma_0, \sigma_1)] = [(\tau_0, g\sigma_1 g^{-1})] \in U$. Similarly, there is $h \in N$ such that $\sigma_1 = h\tau_1 h^{-1}$ so $[(\sigma_0, \sigma_1)] = [(\tau_0, (gh)\tau_1(gh)^{-1})]$, and $gh = \nu \in N$.

Next, we show (2.2.3) is injective when restricted to generating pairs. Suppose $[(\tau_0, \nu\tau_1\nu^{-1})] = [(\tau_0, \mu\tau_1\mu^{-1})] \in U$ with $\mu, \nu \in N$. Then there exists $\rho \in S$ with

$$\rho(\tau_0, \nu\tau_1\nu^{-1})\rho^{-1} = (\tau_0, \mu\tau_1\mu^{-1}). \tag{2.2.4}$$

Since then $\rho\langle \tau_0, \nu\tau_1\nu^{-1}\rangle\rho^{-1} = \rho G\rho^{-1} = \langle \tau_0, \mu\tau_1\mu^{-1}\rangle = G$ under the hypotheses on generation, so we have $\rho \in N$. The equation in the first component reads $\rho\tau_0\rho^{-1} = \tau_0$, so $\rho \in Z_N(\tau_0)$ by definition. The second equation yields

$$\begin{aligned} \rho\nu\tau_1\nu^{-1}\rho^{-1} &= \mu\tau_1\mu^{-1} \\ (\mu^{-1}\rho\nu)\tau_1(\mu^{-1}\rho\nu)^{-1} &= \tau_1 \end{aligned} \tag{2.2.5}$$

so $\mu^{-1}\rho\nu \in Z_N(\tau_1)$. Writing $\nu = (\rho^{-1})\mu(\mu^{-1}\rho\nu)$, we find that $Z_N(\tau_0)\nu Z_N(\tau_1) = Z_N(\tau_0)\mu Z_N(\tau_1)$, as desired. □

2.3. **Computing passports.** We now describe an algorithm to produce all passports for a given degree d and a representative set of permutation triples in each passport up to simultaneous conjugation. We simplify this description by considering the transitive subgroups of S_d one at a time: these are currently available [5] up to degree 47.

There is a natural permutation action of S_3 on passports and on the permutation triples in a passport, corresponding to postcomposition of Belyĭ maps by an automorphism of the base curve $\mathbb{P}^1$ permuting $\{0, 1, \infty\}$. For the purposes of tabulation, we will choose one passport up to this action of S_3: to do so, we choose a total ordering $\preceq$ on partitions (e.g., refining the dominance partial order).

Algorithm 2.3.1. Let $d \in \mathbb{Z}_{\geq 1}$, let $G \leq S_d$ be a transitive subgroup, and let $N := N_{S_d}(G)$ be the normalizer of G in S_d. This algorithm returns a representative list of passports for G up to the action of S_3; and, for each passport, a representative list of permutation triples (one for each simultaneous conjugacy class).

1. Compute representatives $\{\tau_1, \ldots, \tau_r\}$ for the conjugacy classes $\{C_1, \ldots, C_r\}$ of G up to conjugation by N.
2. Out of the r^2 possible pairs of conjugacy class representatives, only consider pairs (τ_i, τ_j) with $\lambda(\tau_i) \preceq \lambda(\tau_j)$.
3. For each pair (τ_i, τ_j) from Step 2, apply Lemma 2.2.1 to compute the set

$$U_{ij} := \{(\sigma_0, \sigma_1) \in C_i \times C_j : \langle \sigma_0, \sigma_1 \rangle \subseteq G\}/\sim \tag{2.3.2}$$

   by computing the double coset $Z_N(\tau_i)\backslash N/Z_N(\tau_j)$ and applying the map u. Complete each pair $(\sigma_0, \sigma_1) \in U_{ij}$ to a permutation triple by setting $\sigma_\infty := (\sigma_1\sigma_0)^{-1}$, and let T_{ij} denote the resulting set of triples obtained from U_{ij}.
4. Keep only those triples $\sigma \in T_{ij}$ with $\langle \sigma \rangle = G$ and such that $\lambda(\sigma_1) \preceq \lambda(\sigma_\infty)$.
5. Sort the triples obtained from Step 4 into passports by cycle structure.

Proof of correctness. We compute all possible input pairs (τ_0, τ_1) to Lemma 2.2.1 with $\lambda(\tau_0) \preceq \lambda(\tau_1)$. This accounts for all possible input pairs to Lemma 2.2.1 since every passport is S_3-equivalent to such a passport. We do not have control over the conjugacy class of σ_∞ in this process, but Step 4 insists that every resulting passport representative σ has $\lambda(\sigma_0) \preceq \lambda(\sigma_1) \preceq \lambda(\sigma_\infty)$ thereby ensuring a unique passport up to the action of S_3. □

We computed representatives for all passports (without equations) in degree $d \leq 11$ using Algorithm 2.3.1: this took about 18 minutes for all degrees $d \leq 9$, about 3.3 hours for $d = 10$, and 2.37 days for $d = 11$.

3. Numerical computation of Belyi maps

With triples and passports in hand, we now briefly review the numerical method used to compute Belyĭ maps.

3.1. **Overview.** The method of Klug–Musty–Schiavone–Voight [10] takes as input a permutation triple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ and produces as output equations for the curve X and Belyĭ map $\phi\colon X \to \mathbb{P}^1$ over a number field $K \subseteq \mathbb{C}$ that corresponds to σ (in the monodromy bijection of Lemma 2.1.2).

This method is numerical, so it is not guaranteed to terminate (because of loss of precision or convergence issues), but when it terminates, it gives correct output. The method proceeds in the following steps.

1. Form the triangle subgroup $\Gamma \leq \Delta(a, b, c)$ associated to σ and compute its coset graph.
2. Use a reduction algorithm for Γ and numerical linear algebra to compute power series expansions of modular forms $f_i \in S_k(\Gamma)$ for an appropriate weight k.
3. Use numerical linear algebra (and Riemann–Roch) to find polynomial relations among the series f_i to compute equations for the curve X and similarly to express the map ϕ in this model.
4. Normalize the equations of X and ϕ so that the coefficients are algebraic; recognize these coefficients as elements of a number field $K \subseteq \mathbb{C}$.

13 Jun 2018 18:19:42 PDT
Version 4 - Submitted to Open Book Series

5. Verify that ϕ has the correct ramification and monodromy.

For the purposes of this article, the reader may treat this method as a black box with two exceptions: in section 4.4 we describe an improvement to the method in Step 4 for a choice of descent constant, and we discuss a numerical test for hyperellipticity using power series in weight 2 in section 6.2.

3.2. **Discussion.** There are a few key advantages of the above algorithm for our purposes. First, it is uniform, and in particular does not require the permutation triple to have a special form or for the curve to be of any particular genus. Second, it computes one Belyĭ map at a time, without needing the whole passport: and in particular, there are no *parasitic solutions* (degenerate maps that arise in other computational methods). Third, we obtain the bijection between triples and Belyĭ maps by the very construction of the equations (and the embedding $K \hookrightarrow \mathbb{C}$).

There is an alternative method due to Monien [12] that uses noncocompact triangle subgroups $\Gamma \leq \Delta(2,3,\infty) \simeq \mathrm{PSL}_2(\mathbb{Z})$ instead of our cocompact subgroups. This method has been shown to work in genus zero for maps of very large degree.

4. Descent issues

In this section, we discuss issues of descent for Belyĭ maps: when can a Belyĭ map be defined over a minimal field? (The reader eager for Belyĭ map computations should skip this and proceed to the next section.) A satisfactory answer to this question is crucial for understanding the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ on Belyĭ maps.

4.1. **Field of moduli and field of definition.** Let σ be a permutation triple with passport $\mathcal{P}$ and corresponding Belyĭ map $\phi\colon X \to \mathbb{P}^1$ over $\mathbb{Q}^{\mathrm{al}}$. The *field of moduli* $M(X,\phi) \subseteq \mathbb{Q}^{\mathrm{al}} \subset \mathbb{C}$ of ϕ is the fixed field of $\{\tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q}) : \tau(\phi) \simeq \phi\}$. The field of moduli is the intersection of all fields over which (X,ϕ) can be defined.

The degree of $M(X,\phi)$ is bounded above by the size of the passport $\mathcal{P}$; this bound is achieved if and only if the passport is irreducible.

Definition 4.1.1. We say that (X,ϕ) *descends* (to its field of moduli) if (X,ϕ) can be defined over its field of moduli $M(X,\phi)$, that is, if there exists a Belyĭ map $\phi_K\colon X_K \to \mathbb{P}^1$ over K whose base change to $\mathbb{Q}^{\mathrm{al}}$ is isomorphic to $\phi\colon X \to \mathbb{P}^1$.

Weil [15] studied general conditions for descent. For example, if ϕ has trivial automorphism group $\mathrm{Aut}(\phi)$, then ϕ descends—this criterion suffices to deal with a large majority of Belyĭ maps. More generally, to descend the Belyĭ map it is necessary and sufficient to construct a *Weil cocycle*, a collection of isomorphisms $f_\sigma\colon \sigma(X) \to X$, one for every element $\sigma \in \mathrm{Gal}_{M(X,\phi)} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, M(X,\phi))$, such that $f_{\sigma\tau} = f_\sigma \sigma(f_\tau)$ for all $\sigma,\tau \in \mathrm{Gal}_{M(X,\phi)}$. (When $\mathrm{Aut}(\phi)$ is trivial, this condition is satisfied for any collection of isomorphisms f_σ.) This criterion can be made explicit and computable [14, Method 4.1].

4.2. **Pointed descent.** There is another way to sidestep descent issues by rigidifying, as follows.

Definition 4.2.1. A *pointed Belyĭ map* $(X,\phi;P)$ is a Belyĭ map (X,ϕ) together with a point $P \in \phi^{-1}(\{0,1,\infty\}) \subseteq X(\mathbb{Q}^{\mathrm{al}})$. An isomorphism of pointed Belyĭ maps $(X,\phi;P) \xrightarrow{\sim} (X',\phi';P')$ is an isomorphism of Belyĭ maps ι such that $\iota(P) = P'$.

Remark 4.2.2. In our computations we choose the point P to be one of the ramification points of ϕ. Any point on X would do, but only the ramification points can be seen from the combinatorial data.

Definition 4.2.3. A *pointed permutation triple* $(\sigma; c)$ is a permutation triple $\sigma \in S_d^3$ together with a distinguished cycle c in one of the permutations σ_s with $s = 0, 1, \infty$; we call s its *base point* and the length of the cycle c its *length*. We call $(\sigma; c)$ a *pointed refinement* of the permutation triple σ.

Two pointed permutation triples $(\sigma; c)$ and $(\sigma'; c')$ are *simultaneously conjugate* if the permutation triples σ, σ' are simultaneously conjugate by an element $\tau \in S_d$ such that $c^\tau = c'$. The automorphism group $\mathrm{Aut}(\sigma; c) \leq \mathrm{Aut}(\sigma)$ is the subgroup of S_d that simultaneously conjugates $(\sigma; c)$ to itself.

Returning to the correspondence of Lemma 2.1.2, we see that pointed permutation triples of degree d up to simultaneous conjugation are in bijection with pointed Belyĭ maps of degree d up to isomorphism.

Proposition 4.2.4. *The base point, length, and cardinality of the automorphism group of a pointed permutation triple are invariant under simultaneous conjugation and under the action of* $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$.

Proof. The statements for simultaneous conjugation are clear. For the Galois action, we pass back to Belyĭ maps: the base point, the ramification index, and the automorphism group of a pointed Belyĭ map are Galois invariant. □

We similarly define the field of moduli $M(X, \phi; P)$ for a pointed Belyĭ map. The following theorem gives us a widely applicable criterion for descent (even in the presence of automorphisms).

Theorem 4.2.5. *A pointed Belyĭ map $(X, \phi; P)$ descends, i.e., the curve X, the map ϕ, and the point P can all be defined over $M(X, \phi; P)$.*

Proof. The statement is given by Birch [4, Theorem 2]; for a constructive proof using branches, see Sijsling–Voight [13, Theorem 1.12]. □

4.3. **Pointed passports.** Given the simplicity and importance of Theorem 4.2.5, we refine our notion of passport as follows.

Definition 4.3.1. A *pointed passport* is the data $(g, G, \lambda; c)$ where (g, G, λ) is a passport and $c = (s, e, a)$ consists of the data: $s \in \{0, 1, \infty\}$, and $e \in \mathbb{Z}_{\geq 1}$ a summand in the partition λ_s, and finally $a \in \mathbb{Z}_{\geq 1}$.

Given a pointed Belyĭ map $(X, \phi; P)$, we define its *pointed passport* $\mathcal{P}(X, \phi; P)$ to be its passport together with the data $s = \phi(P)$, the ramification degree $e = e_\phi(P)$, and $a = \#\mathrm{Aut}(X, \phi; P)$. Likewise, we define the pointed passport $\mathcal{P}(\sigma; c)$ to be the passport with s its base point, e its length, and a the cardinality of its automorphism group. We define the *size* of a pointed passport $\mathcal{P}$ to be the number of isomorphism classes of pointed Belyĭ maps (equivalently, number of classes of pointed permutation triples) with pointed passport $\mathcal{P}$.

Corollary 4.3.2. *A pointed Belyĭ map is defined over a field whose degree is at most the size of its pointed passport.*

Proof. Apply Theorem 4.2.5. □

Proposition 4.3.3. *If the size of $\mathcal{P}(\sigma; c)$ is equal to the size of $\mathcal{P}(\sigma)$, then all Belyĭ maps with passport $\mathcal{P}(\sigma)$ descend.*

Proof. Any field of definition of a pointed Belyĭ map is also a field of definition of the underlying Belyĭ map, so the fields of moduli and pointed moduli coincide by hypothesis. Descent follows by Theorem 4.2.5, since the moduli field of the pointed curve is a field of definition. □

It seems quite common for a permutation triple to have a pointed refinement of size 1. The first example where no such refinement exists occur in degree 8: see Example 4.5.1 below.

4.4. **Descent from $\mathbb{C}$.** In Step 4 of our numerical method (see section 3.1), there is a normalization procedure which we may interpret as an application of pointed descent, as follows. In the original method [10, §5], modular forms are expanded as power series centered in a neighborhood of a ramification point of the form $|w| < 1$ in a parameter w, and the coefficients of these power series are renormalized by writing them in terms of Θw for a certain transcendental factor Θ, computed as the ratio of two 'consecutive' terms in the power series expansion. In our setting, we instead normalize not the coefficients of the power series but instead coefficients of the Belyĭ map itself, now setting 'consecutive' coefficients equal. In practice, we find that this normalization requires smaller precision to recognize the Belyĭ map exactly from its numerical approximation.

Remark 4.4.1. In every example we computed, and in both ways of normalizing, we obtained normalized power series expansions that numerically agree with series defined over $M(X, \phi; P)$ with chosen ramification point P. Currently this is only a numerical observation; but it is a sensible expectation, as the method works by computing the pluricanonical image using expansions at the designated point.

Example 4.4.2. Consider the passport $(1, S_5, (5^1, 4^1 1^1, 4^1 1^1))$. The unique representative up to simultaneous conjugation is given by σ with

$$\sigma_0 = (1\ 4\ 2\ 5\ 3), \quad \sigma_1 = (1\ 2\ 3\ 4), \quad \sigma_\infty = (1\ 2\ 3\ 5)\,. \tag{4.4.3}$$

We take $c = (1\ 4\ 2\ 5\ 3)$, which has length 5 and trivial automorphism group. Since the pointed passport also has size 1, the field of moduli of the Belyĭ map equals $\mathbb{Q}$ by Corollary 4.3.2, and we can descend to this field by Proposition 4.3.3. Computing with 50 digits of precision (here and throughout, we only ever display 5 digits), we find $X\colon y^2 = x^3 - 27c_4x - 54c_6$ with

$$c_4 \approx 0.01030 + 0.00748i \qquad c_6 \approx -0.00270 + 0.00196i \tag{4.4.4}$$

and Belyĭ map ϕ with:

$$\phi \approx \frac{2.0000}{-1 + (2.21275 + 0.71897i)y + (1.77422i)xy} = \frac{2}{-1 + b_3y + b_5xy} \tag{4.4.5}$$

(where $i^2 = -1$). The indeterminacy in this approximation is by $\lambda \in \mathbb{C}^\times$, acting according to the degree of the pole at ∞, so $(c_4, c_6) \leftarrow (\lambda^{-4}c_4, \lambda^{-6}c_6)$ and $(x, y) \leftarrow (\lambda^{-2}x, \lambda^{-3}y)$. Taking

$$\lambda := \frac{b_5}{b_3^2} \approx -0.19265 - 0.26516i \tag{4.4.6}$$

the rescaled values $b_3' := \lambda^3 b_3 \approx 2^{16}/5^{10}$ and $b_5' := \lambda^5 b_5 \approx -2^8/5^5$ have $(b_3')^2/b_5' = 1$ (and there exists a descent with this ratio, defined over $\mathbb{Q}$). Now all the coefficients $a_0, b_3, b_5, c_4, c_6 \in \mathbb{Q}$ are easily identified. After computing a minimal model and swapping $0, \infty \in \mathbb{P}^1$ for cosmetics, we obtain $X\colon y^2 = x^3 + 5x + 10$ with map

$$\phi(x, y) = ((x - 5)y + 16)/32\,. \tag{4.4.7}$$

4.5. **Examples.** We now discuss some examples to see the various subtleties that play a role when descending Belyĭ maps.

Example 4.5.1. The first case of a passport for which Proposition 4.3.3 does not apply occurs in degree 8, given by $(1, V_4^2 : S_3, (3^2 1^2, 4^2, 4^2))$. The passport is size 1 but all pointed passports are size 2. The Belyĭ map descends because its automorphism group is trivial. A descent is given by $X\colon y^2 = x^3 + x^2 + 8x + 8$ and

$$\phi(x, y) = \frac{4(7x^4 + 24x^3 + 92x^2 + 320x + 272)y - 16(x + 1)(x^2 + 8)(x^2 + 16x + 24)}{27x^4 y}.$$

Because $\mathrm{Aut}(X, \phi)$ is trivial, this is the only model over $\mathbb{Q}$ up to isomorphism. Finally, none of its ramification points is rational, so no descent of a pointed refinement immediately gets us to the field of moduli $\mathbb{Q}$.

Example 4.5.2. The first dessin that does not descend to its field of moduli is of degree 16. Indeed, in lower degree, there are only three passports for which Proposition 4.3.3 does not apply *and* the automorphism group is nontrivial: all occur in degree 12, one with size 1, the other two of size 2. Yet explicit calculation shows that these three examples all descend.

For purposes of illustration, we consider the passport $(4, \mathrm{t12n57}, (6^2, 6^2, 6^2))$ of size 2, where t12n57 denotes the transitive group in S_{12} numbered 57. The passport is irreducible and the curves are nonhyperelliptic: they arise as degree 2 covers branching at the ramification points of the unique Belyĭ map with passport $(1, A_4(6), (3^2, 3^2, 3^2))$, given by $E\colon y^2 = x^3 + 6x^2 - 3x$ and Belyĭ map $\phi(x, y) = (x^2 + 3)y/(8x^2)$. The ramification points are then exactly the $\mathbb{Q}$-rational points ∞, $(0, 0)$, $(1, \pm 2)$, $(-3, \pm 6)$ on E. To construct the resulting degree 2 cover, we choose a 4-torsion point P_4 on E. Then the sum of the ramification points and $2P_4$ is equivalent to 8∞, so that we get a function whose square root gives rise to the requested cover. The four possible covers thus obtained are all Galois conjugate; we get the same Belyĭ map, this from the curve

$$X\colon \begin{array}{l} y^2 = x^3 + 6x^2 - 3x, \\ w^2 = yx^2 + 2yx - 3y + \alpha x^3 + 2\alpha x^2 - 3\alpha x, \end{array} \tag{4.5.3}$$

where $\alpha^4 - 12\alpha^2 + 48 = 0$. The field $\mathbb{Q}(\alpha)$ contains $\mathbb{Q}(\sqrt{-3})$. This unique quadratic subfield is also the field of moduli of the Belyĭ map from X, since one can show that it is mapped to its $\mathbb{Q}(\sqrt{-3})$-conjugate by the automorphism

$$(x, y, w) \mapsto \left(\frac{-3}{x}, \frac{3y}{x^2}, \frac{3iw}{x^2}\right) \tag{4.5.4}$$

of X. To show that the Belyĭ map descends, it suffices [7, Cor. 5.4] (or [13, Theorem 3.4.8] with $\mathcal{R} = \emptyset$) to show that the canonical model E_0 of E corresponding to the cocycle defined by the first two entries of (4.5.4) has a rational point. It does; in fact E_0 is isomorphic to E. Still, none of the points on E_0 that correspond to the ramification points of E are rational over $\mathbb{Q}(\sqrt{-3})$. We conclude that there is no

choice of *pointed refinement* that will give rise to a descent to $\mathbb{Q}(\sqrt{-3})$ in this case, even though the Belyĭ map descends.

5. Genus one

In this section, we discuss some details for Belyĭ maps of genus 1.

5.1. **Newton's method.** Let (X, ϕ) be a Belyĭ map with X of genus 1 defined by $X\colon y^2 = f(x) = x^3 - 27c_4x - 54c_6$. In our numerical method (see section 3.1, or the Genus 1 subsection of [10, §5]), we compute a numerical Weierstrass X and Belyĭ map ϕ on X to arbitrary precision.

Klug–Musty–Schiavone–Voight [10, Example 5.28] describe how to use Newton's method in the case of genus 0 to achieve very accurate approximations of the coefficients of the Belyĭ map, allowing us to quickly pass from tens of digits of precision to tens of thousands. We now explain how Newton's method can be extended to the case of genus 1 Belyĭ maps, ironing out some wrinkles.

Let $P = (x_P, y_P) \in X(\mathbb{C})$ be an affine point and let $t := x - x_P$ and $s := y - y_P$. Insisting that ϕ have a zero or pole of a given order at P imposes equations that can be determined by working in the completed local ring $\widehat{\mathbb{C}[X]}_P$ as follows.

If P is not a 2-torsion point of X, then t is a uniformizer for $\widehat{\mathbb{C}[X]}_P$. We solve for s in terms of t by substituting $x = t + x_P$ and $y = s + y_P$ into the equation for X, thereby obtaining a quadratic equation in s whose solution is

$$s := -y_P + y_P\sqrt{1 + \frac{t^3 + 3x_Pt^2 + (3x_P^2 - 27c_4)t}{y_P^2}}\,. \tag{5.1.1}$$

If instead P is a 2-torsion point, then s is a uniformizer for $\widehat{\mathbb{C}[X]}_P$; substituting as above, we obtain a cubic equation in s, which we solve via Hensel lifting. In either case, we may express the numerator and denominator of ϕ as power series in the local parameter. Once this has been accomplished, we obtain the equations imposed by a zero (resp., pole) at P of order e_P by insisting that the first e_P coefficients of the series for the numerator (resp., denominator) of ϕ vanish.

Newton's method has proven invaluable in our computations: it has allowed us to compute genus 1 maps that were previously out of reach, and has also sped up our computations considerably.

5.2. **Example.** We illustrate the above method with an example.

Example 5.2.1. Consider the passport $(1, S_7, (6^1 1^1, 6^1 1^1, 2^2 3^1))$ of size 13. Its pointed refinement taking the 6-cycle over 0 also has size 13. A representative permutation triple is

$$\sigma_0 = (1\ 2\ 3\ 4\ 5\ 6), \qquad \sigma_1 = (2\ 7\ 6\ 3\ 4\ 5), \qquad \sigma_\infty = (1\ 7\ 2)(3\ 5)(4\ 6). \tag{5.2.2}$$

This ramification data and a Riemann–Roch calculation implies that ϕ can be written as $\phi = \phi_0/\phi_\infty$ for $\phi_0 \in \mathscr{L}(2\infty)$ and $\phi_\infty \in \mathscr{L}(8\infty)$. (For details, see section 6.3 below.) Since $1, x$ and $1, x, y, x^2, xy, \ldots, x^4$ are bases for $\mathscr{L}(2\infty)$ and $\mathscr{L}(8\infty)$, respectively, pulling out leading coefficients and changing notation, we write

$$\phi = u\frac{\phi_0}{\phi_\infty} = u\frac{a_0 + x}{b_0 + b_2x + b_3y + \cdots + b_7x^2y + x^4} \tag{5.2.3}$$

for some $a_0, a_2, b_0, b_2 \ldots, b_7 \in \mathbb{Q}^{\mathrm{al}} \subset \mathbb{C}$. Computing with 40 digits of precision (displaying 5), we find after 20 seconds on a standard CPU the initial approximation for X and ϕ. After normalizing as in section 4.4 to obtain $b_7 (= b_8) = 1$, we obtain

$$\begin{aligned} c_4, c_6 &\approx -0.00031, 0.0000035 \\ \phi &\approx 0.0024 \frac{-0.18587 + x}{-0.00042 + 0.00112x + \cdots + 0.03839x^3 + x^2y + x^4}. \end{aligned} \tag{5.2.4}$$

Let $P = (x_P, y_P)$ be the point corresponding to the 3-cycle in σ_∞. Since $P \in X(\mathbb{C})$, our first equation is $y_P^2 = x_P^3 - 27c_4x_P - 54c_6$. Computing s as in (5.1.1), we find

$$\begin{aligned} s = \frac{\frac{3}{2}x_P^2 - \frac{27}{2}c_4}{y_P}t + \frac{-\frac{9}{8}x_P^4 + \frac{81}{4}c_4x_P^2 + \frac{3}{2}x_Py_P^2 - \frac{729}{8}c_4^2}{y_P^3}t^2 \\ + \frac{\frac{27}{16}x_P^6 - \frac{729}{16}c_4x_P^4 + \cdots + \frac{81}{4}c_4x_Py_P^2 + \frac{1}{2}y_P^4 - \frac{19683}{16}c_4^3}{y_P^5}t^3 + O(t^4)\,. \end{aligned} \tag{5.2.5}$$

Substituting $x = t + x_P$ and $y = s + y_P$ into the above expression for ϕ_∞ yields

$$\begin{aligned} \phi_\infty = x_P^4 + x_P^3b_6 + x_P^2y_Pb_7 + x_P^2b_4 + x_Py_Pb_5 + x_Pb_2 + y_Pb_3 + b_0 \\ + \left(\tfrac{3}{2}x_P^4b_7 + 4x_P^3y_P + \tfrac{3}{2}x_P^3 + \cdots + b_5 + y_Pb_2 - \tfrac{27}{2}c_4b_3\right)\frac{t}{y_P} \\ + \left(-\tfrac{9}{8}x_P^6b_7 - \tfrac{9}{8}x_P^5b_5 + \cdots + \tfrac{729}{8}c_4^2b_3\right)\frac{t^2}{y_P^3} + O(t^3)\,. \end{aligned} \tag{5.2.6}$$

To impose the condition that ϕ has a pole of order 3 at P, we set the first three coefficients of ϕ_∞ equal to zero, giving 3 relations.

Proceeding similarly with the other ramification points, we obtain 22 polynomial equations in the 23 variables $u, c_4, c_6, a_0, b_0, \ldots, b_7$ and x_P, y_P for each of the ramification points, other than the point corresponding to the cycle containing 1 in σ_0. (The point corresponding to this cycle is ∞, and we have already imposed the condition that ϕ vanishes to order 6 at ∞ by taking $\phi_0 \in \mathscr{L}(2\infty)$ and $\phi_\infty \in \mathscr{L}(8\infty)$.) This system is underdetermined, so in order to apply Newton's method, we must find at least one more equation. We observe that although ϕ is a degree 7 map, ϕ_∞ has degree 8, so there must be a common zero of ϕ_0 and ϕ_∞. Calling this point $P_s = (x_s, y_s)$, we obtain 3 more equations

$$\begin{aligned} y_s^2 = x_s^3 - (27c_4x_s - 54c_6) \qquad 0 = \phi_0(P_s) = a_0 + x_s \\ 0 = \phi_\infty(P_s) = b_0 + b_2x_s + b_3y_s + \cdots + b_7x_s^2y_s + x_s^4\,. \end{aligned} \tag{5.2.7}$$

We have adjoined two more variables x_s, y_s and produced three more equations to ensure non-degeneracy. This produces a system of 25 equations in 25 variables. Applying Newton's method to this system, in 16.20 seconds we obtain approximations of coefficients with 2000 digits of precision, which allows us to recognize the coefficients of ϕ as algebraic numbers. After a change of variables to reduce the size of the output, we find the elliptic curve

$$X\colon y^2 = x^3 - (24\nu + 75)x + \tfrac{1}{2}(-657\nu^2 - 1014\nu + 3278) \tag{5.2.8}$$

and Belyĭ map $\phi = u\phi_0/\phi_\infty$ where $u = 1/(2^9 3^2)$ and

$$\begin{aligned}\phi_0 &= (-419\nu^2 - 358\nu + 2947) + 49x \\ \phi_\infty &= (-806361\nu^2 - 724014\nu + 5449304) + (-3150\nu^2 - 15652\nu + 84560)x \\ &\quad + (-11310\nu^2 + 17940\nu + 118656)y + (-33180\nu^2 + 74760\nu - 55104)x^2 \\ &\quad + (59556\nu^2 - 189336\nu + 233856)xy + (5166\nu^2 - 16380\nu + 20720)x^3 \\ &\quad + (-59022\nu^2 + 184980\nu - 225792)x^2y + (25557\nu^2 - 80122\nu + 97832)x^4\end{aligned}$$

over the number field $\mathbb{Q}(\nu)$ where $\nu^3 - 6\nu + 12 = 0$. It turns out that this passport decomposes into two Galois orbits, one of size 3 as shown above, and the other of size 10. The coefficients of the Belyĭ map for the size 10 orbit are too large for us to display here, but it is defined over the number field $\mathbb{Q}(\mu)$ where

$$\mu^{10} - 2\mu^9 + 15\mu^8 - 78\mu^7 + 90\mu^6 + 48\mu^5 + 90\mu^4 - 78\mu^3 + 15\mu^2 - 2\mu + 1 = 0\,. \tag{5.2.9}$$

Remark 5.2.10. The "extra zero" phenomenon in (5.2.7) is typical; it can be avoided in the special case when 0 is totally ramified (i.e., when σ_0 is a d-cycle).

6. Hyperelliptic curves

We now discuss some issues and improvements for hyperelliptic curves.

6.1. **Setup.** Recall that a hyperelliptic curve of genus $g \geq 2$ over K has a model

$$X\colon y^2 + u(x)y = v(x) \tag{6.1.1}$$

where $\deg(u) \leq g+1$ and $\deg(v) \leq 2g+2$. Letting $f(x) := u(x)^2 + 4v(x)$, we have $f(x)$ separable with $\deg f(x) = 2g+1$ or $2g+2$; we refer to the model as *even* or *odd* according to the parity of $\deg f(x)$. Note that an odd model has the single point $\infty = (1:1:0)$ at infinity while an even model has two, $\infty' = (1:\sqrt{f_0}:0)$ and $\infty = (1:-\sqrt{f_0}:0)$ where f_0 is the leading coefficient of $f(x)$ (I.e., the point ∞ is a Weierstrass point if and only if the model is odd.) In constructing the Belyĭ map, in both cases we take ∞ to be the marked point (around which we expand series), and by convention it corresponds to the cycle containing 1 in σ_0.

6.2. **Numerical test for hyperellipticity.** Let Γ be a triangle subgroup with $X = X(\Gamma)$ of genus $g \geq 2$. We test if X is numerically hyperelliptic (in the sense the curve appears to be hyperelliptic to the precision computed) as follows. First, we compute power series expansions of an *echelonized* basis $f_1, f_2, \ldots, f_g$ of $S_2(X(\Gamma))$. We have an isomorphism $S_2(X(\Gamma)) \cong \Omega(X(\Gamma))$ given by $f(z) \mapsto f(z)\,\mathrm{d}z$ where $\Omega(X(\Gamma))$ is the $\mathbb{C}$-vector space of holomorphic differential 1-forms on $X(\Gamma)$. If X is hyperelliptic with model as in (6.1.1), since $f_1, \ldots, f_g$ is an echelonized basis we have the further isomorphism

$$\begin{aligned}\Omega(X(\Gamma)) &\xrightarrow{\sim} \Omega(X) \\ f_i(z)\,\mathrm{d}z &\mapsto x^{g-i}\frac{\mathrm{d}x}{y}\end{aligned} \tag{6.2.1}$$

for $i = 1, \ldots, g$. Thus, to recover x, y defined on $X(\Gamma)$, we can take

$$x := f_1/f_2 \qquad\qquad y := x'/f_g \tag{6.2.2}$$

where x' denotes the derivative of x with respect to w (the coordinate in the hyperbolic disc). If the model is odd, then $\operatorname{ord}_\infty x = -2$ and $\operatorname{ord}_\infty y = -(2g+1)$; if the model is even, then $\operatorname{ord}_\infty x = -1$ and $\operatorname{ord}_\infty y = -(g+1)$.

Consider the rational map $X(\Gamma) \to \mathbb{A}^2_{\mathbb{C}}$ with coordinates x, y. Using numerical linear algebra, we test if there is an approximate linear relation among

$$1, x, \dots, x^{2g+2}, y, xy, \dots, x^{g+1}y, y^2 \in \mathbb{C}[[w]]. \tag{6.2.3}$$

If there is such a relation, we obtain a rational map from X to a hyperelliptic curve $X' \subseteq \mathbb{A}^2$. If $g(X') = g(X)$, then the Riemann–Hurwitz formula implies that this map is birational, hence X' is a model of X as in (6.1.1). If no such relation exists, then we conclude that X is not numerically hyperelliptic.

6.3. **Computing a hyperelliptic Belyi map.** Suppose now that X is hyperelliptic with model as in (6.1.1). We compute the expression of the Belyĭ map ϕ as a rational function in x and y roughly as follows. (1) Determine an appropriate Riemann–Roch space $\mathscr{L}(D)$. (2) Compute a basis of $\mathscr{L}(D)$ in terms of x and y. (3) Using numerical linear algebra, express ϕ as a linear combination of functions in this basis.

We make this precise as follows, following Javanpeykar–Voight [9, Lemma 3.2]. Let $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ be a transitive permutation triple of degree d with corresponding hyperelliptic Belyĭ map (X, ϕ), and let g be the genus of X. Let s be the length of the cycle containing 1 in σ_0 and let $k_1, \dots k_r$ be the lengths of the remaining cycles in σ_0. Then the divisor of poles of $1/\phi$ is $\operatorname{div}_\infty(1/\phi) = s\infty + \sum_{i=1}^r k_i P_i$ for some points $P_1, \dots, P_r \in X(\mathbb{C})$. Since we do not have control over the points $P_1, \dots, P_r$, we "cancel" these poles by multiplying ϕ by a suitable function ϕ_0 that has zeroes at $P_1, \dots, P_r$ and has poles only at ∞. Such a ϕ_0 will belong to the space $\mathscr{L}(D) \subseteq \mathscr{L}(t\infty)$ where

$$D := -\textstyle\sum_{i=1}^r k_i P_i + t\infty \tag{6.3.1}$$

for some (as of yet undetermined) $t \in \mathbb{Z}_{\geq 0}$. Once we have obtained ϕ_0, then $\phi_0/\phi \in \mathscr{L}((s+t)\infty)$. As we will describe in the next step, we can write down a basis for Riemann–Roch spaces for divisors of the form $m\infty$. This allows us to compute ϕ_0 and $\phi_\infty := \phi_0/\phi \in \mathscr{L}((s+t)\infty)$ with respect to this basis. Thus we have $\phi = \phi_0/\phi_\infty$ for some $\phi_0 \in \mathscr{L}(t\infty)$ and $\phi_\infty \in \mathscr{L}((s+t)\infty)$.

It remains to determine a value of t so that such a ϕ_0 exists. To do this, we apply Riemann–Roch to the divisor D. Since $\sum_{i=1}^r k_i = d - s$, this yields

$$\ell(D) - \ell(K_X - D) = 1 - g + \deg(D) = 1 - g + (s - d + t) \tag{6.3.2}$$

where K_X is a canonical divisor of X. To ensure the existence of a nonzero ϕ_0 as above, we must have $\ell(D) \geq 1$. By (6.3.2), this holds if $1 - g + s - d + t \geq 1$, i.e., if $t \geq d - s + g$. Thus we may take $t = d - s + g$. (This conclusion actually does not require X to be hyperelliptic.)

Next, we explain how to compute bases for $\mathscr{L}(t\infty)$ and $\mathscr{L}((s+t)\infty)$ as in step 2. In the case of an odd model, this basis is particularly simple: x and y have poles at ∞ of orders 2 and $2g+1$, respectively, so

$$1, x, x^2, \dots, x^{\lfloor m/2 \rfloor}, y, xy, \dots, x^{\lfloor \frac{m-(2g+1)}{2} \rfloor} y \tag{6.3.3}$$

is a basis for $\mathscr{L}(m\infty)$. In the case of an even model the situation is more complicated. Now $x, y \notin \mathscr{L}(m\infty)$ because they have poles at ∞'. We compute a basis for $\mathscr{L}(m\infty)$ as follows. Since x has a simple pole at ∞' then $t = 1/x$ has a simple

zero, hence is a uniformizing parameter at ∞'. Working in the completed local ring $\widehat{\mathcal{O}}_{X,\infty'} \simeq \mathbb{C}[[t]]$, we can express y as a Laurent series in t via

$$y = \frac{1}{2}\left(-u(1/t) \pm \sqrt{u(1/t)^2 + 4v(1/t)}\right). \tag{6.3.4}$$

We use the series expansions $x(w), y(w)$ at ∞ to match the correct sign in (6.3.4). For each $j \in \{0, \dots, m-(g+1)\}$ we compute the Laurent tail $P_j \in \mathbb{C}[1/t] = \mathbb{C}[x]$ of $x^j y$, so that $x^j y - P_j$ is holomorphic at ∞'. In this way we obtain the basis

$$1, y - P_0, xy - P_1, \dots, x^{m-(g+1)}y - P_{m-(g+1)} \tag{6.3.5}$$

for $\mathscr{L}(m\infty)$.

Example 6.3.6. We illustrate the above procedure with an example. Consider the passport $(2, G, (6^1, 6^1, 3^2))$, where $G := 2A_4(6) \simeq A_4 \times C_2$. The passport (and pointed passport) are size 1, with representative triple

$$\sigma_0 = (1\ 6\ 2\ 4\ 3\ 5), \quad \sigma_1 = (1\ 3\ 5\ 4\ 6\ 2), \quad \sigma_\infty = (1\ 3\ 5)(2\ 4\ 6). \tag{6.3.7}$$

Computing the coordinate functions x, y as in (6.2.2) to 50 digits (displaying 5), we find approximate series

$$\begin{aligned} x &\approx 0.99999w^{-1} - 0.79370w - 0.31498w^3 + O(w^4) \\ y &\approx -0.99999w^{-3} - 0.79370w^{-1} - 0.94494w - 0.02142w^3 + O(w^4)\,. \end{aligned} \tag{6.3.8}$$

Since the series for y has a pole of order $3 = g+1$, we are in the case of an even model. Forming the matrix of coefficients of the monomials

$$1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^3y, y^2\,, \tag{6.3.9}$$

we find a hyperelliptic equation as in (6.1.1) with $u = 0$ and

$$v \approx 1.00000x^6 + 6.34960x^4 + 15.11905x^2 + 11.99999 \tag{6.3.10}$$

This gives the local expansion

$$\begin{aligned} y = \sqrt{v(1/t)} &= \sqrt{1.00000t^{-6} + 6.34960t^{-4} + 15.11905t^{-2} + 11.99999} \\ &= 1.00000t^{-3} + 3.17480t^{-1} + 2.51984t - 1.99999t^3 + O(t^4)\,. \end{aligned} \tag{6.3.11}$$

Thus the Laurent tail of y is $1.00000x^3 + 3.17480x$, and the first nonconstant element of our basis for $\mathscr{L}(m\infty)$ for $m \geq 3$ is thus

$$\begin{aligned} &y - (1.00000x^3 + 3.17480x) \\ &\qquad \approx -2.00000w^{-3} - 1.58740w^{-1} + 0.62996w - 0.04285w^3 + O(w^4) \end{aligned} \tag{6.3.12}$$

and we can compute the remaining elements of the basis similarly. Proceeding as explained above, we obtain the Belyĭ map

$$\phi(x, y) = \frac{x^4 + 2x^2 + xy + 1}{2(x^2+1)^2} \tag{6.3.13}$$

defined on the hyperelliptic curve $X\colon y^2 = x^6 + 4x^4 + 6x^2 + 3$.

7. Database

7.1. **Technical description.** Our database is organized by passports as computed in Algorithm 2.3.1. For each passport we store basic information such as degree, genus, ramification indices, and the monodromy group. We also store the automorphism group and passport representatives, as well as their pointed counterparts. After computing equations for every Belyĭ map in a passport, we store the Belyĭ maps, curves, the fields over which they are defined, and the associated complex embedding. We then partition the pointed passport representatives into Galois orbits obtained from this information. Lastly, the numerical power series and information to recover the normalization in Section 3.1 Step 4 are also saved.

7.2. **Running time.** Since our numerical method for computing equations sometimes requires a workaround for corner cases, we do not have detailed information about the total running time. To give a rough idea of the running time, we consider some examples. In (7.2.1) we list the approximate CPU time to compute *one* Belyĭ map in the listed passport, with power series computed to the specified number of decimal digits of precision and then precision obtained in Newton iteration.

(7.2.1)

Passport	Size	Precision (Newton)	CPU Time
$(0, A_9, (5^1 2^2, 3^3, 4^1 2^1 1^3))$	2	20 (1000)	7s
$(0, S_9, (7^1 2^1, 4^1 2^1 1^3, 4^1 2^2 1^1))$	23	20 (16000)	2m46s
$(1, A_7, (7^1, 3^1 2^2, 3^1 2^2))$	2	30 (1000)	23s
$(1, S_7, (5^1 2^1, 5^1 2^1, 3^1 2^2))$	4	40 (1500)	2m48s
$(1, A_7, (7^1, 4^1 2^1 1^1, 4^1 2^1 1^1))$	22	20 (1500)	10s
$(2, \mathrm{GL}_3(\mathbb{F}_2), (7^1, 7^1, 3^2 1^1))$	4	20	4m59s

The current database of Belyĭ maps consists of approximately 240MB of text files.

7.3. **Observations.** Having completed a large scale computation of Belyĭ maps, it remains to analyze our data.

- The largest passport sizes in each degree are:

(7.3.1)

Degree	≤ 4	5	6	7	8	9	10	11
Passport size	1	3	8	38	177	1260	8820	72572

- The largest degree number field arising as a field of definition of a Belyĭ map in our database occurs for the passport $(1, S_7, (6^1 1^1, 6^1 1^1, 4^1 2^1 1^1))$ which is irreducible of size 32. This degree 32 number field has discriminant $2^{68}3^{27}5^9 7^{15}$ and Galois group $\mathbb{Z}/2\mathbb{Z} \wr S_{16}$.
- The passport $(2, A_7, (7^1, 7^1, 5^1 1^1 1^1))$ provides an example of a highly reducible passport: it has size 24 and decomposes into 6 Galois orbits of sizes $1, 2, 3, 4, 6$, and 8. The associated number fields are $\mathbb{Q}$, and those with defining polynomials $x^2 - x - 5$, $x^3 + 2x - 2$, $x^4 - 2x^3 - 2x^2 + 3x - 3$, $x^6 - 2x^4 - 5x^3 - 2x^2 + 1$, and $x^8 - 4x^7 + 14x^5 - 35x^4 + 42x^3 - 126x^2 + 108x + 135$.
- There are 262 passports with degree $d \leq 7$. We have computed equations for all Belyĭ maps in 255 of these passports and found that 37 are reducible. For a passport $\mathcal{P}$ of size l, the Galois action determines a partition of l with parts $l_1, \ldots, l_r$. To measure the irreducibility of $\mathcal{P}$, define

(7.3.2)
$$\mathrm{w}(\mathcal{P}) := \begin{cases} 1, & \text{if } l = 1; \\ (l-1)^{-2} \sum_{i=1}^{r} (l_i - 1)^2, & \text{if } l \geq 2. \end{cases}$$

Let $\mathscr{P}_d$ be the set of passports with degree no larger than d and define

$$\beta(d) := (\#\mathscr{P}_d)^{-1} \sum_{\mathcal{P} \in \mathscr{P}_d} \mathrm{w}(\mathcal{P}). \tag{7.3.3}$$

From the database we find that $\beta(d) = 1$ for $d \leq 4$, $\beta(5) \approx 0.9393$, $\beta(6) \approx 0.9444$, and $0.8779 < \beta(7) < 0.9046$.

References

[1] N. M. Adrianov, N. Ya. Amburg, V. A. Dremov, Yu. A. Levitskaya, E. M. Kreines, Yu. Yu. Kochetkov, V. F. Nasretdinova, G. B. Shabat, *Catalog of dessins d'enfants with* ≤ 4 *edges*, `arXiv:0710.2658v1`, 14 October 2007.

[2] G.V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. **14** (1980), no. 2, 247–256.

[3] Jean Bétréma, Danielle Péré, Alexander Zvonkin, *Plane trees and their Shabat polynomials*, Catalog (5th ed.) Publication du LaBRI No. 92-75 (1992).

[4] Bryan Birch, *Noncongruence subgroups, covers and drawings*, The Grothendieck theory of dessins d'enfants (ed. Leila Schneps), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, 25–46.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265.

[6] Jean-Marc Couveignes and Louis Granboulan, *Dessins from a geometric point of view*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 79–113.

[7] P. Dèbes and M. Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.

[8] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ. 16, Springer, 1989, 79–297.

[9] Ariyan Javanpeykar and John Voight, *The Belyi degree of a curve is computable*, preprint.

[10] M. Klug, M. Musty, S. Schiavone, and J. Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS J. Comput. Math. **17** (2014), no. 1, 379–430.

[11] Gunter Malle, *Fields of definition of some three point ramified field extensions*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 147–168.

[12] Hartmut Monien, *The sporadic group J2, Hauptmodul and Belyi map*, `arXiv:1703.05200`.

[13] Jeroen Sijsling and John Voight, *On explicit descent of marked curves and maps*, Res. Number Theory 2 (2016), Art. 27, 35 pp.

[14] Jeroen Sijsling and John Voight, *On computing Belyĭ maps*, Publ. Math. Besançon: Algèbre Théorie Nr. 2014/1, Presses Univ. Franche-Comté, Besançon, 73–131.

[15] André Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524.

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

Email address: `michaelmusty@gmail.com, sam.schiavone@gmail.com`

Universität Ulm, Institut für Reine Mathematik, D-89068 Ulm, Germany

Email address: `jeroen.sijsling@uni-ulm.de`

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

Email address: `jvoight@gmail.com`

13 Jun 2018 18:19:42 PDT
Version 4 - Submitted to Open Book Series

ZETA FUNCTIONS OF NONDEGENERATE HYPERSURFACES IN TORIC VARIETIES VIA CONTROLLED REDUCTION IN p-ADIC COHOMOLOGY

EDGAR COSTA, DAVID HARVEY, AND KIRAN S. KEDLAYA

Abstract. We give an interim report on some improvements and generalizations of the Abbott–Kedlaya–Roe method to compute the zeta function of a nondegenerate ample hypersurface in a projectively normal toric variety over $\mathbb{F}_p$ in linear time in p. These are illustrated with a number of examples including K3 surfaces, Calabi–Yau threefolds, and a cubic fourfold. The latter example is a non-special cubic fourfold appearing in the Ranestad–Voisin coplanar divisor on moduli space; this verifies that the coplanar divisor is not a Noether–Lefschetz divisor in the sense of Hassett.

1. Introduction

We consider the problem of computing the zeta function $Z(\mathcal{X}, t)$ of an explicitly specified variety $\mathcal{X}$ over a finite field $\mathbb{F}_q$ of characteristic p. For curves and abelian varieties, Schoof's method and variants [Sch85, Pil90, GS04, GKS11, GS12] can compute $Z(\mathcal{X}, t)$ in time and space polynomial in $\log q$ and exponential in the genus/dimension; these have only been implemented for genus/dimension at most 2. Such methods may be characterized as *ℓ-adic*, as they access the ℓ-adic cohomology (for $\ell \neq p$ prime) of the variety via torsion points; there also exist *p-adic methods* which compute approximations of the Frobenius action on p-adic cohomology (Monsky–Washnitzer cohomology), and which have proven to be more viable in practice for large genus. Early examples include Kedlaya's algorithm [Ked01] for hyperelliptic curves, in which the time/space dependence is polynomial in the genus and quasi-linear in p, and Harvey's algorithm [Har07] which improves the dependence on p to $p^{1/2+\epsilon}$. These methods have been subsequently generalized [GG01, DV06a, DV06b, Har12], notably by Tuitman's algorithm [Tui16, Tui17] which applies to (almost) all curves while keeping the quasi-linear dependence on p. In another direction, Harvey [Har14] has shown that when computing the zeta functions of reductions of a fixed hyperelliptic curve over a number field, p-adic methods can achieve *average* polynomial time in $\log p$ and the genus; this has been implemented in small genus [HS14, HS16].

One advantage of p-adic methods over ℓ-adic ones is that they scale much better to higher-dimensional varieties. For example, there are several p-adic constructions that apply to *arbitrary* varieties with reasonable asymptotic complexity [LW08, Har15], although we are not aware of any practical implementations.

The first author was partially supported by the Simons Collaboration Grant #550029. The second author was supported by the Australian Research Council (grants DP150101689 and FT160100219). The third author was supported by NSF (grants DMS-1101343, DMS-1501214); UC San Diego (Warschawski Professorship); and a Guggenheim Fellowship. All three authors thank ICERM for its hospitality during fall 2015.

Various algorithms, and some implementations, have been given using Lauder's *deformation method* of computing the Frobenius action on the Gauss–Manin connection of a pencil [Lau04a, Lau04b, Ger07, Hub08, PT15, Tui18].

In this paper, we build on an algorithm of Abbott–Kedlaya–Roe [AKR10] which adapts the original approach of [Ked01] to smooth projective hypersurfaces. Here, we add two key improvements.

- We use *controlled reduction* in de Rham cohomology, as described in some lectures of Harvey [Har10a, Har10b, Har10c], to preserve sparsity of certain polynomials, thus reducing the time (respectively, space) dependence on p from polynomial to quasi-linear (respectively, $O(\log p)$). The resulting *controlled AKR method* was implemented, with further improvements, in Costa's Ph.D. thesis [Cos15], with examples of generic surfaces and threefolds over $\mathbb{F}_p$ for $p \sim 10^6$ [Cos15, Section 1.6]; by contrast, the largest p used in [AKR10] is 29. Costa and Harvey are currently preparing a paper on this method; meanwhile, Costa's GPL-licensed code is available on GitHub [Cos], and is slated to be integrated into SageMath [Sag].
- We also generalize to toric hypersurfaces, subject to a standard genericity condition called *nondegeneracy*. This greatly increases the applicability of the method while preserving much of its efficiency. Some previous attempts have been made to compute zeta functions in this setting, such as work of Castryck–Denef–Vercauteren [CDV06] for curves and Sperber–Voight [SV13] in general; it is the combination with controlled reduction that makes our approach the most practical to date.

It may be possible to improve the dependence on p to square-root (as in [Har07]) or average polynomial time (as in [Har14]), but we do not attempt to do so here.

For reasons of space, we give only a summary of the algorithm, with further details to appear elsewhere. In lieu of these details, we present a number of worked examples in dimensions 2-4 that demonstrate the practicality of this algorithm in a wide range of cases. The results are based on an implementation in `C++`, using `NTL` [Sho] for the underlying arithmetic operations. Our examples in dimensions 2 and 3 were computed on one core of a desktop machine with an `Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz`; our sole example in dimension 4 was computed on one core of a server with an `AMD Opteron Processor 6378 @ 1.6GHz`. (We have not yet optimized our vector-matrix multiplications in any way; as a consequence, we observe a serious performance hit whenever the working moduli exceeds 2^{62}.)

In dimensions 2 and 3, our examples are *Calabi–Yau varieties*, i.e., smooth, proper, simply connected varieties with trivial canonical bundle. In dimension 1, these are simply elliptic curves. In dimension 2, they are *K3 surfaces*, whose zeta functions are of computational interest for various reasons. For instance, these zeta functions can (potentially) be used to establish the infinitude of rational curves on a K3 surface (see the introduction to [CT14] for discussion); there has also been recent work on analogues of the Honda–Tate theorem, establishing conditions under which particular zeta functions are realized by K3 surfaces [Tae16, Ito16].

As for Calabi–Yau threefolds, much of the interest in their zeta functions can be traced back to *mirror symmetry* in mathematical physics. An early example is the work of Candelas–de la Ossa–Rodriguez Villegas [CdlORV03] on the Dwork pencil; a more recent example is [DKS+16], in which (using p-adic cohomology) certain mirror families of Calabi–Yau threefolds are shown to have related zeta functions.

4 Jun 2018 15:52:35 PDT
Version 4 - Submitted to Open Book Series

Our four-dimensional example is a cubic projective fourfold. Such varieties occupy a boundary region between rational and irrational varieties; it is expected that a cubic fourfold is rational if and only if it is *special* in the sense of having a primitive cycle class in codimension 2. The geometry of special cubic fourfolds is in turn closely linked to that of K3 surfaces; in many cases, the Hodge structure of a K3 surface occurs (up to a twist) inside the Hodge structure of a special cubic fourfold, and (modulo standard conjectures) this implies a similar relationship between zeta functions. See [Has16] for further discussion.

The specific example we consider is related to the geometry of the moduli space of cubic fourfolds over $\mathbb{C}$. On this space, one can construct various divisors consisting entirely of special cubic fourfolds; Hassett calls these *Noether–Lefschetz divisors*. Recently, Ranestad–Voisin [RV17] exhibited four divisors which they believed not to be Noether–Lefschetz, but only checked this in one case. Addington–Auel [AA18] checked two more cases by finding in these divisors some cubic fourfolds over $\mathbb{Q}$ with good reduction at 2, such that the zeta functions over $\mathbb{F}_2$ show no primitive Tate classes in codimension 2. By replacing the brute-force point counts of Addington–Auel with p-adic methods, we are able to work modulo a larger prime to find an example showing that the fourth Ranestad–Voisin divisor is not Noether–Lefschetz.

To sum up, the overall goal of this project is to vastly enlarge the collection of varieties for which computing the zeta function is practical. It is our hope that doing so will lead to a rash of new insights, conjectures, and theorems of interest to a broad range of number theorists and algebraic geometers.

2. Toric hypersurfaces

We begin by reviewing the construction of a projective toric variety from a lattice polytope. For more details we recommend [CLS11].

Let $n \geq 1$ be an integer. For any commutative ring R, let $R[x^{\pm}]$ denote the Laurent polynomial ring in n variables $x_1, \dots, x_n$ with coefficients in R. For $\alpha := (\alpha_i) \in \mathbb{Z}^n$, we write x^α for the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. We denote the R-torus by $\mathbb{T}^n_R := \operatorname{Spec}(R[x^{\pm}])$.

Let $\Delta \subset \mathbb{R}^n$ be the convex hull of a finite subset of $\mathbb{Z}^n$ that is not contained in any hyperplane, so that $\dim \Delta = n$. For $r \in \mathbb{R}$, let $r\Delta$ be the r-fold dilation of Δ. For an integer $d \geq 0$, let

$$P_d := \langle x^\alpha : \alpha \in d\Delta \cap \mathbb{Z}^n \rangle_R \quad (\text{resp. } P_d^{\mathrm{Int}} := \langle x^\alpha : \alpha \in \operatorname{Int}(d\Delta) \cap \mathbb{Z}^n \rangle_R)$$

be the free R-module on the set of monomials with exponents in $d\Delta \cap \mathbb{Z}^n$ (resp. $\operatorname{Int}(d\Delta) \cap \mathbb{Z}^n$). Define the R-graded algebras

$$P_\Delta := \bigoplus_{d=0}^{+\infty} P_d \quad \text{and} \quad P_\Delta^{\mathrm{Int}} := \bigoplus_{d=0}^{+\infty} P_d^{\mathrm{Int}}.$$

with the usual multiplication in $R[x^{\pm}]$. We define the polarized toric variety associated to Δ as the pair $(\mathbb{P}_\Delta, \mathcal{O}_\Delta)$, where $\mathbb{P}_\Delta := \operatorname{Proj} P_\Delta$ and $\mathcal{O}_\Delta$ is the ample line bundle on $\mathbb{P}_\Delta$ associated to the graded P_Δ-module $P_\Delta(1)$. Note that P_Δ and P_Δ^{Int} admit n commuting degree-preserving differential operators $\partial_i := x_i \frac{\partial}{\partial x_i}$ for $i = 1, \dots, n$.

In order to suppress some expository and algorithmic complexity, we make the simplifying assumption that Δ is a *normal* polytope; that is, the map

$$(\Delta \cap \mathbb{Z}^n)^d \to d\Delta \cap \mathbb{Z}^n : (x_1, \dots, x_d) \mapsto x_1 + \cdots + x_d$$

4 Jun 2018 15:52:35 PDT
Version 4 - Submitted to Open Book Series

is surjective for $d \geq 1$. This corresponds to the pair $(\mathbb{P}_\Delta, \mathcal{O}_\Delta)$ being *projectively normal*; this will be the case in our examples. As a consequence, we have that $\mathcal{O}_\Delta$ is indeed very ample.

Example 2.1. Let Δ be the regular n-simplex, the convex hull of $0, e_1, \dots, e_n$. We may then identify P_d with the set of homogeneous polynomials of degree d in $x_0, \dots, x_n$, by identifying $x^\alpha \in P_{\Delta,d}$ with the monomial $x_0^{d-\alpha_1-\cdots-\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$; then $(\mathbb{P}_\Delta, \mathcal{O}_\Delta)$ is isomorphic to $(\mathbb{P}^n_R, \mathcal{O}(1))$.

We obtain the weighted projective space $\mathbb{P}(w_0, \dots, w_n)$ by taking

$$\Delta = \{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} : \sum_{i=0}^{n} w_i x_i = w_0 \cdots w_n\}, \quad \text{see [Dol82, 1.2.5].}$$

We obtain $\mathbb{P}^k_R \times_R \mathbb{P}^r_R$ by taking Δ to be the Cartesian product of the regular k-simplex by the regular r-simplex [CLS11, §2.4].

We now turn our attention to toric hypersurfaces over $R = \mathbb{F}_q$, the finite field with $q = p^a$ elements and characteristic p. Let $\mathcal{Y}$ be the hypersurface in $\mathbb{T}^n_{\mathbb{F}_q}$ defined by a Laurent polynomial $\overline{f} \in \mathbb{F}_q[x^\pm]$, $\mathcal{Y} := V(\overline{f}) \subset \mathbb{T}^n_{\mathbb{F}_q}$. Let

$$\operatorname{supp} \overline{f} = \{\alpha \in \mathbb{Z}^n : \overline{c}_\alpha \neq 0\}$$

be the support of $\overline{f}$ in $\mathbb{R}^n$; the convex hull of $\operatorname{supp} \overline{f}$ is the *Newton polytope* of $\overline{f}$, which we denote by Δ. We will work under the hypothesis that $\overline{f}$ is ($\Delta-$)*non-degenerate*:[1] for all faces $\tau \subseteq \Delta$ (including Δ itself), the system of equations

$$\overline{f}_{\restriction \tau} = \partial_1 \overline{f}_{\restriction \tau} = \cdots = \partial_n \overline{f}_{\restriction \tau} = 0$$

has no solution in $\overline{\mathbb{F}}_q^{\times n}$, where $\overline{\mathbb{F}}_q$ denotes an algebraic closure of $\mathbb{F}_q$. Furthermore, nondegeneracy implies quasi-smoothness, see [BC94, Definition 3.1 and Proposition 4.15]. For fixed normal Δ over an infinite field, this condition holds for generic $\overline{f}$. Others have given point-counting algorithms under this assumption [CDV06, SV13].

Let $\mathcal{X} := \operatorname{Proj} P_\Delta / (\overline{f})$ denote the closure of $\mathcal{Y}$ in $\mathbb{P}_\Delta$ (placing $\overline{f}$ in degree 1) and set $\mathcal{U} := \mathbb{T}^n \backslash \mathcal{Y}$. Let H^i_{rig} denote the ith rigid cohomology group in the sense of Berthelot [Ber97]. The Lefschetz hyperplane theorem, combined with Poincaré duality, show that the map

$$H^i_{\mathrm{rig}}(\mathbb{P}_\Delta) \to H^i_{\mathrm{rig}}(\mathcal{X}),$$

induced by the inclusion $\mathcal{X} \hookrightarrow \mathbb{P}_\Delta$ is an isomorphism for $i \neq n-1$ [BC94, 10.8]. This implies that the "interesting" part of the cohomology of $\mathcal{X}$ occurs in dimension $n-1$ and consists of those classes that do not come from P_Δ. Denote by $PH^{n-1}_{\mathrm{rig}}(\mathcal{X})$ the primitive cohomology group of X, defined by the (Frobenius-equivariant) exact sequence

$$0 \to H^{n-1}_{\mathrm{rig}}(\mathbb{P}_\Delta) \to H^{n-1}_{\mathrm{rig}}(\mathcal{X}) \to PH^{n-1}_{\mathrm{rig}}(\mathcal{X}) \to 0$$

With this notation, we may write

$$Z(\mathcal{X}, t) = Z(\mathbb{P}_\Delta, t) Q(t)^{(-1)^n}.$$

where

$$Q(t) := \det\bigl(1 - t \operatorname{Frob}_q | PH^{n-1}_{\mathrm{rig}}(\mathcal{X})\bigr).$$

[1] This condition was introduced by Dwork [Dwo62] without a name; the term *nondegenerate* first appears in [Kou76, Var76]. Synonyms include Δ-*regular* [Bat93, §4] and *schön* [Tev07].

Thus given $\overline{f}$, we would like to compute $Q(t)$.

The cohomology group $PH^{n-1}_{\mathrm{rig}}(\mathcal{X})$ is closely related to $H^n_{\mathrm{rig}}(\mathbb{P}_\Delta \backslash \mathcal{X})$. For example, if $\mathbb{P}_\Delta$ is a (weighted) projective space, as in [AKR10] and [Cos15], the two cohomology groups are isomorphic; see [BC94, 10.11].

3. de Rham cohomology of toric hypersurfaces

In preparation for our use of p-adic cohomology to compute $Q(t)$, we give an explicit description of the algebraic de Rham cohomology of a nondegenerate toric hypersurface in characteristic zero. We take R to be the ring $\mathbb{Z}_q$, the ring of integers of $\mathbb{Q}_q$, the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$.

Let $f \in \mathbb{Z}_q[x^{\pm}]$ be a lift of $\overline{f}$ to characteristic zero with the same support as f (it will also be nondegenerate). Consider $Y := V(f) \subset \mathbb{T} := \mathbb{T}_{\mathbb{Q}_q}$ and X, the closure of Y in $\mathbb{P}_\Delta$. Write $U := \mathbb{T} \backslash Y$, and $V := \mathbb{P}_\Delta \backslash X \simeq \operatorname{Spec}(A)$, where A is the coordinate ring of V; explicitly,

$$A \simeq \bigcup_{d=0}^{+\infty} f^{-d} P_d.$$

Let I_f be the ideal in P_Δ generated by $f, \partial_1 f, \dots, \partial_n f$. We call I_f the *toric Jacobian ideal* and the quotient ring $J_f := P_\Delta / I_f$ the *toric Jacobian ring*. Since f is nondegenerate, the ideal I_f is irrelevant in P_Δ and $\operatorname{rank}_{\mathbb{Z}_q} J_f = n! \operatorname{Vol}(\Delta)$; furthermore, $(J_f)_d = 0$ for $d > n$ [Bat93, §4]. If $\mathcal{O}_\Delta$ is not very ample, then I_f might not be generated in degree 1 and we might have $(J_f)_d = 0$ only for $d \gg n$.

Let $\Omega^\bullet$ denote the logarithmic de Rham complex of V with poles along $\mathbb{P}_\Delta \backslash \mathbb{T}$. Let $H^\bullet$ be the cohomology groups of $\Omega^\bullet$; these are naturally isomorphic to $H^\bullet_{\mathrm{dR}}(V \cap \mathbb{T} = \mathbb{T} \backslash Y = U)$ and $H^\bullet_{\mathrm{rig}}(\mathbb{T}_{\mathbb{F}_q} \backslash \mathcal{Y} = \mathcal{U})$ [Kat89].

We now provide an explicit description of the group H^n, as in [Bat93, §6 and 7], in which we will compute $Q(t)$. Set

$$\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n} \in \Omega^n,$$

and define the ascending filtration in Ω^n by

$$\operatorname{Fil}^d \Omega^n := \left\{ g f^{-d} \omega : g \in P_d \right\}.$$

The associated graded ring

$$\Omega^n := \bigoplus_{d=0}^{\infty} \operatorname{Gr}^d \Omega^n, \qquad \operatorname{Gr}^d \Omega^n := \operatorname{Fil}^d \Omega^n / \operatorname{Fil}^{d-1} \Omega^n$$

is then isomorphic to $P_\Delta/(f)$ (again placing f in degree 1).

Equip H^n with the filtration induced from Ω^n, and view H^n as the quotient of Ω^n by the $\mathbb{Q}_q$-submodule generated by the relations

$$\frac{g}{f^d}\omega - \frac{gf}{f^{d+1}}\omega \quad \text{and} \quad \frac{\partial_i(g)}{f^d}\omega - \frac{dg\partial_i(f)}{f^{d+1}}\omega \tag{3.1}$$

for each $i = 1, \dots, n$, each nonnegative integer d, and each $g \in P_d$. From these relations, we see that

$$\operatorname{Gr}^1 H^n \simeq P_1/(f) \quad \text{and} \quad \operatorname{Gr}^d H^n \simeq (J_f)_d \qquad (d > 1).$$

This gives a way to compute explicitly in H^n: for any $h \in (J_f)_{d+1}$ with $d > n$, we can find a relation of the form

$$d\frac{h}{f^{d+1}}\omega = d\frac{g_0 f + \sum_{i=1}^n g_i \partial_i f}{f^{d+1}}\omega \equiv \frac{dg_0 + \sum_{i=1}^n \partial_i g_i}{f^d}\omega. \tag{3.2}$$

because $P_d \subset (I_f)_d$, so in H^n we can reduce the pole order of any form to at most n. This process was introduced for smooth projective hypersurfaces in [Gri69] and attributed to Dwork; it is commonly known as *Griffiths–Dwork reduction*.

With the above representation of H^n, we may also identify $PH^{n-1}_{\mathrm{dR}}(X)$ with $(P_\Delta^{\mathrm{Int}} + I_f)/I_f \subset H^n$, where the filtration by pole order is the Hodge filtration; see [Bat93, BC94, §9, §11].

We now introduce a variation of Griffiths–Dwork reduction, called *controlled reduction*. This will be crucial for our application to p-adic cohomology, as careless application of Griffiths–Dwork reduction to a sparse form will easily lead to a dense form. For $d = 1, \dots, n+1$, choose a $\mathbb{Z}_q$-linear splitting $P_d \approx (J'_f)_d \oplus C_d$, where $(J'_f)_d$ is a lift of $(J_f)_d$ into P_d. Let $\rho_d \colon P_d \to (J'_f)_d$ and $\pi_{d,0}, \dots, \pi_{d,n} \colon P_d \to P_{d-1}$ be $\mathbb{Z}_q$-linear maps such that

$$g = \rho_d(g) + \pi_{d,0}(g) \cdot f + \sum_{i=1}^n \pi_{d,i}(g) \cdot \partial_i f; \quad g \in P_d.$$

These maps may be constructed one monomial at a time.

Proposition 3.1 (Controlled reduction)**.** *Let $x^\nu \in P_1$ and $x^\mu \in P_d$ be two monomials and define the following $\mathbb{Z}_q$-linear maps:*

$$R_{\mu,\nu}(g) := (d+n)\pi_{n+1,0}(x^\nu g) + \sum_{i=1}^n (\partial_i + \mu_i)(\pi_{n+1,i}(x^\nu g))$$

$$S_\nu(g) := \pi_{n+1,0}(x^\nu g) + \sum_{i=1}^n \nu_i \pi_{n+1,i}(x^\nu g)$$

Then for any $g \in P_n$ and any nonnegative integer j, in H^n we have

$$g\frac{x^{(j+1)\nu+\mu}}{f^{d+n+j+1}}\omega \equiv (d+n+j)^{-1}(R_{\mu,\nu}(g) + jS_\nu(g))\frac{x^{j\nu+\mu}}{f^{d+n+j}}\omega.$$

Proof. This is straightforward from (3.1) and (3.2). □

Note that Proposition 3.1 enables us to reduce the pole order of a differential form from $d+n+j+1$ to $d+n+j$ without increasing its total number of monomials; we can thus reduce the pole order of a sparse form without making it dense.

Corollary 3.2. *With notation as in Proposition 3.1, let k be a positive integer. Then for any $g \in P_n$,*

$$g\frac{x^{\mu+k\nu}}{f^{d+n+k}}\omega \equiv \frac{\prod_{j=0}^{k-1}(R_{\mu,\nu} + jS_\nu)(g)}{\prod_{j=0}^{k-1}(d+n+j)}\frac{x^\mu}{f^{d+n}}\omega,$$

forming the composition product from left to right.

Using Proposition 3.1 amounts to performing linear algebra on matrices of size $\#(n\Delta \cap \mathbb{Z}^n) \sim n^n \operatorname{Vol}(\Delta)$. One can reduce this by a factor of $n^n/n! \sim e^n$ at the expense of making the expression for the reduction matrix more convoluted; compare [Cos15, Proposition 1.17 and 1.18].

4 Jun 2018 15:52:35 PDT
Version 4 - Submitted to Open Book Series

4. Monsky–Washnitzer cohomology

We now indicate how Monsky–Washnitzer cohomology, as introduced in [MW68, Mon68, Mon71], provides a crucial link between algebraic de Rham cohomology and p-adic rigid cohomology, by transferring to the former the canonical Frobenius action on the latter; see also [vdP86]. To simplify, we assume $p > \max\{n, 2\}$.

Let $A^\dagger$ denote the *weak p-adic completion* of A, the ring consisting of formal sums $\sum_{d=0}^{+\infty} g_d f^{-d}$ such that for some $a, b > 0$, $g_d \in p^{\max\{0, \lfloor ad-b \rfloor\}} P_d$ for all $d \geq 0$. We define the associated logarithmic de Rham complex $\Omega^{\dagger,\bullet}$ by $\Omega^{\dagger,i} := \Omega^i \otimes_A A^\dagger$; denote the cohomology groups of this complex by $H^{\dagger,\bullet}$. We may then obtain p-adic Monsky–Washnitzer cohomology groups $H^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$. The map $\Omega^\bullet \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \to \Omega^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ is a quasi-isomorphism [Mon70, vdP86, Kat89]; that is, the induced maps $H^i \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \to H^{\dagger,i} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ are isomorphisms. We can thus identify the algebraic de Rham cohomology of U with the Monsky–Washnitzer cohomology of $\mathcal{U}$.

On the other hand, we also have $H^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \simeq H^\bullet_{\mathrm{rig}}(\mathcal{U})$ and the latter object is functorial with respect to geometry in characteristic p [Ber97]. In this way, $H^{\dagger,i}$ receives an action of the Frobenius automorphism, which we can make explicit by constructing a lift σ of the p-th power Frobenius on $\mathbb{F}_q$ to $A^\dagger$. To do so, we take the Witt vector Frobenius on $\mathbb{Z}_q$ and set $\sigma(\mu) = \mu^p$ for any monomial $\mu \in P_\Delta$. We then extend σ to $A^\dagger$ by the formula

$$\sigma\left(\frac{g}{f^d}\right) := \sigma(g)\sigma(f)^{-d} = \sigma(g) \sum_{i \geq 0} \binom{-d}{i} \frac{(\sigma(f) - f^p)^i}{f^{p(d+i)}}. \tag{4.1}$$

The above series converges (because p divides $\sigma(f) - f^p$) and the definitions ensure that σ is a semilinear (with respect to the Witt vector Frobenius) endomorphism of $A^\dagger$. We finally extend σ to $\Omega^{\dagger,\bullet}$ by $\sigma(g\,\mathrm{d}h) := \sigma(g)\,\mathrm{d}(\sigma(h))$.

5. Sketch of the algorithm

We now indicate briefly how to use controlled reduction to compute the Frobenius action on the cohomology of nondegenerate toric hypersurfaces. We start as in [Har07, Proposition 4.1], by rewriting the Frobenius action in a sparser form.

Lemma 5.1. *For any positive integers d, N and $g \in P_d$, in $A^\dagger$ we have*

$$\sigma\left(\frac{g}{f^d}\right) \equiv \sum_{j=0}^{N-1} \binom{-d}{j} \binom{d+N-1}{d+j} \sigma(gf^j) f^{-p(d+j)} \pmod{p^N}.$$

Proof. This follows from (4.1) by truncating the sum and then rewriting formally; see [Cos15, Lemma 1.10]. □

In order to compute a p-adic approximation of the Frobenius action on $PH^{n-1}(\mathcal{X})$, we must first fix a basis of the latter; we do this by constructing a monomial basis for $PH^{n-1}_{\mathrm{dR}}(X)$ via explicit linear algebra. We then apply Frobenius to each basis element in the sparse truncated form given by Lemma 5.1; recursively reduce the pole order using Corollary 3.2 (using $k = p$ as much as possible); and project to the chosen monomial basis. The dominant step is controlled reduction, which amounts to $O(pn^N \operatorname{Vol}(\Delta))$ matrix multiplications of size $n! \operatorname{Vol}(\Delta)$ per basis element.

We will not address precision estimates in this report, except to note that the machinery of [AKR10, §3.4] applies. In general, if we want N digits of p-adic accuracy, we must apply Lemma 5.1 with N replaced by $N' = N + O(n + \log N)$

and work modulo $p^{O(N')}$. Hence, with respect to p alone, we expect our algorithm to run in quasi-linear time in p and use $O(\log p)$ space.

6. K3 surfaces

We now turn our attention to examples, starting with K3 surfaces. For X a K3 surface, $\dim H^2(X) = 22$ and the Hodge numbers are $(1, 20, 1)$. A common example of a K3 surface is a smooth quartic surface in $\mathbb{P}^3$; however, they also occur in other ways, such as hypersurfaces in weighted projective spaces. Using a criterion of Miles Reid [Rei80], Yonemura [Yon90] found the complete list of (polarized) weighted projective spaces in which a generic hypersurface is a K3 surface; there are 95 of these. For toric varieties, the corresponding classification is that of reflexive 3-dimensional polytopes, of which there are 4,319 in all [KS98].

In the following examples, we worked modulo p^4 in order to obtain $Q(t)$ with 2 p-adic significant digits. As a result, we observe a performance hit for $p > 2^{16}$.

Example 6.1. Consider the projective quartic surface $\mathcal{X} \subset \mathbb{P}^3_{\mathbb{F}_p}$ defined by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0;$$

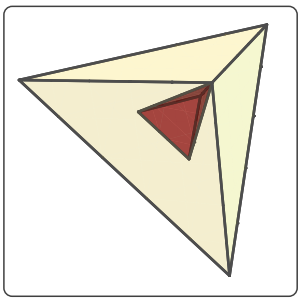
it is a member of the Dwork pencil. For $p = 2^{20} - 3$ and $\lambda = 1$, using the *controlled AKR algorithm* in `22h7m` we compute that

$$Z(\mathcal{X}, t)^{-1} = (1 - t)(1 - pt)^{16}(1 + pt)^3(1 - p^2t)Q(t),$$

where the "interesting" factor is

$$Q(t) = (1 + pt)(1 - 1688538t + p^2t^2).$$

For this family, the remaining factors, apart from $Q(t)$, could have also been deduced by a p-adic formula of de la Ossa-Kadir [Kad04, Chapter 6]. In this context, the Hodge numbers of $PH^2(\mathcal{X})$ are $(1, 19, 1)$.



A similar runtime would be expected if we used our current implementation to compute $Z(\mathcal{X}, t)$ with Δ being the 3-simplex (tetrahedron), as indicated by the outer polytope at right. Instead, we observe that the monomials defining $\mathcal{X}$ generate a sublattice of index 4^2 in $\mathbb{Z}^3$; hence, we can instead run our algorithm with a polytope of significantly smaller volume ($32/3 \approx 10.66$ versus $2/3 \approx 0.66$), as indicated by the inner polytope at right. This leads to a dramatic speedup: with our current implementation, we computed $Q(t)$ in `1m33s`. We present the running times for other p in Table 1; memory usage is about 16MB.

In the new framework, $\mathcal{X}$ is given by the closure (in $\mathbb{P}_\Delta$) of the affine surface defined by the Laurent polynomial

$$x^4y^{-1}z^{-1} + \lambda x + y + z + 1,$$

and the Hodge numbers of $PH^2(\mathcal{X})$ are $(1, 1, 1)$, which explains why $\deg Q(t) = 3$.

Since the Dwork pencil is a "small" deformation of the Fermat quartic, we may also use the Pancratz–Tuitman implementation of the *deformation method* [PT15] to compute $Z(\mathcal{X}, t)$. We did this and verified that our results agree; we compare running times in Table 1. To interpret these fairly, note that Pancratz–Tuitman work in $\mathbb{P}^3$ and so compute the whole numerator of $Z(\mathcal{X}, t)$ rather than just $Q(t)$. (Note that the algorithm of [Tui18] has a square-root dependence on p, as in [Har07].)

4 Jun 2018 15:52:35 PDT
Version 4 - Submitted to Open Book Series

p	CHK time	PT time	p	CHK time
2^8-5	0.03s	1.65s	$2^{17}-1$	11.9s
2^9-3	0.04s	3.64s	$2^{18}-5$	23.4s
$2^{10}-3$	0.04s	7.39s	$2^{19}-1$	46.9s
$2^{11}-9$	0.06s	14.65s	$2^{20}-3$	1m33s
$2^{12}-3$	0.08s	34.80s	$2^{21}-9$	3m6s
$2^{13}-1$	0.13s	34.80s	$2^{22}-3$	6m15s
$2^{14}-3$	0.22s	2m33s		
$2^{15}-19$	0.41s	6m43s		
$2^{16}-15$	5.72s	14m14s		

TABLE 1. The second and fifth columns use our current implementation to compute $Q(t)$. The third column uses the Pancratz–Tuitman implementation [PT15] to compute $Z(\mathcal{X},t)$.

Example 6.2. Consider the projective quartic surface $\mathcal{X} \subset \mathbb{P}^3_{\mathbb{F}_p}$ defined by

$$x^3y + y^4 + z^4 + w^4 - 12xyzw;$$

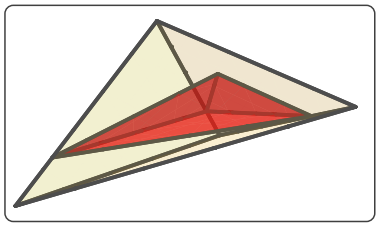
it contains a hypergeometric motive (see [DKS+16, Section 5]). For $p = 2^{15} - 19$, using the *controlled AKR algorithm* in `27m12s` we compute that

$$Z(\mathcal{X},t)^{-1} = (1-t)(1-pt)^2(1+pt)^2(1-pt+p^2t^2)^2(1-p^2t^2+p^4t^4)^2(1-p^2t)Q(t),$$

where the "interesting" factor is (up to rescaling)

$$pQ(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$

As in the previous example, the Newton polytope has volume 8, but the defining monomials generate a sublattice of index 4 in $\mathbb{Z}^3$; we may thus work instead with a polytope of volume 2 (depicted at right) and observe a significant speedup. In this setting, the Hodge numbers of $PH^2(\mathcal{X})$ are $(1,4,1)$. With our current implementation we computed $Q(t)$ in `4s`. We present the running times for other p in Table 2, where the memory footprint was about 52MB.



Alternatively, one could try to use MAGMA [BCP97] to confirm $Q(t)$. Unfortunately, MAGMA is only able to confirm the linear coefficient:

```
> C2F2 := HypergeometricData([6,12], [1,1,1,2,3]);
> EulerFactor(C2F2, 2^10 * 3^6, 2^15 - 19: Degree:=1);
1 + 20508*$.1 + O($.1^2)
```

p	time	p	time	p	time
2^8-5	0.20s	$2^{13}-1$	1.12s	$2^{18}-5$	4m54s
2^9-3	0.23s	$2^{14}-3$	2.08s	$2^{19}-1$	9m46s
$2^{10}-3$	0.29s	$2^{15}-19$	4.00s	$2^{20}-3$	19m32s
$2^{11}-9$	0.41s	$2^{16}-15$	1m11s	$2^{21}-9$	38m58s
$2^{12}-3$	0.64s	$2^{17}-1$	2m30s	$2^{22}-3$	1h18m

TABLE 2. Running times for Example 6.2.

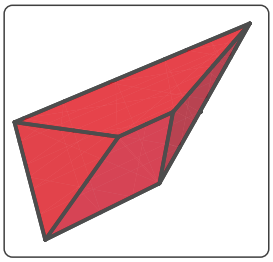
Example 6.3. Consider the closure $\mathcal{X}$ in $\mathbb{P}_\Delta$ (which in this case is not a weighted projective space) of the affine surface defined by the Laurent polynomial

$$3x + y + z + x^{-2}y^2z + x^3y^{-6}z^{-2} + 3x^{-2}y^{-1}z^{-2} \\ - 2 - x^{-1}y - y^{-1}z^{-1} - x^2y^{-4}z^{-1} - xy^{-3}z^{-1};$$

it is a K3 surface of geometric Picard rank 6, and the Hodge numbers of $PH^2(\mathcal{X})$ are $(1, 14, 1)$. For $p = 2^{15} - 19$, using our current implementation, in `6m20s` we obtain the "interesting" factor of $Z(\mathcal{X}, t)$:

$$pQ(t/p) = (1-t)\cdot(1+t)\cdot(p + 33305t^1 + 1564t^2 - 14296t^3 - 11865t^4 \\ + 5107t^5 + 27955t^6 + 25963t^7 + 27955t^8 + 5107t^9 \\ - 11865t^{10} - 14296t^{11} + 1564t^{12} + 33305t^{13} + pt^{14}).$$

We present the running times for other p in Table 3, where the peak memory usage was about 144MB.



The vertices of the associated polytope correspond to the first six terms displayed; the remaining terms are interior points. We depict this polytope of volume 8 at right.

We know of no previous algorithm that can compute $Z(\mathcal{X}, t)$ for p in this range. The defining polynomial is "dense" from the point of the Sperber–Voight algorithm [SV13], which is based on Dwork cohomology and scales with the number of monomials away from the vertices of the Newton polytope.

p	time	p	time	p	time
$2^7 - 1$	`6.46s`	$2^{10} - 3$	`18.93s`	$2^{13} - 1$	`1m46s`
$2^8 - 5$	`9.50s`	$2^{11} - 9$	`31.34s`	$2^{14} - 3$	`3m24s`
$2^9 - 3$	`12.64s`	$2^{12} - 3$	`56.23s`	$2^{15} - 19$	`6m20s`

TABLE 3. Running times for Example 6.3.

Example 6.4. Let $\mathcal{X}$ be the smooth projective surface in $\mathbb{P}^3$ defined by the fully dense, randomly chosen quartic polynomial

$$-9x^4 - 10x^3y - 9x^2y^2 + 2xy^3 - 7y^4 + 6x^3z + 9x^2yz - 2xy^2z + 3y^3z \\ + 8x^2z^2 + 6y^2z^2 + 2xz^3 + 7yz^3 + 9z^4 + 8x^3w + x^2yw - 8xy^2w \\ - 7y^3w + 9x^2zw - 9xyzw + 3y^2zw - xz^2w - 3yz^2w + z^3w - x^2w^2 \\ - 4xyw^2 - 3xzw^2 + 8yzw^2 - 6z^2w^2 + 4xw^3 + 3yw^3 + 4zw^3 - 5w^4;$$

then Δ is the 3-simplex (tetrahedron) of volume $32/3 \approx 10.66$. For this example, we have $PH^2(\mathcal{X}) \simeq H^3(\mathbb{P}^3 \backslash \mathcal{X})$, the Hodge numbers are $(1, 19, 1)$, and

$$Z(\mathcal{X}, t)^{-1} = (1-t)(1-pt)(1-p^2t)Q(t)$$

where $\deg Q(t) = 21$. For $p = 2^{15} - 19$, we obtain

$$pQ(t/p) = (1+t)\big(p - 53159t^1 + 10023t^2 - 3204t^3 + 49736t^4 - 56338t^5 + 43086t^6 \\ - 48180t^7 + 44512t^8 - 42681t^9 + 47794t^{10} - 42681t^{11} + 44512t^{12} - 48180t^{13} \\ + 43086t^{14} - 56338t^{15} + 49736t^{16} - 3204t^{17} + 10023t^{18} - 53159t^{19} + pt^{20}\big)$$

using the *controlled AKR algorithm* in `38m27s`; our current implementation takes roughly the same time. We present the running times for other p in Table 4. The memory footprint was about 230MB.

Unfortunately, the *deformation method* is not suitable for dense quartics with p in this range. For example, for $p = 31$ the running time was `2h8m` and its memory footprint was around 7GB, and both time and space should scale linearly with p.

p	time	p	time	p	time
$2^7 - 1$	`25.41s`	$2^{10} - 3$	`1m30s`	$2^{13} - 1$	`9m26s`
$2^8 - 17$	`37.73s`	$2^{11} - 9$	`2m37s`	$2^{14} - 3$	`18m42s`
$2^9 - 3$	`55.82s`	$2^{12} - 3$	`4m50s`	$2^{15} - 19$	`36m29s`

TABLE 4. Running times for Example 6.4.

7. Calabi–Yau threefolds

We next consider Calabi–Yau threefolds. Unlike for K3 surfaces, the middle Betti numbers of Calabi–Yau threefolds are not *a priori* bounded; the largest value of which we are aware is 984 (found in [KS00]).

A common example is a smooth quintic surface in $\mathbb{P}^4$. Again, additional constructions arise from generic hypersurfaces in weighted projective spaces, of which there are 7,555 in all, or more generally from toric varieties corresponding to reflexive 4-dimensional polytopes, of which there are 473,800,776 in all [KS00].

In all of the following examples, we worked modulo p^6 in order to obtain $Q(t)$ and our memory footprint ranged between 100MB and 270MB.

Example 7.1. Consider the projective quintic threefold $\mathcal{X} \subset \mathbb{P}^3_{\mathbb{F}_p}$ defined by

$$x_0^5 + x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_0x_1x_2x_3x_4 = 0;$$

it is a member of the Dwork pencil. We have

$$Z(\mathcal{X}, t) = \frac{R_1(pt)^{20} R_2(pt)^{30} Q(t)}{(1-t)(1-pt)(1-p^2t)(1-p^3t)}$$

where R_1 and R_2 are the numerators of the zeta functions of certain curves given by a formula of Candelas–de la Ossa–Rodriguez Villegas [CdlORV03].

As it is presented, we would work with $\mathbb{P}_\Delta = \mathbb{P}^4$ where Δ is the 4-simplex of volume 625/24. As in Example 6.1, the monomials of the equation generate a sublattice of index 5^3 in $\mathbb{Z}^4$, so we may instead work with a polytope whose volume is smaller by a factor of 5^3. For $p = 2^{20} - 3$, we compute the "interesting" factor

$$Q(t) = 1 - 1576492860t^1 + 2672053179370pt^2 - 1576492860p^3t^3 + p^6t^4$$

in `11m18s`; if we instead had tried to apply the *controlled AKR algorithm* to compute $Q(t)$ (and not the other factors) we extrapolate that it would take us at least 120 days. We present the running times for other p in Table 5.

Since this is a "small" perturbation of the Fermat threefold, we again attempted to confirm these results using the *deformation method*; however, this was again hampered by the fact that the Pancratz–Tuitman implementation works in $\mathbb{P}_\Delta$ instead of $\mathbb{P}^3$. For $p = 7$, it took `5h4m` and its memory footprint was around 12GB.

p	time	p	time	p	time
2^8-5	0.73s	$2^{13}-1$	6.41s	$2^{18}-5$	2m50s
2^9-3	0.77s	$2^{14}-3$	11.61s	$2^{19}-1$	5m38s
$2^{10}-3$	0.80s	$2^{15}-19$	21.98s	$2^{20}-3$	11m18s
$2^{11}-9$	2.54s	$2^{16}-15$	43.07s	$2^{21}-9$	22m41s
$2^{12}-3$	3.80s	$2^{17}-1$	1m25s	$2^{22}-3$	52m37s

TABLE 5. Running times for Example 7.1.

Example 7.2. Let $\mathcal{X}$ be the threefold defined by

$$x_0^8 + x_1^5x_2 + x_0^2x_1^2x_2x_3 + x_1x_2^3x_3 + x_1^2x_3^3 + x_0x_1x_2x_3x_4 + x_2x_3x_4^2$$

in the weighted projective space $\mathbb{P}(1, 14, 18, 20, 25)$. The Newton polytope has volume $11/3 \approx 3.67$; by changing the lattice we may instead work with a polytope of volume $1/3 \approx 0.33$. In this setting, the Hodge numbers of $PH^3(\mathcal{X})$ are $(1, 1, 1, 1)$.

For $p = 2^{20} - 3$, we compute the "interesting" factor of $Z(\mathcal{X}, t)$

$$1 - 618297672t^1 + 390956360946pt^2 - 618297672p^3t^3 + p^6t^4$$

in 32m33s. We present the running times for other p in Table 6.

p	time	p	time	p	time
2^8-5	1.90s	$2^{13}-1$	18.2s	$2^{18}-5$	8m0s
2^9-3	1.96s	$2^{14}-3$	32.9s	$2^{19}-1$	16m8s
$2^{10}-3$	2.06s	$2^{15}-19$	1m6s	$2^{20}-3$	32m33s
$2^{11}-9$	7.48s	$2^{16}-15$	2m4s	$2^{21}-9$	1h5m
$2^{12}-3$	10.9s	$2^{17}-1$	4m3s	$2^{22}-3$	2h23m

TABLE 6. Running times for Example 7.2.

Example 7.3. Let $\mathcal{X}$ be the threefold defined by

$$x_1^7 + x_0^5x_1x_2 + x_0^2x_1^2x_2x_3 + x_0^4x_2x_4 + x_0x_2^3x_3 + x_0^2x_3^3 + x_0x_1x_2x_3x_4 + x_2x_3x_4^2$$

in the weighted projective space $\mathbb{P}(10, 11, 16, 19, 21)$. Again, by choosing the right lattice, we reduce the volume of the Newton polytope from $55/12 \approx 4.58$ to $11/24 \approx 0.46$, and the Hodge numbers of $PH^3(\mathcal{X})$ are $(1, 2, 2, 1)$. For $p = 2^{20} - 3$, we computed the "interesting" factor of $Z(\mathcal{X}, t)$

$$1 - 2068001468t^1 + 3449674041773pt^2 - 3772715295733197p^2t^3 + 3449674041773p^4t^4 - 2068001468p^6t^5 + p^9t^6$$

in 2h10m. We present the running times for other p in Table 7.

p	time	p	time	p	time
2^8-5	4.47s	$2^{13}-1$	1m8s	$2^{18}-5$	32m25s
2^9-3	4.60s	$2^{14}-3$	2m8s	$2^{19}-1$	1h5m
$2^{10}-3$	4.96s	$2^{15}-19$	4m6s	$2^{20}-3$	2h10m
$2^{11}-9$	25.8s	$2^{16}-15$	8m18s	$2^{21}-9$	4h17m
$2^{12}-3$	39.1s	$2^{17}-1$	16m31s	$2^{22}-3$	9h33m

TABLE 7. Running times for Example 7.3.

Example 7.4. Let $\mathcal{X}$ be the closure in $\mathbb{P}_\Delta$ (which is not a weighted projective space) of the threefold defined by the Laurent polynomial

$$xyz^2w^3 + x + y + z - 1 + y^{-1}z^{-1} + x^{-2}y^{-1}z^{-2}w^{-3} = 0.$$

Choosing the correct lattice reduces the volume of the Newton polytope from $9/8 \approx 1.12$ to $3/8 \approx 0.38$, and the Hodge numbers of $PH^3(\mathcal{X})$ are $(1, 2, 2, 1)$. For $p = 2^{20} - 3$, we computed the "interesting" factor of $Z(\mathcal{X}, t)$

$$(1+718pt+p^3t^2)\cdot(1+1188466826t^1+1915150034310pt^2+1188466826p^3t^3+p^6t^4)$$

in `1h15m`. We present the running times for other p in Table 8.

p	time	p	time	p	time
$2^8 - 5$	`2.74s`	$2^{13} - 1$	`39.28s`	$2^{18} - 5$	`18m34s`
$2^9 - 3$	`2.80s`	$2^{14} - 3$	`1m13s`	$2^{19} - 1$	`38m8s`
$2^{10} - 3$	`3.00s`	$2^{15} - 19$	`1m21s`	$2^{20} - 3$	`1h15m`
$2^{11} - 9$	`14.86s`	$2^{16} - 15$	`4m45s`	$2^{21} - 9$	`2h32m`
$2^{12} - 3$	`22.32s`	$2^{17} - 1$	`9m12s`	$2^{22} - 3$	`5h39m`

TABLE 8. Running times for Example 7.4.

8. Cubic fourfolds

For our final example, we consider a cubic fourfold. For X a smooth cubic fourfold in $\mathbb{P}^5$, $\dim H^4(X) = 23$ and the Hodge numbers are $(0, 1, 21, 1, 0)$.

In this example, we worked modulo p^6 in order to obtain $Q(t)$.

Example 8.1. Let $\mathcal{X}$ be the smooth projective cubic fourfold in $\mathbb{P}^5_{\mathbb{F}_p}$ defined by

$$x_0^3+x_1^3+x_2^3+(x_0+x_1+2x_2)^3+x_3^3+x_4^3+x_5^3+2(x_0+x_3)^3+3(x_1+x_4)^3+(x_2+x_5)^3;$$

it is nondegenerate in $\mathbb{P}^5$. For $p = 31$, in `21h31m` we computed

$$Z(\mathcal{X}, t)^{-1} = (1 - t)(1 - pt)(1 - p^2t)(1 - p^3t)(1 - p^4t)Q(t)$$

where the "interesting" factor is an irreducible Weil polynomial given by

$$\begin{aligned} pQ(t/p^2) = {} & p-7t^1+21t^2-52t^3-8t^4-28t^5+21t^6+35t^7+39t^9+62t^{10}+23t^{11} \\ & +62t^{12}+39t^{13}+35t^{15}+21t^{16}-28t^{17}-8t^{18}-52t^{19}+21t^{20}-7t^{21}+pt^{22}; \end{aligned}$$

the coefficient of t^1 may be confirmed independently by counting $\mathcal{X}(\mathbb{F}_p)$ using the Sage function `count_points`. For $p = 127$ the running time was `23h15m` and for $p = 499$ it was `24h55m`. In both cases, we also observed that the "interesting" factor is an irreducible Weil polynomial. In these three computations, the memory footprint was around 36.5GB.

In this high-dimensional setting, the bottleneck seems to be the linear algebra required to set up controlled reduction. In this example, for $p = 31$ more than half of the running time (`15h32m`) is spent solving a linear problem of size $15{,}504 \times 37{,}128$ modulo p^6. With a more careful implementation of this step (for example, avoiding Hensel lifts) we would expect a significant speedup.

Note that the defining equation for $\mathcal{X}$ is quite sparse. To assess the effect of this sparsity, as well as to cross-check the answer, we recomputed $Z(\mathcal{X}, t)$ after applying a random linear change of variables to obtain a dense defining equation. For $p = 31$, in `27h55m` and using about 41GB we obtained the same value for $Z(\mathcal{X}, t)$ as above.

4 Jun 2018 15:52:35 PDT
Version 4 - Submitted to Open Book Series

As described in the introduction, Example 8.1 has an implication for the moduli of cubic fourfolds. A cubic fourfold is *coplanar* if it is defined by an expression of the form $\sum_{i=1}^{10} a_i^3$, in which each a_i is a linear form and some four of the a_i are linearly dependent. Ranestad–Voisin [RV17] show that the Zariski closure of the coplanar locus on the moduli space of cubic fourfolds is a divisor, denoted D_{copl}. Example 8.1 is a coplanar cubic fourfold over $\mathbb{Q}$ which is non-special: the existence of a primitive cycle class in codimension 2 would imply that $pQ(t/p^2)$ is divisible by some cyclotomic polynomial. This shows (modulo a detailed description and validation of the algorithm) that D_{copl} is not a Noether–Lefschetz divisor.

References

[AA18] Nicolas Addington and Asher Auel. Some non-special cubic fourfolds. *preprint*, 2018. `arXiv:1703.05923`.

[AKR10] T. G. Abbott, K. S. Kedlaya, and D. Roe. Bounding Picard numbers of surfaces using p-adic cohomology. In *Arithmetic, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 125–159. Soc. Math. France, Paris, 2010.

[Bat93] Victor V. Batyrev. Variations of the mixed Hodge structure of affine hypersurfaces in algebraic tori. *Duke Math. J.*, 69(2):349–409, 1993.

[BC94] Victor V. Batyrev and David A. Cox. On the Hodge structure of projective hypersurfaces in toric varieties. *Duke Math. J.*, 75(2):293–338, 1994.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[Ber97] Pierre Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128(2):329–377, 1997. With an appendix in English by Aise Johan de Jong.

[CdlORV03] P. Candelas, X. de la Ossa, and F. Rodriguez-Villegas. Calabi-Yau manifolds over finite fields. II. In *Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001)*, volume 38 of *Fields Inst. Comm.*, pages 121–157. Amer. Math. Soc., Providence, RI, 2003.

[CDV06] W. Castryck, J. Denef, and F. Vercauteren. Computing zeta functions of nondegenerate curves. *IMRP Int. Math. Res. Pap.*, pages Art. ID 72017, 57, 2006.

[CLS11] D. A. Cox, J. B. Little, and H. K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[Cos] Edgar Costa. controlledreduction: `C++` implementation of the controlled reduction method to compute Hasse–Weil zeta functions of smooth projective hypersurfaces over finite fields. https://github.com/edgarcosta/controlledreduction.

[Cos15] Edgar Costa. *Effective computations of Hasse–Weil zeta functions*. PhD thesis, New York University, 2015.

[CT14] Edgar Costa and Yuri Tschinkel. Variation of Néron-Severi ranks of reductions of K3 surfaces. *Exp. Math.*, 23(4):475–481, 2014.

[DKS+16] C. F. Doran, T. L. Kelly, A. Salerno, S. Sperber, J. Voight, and U. Whitcher. Zeta functions of alternate mirror Calabi-Yau families. *preprint*, 2016. `arXiv:1612.09249`.

[Dol82] Igor Dolgachev. Weighted projective varieties. In *Group actions and vector fields (Vancouver, B.C., 1981)*, volume 956 of *Lecture Notes in Math.*, pages 34–71. Springer, Berlin, 1982.

[DV06a] Jan Denef and Frederik Vercauteren. Counting points on C_{ab} curves using Monsky-Washnitzer cohomology. *Finite Fields Appl.*, 12(1):78–102, 2006.

[DV06b] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *J. Cryptology*, 19(1):1–25, 2006.

[Dwo62] Bernard Dwork. On the zeta function of a hypersurface. *Inst. Hautes Études Sci. Publ. Math.*, (12):5–68, 1962.

[Ger07] Ralf Gerkmann. Relative rigid cohomology and deformation of hypersurfaces. *Int. Math. Res. Pap. IMRP*, (1):Art. ID rpm003, 67, 2007.

[GG01] P. Gaudry and N. Gürel. An extension of Kedlaya's point-counting algorithm to superelliptic curves. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.

[GKS11] P. Gaudry, D. Kohel, and B. Smith. Counting points on genus 2 curves with real multiplication. In *Advances in cryptology—ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Comput. Sci.*, pages 504–519. Springer, Heidelberg, 2011.

[Gri69] Phillip A. Griffiths. On the periods of certain rational integrals. I, II. *Ann. of Math. (2) 90 (1969), 460-495; ibid. (2)*, 90:496–541, 1969.

[GS04] Pierrick Gaudry and Éric Schost. Construction of secure random curves of genus 2 over prime fields. In *Advances in cryptology—EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Comput. Sci.*, pages 239–256. Springer, Berlin, 2004.

[GS12] Pierrick Gaudry and Éric Schost. Genus 2 point counting over prime fields. *J. Symbolic Comput.*, 47(4):368–400, 2012.

[Har07] David Harvey. Kedlaya's algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.

[Har10a] D. Harvey. Computing zeta functions of certain varieties in larger characteristic. http://web.maths.unsw.edu.au/~davidharvey/talks/zetasqrtp-talk.pdf, 2010. [Accessed 15-Jan-2018].

[Har10b] D. Harvey. Computing zeta functions of projective surfaces in large characteristic. http://web.maths.unsw.edu.au/~davidharvey/talks/zetasqrtp-talk3.pdf, 2010. [Accessed 15-Jan-2018].

[Har10c] D. Harvey. Counting points on projective hypersurfaces. http://web.maths.unsw.edu.au/~davidharvey/talks/zetasurface.pdf, 2010. [Accessed 15-Jan-2018].

[Har12] Michael C. Harrison. An extension of Kedlaya's algorithm for hyperelliptic curves. *J. Symbolic Comput.*, 47(1):89–101, 2012.

[Har14] David Harvey. Counting points on hyperelliptic curves in average polynomial time. *Ann. of Math. (2)*, 179(2):783–803, 2014.

[Har15] David Harvey. Computing zeta functions of arithmetic schemes. *Proc. Lond. Math. Soc. (3)*, 111(6):1379–1401, 2015.

[Has16] Brendan Hassett. Cubic fourfolds, K3 surfaces, and rationality questions. In *Rationality problems in algebraic geometry*, volume 2172 of *Lecture Notes in Math.*, pages 29–66. Springer, Cham, 2016.

[HS14] D. Harvey and A. V. Sutherland. Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time. *LMS J. Comp. Math.*, 17(suppl. A):257–273, 2014.

[HS16] D. Harvey and A. V. Sutherland. Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II. In *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, volume 663 of *Contemp. Math.*, pages 127–147. Amer. Math. Soc., Providence, RI, 2016.

[Hub08] Hendrik Hubrechts. Point counting in families of hyperelliptic curves. *Found. Comp. Math.*, 8:137–169, 2008.

[Ito16] Kazuhiro Ito. Unconditional construction of K3 surfaces over finite fields with given L-function in large characteristic. *preprint*, 2016. arXiv:1612.05382.

[Kad04] Shabnam N. Kadir. *The arithmetic of Calabi–Yau manifolds and mirror symmetry,*. PhD thesis, Univ. of Oxford, 2004.

[Kat89] Kazuya Kato. Logarithmic structures of Fontaine-Illusie. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 191–224. Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[Kou76] A. G. Kouchnirenko. Polyèdres de Newton et nombres de Milnor. *Invent. Math.*, 32(1):1–31, 1976.

[KS98] Maximilian Kreuzer and Harald Skarke. Classification of reflexive polyhedra in three dimensions. *Adv. Theor. Math. Phys.*, 2(4):853–871, 1998.

[KS00] Maximilian Kreuzer and Harald Skarke. Complete classification of reflexive polyhedra in four dimensions. *Adv. Theor. Math. Phys.*, 4(6):1209–1230, 2000.

[Lau04a] Alan G. B. Lauder. Counting solutions to equations in many variables over finite fields. *Found. Comput. Math.*, 4(3):221–267, 2004.

[Lau04b] Alan G. B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc.*, 3:565–602, 2004.

[LW08] Alan G. B. Lauder and Daqing Wan. Counting points on varieties over finite fields of small characteristic. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 579–612. Cambridge Univ. Press, Cambridge, 2008.

[Mon68] P. Monsky. Formal cohomology. II. The cohomology sequence of a pair. *Ann. of Math. (2)*, 88:218–238, 1968.

[Mon70] Paul Monsky. *p-adic analysis and zeta functions*, volume 4 of *Lectures in Mathematics, Department of Mathematics, Kyoto University*. Kinokuniya Book-Store Co., Ltd., Tokyo, 1970.

[Mon71] Paul Monsky. Formal cohomology. III. Fixed point theorems. *Ann. of Math. (2)*, 93:315–343, 1971.

[MW68] P. Monsky and G. Washnitzer. Formal cohomology. I. *Ann. of Math. (2)*, 88:181–217, 1968.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[PT15] S. Pancratz and J. Tuitman. Improvements to the deformation method for counting points on smooth projective hypersurfaces. *Found. Comp. Math.*, 15(6):1413–1464, 2015.

[Rei80] Miles Reid. Canonical 3-folds. In *Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979*, pages 273–310. Sijthoff & Noordhoff, Alphen aan den Rijn—Germantown, Md., 1980.

[RV17] Kristian Ranestad and Claire Voisin. Variety of power sums and divisors in the moduli space of cubic fourfolds. *Doc. Math.*, 22:455–504, 2017.

[Sag] The Sage Developers. *SageMath*. `http://www.sagemath.org`.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp.*, 44(170):483–494, 1985.

[Sho] Victor Shoup. NTL: Number Theory Library. http://www.shoup.net/ntl/.

[SV13] Steven Sperber and John Voight. Computing zeta functions of nondegenerate hypersurfaces with few monomials. *LMS J. Comput. Math.*, 16:9–44, 2013.

[Tae16] Lenny Taelman. K3 surfaces over finite fields with given *L*-function. *Algebra Number Theory*, 10(5):1133–1146, 2016.

[Tev07] Jenia Tevelev. Compactifications of subvarieties of tori. *Amer. J. Math.*, 129(4):1087–1104, 2007.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017.

[Tui18] Jan Tuitman. Computing zeta functions of generic projective hypersurfaces in larger characteristic. *Math. Comp.*, 2018.

[Var76] A. N. Varchenko. Zeta-function of monodromy and Newton's diagram. *Invent. Math.*, 37(3):253–262, 1976.

[vdP86] Marius van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France (N.S.)*, (23):4, 33–59, 1986.

[Yon90] Takashi Yonemura. Hypersurface simple $K3$ singularities. *Tohoku Math. J. (2)*, 42(3):351–380, 1990.

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
E-mail address: edgarcosta@math.dartmouth.edu
URL: http://www.math.dartmouth.edu/~edgarcosta/

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
E-mail address: d.harvey@unsw.edu.au
URL: http://web.maths.unsw.edu.au/~davidharvey/

Univ. of California, San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093 USA
E-mail address: kedlaya@ucsd.edu
URL: http://kskedlaya.org/

4 Jun 2018 15:52:35 PDT
Version 4 - Submitted to Open Book Series

NUMERICAL COMPUTATION OF ENDOMORPHISM RINGS OF JACOBIANS

NILS BRUIN, JEROEN SIJSLING, AND ALEXANDRE ZOTINE

Abstract. We give practical numerical methods to compute the period matrix of a plane algebraic curve (not necessarily smooth). We show how automorphisms and isomorphisms of such curves, as well as the decomposition of their Jacobians up to isogeny, can be calculated heuristically. Particular applications include the determination of (generically) non-Galois morphisms between curves and the identification of Prym varieties.

1. Introduction

Let k be a field of characteristic 0 that is finitely generated over $\mathbb{Q}$. We choose an embedding of k into $\mathbb{C}$. In this article, we consider nonsingular, complete, absolutely irreducible algebraic curves C over k of genus g. We represent such a curve C by a possibly singular affine plane model

$$\widetilde{C}\colon f(x,y)=0, \text{ where } f(x,y)\in k[x,y]. \tag{1.1}$$

Associated to C is the Jacobian variety $J=\mathrm{Jac}(C)$ representing $\mathrm{Pic}^0(C)$. Classical results by Abel and Jacobi establish

$$J(\mathbb{C})\cong \mathrm{H}^0(C_{\mathbb{C}},\Omega^1_C)^*/\,\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})\cong \mathbb{C}^g/\Omega\mathbb{Z}^{2g},$$

for a suitable $g\times 2g$ matrix Ω, called a *period matrix* of C.

Let $J_1=\mathrm{Jac}(C_1)$ and $J_2=\mathrm{Jac}(C_2)$ be two such Jacobian varieties. The $\mathbb{Z}$-module $\mathrm{Hom}_{\overline{k}}(J_1,J_2)$ of homomorphisms defined over the algebraic closure $\overline{k}$ of k is finitely generated and can be represented as the group of $\mathbb{C}$-linear maps $\mathbb{C}^{g_1}\to\mathbb{C}^{g_2}$ mapping the columns of Ω_1 into $\Omega_2\mathbb{Z}^{g_2}$. As described in [10, §2.2], we can heuristically determine homomorphism modules, along with their tangent representations, from numerical approximations to Ω_1,Ω_2. can then serve as input for rigorous verification as in loc. cit.

In this article we consider the problem of computing approximations to period matrices for arbitrary algebraic curves for the purpose of numerically determining homomorphism modules and endomorphism rings. We also describe how to identify the (finite) symplectic automorphism groups in these rings, and with that the automorphism group of the curve. We give several examples of how the heuristic determination of such objects can be used to obtain rigorous results.

Date: May 28, 2018.

2010 *Mathematics Subject Classification.* 14H40, 14H37, 14H55, 14Q05.

Key words and phrases. curves, Riemann surfaces, period matrices, automorphisms, endomorphisms, isogeny factors.

The research of the first and third author is partially supported by NSERC.

There is extensive earlier work on computing period matrices for applications in scientific computing to Riemann theta functions and partial differential equations. For these applications, approximations that fit in standard machine precision tend to be sufficient. Number-theoretic applications tend to need higher accuracy and use arbitrary-precision approximation. Hyperelliptic curves have received most attention, see for instance Van Wamelen's [28] implementation in Magma. In practice it is limited to about 2000 digits. Recent work by Molin–Neurohr [23] can reach higher accuracy and also applies to superelliptic curves.

For general curves, a Maple package based on Deconinck and Van Hoeij [12] computes period matrices at system precision or (much more slowly) at arbitrary precision. Swierczewski's reimplementation in SageMath [26] only uses machine precision and no high-order numerical integration. During the writing of this article, another new and fast Magma implementation was developed by Neurohr [24]. See the introduction of [24] for a more comprehensive overview of the history and recent work on the subject.

Our approach is similar to the references above (in contrast to, for instance, the deformation approach taken in [25]) in that we basically use the definition of the period matrix to compute an approximation.

Algorithm Compute approximation to period matrix.
Input: f as in (1.1) over a number field and a given working precision.
Output: Approximation of a period matrix of the described curve.

1. Determine generators of the fundamental group of C (Section 2.3).
2. Derive symplectic basis $\{\alpha_1, \dots \alpha_g, \beta_1, \dots, \beta_g\}$ of the homology group $H_1(C(\mathbb{C}), \mathbb{Z})$ (Section 2.4).
3. Determine a basis $\{\omega_1, \dots, \omega_g\}$ of the space of differentials $\mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)$ (Section 3.1).
4. Approximate the period matrix $\Omega = (\int_{\alpha_j} \omega_i, \int_{\beta_j} \omega_i)_{i,j}$ using numerical integration (Section 3.2).

We list some notable features of our implementation.

a. We use *certified* homotopy continuation [19] to guarantee that the analytic continuations on which we rely are indeed correct. This allows us to guarantee that increasing the working precision sufficiently will improve accuracy.
b. We base our generators of the fundamental group on a Voronoi cell decomposition to obtain paths that stay away from critical points. This is advantageous for the numerical integration.
c. We determine homotopy generators by directly lifting the Voronoi graph to the Riemann surface via analytic continuation and taking a cycle basis of that graph. This avoids the relatively opaque procedure [27] used in [12] and [24].
d. We provide an implementation in a free and open mathematical software suite (SageMath version 8.0+), aiding verification of the implementation and adaptation and extension of its features.

We share the use of Voronoi decompositions with [28]. This is no coincidence, since the first author suggested its use to Van Wamelen at the time, while sharing an office in Sydney, and was eager to see its use tested for general curves. Dealing with hyperelliptic and superelliptic curves, [28] and [23] use a shortcut in determining homotopy generators. The explicit use of a graph cycle basis in step 1 above, while directly suggested by basic topological arguments, is to our knowledge new for an implementation in arbitrary precision.

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

The runtime of these implementations is in practice dominated by the numerical integration. The complexity for all these methods is essentially the same, see [24, §4.8] for an analysis, as well as a fairly systematic comparison. For a rough idea of performance we give here some timings for the computation of period matrices of the largest genus curves in each of our examples. Timings were done using Linux on a Intel i7-2600 CPU at 3.40GHz, at working precision of 30 decimal digits; 100 binary digits.

Curve	Maple 2018	SageMath 8.3-β0
C from Example 5.1	99.6 sec	45.5 sec
C from Example 5.2	133.2 sec	8.59 sec
D from Example 5.3	119.2 sec	12.8 sec

With recent work on rigorous numerical integration [17], which is now also available in SageMath, it would be possible to modify the program to return certified results. While this is worthwhile and part of future work, rigorous error bounds would make little difference for our applications, since we have no *a priori* height bound on the rational numbers we are trying to recognize from floating point approximations. One of our objectives is to provide input for the rigorous verification procedures described in [10].

Our main application is to find decompositions of $\mathrm{Jac}(C)$ via its endomorphism ring $\mathrm{End}_{\overline{k}}(J) = \mathrm{Hom}_{\overline{k}}(J, J)$. Idempotents of $\mathrm{End}(J)$ give rise to isogenies to products of lower-dimensional abelian varieties [5, Ch. 5], [18]. Furthermore, since $\mathrm{End}(J)$ has a natural linear action on $\mathrm{H}^0(C, \Omega^1_C)^*$, idempotents induce projections from the canonical model of C. For composition factors arising from a cover $\phi\colon C \to D$, the corresponding projection factors through ϕ, so we can recover ϕ from it. In the process, we verify ϕ rigorously, as well as the numerically determined idempotent.

Finally, having determined $\mathrm{End}(J)$, we can compute the finite group automorphisms of J that are fixed by the Rosati involution. Its action on $\mathrm{H}^0(C, \Omega^1_C)$ gives, via the Torelli Theorem [21, Theorem 12.1], a representation of the automorphism group $\mathrm{Aut}(C) = \mathrm{Aut}_{\overline{k}}(C)$ of C on a canonical model. There are other approaches to computing automorphism groups of curves, for instance [15]. The approach described here naturally finds a candidate for the *geometric* automorphism group (members of which are readily rigorously verified to give automorphisms) whereas more algebraically oriented approaches, such as the one in [15], tend only to find the automorphisms defined over a given base field or have prohibitive general running times. We describe the corresponding algorithm in Section 4.2.

These results are applied to numerically identify some Prym varieties in higher genus. In particular, we find isogeny factors $\mathrm{Jac}(D)$ of Jacobians $\mathrm{Jac}(C)$ that do not come from any morphism $C \to D$, or come from a morphism that is not a quotient by automorphisms of C.

2. Computation of homology

We compute a homology basis for $C(\mathbb{C})$ from its fundamental group. We obtain generators for this group by pulling back generators of of the fundamental group of a suitably punctured Riemann sphere covered by C. Such pullbacks can be found by determining the analytic continuations of appropriate algebraic functions. In order to make these continuations amenable to computation, we use paths that stay away from any ramification points.

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

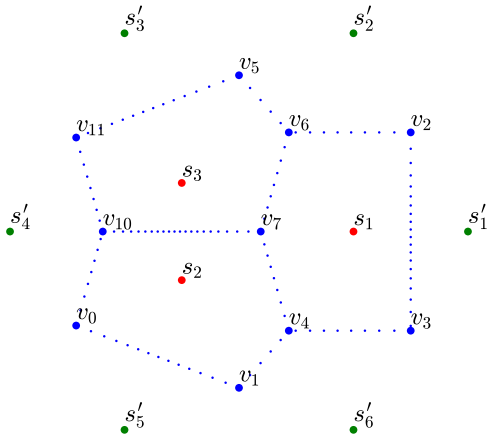


FIGURE 1. Paths for $C\colon y^2 = x^3 - x - 1$. The dots marking the edges indicate the step size used for the certified homotopy continuation.

The function x on $\widetilde{C}$ induces a morphism $x\colon C \to \mathbb{P}^1$ and therefore expresses C as a finite (ramified) cover of $\mathbb{P}^1$ of degree n say. We collect terms with respect to y and write

$$f(x,y) = f_n(x)y^n + f_{n-1}(x)y^{n-1} + \cdots + f_0(x),$$

where $f_0(x), \ldots, f_n(x) \in k[x]$, with $f_n(x) \neq 0$. We write $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, and define the *finite critical locus* of x as

$$S = \{x \in \mathbb{C} : \operatorname{disc}_y(f)(x) = 0\}.$$

We set $S_\infty = S \cup \{\infty\}$, so that x induces an unramified cover $C - x^{-1}(S_\infty)$ of $\mathbb{C} - S$.

2.1. **Fundamental group of $\mathbb{C} - S$.** We describe generators of the fundamental group of $\mathbb{C} - S$ by cycles in a planar graph that we build in the following way.

We approximate the circle with center $c_0 = \frac{1}{\#S}\sum_{s\in S} s$ and radius $2\max_{s\in S}|s - c_0|$ using a regular polygon with vertices, say, $s'_1, \ldots, s'_6$. Then we compute the Voronoi cell decomposition (see e.g. [2]) of $\mathbb{C}$ with respect to $S' = S \cup \{s'_1, \ldots, s'_6\}$. This produces a finite set of vertices $V = \{v_1, \ldots, v_r\} \subset \mathbb{C}$ and a set E of line segments e_{ij} between $v_i, v_j \in V$ such that the regions

$$F_s = \{x \in \mathbb{C} : |x - s| \leq |x - s'| \text{ for any } s' \in S' - \{s\}\}$$

have boundaries consisting of e_{ij}, together with some rays for unbounded regions. We define $F_\infty = \bigcup_{s\in S'-S} F_s$. Then we see that F_s for $s \in S_\infty$ has a finite boundary, giving a loop separating s from the rest of S_∞. See Figure 1 for an illustration of the resulting graph for the curve $C\colon y^2 = x^3 - x - 1$. It illustrates the set $S = s_1, s_2, s_3$, together with the additional points $s'_1, \ldots, s'_6$, and the vertices $v_0, \ldots, v_{11}$ and edges between them, bounding the Voronoi cells F_s.

Lemma 2.1. (i) *The boundaries of the regions F_s for $s \in S_\infty$ provide cycles that generate* $\mathrm{H}^1(\mathbb{C} - S, \mathbb{Z})$.

(ii) *The fundamental group $\pi_1(\mathbb{C} - S, v_i)$ is generated by cycles in the graph (V, E).*

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

Proof. The first claim follows because the boundaries exactly form loops around each individual point s. The second claim follows because the graph is connected. Hence, we can find paths that begin and end in v_i and (because of the first claim) provide a simple loop around a point $s \in S_\infty$. □

2.2. **Lifting the graph via homotopy continuation.** Each of our vertices $v_i \in \mathbb{C}$ has exactly n preimages $v_i^{(1)}, \dots, v_i^{(n)}$, determined by the n distinct simple roots of the equation $f(v_i, y) = 0$. We can parametrize each edge e_{ij} from our graph by $x(t) = (1-t)v_i + tv_j$ for $t \in [0, 1]$. We lift e_{ij} to paths $e_{ij}^{(1)}, \dots, e_{ij}^{(n)}$ using the branches $y^{(k)}(t)$ defined by

$$f(x(t), y^{(k)}(t)) = 0 \text{ and } y^{(k)}(0) = y(v_i^{(k)}).$$

Since e_{ij} stays away from the critical locus, the function $y^{(k)}(t)$ is well-defined by continuity. Moreover, it is analytic in a neighbourhood of $e_{ij}^{(k)}$.

Given k, we have $y^{(k)}(1) = v_j^{k'}$ for some k'. Hence, every edge e_{ij} determines a permutation σ_{ij} such that $\sigma_{ij}(k) = k'$. The lifted edge $e_{ij}^{(k)}$ connects $v_i^{(k)}$ to $v_k^{(\sigma_{ij}(k))}$. We write (V', E') for this lifted graph on $C(\mathbb{C})$. If we split up the path in sufficiently small steps, we can determine these permutations.

Lemma 2.2. *With the notation above and for given i, j, we can algorithmically determine a subdivision*

$$0 = t_0 < t_1 < t_2 < \cdots < t_{m_{ij}} = 1$$

and real numbers $\varepsilon_0, \dots, \varepsilon_{m_{ij}-1}$ such that for t, m satisfying $t_m \le t \le t_{m+1}$, we have that $|y^{(k')}(t) - y^{(k)}(t_m)| < \varepsilon_m$ if and only if $k' = k$.

Proof. We construct the t_m, ε_m iteratively, starting with $m = 0$. We set

$$\varepsilon_m = \frac{1}{3} \min\{|y^{(k_1)}(t_m) - y^{(k_2)}(t_m)| : k_1 \neq k_2\}$$

Using [19, Theorem 2.1], we can determine from $f(x(t), y)$, ε, and $x(t_m)$ a value $\delta > 0$ such that for values t satisfying $t_m \le t \le t_m + \delta$ we have that $|y^{(k)}(t) - y^{(k)}(t_m)| < \varepsilon_m$. It follows that we can set $t_{m+1} = \min(1, t_m + \delta)$. Inspection of the formulas for δ give us that if the distance of any critical point from the path is positive, then there is a finite m such that $t_m = 1$. □

Remark 2.3. In Figure 1, the dots on the edges mark the sequence $x(t_0), x(t_1), \dots, x(t_{m_{ij}})$. In particular, on the edge from v_7 to v_{10} one can see that as the distance to the branch points s_2, s_3 gets smaller, the step sizes are reduced accordingly.

Lemma 2.4. *Given $\varepsilon < \varepsilon_m$, t with $t_m < t \le t_{m+1}$, and $\widetilde{y}_m$ with $|\widetilde{y}_m - y^{(k)}(t_m)| < \varepsilon$, we can use Newton iteration to compute $\widetilde{y}$ such that $|\widetilde{y} - y^{(k)}(t)| < \varepsilon$.*

Proof. We use Newton iteration to approximate a root of $f(t, y)$, with initial value $\widetilde{y}_m$. We are looking for the unique root that lies within a radius of ε_m of the initial value. If at any point the Newton iteration process escapes this disk, or if the iteration does not converge sufficiently quickly, we insert the point $(t_m + t)/2$ and restart. We know that if Newton iteration converges to a value in the disk, it must be the correct value. Furthermore, continuity implies that convergence will occur if if $|t - t_m|$ is small enough. □

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

FIGURE 2. Examples of the intersection pairing

Since $x(t_0) \notin S$ we can use standard complex root finding algorithms on $f(x(t_0), y) = 0$, to find approximations $\widetilde{y}_0^{(k)}$ to any desired finite accuracy. We then use Lemma 2.4 iteratively to find an approximation $\widetilde{y}_m^{(k)}$ to $y^{(k)}(t_m)$, for each $m = 1, \ldots, m_{ij}$.

The Voronoi graph (V, E) generates the fundamental group of $\mathbb{C} - S$, so the lifted graph (V', E') generates the fundamental group of the unramified cover $C(\mathbb{C}) - x^{-1}(S_\infty)$, and therefore also of $C(\mathbb{C})$. We have assumed that C is an absolutely irreducible algebraic curve, so the graph is connected.

Remark 2.5. For computing integrals along $v_{ij}^{(k)}$ in Section 3.2, we store for each relevant edge e_{ij} the vectors $\{(t_m, \varepsilon_m, \widetilde{y}_m^{(1)}, \ldots, \widetilde{y}_m^{(n)}) : m \in \{0, \ldots, m_{ij}\}\}$. With this information we can quickly, reliably, and accurately approximate $y^{(k)}(t)$ for $t \in [0, 1]$ using Lemma 2.4.

2.3. **Computing the monodromy of $C \to \mathbb{P}^1$.** We do not need this in the rest of the paper, but a side effect of computing the lifted graph is that we can also compute the monodromy of the cover $C \to \mathbb{P}^1$. To any path in the Voronoi graph we associate a permutation by composing the permutations associated with the constituant edges. For example, to the path $p = (v_1, v_2, v_3)$ we associate the permutation $\sigma_p = \sigma_{12}\sigma_{23}$ (assuming that our permutations act on the right). Choosing, say, v_1 as our base point, this provides us with a group homomorphism $\pi_1(\mathbb{C} - S, v_1) \to \mathrm{Sym}(n)$. The image gives the group of deck transformations of the cover or, in terms of field theory, a geometric realization of the Galois group of the degree n field extension of $\mathbb{C}(x)$ given by $\mathbb{C}(x)[y]/(f(x, y))$. In particular, by taking a path that forms a loop around a single point $s \in C \cup \{\infty\}$, we can obtain the local monodromy of s. The cycle type of the corresponding permutation gives the ramification indices of the fibre over s. In particular, if the permutation is trivial, then $C \to \mathbb{P}^1$ is unramified over s.

2.4. **Symplectic homology basis.** Since $C(\mathbb{C})$ is a Riemann surface, it is orientable and hence we have a symplectic structure on its first homology. The pairing on cycles can be computed in the following way. Suppose that α, β are two paths intersecting at $v_0^{(1)}$, and that α contains the segment $v_1^{(1)} \to v_0^{(1)} \to v_2^{(1)}$ and that β contains the segment $v_3^{(1)} \to v_0^{(1)} \to v_4^{(1)}$. We define

$$\langle \alpha, \beta \rangle_{v_0^{(1)}} = \langle \alpha, \beta \rangle^{\text{in}}_{v_0^{(1)}} + \langle \alpha, \beta \rangle^{\text{out}}_{v_0^{(1)}}, \text{ and } \langle \alpha, \beta \rangle = \sum_v \langle \alpha, \beta \rangle_v,$$

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

where $\langle \alpha, \beta \rangle_{v_0^{(1)}} = 0$ if α or β do not pass through $v_0^{(1)}$, and otherwise

$$\langle \alpha, \beta \rangle^{\text{in}}_{v_0^{(1)}} = \begin{cases} 0 & \text{if } v_3 = v_1 \text{ or } v_3 = v_2 \\ \frac{1}{2} & \text{if } v_1, v_3, v_2 \text{ are counterclockwise oriented around } v_0 \\ -\frac{1}{2} & \text{if } v_1, v_3, v_2 \text{ are clockwise oriented around } v_0, \end{cases}$$

$$\langle \alpha, \beta \rangle^{\text{out}}_{v_0^{(1)}} = \begin{cases} 0 & \text{if } v_3 = v_1 \text{ or } v_4 = v_2 \\ \frac{1}{2} & \text{if } v_1, v_2, v_4 \text{ are counterclockwise oriented around } v_0 \\ -\frac{1}{2} & \text{if } v_1, v_2, v_4 \text{ are clockwise oriented around } v_0. \end{cases}$$

At vertices where α, β meet transversely, this is clearly the usual intersection pairing on $H_1(C(\mathbb{C}), \mathbb{Z})$. A deformation argument verifies that the half-integer weights extend it properly to cycles with edges in common.

Lemma 2.6. *By applying an algorithm by Frobenius* [14, §7] *we can find a* $\mathbb{Z}$*-basis* $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$ *for* $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$ *such that* $\langle \alpha_i, \alpha_j \rangle = \langle \beta_i, \beta_j \rangle = 0$ *and* $\langle \alpha_i, \beta_j \rangle = \delta_{ij}$.

Proof. We first compute a cycle basis for the lifted graph (V', E') described in Section 2.2, say $\gamma_1, \ldots, \gamma_r$ and compute the antisymmetric Gram matrix $G_\gamma = (\langle \gamma_i, \gamma_j \rangle)_{ij}$. Frobenius's algorithm yields an integral transformation B such that $BG_\gamma B^T$ is in symplectic normal form, i.e., a block diagonal matrix with g blocks

$$\begin{pmatrix} 0 & d_i \\ -d_i & 0 \end{pmatrix},$$

possibly followed by zeros, with $d_1 \mid d_2 \mid \cdots \mid d_g$. Because $C(\mathbb{C})$ is a complete Riemann surface, we know that $d_1 = \cdots = d_g = 1$ and that g is the genus of $C(\mathbb{C})$. The matrix B gives us $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ as $\mathbb{Z}$-linear combinations of our initial cycle basis $\gamma_1, \ldots, \gamma_r$. □

3. Computing the period lattice

3.1. **A basis for** $\mathrm{H}^0(C, \Omega^1_C)$**.** From the adjunction formula [1] we know that $\mathrm{H}^0(C, \Omega^1_C)$ is naturally a subspace of the span of

$$\left\{ \frac{h\,dx}{\partial_y f(x,y)} : h = x^i y^j \text{ with } 0 \le i, j \text{ and } i + j \le n - 3 \right\}.$$

If the projective closure of $\widetilde{C}$ is nonsingular, then $\mathrm{H}^0(C, \Omega^1_C)$ is exactly this span. If $\widetilde{C}$ has only singularities at the projective points $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$ then Baker's theorem [4] states that we can take those (i, j) for which $(i + 1, j + 1)$ is an interior point to the Newton polygon of $f(x, y)$. In even more general situations, the adjoint ideal [1, A§2] specifies exactly which subspace of polynomials g corresponds to the regular differentials on C. We use Baker's theorem when it applies and otherwise rely on Singular [11] to provide us with a basis

$$\left\{ \omega_i = \frac{h_i dx}{\partial_y f(x,y)} : i = 1, \ldots, g \right\} \subset \mathrm{H}^0(C, \Omega^1_C).$$

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

3.2. **Computing the period matrix.** Given a basis $\omega_1, \ldots, \omega_g$ for $\mathrm{H}^0(C, \Omega^1_C)$ and a symplectic basis $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$ for $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$, the corresponding *period matrix* is

$$\Omega_{\alpha\beta} = (\Omega_\alpha | \Omega_\beta) = \left(\int_{\alpha_j} \omega_i \,\middle|\, \int_{\beta_j} \omega_i \right)_{ij}.$$

The resulting *period lattice* is the $\mathbb{Z}$-span $\Lambda = \Omega_{\alpha\beta}\mathbb{Z}^{2g}$ of the columns in $\mathbb{C}^g$. As an analytic space, the Jacobian of C is isomorphic to the complex torus $\mathbb{C}^g/\Lambda$. Our paths consist of lifted line segments, so we numerically approximate the integrals along the edges $e_{ij}^{(k)}$ that occur in our symplectic basis and compute $\Omega_{\alpha\beta}$ by taking the appropriate $\mathbb{Z}$-linear combinations of these approximations. To lighten notation we describe the process for the edge $e_{12}^{(1)}$. As in Section 2.2 we parametrize the edge by

$$x(t) = (1-t)v_1 + tv_2$$

and with the stored information (see Remark 2.5), we can quickly compute $y^{(k)}(t)$ for given values of t. We obtain

$$\int_{e_{12}^{(1)}} \omega_i = (v_2 - v_1) \int_{t=0}^{1} \frac{g_i(x(t)y(t))}{\partial_y f(x(t), y(t))} dt.$$

Note that our integrand is holomorphic, so well suited for high order integration schemes such as Gauss-Legendre and Clenshaw-Curtis. We implemented Gauss-Legendre with relatively naive node computation. While in our experiments this was sufficient, there is the theoretical drawback that for very high order approximations, the determination of the integration nodes becomes the dominant part. There are sophisticated methods for obtaining the nodes with a better complexity (see [6]). Alternatively, quadrature schemes like Clenshaw-Curtis may need more evaluation nodes to obtain the same accuracy, but allow for faster computation of these nodes.

Rather than compute guaranteed bounds, we have settled on a standard error estimation scheme, as described in, for instance, [3, Section 5] to adapt the number of evaluation nodes. Since our applications will not provide proven results anyway, this is sufficient for our purposes.

Remark 3.1. There is a split in literature on how to order the symplectic basis for the period matrix. With the normalization we use, one gets that

$$\Omega_\alpha^{-1}\Omega_{\alpha\beta} = (1 \,|\, \Omega_\alpha^{-1}\Omega_\beta) = (1 \,|\, \tau)$$

where τ is a Riemann matrix, i.e., a symmetric matrix with positive definite imaginary part. Here τ represents the corresponding lattice in Siegel upper half space. In [5], the period matrix is taken to be $\Omega_{\beta\alpha}$.

4. Homomorphism and isomorphism computations

4.1. **Computing homomorphisms between complex tori.** Let C_1 and C_2 be two curves with Jacobians J_1 and J_2. Let Ω_1, Ω_2 be period matrices such that $J_1(\mathbb{C}) = \mathbb{C}^{g_1}/\Omega_1\mathbb{Z}^{2g_1}$ and $J_2(\mathbb{C}) = \mathbb{C}^{g_2}/\Omega_2\mathbb{Z}^{2g_2}$ as analytic groups.

A homomorphism $\phi\colon J_1 \to J_2$ induces a tangent map $\mathrm{H}^0(C_1, \Omega^1_{C_1})^* \to \mathrm{H}^0(C_2, \Omega^1_{C_2})^*$ and a map on homology $\mathrm{H}_1(C_1, \mathbb{Z}) \to \mathrm{H}_1(C_2, \mathbb{Z})$. After a choice of bases, these correspond

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

to matrices $T = T_\phi \in M_{g_2,g_1}(\mathbb{C})$ and $R = R_\phi \in M_{2g_2,2g_1}(\mathbb{Z})$, which we call the *tangent representation* and the *homology representation* of ϕ.

Proposition 4.1. *Let $\phi\colon J_1 \to J_2$ be a homomorphism and let T, R be the induced matrices described above.*

(i) *The matrices $T = T_\phi$ and $R = R_\phi$ satisfy $T\Omega_1 = \Omega_2 R$.*
(ii) *A pair (T, R) as in (i) comes from a uniquely determined homomorphism $\phi\colon J_1 \to J_2$.*
(iii) *Either of the elements T and R in (i) is determined by the other.*
(iv) *If the curves C_1 and C_2 as well as the chosen bases of differentials and ϕ are defined over $k \subset \overline{\mathbb{Q}}$, then the matrix T is an element of $M_{g_2,g_1}(k)$.*

Proof. These results are in [5, §1.2]. Writing $\overline{\Omega}_2$ for the element-wise complex conjugate of Ω_2, we remark for part (iii) that we can determine R from T by considering

$$\begin{pmatrix} T\Omega_1 \\ \overline{T\Omega}_1 \end{pmatrix} = \begin{pmatrix} \Omega_2 \\ \overline{\Omega}_2 \end{pmatrix} R, \tag{4.2}$$

since the first matrix on the right hand side of (4.2) is invertible. Conversely, we can determine T from R by considering the first g_1 columns on either side of $T\Omega_1 = \Omega_2 R$ since the corresponding matrices are invertible. □

We seek to recover these pairs (T, R) numerically. This question was briefly touched upon in [7, 6.1], and before that in [28, §3], but here we give some more detail.

Lemma 4.3. *Given approximations of Ω_1, Ω_2 to sufficiently high precision, we can numerically recover a $\mathbb{Z}$-basis for $\mathrm{Hom}(J_1, J_2)$, represented by matrices $R \in M_{2g_2,2g_1}(\mathbb{Z})$ and $T \in M_{g_2,g_1}(\mathbb{C})$ as in Proposition 4.1.*

Proof. Following Remark 3.1, we can normalize Ω_i to be of the form $(1 \mid \tau_i)$. We write

$$R = \begin{pmatrix} D & B \\ C & A \end{pmatrix}, \text{ where } D, B, C, A \in M_{g_2,g_1}(\mathbb{Z}).$$

Then $T = D + \tau_2 C$, and

$$B + \tau_2 A = (D + \tau_2 C)\tau_1.$$

Considering real and imaginary parts separately, we obtain $m = 2g_1g_2$ equations with real coefficients in $n = 4g_1g_2$ integer variables, denoted by $M \in M_{m,n}(\mathbb{R})$. We recognize integer solutions that are small compared to the precision to which we calculated τ_1, τ_2 in the following way. Observe that such solutions correspond to short vectors in the lattice generated by the columns of $(I \mid \varepsilon^{-1}M)$, where ε is some small real number. The LLL algorithm can find such vectors, and we keep the ones that lie in the kernel to the specified precision.

If sufficient precision is used, then we obtain a basis for $\mathrm{Hom}(J_1, J_2)$ in this way. (Heuristically, any approximation to high precision will do.) Proposition 4.1 shows how to recover the tangent representation T from the corresponding homology representations R. □

Remark 4.4. An important tuning parameter for applications of LLL is the precision. We have an (estimated) accuracy of the entries in the matrix M. We choose ε such that we $\varepsilon^1 M$ has accuracy to within 0.5. If we have computed the period matrices to a precision of b bits, then M contains about $2g_1g_2b$ bits of information. We would therefore expect that the entries in the LLL basis have entries of size about $(2g_1g_2b)/(4g_1g_2) = b/2$. We only keep vectors that have entries of bit-size at most half that.

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

In the context of Proposition 4.1(iv), the algebraic entries of T can be recognized by another application of the LLL algorithm; for example, the SageMath implementation `number_field_elements_from_algebraics` can be used to this end. We emphasize that in order to recover this algebraicity, we need the original period matrices Ω_i with respect to a basis of $H^0(C, \Omega^1_C)$ defined over $\overline{\mathbb{Q}}$. A differential basis for which the period matrix takes the shape $(1 \mid \tau_i)$ usually has a transcendental field of definition.

For a Jacobian J, the natural principal polarization gives rise to the Rosati-involution on $\mathrm{End}(J)$ (cf. [5, §5.1]). We choose a symplectic basis for $H_1(C(\mathbb{C}), \mathbb{Z})$ and denote the standard symplectic form by

$$E = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in M_{2g,2g}(\mathbb{Z}).$$

Proposition 4.5. *Let $\phi\colon J \to J$ be an endomorphism with corresponding pair (T, R) as in Proposition 4.1(i). Then the Rosati involution $\phi^\dagger$ of ϕ corresponds to the pair $(T^\dagger, R^\dagger)$ with*

$$R^\dagger = -ER^tE.$$

Proof. Since we chose our homology basis to be symplectic, the Rosati involution of the endomorphism corresponding to R corresponds to the adjoint with respect to the pairing defined by E, which is $ER^tE^{-1} = -ER^tE$. □

Remark 4.6. Proposition 4.1(iii) shows how to obtain $T^\dagger$ from $R^\dagger$.

Recall [5, Chapter 5] that any polarized abelian variety allows a decomposition up to isogeny

$$J \sim \prod_i A_i^{e_i} \tag{4.7}$$

into powers of simple polarized quotient abelian varieties A_i.

Corollary 4.8. *Let J be the Jacobian of a curve C, and let Ω be a corresponding period matrix. If we know Ω to sufficiently high precision, then we can numerically determine the factors in (4.7). Furthermore, if J is defined over $\overline{\mathbb{Q}}$, we can numerically determine a field of definition for each of the conjectural factors A_i.*

Proof. Using Lemma 4.3 we can compute generators for $\mathrm{End}(J)$. We can then determine symmetric idempotent matrices $e \in M_{2g,2g}(\mathbb{Q})$ by using meataxe algorithms, or alternatively by directly solving $e^2 = e$ in the subring of $\mathrm{End}(J)$ fixed by the Rosati involution. The columns of Ωe span a complex torus of smaller dimension. By [18] all isogeny factors of J occur this way.

In order to find a field of definition, we can determine the matrix T corresponding to e and recognize its entries as algebraic numbers. Then [18] shows that the image of the projection T is still polarized, and defined over the corresponding field. □

4.2. **Computing symplectic isomorphisms.** When $g_1 = g_2$, Lemma 4.3 allows us to recover possible isomorphisms between J_1 and J_2, as these correspond to the matrices R with $\det(R) = \pm 1$.

In particular, this gives us a description of the automorphism group of a Jacobian variety J as the subgroup of elements of $\mathrm{End}(J)$ with determinant 1. This group can be infinite. However, note that we have principal polarizations on J_1 and J_2. We take symplectic bases

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

for the homology of both Jacobians, and let $\alpha : J_1 \to J_2$ be an isomorphism, represented by $R \in M_{2g,2g}(\mathbb{Z})$.

Definition 4.9. We say that α is *symplectic* if we have $R^t E R = E$.

Remark 4.10. More intrinsically, the definition demands that the canonical intersection pairings E_1 and E_2 on on $\mathrm{H}_1(C_1, \mathbb{Z})$ and $\mathrm{H}_1(C_2, \mathbb{Z})$ satisfy $\alpha^* E_2 = E_1$.

The symplectic automorphisms of J form a group, which is called the *symplectic automorphism group* $\mathrm{Aut}(J, E)$ of the principally polarized abelian variety (J, E).

Theorem 4.11. *Suppose that C is a smooth curve of genus at least 2. Then we have the following.*

(i) *The symplectic automorphism group of J is finite.*
(ii) *There is a canonical map $\mathrm{Aut}(C) \to \mathrm{Aut}(J, E)$. If C is non-hyperelliptic, then this map is an isomorphism; otherwise it induces an isomorphism $\mathrm{Aut}(C) \xrightarrow{\sim} \mathrm{Aut}(J, E)/\langle -1 \rangle$.*

Proof. Part (i) is [5, 5.1.9], and (ii) is the Torelli theorem [21, Theorem 12.1]. □

This shows we can recover $\mathrm{Aut}(C)$ from $\mathrm{Aut}(J, E)$. In fact, from the linear action of the symplectic automorphism on $H^0(C, \Omega^1_C)^*$ we can recover its action on a canonical model of C in $\mathbb{P}H^0(C, \Omega^1_C)^*$. For non-hyperelliptic curves this realizes the isomorphism $\mathrm{Aut}(J, E)/\langle -1 \rangle \simeq \mathrm{Aut}(C)$ explicitly. For hyperelliptic curves it recovers the *reduced* automorphism group, which can in fact be determined more efficiently by purely algebraic methods, as described in [20].

If C is defined over $\overline{\mathbb{Q}}$, then we can verify that the numerical automorphisms thus obtained are correct by working purely algebraically: by Proposition 4.1(iv) we obtain an algebraic expression for T. We can then check by exact calculation that it fixes the defining ideal of the canonical embedding of C.

More generally, given two Jacobians J_1 and J_2, we can determine the numerical symplectic isomorphisms between them. To this end, one proceeds as in the proof of [5, 5.1.8]: we have

$$R^t E_2 R = E_1 \tag{4.12}$$

or

$$(E_1^{-1} R^t E_2) R = 1. \tag{4.13}$$

In particular, we get

$$\mathrm{tr}((E_1^{-1} R^t E_2) R) = 2g \tag{4.14}$$

for the common genus g of C_1 and C_2. Let $B = \{B_1, \ldots, B_d\}$ be a $\mathbb{Z}$-basis of $\mathrm{Hom}(J_1, J_2)^\dagger$. Then we can write

$$R = \sum_{i=1}^{d} \lambda_i B_i. \tag{4.15}$$

The positivity of the Rosati involution implies that the set of solutions $\lambda_1, \ldots, \lambda_d$ of (4.14) is finite. Explicitly, these can be obtained by using the Fincke-Pohst algorithm [13]. For the finite set of solutions thus obtained, we check which yield matrices R in (4.15) that numerically satisfy (4.13). These matrices constitute the homology representations R of the elements of our numerical approximation to $\mathrm{Aut}(J, E)$. From this, we can obtain the

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

corresponding tangent representations T by Proposition 4.1(iii), and we can verify these algebraically as above.

Remark 4.16. Using the same methods, one can determine the maps $C_1 \to C_2$ of a fixed degree d by finding the α for which $\alpha_* E_1 = dE_2$. This is especially useful if the genus g_2 of C_2 is larger than 2, since then we can bound d by $(2g_1 - 2)/(2g_2 - 2)$.

In this way, we obtain the following pseudocode.

Algorithm Compute isomorphisms between curves.
Input: Planar equations f_1, f_2 for two curves C_1, C_2, as well as a given working precision.
Output: A numerical determination of the set of isomorphisms $C_1 \to C_2$.

1. Check if $g(C_1) = g(C_2)$; if not, return the empty set;
2. Check if C_1 and C_2 are hyperelliptic; if so, use the methods in [20];
3. Determine the period matrices P_1, P_2 of C_1, C_2 to the given precision, using the algorithm in the introduction;
4. Using Lemma 4.3 (see also [7, 6.1]), determine a $\mathbb{Z}$-basis of $\mathrm{Hom}(J_1, J_2) \subset M_{2g,2g}(\mathbb{Z})$ represented by integral matrices $R \in M_{2g,2g}(\mathbb{Z})$;
5. Using linear algebra over $\mathbb{Z}$, determine a $\mathbb{Z}$-basis $B = \{B_1, \dots, B_d\}$ of the abelian subgroup $\mathrm{Hom}(J_1, J_2)^\dagger = \{R \in \mathrm{Hom}(J_1, J_2) \mid -ER^tE = R\}$;
6. Using Fincke-Pohst, determine the finite set $S = \left\{R \in \mathrm{Hom}(J_1, J_2)^\dagger \mid \mathrm{tr}((E_1^{-1}R^tE_2)R) = 2g\right\}$;
7. Using the canonical morphisms with respect to the chosen bases of differentials, return the subset of elements of S that indeed induce an isomorphism $C_1 \to C_2$.

5. Examples

The examples in this section can be found online at [9].

Example 5.1. Consider the curve

$$C : 4x^6 - 54x^5y - 729x^4 + 108x^3y^3 + 39366x^2 - 54xy^5 - 531441.$$

This is a non-hyperelliptic curve of genus 6. Theorem 4.11 shows that, at least numerically, its geometric automorphism group is of order 2 and generated by the involution $\iota : (x, y) \mapsto (-x, -y)$. Lemma 4.3 shows that its numerical geometric endomorphism ring is of index 6 in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

The quotient of C by its automorphism group gives a morphism of degree 2 to the genus 2 curve

$$D_1 : y^2 = x^6 - x^5 + 1.$$

This corresponds to the symmetric idempotent $e_1 = 1 - (1 + \iota)/2$ in the endomorphism algebra, whose tangent representation has numerical rank 4. Numerically, there are two other such symmetric idempotents e_2, e_3. Together, their kernels span $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$, and all of these are of dimension $4 = 2 \cdot 2$. This means that along with $A_1 = \mathrm{Jac}(D_1)$ there should be two other 2-dimensional abelian subvarieties A_2, A_3 of $\mathrm{Jac}(C)$ such that

$$\mathrm{Jac}(C) \sim A_1 \times A_2 \times A_3.$$

We now describe the abelian varieties A_2 and A_3.

The tangent representation of an idempotent e_i corresponding to a factor A_i has dimension 4. Its kernel is therefore a subspace W_i of $\mathrm{H}^0(C, \Omega^1_C)$ of dimension 2. If the idempotent e_i

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

is induced by a map of curves $p : C \to D_i$, then $W_i = p^* \mathrm{H}^0(D_i, \Omega^1_{D_i})$ for some curve D_i and some projection $p\colon C \to D_i$.

By composing the canonical map with the projection to the projective line $\mathbb{P}W_i$, all the idempotents e_i give rise to a cover $C \to \mathbb{P}W_i$. Now if e_i is induced by a projection $C \to D_i$ at all, then D_i is a subcover of this map $C \to \mathbb{P}W_i$. It turns out that all e_i give rise a subcover of the degree 6 non-Galois cover

$$C \to \mathbb{P}^1$$
$$(x, y) \to y/x.$$

A monodromy calculation gives the Galois closure $Z \to \mathbb{P}^1$ of this cover: its Galois group G is dihedral of order 12. In particular, considering the subgroups of G that properly contain the degree 2 subgroup corresponding to $C \to \mathbb{P}^1$, we see that there exist exactly two non-trivial subcovers $p_1\colon C \to D_1$ and $p_2\colon C \to D_2$ of $C \to \mathbb{P}^1$. These subcovers have degree 2 and degree 3, respectively.

The curves D_1 and D_2 are both of genus 2. The first subcover p_1 is a quotient of C and corresponds to the curve D_1 above. The second subcover p_2 is not a quotient of C, but using Galois theory for the normal closure still furnishes us with a defining equation of D_2, namely

$$D_2\colon y^2 = -16x^5 - 40x^4 + 32x^3 + 88x^2 - 32x - 23.$$

We take A_2 to be the Jacobian of D_2.

Since we have exhausted all subcovers of the Galois closure $Z \to \mathbb{P}^1$, we conclude that A_3 does not arise from a cover $C \to D_3$. Still, using analytic methods we find that numerically the subvariety A_3 is simple and admits a (unique) principal polarization. It is therefore the Jacobian of a curve D_3 of genus 2. Calculating the Igusa invariants numerically, we reconstruct

$$D_3\colon y^2 = x^6 + 3x^4 + 3x^2 + x + 1.$$

We can numerically check that there is a morphism of abelian varieties $\mathrm{Jac}(C) \to \mathrm{Jac}(D_3)$ that is compatible with the polarizations on both curves. A computation on homology again shows that this morphism cannot come from a morphism of curves $C \to D_3$; if it did, the degree of such a morphism would have to be 6, which is impossible in light of the Riemann-Hurwitz formula. An explicit correspondence between C and D_3 can in principle be found by using the methods in [10]; however, this will still be a rather involved calculation, which we have therefore not performed yet.

Example 5.2. Consider the plane model

$$C\colon f(x, y) = 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$$

of the Macbeath curve from [16], which is due to Bradley Brock. Its automorphism group is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_8)$ and has order 504. We illustrate that the algorithm described in Section 4.2 indeed recovers that $\mathrm{Aut}(C)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_8)$, that C is indeed the Macbeath curve, and moreover that all the automorphisms of C are already defined over the cyclotomic field $\mathbb{Q}(\zeta_7)$.

From the adjoint ideal computed by Singular [11] we find a $\mathbb{Q}$-rational basis of 7 global differentials of the form $h\omega$, where $\omega = \frac{\partial f}{\partial y}dx$ and where h is one of

$$\{h_1, \ldots, h_7\} = \{4x^2y^2 + 3xy + 1, 2y^5 - x^3y - x^2, 2xy^4 + x^4 + y^3,$$
$$4x^2y^3 + 3xy^2 + y, 4x^3y^2 + 3x^2y + x, 2x^4y + y^4 + x^3, 2x^5 - xy^3 - y^2\}.$$

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

We can determine a corresponding period matrix to binary precision 100 after about a minute's calculation, and find the corresponding numerical symplectic automorphism group. It indeed has cardinality 1008, and its elements are well-approximated by relatively simple matrices in the cyclotomic field $\mathbb{Q}(\zeta_7)$ that also generate a group $G \subset \mathrm{GL}_7(\mathbb{Q}(\zeta_7))$ of order 1008 with $G \cap \mathbb{Q}(\zeta_7)^* = \langle -1 \rangle$ and with $G/\langle -1 \rangle \cong \mathrm{PSL}_2(\mathbb{F}_2^3)$. In practice this is of course indication enough that the automorphism group has been found.

To prove this, we choose two elements T_1, T_2 of G. The first of these is the diagonal matrix with entries $\{1, \zeta_7^2, \zeta_7^4, \zeta_7^6, \zeta_7, \zeta_7^3, \zeta_7^5\}$; the other has relatively modest entries but is still too large to write down here. We check that these matrices generate a subgroup of G of cardinality 504 that projects isomorphically to $G/\langle -1 \rangle$. If we show that T_1 and T_2 indeed correspond to automorphisms of C, then our claims will be proved, since any curve of genus 7 with (at least) 504 automorphisms is birational to the Macbeath curve.

To verify this claim, one can use the canonical embedding of C with respect to the given basis of global differentials $\{h_i\omega\}$. Alternatively, one observes that

$$x = h_5/h_1,\ y = h_4/h_1.$$

This means that after applying one of the transformations T_1, T_2 to the basis of global differentials to obtain the linear transformations $\{T_i(h_j\omega)\}_j$, we can recover corresponding transformations x' and y' in x and y via

$$x' = T_i(h_5\omega)/T_i(h_1\omega),\ y' = T_i(h_4\omega)/T_i(h_1\omega).$$

For T_1, we get

$$x' = \zeta_7 x,\ y' = \zeta_7^6 y,$$

while when evaluating natively for T_2 we get two decidedly unpleasant rational expressions the degree of whose denominator and numerator both equal 5. In either case, we can check that the corresponding substitutions leave the equation for C invariant, which provides us with the desired verification of correctness of T_1 and T_2.

Example 5.3. This example illustrates the value of being able to verify isogeny factors of Jacobians numerically. We consider a genus 4 curve C and an unramified double cover $\pi\colon D \to C$. Then D is of genus 7, and $\mathrm{Jac}(D)$ is isogenous to $\mathrm{Jac}(C) \times A$ for some 3-dimensional abelian variety A. The theory of Prym varieties shows we can take A to be principally polarized. It follows that generally A is a quadratic twist of a Jacobian of a genus 3 curve F. In [22] W.P. Milne constructs a plane quartic F from a genus 4 curve C with data that amounts to specifying an unramified double cover of C. One would guess that $\mathrm{Jac}(F)$ is indeed the Prym variety of D/C. Here we check this numerically for a particular example. A modern, systematic treatment of this construction is in preparation [8].

Let C be the canonical genus 4 curve in $\mathbb{P}^3$, described by $\Gamma_2 = \Gamma_3 = 0$, where

$$\Gamma_2 = x^2 + xy + y^2 + 3xz + z^2 - yw + w^2, \Gamma_3 \ = xyz + xyw + xzw + yzw.$$

A plane model for this curve is given by

$$\begin{aligned}\widetilde{C}\colon\ & y^4w^2 - y^3w^3 + y^2w^4 + 2y^4w - y^3w^2 + 2yw^4 + y^4 - 2y^2w^2 \\ & + yw^3 + w^4 - y^2w - yw^2 + y^2 + 2yw + w^2 = 0.\end{aligned}$$

Since Γ_3 has four nodal singularities in general position, it is a Cayley cubic. It admits a double cover unramified outside the nodes, obtained by adjoining the square root of the

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

Hessian of Γ_3. Since C does not pass through the nodes, this induces an unramified double cover D of C. It is geometrically irreducible and admits a plane model

$$\widetilde{D}\colon u^4v^4 - 3u^4v^2 + u^4 - u^3v^3 - 2u^3v + u^2v^2 - u^2 + 3uv^3 + 2uv + v^4 + v^2 + 1 = 0.$$

Milne's construction yields a plane quartic

$$\begin{aligned} F\colon 5s^4 + 28s^3t + 28s^3 + 47s^2t^2 + 76s^2t + 44s^2 + 34st^3 + 82st^2 \\ +66st + 18s + 16t^4 + 34t^3 + 32t^2 + 18t + 1 = 0. \end{aligned}$$

Numerical computation shows that $\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}$ and that $\mathrm{End}(\mathrm{Jac}(F)) = \mathbb{Z}$, which can be confirmed by the ℓ-adic methods in [10]. It follows that $\mathrm{Hom}(\mathrm{Jac}(F), \mathrm{Jac}(C)) = 0$. Furthermore, we find that $\mathrm{Hom}(\mathrm{Jac}(C), \mathrm{Jac}(D))$ and $\mathrm{Hom}(\mathrm{Jac}(F), \mathrm{Jac}(D))$ are 1-dimensional, so it follows that $\mathrm{Jac}(D) \sim \mathrm{Jac}(C) \times \mathrm{Jac}(F)$ and that $\mathrm{Jac}(F)$ lies in the Prym variety of the cover $D \to C$. Thus, we obtain numerical evidence that Milne indeed provides a construction of a curve F generating the Prym variety.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften, vol. 267, Springer-Verlag, New York, 1985.

[2] Franz Aurenhammer, *Voronoi diagrams–a survey of a fundamental geometric data structure*, ACM Comput. Surv. **23** (September 1991), no. 3, 345–405.

[3] David H. Bailey, Karthik Jeyabalan, and Xiaoye S. Li, *A comparison of three high-precision quadrature schemes*, Experiment. Math. **14** (2005), no. 3, 317–329.

[4] H. F. Baker, *Examples of the application of Newton's polygon to the theory of singular points of algebraic functions*, Transactions of the Cambridge Philosophical Society **15** (1893), 403.

[5] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, Second, Grundlehren der Mathematischen Wissenschaften, vol. 302, Springer-Verlag, Berlin, 2004.

[6] I. Bogaert, *Iteration-free computation of Gauss-Legendre quadrature nodes and weights*, SIAM J. Sci. Comput. **36** (2014), no. 3, A1008–A1026.

[7] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 235–254.

[8] Nils Bruin and Emre Sertoz, *Prym varieties of genus 4 curves*, 2018. In preparation.

[9] Nils Bruin, Jeroen Sijsling, and Alexandre Zotine, *Calculations with numerical Jacobians*, 2018. https://github.com/nbruin/examplesNumericalEndomorphisms.

[10] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, 2016. arXiv:1707.01158.

[11] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *4-1-1 — A computer algebra system for polynomial computations*, 2018.

[12] Bernard Deconinck and Mark van Hoeij, *Computing Riemann matrices of algebraic curves*, Phys. D **152/153** (2001), 28–46. Advances in nonlinear mathematics and science.

[13] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), no. 170, 463–471.

[14] G. Frobenius, *Theorie der linearen Formen mit ganzen Coefficienten*, Crelle **86** (1879), 146–208.

[15] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*, Algorithmic number theory, 2004, pp. 263–271.

[16] Ruben A. Hidalgo, *About the Fricke-Macbeath curve*, 2017. arXiv:1703.01869.

[17] Frederik Johansson, *Numerical integration in arbitrary-precision ball arithmetic*, 2018. arXiv:1802.07942.

[18] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327.

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

[19] Stefan Kranich, *An epsilon-delta bound for plane algebraic curves and its use for certified homotopy continuation of systems of plane algebraic curves*, 2015. arXiv:1505.03432.
[20] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, 2013, pp. 463–486.
[21] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 167–212.
[22] W. P. Milne, *Sextactic cones and tritangent planes of the same system of a quadri-cubic curve*, Proceedings of the London Mathematical Society **s2-21** (1923), no. 1, 373–380.
[23] Pascal Molin and Christian Neurohr, *Computing period matrices and the Abel-Jacobi map of superelliptic curves*, 2017. arXiv:1707.07249.
[24] Christian Neurohr, *Efficient integration on Riemann surfaces and applications*, Ph.D. Thesis, 2018.
[25] Emre Can Sertöz, *Computing periods of hypersurfaces*, 2018. arXiv:1803.08068.
[26] Chris Swierczewski, *abelfunctions: A library for computing with Abelian functions, Riemann surfaces, and algebraic curves*, 2017. https://github.com/abelfunctions/abelfunctions.
[27] C. L. Tretkoff and M. D. Tretkoff, *Combinatorial group theory, Riemann surfaces and differential equations*, Contributions to group theory, 1984, pp. 467–519.
[28] Paul B. van Wamelen, *Computing with the analytic Jacobian of a genus 2 curve*, Discovering mathematics with Magma, 2006, pp. 117–135.

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6
E-mail address: nbruin@sfu.ca

Institut für Reine Mathematik, Universität Ulm, Helmholtzstrasse 18, 89081 Ulm, Germany
E-mail address: jeroen.sijsling@uni-ulm.de

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6

18 Jun 2018 10:13:10 PDT
Version 3 - Submitted to Open Book Series

MOD-2 DIHEDRAL GALOIS REPRESENTATIONS OF PRIME CONDUCTOR

KIRAN S. KEDLAYA AND ANNA MEDVEDOVSKY

Abstract. For all odd primes N up to 500000, we compute the action of the Hecke operator T_2 on the space $S_2(\Gamma_0(N), \mathbb{Q})$ and determine whether or not the reduction mod 2 (with respect to a suitable basis) has 0 and/or 1 as eigenvalues. We then partially explain the results in terms of class field theory and modular mod-2 Galois representations. As a byproduct, we obtain some nonexistence results on elliptic curves and modular forms with certain mod-2 reductions, extending prior results of Setzer, Hadano, and Kida.

1. Introduction

1.1. **Computations and theorems.** For N a positive integer and k a positive even integer, let $S_k(\Gamma_0(N), \mathbb{Q})$ be the space of weight-k rational cusp forms for the group $\Gamma_0(N)$, equipped with the Hecke operators T_p for all primes p not dividing N. For N prime with $2 < N < 500000$, we computed the matrix of T_2 acting on some basis of $S_2(\Gamma_0(N), \mathbb{Q})$; this was done using Cremona's implementation of modular symbols, as documented in [9], via the `eclib` package in `Sage` [29]. We then used the `m4ri` package in `Sage`, which implements the "method of four Russians" [1, Chapter 9], to compute the rank of the reductions of T_2 and $T_2 - 1$ mod 2. These computations took a few CPU-months; we did not make an accurate costing because our method is almost certainly not optimal (see below).

From this data, we observed the following behavior of the mod-2 matrix of T_2.

- For $N \equiv 3 \bmod 8$, the eigenvalue 0 always occurs if $N > 3$.
- For $N \equiv 1, 3, 5 \bmod 8$, the eigenvalue 1 always occurs if $N > 163$.
- For $N \equiv 1 \bmod 8$, the eigenvalue 0 occurs with probability 16.8%.
- For $N \equiv 5 \bmod 8$, the eigenvalue 0 occurs with probability 42.2%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 0 occurs with probability 17.3%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 1 occurs with probability 47.9%.

These results can be partially explained (see section 7) by combining the Cohen-Lenstra heuristics [8] with a detailed count of the maximal ideals of the mod-2 Hecke algebra with residue field $\mathbb{F}_2$. The bulk of the paper is devoted to making these counts (Theorems 2 and 12) using class field theory plus the theory of modular Galois representations. As a byproduct, we recover some nonexistence results of Setzer [33], Hadano [14], and Kida [20] for elliptic curves of conductor N or $2N$ with N prime, derived using a totally different approach: a diophantine analysis of discriminants of Weierstrass equations due to Ogg [26].

The first author was supported by NSF (grant DMS-1501214) and UC San Diego (Warschawski Professorship). The second author was supported by an NSF postdoctoral research fellowship (grant DMS-1703834) and has gratefully enjoyed the hospitality of the Max Planck Institute for Mathematics during the writing of this paper.

11 Jun 2018 17:59:18 PDT
Version 2 - Submitted to Open Book Series

For $N < 200000$, we also computed the multiplicities of 0 and 1 as generalized eigenvalues of the mod-2 reduction of the matrix of T_2. (These multiplicities are independent of the choice of basis.) These are somewhat more complicated to analyze because the self-adjointness of T_p with respect to the Petersson inner product does not guarantee diagonalizability mod ℓ; hence the computed multiplicity is an upper bound for the count of maximal ideals, and either both are zero or both are nonzero, but more work is needed to explain the full multiplicity. See Conjecture 13 for a step in this direction; existing work on failure of multiplicity one in characteristic 2 (e.g., [21]) suggests that even conjecturally, it may be difficult to formulate a more precise conjecture without allowing for some sporadic exceptions.

1.2. **Motivation: tabulation of rational eigenforms.** Although these results may be of independent interest, for context we indicate how they were motivated by some considerations around the tabulation of rational eigenforms. Via the modularity theorem, isogeny classes of elliptic curves of conductor N correspond to rational newforms in $S_2(\Gamma_0(N), \mathbb{Q})$; finding rational eigenforms within $S_2(\Gamma_0(N), \mathbb{Q})$ is the rate-limiting step in Cremona's algorithm for tabulating rational elliptic curves of a given conductor, as documented in [9] and executed to date for $N \leq 400000$ [13]. (The table is also available in `PARI/GP` [27], `Magma` [36], and `Sage`.)

Within this step of Cremona's algorithm, the rate-limiting substep is the computation of the kernel of $T_p - a_p$ where p is the smallest prime not dividing N and a_p runs over all integers with $|a_p| \leq 2\sqrt{p}$. Once this step is done, the resulting kernels are typically of much smaller dimension than the original space, so it is of negligible difficulty to diagonalize the restrictions of enough additional Hecke operators to isolate all one-dimensional joint eigenspaces. (The fact that this catches all rational eigenforms is a consequence of self-adjointness and strong multiplicity one.)

Recall that linear algebra over $\mathbb{Q}$ is not generally performed using generic algorithms due to intermediate coefficient explosion; it is better to use a multimodular approach in which one does linear algebra over $\mathbb{F}_\ell$ for various small primes ℓ and reconstructs the final answer using the Chinese remainder theorem. In Cremona's implementation of his algorithm, he uses only the single prime $\ell = 2^{30} - 35$; to date, this has provided enough information to identify the kernel of $T_p - a_p$.

The present work was motivated by a desire to understand the following question: to what extent (if any) can this algorithm be accelerated using linear algebra over $\mathbb{F}_\ell$ for a single small ℓ, such as $\ell = 2$? Of course, one does not expect the result of computing the kernel of $T_p - a_p$ mod ℓ to provide enough information to identify the kernel over $\mathbb{Q}$. However, for N large, the probability that $S_2(\Gamma_0(N), \mathbb{Q})$ admits any rational newforms is relatively small: by analogy with the corresponding estimate for elliptic curves sorted by naïve height [5] or Faltings height [17], one expects that only $O(X^{5/6})$ of positive integers up to X occur as levels of rational newforms. Consequently, there are likely to be many values of N for which $T_p - a_p$ has no kernel at all over $\mathbb{Q}$; if this remains true mod ℓ, then finding this out would provide an early abort mechanism. A more sophisticated early abort strategy would be to calculate not the rank of $T_p - a_p$, but rather

$$\begin{aligned}&\text{(contribution from level } N \text{ newforms)}\\ &= \text{(eigenvalue multiplicity of 0)} - \sum_{d<N, d|N} \tau(N/d)\text{(contribution from level } d \text{ newforms)}\end{aligned}$$

where $\tau(n)$ is the number of divisors of n; an early abort occurs if this contribution does not increase under reduction modulo ℓ.

The restriction to N prime in this paper was made for several reasons; notably, a key role in the theoretical analysis is played by Eisenstein ideals, which are well understood for N prime by the work of Mazur [23] but remain largely mysterious for general N (but still tractable for squarefree N, as in the work of Yoo [39]). However, for N prime there is no need to optimize Cremona's method: the method used by Bennett–Rechnitzer [2] to extend the tables of Stein–Watkins [34] is sufficient to compute (rigorously) a table of elliptic curves of all prime conductors up to 10^{10}. Nonetheless, we hope that a thorough understanding of the present situation will provide a blueprint for extending the analysis; see below.

1.3. **Additional questions.** We conclude this introduction with discussion of further work to be done in this direction. To begin with, our final analysis of the experimental data remains somewhat incomplete because our analysis of mod-2 Galois representations focuses on the ones with dihedral image; while representations with larger image are somewhat rarer, they do appear to make measurable contributions which we would like to see quantified.

In addition, one could repeat the analysis in various alternate situations: one could treat nonprime N, work modulo ℓ for some other prime ℓ, and/or replace weight 2 with some higher weight k. While all of these variants are of intrinsic interest, we would like to point out some recent developments in the computation of modular forms which draw attention to some particular cases.

We first reconsider our choice of method to compute the Hecke actions on $S_k(\Gamma_0(N), \mathbb{Q})$. The method of modular symbols is implemented in `Magma` [36] and `Sage` [29], and in a specially optimized form for $k = 2$ in Cremona's `eclib`. The approach used in `PARI/GP` [27] is based on trace formulas. However, for a large-scale tabulation of rational eigenforms, we believe the best approach is the method of [3] as extended by Hein–Tornaría–Voight [15] (see also [37]). Birch's original method is a variant of the Mestre–Oesterlé method of graphs [25] in the case where $k = 2$ and N is prime; Birch (partially) described his method for $k = 2$ and N squarefree, in terms of reduction of definite quadratic forms, while Hein–Tornaría–Voight generalize to higher weight by considering the action of SO(3) on nonstandard representations. Hein [16] has implemented the method in C++ for $k = 2$ and N squarefree; experimenting with this code reveals several computational benefits.

- It is extremely efficient in practice.
- The matrix of T_p is guaranteed[(i)] to be integral (but not symmetric) and optimally sparse, with at most $p + 1$ nonzero entries per row.
- It separates eigenspaces for the Atkin-Lehner involutions, thus reducing the complexity of the resulting linear algebra.
- It removes some oldforms, thus again simplifying the linear algebra. For example, if N is squarefree with an odd number of prime factors, then no oldforms appear; if N is squarefree with an even number of prime factors, one gets an old subspace from the smallest prime factor of N. For general N, one sees oldforms from levels which differ from N by a square factor.

[(i)]This is not true in Cremona's setup because projecting onto the minus part of the space of modular symbols could in principle introduce a denominator of 2; we have yet to observe this.

The early abort strategy of computing ranks modulo ℓ is potentially even more effective when using the Birch–Hein–Tornaría–Voight method, due to the separation of Atkin–Lehner eigenspaces. However, in order to realize this benefit one must probably take $\ell > 2$, as for $\ell = 2$ the two possible eigenvalues of an involution come together, so there is the chance of some problematic (for our purposes) interaction between the eigenspaces. An analysis of the case $k = 2$, N prime, $\ell = 3$ would be a natural variant of what we have done here.

Moreover, for $k > 2$ the early abort strategy may be of even greater value, as rational newforms in $S_k(\Gamma_0(N), \mathbb{Q})$ correspond to Galois representations for which there is no systematic construction available. Indeed, there is some evidence that there are only finitely many such forms for $k > 4$ [28]; extending previous exhaustive searches, particularly in the borderline case $k = 4$, would be a natural next step.

1.4. **Acknowledgments.** The authors thank Frank Calegari, Fred Diamond, Robert Pollack, Gabor Wiese, and Hwajong Yoo for helpful conversations.

2. Elliptic curves and their 2-torsion

For K a quadratic extension of $\mathbb{Q}$, write $\mathcal{O}_K$ for its ring of integers, $\mathrm{Cl}(K)$ for its class group, $h(K)$ for its class number, and $H(K)$ for its Hilbert class field. Write $\mathrm{Cl}(K, \mathfrak{a})$ for the ray class group of K with conductor $\mathfrak{a}$ and $h(K, \mathfrak{a})$ for the order of $\mathrm{Cl}(K, \mathfrak{a})$. Let $\mathfrak{p}(K)$ be a prime of K above (2), and write $\langle \mathfrak{p}(K) \rangle \subset \mathrm{Cl}(K)$ for the subgroup that $\mathfrak{p}(K)$ generates. If K is real, let $u(K)$ be a fundamental unit of K.

For E an elliptic curve, write N_E for the conductor of E. Let $\bar{\rho}_{E,2} : G_{\mathbb{Q},2N_E} \to \mathrm{GL}_2(\mathbb{F}_2)$ be the mod-2 Galois representation associated to E; it factors through G_{K_E} where $K_E := \mathbb{Q}(E[2])$ has Galois group contained in $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. By considering the subgroups of S_3 and their embeddings in $\mathrm{GL}_2(\mathbb{F}_2)$, we see that exactly one of the following alternatives holds.

(1) $E[2]$ is reducible as a Galois module, and K_E is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ unramified away from $2N$. In other words, E has at least one rational 2-torsion point.
(2) $E[2]$ is irreducible over $\mathbb{F}_2$ but becomes reducible over $\mathbb{F}_4$, and K_E is a cubic Galois extension of $\mathbb{Q}$. In other words, $G_{\mathbb{Q}}$ permutes the three non-identity points of $E[2]$ cyclically.[(ii)]
(3) $E[2]$ is absolutely irreducible over $\mathbb{F}_2$, and K_E is an S_3-extension of $\mathbb{Q}$.

Proposition 1. *If $N_E = 2^r M$ for some odd squarefree integer M and some $r \geq 0$, then $E[2]$ is either reducible or absolutely irreducible.*

Proof. Suppose to the contrary that K_E is cubic. Let ℓ be an odd prime dividing N_E. Since ℓ divides N_E exactly once, E has multiplicative reduction at ℓ; hence the action of $G_{\mathbb{Q}_\ell}$ on the 2-adic Tate module of E is reducible, and likewise for the action on $E[2]$. However, the (unique) order-3 subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ is $\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\}$, which acts irreducibly. Therefore the image of $G_{\mathbb{Q}_\ell}$ is trivial in $\mathrm{GL}_2(\mathbb{F}_2)$, and so K_E is unramified at ℓ. Since this is true for every odd ℓ dividing N_E, K_E is ramified at most at 2. But there are no cubic extensions of $\mathbb{Q}$ unramified outside 2: the maximal abelian extension unramified outside 2 is $\mathbb{Q}(\zeta_{2^\infty})$, whose Galois group is pro-2. □

[(ii)] This happens, for example, for both isogeny classes of elliptic curves of conductor 196 (`http://www.lmfdb.org/EllipticCurve/Q/196/`) and isogeny classes `a` and `c` of conductor 324 (`http://www.lmfdb.org/EllipticCurve/Q/324/`).

In light of Proposition 1, when N_E is squarefree, we say that E is *reducible* if $E[2]$ is a reducible representation of $G_{\mathbb{Q}}$ and K*-dihedral*, or simply *dihedral*, if K_E is an S_3-extension containing a quadratic extension K of $\mathbb{Q}$.

Recall that E is *ordinary (at 2)* if $a_2(E)$ is odd, and *supersingular (at 2)* otherwise. By theorems of Deligne and Fontaine (see Theorem 11), E is ordinary at 2 if and only if $\bar{\rho}_{E,2}|_{G_{\mathbb{Q}_2}}$ is reducible. In particular, reducible elliptic curves are ordinary.

The following theorem will be proved in section 5.

Theorem 2. *Let N be an odd prime.*

(1) *Every dihedral elliptic curve of conductor N is either $\mathbb{Q}(\sqrt{N})$-dihedral or $\mathbb{Q}(\sqrt{-N})$-dihedral.*

(2) **Ordinary dihedral elliptic curves:** *For $K = \mathbb{Q}(\sqrt{\pm N})$, if $3 \nmid \dfrac{h(K)}{\#\langle \mathfrak{p}(K)\rangle}$, then there are no ordinary K-dihedral elliptic curves of conductor N.*

(3) **Supersingular elliptic curves.**
   (a) *If $N \equiv 1, 7 \bmod 8$, then there are no supersingular elliptic curves of conductor N.*
   (b) *If $N \equiv 3 \bmod 8$, then every supersingular elliptic curve of conductor N is $\mathbb{Q}(\sqrt{-N})$-dihedral.*
   (c) *If $N \equiv 5 \bmod 8$, then every supersingular elliptic curve of conductor N is $\mathbb{Q}(\sqrt{N})$-dihedral. If $u(K) \not\equiv 1 \bmod 2\mathcal{O}_K$, then there are no supersingular elliptic curves of conductor N.*

(4) **Reducible elliptic curves:** *If $N \not\equiv 1 \bmod 8$, then there are no reducible elliptic curves of conductor N.*

For prime N and $K = \mathbb{Q}(\sqrt{\pm N})$, the order of $\mathfrak{p}(K)$ in $\mathrm{Cl}(K)$ divides 2 unless $N \equiv 1 \bmod 8$, so if $N \equiv 3, 5, 7 \bmod 8$ then the condition $3 \nmid \frac{h(K)}{\#\langle \mathfrak{p}(K)\rangle}$ in (2) is equivalent to $3 \nmid h(K)$. Similarly, if $N \not\equiv 7 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-N})$, then the condition $3 \nmid \frac{h(K)}{\#\langle \mathfrak{p}(K)\rangle}$ in (2) is equivalent to $3 \nmid h(K)$.

Theorem 2 includes a theorem of Setzer [33, Theorem 1]: if N is a prime congruent to 1 or 7 mod 8 such that $3 \nmid h(\mathbb{Q}(\sqrt{\pm N}))$, then every elliptic curve of conductor N is reducible. With similar methods, we also recover the following results of Hadano [14, Theorem II, Theorem III] and Kida [20, Theorem 3.3]. (Kida's original statement requires $N - 64$ to not be a square; for $N \neq 17$, this is equivalent to existence of a reducible elliptic curve of conductor N [33, Theorem 2]. See also [14, Theorem I].)

Theorem 3 (Hadano)**.** *Let N be a prime such that $3 \nmid h(\mathbb{Q}(\sqrt{\pm N})), h(\mathbb{Q}(\sqrt{\pm 2N}))$.*

(1) *If $N \equiv 1, 7 \bmod 8$, then every elliptic curve of conductor $2N$ is reducible.*
(2) *If $N \equiv 3, 5 \bmod 8$, there are no elliptic curves of conductor $2N$.*

Theorem 4 (Kida)**.** *Let N be a prime such that none of*

$$h(\mathbb{Q}(\sqrt{\pm N})), \quad h(\mathbb{Q}(\sqrt{(-1)^{(N-1)/2}N}), 2)$$

is divisible by 3. Then every elliptic curve of conductor N is reducible.

3. Representation theory preliminaries

To prepare for the proof of Theorem 2, we make some representation-theoretic calculations. Fix a prime p and a field $\mathbb{F}$ of characteristic p, let G be any group, and let $\rho : G \to \mathrm{GL}_2(\mathbb{F})$ be a semisimple representation. Let $\rho(G) \subset \mathrm{GL}_2(\mathbb{F})$ and

$\widetilde{\rho(G)} \subset \mathrm{PGL}_2(\bar{\mathbb{F}})$ be the image and projective image of ρ, respectively. Then exactly one of the following statements holds [32, Propositions 15–16].

(1) **Reducible case:** $\widetilde{\rho(G)}$ is a cyclic group C_n. In other words, ρ is reducible (over $\bar{\mathbb{F}}$), a sum of two characters $\chi \oplus \chi'$, and the order of χ/χ' is n.
(2) **Dihedral case:** $\widetilde{\rho(G)}$ is a dihedral group D_n of order $2n$ with $n \geq 2$. In other words, ρ is irreducible but there is an index-2 subgroup H of G, determined uniquely if $n \geq 3$, so that $\rho|_H$ splits as a sum of two characters.
(3) **Exceptional case:** $\widetilde{\rho(G)}$ is isomorphic to A_4, S_4, or A_5.
(4) **Big-image case:** $\widetilde{\rho(G)}$ contains $\mathrm{PSL}_2(\mathbb{F}_q)$ for some $q \geq 5$, but $\rho(G) \neq \mathrm{SL}_2(\mathbb{F}_5)$.[(iii)]

Call ρ *reducible*, *dihedral*, *exceptional*, or *big-image* accordingly.

3.1. The dihedral case in detail.

3.1.1. *Inducing a character.* Let $H \subset G$ be a normal subgroup. Any character $\psi : H \to F^\times$ to a field F may be twisted by any $g \in G$ to obtain a new character ${}^g\psi$, defined by ${}^g\psi(h) := \psi(g^{-1}hg)$. Because ψ factors though an abelian quotient of H, one can show that ${}^g\psi$ depends only on the class $\bar{g}$ of g in G/H. We therefore write ${}^{\bar{g}}\psi$ for the twist of ψ by $\bar{g} \in G/H$.

Now suppose that $H \subset G$ has index 2 and take ρ to be the induced representation $\mathrm{Ind}_H^G \psi : G \to \mathrm{GL}_2(F)$. Let ε_H be the (at most quadratic) character of G that takes H to 1 and $G - H$ to -1. Let $\bar{g}$ be the nontrivial element of G/H. The following are well-known (e.g., see [31, 7.2.1]):

(1) $\rho|_H = \psi \oplus {}^{\bar{g}}\psi$;
(2) ρ is an irreducible representation of G if and only if $\psi \neq {}^{\bar{g}}\psi$;
(3) $\det \rho = \varepsilon_H \cdot \psi(\mathrm{Ver}_H^G)$, where $\mathrm{Ver}_H^G : G \to H^{\mathrm{ab}}$ is the *Verlagerung* (transfer) homomorphism taking $x \in G$ to $x\, g^{-1} x g$[(iv)];
(4) $\widetilde{\rho(G)} \cong D_n$, where n is the order of ${}^{\bar{g}}\psi/\psi$ (assuming ψ has finite order).

3.1.2. *Dihedral representations.* Conversely, suppose that $\rho : G \to \mathrm{GL}_2(F)$ is a dihedral representation with $\widetilde{\rho(G)} = D_n$. If $n \geq 3$, then D_n contains a unique index-2 subgroup isomorphic to C_n.[(v)] Let $H \subset G$ be the inverse image of that cyclic subgroup under the map $G \to \mathrm{GL}_2(F) \to \mathrm{PGL}_2(F)$. Since $\widetilde{\rho(H)}$ is a cyclic group, $\rho|_H$ is a reducible representation, a sum of two characters, each defined over an at-most-quadratic extension of F. Let $\psi : H \to \bar{F}^\times$ be one of these characters. Then Frobenius reciprocity and dimension considerations guarantee that the map $\mathrm{Ind}_H^G \psi \to \rho$ induced by $\psi \to \rho|_H$ is an isomorphism.

3.1.3. *The image of a dihedral representation.* Suppose further that ρ is a faithful dihedral representation of G. With H, ψ, and ${}^{\bar{g}}\psi$ as above, we have the following:

Lemma 5. (1) $\ker \psi \cap \ker {}^{\bar{g}}\psi = 1$.
(2) *H is an abelian subgroup of G.*
(3) *If $\ker \psi \subset H$ is normal in G, then ψ is faithful, so H is cyclic.*

[(iii)] The restrictions are explained by exceptional isomorphisms for small primes: $\mathrm{SL}_2(\mathbb{F}_2) \cong D_3$, $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$, $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$, $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \cong A_5$, and $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

[(iv)] One can show that $\psi(\mathrm{Ver}_H^G)$ takes $x \in H$ to $\psi\, {}^{\bar{g}}\psi(x)$ and takes $x \in G - H$ to $\psi(x^2)$.

[(v)] For $n = 2$, there are three such subgroups. But n is the order of a character to $\bar{\mathbb{F}}_p^\times$ (see section 3.1.1 (4)) and hence prime to p; as we will later restrict to $p = 2$, we ignore $n = 2$ here.

The proofs are straightforward but not completely standard, so we include them.

Proof. (1) Indeed, $\rho|_H = \psi \oplus {}^{\bar{g}}\psi$ and we have assumed that $\ker\rho$ is trivial.
(2) The commutator of any two elements of H is in both $\ker\psi$ and $\ker{}^{\bar{g}}\psi$; the claim follows from part (1).
(3) By part (2), G/H acts on H by conjugation, and $\ker{}^{\bar{g}}\psi$ is the image of $\ker\psi$ under the action of the nontrivial element. Now use (1). □

Note that even if ψ is faithful and H is finite cyclic of order n and the sequence

$$1 \to H \to G \to G/H \to 1$$

splits (i.e., there is an order-2 element in $G - H$), we cannot conclude that G is isomorphic to D_n: the dicyclic groups give a counterexample for every even n.

3.1.4. *Translating to Galois representations.* Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ be a finite-image dihedral representation such that $\left|\widetilde{\rho(G_{\mathbb{Q}})}\right| \geq 6$. Let K be the quadratic extension of $\mathbb{Q}$ for which $[\widetilde{\rho(G_{\mathbb{Q}})} : \widetilde{\rho(G_K)}] = 2$, so that $\rho|_{G_K}$ is reducible. Let $\psi : G_K \to F^\times$ be a character appearing in $\rho|_{G_K}$ and let L_ψ be the fixed field of $\ker\psi$. If $L_\psi/\mathbb{Q}$ is Galois, then $L_\psi = \ker\rho$. Otherwise, writing $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$, we obtain the twist ${}^{\sigma}\psi$; its fixed field $L_{{}^{\sigma}\psi}$ is the image $\tilde{\sigma}(L_\psi) \subset \bar{\mathbb{Q}}$ for any lift $\tilde{\sigma}$ of σ to $G_{\mathbb{Q}}$; and $\ker\rho =: M$ is the compositum $L_\psi L_{{}^{\sigma}\psi}$ (inside $\bar{\mathbb{Q}}$). In particular, it is clear that M is an abelian extension of K.

3.1.5. *Artin conductor formulas.* We will also make use of the following formula (see, for example, [35, Corollary 1]) for the Artin conductor of $\mathrm{Ind}_K^{\mathbb{Q}}\psi$ in terms of the Artin conductor of ψ :

$$\mathrm{cond}(\mathrm{Ind}_K^{\mathbb{Q}}\psi) = |\Delta_K|\ \mathcal{N}_{\mathbb{Q}}^K\big(\mathrm{cond}\,\psi\big), \tag{1}$$

where $\mathcal{N}_{\mathbb{Q}}^K$ is the field norm and Δ_K is the discriminant of K.

If F is a finite extension of $\mathbb{F}_p$ or a p-adic field, we will denote the *tame* or prime-to-p Artin conductor by $\mathrm{cond}^{(p)}$. The analogous formula holds:

$$\mathrm{cond}^{(p)}(\mathrm{Ind}_K^{\mathbb{Q}}\psi) = \left|\Delta_K^{(p)}\right|\ \mathcal{N}_{\mathbb{Q}}^K\big(\mathrm{cond}^{(p)}\chi\big). \tag{2}$$

Here $\Delta_K^{(p)}$ is the prime-to-p part of the discriminant of K.

3.2. **Mod-2 dihedral Galois representations.** From now on, we work with $F = \mathbb{F}$, a finite extension of $\mathbb{F}_2$. Suppose that $\rho = \mathrm{Ind}_K^{\mathbb{Q}}\psi : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ is a K-dihedral representation for some quadratic K over $\mathbb{Q}$ and ray class (i.e., Hecke) character $\psi : G_K \to \mathbb{F}^\times$.

3.2.1. *Implications of* $\det\rho = 1$. Again, let L_ψ be the fixed field of $\ker\psi$.

Lemma 6. *If* $\det\rho = 1$*, then* L_ψ *is Galois over* $\mathbb{Q}$*.*

Proof. If $\det\rho = 1$, then considering $\det\rho$ on the subgroup G_K, we see that ${}^{\sigma}\psi = \psi^{-1}$. Therefore L_ψ is also the fixed field of $\ker{}^{\sigma}\psi$, which means that $L_\psi/\mathbb{Q}$ is Galois and L_ψ is the fixed field of $\ker\rho$. □

11 Jun 2018 17:59:18 PDT
Version 2 - Submitted to Open Book Series

3.2.2. *The conductor of ψ.* Let $\mathfrak{a}$ be the conductor of ψ. Since we work in characteristic 2, we are only interested in odd-order ψ here; we thus ignore consideration of any real places of K and view $\mathfrak{a}$ as an integral ideal of K. We have a standard exact sequence relating the class group $\mathrm{Cl}(K)$ to the ray class group $\mathrm{Cl}(K, \mathfrak{a})$:

$$\mathcal{O}_K^\times \to \left(\mathcal{O}_K/\mathfrak{a}\right)^\times \to \mathrm{Cl}(K, \mathfrak{a}) \to \mathrm{Cl}(K) \to 1 \tag{3}$$

Lemma 7. *If $\mathfrak{a} = \mathfrak{q}^n$ is a power of a prime of $\mathcal{O}_K$ lying over a prime q of $\mathbb{Z}$, then*

$$[\mathrm{Cl}(K, \mathfrak{a}) : \mathrm{Cl}(K)] \text{ divides } \begin{cases} (q-1)q^k \text{ for some } k \geq 0 & \text{if } (q) \text{ splits or ramifies in } K, \\ (q^2-1)q^k \text{ for some } k \geq 0 & \text{if } (q) \text{ is inert in } K. \end{cases}$$

Proof. Immediate from sequence (3) in light of the exact sequence

$$1 \to 1 + \mathfrak{q}^n\mathcal{O}_K \to 1 + \mathfrak{q}\mathcal{O}_K \to (\mathcal{O}_K/\mathfrak{q}^n)^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{q})^\times \to 1, \tag{4}$$

combined with the fact that $1 + \mathfrak{q}\mathcal{O}_K$ is pro-q. □

Corollary 8. (1) *If 2 ramifies or splits in K, then any Hecke character $\psi : G_K \to \mathbb{F}^\times$ of modulus $2^n\mathcal{O}_K$ has trivial conductor and hence factors through $\mathrm{Cl}(K)$.*
(2) *If 2 is inert in K, then any Hecke character $\psi : G_K \to \mathbb{F}^\times$ of modulus $2^n\mathcal{O}_K$ has conductor dividing $2\mathcal{O}_K$ and hence factors through $\mathrm{Cl}\big(K, (2)\big)$.*

Proof. (1) If 2 ramifies in K, then this follows immediately from Lemma 7, since $(q-1)q^n$ is a power of 2. If 2 splits as $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then argue as in Lemma 7, noting that $\left(\mathcal{O}_K/(2\mathcal{O}_K)^n\right)^\times = (\mathcal{O}_K/\mathfrak{p}^n)^\times \times \left(\mathcal{O}_K/\mathfrak{p}'^n\right)^\times$ by the Chinese remainder theorem.
(2) From the proof of Lemma 7 and sequence (4), it's clear that the only odd contribution to $[\mathrm{Cl}\big(K, (2)^n\big) : \mathrm{Cl}(K)]$ comes at $n = 1$. □

3.2.3. *The local behavior of ρ.* Fixing an embedding $\iota : G_{\mathbb{Q}_2} \hookrightarrow G_{\mathbb{Q}}$, we can consider the restriction ρ_2 of ρ to $G_{\mathbb{Q}_2}$. Let $\mathfrak{p}$ be the prime of $\mathcal{O}_K$ above 2 corresponding to ι, and let ψ_2 be the restriction of ψ to $G_{K_\mathfrak{p}}$. Then ρ_2 is reducible if and only if either

(1) 2 splits in K, or
(2) 2 is inert or ramified in K and ${}^\sigma\psi_2 = \psi_2$.
(Note that σ is in the decomposition group at $\mathfrak{p}$ in this case.)

3.3. **Mod-2 dihedral Galois representations of prime conductor.** Retaining the notation $(\mathbb{F}, \rho, K, \psi)$ from the previous subsection, we now additionally suppose that N is an odd prime and ρ has (tame Artin) conductor N. The induced tame conductor formula (2) guarantees that either

$$\Delta_K^{(2)} = (1), \mathcal{N}_\mathbb{Q}^K(\mathrm{cond}^{(2)}\psi) = (N) \quad \text{or} \quad \Delta_K^{(2)} = (N), \mathcal{N}_\mathbb{Q}^K(\mathrm{cond}^{(2)}\psi) = (1).$$

We analyze each scenario in turn.

3.3.1. *First scenario: $\Delta_K^{(2)} = (1)$ and $\mathcal{N}_\mathbb{Q}^K(\mathrm{cond}^{(2)}\,\psi) = (N)$.* Here, $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{\pm 2})$, and N splits in K as $(N) = \mathfrak{q}\mathfrak{q}'$ with $\mathrm{cond}^{(2)}\,\psi = \mathfrak{q}$. Hence ψ is a ray class character of conductor $\mathfrak{q}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of K divisible only by primes above 2.

Lemma 9. *In this scenario, $\det\rho : G_\mathbb{Q} \to \mathbb{F}^\times$ is a nontrivial character.*

Proof. Since $\mathrm{cond}\,\psi$ is not Galois-invariant, L_ψ is not Galois over $\mathbb{Q}$. Lemma 6 then implies the desired conclusion. □

11 Jun 2018 17:59:18 PDT
Version 2 - Submitted to Open Book Series

3.3.2. *Second scenario:* $\Delta_K^{(2)} = (N)$ *and* $\mathcal{N}_{\mathbb{Q}}^K(\mathrm{cond}^{(2)}\,\psi) = (1)$. Here, $K = \mathbb{Q}(\sqrt{\pm N})$ or $\mathbb{Q}(\sqrt{\pm 2N})$ and ψ is a ray class character of conductor dividing $(2\mathcal{O}_K)^n$.

Corollary 10. *In this scenario,* ψ *factors through* $\mathrm{Cl}(K)$ *unless*

- $N \equiv 5 \bmod 8$ *and* $K = \mathbb{Q}(\sqrt{N})$ *or*
- $N \equiv 3 \bmod 8$ *and* $K = \mathbb{Q}(\sqrt{-N})$,

in which cases ψ *factors through* $\mathrm{Cl}\big(K, (2)\big)$.

Proof. Combine Corollary 8 with the ramification of 2 in $\mathbb{Q}(\sqrt{\pm N})$: see Table 1. □

TABLE 1. Class number parity and splitting of 2 in $\mathbb{Q}(\sqrt{\pm N})$ for N prime.

$N \bmod 8$	$K = \mathbb{Q}(\sqrt{N})$			$K = \mathbb{Q}(\sqrt{-N})$		
	(2) in K	$h(K)$	$\#\langle\mathfrak{p}(K)\rangle$	(2) in K	$h(K)$	$\#\langle\mathfrak{p}(K)\rangle$
1	splits	odd	varies	ramifies	even > 4	2
3	ramifies	odd	1	inert	odd	1
5	inert	odd	1	ramifies	2·odd	2
7	ramifies	odd	1	splits	odd	varies

3.4. **Mod-2 modular Galois representations of weight 2.** We now suppose that N is an odd integer (not necessarily prime) and $f \in S_2(\Gamma_0(N), \bar{\mathbb{Z}}_2)$ is a normalized weight-2 Hecke eigenform of level N. By a theorem of Breuil–Conrad–Diamond–Taylor [4], such f with coefficients in $\mathbb{Q}$ correspond precisely to isogeny classes of elliptic curves E of conductor N, with the ℓ^{th} Fourier coefficient satisfying $a_\ell(f) = \ell + 1 - \#E(\mathbb{F}_\ell)$ for all primes $\ell \nmid 2N$. As for elliptic curves, the form f is *ordinary* or *supersingular* according to whether $a_2(f)$ is a unit in $\bar{\mathbb{Z}}_2$. Reducing any $G_{\mathbb{Q}}$-stable lattice of the Galois representation associated by Eichler and Shimura to f, we obtain a mod-2 representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{SL}_2(\bar{\mathbb{F}}_2)$ which for prime $\ell \nmid 2N$ is unramified at ℓ and satisfies $\mathrm{Tr}\,\rho_f(\mathrm{Frob}_\ell) = \bar{a}_\ell(f)$, where $\bar{a}_\ell(f) \in \bar{\mathbb{F}}_2$ is the mod-2 reduction of $a_\ell(f)$. If f corresponds to an elliptic curve E (up to isogeny,) then ρ_f is the representation $\rho_{E,2}$ (up to semisimplification) discussed in section 2.

Fixing a prime of $\bar{\mathbb{Q}}$ above 2, we consider the corresponding decomposition group of $G_{\mathbb{Q}}$, which one can identify with the absolute Galois group $G_{\mathbb{Q}_2} = \mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2)$ of the local field $\mathbb{Q}_2$. The following theorem relates the shape of the local representation $\rho_{f,2} := \rho_f|_{G_{\mathbb{Q}_2}}$ to the invertibility of $a_2(f)$. In the statement and the proof, $\mathbb{Q}_{p^2}$ refers to the unique unramified degree-2 extension of $\mathbb{Q}_p$.

Theorem 11 (Deligne, Fontaine, Edixhoven, Serre)**.** *One of the following holds.*

(1) $\rho_{f,2}$ *is reducible, in which case* f *is ordinary, and*

$$\rho_{f,2} \sim \begin{pmatrix} \lambda^{-1} & * \\ 0 & \lambda \end{pmatrix},$$

where $\lambda : G_{\mathbb{Q}_2} \to \overline{\mathbb{F}}_2^\times$ *is the unramified character sending* Frob_2 *to* $\bar{a}_2(f)$. *Moreover* $\rho_{f,2}$ *is at most peu wildly ramified in the sense of Serre.*[vi]

[vi] An extension $M/\mathbb{Q}_p$ is *at most peu wildly ramified* if $M = M^{\mathrm{tr}}(\alpha_1^{1/p}, \ldots, \alpha_d^{1/p})$, where $M^{\mathrm{tr}}/\mathbb{Q}_p$ is the at most tamely ramified subextension of M, and the α_i can be taken to be units in

(2) *$\rho_{f,2}$ is irreducible, in which case f is supersingular. In this case, $\rho_{f,2}$ is the induction of a character of $G_{\mathbb{Q}_4}$ (the second fundamental character) and is therefore at most tamely ramified.*

Proof. Write p in place of 2 to avoid confusion with weight 2. For the shape of $\rho_{f,p}$, see Edixhoven [11, Theorems 2.5, 2.6]. In the ordinary case, since f has level prime to p and weight 2, $\rho_{f,p}$ is *finite at p*: it arises from a finite flat group scheme over $\bar{\mathbb{Z}}_p$ (the p-torsion of a certain abelian variety of GL_2-type), forcing $\rho_{f,p}$ to be at most peu wildly ramified [11, Proposition 8.2]. In the supersingular case, $\rho_{f,2}$ is at most tamely ramified by [32, Proposition 4]; for the description of $\rho_{f,p}$ as the induction of the second fundamental character of $G_{\mathbb{Q}_{p^2}}$, see [30, §2.2]. □

4. Mod-2 dihedral representations appearing in weight 2

Before proving Theorem 2, we state an analogous theorem for cuspforms of weight 2: see Theorem 12 below. As many of the arguments are identical, the two theorems will be proved together in section 5.

For N an odd squarefree positive integer, we study the distribution of generalized T_2-eigenvalues on $S_2(\Gamma_0(N), \bar{\mathbb{F}}_2)^{\mathrm{new}}$. Write $m(N)$ for the dimension of this space. For $\alpha \in \bar{\mathbb{F}}_2$, write $m(N, \alpha)$ for the dimension of the generalized kernel of $T_2 - \alpha$ on this space (i.e., the dimension of the generalized eigenspace corresponding to T_2-eigenvalue α). Let $m_{\mathrm{ord}}(N) := m(N) - m(N, 0)$, the dimension of the *ordinary* subspace. Our aim will be to give lower bounds on $m_{\mathrm{ord}}(N)$, $m(N, 1)$, and $m(N, 0)$ by enumerating dihedral forms with multiplicities. Note that, for squarefree N, forms defined over $\mathbb{F}_2$ will be either dihedral or reducible (that is, the analog of Proposition 1 holds).

To this end, write $S_2(N) := S_2(\Gamma_0(N), \bar{\mathbb{F}}_2)^{\mathrm{new}}$ and let $\mathbb{T}_2(N) := \mathbb{T}_2(N, \bar{\mathbb{F}}_2)^{\mathrm{new}}$ be the shallow Hecke algebra acting on $S_2(N)$. In other words, $\mathbb{T}_2(N)$ is the (commutative) $\bar{\mathbb{F}}_2$-algebra generated inside $\mathrm{End}_{\bar{\mathbb{F}}_2}\big(S_2(N)\big)$ by the action of all the Hecke operators T_n with n prime to $2N$. Then $\mathbb{T}_2(N)$ is a semilocal artinian ring whose maximal ideals $\mathfrak{m}$ correspond to mod-2 Hecke eigensystems appearing in $S_2(N)$. For ℓ prime to $2N$, let $a_\ell(\mathfrak{m}) \in \bar{\mathbb{F}}_2$ be the T_ℓ-eigenvalue corresponding to $\mathfrak{m}$; note that $\mathfrak{m}$ is generated by the $T_\ell - a_\ell(\mathfrak{m})$ for $\ell \nmid 2N$. By Serre reciprocity (a/k/a Serre's conjecture [30], now known by work of Khare–Wintenberger [18, 19], Kisin [22], and Dieulefait [10]), the maximal ideals $\mathfrak{m}$ also correspond to semisimple Galois representations $\rho_{\mathfrak{m}} : G_{\mathbb{Q},2N} \to \mathrm{SL}_2(\bar{\mathbb{F}}_2)$ that are at most peu wildly ramified at 2. The correspondence is codified by the Eichler-Shimura relation $a_\ell(\mathfrak{m}) = \mathrm{tr}\rho_{\mathfrak{m}}(\mathrm{Frob}_\ell)$. Theorem 11 implies that given $\mathfrak{m}$, one can determine whether $a_2(\mathfrak{m})$ is 0 or 1; otherwise $a_2(\mathfrak{m})$ is only defined up to inverse.[(vii)]

We decompose $\mathbb{T}_2(N)$ as a product of localizations at its maximal ideals, and correspondingly decompose of $S_2(N)$ into generalized $\mathfrak{m}$-eigenspaces $S_2(N)_{\mathfrak{m}}$:

$$\mathbb{T}_2(N) = \prod_{\mathfrak{m}} \mathbb{T}_2(N)_{\mathfrak{m}}, \qquad S_2(N) = \bigoplus_{\mathfrak{m}} S_2(N)_{\mathfrak{m}}.$$

M^{tr}. If M is still an elementary p-extension of M^{tr} but at least one of the α_i must be a nonunit, then M is *très wildly ramified*. See [30, 2.4.ii]. A representation of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ as usual inherits the ramification properties of the fixed field of its kernel.

[(vii)]Note that $a_2(\mathfrak{m})$ is not in general the trace of a Frobenius element at 2 of the $\rho_{\mathfrak{m}}$ corresponding to $\mathfrak{m}$ (indeed, $\rho_{\mathfrak{m}}$ may be ramified at 2). Therefore $a_2(\mathfrak{m})$ is not a priori determined by $\mathfrak{m}$. In fact, $a_2(\mathfrak{m})$ may not even be defined over the field of definition of $\rho_{\mathfrak{m}}$. This happens, for example, in level 257 for the $\mathbb{Q}(\sqrt{257})$-dihedral Galois orbit of forms.

Note that if $\mathfrak{m} \subset \mathbb{T}_2(N)$ is a maximal ideal, then the eigenspace $S_2(N)[\mathfrak{m}]$ is nonzero, so that the dimension of the generalized eigenspace $S_2(N)_{\mathfrak{m}}$ is at least 1.

We say that a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_2(N)$ is *reducible*, *dihedral*, *exceptional*, or *big-image* if $\rho_{\mathfrak{m}}$ has the corresponding property. Similarly, we say that $\mathfrak{m}$ is *supersingular* or *ordinary* if $\rho_{\mathfrak{m}}$ is so at 2.

We determine the fields K for which there exist K-dihedral $\mathfrak{m}$ occurring in $\mathbb{T}_2(N)$ for N prime and how many such $\mathfrak{m}$ there are (Theorem 12 below). In section 6, we study the multiplicity of $S_2(N)_{\mathfrak{m}}$ in each case (Conjecture 13 and Proposition 14).

Theorem 12. *Let N be an odd prime, and $\mathfrak{m} \subset \mathbb{T}_2(N)$ a maximal ideal.*

(1) *If $\mathfrak{m}$ is dihedral, then it is either $\mathbb{Q}(\sqrt{N})$-dihedral or $\mathbb{Q}(\sqrt{-N})$-dihedral.*

(2) **Ordinary dihedrals:** *For $K = \mathbb{Q}(\sqrt{\pm N})$, there are exactly $\dfrac{h(K)^{\text{odd}} - 1}{2}$ ordinary K-dihedral maximal ideals in $\mathbb{T}_2(N)$. Of these, $\dfrac{h(K)^{\text{odd,2-split}} - 1}{2}$ have $a_2(\mathfrak{m}) = 1$.*

(3) **Supersingular dihedrals.**
   (a) *If $\mathfrak{m}$ is supersingular K-dihedral, then either $N \equiv 3 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-N})$, or $N \equiv 5 \bmod 8$ and $K = \mathbb{Q}(\sqrt{N})$.*
   (b) *Let $N \equiv 3 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-N})$. If $N > 3$, then there are exactly $h(K)$ supersingular maximal ideals of $\mathbb{T}_2(N)$.*
   (c) *Let $N \equiv 5 \bmod 8$ and $K = \mathbb{Q}(\sqrt{N})$. If $u(K) \equiv 1 \bmod 2\mathcal{O}_K$, then there are $h(K)$ supersingular maximal ideals of $\mathbb{T}_2(N)$; otherwise, there are none.*

(4) **Reducibles:** *If $N \equiv 1 \bmod 8$, then there is one reducible maximal ideal of $\mathbb{T}_2(N)$, generated by T_ℓ for every prime $\ell \nmid 2N$; otherwise, there are none.*

Note that $h(\mathbb{Q}(\sqrt{N}))$ is always odd, and $h(\mathbb{Q}(\sqrt{-N}))$ is even only for $N \equiv 1 \bmod 4$. Note also that a prime $\mathfrak{p}$ above 2 of $K = \mathbb{Q}(\sqrt{\pm N})$ has order 1 or 2 in the class group unless $N \equiv \varepsilon \bmod 8$ and $K = \mathbb{Q}(\sqrt{\varepsilon N})$ for $\varepsilon = \pm 1$, so the 2-split condition is vacuous outside those two cases.

5. Proofs of theorems

We prove the various parts of Theorems 2 and 12 in parallel. We then adapt the ideas to recover the theorems of Hadano (Theorem 3) and Kida (Theorem 4).

5.1. **Proof of parts** (1)**.** Suppose that $f \in S_2(N)$ is a K-dihedral modular form for some quadratic extension K of $\mathbb{Q}$ (corresponding to an elliptic curve for Theorem 2 or to a maximal ideal of the Hecke algebra for Theorem 12). Since ρ_f factors through an extension of $\mathbb{Q}$ unramified outside of 2 and N, K must be one of the following:

$$\mathbb{Q}(\sqrt{N}), \mathbb{Q}(\sqrt{-N}), \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2N}), \mathbb{Q}(\sqrt{-2N}).$$

If $K = \mathbb{Q}(\sqrt{\pm 2N})$, then K is très wildly ramified at 2 [30, 2.6, Exemple], so no modular forms of weight 2 (and in particular no elliptic curves) can be K-dihedral (Theorem 11). If $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, or $\mathbb{Q}(\sqrt{2})$, then we are in the first scenario of subsection 3.3, and Lemma 9 guarantees that a K-dihedral representation cannot come from a $\Gamma_0(N)$-modular form. Thus $K = \mathbb{Q}(\sqrt{\pm N})$, as claimed.

5.2. **Proof of parts** (2)**.** Suppose $K = \mathbb{Q}(\sqrt{\pm N})$ and $f \in S_2(N)$ is a K-dihedral ordinary form, with $\rho = \rho_f = \mathrm{Ind}_K^{\mathbb{Q}} \psi$ for some character ψ of G_K ramified only at primes above 2 (section 3.3.2). Write $H = H(K)$ and $\mathfrak{p} = \mathfrak{p}(K)$. Let L be the fixed field of $\ker \psi$. Since $\det \rho = 1$, by Lemma 6 the extension $L/\mathbb{Q}$ is Galois. Choose a prime $\mathcal{P}$ of L above $\mathfrak{p}$, and write ψ_2 for the restriction of ψ to $\mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$.

We first show that ψ is in fact unramified at 2, and hence will factor through H^{odd}, the maximal odd-degree subextension of H. By Corollary 10 and Table 1, ψ is unramified in all cases except possibly when 2 is inert in K. In that case, $\rho_{f,2} = \mathrm{Ind}_{K_{\mathfrak{p}}}^{\mathbb{Q}_2} \psi_2$, so by 3.1.1 (2) we know that $\psi_2 = {}^{\sigma_2}\psi_2$ for σ_2 a generator of $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_2)$. In this case, Theorem 11 (1) tells us that ψ_2 is unramified above 2, as then is ψ. In fact, the determinant condition further forces ${}^{\sigma_2}\psi_2 = \psi_2^{-1}$, which implies $\psi_2 = 1$ because we are in characteristic 2.

Next, from Theorem 11 (1), the condition $a_2(f) = 1$ is equivalent to the condition $\psi_2 = 1$, which exactly means that ψ factors through $H^{\mathrm{odd,2\text{-}split}}$, the maximal odd subextension of H over K in which 2 splits completely.

To complete the proof of Theorem 2 (2), we observe that $[H^{\mathrm{odd,2\text{-}split}} : K] = \frac{h(K)^{\mathrm{odd}}}{\#\langle \mathfrak{p} \rangle}$. If ρ comes from a K-dihedral elliptic curve, then it has image D_3 so that ψ must have order 3. So a K-dihedral elliptic curve of conductor N is only possible if 3 divides $\frac{h(K)^{\mathrm{odd}}}{\#\langle \mathfrak{p} \rangle}$, or equivalently $\frac{h(K)}{\#\langle \mathfrak{p} \rangle}$.

To complete the proof of Theorem 12 (2), we recall that in general, $\mathrm{Ind}_K^{\mathbb{Q}} \psi = \mathrm{Ind}_K^{\mathbb{Q}} \psi'$ if and only if $\psi = \psi'$ or ${}^{\sigma}\psi = \psi'$ for σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$. In our unit-determinant case, ${}^{\sigma}\psi = \psi^{-1}$. Therefore there are $\frac{h(K)^{\mathrm{odd}}-1}{2}$ distinct ordinary K-dihedral ρ, as claimed. The $a_2 = 1$ condition works similarly.

5.3. **Proof of parts** (3)**.** Suppose that $K = \mathbb{Q}(\sqrt{\pm N})$ and $f \in S_2(N)$ is a K-dihedral form with $\rho = \rho_f = \mathrm{Ind}_K^{\mathbb{Q}} \psi$ for some character ψ of G_K ramified only at primes above 2. Maintain the notation H, $\mathfrak{p}$, σ, ρ_2 as above. As in the second paragraph of section 5.2, ψ does not factor through H (or else ρ_2 would be reducible, contradicting Theorem 11). Therefore ψ must be a character of $\mathrm{Cl}(K, \mathfrak{a})$ for some ideal $\mathfrak{a}$ of K divisible only by primes above 2. By Corollary 8, $\mathfrak{a} = (2)$ and either $N \equiv 3 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-N})$, or $N \equiv 5 \bmod 8$ and $K = \mathbb{Q}(\sqrt{N})$.

Now suppose we are in one of these two cases. Since ${}^{\sigma}\psi = \psi^{-1}$, the character ${}^{\sigma}\psi$ will also factor through $H\big(K, (2)\big)$ and not through H. This gives exactly $\frac{h(K,(2))-h(K)}{2}$ representations, and hence maximal ideals of $\mathbb{T}_2(N)$.

The formulations in part (3b) of Theorem 12 and part (3c) of both theorems come from analyzing the sequence (3) from the proof of Lemma 7. For N congruent to 3 modulo 8, we have $K = \mathbb{Q}(\sqrt{-N})$, so that

$$\mathcal{O}_K = \begin{cases} \{\pm 1\} & \text{if } N > 3 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } N = 3 \end{cases}$$

for ω a cube root of unity in $\mathbb{Q}(\sqrt{-3})$. Since (2) is inert in K, we have $\mathcal{O}_K/(2) = \mathbb{F}_4$. Therefore, for $N > 3$ (still congruent to 3 modulo 8), sequence (3) becomes

$$\{\pm 1\} \to \mathbb{F}_4^{\times} \to H(K, (2)) \to H(K) \to 1,$$

so that $h(K, (2)) = 3h(K)$. For $N = 3$, on the other hand, the global units exactly cancel out the mod-(2) units, so that $h(K, (2)) = h(K)$. For N congruent to 5

modulo 8, we still have $\mathcal{O}_K/(2) = \mathbb{F}_4$, but this time $\mathcal{O}_K = \{\pm 1\} \times u^{\mathbb{Z}}$ for some fundamental unit $u = u(K)$, and therefore we similarly have the two cases

$$h(K,(2)) = \begin{cases} 3h(K) & \text{if } u \text{ maps to 1 in } \big(\mathcal{O}_K/(2)\big)^\times \\ h(K) & \text{otherwise.} \end{cases}$$

5.4. **Proof of parts** (4)**.** If $N \not\equiv 1 \bmod 8$, then 2 is not an Eisenstein prime for N (see Mazur [23] or Mazur–Serre [24]), so there are no cuspforms in $S_2(N, \overline{\mathbb{Z}})$ congruent to the Eisenstein series $E_{2,N}$ modulo 2, which carries the unique reducible maximal ideal in squarefree level. In particular, there are no rational newforms whose associated mod-2 Galois representation is reducible.

This completes the proof of Theorem 2 and Theorem 12.

5.5. **Proof of Theorem 4.** By Theorem 12 (2), the condition $3 \nmid h(\mathbb{Q}(\sqrt{\pm N}))$ rules out the existence of an ordinary elliptic curve of conductor N. For a supersingular elliptic curve, with notation as in the proof of Theorem 12 (3), $K = \mathbb{Q}(\sqrt{(-1)^{(N-1)/2}N})$ and ψ is a nontrivial order-3 character of $H(K,(2))$; this is ruled out by assuming that $3 \nmid h(K,(2))$. This completes the proof of Theorem 4.

5.6. **Proof of Theorem 3.** We now change notation to address Theorem 3. Let N be a prime such that $3 \nmid h(K)$ for $K = \mathbb{Q}(\sqrt{\pm N}), \mathbb{Q}(\sqrt{\pm 2N})$, and let E be an elliptic curve of conductor $2N$. Let $f \in S_2(2N)$ be the corresponding modular form and let $\mathfrak{m} \subseteq \mathbb{T}_2(2N)$ be the corresponding maximal ideal. Since E has multiplicative reduction at 2, f is ordinary and the conclusion of Theorem 11 (1) holds. By Proposition 1, $\mathfrak{m}$ is either reducible or ordinary dihedral.

In the reducible case, $\mathfrak{m}$ is an Eisenstein ideal; by the proof of [39, Theorem 6.1], the difference of the cusps of $X_0(2N)$ corresponding to $1, 1/2 \in \mathbb{P}^1(\mathbb{Q})$ must have even order in the Jacobian. By [39, Theorem 1.3] this order is the numerator of $(N^2-1)/8$, forcing $N \equiv 1, 7 \bmod 8$.

In the ordinary dihedral case, by Lemma 9 we must be in the second scenario of subsection 3.3; that is, that is, $\rho_f = \operatorname{Ind}_K^{\mathbb{Q}} \psi$ where K is one of $\mathbb{Q}(\sqrt{\pm N}), \mathbb{Q}(\sqrt{\pm 2N})$ and ψ is an order-3 character of G_K ramified only at primes above 2. As in subsection 5.2, we see that ψ is also unramified at 2 and so factors through $\mathrm{Cl}(K)$; however, this contradicts the hypothesis that $3 \nmid h(K)$.

This completes the proof of Theorem 3.

6. Multiplicities of mod-2 dihedral cuspforms in weight 2

The following conjecture complements Theorem 12. Note that the fact that $\mathfrak{m} \subset \mathbb{T}_2(N)$ is a maximal ideal automatically implies that $\dim S_2(N)_{\mathfrak{m}} \geq 1$.

Conjecture 13. *Let N be an odd prime and $\mathfrak{m}$ a maximal ideal of $\mathbb{T}_2(N)$.*

(1) *Suppose $N \equiv 1 \bmod 8$.*
   (a) *If $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{N})$-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 4$.
   (b) *If $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{-N})$-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq h(-N)^{\mathrm{even}}$.
   (c) *If $\mathfrak{m}$ is reducible, then* $\dim S_2(N)_{\mathfrak{m}} \geq \dfrac{h(-N)^{\mathrm{even}} - 2}{2}$.

(2) *Suppose $N \equiv 5 \bmod 8$.*
   (a) *If $\mathfrak{m}$ is ordinary $\mathbb{Q}(\sqrt{N})$-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 4$.
   (b) *If $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{-N})$-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

(3) *Suppose $N \equiv 3 \bmod 4$ and $K = \mathbb{Q}(\sqrt{\pm N})$.*

(a) *If* $\mathfrak{m}$ *is ordinary* K*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

In the case that $N \equiv 9 \bmod 16$, part (1c) has been proved by Calegari and Emerton [6, Theorem 1.1]: indeed, they establish that $\dim S_2(N)_{\mathfrak{m}} = \frac{h(-N)^{\text{even}}-2}{2}$ for the unique reducible $\mathfrak{m}$ in this case.

Proposition 14. *Part* (3) *of Conjecture 13 is true when* $K = \mathbb{Q}(\sqrt{-N})$.

Proof. If $K = \mathbb{Q}(\sqrt{-N})$, and $N \equiv 3 \bmod 4$ is a prime, and $\varepsilon = \varepsilon_K$, then there are exactly $\frac{h(-N)-1}{2}$ distinct K-dihedral forms in $S_1(N, \varepsilon, \mathbb{C})$ corresponding to inductions of characters $\psi : \mathrm{Gal}(H(K)/K) \to \mathbb{C}^\times$ (see, for example, [31, §8.1.I] for details). Since $h(-N)$ is odd, all of these reduce to distinct representations modulo 2, so that $S_1(N, \varepsilon_K, \bar{\mathbb{F}}_2)^{K\text{-dih}}$ splits as a Hecke module into a direct sum of $\frac{h(-N)-1}{2}$ non-isomorphic one-dimensional lines spanned by ordinary forms. The two maps $S_1(\Gamma_1(N), \mathbb{F}_2) \hookrightarrow S_2(\Gamma_1(N), \mathbb{F}_2)$ given by $f \mapsto f^2$ and $f \mapsto E_{1,\varepsilon} f$ preserve Hecke eigenspaces (the former because we are in characteristic 2; the latter because $E_{1,\varepsilon}$ in characteristic zero lifts the Hasse invariant: see user Electric Penguin's answer to MathOverflow question 228497[(viii)]) and are linearly independent [12, Prop. 4.4]. Since ε is quadratic, we obtain a Hecke equivariant embedding $\left(S_1(N, \varepsilon, \bar{\mathbb{F}}_2)^{K\text{-dih}}\right)^2 \hookrightarrow S_2(N, \bar{\mathbb{F}}_2)$ that doubles the eigenspace. □

7. Comparison with experimental results

To conclude, we compare our results to the empirical assertions about the mod-2 reduction of T_2 acting on $S_2(\Gamma_0(N), \mathbb{Q})$ for N prime from the introduction.

- For $N \equiv 3 \bmod 8$, the eigenvalue 0 always occurs if $N > 3$.
- For $N \equiv 1, 3, 5 \bmod 8$, the eigenvalue 1 always occurs if $N > 163$.
- For $N \equiv 1 \bmod 8$, the eigenvalue 0 occurs with probability 16.8%.
- For $N \equiv 5 \bmod 8$, the eigenvalue 0 occurs with probability 42.2%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 0 occurs with probability 17.3%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 1 occurs with probability 47.9%.

Of these, the first assertion is implied by part (3b) of Theorem 12 and the second assertion is implied by part (2) of Theorem 12. Combining the other parts of Theorem 12 with the Cohen-Lenstra heuristics yields the following statements.

- For $N \equiv 5 \bmod 8$, the eigenvalue 0 occurs for "dihedral reasons" when $u(N) \equiv 1 \bmod 2\mathcal{O}(N)$. The three possible nonzero reductions of $u(N)$ mod $2\mathcal{O}(N)$ being equally likely, this should occur with probability $\frac{1}{3} = 33.3\%$.
- For $N \equiv 7 \bmod 8$, the eigenvalue 1 occurs for "dihedral reasons" when $h(N) > 1$ or $h(-N)^{\text{odd,2-split}} > 1$. Each of these is modeled by the probability that a random finite abelian group, modulo the subgroup generated by a random element, yields a nontrivial quotient; this probability is
$$1 - \prod_{p>2} \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^{j+1}}\right) = 0.2455\ldots.$$
Since the two events are presumed to be independent, at least one should occur with probability 43.1%.

Removing these cases leaves the following occurrence of eigenvalues arising from exceptional or big-image maximal ideals.

(viii) https://mathoverflow.net/questions/228497

- For $N \equiv 1 \bmod 8$, the eigenvalue 0 occurs with probability 16.8%.
- For $N \equiv 5 \bmod 8$, the eigenvalue 0 occurs with probability 13.3%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 0 occurs with probability 17.3%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 1 occurs with probability 8.4%.

It would of course be desirable to explain these probabilities also. This will require combining some analysis of the corresponding representations with Wood's non-abelian analogue of the Cohen-Lenstra heuristics [38], which for a given pair of finite groups G, G' predicts the probability that a quadratic number field K admits a Galois G-extension L for which $L/\mathbb{Q}$ is a Galois G'-extension.

For $N < 200000$ prime, we also checked whether Theorem 12 and Conjecture 13 together give a sharp lower bound on the eigenvalue multiplicities of 0 and 1. For each residue mod 8, the percentage of cases where this fails is shown in Table 2.

TABLE 2. Frequency of unexplained eigenvalue multiplicity in the mod-2 reduction of T_2 on $S_2(\Gamma_0(N), \mathbb{Q})$ for $N < 200000$ prime.

N mod 8	excess multiplicity of 0	excess multiplicity of 1
1	16.4%	43.8%
3	53.0%	45.7%
5	22.5%	45.8%
7	17.3%	39.0%

Note that these percentages include both uncounted (exceptional or big-image) maximal ideals and non-sharpness in Conjecture 13. The preceding calculation suggests that excess multiplicity of 0 for $N \equiv 1, 7 \bmod 8$ arises almost entirely from uncounted maximal ideals, but in other cases Conjecture 13 may need to be refined.

REFERENCES

[1] G. Bard, *Algebraic Cryptanalysis*, Springer, Dordrecht, 2009.

[2] M. Bennett and A. Rechnitzer, Computing elliptic curves over $\mathbb{Q}$: bad reduction at one prime, in *Recent progress and modern challenges in applied mathematics, modeling and computational science*, Fields Inst. Commun., 79, Springer, New York, 2017, 387–415.

[3] B. Birch, Hecke actions on classes of ternary quadratic forms, *Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991*, 191–212.

[4] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.

[5] A. Brumer, The average rank of elliptic curves. I, *Invent. Math.* **109** (1992), 445–472.

[6] F. Calegari and M. Emerton, On the ramification of Hecke algebras at Eisenstein primes, *Invent. Math.* **160** (2005), 97–144.

[7] F. Calegari and M. Emerton, Elliptic curves of odd modular degree, *Israel J. Math.* **169** (2009), 417–444.

[8] H. Cohen and H.W. Lenstra, Jr., Heuristics on class groups, *Number theory (New York, 1982)*, Lecture Notes in Math. 1052, Springer, Berlin, 1984, 26–36.

[9] J.E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge Univ. Press, 1997; `http://homepages.warwick.ac.uk/~masgaj/book/fulltext/index.html`.

[10] L. Dieulefait, Remarks on Serre's modularity conjecture, *Manuscripta Math.* **139** (2012), 71–89.

[11] Bas Edixhoven, The weight in Serre's conjecture on modular forms, *Invent. Math.* **109** (1992), 563–594.

[12] B. Edixhoven, Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one, *J. Inst. Math. Jussieu* **5** (2006), 1–34.

[13] The LMFDB Collaboration, *L-Functions and Modular Forms Database*, `http://www.lmfdb.org` (retrieved February 2018).
[14] T. Hadano, On the conductor of an elliptic curve with a rational point of order 2, *Nagoya Math. J.* **53** (1974), 199–210.
[15] J. Hein, Orthogonal modular forms: an application to a conjecture of Birch, algorithms and computations, PhD thesis, Dartmouth College, 2016.
[16] J. Hein, `git` repository `https://github.com/jefferyphein/ternary-birch` (retrieved February 2018).
[17] R. Hortsch, Counting elliptic curves of bounded Faltings height, *Acta Arith.* **173** (2016), 239–253.
[18] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (I), *Invent. Math.* **178** (2009), 485–504.
[19] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (II), *Invent. Math.* **178** (2009), 505–586.
[20] M. Kida, Ramification in the division fields of an elliptic curve, *Abh. Math. Sem. Univ. Hamburg* **73** (2003), 195–207.
[21] L.J.P. Kilford and G. Wiese, On the failure of the Gorenstein property for Hecke algebras of prime weight, *Exper. Math.* **17** (2008), 37–52.
[22] M. Kisin, Modularity of 2-adic Barsotti-Tate representations, *Invent. Math.* **178** (2009), 587–634.
[23] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHÉS* **47** (1977), 33–186.
[24] B. Mazur and J.-P. Serre, Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg), *Séminaire Bourbaki (1974/1975), Exp. No. 469*, Lecture Notes in Math. 514, Springer, Berlin, 1976, 238–255.
[25] J.-F. Mestre, La méthode des graphes. Exemples et applications, in *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, Nagoya Univ., Nagoya, 1986, 217–242.
[26] A. Ogg, Abelian curves of small conductor, *J. reine angew Math.* **226** (1967), 204–215.
[27] The PARI group, `PARI/GP`, `http://pari.math.u-bordeaux.fr/`, version 2.9.4 (2017).
[28] D. Roberts, Newforms with rational coefficients, *Ramanujan J.* (2018), 28 pages.
[29] The Sage Development Team, `Sage`, `http://www.sagemath.org`, version 8.1 (2017).
[30] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J* **54** (1987), 179–230.
[31] J.-P. Serre, Modular forms of weight one and Galois representations, *Algebraic Number Fields* (A. Fröhlich, ed.), Academic Press (1977), pp.193–268.
[32] J.-P. Serre, Proprietés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
[33] B. Setzer, Elliptic curves of prime conductor, *J. London Math. Soc.* **10** (1975), 367–378.
[34] W.A. Stein and M. Watkins, A database of elliptic curves–first report, *Algorithmic number theory (Sydney, 2002)*, Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 267–275.
[35] Yuichiro Taguchi, Induction formula for the Artin conductors of mod ℓ Galois representations, *Proc. Amer. Math. Soc.* **130** (2002), 2865–2869.
[36] The University of Sydney Computational Algebra Group, `Magma`, `http://magma.maths.usyd.edu.au/magma/`, version 2.23-8 (2018).
[37] J. Voight, Computing classical modular forms as orthogonal modular forms, lecture notes (2017) available at `http://www.cirm-math.fr/ProgWeebly/Renc1608/voight.pdf`.
[38] M.M. Wood, Nonabelian Cohen-Lenstra moments, arxiv:1702.04644v1 (2017).
[39] H. Yoo, On Eisenstein ideals and the cuspidal group of $J_0(N)$, *Israel J. Math.* **214** (2016), 359–377.

Univ. of California, San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093 USA
Email address: `kedlaya@ucsd.edu`
URL: `http://kskedlaya.org/`

Max-Planck-Institut für Mathematik, Vivatsgasse 7, 53111 Bonn GERMANY
Email address: `medvedov@post.harvard.edu`

11 Jun 2018 17:59:18 PDT
Version 2 - Submitted to Open Book Series

Analytic evaluation of Hecke eigenvalues for Siegel modular forms of degree two

Owen Colman[*], Alexandru Ghitza[†] and Nathan C. Ryan[‡]

June 18, 2018

The standard approach to evaluate Hecke eigenvalues of a Siegel modular eigenform F is to determine a large number of Fourier coefficients of F and then compute the Hecke action on those coefficients. We present a new method based on the numerical evaluation of F at explicit points in the upper-half space and of its image under the Hecke operators. The approach is more efficient than the standard method and has the potential for further optimization by identifying good candidates for the points of evaluation, or finding ways of lowering the truncation bound. A limitation of the algorithm is that it returns floating point numbers for the eigenvalues; however, the working precision can be adjusted at will to yield as close an approximation as needed.

1 Introduction

The explicit computation of classical modular forms and their associated L-functions has been very useful to formulate and verify conjectures, to discover new phenomena and to prove theorems. There are a variety of ways to effectively compute the Fourier coefficients of classical modular forms and, therefore, their L-functions. Analogous work for Siegel modular forms of degree two is less well-developed for, perhaps, two main reasons:

1. the methods for computing Siegel modular forms are *ad hoc* and less efficient than those for computing classical modular forms;

2. computing Siegel modular forms does not immediately give you the associated L-functions since the Hecke eigenvalues of Siegel modular forms, unlike in the classical case, are not equal to the Fourier coefficients and because the Euler factors of the L-function involve knowing both the pth and the p^2th eigenvalues.

To give an idea of the difficulty of computing the L-function of a Siegel modular form, we consider an example. Let Υ_{20} be the unique normalized Siegel modular form of degree 2 and weight 20 that is a Hecke eigenform and not a Saito-Kurokawa lift. Skoruppa [14] gave an explicit formula for Υ_{20} in terms of the generators of the ring of Siegel modular forms of degree 2 and the largest calculation of Υ_{20} has been carried out by Kohnen and Kuss [8] (we point out that Kurokawa [10, 11] was the first to compute Υ_{20} but his computations

[*] owencolman@gmail.com
[†] aghitza@alum.mit.edu
[‡] nathan.ryan@bucknell.edu

were not very extensive). The computation that Kohnen and Kuss carried out was enough to find the pth eigenvalue for $p \leq 997$ and the p^2th eigenvalue for $p \leq 79$. They compute Fourier coefficients indexed by quadratic forms with discriminant up to 3000000 and then use them to determine the Hecke eigenvalues. An examination of the formulas on page 387 of [14] shows that to find the eigenvalue $\lambda(n)$ of T_n, for $n = p^2$, requires the Fourier coefficients indexed by quadratic forms of discriminant up to $n^2 = p^4$. This relation makes it infeasible to compute many more Fourier coefficients, and thus Hecke eigenvalues, using this approach. Instead, in this paper, we propose a different approach.

Our method does not compute *any* of the Fourier coefficients of the Siegel modular form being studied. Instead, we take suitable truncations of the Fourier expansions of the *Igusa generators* (whose coefficients are inexpensive to compute) and use these truncations to evaluate our modular form numerically at points in the upper half space. This approach is based on work of Bröker and Lauter [3] in which they use such techniques to evaluate Igusa functions. Using their method we find the eigenvalue $\lambda(p)$ of an eigenform F by doing the following:

- evaluate F at some point Z in the Siegel upper half-space;
- evaluate $F|T_p$ at the same point Z;
- take the ratio $(F|T_p)(Z)/F(Z)$.

The conceptual shift that we are proposing is that, instead of representing the Siegel modular form F as a list of Fourier coefficients, we represent F by its values at points in the Siegel upper half-space. The idea is simple but its importance can be seen by virtue of the results. We remark that in [2] we describe an implementation of the analogous method for classical modular forms and, in some cases, outperform the standard method using modular symbols.

The potential to parallelize our algorithm stems from the fact that we sum over the coset decomposition of the Hecke operators, and the computation of each summand is independent; these computations can therefore be performed in parallel. Such approaches have been used in the past, for instance in determining the Hecke eigenvalues of paramodular forms, see [13, 4]. We thank the referees for pointing this out, and note that the similarity ends at the level of the sum itself: Poor and Yuen specialize the paramodular eigenform to a modular curve, then compute the summands (which are power series in one variable) exactly. We work with the Siegel eigenform itself (as a power series in three variables) and compute good numerical approximations to the summands.

It is important to emphasize that our method takes as input the expression of a Siegel eigenform as a polynomial in the Igusa generators. Our objective is then to efficiently compute approximate values of the Hecke eigenvalues. We do not claim to obtain further information about the Fourier coefficients of the eigenform, nor that this is an efficient way of determining the exact value of the eigenvalues (unless the latter happen to be integers).

The paper is organized as follows. We begin by stating some numerical preliminaries used in our method. Then, we give the relevant background on Siegel modular forms and discuss Bröker and Lauter's work and how to compute $F|T_p$ both in theory and in practice. We conclude by presenting some results of our computations, together with details of the implementation and ideas for further improvement.

Acknowledgments:

We thank John Voight for proposing this project to us. We also thank the anonymous referees for many helpful suggestions.

2 Numerical preliminaries

Before we describe our algorithm to compute Hecke eigenvalues of Siegel modular forms analytically, we begin by stating some results related to bounding the error introduced when we evaluate a given Siegel modular form and its image under the Hecke operators T_p and T_{p^2} at a point in the upper half-plane.

2.1 Error in quotient

We have a quantity defined as

$$z = \frac{x}{y} \quad \text{with } x, y \in \mathbb{C}.$$

The numerator and denominator can be approximated to x_A, resp. y_A; we define $z_A := \frac{x_A}{y_A}$. Given $\varepsilon > 0$, what values of ε_x and ε_y ensure that

$$\text{if } |x - x_A| < \varepsilon_x \text{ and } |y - y_A| < \varepsilon_y \text{ then } |z - z_A| < \varepsilon?$$

Lemma 1. *With the above notation, let $e_x = x - x_A$ and $e_y = y - y_A$. Then*

$$z - z_A = \frac{e_x - e_y z_A}{y_A + e_y}.$$

Proof. Straightforward calculation. □

Proposition 2. *For any $h \in (0, 1)$, if*

$$\varepsilon_x < \frac{h\varepsilon|y_A|}{2} \quad \textit{and} \quad \varepsilon_y < \min\left\{\frac{(1-h)\varepsilon|y_A|}{2|z_A|}, \frac{|y_A|}{2}\right\},$$

then $|z - z_A| < \varepsilon$.

Proof. Under the hypotheses, we have $|y_A + e_y| > |y_A|/2$ so

$$|z - z_A| < \frac{2}{|y_A|}\left(|e_x| + |e_y z_A|\right) < h\varepsilon + (1-h)\varepsilon = \varepsilon.$$

□

The value of the parameter h can be chosen in such a way that the calculations of x_A and of y_A are roughly of the same level of difficulty.

In order to use the results of Proposition 2 in practice, we need a lower bound on $|y_A|$ and an upper bound on $|z_A|$ (which can be obtained from the lower bound on $|y_A|$ and an upper bound on $|x_A|$). How do we bound $|x_A|$? We compute a very coarse estimate $\tilde{x}$ to x, with $\tilde{\varepsilon}_x$ just small enough that $|\tilde{x}| - 2\tilde{\varepsilon}_x > 0$. (We can start with $\tilde{\varepsilon}_x = 0.1$ and keep dividing by 10 until the condition holds.) Later we will make sure that ε_x is smaller than $\tilde{\varepsilon}_x$. Then we know that

$$|\tilde{x} - x| < \tilde{\varepsilon}_x \qquad \text{and} \qquad |x_A - x| < \varepsilon_x \le \tilde{\varepsilon}_x,$$

so

$$\big||x_A| - |\tilde{x}|\big| \le |x_A - \tilde{x}| < 2\tilde{\varepsilon}_x \qquad \Rightarrow \qquad 0 < |\tilde{x}| - 2\tilde{\varepsilon}_x < |x_A| < |\tilde{x}| + 2\tilde{\varepsilon}_x,$$

giving us lower and upper bounds on $|x_A|$. A similar argument works for $|y_A|$.

3 Siegel modular forms

Let the symplectic group of similitudes of genus 2 be defined by

$$\mathrm{GSp}(4) := \{G \in \mathrm{GL}(4) : {}^tGJG = \lambda(G)J, \lambda(G) \in \mathrm{GL}(1)\}$$

$$\text{where } J = \begin{bmatrix} & I_2 \\ -I_2 & \end{bmatrix}.$$

Let $\mathrm{Sp}(4)$ be the subgroup with $\lambda(G) = 1$. The group $\mathrm{GSp}^+(4,\mathbb{R}) := \{G \in \mathrm{GSp}(4,\mathbb{R}) : \lambda(G) > 0\}$ acts on the Siegel upper half space $\mathbb{H}_2 := \{Z \in M_2(\mathbb{C}) : {}^tZ = Z, \mathrm{Im}(Z) > 0\}$ by

$$G\langle Z\rangle := (AZ+B)(CZ+D)^{-1}, \quad \text{where } G = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{GSp}^+(4,\mathbb{R}), Z \in \mathbb{H}_2. \tag{1}$$

Let $S_k^{(2)}$ be the space of holomorphic Siegel cusp forms of weight k, genus 2 with respect to $\Gamma^{(2)} := \mathrm{Sp}(4,\mathbb{Z})$. Then $F \in S_k^{(2)}$ satisfies

$$F(\gamma\langle Z\rangle) = \det(CZ+D)^k F(Z)$$

for all $\gamma = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Gamma^{(2)}$ and $Z \in \mathbb{H}_2$. This also can be written in terms of the slash operator: for $M \in \mathrm{GSp}^+(4,\mathbb{R})$ let $(F|_k M)(Z) = \det(CZ+D)^{-k} F(M\langle Z\rangle)$. Then the functional equation satisfied by a Siegel modular form can be written as:

$$(F|_k M)(Z) = F(z)$$

for all $M \in \mathrm{Sp}(4,\mathbb{Z})$.

Now we describe the Hecke operators acting on $S_k^{(2)}$. For $M \in \mathrm{GSp}^+(4,\mathbb{R}) \cap M_4(\mathbb{Z})$, define the Hecke operator $T(\Gamma^{(2)} M \Gamma^{(2)})$ on $S_k^{(2)}$ as in [1, (1.3.3)]. For a positive integer m, we define the Hecke operator T_m by

$$T_m := \sum_{\lambda(M)=m} T(\Gamma^{(2)} M \Gamma^{(2)}). \tag{2}$$

See Section 5.1 for an explicit decomposition of the double cosets T_p and T_{p^2} into right cosets. Suppose

$$T_m = \sum \Gamma^{(2)} \alpha$$

is a right coset decomposition of the Hecke operator T_m. Then the operator T_m acts on a Siegel modular form F of weight k as

$$(F|_k T_m)(Z) = \sum (F|_k \alpha)(Z).$$

This action can be described in terms of the Fourier coefficients of the Siegel modular form F.

Any Siegel modular form F of degree 2 has a Fourier expansion of the form

$$F(Z) = \sum_N a_N(F) \exp(2\pi i \,\mathrm{Tr}(NZ)) \qquad a_N(F) \in \mathbb{C},$$

where the sum ranges over all positive semi-definite matrices $N = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ with $a, b, c \in \mathbb{Z}$. The quadratic form N is often written $[a, b, c]$ using Gauss's notation. Using

the decompositions of the Hecke operators in Section 5.1 one can derive formulas for the action of T_p and T_{p^2} on a Siegel modular form F. When these formulas are written down as in [14, p. 387] one can see that to compute $\lambda_F(p)$, the Hecke eigenvalue of F with respect to the Hecke operator T_p, one needs Fourier coefficients up to discriminant of order p^2. To compute $\lambda_F(p^2)$, the Hecke eigenvalue of F with respect to the Hecke operator T_{p^2}, one needs Fourier coefficients up to discriminant p^4. With current methods, computing this number of coefficients of a Hecke eigenform that is not a Saito-Kurokawa lift has proven impossible.

A bottleneck to computing such a large number of coefficients is the fact that there is no known way to compute individual coefficients in parallel. The determination of a single Fourier coefficient requires knowledge of many other Fourier coefficients. Our method, described above, has approximately the same number of steps to compute a new Hecke eigenvalue but these steps, in our method, are easily done in parallel.

4 Evaluating Hecke eigenforms

4.1 Bounds on the coefficients of the Igusa generators

Proposition 3. *Let E_4, E_6, χ_{10} and χ_{12} denote the Igusa generators of the ring of even-weight Siegel modular forms of genus 2 with respect to $Sp(4,\mathbb{Z})$.*

We have the following bounds on the Fourier coefficients of these forms:

$$\begin{aligned}
|a_N(E_4)| &< 19\,230\, t^5,\\
|a_N(E_6)| &< 12\,169\, t^9,\\
|a_N(\chi_{10})| &< \frac{1}{236}\, A(\varepsilon,9)\, t^{9+\varepsilon},\\
|a_N(\chi_{12})| &< \frac{1}{311}\, A(\varepsilon,11)\, t^{11+\varepsilon},
\end{aligned}$$

where the last two hold for any $\varepsilon > 0$, $t = \mathrm{Tr}(N)$, and the function $A(\varepsilon, s)$ is defined by

$$A(\varepsilon,s) = \frac{1}{(2\pi)^{1/4}} \exp\left(9\varepsilon^{-1}2^{3/\varepsilon}/\log(2)\right)\, \zeta(1+\varepsilon)\, \max\left\{1, \sqrt{\frac{\Gamma(s+1/2+\varepsilon)}{\Gamma(s-1/2-\varepsilon)}}\right\}.$$

Proof. It follows directly from [3, Corollary 3.6 and Remark 3.7] that

$$\begin{aligned}
|a_N(E_4)| &< 19\,230\left(4ac-b^2\right)^{5/2} \le 19\,230\,\mathrm{Tr}(N)^5,\\
|a_n(E_6)| &< 12\,169\left(4ac-b^2\right)^{9/2} \le 12\,169\,\mathrm{Tr}(N)^9.
\end{aligned}$$

The second two inequalities follow from [3, Theorem 5.10] with $\gamma = \eta = \varepsilon/3$. □

Remark 4. The bounds for χ_{10} and χ_{12} in Proposition 3 allow for further optimization by choosing the parameter ε appropriately.

Considering χ_{10}, the factor $t^{9+\varepsilon}$ is of course dominant as $t \to \infty$, but choosing ε as small as possible is counterproductive for practical computations, as the factor $A(\varepsilon, 9)$ explodes for small ε.

In our computations, we use $\varepsilon = 2$, so the bounds can be summarized as:

$$\begin{aligned}
|a_N(E_4)| &< 19\,230\, t^5,\\
|a_N(E_6)| &< 12\,169\, t^9,\\
|a_N(\chi_{10})| &< 220\,439\, t^{11},\\
|a_N(\chi_{12})| &< 287\,248\, t^{13},
\end{aligned}$$

where $t = \mathrm{Tr}(N)$.

4.2 The truncation error for Siegel modular forms

Let F be a Siegel modular form of degree 2, with Fourier expansion

$$F(Z) = \sum_N a_N(F) \exp\left(2\pi i \,\mathrm{Tr}(NZ)\right).$$

Given a positive integer T, we will truncate the Fourier expansion of F by considering only those indices N whose trace is at most T:

$$F_T(Z) = \sum_{\mathrm{Tr}(N)\le T} a_N(F) \exp\left(2\pi i \,\mathrm{Tr}(NZ)\right).$$

Lemma 5. *For any $t \in \mathbb{N}$, the number of Fourier indices of trace t satisfies*

$$\#\{N \mid \mathrm{Tr}(N) = t\} \le (t+1)(2t+1) = 2t^2 + 3t + 1 \le 6t^2.$$

Proof. We have

$$\#\{N \mid \mathrm{Tr}(N) = t\} = \sum_{a=0}^{t} \left(1 + 2\left\lfloor 2\sqrt{a(t-a)} \right\rfloor\right).$$

There are $t+1$ terms in the sum, and the largest corresponds to $a = t/2$ (or $a = (t-1)/2$ if t is odd). In any case, every term in the sum is at most $1 + 2t$. □

Suppose we have, like in Proposition 3, an upper bound on the Fourier coefficients of F:

$$|a_N(F)| \le C t^d \qquad \text{where } C \in \mathbb{R}_{>0},\ d \in \mathbb{N} \text{ and } t = \mathrm{Tr}(N). \tag{3}$$

We are interested in bounding the gap between the true value $F(Z)$ and its approximation $F_T(Z)$.

Proposition 6. *Suppose F is a Siegel modular form of degree two whose Fourier coefficients satisfy Equation (3), $Z \in \mathbb{H}_2$ and we wish to approximate the value $F(Z)$ with error at most 10^{-h}. It is then sufficient to use the truncation $F_T(Z)$ containing all terms of the Fourier expansion of F with indices of trace at most T, where*

$$T > \frac{d+2}{\alpha(Z)} \qquad \text{and} \qquad 6C\frac{d+3}{\alpha(Z)} \exp(-\alpha(Z)T) T^{d+2} < 10^{-h}.$$

Here

$$\delta(Z) = \sup\left\{\delta' \in \mathbb{R} \mid \mathrm{Im}(Z) - \delta' I \text{ is positive semi-definite}\right\}$$

and $\alpha(Z) = 2\pi\delta(Z)$.

Proof. Using [3, Lemma 6.1], we have

$$\begin{aligned}
|F(Z) - F_T(Z)| &= \left| \sum_{\mathrm{Tr}(N)>T} a_N(F) \exp\left(2\pi i \,\mathrm{Tr}(NZ)\right) \right| \\
&\leq \sum_{\mathrm{Tr}(N)>T} |a_N(F)| \left|\exp\left(2\pi i \,\mathrm{Tr}(NZ)\right)\right| \\
&\leq \sum_{\mathrm{Tr}(N)>T} |a_N(F)| \exp\left(-\alpha(Z)\,\mathrm{Tr}(N)\right) \\
&< \sum_{t=T+1}^{\infty} \sum_{\mathrm{Tr}(N)=t} |a_N(F)| \exp\left(-\alpha(Z)t\right) \\
&\leq \sum_{t=T+1}^{\infty} 6Ct^{d+2} \exp\left(-\alpha(Z)t\right) \\
&\leq 6C \int_T^{\infty} x^{d+2} \exp\left(-\alpha(Z)x\right)\, dx \\
&= 6C \exp(-\alpha(Z)T) \sum_{j=0}^{d+2} \frac{(d+2)!}{j!\alpha(Z)^{d-j+3}} T^j \\
&< \frac{6C(d+3)}{\alpha(Z)} \exp(-\alpha(Z)T) T^{d+2},
\end{aligned}$$

where the last inequality holds if T is in the half-infinite interval on which the integrand is decreasing (i.e. $T > (d+2)/\alpha(Z)$). □

Example 7. We determine T sufficient for computing $E_4(Z)$ within 10^{-20} at the point

$$z = \begin{pmatrix} 5i & i \\ i & 6i \end{pmatrix}.$$

We have

$$\alpha(Z) = 27.5327$$

so we are looking for T such that

$$\exp(-\alpha(Z)T)T^7 < 2.983 \cdot 10^{-25},$$

which is easily seen (numerically) to hold as soon as $T \geq 3$.

We proceed similarly to obtain the values in Table 1.

	T			
error	E_4	E_6	χ_{10}	χ_{12}
10^{-10}	2	2	2	2
10^{-20}	3	3	3	3
10^{-100}	10	10	10	11
10^{-1000}	86	86	87	87

Table 1: Truncation necessary for computing $F(Z)$ within specified error

5 Our method

As described above, our method is rather straightforward. We fix a $Z \in \mathbb{H}^2$ and evaluate $F(Z)$, using methods in Section 4. Consider the double coset $T_p = \sum \Gamma^{(2)} \alpha$ and its action on F:

$$(F|_k T_p)(Z) = \sum (F|_k \alpha)(Z).$$

What is left to do, then, is, for α in the decomposition, to compute $(F|_k \alpha)(Z)$. That is, to be able to write α as $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and to be able to evaluate

$$\det(CZ+D)^{-k} F\left((AZ+B)(CZ+D)^{-1}\right).$$

In Section 5.1 we present the desired decompositions for the Hecke operators T_p and T_{p^2} and we use the methods of Section 4 to evaluate the Siegel modular form at the points $(AZ+B)(CZ+D)^{-1} \in \mathbb{H}^2$.

5.1 Hecke action

Hecke operators are defined in terms of double cosets $\Gamma M \Gamma$ and the action of such an operator is determined by the right cosets that appear in the decomposition of these double cosets. For a prime p we consider the double coset $T_p = \Gamma^{(2)} \operatorname{diag}(1,1,p,p) \Gamma^{(2)}$. An explicit version of a formula, due to Andrianov, for the right cosets that appear in the decomposition of T_p, is given by Cléry and van der Geer:

Proposition 8. *[1, 6] The double coset T_p admits the following left coset decomposition:*

$$\Gamma^{(2)} \begin{pmatrix} p&0&0&0\\0&p&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix} + \sum_{0\le a,b,c\le p-1} \Gamma^{(2)} \begin{pmatrix} 1&0&a&b\\0&1&b&c\\0&0&p&0\\0&0&0&p \end{pmatrix} + \sum_{0\le a\le p-1} \Gamma^{(2)} \begin{pmatrix} 0&-p&0&0\\1&0&a&0\\0&0&0&-1\\0&0&p&0 \end{pmatrix} + \sum_{0\le a,m\le p-1} \Gamma^{(2)} \begin{pmatrix} p&0&0&0\\-m&1&0&a\\0&0&1&m\\0&0&0&p \end{pmatrix}$$

and we have that the degree of T_p is p^3+p^2+p+1.

Thus, in particular, in order to find λ_p, then, p^3+p^2+p+1 independent evaluations of our Siegel modular form F at points in $\mathbb{H}^2$ are required. This is why our method is so amenable to parallelization.

Similarly, for a prime p define the operator T_{p^2} as a sum of double cosets:

$$T_{p^2} = \Gamma^{(2)} \begin{pmatrix} p&0&0&0\\0&p&0&0\\0&0&p&0\\0&0&0&p \end{pmatrix} \Gamma^{(2)} + \Gamma^{(2)} \begin{pmatrix} 1&0&0&0\\0&p&0&0\\0&0&p^2&0\\0&0&0&p \end{pmatrix} \Gamma^{(2)} + \Gamma^{(2)} \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&p^2&0\\0&0&0&p^2 \end{pmatrix} \Gamma^{(2)}$$

Again, based on a result of Andrianov, Cléry and van der Geer give an explicit decomposition of the operator T_{p^2}:

Proposition 9. *[1, 6] The Hecke operator T_{p^2} has degree $p^6+p^5+2p^4+2p^3+p^2+p+1$ and admits a known explicit left coset decomposition.*

One can do better, however; we can reduce the number of summands at which we need to evaluate F to be $\mathcal{O}(p^4)$ instead of $\mathcal{O}(p^6)$ by using some standard facts about the Hecke

algebra for Siegel modular forms of degree 2. The Hecke operator T_{p^2} is itself a linear combination of three double cosets:

$$T_{p^2,0} = \Gamma^{(2)} \operatorname{diag}(p,p;p,p)\Gamma^{(2)},\ T_{p^2,1} = \Gamma^{(2)} \operatorname{diag}(1,p;p^2,p)\Gamma^{(2)},\ \text{ and } T_{p^2,2} = \Gamma^{(2)} \operatorname{diag}(1,1;p^2,p^2)\Gamma^{(2)}. \tag{4}$$

The decomposition in Proposition 9 is itself the (disjoint) sum of the decomposition of three double cosets $T_{p^2,0}$, $T_{p^2,1}$ and $T_{p^2,2}$.

The p-part of the Hecke algebra is generated by the operators T_p, $T_{p^2,0}$ and $T_{p^2,1}$ and, in fact, in [9, 17], it is shown that

$$(T_p)^2 = T_{p^2,0} + (p+1)T_{p^2,1} + (p^2+1)(p+1)T_{p^2,2}. \tag{5}$$

To determine the eigenvalue $\lambda_{p^2}(F)$ for $F \in S_k^{(2)}$ with respect to the Hecke operator T_{p^2}, using Proposition 8, we first find the eigenvalue $\lambda_p(F)$ for the operator T_p. Then, we find the eigenvalues $\lambda_{p^2,0}(F)$ (known to be p^{-2k} by the definitions in Section 3) and the eigenvalue $\lambda_{p^2,1}(F)$ for the operator $T_{p^2,1}$. Then using (5) we can find the eigenvalue $\lambda_{p^2,2}(F)$ for the operator $T_{p^2,2}$. Putting it all together, then, all we need is an explicit decomposition of $T_{p^2,1}$ into left cosets, in order to compute $\lambda_{p^2}(F)$.

Proposition 10 ([1])**.** *The Hecke operator $T_{p^2,1}$ admits the following left coset decomposition:*

$$\sum_{0\le\alpha<p} \Gamma^{(2)} \begin{pmatrix} p^2 & 0 & 0 & 0 \\ -p\alpha & p & 0 & 0 \\ 0 & 0 & 1 & \alpha \\ 0 & 0 & 0 & p \end{pmatrix} \Gamma^{(2)} + \Gamma^{(2)} \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p^2 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \Gamma^{(2)} + \sum_{\substack{0\le a,b,c<p \\ ac-b^2\equiv 0 \pmod p \\ \text{and not all zero}}} \Gamma^{(2)} \begin{pmatrix} p & 0 & a & b \\ 0 & p & b & c \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} \Gamma^{(2)} + \sum_{\substack{0\le\alpha,\beta<p \\ 0\le C<p^2}} \Gamma^{(2)} \begin{pmatrix} p & 0 & 0 & p\beta \\ -\alpha & 1 & \beta & \alpha\beta+C \\ 0 & 0 & p & p\alpha \\ 0 & 0 & 0 & p^2 \end{pmatrix} \Gamma^{(2)} + \sum_{\substack{0\le\beta<p \\ 0\le A<p^2}} \Gamma^{(2)} \begin{pmatrix} 1 & 0 & A & \beta \\ 0 & p & p\beta & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{pmatrix} \Gamma^{(2)}.$$

Thus the degree of $T_{p^2,1}$ is $p^4+p^3+p^2+p$.

Remark 11. In the Introduction, we discussed the difficulty of computing $\lambda_{p^2}(F)$ using the action of T_{p^2} on the coefficients of the eigenform F. One might ask whether we could more efficiently compute $\lambda_{p^2}(F)$ using the action of $T_{p^2,1}$ on F as described in Proposition 10 and (5). It turns out, though, that one still would require coefficients up to discriminant p^4 using $T_{p^2,1}$ and (5).

6 Some computations and implementation details

We describe some sample computations involving the eigenform of smallest weight that is not a lift from lower rank groups, namely the cusp form Υ_{20} mentioned in the introduction:

$$\Upsilon_{20} = -E_4^2\chi_{12} - E_4E_6\chi_{10} + 1785600\chi_{10}^2.$$

As a gauge of the performance of the algorithm, we compared the timings to those required by the implementation [16] of the standard method[1] by Sho Takemori.

[1]The only other publicly-available implementation we are aware of is [5]. We did not compare against it for two reasons: (a) at the moment, the computation of the Hecke image appears to be incorrect for primes that are congruent to 1 mod 4 and (b) it uses Cython for the most expensive part of the computation, namely the multiplication of the q-expansions. Since both our code and S. Takemori's are pure Python, we deemed this to be a more useful comparison of the two algorithms.

We implemented the method described in this paper in SageMath [15]; this implementation is available at [7]. The benchmarks described below were performed using a single core of a Linux machine with an i7-6700 CPU at 3.40GHz and 64GB of RAM, via the following helper functions:

```
def ups20_eigenvalue_numerical(p, prec, y11):
    CRING = _initialise_rings(prec, 2*p)
    Z = matrix(CRING, 2, 2, [y11*i, i, i, (y11+1)*i])
    R.<a, b, c, d> = QQ[]
    f = -a^2*d-a*b*c+1785600*c^2
    return _eigenvalue_T_fixed_trace(f, Z, p, 2*p)

def ups20_eigenvalue_standard(p):
    with degree2_number_of_procs(1):
        a = eisenstein_series_degree2(4, p)
        b = eisenstein_series_degree2(6, p)
        c = x10_with_prec(p)
        d = x12_with_prec(p)
        f = -a^2*d-a*b*c+1785600*c^2
        return f.hecke_eigenvalue(p)
```

p	y_{11}	precision (bits)	numerical (s)	standard (s)
2	2.7	37	0	0
3	4.3	62	0	0
5	6.1	101	0	0
7	7.5	130	1	1
11	9.5	172	3	7
13	10.3	190	6	15
17	10.9	208	16	55
19	11.9	226	25	90
23	12.3	240	54	230
29	13.5	267	140	735
31	13.9	275	186	1185
37	14.5	295	406	2876

Table 2: Benchmarks comparing the numerical and standard algorithms for computing the Hecke eigenvalues of Υ_{20}. The timings are rounded to the nearest second. The working precision was chosen so that the eigenvalue is the closest integer to the computed floating point number.

For the standard algorithm, the most expensive step appears to be the multiplication of the q-expansions of the Igusa generators. In the case of our numerical algorithm, the majority of the time is spent evaluating truncations of the q-expansions of the Igusa generators at various points in the Siegel upper half space. These functions are polynomials in the variables q_1, q_2, q_3 and q_3^{-1}, where

$$Z = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix} \qquad \text{and} \qquad q_j = e^{2\pi i z_j}.$$

To evaluate such functions efficiently at a large number of points, we implemented an iterative version of Horner's method; to illustrate what is involved, here is how the truncation of the Igusa generator χ_{10} at trace up to 3 is evaluated:

$$q_1\Big(q_2\Big(q_3^{-1}-2+q_3+q_2\left(-2q_3^{-2}-16q_3^{-1}+36-16q_3-2q_3^2\right)\Big) + q_1\Big(q_2\left(-2q_3^{-1}-16q_3^{-1}+36-16q_3-2q_3^2\right)\Big)\Big)$$

Many of the partial evaluations are repeated for different summands of the expression for the Hecke operators. We take advantage of this phenomenon by caching the results of evaluations of polynomials in q_3 and q_3^{-1}. All the operations are performed using interval arithmetic (via the `ComplexIntervalField` available in Sage). While this introduces a small overhead, it frees us from having to keep track of precision loss due to arithmetic operations (and evaluations of the complex exponential function). Sage gives the final approximation of the Hecke eigenvalue in the form

```
1.0555282184708004141101491800000000000000?e27 + 0.?e-13*I
```

from which we observe that the answer is most likely the integer

```
105552821847080041411014918
```

which is indeed $\lambda_{29}(\Upsilon_{20})$. The question mark in the floating point number indicates that the last decimal may be incorrect due to rounding errors (but all preceding decimals are guaranteed to be correct).

There are certainly many variants of our choices that deserve further scrutiny and may lead to improved performance. Here are some of the more interesting ones:

- For computing the eigenvalue λ_p, we chose to focus on the initial evaluation point

$$Z=\begin{pmatrix} y_{11}i & i \\ i & (y_{11}+1)i \end{pmatrix},$$

  where the parameter y_{11} is (at the moment) determined by trial and error. The optimal values of y_{11} for Υ_{20} and small p are listed in the second column of Table 2. We note that the dependence of this optimal y_{11} on p appears to be linear in $\log(p)$.

  The choice of Z is significant for another reason: the fact that Z is a "purely imaginary matrix" gives an extra symmetry that allows to reduce the number of overall computations by almost a factor of 2. Note that the timings listed in Table 2 do not incorporate this optimization.

- Our experiments indicate that computing the value of λ_p accurately using the choice of point Z described above requires truncating the q-expansions of the Igusa generators at trace up to $2p$. It would be very interesting to see if this trace bound can be lowered; even a small improvement in the trace can reduce the computation time significantly. We have observed such phenomena in the case of classical modular forms (treated in [2]).

6.1 Summary of further computations

We performed similar numerical experiments with the following forms:

$$\begin{aligned}
\Upsilon_{22} &= 61E_4^3\chi_{10} - 30E_4E_6\chi_{12} + 5E_6^2\chi_{10} - 80870400\chi_{10}\chi_{12} \\
\Upsilon_{24a} &= -67E_4^3\chi_{12} + 78E_4^2E_6\chi_{10} - 274492800E_4\chi_{10}^2 + 25E_6^2\chi_{12} + 71539200\chi_{12}^2 \\
\Upsilon_{24b} &= +70E_4^3\chi_{12} - 69E_4^2E_6\chi_{10} - 214341120E_4\chi_{10}^2 + 53E_6^2\chi_{12} - 137604096\chi_{12}^2 \\
\Upsilon_{26a} &= -22E_4^4\chi_{10} - 3E_4^2E_6\chi_{12} + 31E_4E_6^2\chi_{10} - 96609024E_4\chi_{10}\chi_{12} - 13806720E_6\chi_{10}^2 \\
\Upsilon_{26b} &= 973E_4^4\chi_{10} + 390E_4^2E_6\chi_{12} - 1255E_4E_6^2\chi_{10} + 3927813120E_4\chi_{10}\chi_{12} - 4438886400E_6\chi_{10}^2
\end{aligned}$$

These have in common that they are all "interesting" forms (Skoruppa's terminology and notation), not arising as lifts from lower rank groups. They also all have rational coefficients (and are very likely the only rational "interesting" forms in level one).

As we can see in Table 3, while the standard method slows down rapidly with the increase in the weight, the numerical method seems unaffected by the weight (in this range).

f	numerical (s)	standard (s)	$\lambda_{23}(f)$
Υ_{20}	57	240	$-7159245922546757692913520$
Υ_{22}	59	410	$1288399464282335021926848240$
Υ_{24a}	59	559	$-570470777436335163580113325944 0$
Υ_{24b}	59	563	$-261273822435247506929686143403 2$
Υ_{26a}	59	658	$172396563934606128778531610105208 0$
Υ_{26b}	60	659	$-245569424911800457763798623615752 0$

Table 3: Benchmarks comparing the numerical and standard algorithms for computing the Hecke eigenvalue λ_{23} of the rational "interesting" eigenforms. The timings are rounded to the nearest second.

As we increase the weight further, we encounter "interesting" eigenforms defined over number fields of increasing degree. Our implementation treats these in the same way as the rational eigenforms; the algebraic numbers appearing in the expression of an eigenform as a polynomial in the Igusa generators are first embedded into the `ComplexIntervalField` with the working precision, and the computations are then done exclusively with complex intervals.

We illustrate this with a number of examples from the L-functions and Modular Forms Database (LMFDB [12]): $\Upsilon_{28}, \Upsilon_{30}, \ldots, \Upsilon_{56}$, contributed by Nils-Peter Skoruppa. These are representatives of the unique Galois orbit of "interesting" Siegel modular eigenforms of level one and weights given by the indices. We computed the integer closest to the eigenvalues $\lambda_2, \lambda_3, \ldots, \lambda_{11}$ of these forms and verified the results against Sho Takemori's implementation.[2] The timings for λ_{11} appear in Table 4. We note once again that the change in weight has only a very minimal effect on the timings for the numerical approach. The degree of the number field over which each eigenform is defined varies from 3 for Υ_{28} to 29 for Υ_{56}.

[2] The LMFDB contains only λ_2, λ_3 and λ_5 for the forms $\Upsilon_{28}, \ldots, \Upsilon_{48}$. We are not aware of the other eigenvalues we computed having been published anywhere.

f	numerical (s)	standard (s)	integer closest to $\lambda_{11}(f)$
Υ_{28}	5	42	$-5759681178477373721671849774$
Υ_{30}	5	55	$25584027381199484130020567509 2$
Υ_{32}	5	72	$-628890798375000734680614968155 55$
Υ_{34}	5	99	$43908608457248526492250997024 4600$
Υ_{36}	5	145	$-10852481167835674840887932009964419 65$
Υ_{38}	5	171	$99082752899176432104304580529696472526$
Υ_{40}	6	316	$21639993149436935203941512756710465353890$
Υ_{42}	6	405	$13264330942760158288281314223206125058026 42$
Υ_{44}	6	697	$-21625483413302053328965786688617691090427 9874$
Υ_{46}	6	1156	$30250103567979818612290216822701780234205991 62$
Υ_{48}	6	2147	$36236812596076837013528898632469012510923854433 64$
Υ_{50}	6	3558	$-50111326406849287661448298549933139673192742821477$
Υ_{52}	6	7701	$-33891727074702812676183940887995219801531644658145401$
Υ_{54}	6	12205	$-43243637347378158947714106282591338511537833758853668 74$
Υ_{56}	7	19290	$80732614396781887621126152474073976989563190354429878522 1$

Table 4: Benchmarks comparing the numerical and standard algorithms for computing the Hecke eigenvalue λ_{11} of a representative of the unique Galois orbit of "interesting" eigenforms in each of the listed weights. The timings are rounded to the nearest second.

References

[1] A. N. Andrianov. *Quadratic forms and Hecke operators*, volume 286 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1987.

[2] D. Armendáriz, O. Colman, A. Ghitza, N. C. Ryan, and D. Terán. Analytic evaluation of Hecke eigenvalues for classical modular forms. arXiv:1806.01586 [math.NT], 2018.

[3] R. Bröker and K. Lauter. Evaluating Igusa functions. *Math. Comp.*, 83(290):2977–2999, 2014.

[4] A. Brumer, A. Pacetti, C. Poor, G. Tornaria, J. Voight, and D. S. Yuen. On the paramodularity of typical abelian surfaces. arXiv:1805.10873 [math.NT], 2018.

[5] C. Citro, A. Ghitza, M. Raum, N. Ryan, N.-P. Skoruppa, and G. Tornaria. Implement scalar-valued Siegel modular forms on $\mathrm{Sp}(4,\mathbb{Z})$. https://trac.sagemath.org/ticket/8701, 2010. [Online; last accessed 2 March 2018].

[6] F. Cléry and G. van der Geer. Constructing vector-valued Siegel modular forms from scalar-valued Siegel modular forms. *Pure and Applied Mathematics Quarterly*, 11(1):21–47, 2015.

[7] O. Colman, A. Ghitza, and N. C. Ryan. SageMath code for the analytic calculation of the Hecke eigenvalues of Siegel modular forms of degree two. https://bitbucket.org/aghitza/hecke-analytic-siegel, 2018. [Online; accessed 5 June 2018].

[8] W. Kohnen and M. Kuss. Some numerical computations concerning spinor zeta functions in genus 2 at the central point. *Math. Comp.*, 71(240):1597–1607, 2002.

[9] A. Krieg. Hecke algebras. *Mem. Amer. Math. Soc.*, 87(435):x+158, 1990.

[10] N. Kurokawa. Examples of eigenvalues of Hecke operators on Siegel cusp forms of degree two. *Invent. Math.*, 49(2):149–165, 1978.

[11] N. Kurokawa. Congruences between Siegel modular forms of degree two. *Proc. Japan Acad. Ser. A Math. Sci.*, 55(10):417–422, 1979.

[12] The LMFDB Collaboration. The L-functions and Modular Forms Database. http://www.lmfdb.org, 2018. [Online; accessed 30 May 2018].

[13] C. Poor and D. Yuen. Paramodular cusp forms. *Math. Comp.*, 84(293):1401–1438, 2015.

[14] N.-P. Skoruppa. Computations of Siegel modular forms of genus two. *Math. Comp.*, 58(197):381–398, 1992.

[15] W. A. Stein et al. *Sage Mathematics Software (Version 8.2)*. The Sage Development Team, 2018. http://www.sagemath.org.

[16] S. Takemori. A Sage package for computation of degree 2 Siegel modular forms. https://github.com/stakemori/degree2, 2018. [Online; last accessed 2 March 2018].

[17] G. van der Geer. Siegel modular forms and their applications. In *The 1-2-3 of modular forms*, Universitext, pages 181–245. Springer, Berlin, 2008.

ARITHMETIC STATISTICS OF GALOIS GROUPS

DAVID KOHEL

Abstract. We develop a computational framework for the statistical characterization of Galois characters with finite image, with application to characterizing Galois groups and establishing equivalence of characters of finite images of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1. Introduction

The absolute Galois group $\mathcal{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a fundamental object of study in number theory. The objective of this work is to develop an explicit computational framework for the study of its finite quotients. We may replace $\mathcal{G}$ with the absolute Galois group of any global field, but restrict to that of $\mathbb{Q}$ for simplicity of exposition.

As point of departure, we consider an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n as input. We set $K = \mathbb{Q}[x]/(f(x))$, denote by L its normal closure and by $\mathcal{G}(K)$ the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ equipped with a permutation representation in $\mathcal{S}_n$ determined by the action on the roots of $f(x)$. Let $\mathcal{P}_S(\mathbb{Z})$ be the set of primes, coprime to the finite set S of primes ramified in $\mathbb{Z}[x]/(f(x))$.

The statistical perspective we develop expresses the map from $\mathcal{P}_S(\mathbb{Z})$ to factorization data as an equidistributed map to a finite set $\mathcal{X}(K)$ equipped with a probability function induced from the Haar measure on $\mathcal{G}(K)$. A Frobenius lift at p, defined up to conjugacy, acts on the roots of $f(x)$. The permutation action on the roots of $f(x)$ induces a representation in $\mathrm{O}(n)$, fixing the formal sum of the roots. The orthogonal complement gives the standard representation in $\mathrm{O}(n-1)$, spanned by differences of basis elements. Let $P(x)$ be the characteristic polynomial of Frobenius in the permutation representation and

$$S(x) = P(x)/(x-1) = x^{n-1} - s_1 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1}.$$

the characteristic polynomial in the standard representation. This polynomial is independent of choices of lift of Frobenius and choice of basis. As such, the coordinates $(s_1, \ldots, s_{n-1}) \in \mathbb{Z}^{n-1}$ are invariants of the Frobenius conjugacy class Frob_p in the set $\mathcal{C}\ell(\mathcal{G}(K))$ of conjugacy classes of $\mathcal{G}(K)$. Denote the finite set of such class points by $\mathcal{X}(K)$. We note that the class points are entirely determined by the factorization data of $f(x) \bmod p$, and $\mathcal{X}(K) \subset \mathbb{Z}^{n-1}$ is equipped with the structure of a finite probability space, induced from the cover $\mathcal{C}\ell(\mathcal{G}(K)) \to \mathcal{X}(K)$. The irreducible characters are known to form an orthogonal basis for the class functions on $\mathcal{C}\ell(\mathcal{G}(K))$, and the rational characters are integer-valued class functions on the class space $\mathcal{X}(K)$.

In what follows we develop this approach by describing systems of rational characters on $\mathcal{G}(K)$ algebraically as a basis of polynomials in $\mathbb{Z}[s_1, \ldots, s_{n-1}]$ modulo the defining ideal for $\mathcal{X}(K)$, together with their associated inner product. As a consequence we develop algorithms for the characterization of Galois groups, and more generally, tools for determining equivalence of finite Galois representations.

2. Representations of orthogonal groups

Let G be a compact Lie group. In practice, G will be an orthogonal group

$$G = \mathrm{O}(n-1) \subset \mathrm{O}(n) \text{ or } G = \mathrm{SO}(n-1) \subset \mathrm{O}(n-1),$$

or a finite permutation group, equipped with the standard representation in $\mathrm{O}(n-1)$,

$$G \subseteq \mathcal{S}_n \subset \mathrm{O}(n-1) \text{ or } G \subseteq \mathcal{A}_n \subset \mathrm{SO}(n-1).$$

18 Jun 2018 06:36:13 PDT
Version 7 - Submitted to Open Book Series

The standard representation of $\mathcal{S}_n$ provides the motivation for an algebraic presentation of the character ring of a permutation group. For the character theory of permutation groups, we appeal to known algorithms for its computation.

The symmetric group $\mathcal{S}_n$ acts on a set of n elements, and the linear extension to a basis of $\mathbb{Z}^n \subset \mathbb{R}^n$ gives the *permutation representation* of $\mathcal{S}_n$. Denote a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Since $\mathbf{e}_1 + \cdots + \mathbf{e}_n$ is fixed by $\mathcal{S}_n$, a line is fixed, and we consider the action on the hyperplane spanned by the orthogonal complement. In the basis $\{\mathbf{e}_1 - \mathbf{e}_2, \ldots, \mathbf{e}_{n-1} - \mathbf{e}_n\}$, we obtain the *standard representation* of $\mathcal{S}_n$ in $\mathrm{O}(n-1)$. The choice of basis is noncanonical, but the character theory is independent of any such choice. The orthogonal group $\mathrm{O}(n)$ and its subgroup $\mathrm{O}(n-1)$ have two connected components, with principal component $\mathrm{SO}(n-1) \subset \mathrm{SO}(n)$, such that $\mathcal{A}_n = \mathcal{S}_n \cap \mathrm{SO}(n-1)$.

Representation ring. For a compact Lie group G, we denote the set of conjugacy classes of G by $\mathcal{C}\ell(G)$. We define the representation ring of G,

$$\mathfrak{R}(G) = \bigoplus_{\chi} \mathbb{Z}\chi,$$

as the free abelian group on irreducible characters $\chi : G \to \mathbb{C}$ of finite degree. We identify addition with direct sum, and thereby the abelian submonoid $\bigoplus \mathbb{N}\chi \subseteq \mathfrak{R}(G)$ with characters, and define multiplication on $\mathfrak{R}(G)$ by the linear extension of tensor product on $\bigoplus \mathbb{N}\chi$. We refer to elements of $\mathfrak{R}(G)$ as virtual characters.

As class functions, $\mathfrak{R}(G)$ can be identified with a subring of complex-valued functions on $\mathcal{C}\ell(G)$. Indeed, when G is finite, the number h of conjugacy classes (and of irreducible characters) is finite, and the character table is defined as the evaluation vectors

$$(\chi_i(\mathcal{C}_1), \ldots, \chi_i(\mathcal{C}_h)).$$

in the ring $\mathbb{C}^h = \mathbb{C} \times \cdots \times \mathbb{C}$, for χ_i running over the irreducible characters, forming a generator set for the representation ring. For a subfield $F \subset \mathbb{C}$, we denote by $\mathfrak{R}_F(G)$ the subring of F-valued virtual characters. While $\mathfrak{R}(G) = \mathfrak{R}_{\mathbb{Q}}(G)$ for $G = \mathcal{S}_n$ or $G = \mathrm{O}(n-1)$, for a general finite group that we may consider, the field of definition of an irreducible character may be a proper extension of $\mathbb{Q}$.

Considering the group $\mathrm{O}(n)$ in $\mathrm{GL}_n(\mathbb{R})$, an element g satisfies a characteristic polynomial of the form

$$x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n.$$

The coefficient s_1 is the trace in its representation on $\mathbb{R}^n$, and s_n is its determinant character. We note that s_k is an invariant of the class of g, and we can identify $g \mapsto s_k$ as characters. Specifically, s_k is the character on the k-th exterior power $\bigwedge^k \mathbb{R}^n$. We recall the structure of the character ring for $\mathrm{O}(n)$ (cf. Takeuchi [20]).

Lemma 1. *The virtual character ring $\mathfrak{R}(O(n))$ is generated by s_k, $1 \le k \le n$, and*

$$\mathfrak{R}(\mathrm{O}(n)) \cong \frac{\mathbb{Z}[s_1, \ldots, s_n]}{(s_k s_n - s_{n-k}, s_n^2 - 1)}.$$

The restriction $\mathrm{Res} : \mathfrak{R}(\mathrm{O}(n)) \to \mathfrak{R}(\mathrm{SO}(n))$ *surjects on*

$$\mathfrak{R}(\mathrm{SO}(n)) \cong \frac{\mathbb{Z}[s_1, \ldots, s_n]}{(s_k - s_{n-k}, s_n - 1)}$$

with kernel ideal $(s_n - 1)$.

Remark. If $n = 2m$ or $n = 2m+1$, then $\mathfrak{R}(\mathrm{SO}(n)) = \mathbb{Z}[s_1, \ldots, s_m]$, and $\mathfrak{R}(\mathrm{O}(n))$ is an extension by the quadratic character $\xi = s_n$ such that $\xi|_{\mathrm{SO}(n)} = 1$.

Algebraic parametrization. If H is a subgroup of G, there is an induced map $\mathcal{C}\ell(H) \to \mathcal{C}\ell(G)$ on conjugacy classes and concomitant restriction homomorphism $\mathrm{Res} : \mathfrak{R}(G) \to \mathfrak{R}(H)$ on representation rings. Applied to the standard representation of $\mathcal{S}_n$ in $\mathrm{O}(n-1)$, the restriction homomorphism equips the representation ring of $\mathfrak{R}(\mathcal{S}_n)$ with a surjective restriction map from $\mathfrak{R}(\mathrm{O}(n-1))$, giving an algebraic presentation of $\mathfrak{R}(\mathcal{S}_n)$ by polynomials in $\mathbb{Z}[s_1, \ldots, s_{n-1}]$ modulo the defining ideal $(s_k s_{n-1} - s_{n-k-1}, s_{n-1}^2 - 1)$. Given a permutation group $G \subset \mathcal{S}_n$, the subsequent restriction captures a significant subring of $\mathfrak{R}_{\mathbb{Q}}(G) \subset \mathfrak{R}(G)$.

As a tool to characterize permutation groups in $\mathcal{S}_n$, for subgroups G and H, with $H \subseteq G \subseteq \mathcal{S}_n$, we develop the *branching rules* — explicit forms for the decomposition

$$\mathrm{Res}(\chi_i) = \sum_{j=1}^{n_i} a_{ij} \psi_j.$$

of irreducible characters $\{\chi_1, \ldots, \chi_r\}$ on G in terms of the irreducible characters $\{\psi_1, \ldots, \psi_s\}$ on H. In light of the algebraic parametrization by $\mathbb{Z}[s_1, \ldots, s_{n-1}]$, we deduce the kernel ideals $I_G \subseteq I_H$ for each permutation group in the lattice (poset) of subgroups. A basis of generators provides test functions for membership in a given subgroup. We develop the algorithmic details later.

Using the Brauer-Klimyk formula (see Bump [11, Proposition 22.9]), it is possible to develop recursive formulas for the character theory of orthogonal groups, as done in Shieh [18, 19] for $\mathrm{USp}(2m)$, and using the algebraic presentation, to deduce recursive branching rules for $\mathrm{Res} : \mathfrak{R}(\mathrm{O}(n-1)) \to \mathfrak{R}(G)$. Instead, we content ourselves with the algebraic parametrization from $\mathfrak{R}(\mathrm{O}(n-1))$ and exploit the well-established computational character theory of permutation groups to develop branching rules in the lattice of permutation subgroups of $\mathcal{S}_n$.

3. Representations of permutation groups

Let G be a *permutation group* — a finite group equipped with an embedding in $\mathcal{S}_n$. The *cycle type* of $g \in G$ is the multiset of cardinalities of its orbits under the action of $\mathcal{S}_n$ on $\{1, \ldots, n\}$. A multiset can be denoted by a tuple $(d_1, \ldots, d_t)$ or a formal product $m_1^{e_1} \cdots m_s^{e_s}$, where

$$d_1 \leq d_2 \leq \cdots \leq d_t \text{ or } m_1 < \cdots < m_s \text{ such that } \sum_{i=1}^{t} d_i = \sum_{i=1}^{s} e_i m_i = n.$$

The cycle type is invariant under conjugation in $\mathcal{S}_n$, thus the cycle type is well-defined for the conjugacy class $\mathcal{C} = \mathcal{C}(g) \in \mathcal{C}\ell(G)$, where $\mathcal{C}(g) = \{xgx^{-1} : x \in G\}$.

Lemma 2. *The map $\mathcal{C}\ell(\mathcal{S}_n) \longrightarrow \{(d_1, \ldots, d_t) : \sum_{i=1}^{t} d_i = n\}$ from conjugacy classes of $\mathcal{S}_n$ to cycle types is a bijection.*

Proof. Clearly, giving a cyclic ordering to any partition of $\{1, \ldots, n\}$ into orbits determines an element of $\mathcal{S}_n$, hence the map is surjective. Moreover, by definition the symmetric group is n-transitive, conjugating any cyclically ordered orbit partition to any another of the same cycle type. Consequently the map is injective. □

Remark. For a permutation group $G \subset \mathcal{S}_n$ the induced map $\mathcal{C}\ell(G) \to \mathcal{C}\ell(\mathcal{S}_n)$ in general is neither injective nor surjective. The failure of injectivity means that the cycle type fails to distinguish the conjugacy classes. We will later see this in the failure of $\mathfrak{R}(\mathcal{S}_n)$ to surject on $\mathfrak{R}(G)$. In fact, the irreducible characters are known to form a basis of the class functions on G (cf. Serre [17, Theorem 6]), hence the failure to separate conjugacy classes means that the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_n)$ does not surject on $\mathfrak{R}(G)$.

On the one hand, the cycle type of a conjugacy class characterizes the class. On the other hand, the characteristic polynomial (hence its coefficients) is class invariant of an orthogonal group element, and the permutation and standard representations thus provide other class invariants. We make this association explicit. Given $(d_1, \ldots, d_t)$ be the cycle type of an element $g \in \mathcal{S}_n$. It is easy to see that the characteristic polynomial of the permutation representation of g is

$$P(x) = (x^{d_1} - 1) \cdots (x^{d_t} - 1) = (x^{m_1} - 1)^{e_1} \cdots (x^{m_s} - 1)^{e_s}.$$

The eigenvalue on the trivial space is 1, so the characteristic polynomial in the standard representation is

$$S(x) = \frac{P(x)}{(x-1)} = x^{n-1} - s_1 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1},$$

and $(s_1, \ldots, s_{n-1})$ is the tuple of class invariants associated to the the conjugacy class $\mathcal{C}(g)$ under the standard representation in $\mathrm{O}(n-1)$. This gives the following lemma.

Lemma 3. *The map $\mathcal{Cl}(\mathcal{S}_n) \to \mathbb{Z}^{n-1}$ from conjugacy classes to the $(n-1)$-tuples $(s_1, \ldots, s_{n-1})$ of coefficients of the characteristic polynomial under the standard embedding is injective.*

Proof. By Lemma 2 the map from conjugacy classes to cycle types is a bijection. However, by unique factorization in $\mathbb{Q}[x]$, a polynomial of the form $(x^{d_1}-1)\cdots(x^{d_t}-1)$ is uniquely determined by the cycle type $(d_1, \ldots, d_t)$, hence the map to its coefficients $(s_1, \ldots, s_{n-1})$ is injective. □

Representation rings and character tables. Let G be a permutation group and let $\mathcal{Cl}(G) = \{\mathcal{C}_1, \ldots, \mathcal{C}_h\}$, and $\{\chi_1, \ldots, \chi_h\}$ be its irreducible characters. For a conjugacy class $\mathcal{C}$, define the ideal

$$\mathfrak{m}_{\mathcal{C}} = \{f \in \mathfrak{R}(G) \,:\, f(\mathcal{C}) = 0\}.$$

such that the value $f(\mathcal{C})$ of a virtual character f at $\mathcal{C}$ is a well-defined class in the residue class ring $\mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}}$. The character table of G is typically represented as a matrix whose i-th row is the evaluation vector $(\chi_i(\mathcal{C}_1), \ldots, \chi_i(\mathcal{C}_h))$. With this notation, we interpret as the embedding of the character χ_i in the product ring, under the injection

$$\mathfrak{R}(G) \longrightarrow \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_1} \times \cdots \times \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_h}.$$

Lemma 4. *The image of the homomorphism $\mathfrak{R}(G) \to \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_1} \times \cdots \times \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_h}$ has finite index in its codomain.*

Proof. Clearly $\mathfrak{R}(G)$ is torsion-free, since the image of a virtual character is a subring of $\mathbb{C}$. Thus $\mathfrak{R}(G)$ embeds in $\mathfrak{R}(G) \otimes \mathbb{Q}$, which is an étale algebra, and $\mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_i} \otimes \mathbb{Q}$ its component fields (see Brakenhoff [1] for details). It follows that the index is finite. □

More generally in the direction of the Lemma, Brakenhoff [1] finds that the center of the group ring $\mathbb{Q}[G]$ over $\mathbb{Q}$ and the tensor product of the representation ring $\mathfrak{R}(G) \otimes \mathbb{Q}$ are related by Brauer equivalence. We give two examples below. In view of the restriction map from $\mathfrak{R}(\mathcal{S}_n)$ to $\mathfrak{R}(G)$, and since all characters on $\mathcal{S}_n$ are rational, the image of $\mathfrak{R}(\mathcal{S}_n) = \mathfrak{R}_{\mathbb{Q}}(\mathcal{S}_n)$ lies in the subring $\mathfrak{R}_{\mathbb{Q}}(G) \subset \mathfrak{R}(G)$. In the examples below, we illustrate the role of nontrivial Galois action and of quadratic characters in failure of surjectivity of $\mathfrak{R}(\mathcal{S}_n)$ on $\mathfrak{R}(G)$ and on $\mathfrak{R}_{\mathbb{Q}}(G)$. In the next section we exploit the embedding by interpolating the character table values by the polynomial presentation $\mathbb{Z}[s_1, \ldots, s_{n-1}] \to \mathfrak{R}_{\mathbb{Q}}(G)$.

Orthogonality relations. The role of arithmetic statistics of G comes from the orthogonality relations for the irreducible characters. Let $\{\chi_1, \ldots, \chi_h\}$ be the irreducible characters for G, and $A(G)$ be the character matrix:

$$A(G) = \begin{bmatrix} \chi_1(\mathcal{C}_1) & \cdots & \chi_1(\mathcal{C}_h) \\ \vdots & & \vdots \\ \chi_h(\mathcal{C}_1) & \cdots & \chi_h(\mathcal{C}_h) \end{bmatrix}$$

The orthogonality relations for characters (see Serre [17, Section 2.3]), expressed in terms of group elements, reformulated in terms of conjugacy classes, takes the form

$$\delta_{ij} = \langle \chi_i, \chi_j \rangle_G := \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \sum_{k=1}^{h} \frac{|\mathcal{C}_k|}{|G|} \chi_i(\mathcal{C}_k)\overline{\chi_j(\mathcal{C}_k)}.$$

Set $D(G)$ to be the diagonal matrix with diagonal entries $(p_1, \ldots, p_h)$, where $p_k = |\mathcal{C}_k|/|G|$ is the weight of the conjugacy class $\mathcal{C}_k$. The orthogonality relations are then expressed by the equality

$$I_h = A(G)D(G)A(G)^{\dagger},$$

where † denotes the conjugate transpose. The matrix $D(G)$ can be viewed as the inner product matrix of the Haar measure induced by G on $\mathcal{C}\ell(G)$.

Rational character table. Let χ be a character on G, let m be the exponent of G, and let $\mathcal{C} = \mathcal{C}(g)$ be a conjugacy class. As the trace of a representation of g, the value $\chi(\mathcal{C})$ lies in $\mathbb{Z}[\zeta_m]$, since each of its eigenvalues are in $\boldsymbol{\mu}_m = \langle \zeta_m \rangle$. We thus obtain two actions of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Denote $\sigma : (\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ the isomorphism such that $\zeta_m^{\sigma(k)} = \zeta_m^k$. The first of the actions is on conjugacy classes, by $\mathcal{C}(g) \mapsto \mathcal{C}(g^k)$, and the second on characters by $\chi^{\sigma(k)}(\mathcal{C}(g)) = \chi(\mathcal{C}(g))^{\sigma(k)}$. Considering the action on eigenvalues we see immediately that

$$\chi^{\sigma(k)}(\mathcal{C}(g)) = \chi(\mathcal{C}(g^k)).$$

Restriction from $\mathfrak{R}(\mathcal{S}_n)$. Only characters in the image of $\mathfrak{R}(\mathcal{S}_n)$ can be parametrized by polynomials in $\mathbb{Z}[s_1, \ldots, s_{n-1}]$ from the standard representation. We note by example, that the pre-image of $\mathcal{C}$ in $\mathcal{C}\ell(\mathcal{S}_n)$ under the induced map $\mathcal{C}\ell(G) \to \mathcal{C}\ell(\mathcal{S}_n)$ can split into an even number of conjugacy class separated by a quadratic character not coming from $\mathcal{S}_n$. We observe this phenomenon for $G = D_4$ and $G = Q_8$ in the examples section below.

4. Algorithms for Galois representations

In what follows we describe algorithms for testing equivalence of finite Galois characters. As principal application, we consider input $f(x)$ of degree n, determining a number field $K = \mathbb{Q}[x]/(f(x))$, and describe how to evaluate a sample set of primes S at characters on the permutation group $\mathcal{G}(K)$. The approach is completely general, allowing one to compare the set of characters on the absolute group $\mathcal{G}$ mapping through permutation groups $\mathcal{G}(K_1)$ and $\mathcal{G}(K_2)$ determined by number fields K_1 and K_2.

Factorization types of irreducible polynomials. Consider an irreducible polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree n, set $K = \mathbb{Q}[x]/(f(x))$ and let L be its normal closure with maximal order $\mathcal{O}_L$. For a rational prime p and prime $\mathfrak{P}$ over p in $\mathcal{O}_L$, the Frobenius lift $\mathrm{Frob}_{\mathfrak{P}}$ is the unique element of the decomposition subgroup $D_{\mathfrak{P}} \subset G = \mathcal{G}(K)$, such that

$$\mathrm{Frob}_{\mathfrak{P}}(a) \equiv a^p \bmod \mathfrak{P}$$

for all a in $\mathcal{O}_L$. Denote by Frob_p the conjugacy class of $\mathrm{Frob}_{\mathfrak{P}}$ in $\mathcal{C}\ell(G)$.

For p not dividing $\mathrm{disc}(f(x))$ we define the *factorization type* of $f(x)$ mod p to be the multiset of degrees of the factorization of $f(x)$ in $\mathbb{F}_p[x]$, which we may denote $(d_1, \ldots, d_t)$, where $d_1 \leq \cdots \leq d_t$ and $d_1 + \cdots + d_t = n$. We can now identify the data of the factorization type with the cycle type of the Galois group $G = \mathcal{G}(K)$ equipped with its embedding in $\mathcal{S}_n$.

Lemma 5. *The factorization type of* $f(x)$ mod p *is the cycle type of* $\mathrm{Frob}_p \subset \mathcal{G}(K)$.

Proof. The factorization $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ is determined from $f(x) \equiv f_1(x) \cdots f_t(x) \bmod p$, with $\mathfrak{p}_k = (p, f_k(x))$ a prime of degree $d_k = \deg(f_k)$. The Galois group acts transitively on primes of $\mathcal{O}_L$ over p, and there exist conjugates $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ over $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, from which we see that d_k divides $\deg(\mathfrak{P})$, and each d_k is the cardinality of an orbit of roots modulo p under the action of $\mathrm{Frob}_{\mathfrak{P}}$. □

Character inner products as expectation. The factorization type of a polynomial gives a means of taking random samples of character values $(s_1, \ldots, s_{n-1})$ at a set S of primes mapping to the group G. Other data, for particular characters, may come from weight one modular eigenforms, character sums, or Kronecker symbols. Let S be such a sample set of primes, and ψ, χ two characters which can be evaluated on S. We write $\psi(p)$ and $\chi(p)$ for the value of the character at a sample point. We obtain an approximation for the orthogonal product $\langle \psi, \chi \rangle$ as the expectation of $\psi\overline{\chi}$:

$$\langle \psi, \chi \rangle = \mathrm{E}(\psi\overline{\chi}) \sim \mathrm{E}_S(\psi\overline{\chi}) = \frac{1}{|S|} \sum_{p \in S} \psi(p)\overline{\chi}(p).$$

Assuming the multiplicity of each irreducible character in the support of ψ and χ is one, then $m = \langle \psi, \chi \rangle$ is an integer counting the number of irreducible characters in the support of both ψ and χ. When ψ and χ are irreducible, to determine equality $\psi = \chi$, one needs only sufficient precision to distinguish the one bit $\langle \psi, \chi \rangle = 0$ or $\langle \psi, \chi \rangle = 1$.

The interest in working with irreducible characters, or nearly irreducible characters as captured by the image of restriction from $\mathfrak{R}(\mathcal{S}_n)$, is that the variance of the character products $\psi\overline{\chi}$ is minimized, and the number of primes needed to recognize convergence small, as observed by Shieh [18, 19] in the case of symplectic groups $\mathrm{USp}(2m)$ (see also Fité and Guitart [12]).

One should note that in view of classifying the Galois group, nonvanishing of an element of the kernel ideal of the restriction $\mathfrak{R}(\mathcal{S}_n) \to \mathfrak{R}(G)$ can be used to provably exclude G as a Galois group. This was already observed by Pohst [15], who proposed the use of factorization types as a lower bound for the Galois group, and that for $n \geq 8$ the factorization types, and their probabilities, fail to separate groups. This statement, however, concerns the data of the induced Haar measure on $\mathcal{C}\ell(G)$, and not that of the character table of G. Precisely we have two data structures on $\mathcal{C}\ell(G)$ at our disposal, that of a probability space and of class functions (given by a character table):

- $\mathcal{C}\ell(G)$ with Haar measure $p : \mathcal{C}\ell(G) \to \mathbb{R}$, and
- $\mathbb{C}^h = \mathrm{Hom}(\mathcal{C}\ell(G), \mathbb{C})$ with orthonormal basis $\{\chi_1, \ldots, \chi_h\}$.

Due to failure of surjectivity of the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_n)$, the subset of characters determined from the cycle types are unlikely to separate groups for sufficiently large n. Nevertheless, the joint data of Haar measure and character table, plus the system of restriction maps coming from common embeddings in $\mathcal{S}_n$ gives more information than either the Haar measure or character table alone.

Restriction kernel ideal. To a conjugacy class $\mathcal{C}$ for $\mathcal{S}_n$ we associate an ideal $\mathfrak{m}_{\mathcal{C}}$ in $\mathbb{Z}[s_1, \ldots, s_{n-1}]$ of the form

$$\mathfrak{m}_{\mathcal{C}} = (s_1 - s_1(\mathcal{C}), \ldots, s_{n-1} - s_{n-1}(\mathcal{C})),$$

where $(s_1(\mathcal{C}), \ldots, s_{n-1}(\mathcal{C}))$ are the values of s_i at $\mathcal{C}$. Then the kernel ideal for the restriction of $\mathfrak{R}(\mathcal{S}_n)$ to $\mathfrak{R}(G)$ is the intersection ideal

$$I(G) = \bigcap_{\mathcal{C} \in \pi(\mathcal{C}\ell(G))} \mathfrak{m}_{\mathcal{C}},$$

where $\pi : \mathcal{C}\ell(G) \to \mathcal{C}\ell(\mathcal{S}_n)$.

Example. Consider the restriction from $\mathfrak{R}(O(3))$ to $\mathfrak{R}(\mathcal{S}_4)$. Since

$$\mathfrak{R}(O(3)) = \frac{\mathbb{Z}[s_1, s_2, s_3]}{(s_1 s_3 - s_2, s_3^2 - 1)}$$

and the values of (s_1, s_2, s_3) are in

$$\{(3, 3, 1),\ (-1, -1, 1),\ (0, 0, 1),\ (-1, 1, -1),\ (1, -1, -1)\},$$

we obtain a defining ideal of $\mathcal{S}_4$ given by the additional generators:

$$s_1(s_1 + 1)(s_1 - s_3 - 2),\ s_1(s_1 + 1)(s_1 - 1)(s_1 - 3),\ (s_1 + 1)(s_1 - 1)(s_3 - 1).$$

The map $\mathcal{C}\ell(D_4) \to \mathcal{C}\ell(\mathcal{S}_4)$ fails to surject on $(0, 0, 1)$, hence there are only four maximal ideals in the intersection and the kernel ideal for $\mathfrak{R}(\mathcal{S}_4) \to \mathfrak{R}(D_4)$ is generated by:

$$s_1^2 - s_1 - s_2 - s_3 - 2,\ s_2 - s_1 s_3,\ s_3^2 - 1.$$

The first polynomial is not in the kernel ideal for $\mathfrak{R}(\mathcal{S}_4)$ and its vanishing provides a test for D_4. Geometrically, it means that the tensor square of the representation with trace s_1 decomposes into a direct sum of representations with trace $s_1 + s_2 + s_3 + 2$.

Restriction homomorphism. Let $H \subset G$ be permutation groups, and set $\ell = |\mathcal{C}\ell(H)|$ and $h = |\mathcal{C}\ell(G)|$ their cardinalities of their conjugacy class sets. Suppose that $\{\psi_1, \ldots, \psi_\ell\}$ and $\{\chi_1, \ldots, \chi_h\}$ are the irreducible characters, which are given by embeddings in $\mathbb{C}^\ell$ and $\mathbb{C}^h$, respectively. We thus have isomorphisms

$$\mathfrak{R}(H) = \bigoplus_{i=1}^{\ell} \mathbb{Z}\psi_i \longrightarrow \Lambda(H) \subset \mathbb{C}^\ell, \text{ and } \mathfrak{R}(G) = \bigoplus_{j=1}^{h} \mathbb{Z}\chi_j \longrightarrow \Lambda(G) \subset \mathbb{C}^h,$$

where $\Lambda(H)$ and $\Lambda(G)$ are the lattices in $\mathbb{C}^\ell$ and $\mathbb{C}^h$ spanned by the rows of the character table. The restriction homomorphism $\mathfrak{R}(G) \mapsto \mathfrak{R}(H)$ is induced by the map $\pi : \mathcal{C}\ell(H) \to \mathcal{C}\ell(G)$, by

$$\chi \longmapsto (\chi(\pi(\mathcal{C}_1)), \ldots, \chi(\pi(\mathcal{C}_\ell))) \in \Lambda(H) \subset \mathbb{C}^\ell.$$

The linear transformation $\Lambda(G) \to \Lambda(H)$ gives the restriction homomorphism as an integral $(h \times \ell)$-matrix with respect to the respective bases of irreducible characters. The rows of this matrix can be interpretted as *branching rules*, giving the decomposition of an irreducible character on G as a sum of irreducible characters on H.

Inside each $\Lambda(G)$ we have a sublattice (generally of lower rank) $\Lambda_{\mathbb{Q}}(G) = \Lambda(G) \cap \mathbb{Q}^h$ of rational-valued characters. We recall that for a conjugacy class $\mathcal{C}$ of group elements of order m, the value of $\chi(\mathcal{C})$ is a sum of eigenvalues in $\mathbb{Q}(\zeta_m)$. We thus obtain an action by the Galois group of a cyclotomic field on the irreducible characters. As a consequence, the lattice $\Lambda_{\mathbb{Q}}(G)$ is generated by the sums over Galois orbits of irreducible characters. Since these orbits are disjoint, this basis of rational characters remains orthogonal, but not orthonormal, since $\langle \chi, \chi \rangle$ measures the cardinality of the orbit (assuming χ is a sum of irreducible characters of multiplicity one). On the other hand, the restriction images $\mathrm{Res}^G_H(\Lambda(G)) \subset \Lambda(H)$ and $\mathrm{Res}^G_H(\Lambda_{\mathbb{Q}}(G)) \subset \Lambda_{\mathbb{Q}}(H)$ do not possess natural reduced orthogonal bases. In order to determine a generating set which is small with respect to the orthogonality relations on characters, we need to apply a constrained lattice reduction inside the submonoid of characters:

$$\bigoplus_{j=1}^{\ell} \mathbb{N}\psi_j \subset \bigoplus_{j=1}^{\ell} \mathbb{Z}\psi_j = \mathfrak{R}(H).$$

Rather than a generic LLL algorithm, we need to carry out a structured lattice reduction in the character monoid order to be able to invoke the heuristic arguments for convergence of small characters.

Algebraic parametrization. In order to interpret factorization types of polynomials (or splitting types of primes) as conjugacy classes on which we can apply the class functions $s_1, \ldots, s_{n-1}$, we need to find an explicit algebraic parametrization

$$\frac{\mathbb{Z}[s_1, \ldots, s_{n-1}]}{I(\mathcal{S}_n)} \to \mathfrak{R}(\mathcal{S}_n) \to \mathrm{Res}^{\mathcal{S}_n}_G(\Lambda(\mathcal{S}_n)) \subseteq \Lambda(G)$$

The presentation $\mathbb{Z}[s_1, \ldots, s_{n-1}]/I(\mathcal{S}_n) \to \mathfrak{R}(\mathcal{S}_n)$ comes from the standard representation of $\mathcal{S}_n$, and its composition into $\Lambda(\mathcal{S}_n)$ can be effectively computed. In order to lift characters in $\Lambda(\mathcal{S}_n)$ back to representative polynomials in $(s_1, \ldots, s_{n-1})$, we must invert

$$\frac{\mathbb{Z}[s_1, \ldots, s_{n-1}]}{I(\mathcal{S}_n)} \to \Lambda(\mathcal{S}_n).$$

As noted above, the isomorphism $\mathfrak{R}(\mathcal{S}_n) \to \Lambda(\mathcal{S}_n)$ is obtained by the Chinese remainder theorem. More precisely, over $\mathbb{Q}$, we obtain a product decomposition of the étale algebra $\mathfrak{R}(\mathcal{S}_n) \otimes \mathbb{Q}$:

$$\mathfrak{R}(\mathcal{S}_n) \otimes \mathbb{Q} \longrightarrow \frac{\mathfrak{R}(\mathcal{S}_n)}{\mathfrak{m}_{\mathcal{C}_1}} \otimes \mathbb{Q} \times \cdots \times \frac{\mathfrak{R}(\mathcal{S}_n)}{\mathfrak{m}_{\mathcal{C}_h}} \otimes \mathbb{Q} \cong \mathbb{Q}^h.$$

under which $\mathfrak{R}(\mathcal{S}_n) \cong \Lambda(\mathcal{S}_n) \subseteq \mathbb{Z}^h$. Since the generators $s_1, \ldots, s_{n-1}$ can be evaluated at conjugacy classes, we can evaluate a basis of monomials modulo $I(\mathcal{S}_n)$ and invert a matrix to determine the pre-image of a basis of irreducible characters. The same applies to a basis of characters in $\mathrm{Res}^{\mathcal{S}_n}_G(\Lambda(\mathcal{S}_n))$ modulo the restriction kernel $I(G)$.

Database of restriction-induction. Databases of transitive permutation groups of degree up to 30 are available in GAP [6] and Magma [8, 10], computed by Greg Butler, John McKay, Gordon Royle and Alexander Hulpke (see [3], [4], [16], [5], [14]). The above is intended to motivate an interest in a metastructure of the restriction relations (and adjoint induction relations) between character rings $\mathfrak{R}(G)$, and for the algebraic parametrizations arizing from the restriction homomorphism from orthogonal groups.

5. Explicit computations

We illustrate the approach through arithmetic statistics of character theory by applying the methods to groups of low degree. First we analyze the dihedral and quaternionic groups D_4 and Q_8 of order 8, the smallest groups sharing the same character table. Then we consider an example of a pair of permutation groups of degree 8 and order 16 whose cycle types and induced Haar measure on $\mathcal{S}_8$-conjugacy classes are equal. We show how an auxillary (sub)field suffices to distinguish the characters using joint Frobenius cycle data. In a final example, we treat different permutation representations of $\mathcal{A}_5$, to show how this approach can be used to establish the equivalence of the absolute Galois representations determined by different fields.

Dihedral and quaternionic groups of order 8. The groups D_4 and Q_8, known to share the same character table, can nevertheless be separated by the restriction data coming from a permutation representation. We first recall that the common character table takes the form

$$A(G) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{bmatrix}$$

with weights $(1/8, 1/8, 1/4, 1/4, 1/4)$ on the conjugacy classes. The semisemimple group algebras $\mathbb{Q}[D_4]$ and $\mathbb{Q}[Q_8]$ have Wedderburn decompositions

$$\mathbb{Q}[D_4] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q}), \text{ and } \mathbb{Q}[Q_8] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H},$$

where $\mathbb{H}$ is the quaternion algebra over $\mathbb{Q}$ ramified at 2 and ∞. These decompositions correspond to the four linear characters and sole degree-2 irreducible representation.

Only the former group, D_4, embeds in $\mathcal{S}_4$, which shows that the permutation embedding contains distinguishing information not in the character table. We make explicit the above approach through character theory for the degree-4 permutation representation. Let $\{1, \chi_1, \chi_2, \chi_3, \chi_4\}$ be a basis of characters, with χ_1, χ_2, and $\chi_3 = \chi_1\chi_2$ quadratic linear characters, and χ_4 of degree 2. The standard representation of $\mathcal{S}_4$ in $\mathrm{O}(3)$ provides irreducible characters

$$\{1, s_1, s_2, s_3, s_1^2 - s_1 - s_2 - 1\}$$

where s_3 is the quadratic determinant character, s_1 and $s_2 = s_1 s_3$ are degree-3 representations, and the last one is of degree 2. Computing the inner product matrices for these characters on $\mathcal{S}_4$ and D_4, we obtain

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 2 \end{bmatrix}.$$

For example, this was the output to the nearest integer for the expectation method on a sample size of 16 unramified primes, for the polynomials x^4+x+1 and x^4-2x^2+2 with respective Galois groups $\mathcal{S}_4$ and D_4.

One identifies the polynomial expression $\chi = s_1^2 - s_1 - s_2 - 1$ for the irreducible degree-2 character χ on $\mathcal{S}_4$, which decomposes into a direct sum $1 + s_3$ on D_4, from which we deduce that $s_1^2 - s_1 - s_2 - s_3 - 2$ is in the kernel ideal $I(D_4)$. Similarly, we read from the inner products $\langle s_1, s_1\rangle = \langle s_2, s_2\rangle = 2$ and $\langle s_1, s_2\rangle = 1$ on D_4 that each of s_1 and s_2 decompose into two irreducible

characters, which share a common irreducible summand. The restriction homomorphism from $\mathfrak{R}(\mathcal{S}_4)$ thus captures

$$1, s_1 = \chi_1 + \chi_4, s_2 = \chi_2 + \chi_4, s_3 = \chi_3.$$

The restriction fails to span all characters, because the conjugacy classes are not separated by characters on $\mathcal{S}_4$. Indeed the cycle types of the five conjugacy classes in $\mathcal{C}\ell(D_4)$ are 1^4, $1^2 2^1$, 2^2, 2^2, and 4^1, and hence the two classes of cycle type 2^2 map to the same class in $\mathcal{C}\ell(\mathcal{S}_4)$.

The missing character χ_1 is easily recovered. It arises from the quadratic subfield (here with defining polynomial $x^2 - 2x + 2$), which can be expressed as a Legendre symbol. In terms of the basis of characters $\{1, s_1, s_2, s_3, \chi_1\}$, we now obtain an inner product matrix:

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

which can be reduced to an orthonormal basis for $\mathfrak{R}(D_4)$.

Since both D_4 and Q_8 admit permutation representations of degree 8, we carry out a similar analysis of the permutation representations of degree 8 for D_4 and Q_8, given by

$$D_4 \cong \left\langle \begin{array}{l}(1,8)(2,7)(3,4)(5,6),\\ (1,2)(3,5)(4,6)(7,8),\\ (1,6)(2,4)(3,8)(5,7)\end{array} \right\rangle \text{ and } Q_8 \cong \left\langle \begin{array}{l}(1,2,4,7)(3,6,8,5),\\ (1,3,4,8)(2,5,7,6)\end{array} \right\rangle.$$

The cycle types 1^8, 2^4, 4^2 arise with probabilities $(1/8, 5/8, 1/4)$ in D_4 whereas in Q_8, theses same types have probabilities $(1/8, 1/8, 3/4)$. Both groups embed in $\mathcal{A}_8 \subset \mathrm{SO}(7)$, hence the character rings are parametrized by $\mathfrak{R}(\mathrm{SO}(7)) \cong \mathbb{Z}[s_1, s_2, s_3]$ ($s_7 = 1$ and $s_4 = s_3$, $s_5 = s_2$, $s_6 = s_1$). Since the cycle types are the same, the kernel ideals agree, but the Haar measures differentiate the groups. However, a naive tabulation of the probabilities gives a poor empirical invariant. In fact, computing these probabilities is tantamount to evaluating the expectations of the idempotents e_1, e_2, e_3 under the isomorphism

$$\mathfrak{R}(G) \otimes \mathbb{Q} = \frac{\mathbb{Q}[s_1, s_2, s_3]}{I(G) \otimes \mathbb{Q}} \longrightarrow \frac{\mathfrak{R}(G) \otimes \mathbb{Q}}{\mathfrak{m}_{\mathcal{C}_1} \otimes \mathbb{Q}} \times \frac{\mathfrak{R}(G) \otimes \mathbb{Q}}{\mathfrak{m}_{\mathcal{C}_2} \otimes \mathbb{Q}} \times \frac{\mathfrak{R}(G) \otimes \mathbb{Q}}{\mathfrak{m}_{\mathcal{C}_3} \otimes \mathbb{Q}} \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}.$$

To express this computation in the character ring framework, we scale by the group order to have integer values. As a general strategy for a group $G \subset \mathcal{S}_n$ this amounts to asking whether the scaled idempotents converge to

$$(\langle |G| e_1, 1\rangle, \ldots \langle |G| e_s, 1\rangle) = (|\mathcal{C}_1|, \ldots, |\mathcal{C}_s|),$$

where $\mathcal{C}_i$ are the $\mathcal{S}_n$-conjugacy classes for G.

Let $\{1, \chi_1, \chi_2, \chi_3, \psi\}$ be a basis of irreducible characters for D_4, and $\{1, \chi_1', \chi_2', \chi_3', \psi'\}$ be a basis of irreducible characters for Q_8. The parametrization gives a $\mathbb{Q}$-basis $\{1, s_1, s_2\}$ and an idempotent basis $\{e_1, e_2, e_3\}$ which are characteristic functions for the evaluations on conjugacy classes. A reduced basis for the image of $\mathfrak{R}(\mathcal{S}_8)$ in $\mathfrak{R}(D_4)$ is $\{1, \sigma_1, \sigma_2\}$, described as follows in these respective bases:

D_4	$\{1, s_1, s_2\}$	$\{e_1, e_2, e_3\}$	$\{1, \chi_1, \chi_2, \chi_3, \psi\}$
1	1	$e_1 + e_2 + e_3$	1
σ_1	$-s_1 + s_2/2 - 1/2$	$2e_1 - e_2 + e_3$	$\chi_1 + \psi$
σ_2	$2s_1 - s_2/2 + 1/2$	$4e_1 - 2e_3$	$\chi_1 + \chi_2 + \chi_3$

Similarly, a reduced basis for the image of $\mathfrak{R}(\mathcal{S}_8)$ in $\mathfrak{R}(Q_8)$ is $\{1, \tau_1, \tau_2\}$, expressed in the respective bases as follows:

Q_8	$\{1, s_1, s_2\}$	$\{e_1, e_2, e_3\}$	$\{1, \chi_1', \chi_2', \chi_3', \psi'\}$
1	1	$e_1 + e_2 + e_3$	1
τ_1	$-s_1 + s_2/2 - 3/2$	$2e_1 - 2e_2$	ψ'
τ_2	$3s_1 - s_2 + 3$	$3e_1 + 3e_2 - e_3$	$\chi_1' + \chi_2' + \chi_3'$

Relative to the parametrizations from $\mathfrak{R}(\mathrm{SO}(7))$, the bases (σ_1,σ_2) and (τ_1,τ_2) are related by $(\sigma_1,\sigma_2) = (\tau_1+1, \tau_1+\tau_2-1)$, and inversely $(\tau_1,\tau_2) = (\sigma_1-1, \sigma_1+\sigma_2+2)$. we thus express $(8e_1, 8e_2, 8e_3$ in the respective bases:

	$\{1, s_1, s_2\}$	$\{1, \sigma_1, \sigma_2\}$	$\{1, \tau_1, \tau_2\}$
$8e_1$	s_1+1	$1+\sigma_1+\sigma_2$	$1+2\tau_1+\tau_2$
$8e_2$	$5s_1-2s_2+7$	$5-3\sigma_1+\sigma_2$	$1-2\tau_1+\tau_2$
$8e_3$	$-6s_1+2s_2$	$2+2\sigma_1-2\sigma_2$	$6-2\tau_2$

giving inclusions of submodules $\langle 8e_1, 8e_2, 8e_3\rangle \subset \langle 1, \sigma_2, \sigma_3\rangle = \langle 1, \tau_2, \tau_3\rangle \subset \langle e_1, e_2, e_3\rangle$.

Computing the expectations of the test functions $\{1, \sigma_1, \sigma_2\}$, for D_4 on polynomials with Galois groups $G = D_4$ or Q_8, the Gram matrix $M(G) = (\mathrm{E}(\sigma_i\sigma_j))$ $(\sigma_0 = 1)$ takes the form

$$M(G) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 3 \end{bmatrix} \text{ where } G = D_4 \text{ and otherwise } \begin{bmatrix} 1 & 1 & -1 \\ 1 & 2 & 0 \\ -1 & 0 & 5 \end{bmatrix}.$$

With respect to test functions $\{1, \tau_1, \tau_2\}$ for Q_8, the Gram matrices are

$$M(G) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix} \text{ where } G = Q_8 \text{ and otherwise } \begin{bmatrix} 1 & -1 & 2 \\ -1 & 3 & -3 \\ 2 & -3 & 7 \end{bmatrix}.$$

It should be clear that the full Gram matrix gives a more complete picture of the orthogonality relations of charactes than the triple of inner products $(\langle 8e_1, 1\rangle), (\langle 8e_2, 1\rangle), (\langle 8e_3, 1\rangle)$, which is just one linear combination of the rows in the above Gram matrices.

In the next section, we show that the choice of reduced basis for the target group gives a better set of test functions, converging more rapidly to the asymptotic Gram matrix. With respect to the polynomials x^8+6x^4+1 of Galois group D_4 and $x^8-12x^6+36x^4-36x^2+9$ of Galois group Q_8, we obtain reasonably good convergence (to within a half integer) with the first 80 primes.

Non distinguished representations of degree 8**.** The first example of nonisomorphic permutation representations not distinguished by their cycle types and Haar measure are the degree-8 groups of order 16 denoted `8T10` and `8T11` (see the LMFDB [9] Galois groups database). Specifically we define the representative groups

$$G_0 = \langle (1,2,3,8)(4,5,6,7), (1,5)(3,7)\rangle \text{ and}$$
$$G_1 = \langle (1,3,5,7)(2,4,6,8), (1,4,5,8)(2,3,6,7), (1,5)(3,7)\rangle$$

whose character tables are given by

$$A(G_0) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & i & -i & -i & i \\ 1 & -1 & -1 & 1 & -1 & 1 & -i & i & -i & i \\ 1 & -1 & -1 & 1 & -1 & 1 & i & -i & i & -i \\ 1 & -1 & -1 & 1 & 1 & -1 & -i & i & i & -i \\ 2 & -2 & 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } A(G_1) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 2 & -2 & -2i & 2i & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -2 & 2i & -2i & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

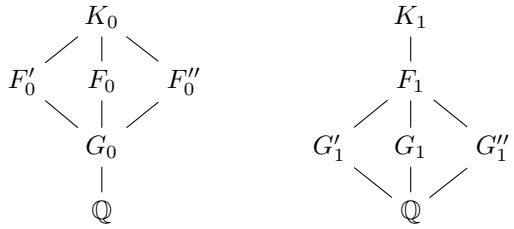
with respective probabilities $(1/16, 1/16, 1/16, 1/16, 1/8, 1/8, 1/8, 1/8, 1/8, 1/8)$. We note that the first 8 characters are linear, and the latter two are of degree 2. The linear characters admit a group structure, isomorphic to $C_2 \times C_4$ and C_2^3, respectively. We denote the characters by $\{1, \chi_1, \chi_2, \chi_3, \rho_1, \bar\rho_1, \rho_2, \bar\rho_2, \psi_1, \psi_2\}$ and $\{1, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7, \psi, \bar\psi\}$. In the groups G_0 and G_1 the character of the standard representation (of degree 7) decomposes as

$$s_1 = \chi_1 + \rho_1 + \bar\rho_1 + \psi_1 + \psi_2 \text{ and } s_1 = \xi_1 + \xi_2 + \xi_2 + \psi + \bar\psi,$$

respectively, but the individual characters in s_1 are not separated.

Given the obvious Galois action (on the codomain field $\mathbb{Q}(i)$), we see that the subrings $\mathfrak{R}_{\mathbb{Q}}(G_0)$ and $\mathfrak{R}_{\mathbb{Q}}(G_1)$ have different ranks, 8 and 9. On the other hand, the images of the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_8)$ have rank 4 in each of $\mathfrak{R}(G_0)$ and $\mathfrak{R}(G_1)$, generated for instance by $\{1, s_1, s_2, s_3\}$. Moreover, since exactly the same four cycle types occur, with the same probabilities $(1/16, 5/16, 1/8, 1/2)$, the characters in the image of restriction from $\mathfrak{R}(\mathcal{S}_8)$ to $\mathfrak{R}(G_0)$ and $\mathfrak{R}(G_1)$ can not be differentiated.

Let K_0 and K_1 be number fields whose normal closures have respective Galois groups G_0 and G_1. In order to distinguish these fields, it suffices to construct missing characters from the linear character groups. In fact these number fields have nontrivial automorphism groups, isomorphic to V_4 and C_4, respectively. This induces respective subfield lattices of the forms



For each field we recover a significant subgroup of the linear character groups from the quartic and quadratic characters. In fact there is a unique cyclic subfield $F_0/\mathbb{Q}$ in K_0 which recovers the characters ρ_1, $\bar{\rho}_2$, and $\chi_1 = \rho_1^2$. (The other fields F_0' and F_0'' are non-normal.) And there exists a unique biquadratic field $F_1/\mathbb{Q}$ in K_1 which yields the quadratic characters ξ_1, ξ_2, ξ_3. The pairs (K_0, F_0) and (K_1, F_1) give characters on the pairs of permutation groups of degree 8 and 4, $(G_0, G_0/H_0 \cong C_4)$ and $(G_1, G_1/H_1 \cong V_4)$, such that the joint factorization types of Frobenius characters separate the Galois structures.

Representations of $\mathcal{A}_5$. We denote the irreducible characters of the alternating groups $\mathcal{A}_5$ by $\{1, \chi_1, \chi_2, \chi_3, \chi_4\}$, where χ_1 is the character of the degree-4 standard representation, χ_2 is the character of a degree-5 representation, and χ_3 and χ_4 are the conjugate characters of degree-3 icosohedral representations over $\mathbb{Q}(\sqrt{5})$. The rational representations are thus spanned by the orthogonal characters $\{1, \chi_1, \chi_2, \chi_3 + \chi_4\}$ of degrees 1, 4, 5, and 6.

On the other hand, the permutation representation of $\mathcal{A}_5$ in $\mathcal{S}_5$ gives a parametrization by

$$\mathfrak{R}(\mathrm{SO}(4)) = \frac{\mathbb{Z}[s_1, s_2, s_3, s_4]}{(s_1 - s_3, s_4 - 1)} \cong \mathbb{Z}[s_1, s_2],$$

and while $|\mathcal{C}\ell(\mathcal{A}_5)| = 5$, there are two conjugacy classes which map to the same cycle type 5^1 in $\mathcal{C}\ell(\mathcal{S}_5)$. Thus the restriction from $\mathfrak{R}(\mathcal{S}_5)$ gives a basis of four independent characters, and we identify:

$$(1, s_1, s_1^2 - s_2 - s_1 - 1, s_2) = (1, \chi_1, \chi_2, \chi_3 + \chi_4).$$

In addition to its degree-5 permutation representation, $\mathcal{A}_5$ admits a faithful permutation representation in $\mathcal{S}_6$. In the restriction of $\mathbb{Z}[s_1, s_2] \cong \mathfrak{R}(\mathrm{SO}(5))$ we recognize the same characters equipped with a different parametrization

$$(1, s_1^2 - 2s_1 - s_2 - 1, s_1, s_2 - \chi_1) = (1, \chi_1, \chi_2, \chi_3 + \chi_4).$$

Consider the number fields, each with Galois group $\mathcal{A}_5$, defined by polynomials

$$f = x^5 - 5x^4 + 48x^3 + 28x^2 + 5x - 1,$$
$$g = x^6 + 4x^5 + 10x^4 - 10x^3 + 17x^2 + 10x + 1$$

constructed as subfields of the same normal closure. Although not isomorphic, we can construct the inner product matrix of the same characters set $\{1, \chi_1, \chi_2, \chi_3 + \chi_4\}$ on $\mathcal{A}_5$ with respect to its different embeddings in $\mathcal{S}_5$ and $\mathcal{S}_6$. Jointly evaluating the characters on factorization types of f or g with those of either f or g, yields the same diagonal inner product matrix ($= \mathrm{diag}(1, 1, 1, 2)$ to nearest integer). This gives a means of recognizing the same character of the absolute Galois group via different presentations. The arithmetic statistic approach through character theory

gives a powerful tool to not only characterize Galois groups, but to recognize equivalence of finite representations of the absolute Galois group $\mathcal{G}$ which may arise in different contexts.

6. Variance, covariance and convergence

The focus on irreducible characters provides, on the one hand, a theoretic framework for understanding the arithmetic statistics of Frobenius distributions. On the computational side, irreducible characters provide test functions with optimal convergence properties. Naively, the orthogonality relations for a system $\{\chi_1, \ldots, \chi_r\}$ of irreducible characters as test functions, it suffices to recognize the integer $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ to one bit of precision. Furthermore, $\chi_i \neq 1$ and $\chi_j \neq 1$ the inner products $\langle \chi_i, 1 \rangle = \langle \chi_j, 1 \rangle = 0$ imply that χ_i and χ_j have mean 0, hence we can interpret

$$\mathrm{E}_S(\chi_i \overline{\chi}_j) = \frac{1}{|S|} \sum_{p \in S} \chi_i(p) \overline{\chi}_j(p)$$

as a (sample) variance ($i = j$) or covariance ($i \neq j$) of the sample S, we see that the use of irreducible characters (or of reduced characters in $\mathfrak{R}(G)$ as the next best approximation when irreducible characters are not in the restriction image from $\mathfrak{R}(\mathcal{S}_n)$) minimizes the variance of the test functions, and orthogonality minimizes the covariance.

We can illustrate the convergence properties with the lattice of subgroups between the representation of $\mathrm{PSL}_2(\mathbb{F}_7)$ on $\mathbb{P}^1(\mathbb{F}_7)$ and $\mathcal{S}_8$:

$$\begin{array}{ccccc} \mathrm{PGL}_2(\mathbb{F}_7) \cong G_1 & & \hookrightarrow & & \mathcal{S}_8 \\ \uparrow & & & & \uparrow \\ \mathrm{PSL}_2(\mathbb{F}_7) \cong H_1 & \hookrightarrow & H_2 & \hookrightarrow & \mathcal{A}_8 \end{array}$$

with respective orders $|H_1| = 168$, $|G_1| = 336$, and $|H_2| = 1344$.

Let $h(G)$ be the number of conjugacy classes of G, equal to the number of irreducible characters and to the rank of $\mathfrak{R}(G)$; let $r(G)$ be the number of characters irreducible over $\mathbb{Q}$, equal to the rank of $\mathfrak{R}_{\mathbb{Q}}(G)$; and let $s(G)$ the rank of the image of the restriction of $\mathfrak{R}(\mathcal{S}_n)$ to $\mathfrak{R}(G)$. For each of the groups we give the respective numbers $h(G)$, $r(G)$ and $s(G)$, as well as a representative polynomial (from the LMFDB [9]) with Galois group G.

G	$h(G)$	$r(G)$	$s(G)$	$f_G(x)$
$\mathcal{S}_8$	22	22	22	$x^8 - x - 1$
$\mathcal{A}_8$	14	12	12	$x^8 - 2x^7 + 3x^5 - 5x^4 + 2x^3 + 2x^2 - x + 1$
G_1	9	8	8	$x^8 - x^7 + x^6 + 4x^5 - x^4 - 3x^3 + 5x^2 - 2x + 1$
H_2	11	10	8	$x^8 - 4x^7 + 8x^6 - 9x^5 + 7x^4 - 4x^3 + 2x^2 + 1$
H_1	6	5	5	$x^8 - 4x^7 + 7x^6 - 7x^5 + 7x^4 - 7x^3 + 7x^2 + 5x + 1$

For the generic group $\mathcal{S}_n$ the characters $(1, s_1, \ldots, s_{n-1})$ are irreducible on $\mathcal{S}_n$ and form a system of test functions for $\mathcal{S}_n$. On $\mathcal{A}_n$ and its subgroups the relations $s_{n-1-i} = s_i$ hold, and so the characters $(1, s_1, \ldots, s_m)$, where $n = 2m + 1$ or $2m + 2$, form a system of test functions for $\mathcal{A}_n$.

The Gram matrices $M(G)$ with respect to the test characters $(1, s_1, \ldots, s_7)$ for $G = \mathcal{S}_8$, $\mathcal{A}_8$, and G_1, respectively are:

$$M(\mathcal{S}_8) = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{bmatrix}, M(\mathcal{A}_8) = \begin{bmatrix} 1&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&1&0 \\ 0&0&1&0&0&1&0&0 \\ 0&0&0&1&1&0&0&0 \\ 0&0&0&1&1&0&0&0 \\ 0&0&1&0&0&1&0&0 \\ 0&1&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&1 \end{bmatrix}, M(G_1) = \begin{bmatrix} 1&0&0&0&1&0&0&0 \\ 0&1&0&1&1&1&0&0 \\ 0&0&3&2&1&1&1&0 \\ 0&1&2&6&4&1&1&1 \\ 1&1&1&4&6&2&1&0 \\ 0&1&1&1&2&3&0&0 \\ 0&0&1&1&1&0&1&0 \\ 0&0&0&1&0&0&0&1 \end{bmatrix}.$$

For the indicated representative polynomials, characters $(\chi_1, \ldots, \chi_r)$ and set of non-ramified primes S, we define the error matrix: $Z_S(G) = \mathrm{E}_S(\chi_i \overline{\chi}_j) - M(G)$ and for an $(r \times r)$-matrix

$Z = (z_{ij})$ and define the normalized ℓ_p-norms

$$||Z||_p = \Big(\frac{1}{r^2}\sum_{i,j}|z_{ij}|^p\Big)^{1/p} \text{ and } ||Z||_\infty = \max_{i,j}\{|z_{ij}|\}.$$

In particular we need $||Z_S(G)||_\infty < 0.50$ in order for the approximation to round to $M(G)$. We say that a sequence stably converges to $M(G)$ after m terms if $||Z_S(G)||_\infty < 0.50$ for all initial segments S of the sequence with $|S| > m$.

Setting S equal to the first $128k$ non-ramified primes, in the case of $\mathcal{S}_8$ and $\mathcal{A}_8$ the symmetric functions give good convergence in the ℓ_2, ℓ_8 and ℓ_∞-norms to $M(G)$ on small sample sets consisting of the first $128k$ non-ramified primes.

	$\mathcal{S}_8$				$\mathcal{A}_8$			
	$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$		$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$
1 :	0.104870	0.184799	0.257812	1 :	0.080624	0.112569	0.140625
2 :	0.104915	0.197659	0.269531	2 :	0.099134	0.174740	0.226562
3 :	0.093747	0.189553	0.255208	3 :	0.074997	0.128586	0.166666
4 :	0.072267	0.138632	0.191406	4 :	0.057739	0.092246	0.119140
5 :	0.063890	0.112834	0.151562	5 :	0.058826	0.128167	0.181250
6 :	0.063620	0.115167	0.171875	6 :	0.053728	0.112338	0.158854
7 :	0.052897	0.083975	0.116071	7 :	0.049278	0.098191	0.138392
8 :	0.045921	0.070367	0.097656	8 :	0.036335	0.065900	0.092773

Even with sample size 128, we obtain a close approximation to the correct Gram matrix, and the convergence remains stable. In contrast, for the group G_1 (of index 120 in $\mathcal{S}_8$) taking increments of size 1024 we find that $2^{14} = 1024 \cdot 16$ primes gives an exact approximation of $M(G_1)$ (in the ℓ_∞-norm) but that at least $1024 \cdot 22$ primes are needed for stable convergence:

	G_1				G_1		
	$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$		$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$
1 :	0.876885	1.841975	2.686523	10 :	0.187304	0.375945	0.533105
2 :	0.229706	0.475835	0.701171	11 :	0.211544	0.429012	0.613725
3 :	0.437539	0.862551	1.233723	12 :	0.231261	0.465137	0.665364
4 :	0.542897	1.080542	1.525878	13 :	0.279154	0.560439	0.800030
5 :	0.267850	0.528893	0.756054	14 :	0.201504	0.399819	0.572195
6 :	0.365931	0.733534	1.035156	15 :	0.189139	0.375454	0.534960
7 :	0.199105	0.407255	0.580217	16 :	0.178182	0.348732	0.493652
8 :	0.229675	0.471416	0.672363	17 :	0.143345	0.282338	0.397633
9 :	0.111158	0.231270	0.333224	18 :	0.136637	0.266879	0.378417

Extending the computation further, we find that the apparent stable convergence fails when $||Z_S(G_1)||_\infty > 0.50$ for $|S| = 1024 \cdot k$ for $19 \le k \le 21$ and again in the range $45 \le k \le 48$.

Passing to a basis of rational irreducible characters ($r(G_1) = s(G_1)$), the rational character table $A(G_1)$ and the inner product matrix $D(G_1)$ of the Haar measure on conjugacy classes are respectively

$$A(G_1) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 6 & -2 & 0 & 0 & 2 & 0 & -1 & 0 \\ 12 & 4 & 0 & 0 & 0 & 0 & -2 & 0 \\ 7 & -1 & 1 & 1 & -1 & 1 & 0 & -1 \\ 7 & -1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 8 & 0 & -2 & -1 & 0 & 1 & 1 & 0 \\ 8 & 0 & 2 & -1 & 0 & -1 & 1 & 0 \end{bmatrix} \text{ and } D(G_1) = \frac{1}{336}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 21 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 28 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 56 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 42 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 56 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 48 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 84 \end{bmatrix},$$

which determine the diagonalized matrix $M(G_1) = A(G_1)D(G_1)A(G_1)^t = \mathrm{diag}(1,1,1,2,1,1,1,1)$ with respect to the rational irreducible characters. With respect to this basis, in increments of

$128k$ primes, we find stable convergence after just $512 = 128 \cdot 4$ primes:

	G_1				G_1		
	$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$		$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$
1 :	0.191903	0.557482	0.937500	9 :	0.114006	0.234514	0.392361
2 :	0.107457	0.204107	0.312500	10 :	0.116967	0.233938	0.390625
3 :	0.111166	0.316320	0.531250	11 :	0.120169	0.241507	0.403409
4 :	0.085609	0.199992	0.335937	12 :	0.090920	0.197313	0.330729
5 :	0.087717	0.208395	0.350000	13 :	0.093108	0.180276	0.300480
6 :	0.094278	0.217121	0.364583	14 :	0.070129	0.145311	0.243303
7 :	0.103194	0.236602	0.397321	15 :	0.074861	0.160193	0.268750
8 :	0.110885	0.249000	0.417968	16 :	0.030534	0.066387	0.111328

For the subgroup chain $H_1 \subset H_2 \subset \mathcal{A}_8$, starting with the characters $(1, s_1, s_2, s_3)$, irreducible on $\mathcal{A}_8$, we find a similar analysis. In particular, the Gram matrices with respect to this basis are

$$M(\mathcal{A}_8) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; M(H_2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \; M(H_1) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 4 & 3 \\ 1 & 2 & 3 & 10 \end{bmatrix}.$$

In the former two cases, the characters are orthogonal and irreducible or nearly so (s_3 decomposes as a sum of three distinct irreducibles on H_2), and convergence is relatively good. In constrast, the Gram matrix $M(H_1)$ has determinant 14, and far from being orthogonal or irreducible (except for 1 and s_1) on H_1. In increments of 1024, we find stable convergence only after $2^{15} = 1024 \cdot 32$ primes:

	H_1				H_1		
	$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$		$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$
1 :	1.300776	2.685076	3.787109	17 :	0.162082	0.331846	0.467773
2 :	0.457035	0.943691	1.331054	18 :	0.249476	0.507743	0.715332
3 :	0.316304	0.671333	0.948242	19 :	0.260497	0.533048	0.751336
4 :	0.149549	0.327977	0.463623	20 :	0.250136	0.514311	0.725195
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
13 :	0.201940	0.417409	0.588792	29 :	0.183952	0.364100	0.511112
14 :	0.219831	0.449876	0.634137	30 :	0.193960	0.384122	0.539257
15 :	0.207462	0.427431	0.602799	31 :	0.148770	0.290129	0.406060
16 :	0.170705	0.352046	0.496520	32 :	0.132390	0.258615	0.362091

Going further one finds that the ℓ_∞-norm gradually decreases and does indeed stay below 0.50 after this point. In contrast, in terms of the basis $(1, \chi_1 = \varphi + \bar{\varphi}, \chi_2, \chi_3, \chi_4)$ of irreducible characters over $\mathbb{Q}$, of degrees $(1, 6, 6, 7, 8)$ given by

$$\chi_1 = (4s_2 + 3s_3 - s_1s_2 - 4s_1 - 2)/2, \quad \chi_3 = s_1,$$
$$\chi_2 = (2s_2 + 5s_3 - s_1s_2 - 6s_1 - 4)/4, \quad \chi_4 = (s_1s_2 + 2s_1 + 2 - 2s_2 - 3s_3)/2,$$

the test characters stable converge to $M(H_1)$ after only 128 primes, with results here in increments of 128 primes:

	H_1				H_1		
	$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$		$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$
1 :	0.227868	0.301886	0.406250	9 :	0.064413	0.088651	0.114583
2 :	0.225747	0.296604	0.398437	10 :	0.079219	0.104501	0.132812
3 :	0.127307	0.165588	0.216145	11 :	0.091419	0.119029	0.154829
4 :	0.149822	0.191605	0.250000	12 :	0.056475	0.076844	0.097656
5 :	0.166819	0.214155	0.271875	13 :	0.047871	0.066901	0.086538
6 :	0.085019	0.114926	0.148437	14 :	0.041653	0.062817	0.083705
7 :	0.101179	0.132950	0.166294	15 :	0.029993	0.041051	0.053125
8 :	0.114860	0.148922	0.193359	16 :	0.041465	0.054989	0.069335

These convergence results give empirical support to the principle of using irreducible characters as test functions, based on the theoretical interpretation of inner product relations on characters as variance and covariance. Moreover, when using irreducible characters, the number of primes necessary to recognize the Gram matrix associated to a Galois group is strikingly small.

7. Asymptotics in the degree

In analyzing the character theory of a permutation group of large degree, one must avoid certain bottlenecks in the complexity. First the number of transitive permutation groups is too large to enumerate, and so clearly the poset must be navigated in a lazy fashion. Second, the number of conjugacy classes (hence of irreducible characters) for $\mathcal{S}_n$ is too large to enumerate. For the generic groups $\mathcal{S}_n$ and $\mathcal{A}_n$, the characters $(1, s_1, \ldots, s_{n-1})$ and $(1, s_1, \ldots, s_m)$, where $n = 2m + 1$ or $2m + 2$, give a subset of rational irreducible test functions (when $n = 2m + 2$, the character s_m is the sum of two characters on $\mathcal{A}_n$, conjugate over a quadratic field). In general the number of conjugacy classes is the partition number $p(n)$, whose asymptotic growth is known by Hardy and Ramanujan [13] to be

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

In particular, we will treat a nontrivial example of degree 120 (and 240) despite the large size $p(120) = 1844349560$ (and $p(240) = 105882246722733$) of the corresponding partition numbers. Finally, computation of the kernel ideal of the restriction $\mathfrak{R}(O(n-1)) \to \mathfrak{R}(G)$ by Groebner basis algorithms is prohibitively expensive, even if the $s(G)$ points in the kernel can be computed.

Polynomials with interesting Galois groups of large degree, outside the generic groups $\mathcal{S}_n$ and $\mathcal{A}_n$ and cyclic and dihedral groups C_n and D_n rely on specific constructions. We consider such an example of Jouve, Kowalski and Zywina [7], a polynomial $f(x)$ of degree 240 with Galois group the Weyl group $W(E_8)$ of the lattice E_8, of order 696729600. In contrast to the large number of conjugacy classes of $\mathcal{S}_{240}$, the number of conjugacy classes of $W(E_8)$ is 112, and the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_{240})$ has full rank. We take the quotient of order 348364800 by its center, which is the Galois group of the degree 120 polynomial $g(x)$ such that $f(x) = g(x^2)$. The quotient group $G = W(E_8)/Z(W(E_8))$ has 67 conjugacy classes, all characters are rational, and the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_{120})$ is a subring of rank 65. We consider the 18 absolutely irreducible rational characters in the image. In increments of 256 primes, we compute the convergence to the Gram matrix $A(G)$ for these 18 characters to $2^{13} = 256 \cdot 32$ primes:

$W(E_8)/Z(W(E_8))$				$W(E_8)/Z(W(E_8))$			
	$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$		$\|\|Z_S(G)\|\|_2$	$\|\|Z_S(G)\|\|_8$	$\|\|Z_S(G)\|\|_\infty$
1 :	0.512041	1.947691	3.843750	17 :	0.122505	0.279019	0.473345
2 :	0.256200	0.868283	1.609375	18 :	0.118703	0.265146	0.452473
3 :	0.180087	0.525172	0.929687	19 :	0.114018	0.254474	0.432360
4 :	0.251753	0.848164	1.571289	20 :	0.110361	0.248728	0.442968
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
13 :	0.161766	0.376064	0.648137	29 :	0.110513	0.283699	0.530980
14 :	0.151537	0.350967	0.611049	30 :	0.108019	0.275711	0.514713
15 :	0.139688	0.325884	0.550000	31 :	0.105191	0.262830	0.491053
16 :	0.128557	0.298173	0.504638	32 :	0.102228	0.251891	0.468505

Extending the computation further suggests that the convergence to $M(G)$ is stable for $m > 2^{13}$.

8. Conclusion

A standard tool in Galois group computation is to recognize the probable group from an analysis of Frobenius cycle types. We use an explicit polynomial parametrization of the character ring to identify the irreducible characters in the restriction from orthogonal groups and subsequently from the symmetric group. As in the thesis work of Shieh [18, 19], with the view to classifying Sato-Tate groups, it is recognized that the irreducible characters on the target group provide optimal test functions for recognizing (or rejecting) a given group coming from a Galois representation. We

develop this perspective in the application to the parametrized representation rings of finite groups, with associated lattice structure. Although we focus on Galois groups arising from splitting fields of polynomials over $\mathbb{Q}$, the same methods apply to Galois representations coming form L-series and modular forms, families of exponential sums, and global fields of any characteristic.

At a higher level, the approach through character theory and arithmetic statistics lets us identify when Frobenius distributions of different degrees admit a common Galois subrepresentation. Examples arise in the form of fields with isomorphic normal closures, as described in the above examples of $\mathcal{A}_5$ representations, but more generally one can recognize whether two normal fields admit a common subfield. In this framework orthogonality relations of characters are measured by correlations of Frobenius distributions associated to different representations of the absolute Galois group. This perspective has promising potential for the computational investigation of Galois representations.

Acknowledgements. The author thanks Fernando Rodriguez–Villegas for suggesting the specialization to finite groups of the author's work with Yih-Dar Shieh and Gilles Lachaud, on explicit character theory of orthogonal groups, and for providing notes of his talk in Leiden on the analysis of Galois groups by explicit character theory (see also the 2012 bachelor's thesis of van Bommel [2]). Thanks go also to Claus Fieker for discussions of his algorithm and code in Magma for constructing subfields of the normal closure of a given number field, used in building test examples of number fields with common Galois closure. Finally, the author thanks an anonymous referee for suggesting the permutation groups `8T10` and `8T11`, as the first example (of lowest degree) for which the cycle distributions fail to distinguish the groups. This work is dedicated to the memory of Gilles Lachaud and our conversations on explicit character theory of compact Lie groups.

References

[1] Jos Brakenhoff. *The representation ring and the center of the group ring*. Masters Thesis, Mathematisch Instituut, Universiteit Leiden, 2005.
[2] R. van Bommel. *Using the Chebatorev density theorem to compute the size of Galois groups*. Bachelor's Thesis, Mathematisch Instituut, Universiteit Leiden, 2012.
[3] Gregory Butler and John Mckay. The transitive groups of degree up to eleven. *Comm. Algebra*, **11**, no. 8 (1983)
[4] Greg Butler. The transitive groups of degree fourteen and fifteen, *J. Symb. Comp.*, **16**, no. 5 (1993), 413–422.
[5] John H. Conway, Alexander Hulpke, and John McKay. On transitive permutation groups. *LMS J. Comp. and Math.*, **1** (1998), 1–8.
[6] The GAP Group. GAP — Groups, Algorithms, and Programming, version 4.8.10 (2018), `https://www.gap-system.org`.
[7] Florent Jouve, Emmanuel Kowalski and David Zywina. An explicit integral polynomial whose splitting field has Galois group $W(E_8)$. *J. Théorie des Nombres de Bordeaux*, **20** (2008), no. 3, 761–782.
[8] Weib Bosma, John Cannon, Catherine Playoust. The Magma Algebra System I: The User Language. *J. Symb. Comp.*, **24** (1997), 235–265.
[9] The LMFDB Collaboration. *The L-functions and Modular Forms Database*, `http://www.lmfdb.org/`, 2018.
[10] Magma Computationa Algebra Group. *The Magma Handbook* (2018), `https://magma.maths.usyd.edu.au/magma/handbook/`.
[11] Daniel Bump. *Lie groups*. Springer, 2013.
[12] Francesc Fité and Xavier Guitart. On the rank and the convergence rate towards the Sato–Tate measure. *International Mathematics Research Notices* (2018), to appear, `https://doi.org/10.1093/imrn/rnx234`.
[13] Harold Hardy and Srinivasa Ramanujan. Asymptotic formulae in combinatory analysis. *Proc. of the London Mathematical Society*, 2, **XVII**, 1918, 75–115.
[14] Alexander Hulpke. Constructing transitive permutation groups. *J. Symb. Comp.*, **39**, no. 1 (2005), 1–30.
[15] Michael E. Pohst. Computing invariants of algebraic number fields. In *Group theory, algebra, and number theory.* Colloquium in memory of Hans Zassenhaus, June 4–5, 1993, de Gruyter (1996), 53–73.
[16] Gordon Royle. The transitive groups of degree twelve. *J. Symb. Comp.*, **4** no. 2 (1987), 255–268.
[17] Jean-Pierre Serre. *Linear Representations of Finite Groups*. GTM **42**, Springer, 1971.
[18] Yih-Dar Shieh. *Arithmetic Aspects of Points Counting and Frobenius Distributions*. Thesis, Aix-Marseille Université, 2015
[19] Yih-Dar Shieh. Character theory approach to Sato-Tate groups. *LMS J. Comp. and Math.*, **19**, Issue A (2016), 301–314.
[20] Masaru Takeuchi. A remark on the character ring of a compact Lie group. *J. Math. Soc. Japan*, **23**, no. 4, (1971), 662–675.
[21] William R. Unger. Computing the character table of a finite group. *J. Symb. Comp.*, **41** (2006), 847–862.

EXPLICIT COLEMAN INTEGRATION IN LARGER CHARACTERISTIC

ALEX J. BEST

Abstract. We describe a more efficient algorithm to compute p-adic Coleman integrals on odd degree hyperelliptic curves for large primes p. The improvements come from using fast linear recurrence techniques when reducing differentials in Monsky-Washnitzer cohomology, a technique introduced by Harvey [Har07] when computing zeta functions. The complexity of our algorithm is quasilinear in $\sqrt{p}$ and is polynomial in the genus and precision. We provide timings comparing our implementation with existing approaches.

1. Introduction

In 2001, Kedlaya introduced an algorithm for computing the action of Frobenius on the Monsky-Washnitzer cohomology of odd degree hyperelliptic curves over $\mathbf{Q}_p$ [Ked01]. This has been used to compute zeta functions of the reductions modulo p of such curves, and, starting with the work of Balakrishnan-Bradshaw-Kedlaya [BBK10], to evaluate Coleman integrals between points on them. Computation of Coleman integrals requires more information to be retained throughout the execution of the algorithm than is needed to compute only the way Frobenius acts on cohomology classes, which is all that is needed to compute zeta functions.

Harvey [Har07] introduced a variant of Kedlaya's algorithm, its run time in terms of p alone is $\widetilde{O}(\sqrt{p}) \coloneqq O(\sqrt{p}\log^k \sqrt{p}))$ for some $k \in \mathbf{Z}$. In [BBK10] the authors asked if it is possible to use Harvey's techniques when computing Coleman integrals.

Here we show that one can obtain the same efficiency improvements in Kedlaya's algorithm as Harvey did, whilst retaining enough information to compute Coleman integrals. Specifically, we obtain the following result:

Theorem 1.1. *Let $X/\mathbf{Z}_p$ be a genus g, odd degree hyperelliptic curve. Then for the basis $\{\omega_i = x^i \,\mathrm{d}x/2y\}_{i=0}^{2g-1}$ of $H^1_{\mathrm{dR}}(X)$, let M be the matrix of Frobenius acting on this basis, and $N \in \mathbf{N}$ be such that X and $P, Q \in X(\mathbf{Q}_p)$ are known to precision p^N, assume $p > (2N-1)(2g+1)$. Then, if multiplying two $g \times g$ matrices requires $O(g^\omega)$ ring operations, the vector of Coleman integrals $(\int_P^Q \omega_i)_{i=0}^{2g-1}$ can be computed in time $\widetilde{O}\left(g^\omega \sqrt{p} N^{5/2} + N^4 g^4 \log p\right)$ to absolute p-adic precision $N - v_p(\det(M-I))$.*

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 11Y16, 14F30.

Key words and phrases. Coleman integration, hyperelliptic curves, Kedlaya's algorithm.

I would like to thank Jennifer Balakrishnan, for suggesting this as something that might be possible, and for many subsequent helpful conversations and comments. Additional thanks are due to Jan Tuitman for remarking that ramified extensions should be avoided, by using Lemma 3.2. I have had many interesting conversations with Sachi Hashimoto about Coleman integration. Finally I would like to thank the reviewers for their suggestions. I am grateful for support from the Simons Foundation as part of the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation #550023.

8 Jun 2018 18:22:09 PDT
Version 2 - Submitted to Open Book Series

As surveyed in [BBK10] there are many applications of Coleman integration in arithmetic geometry, notably they are central to the method of Chabauty-Coleman-Kim. This method has been made explicit in some cases, such as in [BD18] Example 2. There, and in general, when working over number fields it is useful to work only with p that split. This is an additional condition on p, which often results in having to take larger p, which gives one motivation for the current work.

In §2 and §3 we recall the set-up for Coleman integration, and, most importantly, exactly what data is needed to compute Coleman integrals on hyperelliptic curves. In §4 we examine the reduction procedure used by Harvey in more detail. We then come to our main new ideas, creating an appropriate recurrence that computes the data necessary for Coleman integration. In §5 we introduce a modification of the linear recurrence algorithm used by Harvey, which is specialised to the type of recurrences we obtained. This is useful when computing Coleman integrals between many endpoints simultaneously. In §6 we describe the main algorithm in detail. In §7 and §8 we analyse its correctness and complexity. Finally in §9 and §10 we give some timings and examples obtained with a SageMath/C++ implementation, showing its practical use.

2. Set-up and notation

Throughout we work with a fixed prime p and an odd degree hyperelliptic curve $X/\mathbf{Z}_p$, of genus $g \geq 1$, given as $y^2 = Q(x)$ with $Q(x) \in \mathbf{Z}_p[x]$. Where $Q(x) = x^{2g+1} + P(x)$ with $\deg(P) \leq 2g$. We assume that the reduction of $Q(x)$ to $\mathbf{F}_p[x]$ has no multiple roots. We fix a desired p-adic precision $N \geq 1$ such that

$$p > (2N-1)(2g+1). \tag{2.1}$$

Let ι denote the hyperelliptic involution, given on the finite affine chart as $(x, y) \mapsto (x, -y)$; the fixed points of this involution are called *Weierstrass points*.

We will make use of several notions from rigid geometry. Points of $X(\mathbf{Q}_p)$ which reduce to the same point in $X_{\mathbf{F}_p}(\mathbf{F}_p)$ are said to lie in the same *residue disk*. A residue disk that contains a Weierstrass point is a *Weierstrass residue disk*.

3. Coleman integration

Coleman integration is a p-adic (line) integration theory developed by Robert Coleman in the 1980s [Col82, CdS88, Col85]. Here we briefly summarise the set-up for this theory (for more precise details, see, for example, [Bes12]). We also recall the key inputs, which are obtained from Kedlaya's algorithm, for performing explicit Coleman integration on hyperelliptic curves, as described in [BBK10].

The setting for Coleman integration as we will be using it is via the Monsky-Washnitzer weak completion of the coordinate ring of the curve minus its Weierstrass points. So, letting $A = \mathbf{Z}_p[x, y, y^{-1}]/(y^2 - Q(x))$, its weak completion is the space $A^\dagger$ of series $\sum_{i=-\infty}^{\infty} R_i(x)y^{-i}$ with $R_i \in \mathbf{Z}_p[x]$, $\deg R_i \leq 2g$ subject to the condition that $\liminf_{|i|\to\infty} v_p(R_i)/|i| > 0$. The p-power Frobenius on $\overline{A} = A/p$ can be lifted to a function $\phi\colon A^\dagger \to A^\dagger$ by sending $x \mapsto x^p$ and $y \mapsto y^{-p}\sum_{k=0}^{\infty}\binom{-1/2}{k}(\phi(Q(x)) - Q(x)^p)^k/y^{2pk}$. We will consider differentials in $\Omega^1_{A^\dagger} = A^\dagger\,\mathrm{d}x \oplus A^\dagger\,\mathrm{d}y/(2y\,\mathrm{d}y - Q'(x)\,\mathrm{d}x))$ with d the exterior derivative

$$\mathrm{d}\colon A^\dagger \to \Omega^1_{A^\dagger};\ \sum_{i=-\infty}^{\infty}\frac{R_i(x)}{y^i} \mapsto \sum_{i=-\infty}^{\infty} R_i'(x)y^{-i}\,\mathrm{d}x - R_i(x)iy^{-i-1}\,\mathrm{d}y. \tag{3.1}$$

8 Jun 2018 18:22:09 PDT
Version 2 - Submitted to Open Book Series

We will say that f is a *primitive* of the exact differential $\mathrm{d}f$. We then define the Monsky-Washnitzer cohomology of A to be $H^1_{\mathrm{MW}}(\overline{A}) = \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p / \mathrm{d}(A^\dagger \otimes \mathbf{Q}_p)$. The action of Frobenius and of the hyperelliptic involution can be extended to $\Omega^1_{A^\dagger}$ and $H^1_{\mathrm{MW}}(\overline{A})$ and the actions of ϕ and ι commute. In particular we have an eigenspace decomposition of all of these spaces under ι into *even* and *odd* parts; the odd part will be denoted with a $-$ superscript. Let $A_{\mathrm{loc}}(X)$ denote the $\mathbf{Q}_p$-valued functions on $X(\mathbf{Q}_p)$ which are given by a power series on each residue disk.

Theorem 3.1 (Coleman)**.** *There is a unique (up to a global constant of integration) $\mathbf{Q}_p$-linear integration map $\int \colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to A_{\mathrm{loc}}(X)$ satisfying:*

1. *Frobenius equivariance, $\int \phi^* \omega = \phi^* \int \omega$,*
2. *the fundamental theorem of calculus, $\mathrm{d} \circ \int$ is the identity on $\Omega^1_{A^\dagger} \otimes \mathbf{Q}_p$,*
3. *and $\int \circ \mathrm{d}$ is the natural map $A^\dagger \to A_{\mathrm{loc}}/(\text{constant functions})$.*

Given points $P, Q \in X(\mathbf{Q}_p)$ the definite integral $\int_P^Q \omega$ is then defined as $\left(\int \omega\right)(Q) - \left(\int \omega\right)(P)$, which is a well-defined function of P, Q.

After fixing a basis $\{\omega_i\}_{i=0}^{2g-1}$ of $H^1_{\mathrm{MW}}(\overline{A})^- = H^1_{\mathrm{dR}}(X)$, any 1-form of the second kind $\omega \in \Omega^1_{A^\dagger}$ can be expressed as $\omega = \mathrm{d}f + \sum_{i=0}^{2g-1} a_i \omega_i$, $f \in A^\dagger$, so by Theorem 3.1 we see that for some $a_i \in \mathbf{Q}_p$

$$\int_P^Q \omega = f(Q) - f(P) + \sum_{i=0}^{2g-1} a_i \int_P^Q \omega_i. \tag{3.2}$$

We can therefore reduce to the case of integrating only the basis differentials ω_i and evaluating the primitive f. The complexity of reducing to this case depends on how ω is presented. For example, if ω has many terms, the total run time can be dominated by finding f and evaluating $f(Q) - f(P)$ in the above. So we will focus on computing $\left\{\int_P^Q \omega_i\right\}_{i=0}^{2g-1}$. In many applications, all that we need to integrate are $\mathbf{Q}_p$-linear combinations of the basis differentials.

The work of Balakrishnan-Bradshaw-Kedlaya [BBK10] describes how to explicitly compute Coleman integrals for differentials on odd degree hyperelliptic curves. They describe how to reduce the problem of computing general Coleman integrals between two points to that of finding a matrix M and $f_i \in A^\dagger$ such that

$$\phi^* \omega_i = \mathrm{d}f_i + \sum_j M_{ij} \omega_j \in \Omega^1_{A^\dagger}. \tag{3.3}$$

Before stating a form of their algorithm, we recall a useful result which allows us to deal with the difficulties arising when the endpoints of the integral are Weierstrass. This can be problematic, as we need to evaluate primitives as in (3.2); if the endpoints are in Weierstrass residue disks, these power series may not converge.

Lemma 3.2 ([BBK10] Lemma 16)**.** *Let $P, Q \in X(\mathbf{Q}_p)$ with Q Weierstrass and let $\omega \in \Omega^{1,-}_{A^\dagger}$ be an odd differential without poles at P, Q. Then $\int_P^Q \omega = \frac{1}{2} \int_P^{\iota(P)} \omega$.*

In particular, if P is also a Weierstrass point, then the integral is zero.

Lemma 3.2 allows us to express general integrals as linear combinations of integrals between two points in non-Weierstrass residue disks and integrals between two

points in the same residue disk (known as *tiny integrals*). Evaluating tiny integrals uses formal integration of power series, see [BBK10] Algorithm 8.

Note that ∞ is a Weierstrass point so Lemma 3.2 applies with $Q = \infty$; integrals based at ∞ can be rewritten as a linear combination of a tiny integral and an integral between two non-Weierstrass points. Specifically, for a Teichmüller point P, if we know the matrix M expressing the action of Frobenius on the basis differentials ω_i, we can use the Frobenius equivariance of the Coleman integral to deduce

$$\begin{pmatrix} \vdots \\ \int_P^\infty \omega_i \\ \vdots \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \vdots \\ \int_P^{\iota(P)} \omega_i \\ \vdots \end{pmatrix} = \frac{(M-I)^{-1}}{2}\begin{pmatrix} \vdots \\ f_i(P) - f_i(\iota(P)) \\ \vdots \end{pmatrix} = (M-I)^{-1}\begin{pmatrix} \vdots \\ f_i(P) \\ \vdots \end{pmatrix} \tag{3.4}$$

The last equality holds as we are using odd differentials, so the $\mathrm{d}f_i$ must also be odd, so from the expansion of (3.1) we see that the f_i must also be odd (up to the constant term, which cancels).

So we will fix ∞ as our basepoint and compute only integrals of the form $\int_P^\infty \omega$; general integrals can be obtained by subtracting two of the above type. We will use the following algorithm, c.f. [BBK10] Remark 15:

Algorithm 3.3. *Input: $P \in X(\mathbf{Q}_p)$, the matrix of Frobenius M, and if P is not in a Weierstrass residue disk, $\{f_i(P')\}_{i=0}^{2g-1}$ for the unique Teichmüller point P' in the same residue disk as P, and f_i as in (3.3).*
Output: $\left\{\int_P^\infty \omega_i\right\}$ for $0 \leq i \leq 2g-1$.

1. *If P is in a Weierstrass residue disk: Let P' be the Weierstrass point in the same residue disk, so that $\int_{P'}^\infty \omega_i = 0$ for all i.*
   Else: Let P' be the (unique) Teichmüller point in the same residue disk as P. Then compute the vector of $\int_{P'}^\infty \omega_i$ using (3.4).
2. *For each i, compute the tiny integral $\int_P^{P'} \omega_i$, as in* [BBK10] *Algorithm 8.*
3. *For each i, sum the result of Steps 1 and 2 to get $\int_P^\infty \omega_i = \int_P^{P'} \omega_i + \int_{P'}^\infty \omega_i$.*

Variants of this algorithm are possible, c.f. [BBK10] Algorithm 11. From the version stated above, it is clear that, beyond solving a linear system and computing tiny integrals, the matrix of Frobenius and evaluations of the primitives f_i at Teichmüller points in non-Weierstrass residue disks are all the input data that is needed to compute arbitrary Coleman integrals. We shall refer to this data as the *Coleman data*. To compute Coleman integrals efficiently, we require an efficient way of computing this data, possibly for several disks of interest.

Remark 3.4. We do not need to compute the f_i themselves to compute integrals, only evaluations at Teichmüller points in prescribed non-Weierstrass residue disks. This simplification is key to our ability to write down a suitable recurrence. Moreover, once the Coleman data is computed, it can be saved and will not need to be recomputed if integrals between other points in the same residue disks are required.

4. Reductions in cohomology

4.1. **Kedlaya's algorithm and Harvey's work.** Kedlaya's algorithm computes the action of Frobenius on Monsky-Washnitzer cohomology up to a specified precision. The general strategy is to begin with a finite p-adic approximation of $\phi^*\omega$ as a (Laurent) polynomial in x and y multiplied by the differential $\mathrm{d}x/2y$. This is

reduced step-by-step via cohomologous differentials of lower polynomial degree, by subtracting appropriate exact forms $\mathrm{d}g$ for polynomials g. This process is continued until one is left with a $\mathbf{Q}_p$-linear combination of basis elements, and we have an expression of the form (3.3). For a given basis $\{\omega_i\}$ of $H^1_{\mathrm{MW}}(\overline{A})^-$, writing each $\phi^*\omega_i$ in terms of this basis results in a matrix of Frobenius acting on $H^1_{\mathrm{MW}}(\overline{A})^-$.

The innovation in [Har07] is to express the reduction process as a linear recurrence, where the coefficients are linear polynomials in the index of the recurrence. A term several steps later in such recurrences can then be found more efficiently than the straightforward sequential approach, via the algorithm of Bostan-Gaudry-Schost [BGS07] Theorem 15. Here we also ultimately appeal to these methods, and so we must examine in more detail the polynomials g used in the reduction steps. We will describe the sum of the evaluations of these g at points of interest as a linear recurrence, so that they may be computed along with the reductions.

We use the basis of $H^1_{\mathrm{MW}}(\overline{A})^-$ consisting of $\omega_i = x^i\,\mathrm{d}x/2y$ for $0 \leq i \leq 2g-1$. This differs by a factor of 2 from the basis used by Harvey and Kedlaya; this choice reduces the number of 2's appearing in our formulae and so appears more natural here. Changing the basis by a scalar multiple has no effect on the matrix of Frobenius, only the exact differentials. An approximation to $\phi^*\omega_i$ is given in [Har07] (4.1) by letting $C_{j,r}$ be the coefficient of x^r in $Q(x)^j$ and $B_{j,r} = p\phi(C_{j,r})\sum_{k=j}^{N-1}(-1)^{k+j}\binom{-1/2}{k}\binom{k}{j} \in \mathbf{Z}_p$ so that

$$\phi^*\omega_i \equiv \sum_{j=0}^{N-1}\sum_{r=0}^{(2g+1)j} B_{j,r}x^{p(i+r+1)-1}y^{-p(2j+1)+1}\frac{\mathrm{d}x}{2y} \pmod{p^N}. \tag{4.1}$$

In (4.1), there are only $(2g+1)\frac{N(N-1)}{2} + N$ terms in total and the exponents of x and y that appear are always congruent to -1 or 1 mod p respectively.

As in [Har07] Section 5, we work with finite-dimensional vector spaces over $\mathbf{Q}_p$

$$W_{s,t} = \left\{f(x)x^sy^{-2t}\frac{\mathrm{d}x}{2y} : \deg f \leq 2g\right\} = \left\langle x^ix^sy^{-2t}\frac{\mathrm{d}x}{2y}\right\rangle_{i=0}^{2g}, \tag{4.2}$$

for $s \geq -1$, $t \geq 0$, where, in addition, we restrict $W_{-1,t}$ to be the subspace of the above for which the coefficient of x^{-1} is zero (i.e. for which $f(0) = 0$).

Notice that $W_{-1,0}$ is naturally identified with $H^1_{\mathrm{MW}}(\overline{A})^-$ with the basis chosen above, so that ω_i is the ith basis element of $W_{-1,0}$. In order to derive an expression for $\phi^*\omega_i$ as a linear combination of the other basis elements, we begin with the approximation of $\phi^*\omega_i$ from (4.1). Then starting with the terms of highest degree in x, which are each inside of some $W_{s,t}$ we reduce "horizontally", finding a cohomologous element of $W_{s-1,t}$ by subtracting an appropriate exact differential. This process is repeated until $s = -1$, but whenever we reach a space $W_{s,t}$ containing a term from (4.1), we add it to the current differential under consideration. We do this for each t appearing as an exponent for a monomial in the original approximation, and for each such t we obtain an element of $W_{-1,t}$. We then reduce "vertically", beginning with the largest t we have, we subtract appropriate exact differentials to reduce the element of each $W_{-1,t}$ to a cohomologous one in $W_{-1,t-1}$ while $t \geq 1$. This is continued until we have reduced everything to the space $W_{-1,0}$, and we

have obtained a linear combination of the basis differentials that is cohomologous to $\phi^*\omega_i$ up to the specified precision.

Note that many horizontal *rows* will not be considered at all. When p is large enough, most steps simply involve reducing terms we already have, as there are comparatively few terms in the (4.1) compared to the total degree. Doing multiple reduction steps quickly will therefore improve the run time of this procedure, even though we have to add new terms occasionally. This is where Harvey applies linear recurrence techniques to speed up this reduction process. We now state the reductions we will use; compared to [Har07] (5.2) and (5.3) we must be more explicit about the exact form we are subtracting, as this data is important for us.

4.2. **Horizontal reduction.** To reduce horizontally from $W_{s,t}$ to $W_{s-1,t}$, we express the highest order basis element $x^{2g}x^s y^{-2t}\,\mathrm{d}x/2y \in W_{s,t}$ as a cohomologous term in $W_{s-1,t}$. The other basis elements are naturally basis elements for $W_{s-1,t}$ just with their indices shifted by 1.

Lemma 4.1 (Horizontal reduction)**.** *We have*

$$\begin{aligned} &x^{2g}x^s y^{-2t}\frac{\mathrm{d}x}{2y} - \frac{-1}{(2t-1)(2g+1)-2s}\,\mathrm{d}(x^s y^{-2t+1}) \\ &= \frac{2sP(x)-(2t-1)xP'(x)}{(2t-1)(2g+1)-2s}x^{s-1}y^{-2t}\frac{\mathrm{d}x}{2y} \in W_{s-1,t}. \end{aligned} \tag{4.3}$$

Proof. We directly compute

$$\begin{aligned} \mathrm{d}(x^s y^{-2t+1}) =& sx^{s-1}y^{-2t+1}\,\mathrm{d}x + (-2t+1)x^s y^{-2t}\,\mathrm{d}y \\ =& \left(sx^{s-1}y^{-2t+1} + \frac{1}{2}(-2t+1)x^s y^{-2t-1}Q'(x)\right)\mathrm{d}x \\ =& \left(2sQ(x) - (2t-1)xQ'(x)\right)x^{s-1}y^{-2t}\frac{\mathrm{d}x}{2y} \\ =& \left(2s-(2t-1)(2g+1)\right)x^{2g+1}x^{s-1}y^{-2t}\frac{\mathrm{d}x}{2y} \\ &+ \left(2sP(x)-(2t-1)xP'(x)\right)x^{s-1}y^{-2t}\frac{\mathrm{d}x}{2y}. \end{aligned} \tag{4.4}$$

Therefore, by subtracting $\frac{1}{2s-(2t-1)(2g+1)}\,\mathrm{d}(x^s y^{-2t+1})$ from $x^{2g}x^s y^{-2t}\,\mathrm{d}x/2y$, the remaining terms are all as stated, and of lower degree. □

4.3. **Vertical reduction.** To reduce vertically from $W_{-1,t}$ to $W_{-1,t-1}$, we express the $2g$ basis elements $x^i y^{-2t}\,\mathrm{d}x/2y \in W_{-1,t}$ as cohomologous terms in $W_{-1,t-1}$.

Lemma 4.2 (Vertical reduction)**.** *Let $R_i(x), S_i(x) \in \mathbf{Z}_p(x)$ be such that $x^i = R_i(x)Q(x) + S_i(x)Q'(x)$ with $\deg R_i \leq 2g-1$, $\deg S_i \leq 2g$. Then*

$$x^i y^{-2t}\frac{\mathrm{d}x}{2y} - \frac{-1}{2t-1}\,\mathrm{d}(S_i(x)y^{-2t+1}) = \frac{(2t-1)R_i(x)+2S_i'(x)}{2t-1}y^{-2(t-1)}\frac{\mathrm{d}x}{2y} \in W_{-1,t-1}.$$

Proof. We have that

$$x^i y^{-2t}\frac{\mathrm{d}x}{2y} = \left(R_i(x)Q(x) + S_i(x)Q'(x)\right)y^{-2t}\frac{\mathrm{d}x}{2y} = R_i(x)y^{-2t+2}\frac{\mathrm{d}x}{2y} + S_i(x)y^{-2t}\,\mathrm{d}y,$$

and also that $\mathrm{d}(S_i(x)y^{-2t+1}) = S_i'(x)y^{-2t+1}\,\mathrm{d}x + (-2t+1)S_i(x)y^{-2t}\,\mathrm{d}y$. Therefore by subtracting $\frac{1}{-2t+1}\,\mathrm{d}(S_i(x)y^{-2t+1})$ from $x^i y^{-2t}\,\mathrm{d}x/2y$, we see that

$$\begin{aligned} x^i y^{-2t}\frac{\mathrm{d}x}{2y} &\sim R_i(x)y^{-2t+2}\frac{\mathrm{d}x}{2y} + \frac{1}{2t-1}S_i'(x)y^{-2t+1}\,\mathrm{d}x \\ &= \frac{(2t-1)R_i(x) + 2S_i'(x)}{2t-1}y^{-2(t-1)}\frac{\mathrm{d}x}{2y}. \end{aligned} \tag{4.5}$$

□

4.4. **Towards a faster algorithm.** In order to make use of the same linear recurrence techniques as Harvey, we express the reduction process as we descend through the indices s, t as a linear recurrence with coefficients linear polynomials in s, t. We describe such a recurrence that retains enough information to compute Coleman integrals. By working with a number of evaluations of the primitives on prescribed points on the curve, rather than the primitives themselves as power series, we only have to deal with a vector of fixed size at each step. This is preferable to maintaining a power series as we reduce, adding terms at each step.

We will now give an idea of the approach, giving the details in the next section. Let us first consider the end result of one row of the horizontal reduction process. Fixing a row t, after the reduction we have an equality of the form

$$\sum_{s\geq 0} a_s x^s y^{-2t}\frac{\mathrm{d}x}{2y} - \mathrm{d}\left(\sum_{s\geq 0} c_s x^s y^{-2t+1}\right) = \sum_{i=0}^{2g-1} m_i x^i y^{-2t}\frac{\mathrm{d}x}{2y} \in W_{-1,t} \tag{4.6}$$

in which the terms of the exact differential were found in decreasing order as the reductions are performed. Unfortunately, adding each new term as it is obtained is not a *linear* recurrence in the index s, as we have s appearing in the exponent of x in each term. Instead we observe that we can express the exact differential as

$$\mathrm{d}\left((c_0 + x(c_1 + x(\cdots + x(c_r))))y^{-2t+1}\right). \tag{4.7}$$

In essence, we are applying the *Horner scheme* for polynomial evaluation.

Now we specialise to the case of computing the evaluation $f_i(P)$ of the primitive for some point $P = (x(P), y(P))$. We can, at each step, compute a further bracketed term starting from the innermost; using the given x, y values, we get a recurrence whose final term is the same as the original evaluation. So we can compute the terms of a recurrence of the form

$$f_{i,0} = 0,\ f_{i,n} = x(P)f_{i,n-1} - \frac{1}{(2t-1)(2g+1) - 2s}d_{i,n} \tag{4.8}$$

where $s = s_{\max} - n$ decreases from its maximum value, and $d_{i,n}$ is the coefficient of the monomial removed in the nth step of the reduction process. Multiplying the result of this recurrence by the factor y^{-2t+1} (which is constant along the row) will result in the evaluation of the primitive for the row. At each step we will no longer have an evaluation of the primitive so far, it is only after completing all the reduction steps that each term will have the correct power of x.

We may use the same technique for the vertical reductions; here we have

$$\sum_{t\geq 0}\sum_{i=0}^{2g-1} m_i x^i y^{-2t}\frac{\mathrm{d}x}{2y} - \mathrm{d}\left(\sum_{t\geq 1}\sum_{i=0}^{2g} d_{ti}S_i(x)y^{-2t+1}\right) = \sum_{i=0}^{2g-1} M_i x^i\frac{\mathrm{d}x}{2y} \in W_{-1,0},$$

where now writing $d_t = \sum_{i=0}^{2g-1} d_{t,i} S_i(x)$, the exact differential can be expressed as

$$\mathrm{d}\left(y^{-1}(d_1 + y^{-2}(d_2 + y^{-2}(\cdots(d_{r-1} + y^{-2}(d_r))\cdots)))\right). \tag{4.9}$$

Remark 4.3. The factor y^{-2t+1} appears in every term in the primitive in row t. It is the same factor in the primitive for the vertical reduction from row t to row 0. So we can initialise the vertical recurrence from $W_{-1,t}$ with both the differential and the evaluations obtained from horizontal reduction along row t, and let the vertical reduction steps multiply the evaluation of the row primitives by this factor.

Now we write down the recurrences for both horizontal and vertical reductions precisely using matrices acting on appropriate vector spaces.

4.5. **The recurrence.** We will now switch to working with a $\mathbf{Q}_p$ vector $h^t(s) \in W_{s,t} \times \mathbf{Q}_p^L$ (resp. $v(t) \in W_{-1,t} \times \mathbf{Q}_p^L$); these are of length $2g+1+L$ (resp. $2g+L$) in the horizontal case (resp. vertical case). The first entries represent the current differential we have reduced to, with respect to the basis given in (4.2). The last L entries will contain the evaluations of the terms of the primitive picked up so far, one for each of the L points $P_1, \ldots, P_L \in X(\mathbf{Q}_p)$ we want evaluations at.

When we horizontally reduce, using the result of Lemma 4.1, the two terms we are interested in, the exact differential and the reduction, have a common denominator of $D_H^t(s) = (2t-1)(2g+1) - 2s$. Similarly, in the vertical case, the two terms of interest in Lemma 4.2 have a common denominator of $D_V(t) = 2t-1$.

Writing out the result of a single reduction step in terms of these vectors, we see that we need to compute the terms of the recurrence given by $h^t(s) = R_H^t(s+1)h^t(s+1)$ in the horizontal case, for $R_H^t(s)$ defined by

$$D_H^t(s)R_H^t(s) = M_H^t(s) = \left(\begin{array}{cccc|ccc} 0 & \cdots & 0 & p_0^t & & & \\ D_H^t(s) & \cdots & 0 & p_1^t & & & \\ \vdots & \ddots & \vdots & \vdots & & & \\ 0 & \cdots & D_H^t(s) & p_{2g}^t & & & \\ \hline 0 & \cdots & 0 & -1 & x(P_1)D_H^t(s) & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & -1 & 0 & \cdots & x(P_L)D_H^t(s) \end{array}\right), \tag{4.10}$$

where p_i^t is the linear function of s obtained as the coefficient of x^i in $2sP(x) - (2t-1)xP'(x)$. To divide through by $D_H^t(s)$ we must multiply some terms by $D_H^t(s)$.

For the vertical reductions we use $R_V(t)$ defined by

$$D_V(t)R_V(t) = M_V(t) = \left(\begin{array}{ccc|ccc} (2t-1)r_{0,0} + 2s'_{0,0} & \cdots & (2t-1)r_{2g-1,0} + 2s'_{2g-1,0} & & & \\ \vdots & \ddots & \vdots & & & \\ (2t-1)r_{0,2g-1} + 2s'_{0,2g-1} & \cdots & (2t-1)r_{2g-1,2g-1} + 2s'_{2g-1,2g-1} & & & \\ \hline -S_0(x(P_1)) & \cdots & -S_{2g-1}(x(P_1)) & y(P_1)^{-2}D_V(t) & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -S_0(x(P_L)) & \cdots & -S_{2g-1}(x(P_L)) & 0 & \cdots & y(P_L)^{-2}D_V(t) \end{array}\right), \tag{4.11}$$

where $r_{i,j}$ is the coefficient of x^j in $R_i(x)$ and $s'_{i,j}$ is the coefficient of x^j in $S'_i(x)$. Once again we have multiplied the rightmost block by $D_V(t)$ to extract the common denominator. We do this to express the reduction steps as linear recurrences with linear polynomial coefficients, rather than rational function coefficients.

Introducing the notation $M_H^t(a,b) = M_H^t(a+1)\cdots M_H^t(b-1)M_H^t(b)$ (and the analogous $M_V(a,b)$), we can write the upshot of the above as

Theorem 4.4. *Let $h^t(s) = (\omega, 0) \in W_{s,t} \times \mathbf{Q}_p^L$, and $f\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p$, write $c(f)$ for the* correction factor*, the linear endomorphism of $W_{s,t} \times \mathbf{Q}_p^L$ that is the identity on $W_{s,t}$ and scales each component of $\mathbf{Q}_p^L$ by $f(P_\ell)$ for the corresponding P_ℓ. Then the reduced vector $c(y^{-1})R_V(0,t)c(y^2)R_H^t(-1,s)h^t(s) \in W_{-1,0} \times \mathbf{Q}_p^L$ is such that the projection onto $W_{-1,0}$ is some $\tilde{\omega}$ with $\tilde{\omega} = \omega - \mathrm{d}(g)$ for some $g \in A^\dagger$, and the projection onto $\mathbf{Q}_p^L$ is $(g(P_1), \ldots, g(P_L))$.*

As the approximation in (4.1) has summands that occur in several different $W_{s,t}$'s, we cannot simply find the product matrix and apply it to a single vector. Instead, we must work through the various subspaces doing as many reductions as possible before we reach a new monomial from the original approximation. As D_H and D_V are scalar matrices, we can commute them past the M_V's and M_H's. This separates out the components so we can work just with products of matrices of linear polynomials. This reduces the problem to finding several of the products $M_V(a,b)$ and $M_H^t(a,b)$. In practice, to use as little p-adic precision as we can, we must not allow too many runs of multiplications by p and then divisions by p, so that the relative precision stays as large as possible. This will be addressed in §7.

5. Linear recurrence algorithms

In this section, we recall and adapt some methods for finding subsequent terms of linear recurrences with linear polynomial coefficients. The set-up is that we are given an $m \times m$ matrix $M(x)$ with entries that are linear polynomials over a ring R and wish to obtain several products $M(x,y) = M(y)M(y-1)\cdots M(x+1)$ for $x < y$ integers. We let $\mathrm{MM}(m,n)$ be the number of ring operations used when multiplying an $n \times m$ matrix by an $m \times m$ matrix, both with entries in R. Then $\mathrm{MM}(m) = \mathrm{MM}(m,m)$ is the cost of multiplying two $m \times m$ matrices. We will not say much about these functions here, as modern theoretical bounds for these functions do not affect the point of our main result; however see [LG12] for some recent work on the topic. Using naive matrix multiplication, we have $\mathrm{MM}(m,n) = O(m^2 n)$, which if $m^2 = o(n)$, cannot be improved upon asymptotically. Whenever $n \geq m$ we can partition an $n \times m$ matrix into roughly n/m blocks each of size $m \times m$. These blocks can then be multiplied individually for a run time of $\mathrm{MM}(m,n) = O(\mathrm{MM}(m)\frac{n}{m})$. We will also let $\mathrm{M}(n)$ be the number of ring operations needed to multiply two polynomials of degree n with coefficients in R.

The method of Bostan-Gaudry-Schost requires that certain elements of R be invertible. Moreover, they assume as input a product $\mathrm{D}(\alpha, \beta, k)$ of several of these inverses. We will apply these methods in $\mathbf{Z}/p^N\mathbf{Z}$ where the cost of computing inverses is negligible compared to the rest of the algorithm, so we will take this step for granted; see [BGS07] for more details.

With the above set-up, Harvey, [Har07] Theorem 6.2, adjusts the algorithm of Bostan-Gaudry-Schost, [BGS07] Theorem 15, to prove the following theorem:

Theorem 5.1. *Let $M(x)$ be a $m \times m$ matrix with entries that are linear polynomials in $R[x]$, let $0 \leq K_1 < L_1 \leq K_2 < L_2 \leq \cdots \leq K_r < L_r \leq K$ be integers, and let $s = \lfloor \log_4 K \rfloor$. Suppose that $2, 3, \ldots, 2^s + 1$ are invertible in R. Suppose also that $r < K^{\frac{1}{2}-\epsilon}$, with $0 < \epsilon < 1/2$. Then $M(K_1, L_1), \ldots, M(K_r, L_r)$ can be computed using $O(\mathrm{MM}(m)\sqrt{K} + m^2\mathrm{M}(\sqrt{K}))$ ring operations in R.*

In order to apply this theorem to the above recurrences for computing the Coleman data, we introduce a variant better suited to the recurrences we obtained in

§4.4. If we simply applied the same algorithm/result as Harvey naively, we would not get as good a run time in general.

Theorem 5.2. *With the same set-up as Theorem 5.1, except that now let $M(x)$ be instead an $(m+n)\times(m+n)$ block lower triangular matrix with 4 blocks, with top left block an $m\times m$ matrix and bottom right block a diagonal matrix:*

$$\left(\begin{array}{c|c} A & 0 \\ \hline B & \begin{smallmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{smallmatrix} \end{array}\right). \tag{5.1}$$

Then the interval products $M(K_1, L_1), \ldots, M(K_r, L_r)$ can be computed using only $O\left((\mathrm{MM}(m)+\mathrm{MM}(m,n))\sqrt{K} + (m^2+mn)\mathrm{M}(\sqrt{K})\right)$ ring operations in R.

Proof. The algorithm to do this is the same as the one given for Theorem 5.1 in [Har07] Theorem 6.2, only adjusted to take advantage of the fact that the matrices used are of a more restricted form as follows:

First, note that a product of matrices of the assumed form is again of the same shape, so one can work only with matrices of this form throughout. Such matrices should then be stored without keeping track of the entries that are always 0, as a pair of matrices A, B of size $m\times m$ and $n\times m$ respectively, and a list containing the n bottom right diagonal entries. Now the algorithm of Harvey and Bostan-Gaudry-Schost should be applied using this fixed representation.

The complexity of this algorithm is dominated by two main subtasks: shifting evaluations of the matrices and matrix multiplication. During the shifting step, we need only interpolate the non-zero entries; there are $(m+n)m+n$ of these. The number of ring operations required for this is then $O((m^2+mn)\mathrm{M}(\sqrt{K}))$.

For the matrix multiplication steps, the restricted form of the matrix once again allows us to use a specialised matrix multiplication routine. Here we can evaluate the block matrix product more efficiently, multiplying only the non-zero blocks, and using the fact that multiplying an $n\times m$ matrix on the right by a square diagonal matrix stored as a list uses only $O(nm)$ operations. Therefore the total complexity of multiplying two matrices of this form is $O(\mathrm{MM}(m,n)+\mathrm{MM}(m))$. As we do not modify the algorithm in any other way, the result follows. □

The conditions on the matrix in Theorem 5.2 are precisely those satisfied by the matrices $M_H^t(s)$ and $M_V(t)$ from §4. So we may use this algorithm for computing block horizontal and vertical reductions for certain intervals.

Remark 5.3. As well as utilising the polynomial structure of our matrices, for any row with sufficiently many terms compared to the desired precision, it is also possible to interpolate p-adically. This idea is due to Kedlaya and is explained in [Har07] Section 7.2.1. Using this allows us to compute fewer interval products using Theorem 5.2 by interpolating the remaining ones.

If we could compute to infinite precision, it would be optimal to reduce as far as possible at each reduction step, i.e., until we get to index of a new term that needs adding. However, in practice, we should divide by p as soon as possible, in order to reduce the number of extra p-adic digits needed throughout. Therefore analysing when divisions by p occur informs which interval products are found.

6. The algorithm

In this section we describe the complete algorithm derived in the previous sections. The flow of the algorithm is the same as that of Harvey, only we use our larger matrices throughout and have to make some small adjustments to the evaluations. Care should be taken in all steps where division occurs, see §7.

Algorithm 6.1 (Computation of Coleman data)**.** *Input: A list of points* $\{P_\ell\}_{1\le\ell\le L}$ *in non-Weierstrass residue disks, precision* N*.*

Output: Matrix of Frobenius M*, modulo* p^N*, such that* $\omega_i = \mathrm{d}f_i + \sum_j M_{ij}\omega_j$*, evaluations* $f_i(P_\ell)$ *modulo* p^N *for all* i, ℓ *also.*

(1) *For each row index* $t = (p(2j+1)-1)/2$ *for* $0 \le j \le N-1$ *do:*
   (a) *Compute the horizontal reduction matrices* $M_H^t((k-1)p, kp-2g-2)$ *and* $D_H^t((k-1)p, kp-2g-2)$ *for* $0 \le k \le (2g+1)(j+1)-1$ *using Theorem 5.2, and the p-adic interpolation outlined in* [Har07] *7.2.1, for* $k > N$*.*
   (b) *For each basis differential* ω_i*,* $0 \le i \le 2g-1$ *do:*
      (i) *Initialise a vector* $h_{ij} \in (\mathbf{Z}/p^{N+1}\mathbf{Z})^{2g+1+L}$
      (ii) *For each column index* $s = p(i+r+1)-1$ *for* $r = (2g+1)j$ *down to* 0 *do:*
         (A) *Add the* $x^s y^{-2t}$ *term of (4.1) to* h_{ij}*.*
         (B) *Set* $h_{ij} = R_H^t(kp-2g-2, kp)h_{ij}$ *by doing* $2g+2$ *matrix-vector products.*
         (C) *Set* $h_{ij} = R_H^t((k-1)p, kp-2g-2)h_{ij}$*.*
         (D) *Set* $h_{ij} = R_H^t((k-1)p)h_{ij}$*.*

(2) *Initialise a* $2g \times L$ *matrix for the evaluations* E *and a* $2g \times 2g$ *matrix for the action of Frobenius* M*.*

(3) *Compute the vertical reduction matrices* $M_V(0, (p-1)/2), M_V((p-1)/2 + jp, (p-1)/2 + (j+1)p)$ *for* $1 \le j < N$ *and the corresponding* $D_V(t)$*'s to precision* p^{N+1} *using Theorem 5.2, and divide through to obtain the corresponding* R_V*'s, label them* R_j*.*

(4) *For each basis differential* ω_i*,* $0 \le i \le 2g-1$*:*
   (a) *Initialise a zero vector* $v_i \in (\mathbf{Z}/p^N\mathbf{Z})^{2g+L}$*.*
   (b) *For each row index* $t = (p(2j+1)-1)/2$ *for* $j = N-1$ *down to* 0 *do:*
      (i) *Add the last* $2g+L$ *entries of* h_{ij} *to* v_i*, correcting the last* L *entries as in Theorem 4.4.*
      (ii) *Set* $v_i = R_j v_i$*.*
   (c) *Set the* i*th column of* M *to be the first* $2g$ *entries of* v_i*.*
   (d) *Set the* i*th row of* E *to be the last* L *entries of* v_i*, correcting them to be evaluations as in Theorem 4.4.*

(5) *Output the matrix of Frobenius* M *and the matrix of evaluations* E*.*

Remark 6.2. We have not used the fact that in Algorithm 3.3 we only needed to evaluate at Teichmüller points. Using Teichmüller points only serves to make the description of Coleman integration a little simpler, and provides a convenient set of points corresponding to residue disks. This allows one to store the output of Algorithm 6.1 for further computations involving the same set of residue disks.

One simpler variant of this algorithm is to compute evaluations for one point at a time, re-running the whole procedure including finding the matrix of Frobenius once for each point. The advantage of this method is not needing a specialised version of

the linear recurrence algorithms as in Theorem 5.2. While this would result in the same theoretical run time if $g^2 \in o(p)$, recomputing the matrix of Frobenius would be a duplication of work and inefficient in many parameter ranges.

7. Precision

In this section we examine the level of p-adic precision that needs to be maintained throughout, in order to compute the matrix of Frobenius and evaluations of primitives to precision $O(p^N)$. We follow Harvey's approach in [Har07] Section 7 and prove that analogous results hold for our recurrence.

Lemma 7.1. *During horizontal reduction, the evaluations of the primitives remain integral. Moreover, if the calculations are performed with initial data known to absolute precision p^N and intermediate computations are performed with an absolute precision cap of p^{N+1}, then whenever division by p occurs, the dividend is known to absolute precision p^{N+1}, so that the quotient is known to absolute precision $O(p^N)$.*

Proof. As we begin with evaluation 0, we must show that if the evaluations are integral, they remain so after several reduction steps. Any point $P = (x, y)$ that we are evaluating at is assumed not be in a Weierstrass residue disk and in particular not in the residue disk at infinity. Hence x is integral and multiplication by it will never reduce p-adic valuation.

In the horizontal reduction matrix (4.10), the only nonzero terms in the bottom left block are the -1s in the rightmost column which will not disturb integrality.

When $D_H^t(s) \equiv 0 \pmod p$, it is shown in [Har07] Claim 7.3, using the assumptions on p in (2.1), that the vector currently being reduced has its $(2g+1)$-component divisible by p and is correct to absolute precision p^{N+1}. Thus this can be divided by $D_H^t(s)$ while keeping absolute precision p^N. Every column of $M_H^t(s)$ other than the $(2g+1)$st has $D_H^t(s)$ as a factor, so the division can be performed.

All other steps follow directly from the work of Harvey. □

Lemma 7.2. *During vertical reduction, the evaluations of the primitives remain integral. Moreover, if the calculations are performed with initial data known to absolute precision p^N and intermediate computations are performed with an absolute precision cap of p^{N+1}, then whenever division by p occurs, the dividend is known to absolute precision p^{N+1}, so that the quotient is known to absolute precision $O(p^N)$.*

Proof. Any point $P = (x, y)$ that we are evaluating at is assumed not to be in a Weierstrass residue disk and in particular not in the residue disk at infinity. Hence y is a unit and multiplying or dividing by it will not change p-adic valuation.

We check that the analysis in [Har07] Lemmas 7.7 and 7.9 may be adjusted to apply with our extended $M_V(t)$. Assume that $t \equiv 1/2 \pmod p$ so that $D_V(t) \equiv 0 \pmod p$, in this case $v_p(D_V(t)) = 1$ as (2.1) implies $D_V(t) < p^2$. Unlike in [Har07] Lemma 7.7, our matrix $M_V(t)$ will not have integral inverse as $D_V(t)$ appears in the bottom right block, so $M_V(t)$ is singular mod p. Instead, the inverse of the block lower triangular $M_V(t)$ has integral top left block, and the bottom two blocks have valuation at least -1. Now letting $t_0 = (p-1)/2$ and $X = D_V(t_0, t_0 + p + 1)^{-1} M_V(t_0, t_0 + p + 1)$, the argument in [Ked01] Lemma 2 implies that pX is integral. The argument says that taking $\omega \in W_{-1,t_0+p+1}$ with integral coefficients, the primitive g of $X\omega - \omega$ becomes integral after multiplication by p, and hence the evaluation of pg at a point in a non-Weierstrass residue disk is

integral. The entries in the bottom left block of X are evaluations of this form up to a power of $y(P)$, which will not affect integrality. The bottom right block of X is integral already as it is simply a power of the diagonal matrix $\mathrm{diag}((y(P_\ell)^{-2})_\ell)$. So each term of the block matrix product $(pX)M_V(t_0+p+1)$ is integral, and $M_V(t_0,t_0+p) = D_V(t_0,t_0+p+1)XM_V(t_0+p+1)^{-1}$ is divisible by p. □

Remark 7.3. Multiplying by $(M-I)^{-1}$, as in (3.4), will lose $v_p(\det(M-I))$ digits of absolute p-adic precision. As $v_p(\det(M-I)) = v_p(\mathrm{Jac}(X)(\mathbf{F}_p)[p])$, this is at most g in the *anomolous case*, and in general we expect that it is 0, so if $g = O(N)$ the whole computation can be repeated with the extra precision required at no extra asymptotic cost.

8. Run time analysis

Having described the algorithm in detail, we now analyse its run time, in order to prove Theorem 1.1. First of all we analyse each step of Algorithm 6.1.

The main step is the computation of the reduction matrices via Theorem 5.2. In this case, we have $m = 2g$ (+1 in the horizontal case) and $n = L$. When reducing horizontally, for each row the largest index is bounded by $K = O(Np)$. When reducing vertically our index is also at most $O(Np)$. As there are N rows in total, we obtain a total of

$$O\left(N((\mathrm{MM}(g)+\mathrm{MM}(g,L))\sqrt{Np}+(g^2+gL)\mathrm{M}(\sqrt{Np}))\right) \tag{8.1}$$

ring operations to compute the matrices. Using that $\mathrm{M}(d) \in \widetilde{O}(d)$, that $\mathrm{MM}(m) = m^\omega$ for some $2 \le \omega \le 3$, and the above discussion of $\mathrm{MM}(m,n)$, we simplify to $O\left((g^\omega + Lg^{\omega-1})\sqrt{p}N^{3/2}\right)$ ring operations, bit complexity $\widetilde{O}\left((g^\omega + Lg^{\omega-1})\sqrt{p}N^{5/2}\right)$.

The remaining operations are exactly as analysed by Harvey in [Har07] Section 7.4. With our larger, but still sparse, horizontal reduction matrices, each reduction step without Theorem 5.2 uses $O(g+L)$ rather than $O(g)$ ring operations, for a total of $O(N^3g^3(g+L))$ ring operations, or $\widetilde{O}(N^4g^3(g+L)\log p)$ bit operations. We then have a total time complexity of

$$\widetilde{O}\left((g^\omega + Lg^{\omega-1})\sqrt{Np}N^2 + N^4g^3(g+L)\log p\right). \tag{8.2}$$

Now we turn to the algorithm for computing Coleman integrals, obtained by running Algorithm 6.1 once and then Algorithm 3.3 once for each point. The analysis here is the same as that in [BBK10] Section 4.2, where, by using Algorithm 6.1 instead of Kedlaya's algorithm, we may replace the $\widetilde{O}(pN^2g^2)$ in their complexity analysis with (8.2). The remaining steps to complete the Coleman integration are logarithmic in p and are dominated by the logarithmic in p term of (8.2).

If L is fixed (for example $L = 2$ when computing integrals between two points) the complexity is as in [Har07] Theorem 1.1. This finishes the proof of Theorem 1.1.

Remark 8.1. The version of Kedlaya's algorithm used in [BBK10] Algorithm 10, seems to have an advantage in that it outputs the power series of the f_i's. This could of course be re-used later to evaluate at further points without re-running Kedlaya's algorithm. However, for p large enough, this series has so many terms that it is faster asymptotically to recompute everything with the algorithm given here, than it is to evaluate the power series at one point.

$p\backslash N$	1	3	5	7	9
131	1.14/0.01	3.67/0.02	9.36/0.07	16.90/0.12	20.06/0.49
257	1.96/0.01	8.90/0.03	20.83/0.07	30.91/0.18	63.14/0.68
521	4.73/0.01	19.23/0.03	39.18/0.08	86.49/0.62	162.81/0.91

TABLE 1. Timings for genus 3: Sage 8.0 time/New time (sec)

9. Implementation

We have implemented this algorithm in C++ as an extension of David Harvey's `hypellfrob` package. This extension has been wrapped and can be easily used from within Sage [Sag18]. The implementation is included as part of the supplementary materials to this paper. This implementation uses naive matrix multiplication (for which $\omega = 3$) and does not take into account the special form of the matrices, as in Theorem 5.2; so the run time of this implementation will not have the asymptotic behaviour stated in (8.2) for the parameter L.

In Table 1, we list some timings obtained using this implementation in genus 3, for various primes p and p-adic precision bounds N. For comparison, we also list timings for the functionality for computing Coleman integrals in Sage 8.0. The implementation in Sage is written in Python, rather than C++, so we would expect some speed-up even if a superior algorithm was not used. Specifically we have compared the time to compute the Coleman data only, and do not include any of the time spent doing the linear algebra and tiny integral steps of Coleman integration, which should be comparatively fast. As such, we only time the components that will differ between the old and new approaches. For the existing Sage code we have timed both finding the matrix of Frobenius and the primitives (by calling `monsky_washnitzer.matrix_of_frobenius_hyperelliptic`), and the time to evaluate the resulting primitive at one point. This is compared with the time taken by the new implementation, called from its Sage wrapper with one point specified, this outputs the matrix of Frobenius and the evaluations at that point. All timings and examples are on a single 16 AMD Opteron 8384 2.7GHz processor on a machine with 16 cores and 82 GB RAM. While this table is mostly intended to show practicality, in the $N = 9$ column the square root dependence on p can be seen. The large jump in the timings between $p \approx 256$ and $p \approx 512$ for $N = 7$ could be explained by the fact that this is the cut off between when an element of $\mathbf{Z}/p^N\mathbf{Z}$ is representable in one machine word.

10. Examples

In this section we give an explicit example of a computation we can perform with this technique, demonstrating how large we can feasibly take the parameters. We compare our implementation to the existing functionality for Coleman integration in Sage 8.0 for this example.

The current implementation uses the basis $x^i\,\mathrm{d}x/y$, to remain consistent with Harvey's notation. As the existing functionality for Coleman integration in Sage 8.0 uses the basis $x^i\,\mathrm{d}x/2y$ for cohomology, we must divide the obtained evaluations by 2 to compare them to those returned by Sage or Algorithm 6.1.

Example 10.1. Let $C\colon y^2 = x^5 + \frac{33}{16}x^4 + \frac{3}{4}x^3 + \frac{3}{8}x^2 - \frac{1}{4}x + \frac{1}{16}$ be Leprévost's curve, as in [BBK10] Example 21. Then letting $P = (-1, 1)$, $Q = (0, \frac{1}{4})$ and

$p = 2^{45} + 59 = 35184372088891$, using our implementation we can compute the matrix of Frobenius M to 1 p-adic digit of precision, and also that

$$f_0(P) - f_0(Q) = O(p), \qquad f_1(P) - f_1(Q) = O(p),$$
$$f_2(P) - f_2(Q) = 7147166195043 + O(p), \quad f_3(P) - f_3(Q) = 9172338112529 + O(p).$$

Computing this (and finding $(M-1)^{-1}$) takes a total of 27.8 minutes (with a peak memory usage of 2.9GB). Evaluating Coleman integrals for such a large prime is far out of the range of what was possible to compute in reasonable amount of time using the previous implementation. In fact, even when $p = 2^{14} + 27$ the existing Sage functionality takes 53.2 minutes, and uses a larger volume of memory (12GB).

As we have used only 1 digit of p-adic precision, the points P and Q are congruent up to this precision to the corresponding Teichmüller point in their residue disk. So, for this example, we do not need to worry about computing tiny integrals; the vector of Coleman integrals $\int_Q^P \omega_i$ can be obtained from the above vector of evaluations by multiplying by $(M-1)^{-1}$. Doing this gives us the vector $(O(p), O(p), 9099406574713 + O(p), 7153144612900 + O(p))$ reflecting the holomorphicity of the first two basis differentials only. We have also run the same example with precision $N = 3$; this took 22.5 hours and used a peak of 50GB of memory.

11. Future directions

The assumptions on the size of p allow us to use at most one extra digit of p-adic precision; it should be possible to relax this assumption somewhat, using a more complicated algorithm instead. Similarly it should be possible to work over extensions of $\mathbf{Q}_p$, or remove the assumption that $Q(x)$ is monic.

Kedlaya's algorithm has been generalised to other curves and varieties, e.g. [Har12, GG01, Gon15, Tui17] and Harvey's techniques have also been generalised to some of these cases [Min10, ABC+18]. Moreover, explicit Coleman integration has also been carried out in some of these settings, for even degree hyperelliptic curves [Bal15], and for general curves [BT17]. It would be interesting to adapt our techniques to those contexts. Iterated Coleman integrals are also of interest and have been made computationally effective [Bal13]. Extending the algorithm presented here to compute iterated integrals is another natural next step. Harvey has also described an *average polynomial time* algorithm for dealing with for many primes at once [Har14]. The author plans to explore the feasibility of analogous techniques when computing Coleman integrals.

References

[ABC+18] Arul V., Best A.J., Costa E., Magner R., Triantafillou N. "Computing Zeta Functions of Cyclic Covers in Large Characteristic". In "ANTS XIII—Proceedings of the Thirteenth Algorithmic Number Theory Symposium", This volume. Math. Sci. Publ., Berkeley, CA, 2018.

[Bal13] Balakrishnan J.S. "Iterated Coleman integration for hyperelliptic curves". In "ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium", volume 1 of *Open Book Ser.*, pages 41–61. Math. Sci. Publ., Berkeley, CA, 2013. doi:10.2140/obs.2013.1.41.

[Bal15] ———. "Coleman integration for even-degree models of hyperelliptic curves". *LMS J. Comput. Math.*, 18(1):258–265, 2015.

[BBK10] Balakrishnan J.S., Bradshaw R.W., Kedlaya K.S. "Explicit Coleman integration for hyperelliptic curves". In "Algorithmic number theory", volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010.

[BD18] Balakrishnan J.S., Dogra N. "Quadratic Chabauty and rational points I: p-adic heights". *Duke Mathematical Journal*, 2018. http://arxiv.org/abs/1601.00388v2.

[Bes12] Besser A. "Heidelberg lectures on Coleman integration". In "The arithmetic of fundamental groups—PIA 2010", volume 2 of *Contrib. Math. Comput. Sci.*, pages 3–52. Springer, Heidelberg, 2012.

[BGS07] Bostan A., Gaudry P., Schost E. "Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator". *SIAM J. Comput.*, 36(6):1777–1806, 2007.

[BT17] Balakrishnan J.S., Tuitman J. "Explicit Coleman integration for curves". 2017. 1710.01673v2.

[CdS88] Coleman R., de Shalit E. "p-adic regulators on curves and special values of p-adic L-functions". *Invent. Math.*, 93(2):239–266, 1988.

[Col82] Coleman R.F. "Dilogarithms, regulators and p-adic L-functions". *Invent. Math.*, 69(2):171–208, 1982.

[Col85] ———. "Torsion points on curves and p-adic abelian integrals". *Ann. of Math. (2)*, 121(1):111–168, 1985.

[GG01] Gaudry P., Gürel N. "An extension of Kedlaya's point-counting algorithm to superelliptic curves". In "Advances in cryptology—ASIACRYPT 2001 (Gold Coast)", volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.

[Gon15] Gonçalves C. "A point counting algorithm for cyclic covers of the projective line". In "Algorithmic arithmetic, geometry, and coding theory", volume 637 of *Contemp. Math.*, pages 145–172. Amer. Math. Soc., Providence, RI, 2015.

[Har07] Harvey D. "Kedlaya's algorithm in larger characteristic". *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.

[Har12] Harrison M.C. "An extension of Kedlaya's algorithm for hyperelliptic curves". *J. Symbolic Comput.*, 47(1):89–101, 2012.

[Har14] Harvey D. "Counting points on hyperelliptic curves in average polynomial time". *Ann. of Math. (2)*, 179(2):783–803, 2014.

[Ked01] Kedlaya K.S. "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology". *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[LG12] Le Gall F. "Faster algorithms for rectangular matrix multiplication". In "2012 IEEE 53rd Annual Symposium on Foundations of Computer Science—FOCS 2012", pages 514–523. IEEE Computer Soc., Los Alamitos, CA, 2012.

[Min10] Minzlaff M. "Computing zeta functions of superelliptic curves in larger characteristic". *Math. Comput. Sci.*, 3(2):209–224, 2010.

[Sag18] Sage Developers, The. *SageMath, the Sage Mathematics Software System (Version 8.0.0)*, 2018. http://www.sagemath.org.

[Tui17] Tuitman J. "Counting points on curves using a map to $\mathbf{P}^1$, II". *Finite Fields Appl.*, 45:301–322, 2017.

111 Cummington Mall, Boston MA 02215
Email address: alex.j.best@gmail.com

COMPUTING ZETA FUNCTIONS OF CYCLIC COVERS IN LARGE CHARACTERISTIC

VISHAL ARUL, ALEX J. BEST, EDGAR COSTA, RICHARD MAGNER, AND NICHOLAS TRIANTAFILLOU

Abstract. We describe an algorithm to compute the zeta function of a cyclic cover of the projective line over a finite field of characteristic p that runs in time $p^{1/2+o(1)}$. We confirm its practicality and effectiveness by reporting on the performance of our SageMath implementation on a range of examples. The algorithm relies on Gonçalves's generalization of Kedlaya's algorithm for cyclic covers, and Harvey's work on Kedlaya's algorithm for large characteristic.

1. Introduction

For $\mathcal{C}$ an algebraic curve of genus g over a finite field $\mathbb{F}_q$ of characteristic p and cardinality $q = p^n$, the zeta function of $\mathcal{C}$ is defined by

$$Z(\mathcal{C}, t) := \exp\left(\sum_{i=1}^{\infty} \#\mathcal{C}(\mathbb{F}_{q^i})\frac{t^i}{i}\right) = \frac{L(\mathcal{C}, t)}{(1-t)(1-qt)},$$

where $L(\mathcal{C}, t) \in 1 + t\mathbb{Z}[t]$ is a degree $2g$ polynomial, with reciprocal roots of complex absolute value $q^{1/2}$, and satisfies the functional equation $L(\mathcal{C}, t) = q^g t^{2g} L(\mathcal{C}, 1/(tq))$. In this paper, we address how to effectively compute $Z(\mathcal{C}, t)$ for a cyclic cover of $\mathbb{P}^1$ defined by $y^r = \overline{F}(x)$, where $\overline{F}(x)$ is squarefree and p is large in comparison to g, without any restrictions on r and $\deg \overline{F}$ sharing a common factor.

For curves of small genus, Schoof's method and its variants [Sch85, Pil90, GS04, GKS11, GS12] can compute $Z(\mathcal{C}, t)$ in time and space polynomial in $\log q$ and exponential in the genus. However, the practicality of these methods has only been shown for genus at most 2. These are known as ℓ-adic methods, as their efficiency derives from the realization of the ℓ-adic cohomology of the variety via torsion points.

Alternatively, Kedlaya [Ked01] showed that $Z(\mathcal{C}, t)$ can be determined in quasi-linear time in p for an odd hyperelliptic curve, i.e., $r = 2$ and $\deg \overline{F} = 2g + 1$, by computing an approximation of the Frobenius matrix acting on p-adic cohomology (Monsky–Washnitzer cohomology). Kedlaya's algorithm and its variants are known as p-adic methods. In [Har07], Harvey improved the time dependence in p to $p^{1/2+o(1)}$. In [Har14], this improvement plays a major role in Harvey's algorithm for computing the p-local zeta functions of an odd hyperelliptic curve over $\mathbb{Z}$ for all

The authors are grateful to the organizers of Sage Days 87, where this project began. We would also like to thank the reviewers for their many helpful comments. The second author was supported by the Simons Collaboration Grant #550023. The third author was partially supported by the Simons Collaboration Grant #550029. The fifth author was supported by the National Science Foundation Graduate Research Fellowship under Grant #1122374.

2010 *Mathematics Subject Classification*: 11G20 (primary) 11Y16, 11M38, 14G10 (secondary)

4 Jun 2018 20:49:04 PDT
Version 2 - Submitted to Open Book Series

p up to some bound. Kedlaya's original algorithm has been subsequently generalized several times, for example to superelliptic curves [GG01], $C_{a,b}$ curves [DV06], even degree hyperelliptic curves [Har12], and nondegenerate curves [CDV06]. More recently, Gonçalves [Gon15] extended Kedlaya's algorithm to cyclic covers of $\mathbb{P}^1$ and Tuitman [Tui16, Tui17] to general covers. All these generalizations kept the quasi-linear time dependence in p. Minzlaff [Min10] improved Gaudry–Gürel's algorithm for superelliptic curves by incorporating Harvey's work, giving a $p^{1/2+o(1)}$ time algorithm. The algorithms described above are efficient in practice, and have been integrated into the current versions of Magma [BCP97] and SageMath [Sag].

In this paper, we build upon Gonçalves, Harvey, and Minzlaff's work to obtain a practical $p^{1/2+o(1)}$ algorithm for cyclic covers of $\mathbb{P}^1$. Theoretically, we already knew of the existence of algorithms with such a time dependence on p (and their average polynomial time versions) for arbitrary schemes (see [Har15]). These algorithms for arbitrary schemes have never been implemented, and it is unclear if they can be made to work in practice. Our algorithm improves the dependence on other parameters over these very general algorithms and provides a step towards a practical average polynomial time in higher genus, analogous to the progression from $p^{1/2+o(1)}$ to average polynomial time for odd hyperelliptic curves by Harvey.

More recently, Tuitman [Tui18] combined Harvey's ideas with a deformation approach to give a $p^{1/2+o(1)}$ algorithm for computing zeta functions of generic projective hypersurfaces of higher dimension. Tuitman's algorithm has a similar theoretical dependence on the degree of the curve and the degree of the field (over $\mathbb{F}_p$) as our algorithm.

Throughout we will use a bit complexity model for computation and the notation $\widetilde{O}(x) = \bigcup_k O(x \log^k(x))$. Our main result is then as follows:

Theorem 1.1. *Let $\mathcal{C}$ be a cyclic cover of $\mathbb{P}^1$, of genus g, defined by*

$$\mathcal{C} : y^r = \overline{F}(x),$$

where $\overline{F} \in \mathbb{F}_q[x]$ is a squarefree polynomial of degree d. Let $\widetilde{\mathcal{C}}$ be the curve obtained from $\mathcal{C}$ by removing the δ points at infinity and the d points on the x-axis corresponding to the zeros of $\overline{F}(x)$. Let M_ϵ be the matrix of Frobenius acting on B_ϵ, where B_ϵ is a basis of the Monsky–Washnitzer cohomology of $\widetilde{C}$ defined in (2.6).

Let $N \geq 1$, and assume

$$p > d(N+\epsilon)r \text{ and } r+d \geq 5. \tag{1.2}$$

Then the entries of M are in $\mathbb{Z}_q$ and we may compute M modulo p^N in time

$$\widetilde{O}(p^{1/2}N^{5/2}d^\omega rn + N^4 r d^4 n \log p + N n^2 \log p)$$

and space

$$O((p^{1/2}N^{3/2} + rN^2)d^2 n \log p),$$

where ω is a real number such that the matrix arithmetic operations on matrices of size $m \times m$ take $\widetilde{O}(m^\omega)$ ring operations.

With the goal of computing $Z(\mathcal{C}, t)$ we may apply Theorem 1.1 with $N = O(nrd)$, for example as in (6.1), and this gives the following result:

Theorem 1.3. *In the same setup as Theorem 1.1, assume $p > dr(\frac{1}{2}gn + \log_p(g) + 2)$. We can compute the numerator of the zeta function of $\mathcal{C}$ in time*

$$\widetilde{O}(p^{1/2}n^{7/2}r^{7/2}d^{5/2+\omega} + n^5 r^5 d^8 \log p)$$

4 Jun 2018 20:49:04 PDT
Version 2 - Submitted to Open Book Series

and space $O((p^{1/2}+n^{1/2}r^{3/2}d^{1/2})n^{5/2}r^{3/2}d^{7/2}\log p)$.

We also provide the following $O(\log p)$ space alternative to Theorem 1.1; see Remark 5.3 for more details.

Theorem 1.4. *In the same setup as Theorem 1.1, we may we may compute* M *modulo* p^N *in time* $\widetilde{O}(prd^3N^3n+n^2N\log p)$ *time and space* $O(rd^2Nn\log p)$.

In comparison with Minzlaff's work, in all the theorems above we do not put any restrictions on r and $\deg(\overline{F})$ sharing a common factor. Theorem 1.4 reduces the space complexity of [Gon15, Proposition 5.1] from quasi-linear to logarithmic. Theorem 1.3 reduces both time and space complexity of [Gon15, Proposition 5.1] from quasi-linear in p to $p^{1/2+o(1)}$. Moreover, we provide a SageMath implementation of our algorithm for computing zeta functions [ACMT18].

As with all adaptations of Kedlaya's algorithm, the heart of our algorithm is a procedure for computing a p-adic approximation to the action of Frobenius on a well-chosen basis for (a slight modification of) the Monsky–Washnitzer cohomology of $\mathcal{C}$. This is described in Lemma 3.1.

The remainder of the paper is organized as follows. In Section 2, we recall the relevant definitions for Monsky–Washnitzer cohomology. In Section 3, we compute a 'sparse' formula for the action of Frobenius on the basis B_ϵ. The formula from Section 3 includes terms of large positive x-degree and large negative y-degree. Sections 4.1 and 4.2 show how to replace terms with cohomologous terms with x- and y-degree closer to zero by 'horizontal' and 'vertical' reductions. Section 5 collects the full algorithms, including complexity statements. We close by demonstrating the practicality of our implementation in Section 6.

2. Setup and notation

Let p be a prime and let $q=p^n$ for some $n\geq 1$. Let $\mathbb{F}_q$ and $\mathbb{F}_p$ be the finite fields with q elements and p elements. We write $\mathbb{Q}_q$ for the unramified extension of degree n of $\mathbb{Q}_p$, and $\mathbb{Z}_q$ for its ring of integers.

We will work under the assumption that (1.2) holds.

Let $\overline{F}(x)\in\mathbb{F}_q[x]$ be a polynomial of degree d with no multiple roots. To $\overline{F}(x)$ we can associate an r-cyclic cover of the projective line $\mathcal{C}$ defined by

$$\mathcal{C}\colon y^r=\overline{F}(x). \tag{2.1}$$

Write $\delta:=\gcd(r,d)$. Then the genus of $\mathcal{C}$ is $g=\frac{1}{2}((d-1)(r-1)-(\delta-1))$. The curve $\mathcal{C}$ is naturally equipped with an automorphism of order r defined by

$$\rho_r\colon (x,y)\longmapsto(x,\zeta_r y) \tag{2.2}$$

where ζ_r is a primitive r-th root of unity in a fixed algebraic closure of $\mathbb{F}_q$.

As in Kedlaya's original algorithm [Ked01] we pick an arbitrary lift $F(x)\in\mathbb{Z}_q[x]$ of $\overline{F}(x)$, also of degree d. Let $\widetilde{\mathcal{C}}$ be the curve obtained from $\mathcal{C}$ by removing the δ points at infinity and the d points on the x-axis corresponding to the zeros of $\overline{F}(x)$. Let $\overline{A}=\mathbb{F}_q[x,y,y^{-1}]/(y^r-\overline{F}(x))$ denote the coordinate ring of $\widetilde{\mathcal{C}}$, and write

$$A=\mathbb{Z}_q[x,y,y^{-1}]/(y^r-F(x)) \tag{2.3}$$

for the lift of $\overline{A}$ associated to $F(x)$. Let $A^\dagger$ be the weak completion of A, i.e.,

$$A^\dagger=\mathbb{Z}_q^\dagger[[x,y,y^{-1}]]/(y^r-F(x)), \tag{2.4}$$

where $\mathbb{Z}_q^\dagger[[x, y, y^{-1}]]$ is the ring of power series whose radius of convergence is greater than one. We lift the p-power Frobenius on $\mathbb{F}_q$ to $A^\dagger$ as follows. On $\mathbb{Z}_q$, we take the canonical Witt vector Frobenius and set $\sigma(x) := x^p$. We then extend σ to $A^\dagger$ by the formula

$$\sigma(y^{-j}) := y^{-jp} \sum_{k=0}^{+\infty} \binom{-j/r}{k} \big(\sigma(F(x)) - F(x)^p\big)^k y^{-kpr}. \tag{2.5}$$

The above series converges (because p divides $\sigma(F(x)) - F(x)^p$) and the definitions ensure that σ is a semilinear (with respect to the Witt vector Frobenius) endomorphism of $A^\dagger$. We extend it to differential forms by $\sigma(f\mathrm{d}g) := \sigma(f)\mathrm{d}(\sigma(g))$.

In the spirit of Kedlaya's algorithm, we determine the zeta function of $\mathcal{C}$ by computing the Frobenius action on subspace of $H^1_{\mathrm{MW}}(\widetilde{\mathcal{C}})$ spanned by the set

$$B_\epsilon = \left\{ x^i \frac{\mathrm{d}x}{y^{j+\epsilon r}} : \ i \in \{0, \dots, d-2\}, j \in \{1, \dots, r-1\} \right\}, \quad \text{where } \epsilon = \begin{cases} 0 & \text{if } \delta = 1 \\ 1 & \text{if } \delta > 1. \end{cases} \tag{2.6}$$

This subspace is Frobenius stable and 0 is the only element fixed by the induced automorphism ρ_r. When $\delta > 1$, using the basis B_1 allows us to avoid divisions by zero while reducing differentials (cf. Lemma 4.6). This is critical for generalizing Harvey's work to this setting.

If $\eta\colon \langle B_\epsilon \rangle \to H^1_{\mathrm{MW}}(\mathcal{C})$ is the projection map, then we have

$$\langle B_\epsilon \rangle = H^1_{\mathrm{MW}}(\mathcal{C}) \oplus \ker(\eta). \tag{2.7}$$

where $\ker(\eta)$ is a $\delta - 1$ dimensional vector space stable under Frobenius. Thanks to Gonçalves's work [Gon15, Proof of Theorem 7.5], we have an explicit description for the characteristic polynomial $U(t) := \det(t \cdot \mathrm{id} - \mathrm{Frob}_q \,|\, \ker(\eta))$ of Frobenius acting on $\ker(\eta)$:

$$U(t) := \det(t \cdot \mathrm{id} - \mathrm{Frob}_q \,|\, \ker(\eta)) = \det(t \cdot \mathrm{id} - P) \cdot (t-1)^{-1} \tag{2.8}$$

where the matrix P represents the permutation induced by q-th power Frobenius action on the roots of $T^\delta - f_d$, where f_d is the leading term of $\overline{F}(x)$. In the case that $\overline{F}(x)$ is monic the expression above simplies to $U(t) = \prod_{i|\delta, i>1} \big(t^{k_i} - 1\big)^{\frac{\varphi(i)}{k_i}}$, where k_i is the order of q in $\big(\mathbb{Z}/i\mathbb{Z}\big)^\times$. Thus our goal is to compute a p-adic approximation of the matrix M_ϵ representing σ with respect to B_ϵ.

3. The Frobenius action on differentials

We now rewrite the Frobenius expansion of a basis element in a sparse way where the number of terms does not depend on p. This is a generalization of [Har07, Proposition 4.1] and [Min10, Proposition 4.1], which is made possible due to the analysis performed by Gonçalves in [Gon15, §6].

Lemma 3.1. *Let $N > 0$ be a positive integer, $0 \le i \le d-2$ and $\epsilon r + 1 \le j \le (1+\epsilon)r - 1$. Suppose $p > d(N+\epsilon)r$ and $x^i y^{-j}\mathrm{d}x \in B_\epsilon$. For $0 \le \ell < N$, write*

$$D_{j,\ell} := \sum_{k=\ell}^{N-1} (-1)^{k-\ell} \binom{-j/r}{k} \binom{k}{\ell} \quad \text{and} \quad \mu_{j,\ell,b} := p D_{j,\ell} \sigma(F)^\ell_b, \tag{3.2}$$

where $\sigma(F)_b^\ell$ *is the coefficient of* x^{pb} *in* $\sigma(F(x))^\ell$*. The differentials* $\sigma(x^iy^{-j}\mathrm{d}x)$ *and*

$$T_{(i,j)} := x^{p(i+1)-1}y^{-jp}\sum_{\ell=0}^{N-1}\sum_{b=0}^{d\ell}\mu_{j,\ell,b}x^{pb}y^{-\ell pr}\mathrm{d}x \tag{3.3}$$

differ in cohomology by an element of $p^N \operatorname{span}_{\mathbb{Z}_q}(B_\epsilon)$.

Proof. From (2.5) we obtain

$$\sigma(x^iy^{-j}\mathrm{d}x) = \sum_{k=0}^{+\infty}\underbrace{px^{p(i+1)-1}\binom{-j/r}{k}\big(\sigma(F(x))-F(x)^p\big)^k y^{-p(j+kr)}\mathrm{d}x}_{=:U_k}. \tag{3.4}$$

We claim that for $k \geq N$ the reductions of U_k lie in $p^N \operatorname{span}_{\mathbb{Z}_q}(B_\epsilon)$.

To show this we start by rewriting U_k. Since p divides $\sigma(F(x))-F(x)^p$, we have

$$U_k = p^{k+1}H(x)y^{-p(j+kr)}\mathrm{d}x \tag{3.5}$$

where $H(x) \in \mathbb{Z}_q[x]$ of degree at most $pi+p-1+dkp < pd(k+1)$. Define

$$L = \begin{cases} p(k+1)-1 & \text{if } \epsilon = 0 \\ \left\lfloor \frac{p(j+kr)}{r} \right\rfloor - \epsilon & \text{if } \epsilon > 0. \end{cases} \tag{3.6}$$

Now we will expand $H(x)$ F-adically to L terms. Taking $j' \in [1,r]$ congruent to $pj \pmod r$, and applying the relation $F(x) = y^r$, we have

$$U_k = p^{k+1}\left(G(x)y^{-\epsilon r-j'} + \sum_{\ell=0}^{L}G_\ell(x)y^{r\ell-p(j+kr)}\right)\mathrm{d}x, \tag{3.7}$$

where each $G_\ell(x) \in \mathbb{Z}_q[x]$ has degree at most $d-1$ and $G(x)$ has degree at most

$$pd(k+1)-1-dL \leq \begin{cases} d-1 & \text{if } \epsilon = 0 \\ 0 & \text{if } \epsilon > 0. \end{cases} \tag{3.8}$$

Taking $\nu = \lfloor \log_p p(j+kr) - r\ell \rfloor \leq 1 + \lfloor \log_p(k+1+\epsilon)r \rfloor$, Gonçalves [Gon15, Proposition 6.1] shows that the reduction of $p^\nu G_\ell(x)y^{r\ell-p(j+kr)}\mathrm{d}x$ lies in $\operatorname{span}_{\mathbb{Z}_q}(B_\epsilon)$.

Similarly, [Gon15, Proposition 6.2] says that taking

$$\mu = \left\lfloor \log_p((r(\deg(G)+1)-(\epsilon r+j')d)/\delta) \right\rfloor \leq 1 + \lfloor \log_p(rd) \rfloor, \tag{3.9}$$

the reduction of $p^\mu G(x)y^{-\epsilon r-j'}\mathrm{d}x$ lies in $\operatorname{span}_{\mathbb{Z}_q}(B_\epsilon)$.

Since $p > d(N+\epsilon)r$, both $\mu = 1$ and $\nu \leq 1+k-N$, so the reductions of U_k for $k \geq N$ lie in $p^N \operatorname{span}_{\mathbb{Z}_q}(B_\epsilon)$.

The lemma follows by the rearranging the truncated series as follows:

$$\begin{aligned}\sum_{k=0}^{N-1}\binom{-j/r}{k}\big(\sigma(F(x))-y^{pr}\big)^k y^{-kpr} &= \sum_{k=0}^{N-1}\sum_{\ell=0}^{k}(-1)^{k-\ell}\binom{-j/r}{k}\binom{k}{\ell}\sigma\big(F(x)\big)^\ell y^{pr(k-\ell)}y^{-prk} \\ &= \sum_{\ell=0}^{N-1}\sum_{b=0}^{d\ell}D_{j,\ell}\sigma(F)_b^\ell x^{pb}y^{-\ell pr}.\end{aligned}$$

□

4. Reducing differentials

The powers of x and y appearing in $T_{(i,j)}$ (as in Lemma 3.1) are much larger than those appearing in our choice of representatives for the basis B_ϵ. We use relations (co-boundaries) coming from the differentials of functions on our curve to 'reduce' the terms from $T_{(i,j)}$ to linear combinations of elements of B_ϵ. We proceed in two-stages. Horizontal reduction reduces the x-degree while leaving the y-pole order constant. Vertical reduction decreases the y-pole order without increasing the x-degree. Given a differential ω, we call the unique cohomologous differential $\omega' \in \mathrm{span}(B_\epsilon)$ the *reduction of* ω. We may also abuse notation and call intermediate products of the vertical/horizonal reduction process *reductions* of ω.

Organizing our work carefully, we can compute the reduction of ω modulo p^N by performing intermediate steps modulo p^{N+1}.

4.1. **Horizontal reductions.** We follow the steps of Harvey and Minzlaff. Decompose $F(x)$ as $F(x) = f_d x^d + P(x)$, where $P(x)$ has degree at most $d-1$.

Definition 4.1. For $s \in \mathbb{Z}_{\geq -1}$ and $t \in \mathbb{Z}_{\geq 0}$ define the vector space

$$W_{s,t} = \{G(x)x^s y^{-t}\mathrm{d}x : \deg G \leq d-1\} \tag{4.2}$$

equipped with the standard monomial basis.

Let $M_H^t(s)\colon W_{s,t} \to W_{s-1,t}$ be the linear map given by the matrix

$$M_H^t(s) = \begin{pmatrix} 0 & 0 & \cdots & 0 & C_0^t(s) \\ D_H^t(s) & 0 & \cdots & 0 & C_1^t(s) \\ 0 & D_H^t(s) & \cdots & 0 & C_2^t(s) \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & D_H^t(s) & C_{d-1}^t(s) \end{pmatrix} \tag{4.3}$$

where $D_H^t(s) = (d(t-r) - rs)f_d$ and where $C_h^t(s)$ is the coefficient of x^h in the polynomial $C^t(x,s) = rsP(x) - (t-r)xP'(x)$. Moreover, for $s_0 < s_1$ we write

$$\begin{aligned} D_H^t(s_0, s_1) &:= D_H^t(s_0+1)D_H^t(s_0+2)\cdots D_H^t(s_1); \\ M_H^t(s_0, s_1) &:= M_H^t(s_0+1)M_H^t(s_0+2)\cdots M_H^t(s_1). \end{aligned} \tag{4.4}$$

Lemma 4.5. *For $s \in \mathbb{Z}_{\geq 0}$, $t \in \mathbb{Z}_{\geq 0}$, and $\omega \in W_{s,t}$, we have $D_H^t(s)\omega \sim M_H^t(s)\omega$ in cohomology.*

Proof. See [Har07, Proposition 5.4] or [Min10, Proposition 5.1]. The same algebraic manipulations hold in the cyclic cover setting, as long we do not divide by $D_H^t(s)$, as this might be zero. □

In the case that d and r share a common factor, i.e. $\delta > 1$ and $\epsilon = 1$, then $D_H^t(s)$ might be identically zero. The next lemma ensures this cannot happen due to our choice of basis B_ϵ.

Lemma 4.6. *We have $D_H^t(s) \neq 0$, while applying horizontal reductions to $T_{(i,j)}$, for $0 \leq i \leq d-2$ and $1 + \epsilon r \leq j \leq (1+\epsilon)r - 1$.*

Proof. By inspecting the Frobenius formula (3.3) for a fixed value of ℓ, (1) the pole order of y is $t = p(j + r\ell)$, where $1 + \epsilon r \leq j \leq (1+\epsilon)r - 1$ and (2) the largest power of x is at most $p(d\ell + i + 1) - 1 \leq pd(\ell+1) - 1$. Since the largest power of x in $W_{s,t}$ is $s + d - 1$, we need only consider the case $s + d - 1 \leq pd(\ell+1) - 1$.

If $\delta = 1$, then $\epsilon = 0$ and $d(t-r) - rs \equiv djp \not\equiv 0 \bmod r$.

If $\delta > 1$, then $\epsilon = 1$, so $j \geq 1+r$ and $t \geq p(1+r(\ell+1))$. Using $s+d < pd(\ell+1)$,

$$d(t-r) - rs = dt - r(s+d) \geq dp(1+r(\ell+1)) - r(pd(\ell+1)) = dp > 0. \quad \square \tag{4.7}$$

Corollary 4.8. *In the same setting as Lemma 4.6, $D_H^t(s) \equiv 0 \pmod p$ if and only if $s \equiv -d \mod p$.*

Proof. As in Lemma 4.6, the pole order of y is $t = p(j + r\ell)$, thus

$$D_H^t(s) := (d(t-r) - rs)f_d \equiv -r(d+s)f_d \pmod p. \tag{4.9}$$

By assumption, neither r nor f_d are divisible by p, so we only divide by p exactly when $s \equiv -d \mod p$. $\square$

Lemma 4.10. *Suppose $p > d(N+\epsilon)r$ and $s \equiv -1 \pmod p$. Then $D_H^t(s-(d-1))$ is divisible by p, but it is not divisible by p^2.*

Proof. As $s-(d-1) \equiv -d \mod p$, we know this denominator is divisible by p. It equals $f_d(d(t-r) - r(s-(d-1))) = f_d(dt - rs - r)$. Since f_d is coprime to p, we analyze the piece $dt - r(s+1)$. Inspecting the Frobenius formula (3.3) and considering that horizontal reduction decreases the exponent of x, we see

$$\begin{aligned} p-1 \leq s \leq p(i+1) - 1 + pd(N-1) \qquad & 0 \leq i \leq d-2 \\ 0 \leq t \leq jp + (N-1)pr \qquad & \epsilon r + 1 \leq j \leq (1+\epsilon)r - 1 \end{aligned} \tag{4.11}$$

where $\epsilon \in \{0,1\}$. From these inequalities we obtain

$$|dt - r(s+1)| \leq \max\{dt, r(s+1)\} < dp(N+\epsilon)r < p^2, \tag{4.12}$$

thus the denominator has p-valuation exactly 1. $\square$

Now we describe the horizontal reduction procedure in a fashion similar to that in Harvey's [Har07, §7.2]. Following the notation of (3.3), let v_ℓ be a vector representing a differential form in $W_{p\ell-1,t}$ that is cohomologous to

$$\sum_{b \geq \ell}^{dk} \mu_{j,k,b-i-1} x^{pb-1} y^{-t} \mathrm{d}x, \quad \text{where } t = p(kr+j). \tag{4.13}$$

As in Harvey [Har07, §7.2], we say a vector is *1-correct* if the first coordinate (corresponding to the highest power of x) is both 0 modulo p and correct modulo p^{N+1}, and the other coordinates are correct modulo p^N.

Given v_ℓ which is 1-correct, we show how to compute $v_{\ell-1}$ which is also 1-correct. First we get down to $W_{\ell p-d-1,t}$, by doing the first d reductions modulo p^{N+1}, as follows:

$$\begin{aligned} v_\ell^{(1)} &= v_\ell & &\in W_{\ell p-1,t} \\ v_\ell^{(2)} &= D_H^t(\ell p-1)^{-1} M_H^t(\ell p-1) v_\ell^{(1)} & &\in W_{\ell p-2,t} \\ &\vdots & &\vdots \\ v_\ell^{(d+1)} &= D_H^t(\ell p-d)^{-1} M_H^t(\ell p-d) v_\ell^{(d)} & &\in W_{\ell p-d-1,t}. \end{aligned} \tag{4.14}$$

Then we get down to $W_{(\ell-1)p,t}$ via

$$v'_\ell = D_H^t((\ell-1)p, \ell p-d-1)^{-1} M_H^t((\ell-1)p, \ell p-d-1) v_\ell^{(d+1)}, \tag{4.15}$$

and then finally

$$v_{\ell-1} = \mu_{j,\ell,(\ell-1)-i-1} x^{p(\ell-1)-1} y^{-t} \mathrm{d}x + D_H^t((\ell-1)p)^{-1} M_H^t((\ell-1)p) v'_\ell. \tag{4.16}$$

An analysis similar to Harvey's [Har07, §7.2.2] shows that all coefficients of $M_H^t(\ell p - d)v_\ell^{(d)}$ are divisible by p and correct modulo p^{N+1}. Then, Lemma 4.10 implies that $v_\ell^{(d+1)}$ is correct modulo p^N. By Corollary 4.8, v'_ℓ is correct modulo p^N. Since the first row of $M_H^t((\ell-1)p)$ is zero modulo p, the vector $v_{\ell-1}$ is 1-correct.

Furthermore, we may also speed up the evaluation of $M_H^t((\ell-1)p, \ell p - d - 1)$ and $D_H^t((\ell-1)p, \ell p - d - 1)$ by p-adically interpolating the remaining values from the first N values. See [Har07, §7.2.1] and Section 5 for more details.

4.2. **Vertical reductions.** Vertical reduction replaces differentials with cohomologous differentials with smaller pole order in y. While we performed horizontal reductions by working with d-dimensional vector spaces of differential forms, vertical reductions arise most naturally on $(d-1)$-dimensional vector spaces.

Definition 4.17. For $t \in \mathbb{Z}_{\geq 0}$ and $j \in \{1, \dots, r-1\}$, define the vector space

$$V_t^j := W_{-1,rt+j} \cap W_{0,rt+j}, \tag{4.18}$$

equipped with the standard monomial basis.

Vertical reduction operates via a series of maps $V_t^j \to V_{t-1}^j$ which are identity maps in cohomology. To define the maps, we need a lemma.

Lemma 4.19. *Let $A \in \mathbb{Z}_q[x]$ be a polynomial with $\deg(A) < 2d-1$. Then, there exist unique polynomials $R, S \in \mathbb{Z}_q[x]$ such that $\deg(R) < d-1, \deg(S) < d$, and $A(x) = R(x)F(x) + S(x)F'(X)$.*

Proof. Since F is separable and $\overline{F}$ is squarefree, we can find R_0 and S_0 such that $1 = R_0F + S_0F'$ by the Euclidean algorithm. Then $A = (AR_0)F + (AS_0)F'$. There is a unique S and T satisfying $AS_0 = TF + S$ and $\deg(S) < d$. Set $R = AR_0 - TF'$. Since $\deg(A) < 2d-1$ and $\deg(SF') < 2d-1$, it follows that $\deg(RF) < 2d-1$, so $\deg(R) < d-1$.

Uniqueness follows immediately, since the vector spaces of polynomials of degree less than $2d-1$ and of pairs of polynomials of degrees less than $d-1$ and less than d both have dimension $2d-1$. □

We may now define the vertical reduction maps.

Definition 4.20. For each $i \in \{0, \dots, d-2\}$, let $R_i, S_i \in \mathbb{Z}_q[x]$ be the unique polynomials of $\deg(R_i) < d-1, \deg(S_i) < d$ such that

$$x^i = R_i(x)F(x) + S_i(x)F'(x). \tag{4.21}$$

Write $(rt - r + j)R_i(x) + rS_i'(x) = \gamma_{i,0} + \gamma_{i,1}x + \cdots + \gamma_{i,d-2}x^{d-2}$. Define $M_V^j(t)$ and $D_V^j(t)$ by

$$M_V^j(t) := \begin{pmatrix} \gamma_{0,0} & \gamma_{1,0} & \cdots & \gamma_{d-2,0} \\ \gamma_{0,1} & \gamma_{1,1} & \cdots & \gamma_{d-2,1} \\ \vdots & & \ddots & \vdots \\ \gamma_{0,d-2} & \gamma_{1,d-2} & \cdots & \gamma_{d-2,d-2} \end{pmatrix}, \tag{4.22}$$

$$D_V^j(t) := rt - r + j.$$

Further define

$$\begin{aligned} M_V^j(t_1, t_2) &:= M_V^j(t_1+1) \cdot M_V^j(t_1+2) \cdots M_V^j(t_2), \\ D_V^j(t_1, t_2) &:= D_V^j(t_1+1) \cdot D_V^j(t_1+2) \cdots D_V^j(t_2). \end{aligned} \tag{4.23}$$

Lemma 4.24. *Consider $M_V^j(t)$ as a linear map from V_t^j to V_{t-1}^j with respect to their standard bases. Then, for any $\omega \in V_t^j$,*

$$D_V^j(t)\omega \sim M_V^j(t)\omega \tag{4.25}$$

in cohomology. More generally, considering $M_V^j(t_1,t_2)$ as a linear map from $V_{t_2}^j$ to $V_{t_1}^j$ with respect to their standard bases, for any $\omega \in V_{t_2}^j$,

$$D_V^j(t_1,t_2)\omega \sim M_V^j(t_1,t_2)\omega. \tag{4.26}$$

Proof. For any $S(x) \in \mathbb{Q}_q[x]$,

$$\begin{aligned} 0 &\sim \mathrm{d}\left(\frac{-r}{rt-r+j}S(x)y^{-(rt-r+j)}\right) \\ &= S(x)F'(x)y^{-(rt+j)}\mathrm{d}x + \frac{-r}{rt-r+j}S'(x)y^{-(rt-r+j)}\mathrm{d}x. \end{aligned} \tag{4.27}$$

So, writing $x^i = R_i(x)F(x) + S_i(x)F'(x)$ as in (4.21), we have

$$\begin{aligned} x^i y^{-(rt+j)}\mathrm{d}x &= R_i(x)F(x)y^{-(rt+j)}\mathrm{d}x + S_i(x)F'(x)y^{-(rt+j)}\mathrm{d}x \\ &\sim R_i(x)y^{-(rt-r+j)}\mathrm{d}x + \frac{r}{rt-r+j}S_i'(x)y^{-(rt-r+j)}\mathrm{d}x \\ &= \frac{(r(t-1)+j)R_i(x) + rS_i'(x)}{r(t-1)+j}y^{-(r(t-1)+j)}\mathrm{d}x \\ &= (D_V^j(t_1,t_2))^{-1}\left(\gamma_{i,0} + \gamma_{i,1}x + \cdots + \gamma_{i,d-2}x^{d-2}\right)y^{-(r(t-1)+j)}\mathrm{d}x. \end{aligned}$$

From this, (4.25) follows by linearity. Then (4.26) is immediate from (4.25). □

Remark 4.28. If we could work at infinite (or even very large) precision without it costing us computation time, this would be sufficient. However, in practice (and in theory), working with fewer extra bits results in significant time savings. Fortunately, we will see that when p is sufficiently large, the valuations of the coefficients of $D_V^j(t_1,t_2)^{-1}M_V^j(t_1,t_2)$ are never less than -1. As a result, given any element of V_t^j, we will be able to compute a cohomologous element of V_0^j while only losing a single digit of p-adic absolute precision.

Now, we follow Harvey's lead and study the coefficients of the matrices $M_V^j(t_1,t_2)$ and scalars $D_V^j(t_1,t_2)$. Lemma 4.29 will be our main technical tool.

Lemma 4.29. *Suppose $A \in \mathbb{Z}_q[x]$ and $B, G_{-t_2+1}, \ldots, G_{-t_1} \in \mathbb{Q}_q[x]$ satisfy*

$$A(x)y^{-rt_2-j}\mathrm{d}x = B(x)y^{-rt_1-j}\mathrm{d}x + \mathrm{d}\left(\sum_{t=-t_2+1}^{-t_1} G_t(x)y^{rt-j}\right). \tag{4.30}$$

Fix $C \in \mathbb{Z}_q$. If $\dfrac{C}{rt_1+j}, \dfrac{C}{r(t_1+1)+j}, \ldots, \dfrac{C}{r(t_2-1)+j} \in \mathbb{Z}_q$ then $C \cdot B(x) \in \mathbb{Z}_q[x]$.

Remark 4.31. In our setting, $rt_1+j \le rt_2+j < p^2$, so we may take $C = p$. Applying Lemma 4.29 with $A(x) = 1, x, \ldots, x^{d-1}$, the coefficients of $pD_V^j(t_1,t_2)^{-1}M_V^j(t_1,t_2)$ all belong to $\mathbb{Z}_q$.

We defer the proof of Lemma 4.29 to the end of the section, and collect the consequences needed for our main algorithm.

Lemma 4.32. *If $r(t-1) \equiv -j \pmod{p}$, then $M_V^j(t)^{-1}$ is integral.*

The proof is identical to the proof of Harvey's [Har07, Lemma 7.7] after replacing each occurrence of $2g$ with $d-1$. Indeed, the matrices are the same, up to multiplication by a unit.

Lemma 4.33. *If $rt_1 \equiv -j \mod p$, then $M_V^j(t_1, t_1+p)$ is zero modulo p.*

Proof. Here, the proof generalizes [Har07, Lemma 7.9]. By Lemma 4.29,

$$X := pD_V^j(t_1, t_1+p+1)^{-1} M_V^j(t_1, t_1+p+1) \tag{4.34}$$

has integral coefficients. By a computation similar to Lemma 4.10, $D_V^j(t_1, t_1+p+1) = p^2 \cdot u$ for some unit $u \in \mathbb{Z}_q^\times$, since the first and last terms contribute exactly one power of p and no other terms contribute. Then,

$$M_V^j(t_1, t_1+p) = p^{-1} D_V^j(t_1, t_1+p+1) X M_V^j(t_1+p+1)^{-1} = puXM_V^j(t_1+p+1)^{-1}.$$

Lemma 4.32 implies $M_V^j(t_1+p+1)^{-1}$ is integral, so $M_V^j(t_1, t_1+p) \equiv 0 \mod p$. □

Lemma 4.33 implies that the matrix $Y := D_V^j(t_1, t_1+p)^{-1} M_V^j(t_1, t_1+p)$ is integral when $rt_1 \equiv -j \mod p$. Hence the denominators of "vertically reductions" of differentials do not grow, at least if we reduce in appropriate batches of p steps.

Unfortunately, we may not start with t_1 satisfying $rt_1 \equiv -j \mod p$. Reducing to this case involves dividing by p at most once. To compensate, we must compute Y to one extra digit of p-adic precision.

Having collected our results, we now prove Lemma 4.29. Much like Kedlaya's proof of [Ked01, Lemma 2], we compare power series expansions of differentials in the uniformizer y near $(\theta_i, 0)$ for all roots θ_i of F. We give a full proof for clarity. The argument relies heavily on the following lemma:

Lemma 4.35. *Let $G \in \mathbb{Q}_q[x]$ be a polynomial with $\deg(G) < d$. View G as an element of $\mathbb{Q}_q[x,y]/(y^r - F(x))$. Let $\theta_1, \dots, \theta_d$ be the roots of F. Let $K_i \cong \mathbb{Q}_q(\!(y)\!)$ be the fraction field of the completion of the local ring at $(\theta_i, 0)$. The following are equivalent:*

(i) G has integral coefficients as a polynomial.
(ii) G has integral coefficients as a power series in K_i for all i.
(iii) The coefficient of y^0 of G as a power series in K_i is integral for all i.

Proof. It is trivial that (ii) implies (iii).
"(iii) implies (i)" follows immediately from the observation that the coefficient of y^0 of G as a power series in K_i is equal to $G(\theta_i)$. Since $\deg(G) < d$ and the roots of F are distinct mod p, the Lagrange interpolation formula shows that $G \in \mathbb{Z}_q[x]$.
"(i) implies (ii)" follows immediately from the fact that F has distinct roots mod p, so expanding x as a power series in y in K_i never requires division by a non-unit. □

With Lemma 4.35, the proof of Lemma 4.29 follows from the observation that the map d commutes with passage to the local ring.

Proof of Lemma 4.29. Note that for all roots θ_i of F, $F'(\theta_i) \in \mathbb{Z}_q^\times$, since $\overline{F}$ is separable. Then, as power series in y (near $(\theta_i, 0)$),

$$A(x)y^{r(-t_2)-j}\mathrm{d}x = rA(x)y^{r(-t_2+1)-j-1}F'(x)^{-1}\mathrm{d}y = \sum_{t=-t_2+1}^{\infty} a_{i,t}y^{rt-j-1}\mathrm{d}y,$$

$$B(x)y^{r(-t_1)-j}\mathrm{d}x = \sum_{t=-t_1+1}^{\infty} b_{i,t}y^{rt-j-1}\mathrm{d}y,$$

where the $a_{i,t}$ are integral by Lemma 4.35, but we have no bounds (yet) on the $b_{i,t}$. Then,

$$\mathrm{d}\left(\sum_{t=-t_2+1}^{-t_1} G_t(x)y^{rt-j}\right) = \sum_{t=-t_2+1}^{-t_1} a_{i,t}y^{rt-j-1}\mathrm{d}y + \sum_{t=-t_1+1}^{\infty}(a_{i,t}-b_{i,t})y^{rt-j-1}\mathrm{d}y.$$

Integrating term by term,

$$\sum_{t=-t_2+1}^{-t_1} G_t(x)y^{rt-j} = \sum_{t=-t_2+1}^{-t_1} \frac{a_{i,t}}{rt-j}y^{rt-j} + \sum_{t=-t_1+1}^{\infty} \frac{a_{i,t}-b_{i,t}}{rt-j}y^{rt-j}, \tag{4.36}$$

In particular, if C satisfies $\frac{C}{r\cdot t+r-j} \in \mathbb{Z}_q$, for all $t \in \{-t_2, \dots, -t_1-1\}$, then the coefficients of $y^{r(-t_2+1)-j}, y^{r(-t_2+2)-j}, \dots, y^{r(-t_1-1)-j}, y^{r(-t_1)-j}$ in all of the power series expansions at points $(\theta_i, 0)$ of $\sum_{t=-t_2+1}^{-t_1} C \cdot G_t(x)y^{rt-j}$ are integral.

In particular, $C \cdot G_{-t_2+1}$ satisfies (iii) of Lemma 4.35. Then the series expansions of $C \cdot G_{-t_2+1}(x)$ are all integral by condition (ii). Subtracting off $C \cdot G_{-t_2+1}$, we see $C \cdot G_{-t_2+2}$ satisfies (iii) of Lemma 4.35, hence condition (ii) and so on, so that all of the coefficients in all of the expansions of $\sum_{t=-t_2+1}^{-t_1} G_t(x)y^{rt-j}$ are integral. They remain integral upon differentiating.

Rearranging (4.30), the expansions of $C \cdot B(x)y^{-rt_1+j}\mathrm{d}x$ at each $(\theta_i, 0)$ as Laurent series in $\mathbb{Q}_q(\!(y)\!)\mathrm{d}y$ are integral. Replacing $\mathrm{d}y$ with $F'(x)y^{1-r}/r\mathrm{d}x$ preserves integrality. A final application of Lemma 4.35 shows that $C \cdot B(x)$ is integral. □

5. Main algorithm

We now combine the techniques of the previous sections to compute the matrix representing the p-th power Frobenius action with respect to $\langle B_\epsilon \rangle \subset H^1_{\mathrm{MW}}(\widetilde{\mathcal{C}})$ modulo p^N. We summarize the procedure in Algorithm 1, where we take all intervals to be discrete, i.e., intersected with $\mathbb{Z}$.

We now analyze the time and space complexity of Algorithm 1. First, we recall that all our underlying ring operations are done in $\mathbb{Z}_q/p^N$ or $\mathbb{Z}_q/p^{N+1}$. Using bit-strings of length $O(Nn\log p)$ to represent elements of these rings, the basic ring operations (addition, multiplication, and inversion) have bit complexity $\widetilde{O}(Nn\log p)$, the matrix arithmetic operations on matrices of size $m \times m$ have bit complexity $\widetilde{O}(m^\omega Nn\log p)$, and polynomial multiplication of polynomials of degree m has bit complexity $\widetilde{O}(mNn\log p)$. Applying Frobenius to such an element has complexity $\widetilde{O}(n\log^2 p + nN\log p)$ [Hub10, Corollary 3].

For p sufficiently large, the dominant steps are the horizontal and vertical reductions, i.e. lines 7 and 23 in Algorithm 1. In either case, we apply a modification of [BGS07, Theorem 15] to achieve the $p^{1/2+o(1)}$ time dependence.

Proposition 5.1 (Linear recurrences method, [Har07, Theorem 6.1])**.** *Let $R = \mathbb{Z}_q/p^N$ or $\mathbb{Z}_q/p^{N+1}$, and $M(x) := M_0 + xM_1 \in R[x]^{m\times m}$. Let $0 \le \alpha_1 < \beta_1 \le \alpha_2 < \beta_2 \le \cdots \le \alpha_h < \beta_h \le K$ be integers. Assume $h < \sqrt{K} < p-1$ and write $M(\alpha,\beta) := M(\alpha+1)\cdots M(\beta)$. Then $M(\alpha_i,\beta_i)$ for $i = 1,\dots,h$ can be computed using $\widetilde{O}(m^\omega\sqrt{K})$ ring operations in space $O(m^2\sqrt{K})$.*

For the horizontal reductions, we apply Proposition 5.1 once for each pair $(k,j) \in [0, N-1]\times[1+\epsilon r, (1+\epsilon)r-1]$ with $K = O(pN)$ and $m = O(d)$. For the vertical reductions, we apply Proposition 5.1 once for each j, again with $K = O(pN)$ and $m = O(d)$. This adds up to $\widetilde{O}(p^{1/2}N^{3/2}rd^\omega)$ ring operations in space $O(p^{1/2}N^{1/2}d^2)$.

for $k \in [0, N-1]$, $i \in [0, d-2]$, $j \in [1+\epsilon r, (1+\epsilon)r - 1]$, $\ell \in [0, dk+i+1]$ **do**
  $T_{(i,j),k,\ell} \leftarrow \mu_{j,k,\ell-i-1} x^{p\ell-1} y^{-p(kr+j)}$; // See Lemma 3.1
// Horizontal reductions
for $k \in [0, N-1]$, $j \in [1+\epsilon r, (1+\epsilon)r - 1]$ **do**
  $t \leftarrow p(kr+j)$
  $L \leftarrow \min(N-1, dk+d-2)$
  // Horizontal reductions modulo p^N, by linear recurrences
  for $\ell \in [0, L]$ **do**
    $D(\ell), M(\ell) \leftarrow D_H(p\ell, p(\ell+1)-d-1), M_H(p\ell, p(\ell+1)-d-1)$;
  // Deduce the remaining $M(\ell)$ modulo p^N, by interpolation
  for $\ell \in [L+1, dk+d-2]$ **do**
    $D(\ell), M(\ell) \leftarrow D_H(p\ell, p(\ell+1)-d-1), M_H(p\ell, p(\ell+1)-d-1)$
  // Reduce $T_{(i,j),k}$ horizontally
  for $i \in [0, d-2]$ **do**
    $v \leftarrow T_{(i,j),k,dk+i+1}$; // $v \in W_{p(dk+i+1)-1,t}$
    for $\ell = dk+i$ **to** 0 **do**
      for $e \in [1, d]$ **do** // $W_{p(\ell+1)-1,t} \to W_{p\ell-1,t}$
        $v \leftarrow D_H^t(p(\ell+1)-e)^{-1} \left(M_H^t(p(\ell+1)-e) \cdot v\right)$;
      $v \leftarrow T_{(i,j),k,l} + \left(D_H^t(p\ell)^{-1} M_H^t(p\ell)\right) \cdot \left(D(\ell)^{-1} M(\ell)\right) \cdot v$
    $w_{(i,j),k} \leftarrow v$; // $w_{(i,j),k} \in W_{-1,t}$
// Vertical reductions
for $j \in [1+\epsilon r, (1+\epsilon)r - 1]$ **do**
  // $p(kr+j) = r(pk+\alpha) + \beta = pr(k+\lambda) + r\gamma + r\epsilon + \beta$
  $\alpha, \beta \leftarrow \lfloor pj/r \rfloor, pj \bmod r$
  $\lambda, \gamma \leftarrow \lfloor (\alpha - \epsilon)/p \rfloor, (\alpha - \epsilon) \bmod r$
  $\delta \leftarrow \gamma + \epsilon$
  // Vertical reductions modulo p^{N+1}, by linear recurrences
  $M(0) \leftarrow D_V^\beta(\epsilon, \delta)^{-1} M_V^\beta(\epsilon, \delta)$
  for $\ell \in [1, \lambda + N - 1]$ **do**
    $M(\ell) \leftarrow D_V^\beta(\delta + p(\ell-1), \delta + p\ell)^{-1} M_V^\beta(\delta + p(\ell-1), \delta + p\ell)$;
  for $i \in [0, d-2]$ **do**
    $v \leftarrow w_{(i,j),N-1+\lambda}$ // $v \in V^\beta_{p(N-1+\lambda)+\delta}$
    for $k = N-1+\lambda$ **to** 1 **do** // $V^\beta_{pk+\delta} \to V^\beta_{p(k-1)+\delta}$
      if $k \geq \lambda$ **then**
        $v \leftarrow w_{(i,j),k-\lambda} + M(k)v$
      else
        $v \leftarrow M(k)v$
    $w_{(i,j)} \leftarrow M(0) \cdot v$;
return $w_{(i,j)}$, $i \in [0, d-2]$, $j \in [1+\epsilon r, (1+\epsilon)r - 1]$

Algorithm 1: Computes the matrix representing the p-th power Frobenius action with respect to $\langle B_\epsilon \rangle \subset H^1_{\mathrm{MW}}(\widetilde{\mathcal{C}})$ modulo p^N

Now we bound the time for the remaining steps. We will see that the number of ring operations for the remaining steps is independent of p, so that they contribute at most a $\log p$ term to the bit complexity.

To compute $\mu_{j,\ell,b}$ we start by replacing the coefficients of $F(x)$ by their images under σ. We then calculate all $\sigma(F)_b^\ell$ in $O(d^2N^2)$ ring operations. Evaluating all the binomial coefficients and finding the $D_{j,\ell}$ uses $O(rN^2)$ ring operations. In total, we compute all the $\mu_{j,\ell,b}$ in $O(rd^2N^2)$ ring operations plus $O(d)$ Frobenius substitutions.

We also use the p-adic interpolation method introduced by Harvey [Har07, §7.2.1] and attributed to Kedlaya. This allows us to reduce the number of matrix products that must be computed using the linear recurrence algorithm. The rest can then be obtained by solving a linear system involving a Vandermonde matrix. In our setting, an analogous complexity analysis holds, and the total number of ring operations required is $O(rd^3N^3)$, where the extra r factor is due to the j loop.

The matrix $M_H^t(s)$ is sparse; for each t, it requires $O(d)$ ring operations to compute. We need to do this $O(rN)$ times, thus the total is $O(rdN)$.

During the horizontal reduction, we do the following for each ℓ: $O(d)$ sparse vector-matrix multiplications, and one dense vector-matrix multiplication. This requires $O(d^2)$ ring operations per ℓ. Hence, lines 10-15 add up to $O(rd^4N^2)$ ring operations. The number of vector-matrix multiplications during the vertical reduction is $O(dN)$, thus negligible in comparison with the horizontal phase.

Computing all the R_i and S_i requires $O(d^3)$ total ring operations. Then for each $j \in [r\epsilon + 1, (1+\epsilon)r - 1]$, the matrix $M_V^j(t)$ can be computed in $O(d^2)$ ring operations. The total number of ring operations for these steps is $O(rd^2 + d^3)$.

The total number of operations is $O(p^{1/2}N^{3/2}rd^\omega + rd^4N^3)$ plus $O(d)$ Frobenius substitutions. Converting this to bit complexity, our algorithm runs in time

$$\widetilde{O}(p^{1/2}N^{5/2}rd^\omega n + N^4rd^4n\log p + Ndn^2\log p). \tag{5.2}$$

In addition to the space required by Proposition 5.1, we use $O(rd^2N)$ space for the interpolation, to store $w_{(i,j),k}$ and to do the vector-matrix multiplications. This adds up to $O((p^{1/2}N^{3/2} + rN^2)d^2n\log p)$ space, and Theorem 1.1 follows.

Remark 5.3. Under certain conditions, the time-space trade-off provided by Proposition 5.1 might not be ideal or possible. In those cases, one can instead do the reductions one step at a time with naive vector-matrix multiplications. The horizontal phase amounts to $O(prd^2N^2)$ sparse matrix-vector multiplications of size $O(d)$ in space $O(rd^2N)$. The vertical phase amounts to $O(prdN)$ dense matrix-vector multiplications of the same size, and no extra space is required. With the single exception of the $O(d)$ Frobenius substitutions, all the other steps are negligible in comparison. In terms of bit complexity, this amounts to $\widetilde{O}(prd^3N^3n + n^2N\log p)$ time and $O(rd^2Nn\log p)$ space, and Theorem 1.4 follows.

6. Sample Computations

We have implemented both versions of our method using SageMath. However, the $p^{1/2+o(1)}$ version, i.e., Theorem 1.3 and Algorithm 1, is only implemented for the case $n = 1$, as we rely on Harvey's implementation of Proposition 5.1 in C++. Our implementation is on track to be integrated in one of the upcoming versions SageMath [ACMT18]. An example session:

```
sage: x = PolynomialRing(GF(10007),"x").gen();
sage: CyclicCover(5, x^5 + 1).frobenius_polynomial()
x^12 + 300420147*x^8 + 30084088241167203*x^4 + 10042073568636025085376 49
```

Our examples were computed on one core of a desktop machine with an `Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz`. In all the examples, we took

$$N = \max\{\lceil \log_p(4g/i) + ni/2 \rceil : i = 1, \dots, g\}, \tag{6.1}$$

and thus by employing Newton identities we can pinpoint the numerator of $Z(\mathcal{C}, t)$; see, for example, [Ked13, sl. 8]. In practice, we may even work with lower N, and then hopefully verify that there is only one possible lift that satisfies the Riemann hypothesis and the functional equation in the Weil conjectures; see [Ked08].

In Table 1 we present the running times for computing $Z(\mathcal{C}, t)$ for three examples where $(g, d, r) = (6, 5, 5), (25, 6, 12)$, and $(45, 11, 11)$, over a range of p values. This sample of running times confirms the practicality and effectiveness of our method for a wide range of p and tuples (d, r). We are not aware of any other alternative method that can handle p and g in these ranges.

p	time	p	time	p	time
$2^{14} - 3$	1.21s	$2^{22} - 3$	21.7s	$2^{30} - 35$	5m58s
$2^{16} - 15$	3.05s	$2^{24} - 3$	40.9s	$2^{32} - 5$	11m36s
$2^{18} - 5$	5.74s	$2^{26} - 5$	1m23s	$2^{34} - 41$	32m59s
$2^{20} - 3$	10.9s	$2^{28} - 57$	2m54s	$2^{36} - 5$	1h7m

(A) Genus 6 curve $\mathcal{C}\colon y^5 = x^5 - x^4 + x^3 - 2x^2 + 2x + 1$ with $N = 4$

p	time	p	time	p	time
$2^{10} + 45$	4m37s	$2^{18} - 5$	12m2s	$2^{26} - 5$	2h38m
$2^{12} - 3$	5m31s	$2^{20} - 3$	21m34s	$2^{28} - 57$	5h24m
$2^{14} - 3$	6m20s	$2^{22} - 3$	37m21s	$2^{30} - 35$	12h12m
$2^{16} - 15$	8m15s	$2^{24} - 3$	1h13m	$2^{32} - 5$	23h35m

(B) Genus 25 curve $\mathcal{C}\colon y^6 = x^{12} + 10x^{11} + x^{10} + 2x^9 - x^7 - x^5 - 4x^4 + 31x$ with $N = 13$

p	time	p	time	p	time
$2^{12} - 3$	24m1s	$2^{18} - 5$	1h2m	$2^{24} - 3$	7h21m
$2^{14} - 3$	29m50s	$2^{20} - 3$	1h52m	$2^{26} - 5$	16h24m
$2^{16} - 15$	37m14s	$2^{22} - 3$	3h22m	$2^{28} - 57$	33h17m

(C) Genus 45, $\mathcal{C}\colon y^{11} = x^{11} + 21x^9 + 22x^8 + 12x^7 + 5x^4 + 15x^3 + 6x^2 + 99x + 11$ with $N = 23$

TABLE 1. Running times for three curves, for various p. Each subsequent row represents a (roughly) four-fold increase in p and a doubling in the running time, confirming that our implementation has a $p^{1/2+o(1)}$ running time.

REFERENCES

[ACMT18] Vishal Arul, Edgar Costa, Richard Magner, and Nicholas Triantafillou. Hasse–Weil zeta function of a cyclic covers of $\mathbb{P}^1$ over finite fields. https://trac.sagemath.org/ticket/20264, 2018.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BGS07] Alin Bostan, Pierrick Gaudry, and Éric Schost. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. *SIAM J. Comput.*, 36(6):1777–1806, 2007.

[CDV06] W. Castryck, J. Denef, and F. Vercauteren. Computing zeta functions of nondegenerate curves. *IMRP Int. Math. Res. Pap.*, pages Art. ID 72017, 57, 2006.

[DV06] Jan Denef and Frederik Vercauteren. Counting points on C_{ab} curves using Monsky-Washnitzer cohomology. *Finite Fields Appl.*, 12(1):78–102, 2006.

[GG01] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya's point-counting algorithm to superelliptic curves. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.

[GKS11] Pierrick Gaudry, David Kohel, and Benjamin Smith. Counting points on genus 2 curves with real multiplication. In *Advances in cryptology—ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Comput. Sci.*, pages 504–519. Springer, Heidelberg, 2011.

[Gon15] Cécile Gonçalves. A point counting algorithm for cyclic covers of the projective line. In *Algorithmic arithmetic, geometry, and coding theory*, volume 637 of *Contemp. Math.*, pages 145–172. Amer. Math. Soc., Providence, RI, 2015.

[GS04] Pierrick Gaudry and Éric Schost. Construction of secure random curves of genus 2 over prime fields. In *Advances in cryptology—EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Comput. Sci.*, pages 239–256. Springer, Berlin, 2004.

[GS12] Pierrick Gaudry and Éric Schost. Genus 2 point counting over prime fields. *J. Symbolic Comput.*, 47(4):368–400, 2012.

[Har07] David Harvey. Kedlaya's algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.

[Har12] Michael C. Harrison. An extension of Kedlaya's algorithm for hyperelliptic curves. *J. Symbolic Comput.*, 47(1):89–101, 2012.

[Har14] David Harvey. Counting points on hyperelliptic curves in average polynomial time. *Ann. of Math. (2)*, 179(2):783–803, 2014.

[Har15] David Harvey. Computing zeta functions of arithmetic schemes. *Proc. Lond. Math. Soc. (3)*, 111(6):1379–1401, 2015.

[Hub10] Hendrik Hubrechts. Fast arithmetic in unramified p-adic fields. *Finite Fields and Their Applications*, 16(3):155 – 162, 2010.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[Ked08] Kiran S. Kedlaya. Search techniques for root-unitary polynomials. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 71–81. Amer. Math. Soc., Providence, RI, 2008.

[Ked13] Kiran S. Kedlaya. Computing zeta functions of nondegenerate toric hypersurfaces via controlled reduction. http://kskedlaya.org/slides/

oxford2013.pdf, 2013. [Online; accessed 25-January-2018].

[Min10] Moritz Minzlaff. Computing zeta functions of superelliptic curves in larger characteristic. *Math. Comput. Sci.*, 3(2):209–224, 2010.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[Sag] Sage Developers, The. *SageMath, the Sage Mathematics Software System*. http://www.sagemath.org.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017.

[Tui18] Jan Tuitman. Computing zeta functions of generic projective hypersurfaces in larger characteristic. *Math. Comp.*, 2018.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
E-mail address: varul@mit.edu
URL: http://math.mit.edu/~varul/

Department of Mathematics and Statistics, Boston University, Boston, MA 02215, USA
E-mail address: alex.j.best@gmail.com
URL: https://alexjbest.github.io/

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
E-mail address: edgarcosta@math.dartmouth.edu
URL: http://www.math.dartmouth.edu/~edgarcosta/

Department of Mathematics and Statistics, Boston University, Boston, MA 02215, USA
E-mail address: rmagner@bu.edu
URL: http://math.bu.edu/people/rmagner/

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
E-mail address: ngtriant@mit.edu
URL: https://math.mit.edu/~ngtriant/

COMPUTATION OF TRIANGULAR INTEGRAL BASES

JENS-DIETRICH BAUCH, HA THANH NGUYEN TRAN

Abstract. Let A be a Dedekind domain, K the fraction field of A, and $f \in A[x]$ a monic irreducible separable polynomial. For a given non-zero prime ideal $\mathfrak{p}$ of A we present in this paper a new algorithm to compute a triangular $\mathfrak{p}$-integral basis of the extension L of K determined by f. This approach can be easily adopted to compute triangular $\mathfrak{p}$-integral basis of fractional ideals I of the integral closure of A in L. Along this process one can compute $\mathfrak{p}$-integral bases for a family of ideals contained in I as a by-product.

Introduction

In computational number theory one of the most important examples for a Dedekind domain is the ring of integers $\mathcal{O}$ of a number field $L = \mathbb{Q}(\theta)$, where θ is the root of a monic irreducible polynomial f over $\mathbb{Z}$ of degree n. In that context a set $(b_0, \ldots, b_{n-1})$ is called a triangular basis of $\mathcal{O}$ if it generates $\mathcal{O}$ as a $\mathbb{Z}$-module and

$$b_0 = 1 \text{ and } b_i = \frac{\theta^i + \sum_{j<i} \lambda_{i,j}\theta^j}{h_i},$$

where $\lambda_{i,j}, h_i \in \mathbb{Z}$ and $1 \leq i \leq n-1$. For a module over a PID, a triangular basis always exists. For instance, in case $L = \mathbb{Q}(\sqrt{5})$ we have

$$\mathcal{O} = \left\langle 1, \frac{\sqrt{5}+1}{2} \right\rangle_{\mathbb{Z}}.$$

Let p be a prime and let $\mathfrak{p} = p\mathbb{Z}$ be the prime ideal generated by p. A triangular $\mathfrak{p}$-integral basis of $\mathcal{O}$ is a triangular basis of $\mathcal{O}$ considered as module over the localization of $\mathbb{Z}$ at $\mathfrak{p}$. In the latter example we see a $\mathfrak{p}$-integral triangular basis of $\mathcal{O}$ with $\mathfrak{p} = 2\mathbb{Z}$, which is already an integral basis.

In [4][p. 217] the computation of an integral basis of a number field L is considered one of the five main computational problems in number theory. Let $\mathrm{Disc}(f) = \mathcal{L} \cdot \mathcal{S}^2$ be the discriminant of f with $\mathcal{L}, \mathcal{S} \in \mathbb{Z}$ and $\mathcal{L}$ be square-free. Denote by p a prime dividing $\mathcal{S}$ and set $\mathfrak{p} = p\mathbb{Z}$. One can distinguish in general two approaches for the computation of an integral basis. The first approach is based on the idea of computing kernels of liner maps in order to compute a $\mathfrak{p}$-radical of the order $\mathcal{O}$ and is known as the Round Two algorithm due to Pohst and Zassenhaus [13]. The second approach is based on constructing certain elements in $\mathcal{O}$ of maximal valuation at the prime ideals lying over $\mathfrak{p}$. The most famous algorithms are the Round Four algorithm [6, 13], those which are based on the OM-representation [8, 15, 3], and in the context of the computation of integral bases of algebraic function fields those using Puiseux expansion [18, 5]. In general, the second approach needs a prime factor of $\mathcal{S}$ as input. However, Guàrdia and Nart found in [7] a $\mathfrak{p}$-adic algorithm, which does not require a pre-factorization of $\mathcal{S}$.

Key words and phrases. p-integral bases, maximal order, Montes algorithm, Dedekind domain.

Our algorithm follows the approach from [15] and is based on simple linear algebra after a $\mathfrak{p}$-adic initialization step.

Let A be a Dedekind domain, K the fraction field of A, and $\mathfrak{p}$ a non-zero prime ideal of A. By $A_{\mathfrak{p}}$ we denote the localization of A at $\mathfrak{p}$ and we set $k_{\mathfrak{p}} = A/\mathfrak{p}$. Let $\pi \in \mathfrak{p}$ be a prime element of $\mathfrak{p}$.

Denote by $\theta \in K^{\text{sep}}$ a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n and $L = K(\theta)$ the finite separable extension of K generated by θ. Let $\mathcal{O}$ be the integral closure of A in L and $\mathcal{O}_{\mathfrak{p}}$ be the integral closure of $A_{\mathfrak{p}}$ in L. A $\mathfrak{p}$-*integral basis of* $\mathcal{O}$ is an $A_{\mathfrak{p}}$-basis of $\mathcal{O}_{\mathfrak{p}}$. In order to determine a $\mathfrak{p}$-integral basis, we compute, for $0 \leq i \leq n-1$, monic polynomials $g_i(x) \in A[x]$ of degree i such that $g_i(\theta)$ has maximal value with respect to a pseudo valuation ω on L (cf. equation 1 below). Then a triangular $\mathfrak{p}$-integral basis is obtained by $(g_i(\theta)/\pi^{w(g_i(\theta))} \mid 0 \leq i \leq n-1)$. The computation of the g_i's can be deduced by straight forward linear algebra, which results in a simple algorithm. The theoretical complexity (counted in the operations in $k_{\mathfrak{p}}$ cf. Subsection 2.4) is slower than the current state of the art methods presented in [8, 15, 3]. The running time of the current methods is asymptotically $n^{2+\epsilon}$, whereas the one of our method is cubic in n. However, after an initialization step the running time drops to n^2. One advantage of our algorithm is that it can be adopted to compute integral bases of families of fractional ideals. That is, for calling once our algorithm for a fractional ideal I of $\mathcal{O}$ with $I \supset \mathcal{O}$ we can determine with no extra time $\mathfrak{p}$-integral bases for certain fractional ideals I' contained in I (cf. Section 3).

In Section 1 we introduce the notation which is needed to explain the main idea of our algorithm in Section 2. Further on we describe the details of our new methods, give an example, and analyze the running time. Finally an application of our algorithm for the computation of $\mathfrak{p}$-integral bases of families of fractional ideals is presented in Section 3.

1. Notation

We keep the notation from the introduction. Every prime ideal $\mathfrak{p}$ induces a discrete valuation $v_{\mathfrak{p}} : A \to \mathbb{Z} \cup \{\infty\}$. We denote the completion of K at $\mathfrak{p}$ by $K_{\mathfrak{p}}$. The valuation $v_{\mathfrak{p}}$ extends in an obvious way to $K_{\mathfrak{p}}$. Denote by $\hat{A}_{\mathfrak{p}}$ the valuation ring of $v_{\mathfrak{p}}$. Let $S = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$ be the set of all prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$. For each $\mathfrak{P}_i \in S$ we define $L_{\mathfrak{P}_i}$ to be the completion of L at $\mathfrak{P}_i$ and $\mathcal{O}_{\mathfrak{P}_i}$ to be the integral closure of $\hat{A}_{\mathfrak{p}}$ in $L_{\mathfrak{P}_i}$.

By the classical theorem of Hensel [12] the prime ideals $\mathfrak{P}_i$ are in one-to-one correspondence with the monic irreducible factors $f_{\mathfrak{P}_i}$ of f in $\hat{A}_{\mathfrak{p}}[x]$. For each $i \in \{1, \ldots, s\}$ denote by θ_i a root and by n_i the degree of $f_{\mathfrak{P}_i}$. Then we can represent $L_{\mathfrak{P}_i}$ as $L_{\mathfrak{P}_i} = K_{\mathfrak{p}}(\theta_i)$ and define the injection $\iota_i : L \to L_{\mathfrak{P}_i}$ via $\theta \mapsto \theta_i$. In particular, $\sum_{1 \leq i \leq s} n_i = n$ since $f = \prod_{1 \leq i \leq s} f_{\mathfrak{P}_i} \in \hat{A}_{\mathfrak{p}}[x]$.

Denote by $\text{Max}(\mathcal{O})$ the set of all maximal ideals of $\mathcal{O}$. As $\mathcal{O}$ is a Dedekind domain every non-zero fractional ideal I of $\mathcal{O}$ can be factored into a finite product of prime ideals:

$$I = \prod_{\mathfrak{P} \in \text{Max}(\mathcal{O})} \mathfrak{P}^{a_{\mathfrak{P}}}$$

with integer exponents $a_{\mathfrak{P}}$. Any fractional ideal can be considered as a free A-module of rank n.

Definition 1.1 (Index)**.** *Let M and M' be two free A-modules of rank n. The* index $[M : M']$ *is defined to be the non-zero fractional ideal generated by the determinant of the transition matrix from an A-basis of M' to one of M.*

2. Computation of $\mathfrak{p}$-integral bases

The goal of this section is to describe an algorithm that computes a triangular $\mathfrak{p}$-integral basis of $\mathcal{O}$ for a fixed non-zero prime ideal $\mathfrak{p}$ of A. In particular, we compute $b_0, \ldots, b_{n-1}$ in L such that $\mathcal{O}_\mathfrak{p} = \langle b_0, \ldots, b_{n-1}\rangle_{A_\mathfrak{p}}$ and

$$b_i = \frac{g_i(\theta)}{\pi^{m_i}}$$

for some monic polynomial $g_i \in A[x]$ of degree i and $m_i \in \mathbb{Z}_{\geq 0}$.

2.1. **The algorithm.** For $\mathfrak{P}_i \in S$, let $e_{\mathfrak{P}_i}$ be the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$ and $v_{\mathfrak{P}_i}$ be the induced discrete valuation on L. Then we define a pseudo valuation on L as follows:

$$\omega = \Big\lfloor \min_{1\leq i\leq s} \Big\{ \frac{v_{\mathfrak{P}_i}}{e_{\mathfrak{P}_i}} \Big\} \Big\rfloor. \tag{1}$$

Definition 2.1. *The monic polynomial $g(x) \in A[x]$ of degree $i < n$ is called i-**maximal** if $\omega(g(\theta)) \geq \omega(h(\theta))$ for all monic polynomials $h \in A[x]$ having the same degree as g.*

Our algorithm is based on the following theorem ([15][Thm. 1.4]):

Theorem 2.2. *Let $b_0, \ldots, b_{n-1} \in L$, where*

$$b_i = \frac{g_i(\theta)}{\pi^{\omega(g_i(\theta))}}, \quad g_i \text{ is } i\text{-maximal}, \tag{2}$$

then $(b_0, \ldots, b_{n-1})$ is a triangular $\mathfrak{p}$-integral basis.

In particular the theorem guarantees the existence of a triangular $\mathfrak{p}$-integral basis.

According to Theorem 2.2 we have to determine i-maximal polynomials $g_i(x) \in A[x]$, for $0 \leq i \leq n-1$. We start with $g_i = x^i$ and successively replace g_i by a monic polynomial g_i' having degree i with $w(g_i'(\theta)) > w(g_i(\theta))$. One can compute g_i' by applying an **augmentation-step** defined as follows. Let $\mathcal{R} \subset A$ be a fixed system of representatives of $k_\mathfrak{p} = A/\mathfrak{p}$.

Definition 2.3. *Let $c_0, \ldots, c_m$ be in L ordered by non-decreasing ω-value and $\lambda_1, \ldots \lambda_m \in \mathcal{R}$ such that*

$$\omega\Big(c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j\Big) > \omega(c_m).$$

*Then we call $c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j$ an **augmentation-step**.*

In particular an augmentation-step increases the module spanned by the vectors:

$$\Big\langle \frac{c_0}{\pi^{\omega(c_0)}}, \ldots, \frac{c_m^*}{\pi^{\omega(c_m^*)}} \Big\rangle_{A_\mathfrak{p}} \supsetneq \Big\langle \frac{c_0}{\pi^{\omega(c_0)}}, \ldots, \frac{c_m}{\pi^{\omega(c_m)}} \Big\rangle_{A_\mathfrak{p}}.$$

The process is as follows: As an initial step we set $b_0 = 1$ and consider the vectors b_0, θ. Next, we determine $\lambda_0 \in \mathcal{R}$ to perform an augmentation-step: $d_{1,0} = \theta + \lambda_0$. If $x + \lambda_0$ is not 1-maximal, one finds $\lambda_1 \in \mathcal{R}$ such that $d_{1,1} = d_{1,0} + \lambda_1$ realizes an

augmentation-step. After finitely many steps, one can obtain some $d_1 = g_1(\theta)$ such that g_1 is 1-maximal. We set $b_1 = d_1/\pi^{\omega(d_1)}$.

Let $1 \leq i \leq n-1$ and assume we already have computed $b_0, \ldots, b_{i-1}$ satisfying (2). After finitely many augmentation-steps we deduce $\lambda_{i,0}, \ldots, \lambda_{i,i-1} \in \mathcal{R}$ such that $d_i = \theta^i + \sum_{j<i} \lambda_{i,j} b_j = g_i(\theta)/\pi^{m_i}$ with $m_i \in \mathbb{Z}$ and g_i is i-maximal. Let $b_i = d_i/\pi^{\omega(d_i)}$. Then $b_0, \ldots, b_i$ are the first $(i+1)$ vectors in a triangular $\mathfrak{p}$-integral basis. After $n-1$ steps this leads to a triangular $\mathfrak{p}$-integral basis.

We summarize this idea with the following pseudocode:

Algorithm 1. (Triangular $\mathfrak{p}$-integral basis)
Input: $(1, \theta, \ldots, \theta^{n-1})$.
Output: A triangular $\mathfrak{p}$-integral basis.

1: $b_0 \longleftarrow 1, \quad \mathcal{B} \longleftarrow (b_0)$
2: **for** $i = 1, \ldots, n-1$ **do**
3: $\quad b_i \longleftarrow \theta^i$
4: $\quad$ **while** possible **do**
5: $\quad\quad b_i \longleftarrow b_i + \sum_{j<i} \lambda_j \pi^{\omega(b_i)-\omega(b_j)} b_j$ **(augmentation-step)**
6: $\quad$ **end while**
7: $\quad \mathcal{B} \longleftarrow \mathrm{Append}(\mathcal{B}, \frac{b_i}{\pi^{\omega(b_i)}})$
8: **end for**
9: **return** $\mathcal{B}$
end

Henceforth we explain how to perform an augmentation-step. We adopt the reduction algorithm from [14, 2] which is used for the computation of Riemann-Roch spaces in the context of algebraic function fields. Because the ω-value is strictly increased at any step, we prefer to use the word augmentation rather than reduction as in [2].

Denote by $\mathcal{B}_i$ an $\hat{A}_{\mathfrak{p}}$-basis for $\mathcal{O}_{\mathfrak{P}_i}$, which is in particular a $K_{\mathfrak{p}}$-basis for $L_{\mathfrak{P}_i}$. In addition, denote by v the $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}$ extended to a fixed algebraic closure of $K_{\mathfrak{p}}$ such that $v(x) = 1$ for all $x \in A_{\mathfrak{p}}^*$. Since $\mathfrak{P}_i$ lies over $\mathfrak{p}$ with ramification index $e_{\mathfrak{P}_i}$, the valuation $v_{\mathfrak{P}_i}$ is an extension of $v_{\mathfrak{p}}$ and relates to the extension v as follows: $v_{\mathfrak{P}_i}(z) = v(\iota_i(z)) e_{\mathfrak{P}_i}$ for any $z \in L$. See [17] for more details.

For $\alpha \in L_{\mathfrak{P}_i}$ we define by $\mathcal{C}_i(\alpha) \in K_{\mathfrak{p}}^{n_i}$ the coordinate vector of α with respect to the basis $\mathcal{B}_i$ and

$$\iota = (\mathcal{C}_i \circ \iota_i)_{1 \leq i \leq s} : L \to K_{\mathfrak{p}}^n.$$

Lemma 2.4. *For $z \in L$ it holds that*

$$\omega(z) = \min_{1 \leq i \leq n} \{v(\zeta_i) \mid \iota(z) = (\zeta_1, \ldots, \zeta_n)\}.$$

Proof. For $1 \leq i \leq s$ we set $w_{\mathfrak{P}_i} = v_{\mathfrak{P}_i}/e_{\mathfrak{P}_i}$. By definition $\omega(z) = \min_{1 \leq i \leq s} \lfloor w_{\mathfrak{P}_i}(z) \rfloor$, thus it is sufficient to show that

$$\Big\lfloor w_{\mathfrak{P}_i}(z) \Big\rfloor = \min_{b \in \mathcal{B}_i} \{v(\zeta_b)\}, \qquad \text{with } \iota_i(z) = \sum_{b \in \mathcal{B}_i} \zeta_b b,$$

for each $1 \leq i \leq s$. As $v_{\mathfrak{P}_i}(z) = v(\iota_i(z)) e_{\mathfrak{P}_i}$, one has $w_{\mathfrak{P}_i}(z) = v_{\mathfrak{P}_i}(z)/e_{\mathfrak{P}_i} = v(\iota_i(z))$. Since $\mathcal{B}_i$ is an integral basis of $\mathcal{O}_{\mathfrak{P}_i}$ by [3][Thm 3.2] it holds that $\mathcal{B}_i$ is v-semi-orthonormal; that is $\big\lfloor v(\iota_i(z)) \big\rfloor = \big\lfloor v(\sum_{b \in \mathcal{B}_i} \zeta_b b) \big\rfloor = \min_{b \in \mathcal{B}_i} \{v(\zeta_b)\}$. □

20 Jun 2018 13:21:11 PDT
Version 3 - Submitted to Open Book Series

Each $\lambda \in K_{\mathfrak{p}}$ can be written as $\lambda = \sum_{j=m}^{\infty} \lambda_j \pi^j$ where $m = v(\lambda)$ and $\lambda_j \in \mathcal{R}$. For an integer $r \geq m$, we set

$$\mathrm{lt}_r(\lambda) = \begin{cases} \lambda_m & \text{if } r = m \\ 0 & \text{else} \end{cases}$$

and call it the **lower term** of λ at r.

Definition 2.5. *Let ψ be a map from L to $K_{\mathfrak{p}}^n$. For $z \in L$ and $r \geq \omega(z)$ we define the **lower term vector** of z at r (with respect to ψ) by*

$$\mathrm{LT}_r(\psi(z)) = (\mathrm{lt}_r(z_i))_{1 \leq i \leq n} \in k_{\mathfrak{p}}^n,$$

where $\psi(z) = (z_1, \ldots, z_n)$.

Recall that $\mathcal{R} \subset A$ is a set of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$.

Lemma 2.6. *Let $c_0, \ldots, c_m \in L$ ordered by non-decreasing ω-value and $\alpha_0, \ldots, \alpha_m \in \mathcal{R}$ with $\alpha_m \neq 0$ such that*

$$\sum_{0 \leq i \leq m} \alpha_i \mathrm{LT}_{\omega(c_i)}(\iota(c_i)) = 0. \tag{3}$$

Then, $c_m^* = c_m + \sum_{j=0}^{m-1} \frac{\alpha_j}{\alpha_m} \pi^{\omega(c_m)-\omega(c_j)} c_j$ realizes an augmentation-step.

Moreover, if the $\mathrm{LT}_{\omega(c_i)}(\iota(c_i))$ are $k_{\mathfrak{p}}$-linearly independent, then no augmentation-step is applicable.

Proof. We write $\iota(c_j) = (c_{j,1}, \ldots, c_{j,n})$, for $j = 0, \ldots, m$. By Lemma 2.4 it holds that $\omega(c_j) = \min_{1 \leq i \leq n}\{v(c_{j,i})\}$. By construction, one can write

$$\iota(c_j) = \mathrm{LT}_{\omega(c_j)}(\iota(c_j))\pi^{\omega(c_j)} + \sum_{i > \omega(c_j)} v_{i,j} \pi^i$$

with $v_{i,j} \in k_{\mathfrak{p}}^n$. If we identify $k_{\mathfrak{p}}$ with $\mathcal{R}$, then ι becomes $k_{\mathfrak{p}}[\pi]$-linear. That is,

$$\iota(c_m^*) = \iota(c_m) + \sum_{j=0}^{m-1} \frac{\alpha_j}{\alpha_m} \pi^{\omega(c_m)-\omega(c_j)} \iota(c_j)$$

The fact that $\sum_{0 \leq i \leq m} \alpha_i \mathrm{LT}_{\omega(c_i)}(\iota(c_i)) = 0$ implies that

$$\iota(c_m^*) = \sum_{i > \omega(c_m)} v_i \pi^i = (c_{m,1}^*, \ldots, c_{m,n}^*)$$

with vectors $v_i \in k_{\mathfrak{p}}^n$. Accordingly, for $\iota(c_m^*) = (c_{m,1}^*, \ldots, c_{m,n}^*)$ it holds that $v(c_{m,i}^*) > \omega(c_m)$, for $i = 1, \ldots, n$. Therefore $\omega(c_m^*) > \omega(c_m)$ by Lemma 2.4.

On the other hand, any augmentation-step implies that $\{\mathrm{LT}_{\omega(c_i)}(\iota(c_i))\}_{i=0,\ldots,m}$ are $k_{\mathfrak{p}}$-linearly dependent.

□

Theorem 2.7. *Algorithm 1 terminates after a finite number of steps and computes a triangular $\mathfrak{p}$-integral basis.*

Proof. Any augmentation-step in Algorithm 1 is performed such that the resulting element b_i is of the form $g_i(\theta)/\pi^{m_i}$ with $g_i(x) \in A[x]$ monic of degree i and $m_i = \omega(g_i(\theta))$ for $0 \leq i \leq n-1$. After any augmentation-step one of the m_i strictly increases. Every m_i is bounded by the $\mathfrak{p}$-valuation of the index $[\mathcal{O} : A[\theta]]$, hence after finitely many steps g_i is i-maximal for $0 \leq i \leq n-1$. Consequently, Algorithm

1 outputs $(g_i(\theta)/\pi^{m_i})_{0\leq i\leq n-1}$, which is a triangular $\mathfrak{p}$-integral basis according to Theorem 2.2. □

2.2. **Algorithmic Details.** In this subsection we give a detailed realization of Algorithm 1. The bottleneck is the computation of $\iota(\theta^j) \in K_{\mathfrak{p}}^n$ for $j = 0, \ldots, n-1$. The components of the vector $\iota(\theta^j)$ are in general infinite power series in π with coefficients in $k_{\mathfrak{p}}$ and cannot be exactly represented in the machine. It is however sufficient to work with approximations. In fact one can write

$$\iota(\theta^j) = \sum_{i=\omega(\theta^j)}^{\infty} v_i \pi^i,$$

where $v_i \in k_{\mathfrak{p}}^n$ and $v_{\omega(\theta^j)} = \mathrm{LT}_{\omega(\theta^j)}(\iota(\theta^j))$. In practice we work with $\iota(\theta^j) (\mathrm{mod}\ \pi^\nu) \equiv \sum_{i=\omega(\theta^j)}^{\nu-1} v_i \pi^i$, where $\nu > \omega(\theta^j)$ has to be chosen such that Algorithm 1 still outputs a triangular $\mathfrak{p}$-integral basis.

First we consider a realization of the computation of $\iota(\theta^j)(\bmod \pi^\nu)$ and later we discuss how to choose ν.

Let $\Phi_i(x) \in A[x]$ be an approximation to $f_{\mathfrak{P}_i}(x)$ with precision $\nu \in \mathbb{Z}$; that is Φ_i is monic and irreducible (over $\hat{A}_{\mathfrak{p}}$) such that

$$f_{\mathfrak{P}_i} \equiv \Phi_i (\mathrm{mod} \pi^\nu). \tag{4}$$

Moreover, every approximation Φ_i defines a finite extension L_{Φ_i} of K. We denote by $\tilde{\theta}_i$ a root of Φ_i such that $L_{\Phi_i} = K(\tilde{\theta}_i)$ and define the map $\iota_{i,\nu}$ via $\theta \mapsto \tilde{\theta}_i$.

Recall that $\mathcal{B}_i$ denotes an integral basis for the completion $L_{\mathfrak{P}_i}$. Every $b \in \mathcal{B}_i$ can be written as $b = g(\theta_i)/\pi^{l_b}$ with $g(x) \in \hat{A}_{\mathfrak{p}}[x]$ and $l_b \in \mathbb{Z}$ minimal. Let $g_\nu(x) \in A[x]$ be the polynomial obtained by reducing the coefficients of g modulo π^ν. This allows us to define, $b_\nu = g_\nu(\tilde{\theta}_i)/\pi^{l_b} \in L_{\Phi_i}$.

Lemma 2.8. *For $\nu > \max\{l_b \mid b \in \mathcal{B}_i\}$, the set $\mathcal{B}_{i,\nu} = \{b_\nu \mid b \in \mathcal{B}_i\}$ is a $\mathfrak{p}$-integral basis of L_{Φ_i}.*

Proof. Denote by $\mathcal{O}_i$ the integral closure of A in L_{Φ_i}. Since Φ_i is irreducible over $\hat{A}_{\mathfrak{p}}$ there exists only one prime ideal $\widetilde{\mathfrak{P}}_i$ of $\mathcal{O}_i$ over $\mathfrak{p}$. Here $b = g(\theta_i)/\pi^{l_b}$ for all $b \in \mathcal{B}_i$ as above. By the choice of ν we have $v_{\widetilde{\mathfrak{P}}_i}(g_\nu(\tilde{\theta}_i)/\pi^{l_b}) \geq 0$ and b_ν is integral. As a consequence $\mathcal{B}_{i,\nu} \subset \mathcal{O}_i$. Now it is enough to show that $\mathcal{B}_{i,\nu}$ generates $\mathcal{O}_i$ but this is directly inherited from $\mathcal{B}_i$.

□

For $z \in L_{\Phi_i}$ we denote by $C_{\mathcal{B}_{i,\nu}}(z) \in K^{n_i}$ the coordinate vector of z with respect to the basis $\mathcal{B}_{i,\nu}$. Then we can define the following map

$$\tilde{\iota}_\nu : L \to K^n, \quad z \mapsto (C_{\mathcal{B}_{i,\nu}}(\iota_{i,\nu}(z)))_{1\leq i\leq s}.$$

Lemma 2.9. *For $z \in L$ and a positive integer ν it holds*

$$\iota(z) (\mathrm{mod} \pi^\nu) \equiv \tilde{\iota}_\nu(z).$$

Proof. The elements b_ν in $\mathcal{B}_{i,\nu}$ are obtained by taking the coefficients of $b \in \mathcal{B}_i$ modulo π^ν. Therefore, it is sufficient to show that $\iota_i(z)$ and $\iota_{i,\nu}(z)$ are the same modulo π^ν for all $z \in L$, for all $1 \leq i \leq s$. Any element $z \in L$ can be written as $z = g(\theta)/h$ with $g(x) \in A[x]$ and $h \in A$. Thus, we may restrict our consideration to elements $g(\theta)$.

Given an index i and a polynomial $g(x) \in A[x]$, we will show that $\iota_i(g(\theta)) = g(\theta_i)$ and $\iota_{i,\nu}(g(\theta)) = g(\tilde{\theta}_i)$ coincide modulo π^ν. We consider $g(\theta_i)$ to be the class of g in $A_\mathfrak{p}[x]/f_{\mathfrak{P}_i}A_\mathfrak{p}[x]$ and $g(\tilde{\theta}_i)$ to be the one of g in $A_\mathfrak{p}[x]/\Phi_i A_\mathfrak{p}[x]$. Then the statement follows immediately by the fact that

$$f_{\mathfrak{P}_i} (\mathrm{mod}\, \pi^\nu) \equiv \Phi_i$$

by the definition of the approximation Φ_i.

□

Theorem 2.10. *Let ν be an integer with $\nu \geq v_\mathfrak{p}([\mathcal{O} : A[\theta]])$. If we replace in the augmentation-steps along Algorithm 1 the map ι by $\tilde{\iota}_\nu$ then the algorithm outputs a triangular $\mathfrak{p}$-integral basis and needs at most $v_\mathfrak{p}([\mathcal{O} : A[\theta]])$ augmentation-steps.*

Proof. For a triangular $\mathfrak{p}$-integral basis $(b_0, \ldots, b_{n-1})$ with $b_i = \frac{g_i(\theta)}{\pi^{\omega(g_i(\theta))}}$ we have $\sum_{0\leq i\leq n-1} \omega(g_i(\theta)) = v_\mathfrak{p}([\mathcal{O} : A[\theta]])$. Algorithm 1 produces b_i with g_i being i-maximal by applying augmentations-steps. Note that any of these steps increases the ω-value by at least one. Consequently, after maximally $v_\mathfrak{p}([\mathcal{O} : A[\theta]])$ steps the algorithm outputs a $\mathfrak{p}$-integral basis.

For the first statement we assume that the precision $\nu \geq v_\mathfrak{p}([\mathcal{O} : A[\theta]])$ is not sufficient. That is Algorithm 1 outputs $b_0, \ldots, b_{n-1}$, which is not a $\mathfrak{p}$-integral basis, at precision $\nu \geq v_\mathfrak{p}([\mathcal{O} : A[\theta]])$. Hence there are still augmentation-steps applicable to $b_0, \ldots, b_{n-1}$, which have not been detected because of the too low precision. This implies that the lower term vectors

$$\mathrm{LT}_{\omega(b_0)}(\tilde{\iota}_\nu(b_0)), \ldots, \mathrm{LT}_{\omega(b_{n-1})}(\tilde{\iota}_\nu(b_{n-1}))$$

are linearly dependent by Lemma 2.6. In particular, for at least one $0 \leq i \leq n-1$ the lower term vector $\mathrm{LT}_{w(b_i)}(\tilde{\iota}_\nu(b_i))$ is zero. Then $b_i = \frac{g_i(\theta)}{\pi^{w(g_i(\theta))}}$ satisfies

$$\iota(g_i(\theta)) = \sum_{j\geq\nu} v_{i,j}\pi^j, \quad v_{i,j} \in k_\mathfrak{p}^n.$$

In particular we have $\omega(g_i(\theta)) \geq \nu$ that leads to the following contradiction:

$$\nu \geq v_\mathfrak{p}([\mathcal{O} : A[\theta]]) > v_\mathfrak{p}([\langle b_0, \ldots, b_{n-1}\rangle_A : A[\theta]]) = \sum_{0\leq i\leq n-1} w(g_i(\theta)) \geq \nu.$$

□

2.3. **Example.** Let $f = x^4 + 4x^3 + (4t^2+4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$ with $A = \mathbb{F}_{13}[t]$ and let L be the function field defined by f. Then $\mathrm{Disc}(f) = \mathcal{L}\cdot\mathcal{S}^2$ with $\mathcal{S} = t^2(t^3+3)(t^3+10)$. Let $\pi = t$ and $\mathfrak{p} = \pi \cdot A$. Then we want to compute a $\mathfrak{p}$-integral basis. Here $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1\cdot\mathfrak{P}_2$, the ramification indices $e_{\mathfrak{P}_1} = e_{\mathfrak{P}_2} = 1$. Moreover f splits into $f = f_{\mathfrak{P}_1}\cdot f_{\mathfrak{P}_2}$ over $\hat{A}_\mathfrak{p} = \mathbb{F}_{13}[[t]]$ with $\deg f_{\mathfrak{P}_1} = \deg f_{\mathfrak{P}_2} = 2$. First, one can compute approximations $\Phi_1 = x^2+2t^2$ and $\Phi_2 = x^2+4x+2t^2+4$ of $f_{\mathfrak{P}_1}$ and $f_{\mathfrak{P}_2}$ with precision $\nu = 8$ using the Montes Algorithm [11]. This precision is sufficient according to Theorem 2.10 because $\nu = 8 > v_\mathfrak{p}(\mathrm{Disc}(f)) = 4 \geq v_\mathfrak{p}([\mathcal{O} : A[\theta]])$. Let θ_i be a root of $f_{\mathfrak{P}_i}$ and $\tilde{\theta}_i$ be one root of Φ_i, for $i = 1, 2$ respectively.

Next, we compute

$$\mathcal{B}_1 = (1, \tilde{\theta}_1/t), \quad \mathcal{B}_2 = (1, (\tilde{\theta}_2+2)/t)$$

$\mathfrak{p}$-integral bases for L_{Φ_1} and L_{Φ_2}, respectively as explained in [10]. Note that $(1, \theta_1/t)$ and $(1, (\theta_2+2)/t)$ are integral bases for $L_{\mathfrak{P}_1}$ and $L_{\mathfrak{P}_2}$. For $0 \leq j \leq$

3, we obtain $\iota_{i,\nu}(\theta^j)$ by computing $x^j (\mathrm{mod} \Phi_i)$, evaluating it in $\tilde{\theta}_i$ and taking its coefficient with respect to $\mathcal{B}_i$, for $i = 1, 2$. This process leads to the following matrix:

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\tilde{\iota}_\nu(1)$	1	0	1	0	0
$\tilde{\iota}_\nu(\theta)$	0	t	11	t	0
$\tilde{\iota}_\nu(\theta^2)$	$11t^2$	0	$11t^2+4$	$9t$	0
$\tilde{\iota}_\nu(\theta^3)$	0	$11t^3$	$12t^2+5$	$11t^3+12t$	0

The rows of the 4 by 4 submatrix represent the vectors $\tilde{\iota}_\nu(\theta^j)$, for $j = 0, \ldots, 3$. The last column shows the value $\omega(\theta^j)$. The blue colored entries of the submatrix are those which attain the minimum; that is their v_t-valuation coincides with the ω-value of the corresponding row.

We consider the lower term vectors in order to perform augmentation-steps:

$$M = \begin{bmatrix} \mathrm{LT}_0(\tilde{\iota}_\nu(1)) \\ \vdots \\ \mathrm{LT}_0(\tilde{\iota}_\nu(\theta^3)) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 5 & 0 \end{bmatrix} \in \mathbb{F}_{13}^{4\times 4}.$$

Since $\mathrm{rank}(M) = 2 < 4$, one can apply augmentation-steps. By Lemma 2.6 we can read out the augmentation-steps from M and deduce $b_2^* = \theta^2 + 2\theta$ and $b_3^* = \theta^3 + 9\theta$. This results in:

(5)

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\tilde{\iota}_\nu(1)$	1	0	1	0	0
$\tilde{\iota}_\nu(\theta)$	0	t	11	t	0
$\tilde{\iota}_\nu(b_2^*)$	$11t^2$	$2t$	$11t^2$	$11t$	1
$\tilde{\iota}_\nu(b_3^*)$	0	$11t^3+9t$	$12t^2$	$11t^3+8t$	1

with $\omega(b_2^*) = \omega(b_3^*) = 1$. We again check the lower term vectors in order to see if another augmentation-step can be applied.

$$M = \begin{bmatrix} \mathrm{LT}_0(\tilde{\iota}_\nu(1)) \\ \mathrm{LT}_0(\tilde{\iota}_\nu(\theta)) \\ \mathrm{LT}_1(\tilde{\iota}_\nu(b_2^*)) \\ \mathrm{LT}_1(\tilde{\iota}_\nu(b_3^*)) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 2 & 0 & 11 \\ 0 & 9 & 0 & 8 \end{bmatrix}.$$

Now $\mathrm{rank}(M) = 4$, so no further augmentation is applicable. That is,

$$\left(1, \theta, \frac{\theta^2+2\theta}{t}, \frac{\theta^3+9\theta}{t}\right)$$

is a $\mathfrak{p}$-integral basis.

2.4. **Complexity.** For the subsequent complexity analysis we define $\delta := v_\mathfrak{p}(\mathrm{Disc} f)$ the $\mathfrak{p}$-valuation of the discriminant of f. Furthermore we admit fast multiplication techniques of Schönhage-Strassen [16]. Let R be a ring and let $g_1, g_2 \in R[x]$ be two polynomials, whose degrees are bounded by d_1 and d_2, respectively. Then, the multiplication $g_1 \cdot g_2$ needs at most $O(\max\{d_1, d_2\}^{1+\epsilon})$ operations in R. Algorithm 1 works well with precision $\nu = \delta$ by Theorem 2.10. Thus, one may consider the elements in A to be finite π-adic developments whose length is equal to $O(\delta)$. We fix a system of representatives $\mathcal{R}$ of $k_\mathfrak{p} = A/\mathfrak{p}$ and call an operation in A $\mathfrak{p}$-*small* if it involves two elements belonging to $\mathcal{R}$. Hence, any multiplication in A can be

performed with at most $O(\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. We assume that the residue field $A/\mathfrak{p}$ is finite with q elements.

The total cost of Algorithm 1 is obtained by adding all the cost from Lemma 2.14 and 2.15 as below.

Theorem 2.11. *Algorithm 1 needs at most*

$$O\left(n^3\delta + n^2\delta^2 + n^{1+\epsilon}\delta\log q + n^{1+\epsilon}\delta^{2+\epsilon}\right)$$

$\mathfrak{p}$*-small operations. In particular, the runtime after the initialization is equal to* $O(n^2\delta^2)$ $\mathfrak{p}$*-small operations.*

Although the complexity depends asymptotically on n^3 in practice the running time is less pessimistic. The factor n^3 is due to the Gaussian elimination process in the Initialization Step (1)(b). We have to invert a $n \times n$ matrix T' with entries in A (see Lemma 2.13 for more details). If $\mathfrak{p}\mathcal{O}$ is a prime ideal then T' is a triangular matrix. In fact the less factors has $\mathfrak{p}\mathcal{O}$ the more looks T' alike a triangular matrix. In that case inverting T' can be performed quickly and the algorithm is practical for large n.

The following steps dominate the runtime of Algorithm 1:

(1) Initialization:
  (a) Computation of approximations Φ_i and local bases $\mathcal{B}_i$, for $1 \le i \le s$.
  (b) Computing the vectors $(C_{\mathcal{B}_i}(\iota_{i,\nu}(\theta^j)))_{1\le i\le s}$, for $0 \le j \le n-1$.
(2) Realization of augmentation-steps.
  (a) Determining the coefficients in the linear relation from (3).
  (b) Performing the augmentation-step.

For the initialization step we use the Montes algorithm [1, 10] to compute approximations Φ_i and the $\mathfrak{p}$-integral basis $\mathcal{B}_i$ of L_{Φ_i}. Details can be found in [11] and [3].

2.4.1. *Initialization.*
(a) The Montes algorithm has a cost of $O\left(n^{2+\epsilon} + n^{1+\epsilon}\delta\log q + n^{1+\epsilon}\delta^{2+\epsilon}\right)$ operations [1]. Once we have called the Montes algorithm we determine the bases $\mathcal{B}_i$ as explained in [3]. The complexity of computing all bases is equal to $O\left(n^{2+\epsilon}\delta^{1+\epsilon}\right)$ $\mathfrak{p}$-small operations.

According to [1, Theorem 5.16], the cost of the computation of an approximation Φ_i of $f_{\mathfrak{P}_i}$ with precision ν is given by

$$O(nn_i\nu^{1+\epsilon} + n\delta^{1+\epsilon})$$

$\mathfrak{p}$-small operations, where $n_i = \deg\Phi_i$. As a result of Theorem 2.10 a sufficient precision is equal to $O(\delta)$. Since $\sum_{i=1}^{s} n_i = n$, the cost of computing all approximations is equal to $O(n^2\delta^{1+\epsilon})$.

(b) Let T be the matrix, which rows are given by $\tilde{\iota}_\nu(\theta^i)$. We analyze the cost of determining T. First we consider $\iota_{i,\nu}(\theta^j)$ for $1 \le i \le s$ and $0 \le j \le n-1$, and then $C_{\mathcal{B}_i}(\iota_{i,\nu}(\theta^j))$. Recall that $\tilde{\theta}_i$ is a root of Φ_i such that $L_{\Phi_i} = K(\tilde{\theta}_i)$ for $1 \le i \le s$.

Lemma 2.12. *The cost of computing* $\iota_{i,\nu}(\theta^j)$ *for* $1 \le i \le s$ *and* $0 \le j \le n-1$ *is equal to* $O(n^2\delta^{1+\epsilon})$ $\mathfrak{p}$*-small operations.*

Proof. Clearly, $\iota_{i,\nu}(\theta^j)$ is equal to $x^j (\mathrm{mod} \Phi_i)$ evaluated in $\tilde{\theta}_i$. For $j < n_i = \deg \Phi_i$ we have $\iota_{i,\nu}(\theta^j) = \tilde{\theta}_i^j$.

When $j = n_i$, let $\psi_{n_i} = x^{n_i} - \Phi_i$. Then $x^{n_i} = \psi_{n_i} + \Phi_i$. Therefore $\iota_{i,\nu}(\theta^{n_i}) = \psi_n(\tilde{\theta}_i)$, which can be computed at no cost.

Assume $j \geq n_i$ and that we have computed $\psi_j = \alpha_{n_i-1} x^{n_i-1} + \cdots + \alpha_0 \in A[x]$ where $\psi_j \equiv x^j (\mathrm{mod} \Phi_i)$. In particular, $x^j = \psi_j + r_j \Phi_i$ with $r_j \in A[x]$. Then it holds

$$\begin{aligned} x^{j+1} = x(\psi_j + r_j \Phi_i) &= \alpha_{n_i-1} x^{n_i} + \cdots + \alpha_0 x + x r_j \Phi_i \\ &= \alpha_{n_i-1}(\psi_{n_i} + \Phi_i) + \alpha_{n_i-2} x^{n_i-1} + \cdots + \alpha_0 x + x r_j \Phi_i \\ &= \psi_{j+1} + r_{j+1} \Phi_i, \end{aligned}$$

where $\psi_{j+1} = \alpha_{n_i-1} \psi_{n_i} + \alpha_{n_i-2} x^{n_i-1} + \cdots + \alpha_0 x$ and $r_{j+1} = (\alpha_{n_i-1} + x r_j) \Phi_i$. As a consequence, one can compute ψ_{j+1} with at most n_i multiplications and additions in A. Then $\iota_{i,\nu}(\theta^{j+1}) = \psi_{j+1}(\tilde{\theta}_i)$. Since the precision is $\nu = O(\delta)$, it is enough to perform this computation modulo π^ν. For this reason, the computation of $\iota_{i,\nu}(\theta^j)$ for $j = 0, \ldots, n-1$ can be performed in $O(n n_i \delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. Because i runs from 1 to s and $n_i = \deg(\Phi_i)$ satisfies $\sum_{i=1}^s n_i = n$, computing $\iota_{i,\nu}(\theta^j)$, for $1 \leq i \leq s$ and $0 \leq j \leq n-1$, can be done in $O(n^2 \delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. □

Lemma 2.13. *The cost of computing the coordinates of the vectors $\iota_{i,\nu}(\theta^j)$ with respect to the basis $\mathcal{B}_i$ is equal to $O(n^3 \delta)$ $\mathfrak{p}$-small operations.*

Proof. Let $W = \prod_{i=1}^s L_{\Phi_i}$ and $\kappa_i : L_{\Phi_i} \longrightarrow W$ be the canonical embedding of L_{Φ_i} into W:

$$z \mapsto (0, \ldots, 0, \underbrace{z}_{i\text{-th}}, 0, \ldots, 0).$$

Then $\mathcal{B} = \cup_{i=1,\ldots,s} \kappa_i(\mathcal{B}_i)$ and $\mathcal{B}' = \{\kappa_i(\tilde{\theta}_i^j) \mid 1 \leq i \leq s,\ 0 \leq j \leq n_i\}$ are both K-basis of W. In particular, T is the basis change matrix from $\mathcal{B}'$ to $\mathcal{B}$. Since $n_i = \deg \Phi_i$ and $\sum_i n_i = n$ the bases $\mathcal{B}$ and $\mathcal{B}'$ have both n elements. In particular T is an $n \times n$ matrix. One computes T by inverting T', the matrix whose rows are the coefficients of the vectors in $\mathcal{B}$ with respect to $\mathcal{B}'$. Clearly T' can be computed at cost zero since it can be read off from the coefficients of the elements in $\mathcal{B}_i$.

As we work with precision $\nu = O(\delta)$ we may assume that the coefficients of $\iota_{i,\nu}(\theta^j) \in A[\hat{\theta}_i]$ are polynomials in $k_\mathfrak{p}[\pi]$ of degree $O(\delta)$, for $0 \leq j \leq n-1$. Accordingly inverting T' can be obtained by $O(n^3 \delta)$ $\mathfrak{p}$-small operations by Gaussian elimination. □

Adding all the cost leads to the following result.

Lemma 2.14. *The cost for the initialization step is*

$$O\left(n^3 \delta + n^2 \delta^{1+\epsilon} + n^{1+\epsilon} \delta \log q + n^{1+\epsilon} \delta^{2+\epsilon}\right) \tag{6}$$

$\mathfrak{p}$-small operations.

2.4.2. *Augmentations-Steps.*

Lemma 2.15. *The cost of the augmentations-steps is $O(n^2 \delta^2)$ $\mathfrak{p}$-small operations.*

Proof. Let $\mathcal{B}$ be the set manipulated along Algorithm 1. We determine the coefficients α_b for $b \in \mathcal{B}$ from (3) by solving a system of linear equations over $k_\mathfrak{p}$ represented by the lower term matrix M whose rows are given by $\mathrm{LT}_{\omega(b)}(\tilde{\iota}_\nu(b))$ for

$b \in \mathcal{B}$. Note that one can obtain M by taking the lower term matrix M' from the previous augmentation-step and refreshes or replaces the last row. Both matrices have at most n rows and n columns with entries in $k_\mathfrak{p}$. If we have stored M' in row echelon form we can transform M into row echelon form and read out the coefficients for the augmentation-steps in $O(n^2)$ operations. After determining the coefficients α_b for $b \in \mathcal{B}$ from (3), one will apply the augmentation-steps to $\mathcal{B}$ and T. That is computing a linear combination of the form $\sum_{b\in\mathcal{B}} \alpha_b \pi^{r_b} b$ with $r_b \in \mathbb{Z}_{\geq 0}$ and then applying the same combinations to the corresponding rows of T. We assume that the coefficients of the elements in $\mathcal{B}$ and the entries in T are represented π-adicly. Then, the multiplication by a π-power is just a shift of the coefficients and its cost can be neglected. Consequently, an augmentation-step can be seen as a $k_\mathfrak{p}$-linear combination of the vectors in $\mathcal{B}$ or the rows of T, respectively.

By Theorem 2.10 we can work out all computation with precision $\nu = O(\delta)$. Thus the entries in T can be considered modulo π^ν and therefore as polynomials in $k_\mathfrak{p}[\pi]$ of degree bounded by δ. Moreover the elements $b \in \mathcal{B}$ are given by $b = g(\theta)/\pi^{\omega(g(\theta))}$ with $g(x) \in (A/\pi^\delta A)[x]$. Therefore any augmentation-step can be performed by $O(n^2\delta)$ $\mathfrak{p}$-small operations. By Theorem 2.10 the number of all augmentation-steps is bounded by δ. As the result, the total cost of all augmentation-steps is equal to $O(n^2\delta^2)$ $\mathfrak{p}$-small operations. □

3. Computing p-integral bases of families of fractional ideals.

Let I be a fractional ideal of $\mathcal{O}$. Since $\mathcal{O}$ is a Dedekind domain I can be factored in a finite product of prime ideals $I = \prod_{\mathfrak{P}\in \mathrm{Max}(\mathcal{O})} \mathfrak{P}^{a_\mathfrak{P}}$ with integer exponents $a_\mathfrak{P}$. We denote by $I_\mathfrak{p} = \prod_{1\leq i\leq s} \mathfrak{P}_i^{a_{\mathfrak{P}_i}}$, the $\mathfrak{p}$-part of I. Clearly I and $I_\mathfrak{p}$ are rank n modules over A. The set $\{b_0, \ldots, b_{n-1}\} \subset I$ is called a $\mathfrak{p}$-integral basis of I if $\{b_0, \ldots, b_{n-1}\}$ forms an $A_\mathfrak{p}$-basis of $I_\mathfrak{p}$.

In this section we generalize the idea of the computation of a $\mathfrak{p}$-integral basis of $\mathcal{O}$ to the computation of a $\mathfrak{p}$-integral basis of fractional ideals. For any fractional ideal I there exists a maximal integer $a_I \leq 0$ such that the ideal $(\mathfrak{p}^{a_I} I_\mathfrak{p})^{-1}$ is integral. We call $I^*_\mathfrak{p} = \mathfrak{p}^{a_I} I_\mathfrak{p}$ the **normalization** of $I_\mathfrak{p}$ and I $\mathfrak{p}$-**normalized** if $I^*_\mathfrak{p} = I_\mathfrak{p}$. Clearly if $\{b_0, \ldots, b_{n-1}\}$ is an $A_\mathfrak{p}$-basis of $I^*_\mathfrak{p}$ then $\{\pi^{-a_I} b_0, , \pi^{-a_I} b_{n-1}\}$ is a $\mathfrak{p}$-integral basis of I. Hence it is sufficient to consider only $\mathfrak{p}$-normalized fractional ideals.

3.1. Basis Computation of fractional Ideals.

Let $I = \prod_{\mathfrak{P}\in \mathrm{Max}(\mathcal{O})} \mathfrak{P}^{a_\mathfrak{P}}$ be a $\mathfrak{p}$-normalized fractional ideal. We define for $z \in L$

$$\omega_I(z) = \Big\lfloor \min_{1\leq i\leq s} \Big\{ \frac{v_{\mathfrak{P}_i}(z) - a_{\mathfrak{P}_i}}{e_{\mathfrak{P}_i}} \Big\} \Big\rfloor.$$

Let $g(x) \in A[x]$ be a monic polynomial of degree $i < n$. Then g is called i-**maximal** in I (or just i-maximal) if $\omega_I(g(\theta)) \geq \omega_I(h(\theta))$ for all monic $h \in A[x]$ having the same degree as g.

One can generalize Theorem 2.2 to the following.

Theorem 3.1. *Let $b_0, \ldots, b_{n-1} \in L$ with*

$$b_i = \frac{g_i(\theta)}{\pi^{\omega_I(g_i(\theta))}}, \quad g_i \text{ is } i\text{-maximal in } I,$$

then $(b_0, \ldots, b_{n-1})$ is a triangular $\mathfrak{p}$-integral basis of I.

Analogous to Definition 2.3, one can generalize an augmentation-step by replacing ω by ω_I. Then Algorithm 1 can be adopted to compute a $\mathfrak{p}$-integral basis of I with a minor adjustment of the realization of an augmentation-step. Let $I_{\mathfrak{p}} = \prod_{1\le i\le s} \mathfrak{P}_i^{a_{\mathfrak{P}_i}}$. For $1 \le i \le s$ denote by $\mathcal{B}_i$ an $\hat{A}_{\mathfrak{p}}$-basis of $\iota_i(\mathfrak{P}_i^{a_{\mathfrak{P}_i}}) \subset L_{\mathfrak{P}_i}$. In particular $\mathcal{B}_i$ is a $K_{\mathfrak{p}}$-basis of $L_{\mathfrak{P}_i}$. We define by $C_{\mathcal{B}_i}(\alpha) \in K_{\mathfrak{p}}^{n_i}$ the coordinate vector of $\alpha \in L_{\mathfrak{P}_i}$ with respect to $\mathcal{B}_i$ and

$$\iota_I = (C_{\mathcal{B}_i} \circ \iota_i)_{1\le i\le s} : L \to K_{\mathfrak{p}}^n.$$

Then Lemma 2.6 and Theorem 2.7 can be stated by replacing ι by ι_I. Similar to Subsection 2.2, one should work with approximations $\Phi_i \in A[x]$ of the irreducible $\mathfrak{p}$-adic factors $f_{\mathfrak{P}_i}$ of f of precision $\nu \in \mathbb{Z}_{>0}$. Analogous we define

$$\iota_{I,\nu} : L \to K^n, \quad z \mapsto (C_{\mathcal{B}_{i,\nu}}(\iota_{i,\nu}(z)))_{1\le i\le s}, \tag{7}$$

where $\mathcal{B}_{i,\nu}$ denotes a $\mathfrak{p}$-integral basis of the fractional ideal $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$. One can prove analogously to Lemma 2.9 that $\iota_I(z)(\mathrm{mod}\pi^\nu) \equiv \iota_{I,\nu}(z)$ for all $z \in L$. Let $1 \le i \le s$ and denote by $\mathcal{B}'_{i,\nu}$ a $\mathfrak{p}$-integral basis of L_{Φ_i} the finite extension of K defined by the approximation Φ_i. Then one can easily derive $\mathcal{B}_{i,\nu}$ from $\mathcal{B}'_{i,\nu}$: We consider the fractional ideal $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$ and write

$$a_{\mathfrak{P}_i} = \tilde{a}_{\mathfrak{P}_i} + l_i(-e_{\mathfrak{P}_i}) \text{ with } l_i \in \mathbb{Z}_{\ge 0} \text{ and } -e_{\mathfrak{P}_i} < \tilde{a}_{\mathfrak{P}_i} \le 0. \tag{8}$$

Denote by $\tilde{\mathfrak{P}}_i = \iota_{i,\nu}(\mathfrak{P}_i)$. Let $\gamma_i \in L_{\Phi_i}$ such that $v_{\tilde{\mathfrak{P}}_i}(\gamma_i) = \tilde{a}_{\mathfrak{P}_i}$. Then, $\mathcal{B}_{i,\nu} = \gamma_i \pi^{-l_i} \cdot \mathcal{B}'_{i,\nu}$ is a $\mathfrak{p}$-integral basis of $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$. Note that one can choose $\gamma_i = \iota_{i,\nu}(\pi_i)^{\tilde{a}_{\mathfrak{P}_i}}$ for a uniformizer π_i of $\mathfrak{P}_i$, which can be computed along the Montes algorithm as a by-product.

Theorem 3.2. *Let $\delta_I = v_{\mathfrak{p}}([I : A[\theta]])$ and ν be an integer with $\nu \ge \delta_I$. If we replace in the augmentation-steps along Algorithm 1 the map ι by $\iota_{I,\nu}$ then the algorithm outputs a triangular $\mathfrak{p}$-integral basis of I and needs at most δ_I augmentation-steps. In particular this basis can be computed in*

$$O\left(n^3\delta_I + n^2\delta_I^2 + n^{1+\epsilon}\delta_I \log q + n^{1+\epsilon}\delta_I^{2+\epsilon}\right)$$

$\mathfrak{p}$-small operations.

Proof. Analogous to the proof of Theorem 2.10 one proves the first statement by replacing δ by δ_I. For the complexity statement one proceeds exactly as in Subsection 2.4 taking into account that the cost for the computation of $\mathcal{B}_{i,\nu}$ can be neglected as mentioned above. □

3.2. **Computation of bases of families of fractional ideals.** Let I and I' be two $\mathfrak{p}$-normalized fractional ideals of L with $I'_{\mathfrak{p}} \subset I_{\mathfrak{p}}$. In particular, let $I_{\mathfrak{p}} = \prod_{1\le i\le s} \mathfrak{P}^{a_{\mathfrak{P}_i}}$ and $I'_{\mathfrak{p}} = \prod_{1\le i\le s} \mathfrak{P}^{a'_{\mathfrak{P}_i}}$ with

$$a_{\mathfrak{P}_i} \equiv a'_{\mathfrak{P}_i} (\mathrm{mod}\ e_{\mathfrak{P}_i}), \quad 1 \le i \le s. \tag{9}$$

We explain how to determine a $\mathfrak{p}$-integral basis $\mathcal{B}_{I'}$ of I' along the process of computing a $\mathfrak{p}$-integral basis $\mathcal{B}_I$ of I. The basic idea is to run the Algorithm 1 with precision δ_I to compute first $\mathcal{B}_{I'}$. Then one just keeps on running the algorithm till $\mathcal{B}_I$ is obtained as below.

Assume that approximations Φ_i with precision $\nu = \delta_I$ have been computed. Then we determine $\mathfrak{p}$-integral bases $\mathcal{B}'_{i,\nu}$ for $\iota_{i,\nu}(\mathfrak{P}^{a'_{\mathfrak{P}_i}})$ as explained above. Let

$\iota_{I',\nu}$ be defined as in (7) with respect to the bases $\mathcal{B}'_{i,\nu}$. Now we can compute the vectors $\iota_{I',\nu}(\theta^j)$, for $1 \leq j \leq n-1$ and apply maximally $\delta_{I'} = v_{\mathfrak{p}}([I' : \mathcal{O}])$ augmentations-steps till obtaining $\mathcal{B}_{I'}$. That is we run Algorithm 1 to compute $\mathcal{B}_{I'}$ with precision $\delta_I \geq \delta_{I'}$. Now one has to calculate $\iota_{I,\nu}(b)$ for $b \in \mathcal{B}_{I'}$ and apply further augmentations-steps until receiving $\mathcal{B}_I$. By (9), any basis $\mathcal{B}_{i,\nu}$ for $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$ can be deduced by

$$\mathcal{B}_{i,\nu} = \pi^{l_i} \cdot \mathcal{B}'_{i,\nu},$$

with l_i such that $a_{\mathfrak{P}_i} = a'_{\mathfrak{P}_i} + l_i e_{\mathfrak{P}_i}$. In other words the basis $\mathcal{B}_{i,\nu}$ is up to a π-power equal to the basis $\mathcal{B}'_{i,\nu}$. Denote by T the matrix, which rows are given by $\iota_{I,\nu}(b)$ for $b \in \mathcal{B}_{I'}$ and let T' be the matrix having the rows $\iota_{I',\nu}(b)$ for $b \in \mathcal{B}_{I'}$. Then T is obtained from T' by multiplying it with a diagonal matrix whose diagonal entries are of the form π^{l_i}. Because we represent the entries in T and T' as polynomials in $k_{\mathfrak{p}}[\pi]$, computing T can be done at no cost by shifting the coefficients of the elements in T' adequately. Thus, $\mathcal{B}_I$ can be determined after maximally $\delta_I - \delta_{I'}$ augmentation-steps.

Clearly, the computation of both, a $\mathfrak{p}$-integral basis $\mathcal{B}_{I'}$ for I' and $\mathcal{B}_I$ for I, has the same complexity as computing just $\mathcal{B}_I$.

Lemma 3.3. *Let $I_{\mathfrak{p}} = \prod_{1 \leq i \leq s} \mathfrak{P}_i^{a_{\mathfrak{P}_i}}$ with $r_i = \lfloor -a_{\mathfrak{P}_i} / e_{\mathfrak{P}_i} \rfloor$. One can compute at the cost of*

$$O\left(n^3\delta_I + n^2\delta_I^2 + n^{1+\epsilon}\delta_I \log q + n^{1+\epsilon}\delta_I^{2+\epsilon}\right)$$

$\mathfrak{p}$-small operations triangular $\mathfrak{p}$-integral bases of $\sum_{1 \leq i \leq s} r_i + 1$ fractional ideals I' contained in I satisfying (9)

Proof. Let us show that there are $\sum_{1 \leq i \leq s} r_i + 1$ many ideals contained in I satisfying (9). Denote by $I_0 = \prod_{1 \leq i \leq s} \mathfrak{P}_i^{\tilde{a}_{\mathfrak{P}_i}}$, where the $\tilde{a}_{\mathfrak{P}_i}$ are satisfying (8). We define $I_{1,l} = I_0 \cdot \mathfrak{P}_1^{-le_{\mathfrak{P}_1}}$ with $l = 1, \ldots, r_1$. Additionally, we set $I_1 = I_{1,r_1}$ and

$$I_{2,l} = I_1 \cdot \mathfrak{P}_2^{-le_{\mathfrak{P}_2}}$$

with $l = 1, \ldots, r_2$. Inductively, let $I_{s-1} = I_{s-1,r_{s-1}}$ and

$$I_{s,l} = I_{s-1} \cdot \mathfrak{P}_s^{-le_{\mathfrak{P}_s}}$$

with $l = 1, \ldots, r_s$. Thus, for each $1 \leq i \leq s$ there are exactly r_i ideals contained in I satisfying (9) and I_0, which can be computed as a by-product while computing a $\mathfrak{p}$-integral basis of I with Algorithm 1. □

3.3. **Example.** We go back to Example 2.3. There we have computed the $\mathfrak{p}$-integral basis $\mathcal{B}_{I'} = (1, \theta, \frac{b_2^*}{t}, \frac{b_3^*}{t})$ for $I' = \mathcal{O}$, where $b_2^* = \theta^2 + 2\theta$ and $b_3^* = \theta^3 + 9\theta$. Using that data, one can compute a $\mathfrak{p}$-integral basis $\mathcal{B}_I$ for the fractional ideal $I = \mathfrak{P}_1^{-1}$. Clearly, $[I : A[\theta]] = [I : \mathcal{O}] \cdot [\mathcal{O} : A[\theta]] = \mathrm{N}_{L/K}(\mathfrak{P}_1) \cdot [\mathcal{O} : A[\theta]]$. The residual degree of $\mathfrak{P}_1$ is 2 and $v_{\mathfrak{p}}([\mathcal{O} : A[\theta]]) = 2$. It follows that

$$v_{\mathfrak{p}}([I : A[\theta]]) = 4.$$

The approximations Φ_1 and Φ_2 are computed with precision $\nu = 8$ that is sufficient for the computation of $\mathcal{B}_I$ by Theorem 3.2. The ramification index of $\mathfrak{P}_1$ satisfies $e_{\mathfrak{P}_1} = 1$, so we are now in the situation of (8). Therefore a $\mathfrak{p}$-integral basis $\mathcal{B}_{1,\nu}$ for $\iota_{1,\nu}(\mathfrak{P}_1)$ is given by $\pi^{-1}\mathcal{B}_1 = (1/t, \tilde{\theta}_1/t^2)$. Clearly $\mathcal{B}_{2,\nu} = \mathcal{B}_2$. Then one can compute the matrix T which rows represent $\iota_{I,\nu}(b)$ for $b \in \mathcal{B}_{I'}$ by manipulating the

matrix from (5). Since we obtained $\mathcal{B}_{1,\nu}$ by dividing the elements in $\mathcal{B}_1$ by t, the matrix T is given by

	$\mathcal{B}_{1,\nu}$		$\mathcal{B}_{2,\nu}$		ω
$\iota_{I,\nu}(1)$	t	0	1	0	0
$\iota_{I,\nu}(\theta)$	0	t^2	11	t	0
$\iota_{I,\nu}(b_2^*/t)$	$11t^2$	$2t$	$11t$	11	0
$\iota_{I,\nu}(b_3^*/t)$	0	$11t^3+9t$	$12t$	$11t^2+8$	0

We consider the lower term vectors in order to check if augmentation-steps are applicable:

$$M = \begin{bmatrix} \mathrm{LT}_0(\iota_{I,\nu}(1)) \\ \mathrm{LT}_0(\iota_{I,\nu}(\theta)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_2^*/t)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_3^*/t)) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 11 \\ 0 & 0 & 0 & 8 \end{bmatrix}.$$

As $\mathrm{rank}(M) = 2$, once can still apply augmentation-steps. According to Lemma 2.6 we can read out the augmentation-steps from M and deduce $b_1' = \theta + 2$ and $b_3' = b_3^*/t + 4b_2^*/t$. This results in:

	$\mathcal{B}_{1,\nu}$		$\mathcal{B}_{2,\nu}$		ω
$\iota_{I,\nu}(1)$	t	0	1	0	0
$\iota_{I,\nu}(b_1')$	2t	t^2	0	$1\ t$	1
$\iota_{I,\nu}(b_2^*/t)$	$11t^2$	$2t$	$11t$	11	0
$\iota_{I,\nu}(b_3')$	$5t^2$	$11t^3+4t$	$4t$	$11t^2$	1

with the lower term matrix

$$M = \begin{bmatrix} \mathrm{LT}_0(\iota_{I,\nu}(1)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_1')) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_2^*/t)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_3')) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 11 \\ 0 & 4 & 4 & 0 \end{bmatrix}.$$

Since $\mathrm{rank}(M) = 4$ no further augmentation-steps are applicable and

$$\mathcal{B}_I = \left(1, \frac{b_1'}{t}, \frac{b_2^*}{t}, \frac{b_3'}{t}\right) = \left(1, \frac{\theta+2}{t}, \frac{\theta^2+2\theta}{t}, \frac{\theta^3+4\theta^2+4\theta}{t^2}\right)$$

is a $\mathfrak{p}$-integral basis of I. Thus we computed $\mathcal{B}_I$ from computing $\mathcal{B}_{I'}$. In other words we first computed $\mathcal{B}_I$ and $\mathcal{B}_{I'}$ is implied as a by-product.

Acknowledgment

The authors would like to thank the Pacific Institute for the Mathematical Sciences (PIMS) for its financial support.

References

[1] J.-D. Bauch, E. Nart, H. D. Stainsby, *Complexity of OM factorizations of polynomials over local fields*, LMS J. Comput. Math. **16** (2013), 139–171.
[2] J. Bauch, *Lattices over Polynomial Rings and Applications to Function Fields*, arXiv:1601.01361v1 [math.NT], 2016.
[3] J.-D. Bauch, *Computation of integral bases*, J. Number Theory **165** (2016), 382–407.
[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Springer, 1993.
[5] J. Boehm, W. Decker, S. Laplagne, G. Pfister, *Computing integral bases via localization and Hensel lifting*, arXiv:1505.05054v1 [math.NT], 2015.
[6] D. Ford, P. Letard, *Implementing the Round Four maximal order algorithm*, J. de Théorie des Nombres de Bordeaux, **6** (1994), no. 1, 39–80.
[7] J. Guàrdia, E. Nart, *Local-to-global computation of integral bases without a previous factorization of the discriminant*, arXiv:1510.01995v1 [math.NT], 2015.
[8] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, J. Number Theory **147** (2015), 549–589.
[9] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.
[10] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Found. Comput. Math. **13** (2013), 729–762.
[11] J. Guàrdia, E. Nart, S. Pauli, *Single-factor lifting and factorization of polynomials over local fields*, J. Symb. Comput. **47** (2012), 1318–1346.
[12] K. Hensel, *Theorie der algebraischen Zahlen*, Teubner, Leipzig, Berlin, 1908.
[13] M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser, Bosten and Basel, 1993.
[14] W. M. Schmidt, *Construction and estimation of bases in function fields*, J. Number Theory **39** (1991), 181–224.
[15] H. D. Stainsby, *Triangular bases of integral closures*, J. Symb. Comput. **87** (July–August 2018), 140–175.
[16] A. Schönhage and V. Strassen, Schnelle Multiplikation großer Zahlen, Computing **7** (1971) 281-292.
[17] J.-P. Serre, *Corps locaux*, 4th corrected Edition, Hermann, Paris, 2004.
[18] M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, J. Symbolic Comput., **18(4)** 353363, 1994.

Department of Mathematics, Simon Fraser University
E-mail address: jbauch@sfu.ca

Department of Mathematics and Statistics, University of Calgary
E-mail address: hatran1104@gmail.com

COMPUTING NORMALIZERS OF TILED ORDERS IN $M_n(k)$

ANGELICA BABEI

Abstract. Tiled orders are a class of orders in matrix algebras over a non-Archimedean local field generalizing maximal and hereditary orders. Normalizers of tiled orders contain valuable information for finding type numbers of associated global orders. In this paper, we describe an algorithm for computing normalizers of tiled orders in matrix algebras.

1. Introduction

Let k be a non-Archimedean local field, R its valuation ring with maximal ideal $\mathfrak{p}$, and $B = M_n(k)$. An order Γ in B is a full R-lattice that is also a subring containing 1_B such that $\Gamma \otimes_R k = B$. Orders of the form $\Gamma = (\mathfrak{p}^{\nu_{ij}}) \subseteq M_n(k)$ containing a conjugate of $\mathrm{diag}(R, R, \ldots, R)$ have been of interest in many contexts. Such orders generalize maximal and hereditary orders, and are known as the graduated orders studied by Plesken in [11], the tiled orders studied by Fujita in [2] and [4], or the split orders studied by Hijikata in [7] and Shemanske in [14]. We will use the term "tiled order" for the rest of the paper.

The goal of this paper is finding ways to compute the normalizer $\mathcal{N}(\Gamma) = \{\xi \in GL_n(k) \,|\, \xi\Gamma\xi^{-1} = \Gamma\}$. Clearly $k^\times\Gamma^\times \subseteq \mathcal{N}(\Gamma)$, and the question we address in this paper is describing $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as a subgroup of S_n.

When $n = 2$, Hijikata [7] used knowledge of $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ to compute the trace formula of Hecke operators. Analogously, when one derives a trace formula for Brandt matrices [10], one obtains as a byproduct a means to compute class numbers of certain orders in quaternion algebras, some of whose localizations are tiled orders. More generally, given a central simple algebra over a global field and an order Γ in such an algebra, one can use information about the normalizer $\mathcal{N}(\Gamma_\nu)$ at each of the completions to compute the type number of the global order.

There has been some work describing the normalizer of tiled orders. In particular, for a tiled order Γ, Haefner and Pappacena [6] describe $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as a subgroup of the automorphisms of a directed multigraph. We will give a more complete description of the normalizer as the group of automorphisms of a certain valued quiver, as described by Roggenkamp and Wiedemann in [16], with an equivalent definition by Müller in [9].

Our algorithm for finding the normalizer of a tiled order Γ consists of five parts. First, we associate to Γ a new "centered" tiled order Γ_0, which reveals the structure of the normalizer more transparently. Second, we compute the valued quiver $Q_v(\Gamma_0)$ for the centered tiled order Γ_0 and we identify $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ with the automorphism group $\mathrm{Aut}(Q_v(\Gamma_0))$. We then partition the vertices of the valued quiver $Q_v(\Gamma_0)$ into sets with the same weights for incoming and outgoing arrows. This partition

The author would like to thank Thomas R. Shemanske for helpful conversations, and the reviewers for their useful comments.

allows us to embed the automorphism group of the valued quiver in a product of symmetric groups $S_{l_1} \times S_{l_2} \times \cdots \times S_{l_r} \subseteq S_n$. Finally, the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ is given by the elements in this product that permute the weights of the arrows.

2. Preliminaries

As we have said, an order Γ in $B = M_n(k)$ is a full R-lattice that is also a subring containing 1_B such that $\Gamma \otimes_R k = B$. It is known [12, Theorem 17.3] that every maximal order Λ in B is conjugate by an element in $B^\times$ to $M_n(R)$. The orders we are interested in are defined as follows.

Definition 1. *We say Γ is a tiled order if it contains a conjugate of the ring $diag(R, R, \ldots, R)$.*

We want to introduce a geometric framework in which a tiled order Γ is realized as a convex polytope C_Γ in a Euclidean space. This geometric realization will give a correspondence between the symmetries of the polytope C_Γ and elements of the normalizer. To do so, we now introduce a bit of the theory of affine buildings and how it relates to tiled orders as described in [14]. For further details the reader may wish to consult [1] and [5].

Let V be an n-dimensional vector space over k, so we identify B with $\mathrm{End}_k(V)$. Fixing a basis $\{e_1, e_2, \ldots, e_n\}$ for V, and letting L_0 be the free R-lattice generated by this basis, we can identify $\mathrm{End}_R(L_0)$ with the maximal order $\Lambda_0 = M_n(R)$. For any maximal order Λ, we have $\Lambda = \xi\Lambda_0\xi^{-1}$ for some $\xi \in B^\times$, so we can identify Λ with $\mathrm{End}_R(\xi L_0)$.

We say that two full R-lattices L_1 and L_2 in V are homothetic if $L_1 = aL_2$ for some $a \in k^\times$. Homothety of lattices is an equivalence relation, and we denote the homothety class of L by $[L]$. It is easy to see that $[L_1] = [L_2]$ if and only if $\mathrm{End}_R(L_1) = \mathrm{End}_R(L_2)$, so we can identify each homothety class of a lattice with a maximal order.

We construct the affine building for $SL_n(k)$ as follows. The vertices are the homothety classes of lattices, so by the remarks above we have identified homothety classes of lattices, vertices in the building, and maximal orders in B. Fixing a uniformizer $\pi \in R$, there is an edge between two vertices if there are lattices L_1 and L_2 in their respective homothety classes such that $\pi L_1 \subsetneq L_2 \subsetneq L_1$. The vertices of an m-simplex correspond to chains of lattices of the form $\pi L_1 \subsetneq L_2 \subsetneq \cdots \subsetneq L_{m+1} \subsetneq L_1$. The maximal $(n-1)$-simplices are called chambers.

Given a basis $\{e_1, e_2, \ldots, e_n\}$ as above, we have an associated subcomplex of the affine building for $SL_n(k)$, called an *apartment*. The vertices of the apartment are homothety classes of lattices of the form $L = R\pi^{m_1}e_1 \oplus R\pi^{m_2}e_2 \oplus \cdots \oplus R\pi^{m_n}e_n$, $m_i \in \mathbb{Z}$, which we encode by $[L] = [m_1, m_2, m_3, \ldots, m_n] = [0, m_2 - m_1, \ldots, m_n - m_1]$. Each apartment is an $(n-1)$-complex and a tessellation of $\mathbb{R}^{n-1}$.

Note that while conjugation changes bases and therefore the apartment we are working with, it doesn't change the structure of the normalizer. Conjugating if necessary, from now on we may and will assume that Γ actually contains $\mathrm{diag}(R, R, \ldots, R)$ and that we are in the apartment where $[0, 0, \ldots, 0]$ corresponds to $\Lambda_0 = M_n(R)$. In this case, by Proposition 2.1 in [14], $\Gamma = (\mathfrak{p}^{\nu_{ij}})$ where

$$\nu_{ij} + \nu_{jk} \geq \nu_{ik} \quad \text{for all } i, j, k \leq n, \quad \nu_{ii} = 0. \tag{1}$$

We denote by $M_\Gamma = (\nu_{ij})$ the *exponent matrix* of Γ. Let $[P_i] = [\nu_{1i}, \nu_{2i}, \ldots, \nu_{ni}]$ be the homothety class with entries the i-th column of M_Γ. By [11, II.4], the set $\{P_i\}_{i=1}^n$ represents a complete set of isomorphism classes of projective indecomposable left Γ-lattices. Similarly, define $[R_i] = [-\nu_{i1}, -\nu_{i2}, \ldots, -\nu_{in}]$ the homothety class with entries the i-th row of $-M_\Gamma$. Analogously, the set $\{R_i\}_{i=1}^n$ are a complete set of injective indecomposable Γ-lattices. We will observe this duality in other instances later in the paper.

For the sake of brevity, for the majority of the paper we will consider *nondegenerate* tiled orders, that is, tiled orders whose n columns correspond to n different homothety classes. The algorithm for finding elements of the normalizers for other orders is almost identical, and we will mention the modifications at the end of Section 4.

Recall our setting, where $\Gamma = (\mathfrak{p}^{\nu_{ij}})$ is a tiled order containing $\mathrm{diag}(R, R, \ldots, R)$. We associate to Γ a polytope C_Γ in the apartment the following way. The equations of the form $x_i - x_j = \nu \in \mathbb{Z}$, $1 \leq i, j \leq n$ determine hyperplanes in $\mathbb{R}^{n-1}$, and the hyperplanes $H_{ij} := x_i - x_j = \nu_{ij}$ with ν_{ij} given by the exponents of the tiled order are the bounding hyperplanes of a convex polytope, which we denote by C_Γ. In addition, the vertices given by $P_1, P_2, \ldots, P_n$ defined above are extremal points on C_Γ, and they uniquely determine Γ [15, Proposition 2.2]. From now on, we will refer to the homothety classes $[P_i] = [\nu_{1i}, \nu_{2i}, \ldots, \nu_{ni}] = [0, \nu_{2i} - \nu_{1i}, \ldots, \nu_{ni} - \nu_{1i}]$ as the *distinguished vertices* of C_Γ.

Example 1. Let Γ be the tiled order with exponent matrix $M_\Gamma = \begin{pmatrix} 0 & 1 & 4 \\ 2 & 0 & 3 \\ 2 & 2 & 0 \end{pmatrix}$. In Figure 1 we see the associated convex polytope C_Γ as determined by

$$-2 \leq x_1 - x_2 \leq 1$$
$$-2 \leq x_1 - x_3 \leq 4$$
$$-2 \leq x_2 - x_3 \leq 3,$$

or also as the convex hull of its distinguished vertices

$$[P_1] = [0, 2, 2], \quad [P_2] = [0, -1, 1] = [1, 0, 2], \quad [P_3] = [0, -1, -4] = [4, 3, 0].$$

Likewise, C_Γ is also the convex hull of the vertices given by the negative of the rows

$$[R_1] = [0, -1, -4], \quad [R_2] = [0, 2, -1] = [-2, 0, 3], \quad [R_3] = [0, 0, 2] = [-2, -2, 0].$$

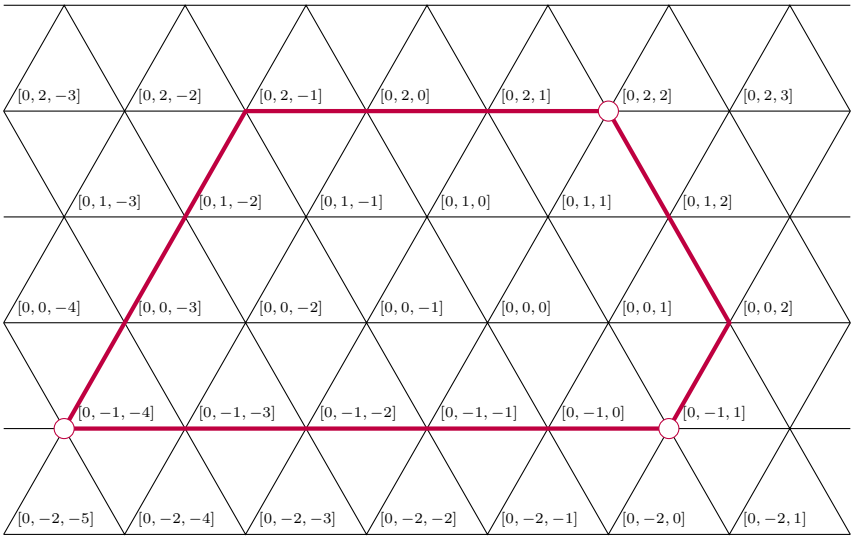
As described in [14] and expanded in [15], the vertices in C_Γ give an additional description of Γ:

Lemma 2 (Shemanske, [14], [15])**.** *Let Γ be a tiled order with convex polytope C_Γ. Then Γ is the intersection $\Gamma = \cap_{v \in C_\Gamma} \Lambda_v$ of maximal orders corresponding to the vertices in C_Γ. In addition, $\Gamma = \cap_{i=1}^n \Lambda_i$, where Λ_i are the maximal orders corresponding to the distinguished vertices of C_Γ.*

Proof. For the first assertion, see [14]. For a fixed $\ell \leq n$, we get $[P_\ell[= [\nu_{1\ell}, \nu_{2\ell}, \ldots, \nu_{n\ell}]$ and the associated maximal order is $\Lambda_\ell = (\mathfrak{p}^{\nu_{i\ell} - \nu_{j\ell}})$ by [14, Corollary 2.3]. Since $\nu_{ij} + \nu_{j\ell} \geq \nu_{i\ell}$, we can easily check that indeed $\Gamma = \cap_{i=1}^n \Lambda_i$. □

Therefore, given a tiled order Γ, we can obtain its convex polytope C_Γ, and in small enough dimensions, we can visualize it and use geometric intuitions to find

FIGURE 1.



elements of the normalizer. We summarize the arguments in [15, Sections 2, 3] that describe $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as the symmetries of C_Γ in the following:

Proposition 3 (Shemanske, [15])**.** *There is a homomorphism $\phi : \mathcal{N}(\Gamma) \to S_n$ with* $\ker(\phi) = k^\times\Gamma^\times$.

Proof. By [11, II.4], the columns of Γ are a complete set of isomorphism classes of indecomposable projective left Γ-lattices. Therefore, $\xi \in \mathcal{N}(\Gamma)$ will permute them, so $\mathcal{N}(\Gamma)$ acts on the set of n distinguished vertices. This gives the homomorphism $\phi : \mathcal{N}(\Gamma) \to S_n$. Next we show that the kernel $\ker(\phi) = k^\times\Gamma^\times$. It follows easily from Lemma 2 that $k^\times\Gamma^\times \subseteq \ker\phi$.

On the other hand, if ξ fixes each distinguished vertex $P_1, P_2, \ldots, P_n$, then ξ normalizes each maximal order $\Lambda_1, \Lambda_2, \ldots, \Lambda_n$ corresponding to each distinguished vertex, so $\xi \in \cap_{i=1}^n \mathcal{N}(\Lambda_i) = \cap_{i=1}^n k^\times\Lambda_i^\times$. We claim that $\cap_{i=1}^n k^\times\Lambda_i^\times = k^\times \cap_{i=1}^n \Lambda_i^\times = k^\times\Gamma^\times$, with the latter equality following from $\Gamma^\times = (\cap_{i=1}^n \Lambda_i)^\times$.

We proceed to prove the first equality. Clearly $k^\times \cap_{i=1}^n \Lambda_i^\times \subseteq \cap_{i=1}^n k^\times\Lambda_i^\times$. To show the nontrivial containment, suppose $\xi \in \cap_{i=1}^n k^\times\Lambda_i^\times$. Then we can write $\xi = \pi^{\nu_1}\lambda_1 = \pi^{\nu_2}\lambda_2 = \cdots = \pi^{\nu_n}\lambda_n$, where each $\lambda_i \in \Lambda_i^\times$. Taking the reduced norm, we get $N(\lambda_i) = 1$ for all $i \leq n$. Therefore $N(\xi) = \pi^{n\nu_1} = \pi^{n\nu_2} = \cdots = \pi^{n\nu_n}$, so $\xi = \pi^\nu\lambda$, where $\nu := \nu_1 = \nu_2 = \cdots = \nu_n$ and $\lambda \in \cap_{i=1}^n \Lambda_i^\times$. Then $\cap_{i=1}^n k^\times\Lambda_i^\times \subseteq k^\times \cap_{i=1}^n \Lambda_i^\times$ and the proposition holds.

□

By Proposition 3 we may view $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as a subgroup of S_n. Moreover, Fujita and Yoshimura show in the proof of their main theorem in [4] that every coset in $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ has a monomial representative. Their argument goes as follows.

Let $\{e_{ii} \,|\, 1 \leq i \leq n\}$ be the set of n primitive orthogonal idempotents of Γ, where e_{ii} is the $n \times n$ matrix with 1 in the (i, i) position and zero everywhere else. Given an automorphism $\varphi : \Gamma \to \Gamma$ acting by conjugation, so $\varphi(x) = \xi x \xi^{-1}$ for some $\xi \in M_n(k)$, by [8, Proposition 3, p. 77] there exists a unit $u \in \Gamma^\times$ and a

12 Jun 2018 23:12:31 PDT
Version 3 - Submitted to Open Book Series

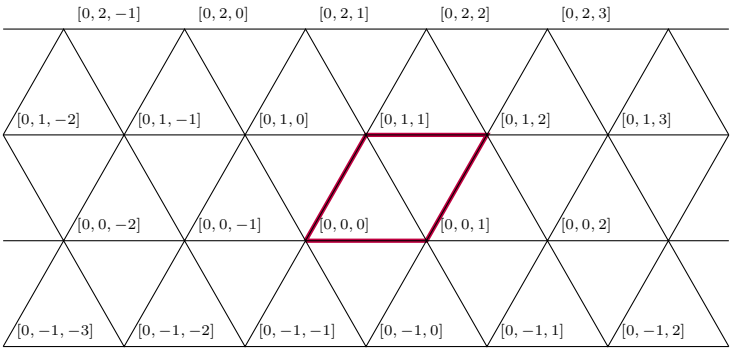
permutation matrix w such that $\xi e_{ii}\xi^{-1} = (uw)e_{ii}(uw)^{-1}$. Fujita and Yoshimura then proceed to find a diagonal matrix d such that $(dw)\Gamma(dw)^{-1} = \Gamma$, where ξ and dw represent the same coset in $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$.

Therefore, each coset in $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ has a monomial representative. Geometrically, conjugation by this monomial matrix corresponds to a product of reflections of the convex polytope C_Γ across hyperplanes in the apartment, so each element of $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ permutes the distinguished vertices of C_Γ by rigid motions. We will refer to elements of $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as the "symmetries of C_Γ", and we associate to $\xi \in \mathcal{N}(\Gamma)/k^\times\Gamma^\times$ the element $\sigma_\xi := \phi(\xi) \in S_n$.

For $n = 3$, C_Γ is 2-dimensional with symmetries a subgroup of S_3 as illustrated below.

Example 2. For $M_{\Gamma_1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 2 & 1 & 0 \end{pmatrix}$ we have the polytope in Figure 2. We see that the symmetries correspond to a fold, so $\mathcal{N}(\Gamma_1)/k^\times{\Gamma_1}^\times \cong \mathbb{Z}/2\mathbb{Z}$.

FIGURE 2.



Example 3. For $M_{\Gamma_2} = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & 2 & 0 \end{pmatrix}$ we have the polytope in Figure 3. We see that the symmetries correspond to a group of rotations of order 3, so $\mathcal{N}(\Gamma)/k^\times\Gamma^\times \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

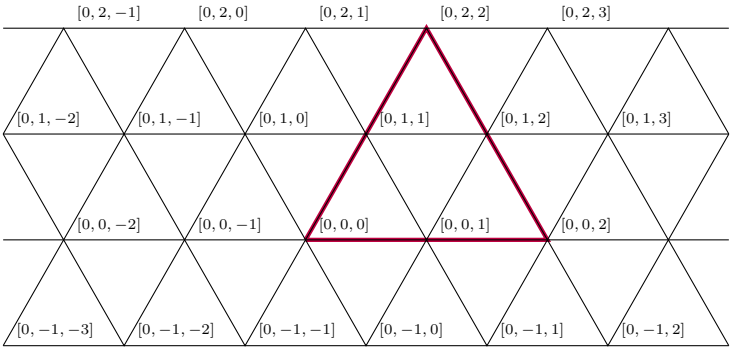
In unpublished work [17] (c.f. [11]), Zassenhaus introduced a set of *structural invariants* for tiled orders, defined by:

$$m_{ijk} = \nu_{ij} + \nu_{jk} - \nu_{ik}, \text{ for } 1 \leq i, j, k \leq n.$$

Note that since for any tiled order $\nu_{ij} + \nu_{jk} \geq \nu_{ik}$, structural invariants are nonnegative. In [15], these structural invariants encode the geometry of the convex polytope C_Γ. When $n = 3$, they correspond to side lengths of C_Γ and gaps between opposite sides; for example, in Example 2 we get $m_{231} = m_{312} = m_{132} = m_{213}$ are the four sides of length 1, and in Example 3 we see that $m_{213} = m_{321} = m_{132} = 2$ gives us the three sides of length 2.

In the general case, the m_{ijk} still encode geometric data.

FIGURE 3.



Lemma 4. *Fix $1 \leq i \leq n$. Then the distinguished vertex P_i is at the intersection of the (affine) hyperplanes $\bigcap_{j \neq i} H_{ji}$, where H_{ji} is given by the equation $x_j - x_i = \nu_{ji}$ when $j \neq i$.*

Proof. Since $P_i = [\nu_{1i}, \nu_{2i}, \ldots, \nu_{ni}] \sim [0, \nu_{2i} - \nu_{1i}, \ldots, \nu_{ni} - \nu_{1i}]$, P_i lies on each of the hyperplanes $x_i - x_j = (\nu_{ii} - \nu_{1i}) - (\nu_{ji} - \nu_{1i}) = -\nu_{ji}$, which are exactly our H_{ji} . □

Proposition 5. *For $i \neq j$, m_{ijk} is the number of hyperplanes between the vertex P_k and H_{ij}.*

Proof. Fix $i, j \leq n$. P_k is on the hyperplane $x_i - x_j = (\nu_{ik} - \nu_{1k}) - (\nu_{jk} - \nu_{1k}) = \nu_{ik} - \nu_{jk}$. Since Γ is an order, we have $\nu_{ij} + \nu_{jk} \geq \nu_{ik}$, so $\nu_{ik} - \nu_{jk} \leq \nu_{ij}$. Thus, the number of hyperplanes between H_{ij} (given by $x_i - x_j = \nu_{ij}$) and P_k is $\nu_{ij} - (\nu_{ik} - \nu_{jk}) = \nu_{ij} - \nu_{ik} + \nu_{jk} = m_{ijk}$.

In particular, if $j = k$ then $m_{ijk} = 0$, and by Lemma 4 P_k already is on H_{ik}, so the claim holds. □

Since the structural invariants encode geometric data, they determine the "shape" of the polytope, and in fact, in [17] (see [11, II.6]), Zassenhaus shows that the structural invariants (and therefore the "shape" of C_Γ) also encode the isomorphism class of the tiled order. Two tiled orders are isomorphic if they have the same structural invariants up to a permutation in S_n:

Proposition 6 (Zassenhaus, [17])**.** *Let Γ, Γ' be two tiled orders containing $\mathrm{diag}(R, R, \ldots, R)$, and let m_{ijk} and respectively, m'_{ijk} be their structural invariants. Then Γ and Γ' are isomorphic if and only if there exists $\sigma \in S_n$ such that $m'_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)}$ for all $1 \leq i, j, k \leq n$.*

Proof. This result is a particular case of Zassenhaus' result as described in [11, Prop. II.6]. Suppose the two orders are isomorphic. By the main theorem in [4, page 107], there exists a monomial matrix $\xi \in B^\times$ with $\Gamma' = \xi\Gamma\xi^{-1}$, where $\xi = (\pi^{\alpha_i}\delta_{\sigma(i)j})$ for some $\sigma \in S_n$, $\alpha_i \in \mathbb{Z}$, and δ_{ij} the Kronecker delta. Let $\Gamma = (\mathfrak{p}^{\nu_{ij}}), \Gamma' = (\mathfrak{p}^{\nu'_{ij}})$. Conjugating by ξ we deduce

$$\nu'_{ij} = \alpha_i - \alpha_j + \nu_{\sigma(i)\sigma(j)}.$$

Therefore,

$$\begin{aligned} m'_{ijk} &= \nu'_{ij} + \nu'_{jk} - \nu'_{ik} \\ &= \alpha_i - \alpha_j + \nu_{\sigma(i)\sigma(j)} + \alpha_j - \alpha_k + \nu_{\sigma(j)\sigma(k)} - \alpha_i + \alpha_k - \nu_{\sigma(i)\sigma(k)} \\ &= m_{\sigma(i)\sigma(j)\sigma(k)}. \end{aligned}$$

Conversely, suppose we have $\tau \in S_n$ such that $m'_{ijk} = m_{\tau(i)\tau(j)\tau(k)}$ for all $1 \leq i, j, k \leq n$. Then let $\alpha_i = \nu'_{i1} - \nu_{\tau(i)\tau(1)}$, $i \leq n$. Note that $\alpha_1 = 0$, and that also $\alpha_i = \nu_{\tau(1)\tau(i)} - \nu'_{1i}$, since

$$\nu'_{i1} + \nu'_{1i} = m'_{i1i} = m_{\tau(i)\tau(1)\tau(i)} = \nu_{\tau(i)\tau(1)} + \nu_{\tau(1)\tau(i)}.$$

If we let $\xi_{ij} = \pi^{\alpha_i}\delta_{\tau(i)j}$, then the exponents of $\xi\Gamma\xi^{-1}$ are $\alpha_i - \alpha_j + \nu_{\tau(i)\tau(j)}$, which give

$$\begin{aligned} \alpha_i - \alpha_j + \nu_{\tau(i)\tau(j)} &= \nu'_{i1} - \nu_{\tau(i)\tau(1)} - \nu_{\tau(1)\tau(j)} + \nu'_{1j} + \nu_{\tau(i)\tau(j)} \\ &= \nu'_{i1} + \nu'_{1j} - \nu'_{ij} + \nu'_{ij} - \nu_{\tau(i)\tau(1)} - \nu_{\tau(1)\tau(j)} + \nu_{\tau(i)\tau(j)} \\ &= m'_{i1j} + \nu'_{ij} - m_{\tau(i)\tau(1)\tau(j)} \\ &= \nu'_{ij}, \end{aligned}$$

and therefore $\xi\Gamma\xi^{-1} = \Gamma'$, so the two orders are isomorphic.

□

Therefore, the structural invariants determine the isomorphism class of an order. We can find the symmetries of a given isomorphism class, and more specifically the representatives of these symmetries in the normalizer for a given tiled order from its structural invariants as follows:

Proposition 7. *Let $\Gamma = (\mathfrak{p}^{\nu_{ij}})$ be a tiled order, $\{m_{ijk} \mid i, j, k \leq n\}$ its set of structural invariants, and $\phi : \mathcal{N}(\Gamma) \to S_n$ the homomorphism defined earlier. If, for some $\sigma \in S_n$, $m_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)}$ $\forall i, j, k \leq n$, then $\xi_\sigma = (\pi^{\alpha_i}\delta_{\sigma(i)j}) \in \mathcal{N}(\Gamma)$, where δ_{ij} is the Kronecker delta and $\alpha_i = \nu_{i1} - \nu_{\sigma(i)\sigma(1)}$. Furthermore, $\phi(\xi_\sigma) = \sigma$.*

Conversely, given $\xi \in \mathcal{N}(\Gamma)$, we have $m_{ijk} = m_{\sigma_\xi(i)\sigma_\xi(j)\sigma_\xi(k)}$, $\forall i, j, k \leq n$ where $\sigma_\xi := \phi(\xi)$.

Proof. Suppose that for some $\sigma \in S_n$, we have $m_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)}$ for all $i, j, k \leq n$. Setting $\xi_\sigma = (\pi^{\alpha_i}\delta_{\sigma(i)j})$ where $\alpha_i = \nu_{i1} - \nu_{\sigma(i)\sigma(1)}$, we get that $\xi_\sigma\Gamma\xi_\sigma^{-1} = (\mathfrak{p}^{\nu'_{ij}})$, where $\nu'_{ij} = \alpha_i - \alpha_j + \nu_{\sigma(i)\sigma(j)}$. The second step in the proof of Proposition 6 then gives

$$\nu'_{ij} = \alpha_i - \alpha_j + \nu_{\sigma(i)\sigma(j)} = \nu_{ij},$$

so indeed $\Gamma = \xi_\sigma\Gamma\xi_\sigma^{-1}$ and $\xi_\sigma \in \mathcal{N}(\Gamma)$. Since ξ_σ is a monomial matrix, the action of ξ_σ on the distinguished vertices of the convex polytope C_Γ is determined by reflections across affine hyperplanes as determined by σ, and therefore $\phi(\xi_\sigma) = \sigma$.

Now suppose $\xi \in \mathcal{N}(\Gamma)$. By the discussion after Proposition 3, we have a monomial matrix $\eta \in \mathcal{N}(\Gamma)$ that permutes the n distinguished vertices the same way ξ does, so define $\sigma = \sigma_\xi := \phi(\xi) = \phi(\eta)$. Since η is monomial, we can write it as $\eta = (\pi^{\alpha_i}\delta_{\sigma(i)j})$, where δ_{ij} is the Kronecker delta and $\alpha_i \in \mathbb{Z}$. The calculation in the first step in the proof of Proposition 6 shows that $m_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)}$ for all $i, j, k \leq n$.

□

Naive algorithm

Based on Proposition 7, a naive algorithm to find elements in the normalizer is to test each element of S_n to see whether $m_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)}$, $\forall i, j, k \leq n$. However, this method doesn't reveal much about the structure of the normalizer, or which subgroups of S_n are realizable as the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$. Our goal for the remainder of the paper is to develop an algorithm which in addition to computing elements of the normalizer, also reveals information about the structure of $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as a subgroup of S_n

3. Centered orders

We now proceed to refine the naive algorithm above. We begin by introducing some geometric motivation for the construction of the tiled centered order Γ_0 in Theorem 8.

Suppose we have $\sigma \in S_n$ a symmetry of C_Γ for a tiled order $\Gamma = (\mathfrak{p}^{\nu_{ij}})$. As discussed in the previous section, defining $\xi_\sigma = (\pi^{\alpha_i}\delta_{\sigma(i)j})$ where $\alpha_i = \nu_{i1} - \nu_{\sigma(i)\sigma(1)}$, gives ξ_σ a monomial matrix such that $\Gamma = \xi_\sigma\Gamma\xi_\sigma^{-1}$. Since ξ_σ is monomial, ξ_σ has a decomposition $\xi_\sigma = d \cdot w_\sigma$ where d is a diagonal matrix and w_σ is a permutation matrix. Geometrically, conjugation of Γ by a diagonal matrix amounts to a translation of C_Γ, while conjugation by a permutation matrix corresponds to a product of reflections of C_Γ across hyperplanes going through the origin $[0, 0, \ldots, 0]$.

Suppose we have a tiled order Γ_0 such that each monomial representative $\xi_\sigma \in \mathcal{N}(\Gamma_0)/k^\times\Gamma_0^\times$ has a decomposition $\xi = d\cdot w_\sigma$ with $d \in k^\times$ a scalar. By the discussion above, the origin $[0, 0, \ldots, 0]$ is fixed under each symmetry of C_{Γ_0}, in which case we say that Γ_0 is **centered**. The following theorem shows how given any tiled order Γ, we can associate to it a centered tiled order Γ_0 whose convex polytope C_{Γ_0} has the same symmetries in S_n as C_Γ. The advantage of this choice of centered tiled order is that we need only check relations between exponents in M_{Γ_0} instead of checking relations between the n^3 structural invariants $\{m_{ijk}\}$ to find all the symmetries. Since there are only $(n^2 - n)$ off-diagonal exponents, this will be a small step refining our algorithm.

Theorem 8. *Given a tiled order $\Gamma = (\mathfrak{p}^{\nu_{ij}})$ with structural invariants $\{m_{ijk} = \nu_{ij} + \nu_{jk} - \nu_{ik} \,|\, 1 \leq i, j, k \leq n\}$, define $\Gamma_0 = (\mathfrak{p}^{\mu_{ij}})$ where $\mu_{ij} = \sum_{k=1}^n m_{ijk}$. Then Γ_0 is a centered tiled order with structural invariants $\widetilde{m}_{ijk} = n \cdot m_{ijk}$ for all $1 \leq i, j, k \leq n$, and $\sigma \in S_n$ is a symmetry of C_Γ if and only if $\mu_{ij} = \mu_{\sigma(i)\sigma(j)}$.*

Proof. First we show Γ_0 is also a tiled order. Note that

$$\mu_{ii} = \sum_{k=1}^n m_{iik} = \sum_{k=1}^n (\nu_{ii} + \nu_{ik} - \nu_{ik}) = 0.$$

Γ_0 has structural invariants $\{\widetilde{m}_{ijl} \,|\, 1 \leq i, j, l \leq n\}$ given by

$$\begin{aligned}\widetilde{m}_{ijl} = \mu_{ij} + \mu_{jl} - \mu_{il} &= \sum_{k=1}^{n} m_{ijk} + \sum_{k=1}^{n} m_{jlk} - \sum_{k=1}^{n} m_{ilk} \\ &= \sum_{k=1}^{n} (m_{ijk} + m_{jlk} - m_{ilk}) \\ &= \sum_{k=1}^{n} (\nu_{ij} + \nu_{jk} - \nu_{ik} + \nu_{jl} + \nu_{lk} - \nu_{jk} - \nu_{il} - \nu_{lk} + \nu_{ik}) \\ &= \sum_{k=1}^{n} (\nu_{ij} + \nu_{jl} - \nu_{il}) \\ &= n \cdot m_{ijl} \geq 0,\end{aligned}$$

and since Γ itself is a tiled order and $m_{ijl} \geq 0$, it follows that Γ_0 is also a tiled order.

Next, we establish the bijection between the symmetries of C_Γ and the elements in S_n such that $\mu_{ij} = \mu_{\sigma(i)\sigma(j)}$. By Proposition 7 we need to show that

$$m_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)} \, \forall \, i,j,k \leq n \iff \mu_{ij} = \mu_{\sigma(i)\sigma(j)} \, \forall \, i,j \leq n.$$

Suppose $\sigma \in S_n$ such that $m_{ijk} = m_{\sigma(i)\sigma(j)\sigma(k)}$ for all $i,j,k \leq n$. Then

$$\mu_{\sigma(i)\sigma(j)} = \sum_{k=1}^{n} m_{\sigma(i)\sigma(j)k} = \sum_{\sigma(k)=1}^{n} m_{\sigma(i)\sigma(j)\sigma(k)} = \sum_{\sigma(k)=1}^{n} m_{ijk} = \sum_{k=1}^{n} m_{ijk} = \mu_{ij}.$$

Conversely, if $\mu_{ij} = \mu_{\sigma(i)\sigma(j)}$, then

$$n \cdot m_{ijk} = \widetilde{m}_{ijk} = \widetilde{m}_{\sigma(i)\sigma(j)\sigma(k)} = n \cdot m_{\sigma(i)\sigma(j)\sigma(k)},$$

so by Proposition 7, σ is a symmetry of C_Γ.

Finally, we show that Γ_0 is centered. To show that the origin $[0,0,\ldots,0]$ is within the convex polytope C_{Γ_0} is almost immediate, since the origin sits on each hyperplane $x_i - x_j = 0$. Each such hyperplane satisfies the condition $-\mu_{ji} \leq x_i - x_j \leq \mu_{ij}$ because $\mu_{ij}, \mu_{ji} \geq 0$ as sums of non-negative structural invariants.

Now we want to show that each symmetry of C_{Γ_0} fixes the origin. Note that since $\widetilde{m}_{ijk} = n \cdot m_{ijk}$, the symmetries of C_Γ are the same as the symmetries of C_{Γ_0}. Given a symmetry $\sigma \in S_n$ of C_{Γ_0}, by Proposition 7 we obtain a representative $\xi_\sigma \in \mathcal{N}(\Gamma_0)$ where $\xi_\sigma = (\pi^{\alpha_i}\delta_{\sigma(i)j})$ and $\alpha_i = \mu_{i1} - \mu_{\sigma(i)\sigma(1)} = 0$, since we have just shown that $\mu_{ij} = \mu_{\sigma(i)\sigma(j)}$ for all $i,j \leq n$. Therefore, ξ_σ is a permutation matrix and $\xi \in M_n(R)^\times$. Hence by [12], $\xi_\sigma \in M_n(R)^\times \subseteq k^\times M_n(R)^\times = \mathcal{N}(M_n(R))$. Conjugation by ξ_σ will fix $M_n(R)$, and therefore the σ will fix the vertex $[0,0,\ldots,0]$ associated to $M_n(R)$. Since this holds for every symmetry of C_{Γ_0}, Γ_0 is by definition centered. □

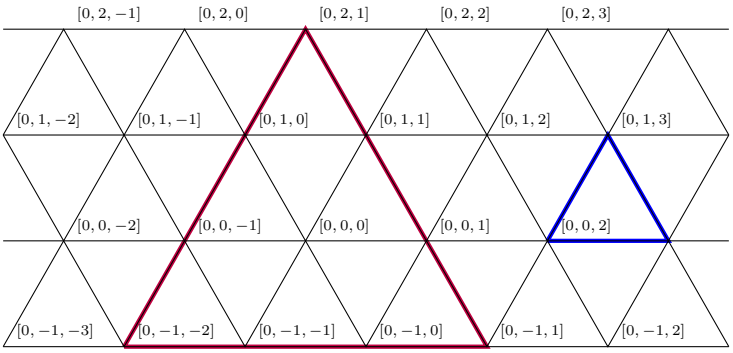
Example 4. Let Γ be the tiled order with $M_\Gamma = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & -2 \\ 3 & 3 & 0 \end{pmatrix}$, with C_Γ depicted in Figure 4 in blue. By Proposition 7, a representative ξ_σ in the normalizer

of Γ is

$$\xi_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \pi^{-2} \\ \pi^3 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \pi^{-2} & 0 \\ 0 & 0 & \pi^3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

The associated tiled order is Γ_0 with $M_{\Gamma_0} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$, with convex polytope depicted in Figure 4 in red. Since $\nu_{12} = \nu_{23} = \nu_{31}, \nu_{13} = \nu_{21} = \nu_{32}$, we get a representative of the normalizer $\xi_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

FIGURE 4.



For $n = 2$, Hijikata [7] showed that if Γ is nonmaximal, then $\mathcal{N}(\Gamma)/k^\times\Gamma^\times \cong \mathbb{Z}/2\mathbb{Z}$. For $n = 3$, $\mathcal{N}(\Gamma)/k^\times\Gamma^\times \subseteq S_3$ and in fact all subgroups of S_3 are realizable as symmetry groups of convex polytopes of tiled orders; we have seen two such subgroups in Examples 2 and 3. As n increases, there are however a number of subgroups of S_n that are not realizable as the symmetry group of C_Γ. In particular, we have the following easy corollary to Theorem 8:

Corollary 9. *Suppose we have a tiled order Γ and $\phi : \mathcal{N}(\Gamma) \to S_n$ the homomorphism defined earlier. If H is a 2-transitive subgroup of S_n, then $H \subseteq \phi(\mathcal{N}(\Gamma))$ implies $\mathcal{N}(\Gamma)/k^\times\Gamma^\times \cong S_n$.*

Proof. Let $\Gamma_0 = (\mathfrak{p}^{\mu_{ij}})$ be the associated centered order of Γ. H being 2-transitive means that given any pairs $(i, j), (k, l)$ with $i \neq j$ and $k \neq l$, there exists $\sigma \in H$ such that $\sigma(i) = k$ and $\sigma(j) = l$. Since H is contained in the image of the normalizer, $\mu_{ij} = \mu_{\sigma(i)\sigma(j)} = \mu_{kl}$. Therefore, all of the off-diagonal exponents are equal and $\mu_{ij} = \mu_{\sigma(i)\sigma(j)}\ \forall\sigma \in S_n$, so $\mathcal{N}(\Gamma_0)/k^\times\Gamma_0^\times \cong \mathcal{N}(\Gamma)/k^\times\Gamma^\times \cong S_n$. □

In this section we have shown that we can completely determine the normalizer of a tiled order by examining the exponents of its associated centered order. By Theorem 8, a refined algorithm to find elements in the normalizer is to go through the (n^2-n) off-diagonal elements to check for which $\sigma \in S_n$ we have $\mu_{ij} = \mu_{\sigma(i)\sigma(j)}$. This is of course a very small improvement, since we still have to check the above relations for elements $\sigma \in S_n$. In the next section we realize the symmetries of C_Γ

as the automorphism group of a directed valued multigraph, which can add to the efficiency of the above algorithm.

4. The normalizer as the automorphisms of a valued quiver

For our main algorithm, we will make use of a realization of the normalizer of a centered tiled order as the automorphism group of a certain valued directed multigraph, also known as a valued quiver.

We construct the *link graph* of $\Gamma = (\mathfrak{p}^{\nu_{ij}})$ as defined by Müller in [9]. Let $M_1, M_2, \ldots, M_n$ be the maximal 2-sided ideals of Γ. It can be shown that $M_\ell = (\mathfrak{p}^{r_{ij}})$ where $r_{ij} = \nu_{ij}$ if $\ell \neq i, j$, and $r_{\ell\ell} = 1$. The vertices of the link graph are labeled by the set $\{1, 2, \ldots, n\}$, and there is an arrow $\alpha : i \to j$ when $M_j M_i \neq M_j \cap M_i$ and the value associated to the arrow α is $v(\alpha) = \nu_{ij}$.

Remark. There is an equivalent way to define the link graph, by projective covers of the Jacobson radicals for the projective left Γ-lattices. However, these directed multigraphs have the arrows pointed the opposite direction. For more information, see [16] for the construction of the graphs and [2] for the proof of the equivalence of the two constructions.

To compute the link graph, we reproduce the following result from [3]:

Lemma 10 (Fujita, Oshima [3])**.** *Given a tiled order Γ, there is an arrow $i \to j$ in $Q_v(\Gamma)$ if $m_{jki} > 0$ for all $k \neq i, j$, and there is an arrow $i \to i$ if $m_{iki} > 1$ for all $k \neq i$.*

Proof. See [3, page 578]. However, note that Fujita and Oshima follow a convention where the arrows are pointed in the opposite direction. □

In [6, Lemmas 1,3], Haefner and Pappacena identify a subgroup of the automorphisms of the unvalued quiver $Q(\Gamma)$ with monomial representatives of $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$, which we have already found to be in bijection with the symmetries of C_Γ. In [6, Theorem 5], they prove that $\sigma \in \mathrm{Aut}(Q(\Gamma)) \subseteq S_n$ is liftable to a symmetry of C_Γ if the system

$$x_i - x_j = \nu_{ij} - \nu_{\sigma(i)\sigma(j)}, \quad i < j$$

has a solution $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$.

We can instead consider automorphisms of the valued quiver $Q_v(\Gamma)$. While as shown in [6, Example 2], the symmetries of C_Γ don't always give us an automorphism of $Q_v(\Gamma)$, they do when we have a centered tiled order:

Theorem 11. *Given a centered tiled order $\Gamma_0 = (\mathfrak{p}^{\nu_{ij}})$, there is a bijection between $Aut(Q_v(\Gamma_0))$ and the symmetries of C_Γ.*

Proof. Let $\sigma \in \mathrm{Aut}(Q_v(\Gamma_0))$. Then $\sigma \in \mathrm{Aut}(Q(\Gamma_0))$ is also an automorphism of the unvalued quiver, and Haefner and Papacenna have shown in [6, Theorem 5] that σ is liftable to an symmetry of C_{Γ_0} if and only if the linear system

$$x_i - x_j = \nu_{ij} - \nu_{\sigma(i)\sigma(j)}, \quad i < j$$

has a solution $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Since $\sigma \in \mathrm{Aut}(Q_v(\Gamma_0))$, for any valued arrow $\alpha : i \to j$, there is an arrow $\beta : \sigma(i) \to \sigma(j)$, and its value is $v(\beta) = v(\alpha)$. Since $v(\alpha) = \nu_{ij}$ and $v(\beta) = \nu_{\sigma(i)\sigma(j)}$, this implies $\nu_{ij} = \nu_{\sigma(i)\sigma(j)}$ for all $i, j \leq n$, so the system above has a solution $(0, 0, \ldots, 0) \in \mathbb{Z}^n$. Therefore, by [6], σ lifts to a symmetry of C_{Γ_0}.

Now suppose σ is a symmetry of C_{Γ_0}. By [6, Lemma 1], σ is an automorphism of the unvalued quiver $Q(\Gamma)$, so for a given arrow $\alpha : i \to j$, there is an arrow $\beta : \sigma(i) \to \sigma(j)$. To show that σ is also an automorphism of the valued quiver $Q_v(\Gamma_0)$, we need in addition that the value of $v(\beta) = v(\alpha)$. Since Γ_0 is centered, we have from Theorem 8 that $\nu_{ij} = \nu_{\sigma(i)\sigma(j)}$. But $v(\alpha) = \nu_{ij}$ and $v(\beta) = \nu_{\sigma(i)\sigma(j)}$, so the result follows. □

As described in Theorem 11, given the valued quiver of a centered order, we can determine the symmetries of C_Γ and therefore representatives of the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ by finding the automorphisms of the valued quiver. First note that given two vertices i and j, an automorphism of the quiver can only permute them if the incoming arrows of i have the same values as the incoming arrows of j, and the same holds for outgoing arrows. Therefore, for each vertex i, we can associate two multisets, one with values for incoming arrows, and the other with values for outgoing arrows. Then we need only look for elements in S_n that would permute both multisets when permuting vertices.

Finally, we summarize the algorithm, where given a tiled order $\Gamma = (\mathfrak{p}^{\nu_{ij}}) \subseteq M_n(k)$, we find $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ as a subgroup of S_n. We illustrate each step with an example.

Algorithm

(1) Given a tiled order Γ with exponent matrix $M_\Gamma = (\nu_{ij})$ and structural invariants $\{m_{ijk}\}_{1\le i,j,k\le n}$, compute its associated centered order Γ_0 with exponent matrix $M_{\Gamma_0} = (\mu_{ij})$ where $\mu_{ij} = \sum_{k=1}^n m_{ijk}$.

Example 5. Let Γ have exponent matrix $M_\Gamma = \begin{pmatrix} 0 & 1 & 3 & 3 & 1 \\ 2 & 0 & 2 & 3 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 2 & 2 & 2 & 2 & 0 \end{pmatrix}$

Γ_0 is given by $M_{\Gamma_0} = (\mu_{ij}) = \begin{pmatrix} 0 & 5 & 10 & 10 & 5 \\ 10 & 0 & 5 & 10 & 5 \\ 5 & 5 & 0 & 10 & 10 \\ 5 & 10 & 5 & 0 & 10 \\ 10 & 10 & 5 & 5 & 0 \end{pmatrix}$

(2) Find the valued quiver of Γ_0:
   (a) The vertices are $1, 2, \ldots, n$
   (b) Let $\tilde{m}_{ikj} = \mu_{ik} + \mu_{kj} - \mu_{ij} = n \cdot m_{ikj}$. For $i \neq j$, there is an arrow $\alpha : i \to j$ if $\tilde{m}_{ikj} > 0$ for all $k \neq i, j$. There is an arrow $\alpha : i \to i$ if $\tilde{m}_{iki} > 1$ for all $k \neq i$.
   (c) Given an arrow $\alpha : i \to j$, set $v(\alpha) = \mu_{ij}$.

   We can represent $Q_v(\Gamma_0)$ by the $n \times n$ matrix $M(Q_v(\Gamma_0)) = (a_{ij})$ where a_{ij} is blank if there is no arrow from i to j, and $a_{ij} = \mu_{ij}$ if there is an arrow $\alpha : i \to j$ and the value $v(\alpha) = \mu_{ij}$.

   Example 5. (cont.) The quiver $Q_v(\Gamma_0)$ is given by the following matrix:

$$\begin{pmatrix} 0 & & 10 & 10 & \\ 10 & 0 & 5 & & \\ & 5 & 0 & 10 & 10 \\ & & 5 & 0 & 10 \\ 10 & 10 & & & 0 \end{pmatrix}$$

(3) For each vertex i, let I_i be the multiset of incoming arrow values and O_i be the multiset of outgoing arrow values. Partition the sets $\{I_i\}_{i=1}^n$ and $\{O_i\}_{i=1}^n$ into equal multisets.

Example 5. (cont.) The multisets I_i are the columns of the above matrix, and the multisets O_i are the rows. Note that

$$I_1 = I_4 = I_5 = \{0, 10, 10\},\ I_2 = \{0, 5, 10\} \text{ and } I_3 = \{0, 5, 5, 10\},$$

so we partition the I_i's into $\{I_1, I_4, I_5\}$, $\{I_2\}$ and $\{I_3\}$. Since

$$O_1 = O_5 = \{0, 10, 10\},\ O_2 = O_4 = \{0, 5, 10\},\ \text{and } O_3 = \{0, 5, 10, 10\},$$

we partition the O_i's into $\{O_1, O_5\}$, $\{O_2, O_4\}$ and $\{O_3\}$.

(4) Consider the partition of the I_i's. An automorphism of the quiver can only permute vertices with the same values for incoming arrows, so if the sets in the partition have lengths $l_1, l_2, \ldots, l_q$, $\sum_{j=1}^q l_j = n$, then the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ is a subgroup of $S_{l_1} \times S_{l_2} \times \cdots \times S_{l_q} \subseteq S_n$, where each S_{l_i} is a copy of the symmetric group on l_i elements.

Now consider the partition of the O_i's. Similarly, an automorphism of the quiver can only permute vertices with the same values for outgoing arrows, so $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ is a subgroup of $S_{t_1} \times S_{t_2} \times \cdots \times S_{t_r} \subseteq S_n$, where $t_1, t_2, \ldots, t_r$ are the lengths of the sets in the partition of the O_i's and $\sum_{j=1}^r t_j = n$.

Therefore, the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ is a subgroup of $(S_{l_1} \times S_{l_2} \times \cdots \times S_{l_q}) \cap (S_{t_1} \times S_{t_2} \times \cdots \times S_{t_r})$.

Example 5. (cont.) Form the partitions in (4), we get that $\mathcal{N}(\Gamma)/k^\times\Gamma^\times \subseteq S_{\{1,4,5\}}$, where as usual $S_{\{1,4,5\}}$ is the symmetric group on the set $\{1, 4, 5\}$. Similarly, we get $\mathcal{N}(\Gamma)/k^\times\Gamma^\times \subseteq S_{\{1,5\}} \times S_{\{2,4\}}$. Therefore,

$$\mathcal{N}(\Gamma)/k^\times\Gamma^\times \subseteq S_{\{1,4,5\}} \cap (S_{\{1,5\}} \times S_{\{2,4\}}) = S_{\{1,5\}}.$$

(5) Check for which elements σ in the intersection found in (4) we have $a_{ij} = a_{\sigma(i)\sigma(j)}$, where a_{ij} are the entries in the matrix defined in (2). The union of these elements is the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$.

Example 5. (cont.) We need to check whether $a_{ij} = a_{\sigma(i)\sigma(j)}$ for $\sigma = (1, 5)$. Since a_{15} is blank, but $a_{51} = 10$, we conclude that σ is not a symmetry of C_Γ, so the $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ has to be trivial.

Remark. We now describe the modifications of our algorithm when Γ is degenerate, so some of the columns correspond to the same homothety classes of lattices. When we create the valued quiver in step (2), if columns P_i and P_j correspond to the same homothety class, we identify vertices i and j together. Therefore, after computing in step (5) the subgroup $H = \{\sigma \in S_n \mid a_{ij} = a_{\sigma(i)\sigma(j)}\}$ where a_{ij} are the entries in $M(Q_v(\Gamma_0))$, the normalizer $\mathcal{N}(\Gamma)/k^\times\Gamma^\times$ is the quotient of H by the product of the symmetric groups that permute each set of equivalent vertices.

References

[1] Peter Abramenko and Kenneth S. Brown. *Buildings: theory and applications*, volume 248. Springer Science & Business Media, 2008.

[2] Hisaaki Fujita. A remark on tiled orders over a local dedekind domain. *Tsukuba Journal of Mathematics*, 10(1):121–130, 1986.

12 Jun 2018 23:12:31 PDT
Version 3 - Submitted to Open Book Series

[3] Hisaaki Fujita and Akira Oshima. A tiled order of finite global dimension with no neat primitive idempotent. *Communications in Algebra*, 37(2):575–593, 2009.
[4] Hisaaki Fujita and Hiroshi Yoshimura. A criterion for isomorphic tiled orders over a local dedekind domain. *Tsukuba Journal of Mathematics*, 16(1):107–111, 1992.
[5] Paul B. Garrett. *Buildings and classical groups*. CRC Press, 1997.
[6] Jeremy Haefner and Christopher J. Pappacena. Automorphisms of tiled orders. *Linear Algebra and its Applications*, 347(1):275 – 282, 2002.
[7] Hiroaki Hijikata. Explicit formula of the traces of hecke operators for $\gamma_0(n)$. *J. Math. Soc. Japan*, 26(1):56–82, 01 1974.
[8] J. Lambek. *Lectures on Rings and Modules*. AMS Chelsea Publishing Series. American Mathematical Society, 2009.
[9] Bruno J. Müller. Localization in fully bounded noetherian rings. *Pacific J. Math.*, 67(1):233–245, 1976.
[10] Arnold Pizer. On the arithmetic of quaternion algebras II. *J. Math. Soc. Japan*, 28(4):676–688, 1976.
[11] Wilhelm Plesken. Group-rings of finite-groups over p-adic integers. *Lecture Notes in Mathematics*, 1026:1–149, 1983.
[12] Irving Reiner. *Maximal orders*, volume 38. Academic press London, 1975.
[13] Anne R. Schwartz and Thomas R. Shemanske. Maximal orders in central simple algebras and bruhat–tits buildings. *Journal of Number Theory*, 56(1):115–138, 1996.
[14] Thomas R. Shemanske. Split orders and convex polytopes in buildings. *Journal of Number Theory*, 130(1):101–115, 2010.
[15] Thomas R. Shemanske. Normalizers of graduated orders. 2016.
[16] Alfred Wiedemann and Klaus W. Roggenkamp. Path orders of global dimension two. *Journal of Algebra*, 80(1):113–133, 1983.
[17] Hans Zassenhaus. Graduated orders. 1975.

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: angelica.babei.gr@dartmouth.edu

12 Jun 2018 23:12:31 PDT
Version 3 - Submitted to Open Book Series

THE INVERSE GALOIS PROBLEM FOR p-ADIC FIELDS

DAVID ROE

Abstract. We describe a method for counting the number of extensions of $\mathbb{Q}_p$ with a given Galois group G, founded upon the description of the absolute Galois group of $\mathbb{Q}_p$ due to Jannsen and Wingberg. Because this description is only known for odd p, our results do not apply to $\mathbb{Q}_2$. We report on the results of counting such extensions for G of order up to 2000 (except those divisible by 512), for $p = 3, 5, 7, 11, 13$. In particular, we highlight a relatively short list of minimal G that do not arise as Galois groups. Motivated by this list, we prove two theorems about the inverse Galois problem for $\mathbb{Q}_p$: one giving a necessary condition for G to be realizable over $\mathbb{Q}_p$ and the other giving a sufficient condition.

1. Introduction

The inverse Galois problem is most commonly studied over $\mathbb{Q}$. There, a theorem of Shafarevich [13, Thm. 9.6.1; 18] shows that every solvable group is realizable as the Galois group of an extension of $\mathbb{Q}$. Attention has thus focused on simple groups, and many have been shown to be realizable; see [11] for background.

Over $\mathbb{Q}$, if a given group arises as a Galois group it will arise for infinitely many extensions. Thus the constructive version of the problem, finding extensions with a given Galois group, has been approached by the method of generic polynomials. A generic polynomial for a group G is a monic polynomial with coefficients in a function field $\mathbb{Q}(c_1, \ldots, c_n)$ so that every extension of $\mathbb{Q}$ with Galois group G will arise via specializing the c_i to elements of $\mathbb{Q}$. Even if G is realizable, it may not have a generic polynomial parameterizing all extensions.

Over $\mathbb{Q}_p$, for fixed p and G, there are only finitely many isomorphism classes of Galois extensions $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$. Thus, rather than trying to produce them via a generic polynomial, one could hope to enumerate them directly. As a first step toward such an enumeration, in this paper we study the less refined question of counting such K.

The counting and enumeration of p-adic fields has a rich history, mostly separate from the study of the inverse Galois problem. Rather than focusing on the Galois group, most approaches have studied the extensions of a given degree, or with a given degree and discriminant. Foundational work of Krasner [10, Thm. 2] gave counts for the number of extensions of degree n in a fixed algebraic closure, and Serre [16] gives a "mass formula" where the counts are weighted appropriately. More recently, Hou and Keating [7] and Monge [12] have described how to count isomorphism classes of extensions with prescribed ramification and inertia degrees.

2010 *Mathematics Subject Classification.* 12F12 (primary) 12Y05, 20C40, 11S15, 11Y40.
Key words and phrases. p-adic extensions, inverse Galois theory, profinite groups.
Supported by Simons Foundation grant 550033.

There has been some work on counting extensions with a given Galois group. When G is a p-group generated by d elements (minimally) and $k/\mathbb{Q}_p$ has degree n, Shafarevich [17] has obtained the following formula for the number of extensions of k with Galois group G, using his description of the maximal pro-p quotient of the absolute Galois group:

$$\frac{1}{|\mathrm{Aut}(G)|}\left(\frac{|G|}{p^d}\right)^{n+1}\prod_{i=0}^{d-1}(p^{n+1}-p^i). \tag{1}$$

The result only holds for k that do not contain the p-th roots of unity, but Yamagishi [20] has generalized it, obtaining a formula involving characters of G.

Other authors have pursued the problem of enumerating p-adic fields [9, 14] of a given degree. Theoretically, this would solve the problem of enumerating with a given Galois group, since one can determine from G the smallest degree where a field can have a normal closure with Galois group G. However, for many groups this degree is prohibitively large for the methods employed, since you also get many other, much larger, Galois groups at the same time.

In this paper, we count Galois extensions with Galois group G by exploiting the explicit description of the absolute Galois group of $\mathbb{Q}_p$. This approach has the benefit of completely avoiding computations with polynomials, allowing for a large number of groups to be considered. The downside is that we do not get any information on many invariants of number theoretic interest, such as the discriminant or the ramification filtration, beyond distinguishing between tame and wild inertia.

We have chosen to focus on the case of $\mathbb{Q}_p$ because it has the most intrinsic interest, and because the number of extensions grows exponentially with the absolute degree of the base field, as illustrated by (1). The calculations were performed using GAP [3] and SageMath [19], and the code can be found at `https://github.com/roed314/padicIGP`.

1.1. **Summary.** We begin Section 2 with the notion of a *potentially p-realizable group*, which encapsulates the obvious conditions on G that come from the first few steps of the ramification filtration. This notion is closed under quotients, and we conjecture that any potentially p-realizable group can be expressed as a semidirect product of its p-core and its tame quotient. This conjecture is supported by experimental evidence, and has consequences for the existence of subextensions complementary to the maximal tame subextension. We close with Section 2.2, where we give algorithms to test whether a group is potentially p-realizable and to enumerate such groups.

In Section 3 we review the structure of the absolute Galois group, which plays a key role in our approach to counting extensions. We use the description to show that our notion of potentially p-realizable has the property that any such group will be realized over some p-adic field k.

Section 4 describes the algorithms used to count extensions $K/\mathbb{Q}_p$ with a given Galois group G. We give an explicit enumeration in the case of abelian groups, since we need this as a base case for inductive lifting methods later. We then summarize the tame case, which follows from the well-known structure of the tame quotient of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Finally we give a lifting method for counting extensions for arbitrary G, and briefly discuss its runtime.

In Section 5 we apply the counting algorithms to the question of whether a potentially p-realizable group is actually realized over $\mathbb{Q}_p$. We start by listing

17 Jun 2018 21:12:55 PDT
Version 4 - Submitted to Open Book Series

minimal examples of groups that are unrealizable. We then proceed, in Section 5.2, to prove Theorems 5.3 and 5.4 giving one necessary and one sufficient condition for p-realizability. Both conditions relate to the structure of the p-core of G as a representation of the tame quotient.

1.2. **Notation and Terminology.** We work throughout with a prime $p \neq 2$ and a finite group G. There are some naturally defined subgroups of G that will play an important role throughout the paper. The p-core V of G is the intersection of all of the p-Sylow subgroups of G:

$$V = \bigcap_{P \ p\text{-Sylow}} P.$$

It is the maximal normal p-group inside G. The quotient $T = G/V$ has the structure of a metacyclic group (an extension of a cyclic group by a cyclic group), but not canonically. It acts on V by conjugation. We call G *tame* if V is trivial and $G = T$.

We will also use the Frattini subgroup W of V, defined as

$$W = V^p V'$$

where V' is the commutator subgroup of V. The quotient V/W is the maximal quotient of V that is an elementary abelian p-group. The action of T on V descends to an action on V/W, yielding a representation of T on an $\mathbb{F}_p$-vector space.

We will refer to groups by their ID in GAP's SmallGroups library [2] using the notation $n\mathrm{G}k$, where n is the order of G and k enumerates groups of that order.

Write $\mathcal{G}$ for the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

2. Potentially p-realizable groups

2.1. **The structure of p-adic Galois groups.** The structure of p-adic field extensions [4, Chapter 16] imposes constraints on the possible Galois groups that can arise. Any finite extension $K \supseteq \mathbb{Q}_p$ can be decomposed into a tower $K \supseteq K_t \supseteq K_u \supseteq \mathbb{Q}_p$, where $K_u/\mathbb{Q}_p$ is unramified, K_t/K_u is tame and totally ramified, and K/K_t is totally wildly ramified. When $K/\mathbb{Q}_p$ is Galois, this tower corresponds to the first parts of the ramification filtration on $G = \mathrm{Gal}(K/\mathbb{Q}_p)$:

$$G = G_{-1} \supseteq G_0 \supseteq G_1. \tag{2}$$

The fixed field of G_0 is the unramified subfield K_u and the quotient G/G_0 must be cyclic. The fixed field of G_1 is the tame subfield K_t and the quotient G_0/G_1 must be cyclic of order relatively prime to p. Finally, $G_1 \cong \mathrm{Gal}(K/K_t)$ is a p-group. Moreover, G_0 and G_1 are normal subgroups of G.

By a theorem of Iwasawa [8, Thm. 2], the Frobenius element of G/G_0 acts on G_0/G_1 by raising to the pth power.

Definition 2.1. A group G is *potentially p-realizable* if it has a filtration $G \supseteq G_0 \supseteq G_1$ so that

(1) G_0 and G_1 are normal in G,
(2) G/G_0 is cyclic, generated by some $\sigma \in G$,
(3) G_0/G_1 is cyclic of order relatively prime to p, generated by some $\tau \in G_0$,
(4) $\tau^\sigma = \tau^p$,
(5) G_1 is a p-group.

We will call such a filtration on G a *tame structure*. A group G is *p-realizable* if there exists an extension $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$.

17 Jun 2018 21:12:55 PDT
Version 4 - Submitted to Open Book Series

Remark 2.2. By the discussion above, any p-realizable group is potentially p-realizable, justifying the terminology. We will also see in Proposition 3.2 that if G is potentially p-realizable then it arises as a Galois group after some finite extension, conforming with the common usage of "potentially."

Remark 2.3. Since every p-group is nilpotent, the condition that G is potentially p-realizable implies that G is solvable. However, some groups G may have multiple tame structures. The simplest example is $G = C_2$ and p odd, where we can take $G_0 = G$ or $G_0 = 1$. An example with varying G_1 is $G = C_{p^2}$, where we can take $G_0 = G_1 = C_p$ or $G_0 = G_1 = 1$.

Proposition 2.4. *Any quotient of a potentially p-realizable group is potentially p-realizable.*

Proof. Suppose G has tame structure $G \supseteq G_0 \supseteq G_1$ and $N \trianglelefteq G$. It suffices to show that $G/N \supseteq G_0N/N \supseteq G_1N/N$ is a tame structure on G/N.

By the third isomorphism theorem, $(G/N)/(G_0N/N) \cong G/(G_0N)$ is a quotient of G/G_0 and thus cyclic, generated by the image of σ. The natural map $G_0 \to (G_0N/N)/(G_1N/N) \cong (G_0N)/(G_1N) \cong G_0/(G_1(G_0 \cap N))$ has kernel containing G_1, showing that $(G_0N/N)/(G_1N/N)$ is cyclic and generated by the image of τ.

Since the relation $\tau^\sigma = \tau^p$ holds in G, it also holds for the images of σ and τ in G/N. Finally, $G_1N/N \cong G_1/(G_1 \cap N)$ is a p-group since G_1 is. □

If G is potentially realizable, the maximal choice for G_1 is the p-core V. We may always enlarge a tame structure on G to make $G_1 = V$:

Proposition 2.5. *If $G \supseteq G_0 \supseteq G_1$ is a tame structure on G, so is $G \supseteq G_0V \supseteq V$.*

Proof. Since G_0 and V are normal subgroups of G, so is G_0V. Moreover, $G/(G_0V)$ is a quotient of G/G_0 and thus cyclic generated by the same $\sigma \in G$. Since the order of G_0/G_1 is prime to p, $G_0 \cap V = G_1$ and the second isomorphism theorem implies that $(G_0V)/V \cong G_0/G_1$ with the image of τ still generating $(G_0V)/V$. □

Define $T = G/V$, the smallest possible tame quotient of G.

Conjecture 2.6. If G is potentially p-realizable, then $G \cong V \rtimes T$.

The conjecture holds for all potentially p-realizable groups G with $p \in \{3, 5, 7, 11, 13\}$ and $|G| \leq 2000$. It also holds when T has order prime to p, by the Schur-Zassenhaus theorem. Note that we may not replace V with an arbitrary G_1, as the example of $C_{p^2} \supseteq C_p \supseteq C_p$ shows. Moreover, attempting to decompose the pieces further fails. The tame quotient T is not necessarily the semidirect product of G_0/G_1 by G/G_0: the quaternion group of order 8 is p-realizable for $p \equiv 3 \pmod 4$ but not a semidirect product of cyclic subgroups.

The conjecture has an interesting corollary for p-adic fields.

Corollary 2.7. *Assume Conjecture 2.6 holds, and suppose that $K/\mathbb{Q}_p$ is Galois. If $K_t/\mathbb{Q}_p$ is the maximal tamely ramified subextension of $K/\mathbb{Q}_p$ and $\mathrm{Gal}(K/K_t)$ is the p-core of $\mathrm{Gal}(K/\mathbb{Q}_p)$ then there is a totally wildly ramified complement $K_0/\mathbb{Q}_p$ with $K = K_0K_t$.*

2.2. **Enumerating small examples.** The first step toward counting p-adic fields by Galois group is computing a list of potential G. Since GAP's database of small groups [2] can identify groups of order n for $n \leq 2000$ except $n = 512, 1024, 1536$, groups of these orders were screened.

17 Jun 2018 21:12:55 PDT
Version 4 - Submitted to Open Book Series

When n is prime to p, we may use the classification of metacyclic groups [5, Lemma 2.1] to screen G. This process is described in Algorithm 1.

Algorithm 1: Finding potentially p-realizable groups: the tame case

Input : An integer n
Output: The list of potentially p-realizable groups of order n with trivial G_1

```
groups = [];
for positive k, m with n = k · m do
    if m divides p^k − 1 then
        step = m / gcd(m, p − 1);
        for ℓ from 0 to m by step do
            Find the GAP id of ⟨x, y | x^k = y^ℓ, y^m = 1, y^x = y^p⟩;
            Add id to groups if not present;
return sorted(groups);
```

When n has p-adic valuation 1, we can build groups as extensions of metacyclic groups. Any group of order n will arise either as an extension of a group of order n/p by C_p, or as a metacyclic group produced by Algorithm 1. The extensions are computable using GAP's `Extensions` method, and we describe the process in Algorithm 2.

Algorithm 2: Finding potentially p-realizable groups: valuation 1

Input : An integer n with $v_p(n) = 1$
Output: The list of potentially p-realizable groups of order n

```
groups = [];
foreach tame group T of order n/p do
    foreach homomorphism φ from T to Aut(C_p) do
        foreach group G in Extensions(T, φ) do
            if x and y lift to elements of G satisfying the tame relation then
                Find the GAP id of G;
                Add id to groups if not present;
foreach tame group T of order n do
    Find the id of T;
    Add id to groups if not present;
return sorted(groups);
```

When n has larger p-adic valuation, this extension method becomes more complicated, since there are more possibilities for V. Moreover, some of the possible V are not elementary abelian p-groups, so GAP's `Extensions` method does not apply. While it would be possible to try to construct the extensions manually using GAP's `GrpConst` package [1], in practice it suffices to check whether each group in the small group database [2] with order n is potentially p-realizable using Algorithm 3.

Algorithm 3: Determining whether a group is potentially p-realizable

Input : A group G
Output: Whether or not G is potentially p-realizable.

```
V = PCore(G);
T = G/ V;
if IsCyclic(T) then
    return True;
D = DerivedSubgroup(G);
if IsCyclic(D) then
    for N in NormalSubgroupsContaining(D) do
        if IsCyclic(N) and IsCyclic(G/N) then
            Let e be the order of N and f the order of G/N;
            Let a be the exponent in the conjugation action of G/N on N;
            Find b with a^b ≡ p (mod e), or continue if not possible;
            Let m be the order of a (mod e);
            if gcd(m, b, f) = 1 then
                return True;
return False;
```

3. The absolute Galois group of a local field

Our approach to counting p-adic fields rests on the following description of the absolute Galois group of $\mathbb{Q}_p$. Let $p \neq 2$, k be a p-adic field, $N = [k : \mathbb{Q}_p]$, q the cardinality of the residue field of k, and p^s the order of the group of p-power roots of unity in the maximal tame extension k^t/k. Choose $g, h \in \mathbb{Z}_p$ with

$$\zeta^\sigma = \zeta^g, \zeta^\tau = \zeta^h \text{ for } \zeta \in \mu_{tr},$$

where $\sigma, \tau \in \mathrm{Gal}(k^t/k)$ with $\tau^\sigma = \tau^q$ as in [8], and μ_{tr} the p-power roots of unity in k^t.

Let $\pi = \pi_p$ be the element of $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ with coordinate 1 in the $\mathbb{Z}_p$-component and 0 in the $\mathbb{Z}_\ell$ components for $\ell \neq p$. Then for x, y in a profinite group[1], set

$$\langle x, y \rangle = (x^{h^{p-1}} y x^{h^{p-2}} y \cdots x^h y)^{\frac{\pi}{p-1}}.$$

Theorem 3.1 ([13, Thm. 7.5.14])**.** *The absolute Galois group* $\mathrm{Gal}(\bar{k}/k)$ *is isomorphic to the profinite group generated by* $N + 3$ *generators* $\sigma, \tau, x_0, \ldots, x_N$*, subject to the following conditions and relations.*

(1) *The closed subgroup topologically generated by* $x_0, \ldots, x_N$ *is normal in* G *and is a pro-p-group.*
(2) *The elements* σ, τ *satisfy the tame relation*
$$\tau^\sigma = \tau^q.$$
(3) *The generators satisfy the following wild relation. If* N *is even then*
$$x_0^\sigma = \langle x_0, \tau \rangle^g x_1^{p^s} [x_1, x_2][x_3, x_4] \ldots [x_{N-1}, x_N].$$

[1]See [15], especially sections 3.3 and 4.1, for relevant background on profinite groups.

If N is odd then

$$x_0^\sigma = \langle x_0, \tau\rangle^g x_1^{p^s}[x_1, y_1][x_2, x_3]\dots[x_{N-1}, x_N],$$

where g and s are defined above and y_1 is an explicit element in the span of x_1, σ, and τ, specified below when $k = \mathbb{Q}_p$.

We will mostly be interested in the case where $k = \mathbb{Q}_p$; recall that we write $\mathcal{G}$ for $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Now $q = p$, $g = 1$ and h is a $(p-1)$st root of unity in $\mathbb{Z}_p$. In order to define y_1, let $\mathbb{Q}_p^t$ be the maximal tamely ramified extension of $\mathbb{Q}_p$ and define $\beta : \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p) \to \mathbb{Z}_p^\times$ by setting $\beta(\sigma) = 1$ and $\beta(\tau) = h$. For ρ in the subgroup of $\mathcal{G}$ generated by σ and τ and $x \in \mathcal{G}$, set

$$\{x, \rho\} = (x\rho^2 x^{\beta(\rho)}\rho^2 \dots x^{\beta(\rho^{p-2})}\rho^2)^{\frac{\pi}{p-1}}.$$

Let $\pi_2 \in \hat{\mathbb{Z}}$ be the element with $\pi_2\hat{\mathbb{Z}} = \mathbb{Z}_2$, and set $\tau_2 = \tau^{\pi_2}$ and $\sigma_2 = \sigma^{\pi_2}$. Set

$$y_1 = x_1^{\tau_2^{p+1}}\{x_1, \tau_2^{p+1}\}^{\sigma_2\tau_2^{(p-1)/2}}\{\{x_1, \tau_2^{p+1}\}, \sigma_2\tau_2^{(p-1)/2}\}^{\sigma_2\tau_2^{(p+1)/2}+\tau_2^{(p+1)/2}}. \tag{3}$$

The wild relation for $\mathbb{Q}_p$ then becomes

$$x_0^\sigma = \langle x_0, \tau\rangle x_1^p[x_1, y_1] \tag{4}$$

We can use this description of absolute Galois groups to show that any potentially p-realizable group occurs as a Galois group over some k with $k/\mathbb{Q}_p$ finite.

Proposition 3.2. *If G is potentially p-realizable and V/W has dimension m then G will be realized over k if $[k : \mathbb{Q}_p] \geq 2m + 1$.*

Proof. It suffices to exhibit a surjective homomorphism $\mathrm{Gal}(\bar{k}/k) \to G$, which we define by specifying the images of the generators. Map $x_0, x_1, x_3, x_5, \dots, x_{2m+1}$ and $x_{2m+2}, \dots, x_N$ to 1. Then the wild relation is automatically satisfied, and we may freely choose the images of $x_2, \dots, x_{2m}$. As long as we map them to elements of V that project to an $\mathbb{F}_p$-basis of V/W, Burnside's basis theorem implies that they will generate V. The fact that G is potentially p-realizable then implies that we may extend this homomorphism to a surjective map on all of $\mathrm{Gal}(\bar{k}/k)$. □

Note that one can decrease $2m + 1$ in some cases using the representation of T on V, and even then this bound is certainly not sharp.

4. Counting p-adic fields

4.1. **Parameterizing extensions.** Following [20], we count the extensions of $\mathbb{Q}_p$ with Galois group G by counting the surjections $\mathcal{G} \to G$, modulo automorphisms of G. We can then translate the description of $\mathcal{G}$ from Theorem 3.1 to a counting problem in G. Let n be the order of G and factor $n = u_p p^r = u_2 2^s$ with $(u_p, p) = 1$ and u_2 odd. Using the Chinese remainder theorem, define integers a and b so that

$$\begin{aligned} a &= 0 \pmod{u_p} & \qquad (p-1)a &= 1 \pmod{p^r} \\ b &= 0 \pmod{u_2} & \qquad b &= 1 \pmod{2^s}. \end{aligned}$$

Since the images of x_0 and x_1 have p-power order, they lie in V.

Definition 4.1. Define T_G to be the set of pairs $(\sigma, \tau) \in G^2$ so that

(1) $\tau^\sigma = \tau^p$,
(2) the images of σ and τ in G/V generate G/V.

Define X_G to be the set of quadruples $(\sigma, \tau, x_0, x_1) \in G^4$ so that

(1) $\tau^\sigma = \tau^p$,
(2) $x_0, x_1 \in V$,
(3) σ, τ, x_0, x_1 generate G,
(4) $x_0^\sigma = \langle x_0, \tau \rangle x_1^p [x_1, y_1]$,

where y_1 is defined as in (3).

Note that we may compute the projections $\pi/(p-1)$ and π_2 by raising to the a and b powers respectively.

Proposition 4.2. *The Galois extensions of $\mathbb{Q}_p$ with Galois group G are in bijection with the orbits of X_G under the action of* $\mathrm{Aut}(G)$.

Proof. Finite extensions K of $\mathbb{Q}_p$ within a fixed algebraic closure of $\mathbb{Q}_p$ correspond to finite index subgroups H_K of $\mathcal{G}$. The condition that K is Galois with Galois group G translates to the condition that H_K is normal with $\mathcal{G}/H_K \cong G$. Different subgroups H cannot yield isomorphic K since an isomorphism of fields would extend to an automorphism of $\bar{\mathbb{Q}}_p$ conjugating one H to the other, which is impossible since both are normal. Finally, elements of X_G correspond to homomorphisms $\mathcal{G} \to G$ by the description of $\mathcal{G}$ in Theorem 3.1, and the kernel of such a homomorphism is preserved by composition with an automorphism of G. □

We will be inductively constructing representatives for the orbits of $\mathrm{Aut}(G)$ on X_G; write Y_G for a choice of such representatives. Then Y_G will be in bijection with the extensions of $\mathbb{Q}_p$ with Galois group G.

4.2. **Abelian groups.** When G is abelian, the wild relation simplifies to $x_0 = x_1^p$. Thus x_0 is determined by x_1, and the wild relation imposes no constraint on x_1. The order of τ must divide $p-1$, the order of x_1 must be a power of p, and the three elements σ, τ, and x_1 must generate G.

Write

$$G \cong \prod_\ell \prod_{i=1}^{m_\ell} \mathbb{Z}/\ell^{n_{\ell,i}}\mathbb{Z}, \tag{5}$$

where $n_{\ell,1} \leq \cdots \leq n_{\ell,m_\ell}$ for each ℓ. We can enumerate the elements of X_G as a function of the $n_{\ell,i}$. Let α_ℓ be the element of G with a 1 in the $\ell, 1$ component and 0s elsewhere, and let β_ℓ be the element with a 1 in the $\ell, 2$ component and 0s elsewhere. Since we will be analyzing the ℓ-components separately, we drop ℓ from the notation, writing a for $n_{\ell,1}$, b for $n_{\ell,2}$, α for α_ℓ and β for β_ℓ.

(1) In the case $m_\ell \geq 3$, set $c_\ell = 0$ and $C_\ell = \{\}$.
(2) In the case $m_\ell = 2$, if $a \neq b$ and $\ell = p$, set $c_\ell = 2$ and $C_\ell = \{(\alpha, 0, p\beta, \beta), (\beta, 0, p\alpha, \alpha)\}$.
(3) In the case $m_\ell = 2$, if $a \neq b$ and ℓ^b divides $p-1$, set $c_\ell = 2$ and $C_\ell = \{(\alpha, \beta, 0, 0), (\beta, \alpha, 0, 0)\}$.
(4) In the case $m_\ell = 2$, if $a = b$ and $\ell = p$, set $c_\ell = 1$ and $C_\ell = \{(\alpha, 0, p\beta, \beta)\}$.
(5) In the case $m_\ell = 2$, if ℓ^a divides $p-1$ but case (3) does not apply, set $c_\ell = 1$ and $C_\ell = \{(\beta, \alpha, 0, 0)\}$.
(6) In the case $m_\ell = 2$, if $\ell \neq p$ and ℓ^a does not divide $p-1$, set $c_\ell = 0$ and $C_\ell = \{\}$.
(7) In the case $m_\ell = 1$, if $\ell = p$, set $c_\ell = p^{a-1}(p+1)$ and $C_\ell = \{(\alpha, 0, pk\alpha, k\alpha) : 0 \leq k < p^a\} \cup \{(pk\alpha, 0, p\alpha, \alpha) : 0 \leq k < p^{a-1}\}$.
(8) In the case $m_\ell = 1$, if ℓ^a divides $p-1$, set $c_\ell = \ell^{a-1}(\ell+1)$ and $C_\ell = \{(\alpha, k\alpha, 0, 0) : 0 \leq k < \ell^a\} \cup \{(pk\alpha, \alpha, 0, 0) : 0 \leq k < \ell^{a-1}\}$.

(9) In the case $m_\ell = 1$, if ℓ^a does not divide $p-1$, set $c_\ell = \gcd(\ell^a, p-1)$ and $C_\ell = \{(\alpha, \frac{\ell^a}{c_\ell} k\alpha, 0, 0) : 0 \le k < c_\ell\}$.

Proposition 4.3. *Let G be abelian, with elementary factors as in* (5)*. Then the number of Galois extensions $K/\mathbb{Q}_p$ with Galois group G is $\prod_\ell c_\ell$ and the set $\{\sum_\ell \eta_\ell : \eta_\ell \in C_\ell\}$ forms a set of representatives for the orbits of* $\mathrm{Aut}(G)$ *on X_G.*

Proof. The role of x_1 at p is almost the same as the role of τ away from p, except that the order of τ must divide $p-1$. For $\ell \neq p$, the ℓ-component of x_1 must be 0; the p-component of τ must be 0. Therefore, if any m_ℓ is at least 3, it is impossible for σ, τ and x_1 to generate G.

When $m_\ell = 2$, generating sets for $\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$ are permuted transitively by $\mathrm{Aut}(G)$ [6, Thm. 3.6], and if $a = b$ then the two generators can be interchanged by an automorphism. When ℓ^b divides $p-1$ then τ can be taken as either generator, whereas if ℓ^a divides $p-1$ but ℓ^b does not then τ can only be the generator of order ℓ^a. If $\ell \neq p$ and ℓ^a does not divide $p-1$ then σ and τ cannot generate G.

When $m_\ell = 1$ then either σ or τ (or both) must be a generator. The descriptions of C_ℓ then follow from the fact that $\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. □

Remark 4.4. It is also possible to count abelian extensions using local class field theory, but the orbits on X_G are used in the lifting algorithm of Section 4.4.

4.3. **Tame groups.** If G has order relatively prime to p, or more generally if V is trivial, then we must have $x_0 = x_1 = 1$. We search for elements of X_G by enumerating the normal subgroups that can contain τ, then finding pairs (σ, τ) that satisfy the tame relation and generate G. We summarize the steps in Algorithm 4.

Algorithm 4: Enumerating extensions: tame case

Input : A group G with trivial p-core
Output: A list of pairs (σ, τ) representing the $\mathrm{Aut}(G)$-orbits in X_G.

```
1  D = DerivedSubgroup(G);
2  pairs = [];
3  if IsCyclic(D) then
4      for N in NormalSubgroupsAbove(D) do
5          if IsCyclic(N) and IsCyclic(G/N) then
6              for s in G that induce pth powering on N do
7                  for t in N that generate G along with s do
8                      if (s,t) not marked then
9                          Append (s,t) to pairs;
10                         Mark images of (s,t) under Aut(G);
11 return pairs;
```

4.4. **Lifting homomorphisms.** For potentially p-realizable groups G that are neither tame nor abelian, we choose a minimal normal subgroup $N \triangleleft G$ (such an N always exists since G is solvable) and set $Q = G/N$. Inductively, we may assume that we have computed a list Y_Q of representatives for the orbits of $\mathrm{Aut}(Q)$ on X_Q.

In particular, if Q is abelian or tame then we may use Section 4.2 or Algorithm 4; otherwise we will recursively use the algorithm described in this section.

The idea is to just test all lifts of quadruples $(\sigma, \tau, x_0, x_1) \in Y_Q$ to see if they are valid elements of X_G. There is a subtlety however: there may be automorphisms of Q which are not induced by automorphisms of G. This problem comes in two parts. First, if N is not a characteristic subgroup then it may not be stabilized by all of $\mathrm{Aut}(G)$, so not all automorphisms descend. Second, the map $\mathrm{Stab}_{\mathrm{Aut}(G)}(N) \to \mathrm{Aut}(Q)$ is not necessarily surjective, so elements of X_Q that are equivalent under $\mathrm{Aut}(Q)$ may lift to elements that are inequivalent under $\mathrm{Aut}(G)$.

We solve the problem by computing a list of coset representatives for the image of $\mathrm{Stab}_{\mathrm{Aut}(G)}(N) \to \mathrm{Aut}(Q)$. Then, instead of just lifting elements of Y_Q, we lift all translates under these automorphisms. We summarize this process in Algorithm 5.

Algorithm 5: Enumerating extensions: lifting method

Input : A potentially p-realizable group G and lists of representatives Y_Q for quotients Q of G

Output: A list Y_G of quadruples (σ, τ, x_0, x_1) representing the $\mathrm{Aut}(G)$-orbits in X_G.

```
Choose a minimal normal subgroup N ◁ G;
Set Q = G/N;
Compute the stabilizer A of N in Aut(G);
Compute a list cokreps of representatives for the cosets of the image of A in
  Aut(Q);
Xreps = [];
foreach (σ, τ, x_0, x_1) ∈ Y_Q do
    foreach α ∈ cokreps do
        foreach lift x_1 of α(x_0) to G that lies in V do
            foreach lift x_0 of α(x_1) to G that lies in V do
                foreach lift τ of α(τ) to G with order prime to p do
                    foreach lift σ of α(σ_0) with τ^σ = τ^p do
                        if (σ, τ, x_0, x_1) not marked then
                            Mark images of (σ, τ, x_0, x_1) under Aut(G);
                            if σ, τ, x_0, x_1 generate G then
                                Append (σ, τ, x_0, x_1) to Xreps;
return Xreps;
```

The runtime of Algorithm 5 depends on the structure of G. If $N \triangleleft G$ is the minimal normal subgroup used, C is the list of coset representatives in $\mathrm{Aut}(Q)$, Y_Q is the list of representatives for the quotient Q, and R is the time it takes to compute the wild relation, then the runtime is bounded by $O(|C| \cdot |Y_Q| \cdot |N|^4 R)$. The actual runtime may be better for some N since we can short circuit some of the loops if the lifts of (x_1, x_0, τ, σ) do not satisfy the appropriate conditions.

Running Algorithm 5 on groups of order up to 2000 for p up to 13 required a few weeks of CPU time. The largest counts found occurred for cyclic groups such as $C_{1458} : p = 3$ (2916) and $C_{1210} : p = 11$ (2376), or for products of cyclic groups

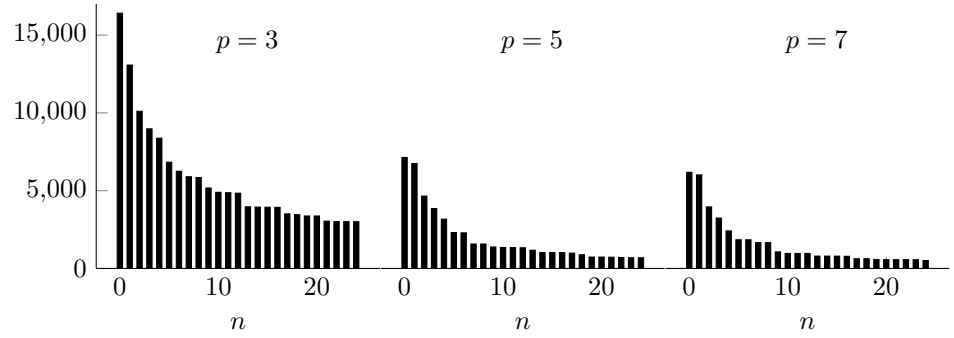


FIGURE 1. Number of pot. p-realizable G with $|G| \leq 2000$ and $|Y_G| \geq n$

with small non-abelian groups such as $C_{243} \times S_3 : p = 3$ (1944). For $p = 3$, other nonabelian groups had large counts such as 1458G553: $(C_{27} \rtimes C_{27}) \rtimes C_2$ (1323) suggesting that the dominance of cyclic groups may not last as the order increases.

Figure 1 shows these counts in aggregate, ignoring the group structure. Specifically, recall that Y_G is in bijection with the set of Galois extensions of $\mathbb{Q}_p$ with Galois group G. Figure 1 plots the function $f(n)$ that counts the number of potentially realizable G with $|G| \leq 2000$ and $|Y_G| \geq n$. The difference between the first and second bars in each chart gives the number of groups that are potentially p-realizable but not actually p-realizable. We have truncated the charts at 25 since they have long tails; the previous paragraph gives examples of G with large $|Y_G|$.

We do not have theoretical results on the possible sizes of N and C, but experimental results are summarized in Tables 2 and 1. The first shows the number of G that have a specified minimum size of N, and the second shows the number of pairs (G, N) with a specified size of C, which we refer to as the *automorphism index*.

TABLE 1. Automorphism index for nonabelian, non-tame G

	Number of $N \triangleleft G$ with given automorphism index				
Index	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$
1	8594	2393	1210	561	663
2	1798	594	421	111	117
3	468	24	73	25	19
4	396	157	59	107	17
5	0	7	0	4	0
6	333	10	58	0	6
8	217	42	47	17	13
9	91	0	4	0	0
10	2	0	0	0	0
12	153	7	4	7	1
13	21	0	0	0	0
16	37	0	8	0	1
18	61	0	2	0	0
20	0	4	0	1	0
24	99	30	4	12	1
> 24	428	12	7	2	0

TABLE 2. Smallest $N \triangleleft G$ for nonabelian, non-tame G

	Number of groups whose N has the given size				
Size	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$
2	8765	2437	1419	638	588
3	3800	423	228	104	110
5	27	392	70	26	45
7	10	6	168	11	18
9	87	0	0	0	0
11	0	3	0	56	7
13	0	3	0	0	68
> 13	9	17	12	12	2

Large indices did occur, but rarely. There were 20 cases of index larger than 10000 for $p = 3$, the largest being 4586868. For $p = 5$, the only index larger than 124 was 3100, occurring 3 times; for other p no index larger than 120 occurred.

5. The inverse Galois problem for p-adic fields

5.1. **Examples of non-realizable groups.** Recall that G is *p-realizable* if there exists an extension $K/\mathbb{Q}_p$ with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$. If G is p-realizable, then every quotient of G is as well, leading us to consider the following class of groups.

Definition 5.1. A group G is *minimally unrealizable* if G is not p-realizable but it is potentially p-realizable and every proper quotient of G is p-realizable.

In Table 3 we list the minimally unrealizable G that have abelian p-core. The label is from the GAP SmallGroups library, which makes precise the description of the group; we write $\mathbb{F}_p^n$ for C_p^n to emphasize the vector space structure. The column V describes the decomposition of V into indecomposable submodules: n^k refers to a submodule of dimension n occurring with multiplicity k. The columns SS, TD, and XC will be described in Section 5.2.

TABLE 3. Minimally unrealizable groups with abelian p-core

p	Label	Description	V	SS	TD	XC
3	27G5	$\mathbb{F}_3^3$	1^3	N	Y	Y
3	36G7	$\mathbb{F}_3^2 \rtimes C_4$	1^2	Y	Y	Y
3	54G14	$\mathbb{F}_3^3 \rtimes C_2$	1^3	Y	N	N
3	72G33	$\mathbb{F}_3^2 \rtimes D_8$	1^2	Y	Y	Y
3	162G16	$C_9^2 \rtimes C_2$	1^2	Y	N	N
3	324G164	$\mathbb{F}_3^4 \rtimes C_4$	2^2	Y	N	Y
3	324G169	$\mathbb{F}_3^4 \rtimes (C_2 \times C_2)$	$1^2 \oplus 1^2$	Y	N	N
3	378G51	$\mathbb{F}_3^2 \rtimes (C_7 \rtimes C_6)$	1^2	Y	Y	Y
3	648G711	$\mathbb{F}_3^4 \rtimes C_8$	2^2	Y	N	Y
5	50G4	$\mathbb{F}_5^2 \rtimes C_2$	1^2	Y	Y	Y
5	125G5	$\mathbb{F}_5^3$	1^3	N	Y	Y
5	200G20	$\mathbb{F}_5^2 \rtimes C_8$	1^2	Y	Y	Y
5	300G34	$\mathbb{F}_5^2 \rtimes (C_3 \rtimes C_4)$	1^2	Y	Y	Y
5	400G149	$\mathbb{F}_5^2 \rtimes (C_8 \times C_2)$	1^2	Y	Y	Y
5	500G48	$\mathbb{F}_5^3 \rtimes C_4$	1^3	Y	N	Y
5	1300G29	$\mathbb{F}_5^2 \rtimes (C_{13} \rtimes C_4)$	1^2	Y	Y	Y

p	Label	Description	V	SS	TD	XC
5	1300G30	$\mathbb{F}_5^2 \rtimes (C_{13} \rtimes C_4)$	1^2	Y	Y	Y
5	1875G21	$\mathbb{F}_5^4 \rtimes C_3$	2^2	Y	Y	Y
7	98G4	$\mathbb{F}_7^2 \rtimes C_2$	1^2	Y	Y	Y
7	147G4	$\mathbb{F}_7^2 \rtimes C_3$	1^2	Y	Y	Y
7	343G5	$\mathbb{F}_7^3$	1^3	N	Y	Y
7	588G22	$\mathbb{F}_7^2 \rtimes C_{12}$	1^2	Y	Y	Y
7	882G23	$\mathbb{F}_7^2 \rtimes C_{18}$	1^2	Y	Y	Y
7	1176G130	$\mathbb{F}_7^2 \rtimes (C_3 \times D_8)$	1^2	Y	Y	Y
11	242G4	$\mathbb{F}_{11}^2 \rtimes C_2$	1^2	Y	Y	Y
11	605G4	$\mathbb{F}_{11}^2 \rtimes C_5$	1^2	Y	Y	Y
11	1331G5	$\mathbb{F}_{11}^3$	1^3	N	Y	Y
13	338G4	$\mathbb{F}_{13}^2 \rtimes C_2$	1^2	Y	Y	Y
13	507G4	$\mathbb{F}_{13}^2 \rtimes C_3$	1^2	Y	Y	Y
13	676G10	$\mathbb{F}_{13}^2 \rtimes C_4$	1^2	Y	Y	Y
13	1014G9	$\mathbb{F}_{13}^2 \rtimes C_6$	1^2	Y	Y	Y

TABLE 4. Minimally unrealizable groups with nonabelian p-core

p	Label	Description	G/W	V/W
3	486G146	$(\mathbb{F}_3^4 \rtimes C_3) \rtimes C_2$	54G13	$1^2 \oplus 1$
3	648G218	$(C_{27} \rtimes C_3) \times D_8$	72G37	1^2
3	648G219	$(\mathbb{F}_3^3 \rtimes C_3) \times D_8$	72G37	1^2
3	648G220	$((C_9 \times C_3) \rtimes C_3) \times D_8$	72G37	1^2
3	648G221	$((C_9 \times C_3) \rtimes C_3) \times D_8$	72G37	1^2
3	972G816	$(\mathbb{F}_3^2 \times (\mathbb{F}_3^2 \rtimes C_3)) \rtimes (C_2^2)$	324G170	$1^2 \oplus 1 \oplus 1$
3	1458G613	$((C_{81} \times C_3) \rtimes C_3) \rtimes C_2$	18G4	1^2
3	1458G640	$(C_9^2 \rtimes C_9) \rtimes C_2$	18G4	1^2

5.2. **Realizability criteria.** We may explain many of the groups in Table 3 by considering V/W as a representation of $T = G/V$ on an $\mathbb{F}_p$-vector space. Note that $|T|$ may be divisible by p: this will occur precisely when there is more than one p-Sylow subgroup in G. In this case V/W may not have a decomposition as a direct sum of irreducible subrepresentations, but it still has a decomposition as a direct sum of indecomposable subrepresentations. The multiplicity of an indecomposable factor is the number of times it appears in such a representation.

Recall from Definition 4.1 that T_G is the set of pairs $(\sigma, \tau) \in G^2$ generating G/V and satisfying the tame relation. In order to show that a potentially p-realizable group G is not p-realizable, we will show that any possible $(\sigma, \tau, x_0, x_1) \in X_G$ that satisfy the tame and wild relations cannot generate G. We will say that G is *strongly split* (SS) if, for every $(\sigma, \tau) \in T_G$, the order of σ in G equals the order of its image in G/V. Note that Conjecture 2.6 would imply that there is some σ with the same order in G as in G/V, but some lifts of σ from G/V to G may have larger order.

We will say that G is *tame-decoupled* (TD) if τ acts trivially on V/W for every $(\sigma, \tau) \in T_G$. Finally, we will say that G is x_0*-constrained* (XC) if the implication

$$x_0^\sigma \langle x_0, \tau \rangle^{-1} \in W \Rightarrow x_0 \in W$$

holds for all $(\sigma, \tau) \in T_G$. The last three columns of Table 3 record whether G is strongly split, tamely-decoupled and x_0-constrained, respectively.

Proposition 5.2. *If G is tame-decoupled then it is x_0-constrained.*

Proof. Each condition holds for G if and only if it holds for G/W, so we may assume that V is an elementary abelian p-group and $W = 1$. Since every τ acts trivially on V by conjugation and h is a $(p-1)$st root of unity,

$$\langle x_0, \tau \rangle = (x_0^{1+h+\cdots+h^{p-2}} \tau^{p-1})^{\frac{\pi}{p-1}} = \tau^\pi = 1.$$

So if $x_0^\sigma \langle x_0, \tau \rangle^{-1} = 1$ then $x_0^\sigma = 1$ and thus $x_0 = 1$. □

Let $n_{G,\mathrm{ss}}$ be 0 if G is strongly split and 1 otherwise; let $n_{G,\mathrm{xc}}$ be 0 if G is x_0-constrained and 1 otherwise.

Theorem 5.3. *Suppose G is potentially p-realizable. Let n be the largest multiplicity of an indecomposable factor of V/W as a representation of T. If $n > 1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$, then G is not p-realizable.*

Proof. We first reduce to the case where $W = 1$. This is easily done, since the definitions of n, $n_{G,\mathrm{ss}}$ and $n_{G,\mathrm{xc}}$ are invariant under quotienting by W, and if we can show that G/W is not p-realizable then G will be unrealizable as well. We may therefore replace V by V/W and assume that V is an elementary abelian p-group.

For sake of contradiction, suppose that G is p-realizable, with $(\sigma, \tau, x_0, x_1) \in X_G$. Suppose that we have an arbitrary word in these generators, and assume that the word is an element of V. Using the conjugation action of T on V and the tame relation, we may rewrite it as $\sigma^c \tau^d x$, where x is a product of conjugates of x_0 and x_1 under the action of T. Thus $\sigma^c \tau^d \in V$, so we may use the fact that τ has order prime to p to rewrite $\sigma^c \tau^d$ as $\sigma^{c'} \in V$. If G is strongly split then we must have $\sigma^{c'} = 1$; otherwise it could be some nonzero element of V.

Since V is an elementary abelian p-group, the wild relation (4) simplifies to

$$x_0^\sigma \langle x_0, \tau \rangle^{-1} = 1. \tag{6}$$

If G is x_0-constrained, we must have $x_0 = 1$; otherwise x_0 can be nontrivial.

Since x_1 is unconstrained, we can write any word in terms of a fixed set of $1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$ elements of V, where we are allowed to act on these elements by T. Let A be a homogeneous component of V with multiplicity n, and consider the projections of our $1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$ elements onto A. Their $\mathbb{F}_p[T]$-span is a proper subspace of A since A has multiplicity $n > 1 + n_{G,\mathrm{ss}} + n_{G,\mathrm{xc}}$, contradicting the assumption that (σ, τ, x_0, x_1) generate G. □

We can get a partial converse, but we now need to assume that $W = 1$.

Theorem 5.4. *Suppose that G is potentially p-realizable with $W = 1$, and that V decomposes as a multiplicity-free direct sum of irreducible T-submodules. Then G is p-realizable.*

Proof. It suffices to construct an element of X_G. Since V is an elementary abelian p-group, we again have the relation (6), which is satisfied for $x_0 = 1$ and arbitrary x_1. Since G is potentially p-realizable, by Proposition 2.5 there are $\sigma, \tau \in G$ satisfying the tame relation and generating G/V. Choose $x_1 \in V$ with nonzero projection onto each irreducible component. The conjugates of x_1 under T generate V, since if they were contained in a proper subspace that subspace would have zero projection onto some irreducible component, contradicting the choice of x_1. Now the fact that σ and τ generate G/V means that x_1, σ and τ generate G. □

17 Jun 2018 21:12:55 PDT
Version 4 - Submitted to Open Book Series

Remark 5.5. There are two groups in Table 3 that are not explained by Theorem 5.3. For 324G169, there are nonzero x_0 satisfying (6), but they all lie in a 1-dimensional indecomposable subrepresentation. The other subrepresentation can't be spanned by x_1 on its own. For 162G16, the quotient by W is p-realizable. Here V is abelian but has exponent 9 rather than 3, so the wild relation takes the form

$$x_0^\sigma \langle x_0, \tau \rangle^{-1} = x_1^p. \tag{7}$$

In order to get a nontrivial x_1, we need to find x_0 with $x_0^\sigma \langle x_0, \tau \rangle^{-1}$ of order 3. Such x_0 exist, but they all have the property that $x_0^\sigma \langle x_0, \tau \rangle^{-1}$ is a multiple of x_0, preventing x_1 from spanning the rest of V.

Remark 5.6. Table 4 gives the groups of order up to 2000 with nonabelian V that are minimally unrealizable. In each case, G/W will be p-realizable, so the methods of this section do not apply. In order to provide an explanation for why they are not p-realizable, one would need to analyze the wild relation more thoroughly.

References

[1] Hans Ulrich Besche and Bettina Eick, *GrpConst, Constructing the Groups of a Given Order, Version 2.5*, 2015.

[2] Hans Ulrich Besche, Bettina Eick, and Eamonn O'Brien, *The SmallGroups library*, 2002.

[3] *GAP – Groups, Algorithms, and Programming*, The GAP Group, 1986-2013.

[4] Helmut Hasse, *Number theory*, Grundlehren der mathematischen Wissenschaften, vol. 229, Springer-Verlag, Berlin, 1969.

[5] C. E. Hempel, *Metacyclic groups*, Comm. Algebra **28** (2000), no. 8, 3865–3897.

[6] Christopher J. Hillar and Darren L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **11** (2007), 917–923.

[7] Xiang-dong Hou and Kevin Keating, *Enumeration of isomorphism classes of extensions of p-adic fields*, Journal of Number Theory **104** (2004), no. 1, 14–61.

[8] Kenkichi Iwasawa, *On galois groups of local fields*, Transactions of the AMS **80** (1955), 448–469.

[9] John Jones and David Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), 80–97.

[10] Marc Krasner, *Nombre des extensions d'un degré donné d'un corps p-adique* (Les Tendances Géométriques en Algèbre et Théorie des Nombres, ed.), CNRS, Paris, 1966.

[11] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[12] Maurizio Monge, *Determination of the number of isomorphism classes of extensions of a p-adic field*, Journal of Number Theory **131** (2011), no. 8, 1429–1434.

[13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Springer-Verlag, Berlin, 2015.

[14] Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659.

[15] Luis Ribes and Pavel Zalesskii, *Profinite groups*, 2nd ed., Springer-Verlag, Berlin, 2010.

[16] Jean-Pierre Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris **286** (1978).

[17] Igor Shafarevich, *On p-extensions*, Mat. Sb. **20** (1947), no. 62, 351–363.

[18] ———, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR, Ser. Mat. **18** (1954), 525–578.

[19] William Stein et al, *Sage Mathematics Software*, The Sage Development Team, 2005-2013.

[20] Masakazu Yamagishi, *On the number of Galois p-extensions of a local field*, Proc. Amer. Math. Soc. **123** (1995), no. 8, 2373–2380.

Department of Mathematics, MIT 2-106, 77 Massachusetts Ave, Cambridge, MA 02139
E-mail address: roed@mit.edu

A DATABASE OF NONHYPERELLIPTIC GENUS 3 CURVES OVER Q

ANDREW V. SUTHERLAND

ABSTRACT. We report on the construction of a database of nonhyperelliptic genus 3 curves over **Q** of small discriminant.

1. INTRODUCTION

Cremona's tables of elliptic curves over **Q** have long been a useful resource for number theorists, and for mathematicians in general [7]. The most current version of Cremona's tables, and similar tables of elliptic curves over various number fields, can be found in the L-functions and modular forms database (LMFDB) [22]. Motivated by the utility of Cremona's tables, the LMFDB now includes a table of genus 2 curves over **Q** whose construction is described in [1]. The goal of this article is to describe the first steps toward the construction of a similar table of genus 3 curves over **Q**.

Thanks to the modularity theorem, elliptic curves over **Q** can be comprehensively tabulated by conductor, as described in [7]. Tabulations by conductor are useful for several reasons, most notably because this invariant can be directly associated to the corresponding L-function. Unfortunately, no comparable method is yet available for higher genus curves, or more generally, for abelian varieties of dimension greater than one. However, one can instead organize curves by discriminant. The discriminant of a curve is necessarily divisible by every prime that divides the conductor of its Jacobian, and it imposes bounds on the valuation of the conductor at those primes. In particular, if the discriminant is prime, it is necessarily equal to the conductor (every abelian variety over **Q** has bad reduction at some prime [10]), and if the discriminant is small, then the conductor must also be small.

Curves of small discriminant (and hence of small conductor) are interesting for several reasons. First, with enough effort one can obtain a reasonably comprehensive list by exhaustively enumerating curves with bounded coefficients, as noted in [1, §3]. Another reason is practical: it is only for such curves that one has reasonable hope of computing certain invariants, such as the analytic rank of the Jacobian, or special values of its L-function. Finally, there is the phenomenon of small numbers: many interesting types of exceptional behavior arise from unlikely collisions that are more likely to be found early in the tabulation. To give just one example of this phenomenon, the smallest prime conductor we found in our search is 8233. This is also the smallest known prime conductor of a Jacobian of a genus 3 hyperelliptic curve over **Q**, and in fact, the two Jacobians appear to be isogenous. Examples of hyperelliptic and nonhyperelliptic curves with isogenous (even isomorphic) Jacobians have been previously

The author was supported by NSF grant DMS-1522526 and Simons Foundation grant 550033.

constructed [18], but these constructions involve abelian varieties with extra structure (typically products of elliptic curves). In our conductor 8233 example the Jacobians are generic and admit no extra endomorphisms, not even over $\overline{\mathbf{Q}}$; see §6 for details.

The methods used in [1] extend fairly easily to genus 3 hyperelliptic curves and have been used to construct a list of genus 3 hyperelliptic curves over $\mathbf{Q}$ of small discriminant, and to compute their conductors, Euler factors at bad primes, endomorphism rings, and Sato-Tate groups. We plan to make this data available in the LMFDB later this year (2018); a preliminary list of these curves can be found at the author's website. In this article we focus on the more difficult case of (nonsingular) nonhyperelliptic curves of genus 3, which represent the generic case of a genus 3 curve and always have a model of the form $f(x,y,z)=0$, where f is a ternary quartic form.

In order to keep the length of this article reasonable, and in recognition of the fact that there is still work in progress to compute some of the invariants mentioned above, we focus only on the first step in the construction of this database: an enumeration of all smooth plane quartic curves with coefficients of absolute value at most $B_c := 9$, with the aim of obtaining a set of unique $\mathbf{Q}$-isomorphism class representatives for all such curves that have absolute discriminant at most $B_\Delta := 10^7$.

Even after accounting for obvious symmetries, this involves more than $10^{17.5}$ possible curve equations and requires a massively distributed computation to complete in a reasonable amount of time. Efficiently computing the discriminants of these equations is a non-trivial task, much more so than in the hyperelliptic case, and much of this article is devoted to an explanation of how this was done. Many of the techniques that we use can be generalized to other enumeration problems and may be of independent interest, both from an algorithmic perspective, and as an example of how cloud computing can be effectively applied to a research problem in number theory. A list of the curves that were found (more than 80 thousand) is available on the author's website [27].

Remark 1.1. The informed reader will know that not every genus 3 curve over $\mathbf{Q}$ falls into the category of smooth plane quartics $f(x,y,z)=0$ or curves with a hyperelliptic model $y^2+h(x)y=f(x)$. The other possibility is a degree-2 cover of a pointless conic; see [14] for a discussion of such curves and algorithms to efficiently compute their L-functions. We plan to conduct a separate search for curves of this form that will also become part of the genus 3 database in the LMFDB.

1.1. **Acknowledgments.** The author thanks John Cremona, Jeroen Sijsling, Michael Stoll, and John Voight for their insight and helpful comments, and the anonymous referees for their careful reading and suggestions.

2. The discriminant of a smooth plane curve

Let $\mathbf{C}[x]_d$ denote the space of ternary forms of degree $d \geq 1$, as homogeneous polynomials in the variables $x := (x_0, x_1, x_2)$. It is a $\mathbf{C}$-vector space of dimension $n_d := \binom{d+2}{2}$ equipped with a standard monomial basis

$$B_d := \{x^u : u \in E_d\}, \qquad E_d := \{(u_0,u_1,u_2) \in \mathbf{Z}^3 : u_0,u_1,u_2 \geq 0,\ u_0+u_1+u_2 = d\}.$$

The dual basis B_d^* for $\mathbf{C}[x]_d^*$ consists of linear functionals $\delta_u\colon \mathbf{C}[x]_d \to \mathbf{C}$ defined by $\sum_u f_u x^u \mapsto f_u$, so that $\delta_u(f)$ is the coefficient of x_u in f. We define $\delta\colon \mathbf{C}[x]_d \to \mathbf{C}^{n_d}$ by $f \mapsto (\delta_u(f))_u$ and $\hat{\delta}\colon \mathbf{C}^{n_d} \to \mathbf{C}[x]_d$ by $(f_u)_u \mapsto \sum_u f_u x^u$.

A polynomial $f \in \mathbf{C}[x]_d$ is *singular* if f and its partial derivatives $\partial_0 f$, $\partial_1 f$, $\partial_2 f$ simultaneously vanish at some point $(z_0, z_1, z_2) \neq (0,0,0)$ in $\mathbf{C}^3$. The curve $f(x) = 0$ is a smooth projective geometrically irreducible curve if and only if f is nonsingular (note that $f = \frac{1}{d}\sum_i x_i \partial_i f$, so any common zero of $\partial_0 f, \partial_1 f, \partial_2 f$ is also a zero of f).

Definition 2.1. For $d \geq 2$ the *discriminant* Δ_d is the integer polynomial in n_d-variables $a := (a_u)_{u \in E_d}$ uniquely determined by the following properties:

- for all $f \in \mathbf{C}[x]_d$ we have $\Delta_d(f) := \Delta_d(\delta(f)) = 0$ if and only if f is singular;
- Δ_d is irreducible and has content 1;
- $\Delta_d(x_0^d + x_1^d + x_2^d) < 0$.

It is a homogeneous polynomial of degree $3(d-1)^2$, by Boole's formula [3, p. 171].[1]

The first two properties determine Δ_d up to sign [11]; our sign convention is consistent with the case of quadratic forms:

$$\Delta_2 = a_{200}a_{011}^2 + a_{101}^2 a_{020} + a_{110}^2 a_{002} - a_{110}a_{101}a_{011} - 4a_{200}a_{020}a_{002}.$$

The discriminant Δ_3 is too large to display here; it is a degree 12 polynomial in 10 variables, with 2040 terms and largest coefficient 26 244. The discriminant Δ_4 of interest to us is larger still: it is a degree 27 polynomial in 15 variables, with 50 767 957 terms and largest coefficient 9 393 093 476 352. Our goal in this section is to briefly explain how we computed it.

Remark 2.2. The discriminant Δ_4 is the largest of the seven projective invariants $I_3, I_6, I_9, I_{12}, I_{15}, I_{18}, I_{27}$ defined by Dixmier [8]. Together with six additional invariants $J_9, J_{12}, J_{15}, J_{18}, J_{21}, J_{21}$ studied by Ohno [24] they generate the full ring of invariants of ternary quartic forms, as conjectured by Shioda in [25, Appendix] and proved by Ohno in an unpublished preprint [24], and later verified by Elsenhans in the published paper [9]. These 13 invariants are collectively known as the *Dixmier-Ohno invariants* and have been studied by many authors [9, 12, 20, 21]. Algorithms to compute the Dixmier-Ohno invariants of a given ternary quartic are described in [9, 12, 21], and Magma [2] implementations of these algorithms are available [9, 12, 26]. For our application we want to explicitly compute Δ_4 as a polynomial in 15 variables. In [24, Rem. 2.2] Ohno considers the question of counting the number of terms in Δ_4, and he proves an upper bound of 58 456 030. As a byproduct of our work, we can now answer Ohno's question: the polynomial Δ_4 has 50 767 957 terms.

Definition 2.3. For $d \geq 1$ the *resultant* R_d is the integer polynomial in $3n_d$ variables $a := (a_{0,u}, a_{1,u}, a_{2,u}) \in E_d^3$ uniquely determined by the following properties:

- for all $f_0, f_1, f_2 \in \mathbf{C}[x]_d$ we have $R_d(f_0, f_1, f_2) := R_d(\delta(f_0), \delta(f_1), \delta(f_2)) = 0$ if and only if f_0, f_1, f_2 have a common root $(z_0, z_1, z_2) \neq (0,0,0)$ in $\mathbf{C}^3$;
- R_d is irreducible and has content 1;
- $R_d(x_0^d, x_1^d, x_2^d) = 1$.

[1] Boole credits this formula to Sylvester.

It is a homogeneous polynomial of degree $3d^2$ [11, Prop. 13.1.7].

Proposition 2.4. *For all $f \in \mathbf{C}[x]_d$ we have $\Delta_d(f) = -d^{-d^2+3d-3}R_{d-1}(\partial_0 f, \partial_1 f, \partial_2 f)$.*

Proof. Up to sign this is implied by [11, Prop. 13.1.7]. To verify the sign, we note that

$$\Delta_d(x_0^d + x_1^d + x_2^d) = -d^{-d^2+3d-3}R_{d-1}(dx_0^{d-1}, dx_1^{d-1}, dx_2^{d-1}) = -d^{d(2d-3)} < 0. \qquad \square$$

Proposition 2.4 implies that to compute Δ_d it suffices to compute R_{d-1}. In fact we only need to compute

$$R_{d-1}(\tilde{\partial}_0(a), \tilde{\partial}_1(a), \tilde{\partial}_2(a)),$$

where $\tilde{\partial}_i := \delta \circ \partial_i \circ \hat{\delta}$, which is a polynomial in n_d variables, rather than $3n_{d-1}$ variables. For $d = 4$ this reduces the number of variables from 30 to 15, which is crucial to us. Computing Δ_4 is a non-trivial but feasible computation, as we explain below; explicitly computing R_3 would be far more difficult.

2.1. **Sylvester's resultant formula for ternary forms.** In this section we briefly recall the classical determinantal formula of Sylvester for computing R_d for $d \geq 2$, following [11, §3.4D]. It provides an efficient method to compute $R_d(f_0, f_1, f_2)$ for particular values of f_0, f_1, f_2, even when R_d is too large to compute explicitly. We will use this formula to compute Δ_4.

Given $f_0, f_1, f_2 \in \mathbf{C}[x]_d$, we define the linear operator

$$\begin{aligned} T_{f_0,f_1,f_2} \colon \mathbf{C}[x]_{d-2}^3 &\to \mathbf{C}[x]_{2d-2} \\ (g_0, g_1, g_2) &\mapsto g_0 f_0 + g_1 f_1 + g_2 f_2. \end{aligned}$$

We now define a second linear operator $D_{f_0,f_1,f_2} \colon \mathbf{C}[x]_{d-1}^* \to \mathbf{C}[x]_{2d-2}$ by defining its value on elements $\delta_u \in B_{d-1}^*$ of the dual basis, where $u \in E_{d-1}$. For each $u \in E_{d-1}$ we may write f_i in the form

$$f_i = \sum_{j=0}^{2} x_j^{u_j+1} F_{ij}^{(u)}$$

with $F_{ij}^{(u)} \in \mathbf{C}[x]_{d-1-u_j}$. Without loss of generality we assume $f_i - x_0^{u_0+1}F_{i0}^{(u)}$ has no terms divisible by $x_0^{u_0+1}$ and $f_i - x_0^{u_0+1}F_{i0}^{(u)} - x_1^{u_1+1}F_{i1}^{(u)}$ has no terms divisible by $x_1^{u_1+1}$, so that the $F_{ij}^{(u)}$ are uniquely determined. We then define

$$D_{f_0,f_1,f_2}(\delta_u) := \det[F_{ij}^{(u)}] \in \mathbf{C}[x]_{2d-2}.$$

Finally, we define the linear operator

$$\begin{aligned} \Phi_{f_0,f_1,f_2} \colon \mathbf{C}[x]_{d-2}^3 \oplus \mathbf{C}[x]_{d-1}^* &\to \mathbf{C}[x]_{2d-2} \\ ((g_0, g_1, g_2), v) &\mapsto T_{f_0,f_1,f_2}(g_0, g_1, g_2) + D_{f_0,f_1,f_2}(v), \end{aligned}$$

and observe that its domain and codomain both have dimension

$$3\binom{d-2+2}{2} + \binom{d-1+2}{2} = 2d^2 - d = \binom{2d-2+2}{2}.$$

Proposition 2.5. *For all $f_0, f_1, f_2 \in \mathbf{C}[x]_d$ we have $R_d(f_0, f_1, f_2) = \pm \det \Phi_{f_0,f_1,f_2}$.*

Proof. This follows from Lemma 4.9 and Theorem 4.10 in [11, §3]. $\square$

Remark 2.6. Unlike Theorem 4.10 in [11, §3], we allow a sign ambiguity in Proposition 2.5. In order to view Φ_{f_0,f_1,f_2} as a linear operator one needs to fix an isomorphism between its domain and its codomain, which we prefer not to do. The most natural way to compute Φ_{f_0,f_1,f_2} is to compute values of T_{f_0,f_1,f_2} and D_{f_0,f_1,f_2} on monomial bases of $\mathbf{C}[x]^3_{d-2}$ and $\mathbf{C}[x]^*_{d-1}$; the sign of $\det\Phi_{f_0,f_1,f_2}$ will depend on how one orders these bases and a monomial basis for $\mathbf{C}[x]_{2d-2}$, but the condition $R_d(x^d,y^d,z^d)=1$ determines the correct sign (see Magma scripts in [27]).

Our explicit description of T_{f_0,f_1,f_2} and D_{f_0,f_1,f_2} above makes it easy to write down the $(2d^2-d)\times(2d^2-d)$ matrix whose determinant is equal to $R_d(f_0,f_1,f_2)$. Each row consists of the coefficients of homogeneous polynomial of degree $2d-2$ that is the image of a basis element of $\mathbf{C}[x]^3_{d-2}\oplus\mathbf{C}[x]^*_{d-1}$, each of which we can identify with an element of E_{d-2} or E_{d-1}. For each $u\in E_{d-2}$ we get 3 rows, the coefficient vectors of x^uf_0, x^uf_1, x^uf_2 and for each $u\in E_{d-1}$ we get one row, the coefficient vector of $D_{f_0,f_1,f_2}(\delta_u)=\det[F^u_{ij}]$.

Example 2.7. Let $f := y^2z-x^3-a_2x^2z-a_4xz^2-a_6z^3$, and let f_0,f_1,f_2 be its partial derivatives with respect to x,y,z respectively. If we order our monomial bases lexicographically (so x^3 comes first) and put the 3 rows of Φ_{f_0,f_1,f_2} corresponding to T_{f_0,f_1,f_2} at the top and the 3 rows corresponding to D_{f_0,f_1,f_2} at the bottom, we have

$$\Phi_{f_0,f_1,f_2}=\begin{bmatrix}-3&0&-2a_2&0&0&-a_4\\0&0&0&0&2&0\\-a_2&0&-2a_4&1&0&-3a_6\\0&0&-4a_2^2+12a_4&0&0&-2a_2a_4+18a_6\\0&6&0&0&4a_2&0\\0&0&-2a_2a_4+18a_6&0&0&12a_2a_6-4a_4^2\end{bmatrix},$$

and therefore

$$\begin{aligned}\Delta_3(f)&=-3^{-3}R_2(f_0,f_1,f_2)=-3^{-3}\det\Phi_{f_0,f_1,f_2}\\&=-64a_2^3a_6+16a_2^2a_4^2+288a_2a_4a_6-64a_4^3-432a_6^2,\end{aligned}$$

which matches the discriminant of the elliptic curve $y^2=x^3+a_2x^2+a_4x+a_6$.

See [5, Ex. 3.15] and the magma script in [27] for further details and more examples.

2.2. **Computing Δ_4.** To compute Δ_4 we put $f:=\sum_{u\in E_4}a_ux^u$ using $\binom{4+2}{2}=15$ formal variables a_u. The resulting polynomial f is then an element of $(\mathbf{Z}[a])[x]_4$, rather than $\mathbf{C}[x]_4$, but we can construct a matrix M_Φ representing the linear operator $\Phi_{\partial_0 f,\partial_1 f,\partial_2 f}$ as in Example 2.7, obtaining a 15×15 matrix whose coefficients are homogeneous polynomials in $\mathbf{Z}[a]$, with $\det M_\Phi\in\mathbf{Z}[a]_{27}$. The first 9 rows of M_Φ (corresponding to $T_{\partial_0 f,\partial_1 f,\partial_2 f}$) each contain 5 zero entries and linear monomials in the nonzero entries. The remaining 6 rows of M_Φ (corresponding to $D_{\partial_0 f,\partial_1 f,\partial_2 f}$) contain a 3×3 submatrix of zeros and homogeneous polynomials of degree 3 in the nonzero entries. After some experimentation we settled on the strategy of computing $\det M_\Phi$ as the sum of $\binom{12}{3}=220$ products of the form $(\det A)(\det B)$ with $A\in\mathbf{Z}[a]^{3\times3}$ and $B\in\mathbf{Z}[a]^{9\times9}$ submatrices of M_Φ with $\det A\in\mathbf{Z}[a]_9$ and $\det B\in\mathbf{Z}[a]_{18}$. Computing the determinants of all the

submatrices A and B takes only a few minutes. We then computed the 220 products in parallel on a 64-core machine and summed the results to obtain Δ_4; in total this computation took about 8 core-hours. The resulting polynomial Δ_4 can be downloaded as a 2GB text file from the author's website [27].

3. Computing discriminants using a monomial tree

In this section we describe our method for enumerating ternary quartic forms

$$f(x) = \sum_{u \in E_4} f_u x^u$$

with coefficients $f_u \in \mathbf{Z}$ satisfying $|f_u| \le B_c$, for some coefficient bound B_c, along with their discriminants $\Delta_4(f)$. As explained in the introduction, our goal is to select from this list all such forms with nonzero discriminants satisfying $|\Delta_4(f)| \le B_\Delta$, for some discriminant bound B_Δ. Rather than separately computing each discriminant via Sylvester's method (which would not require Δ_4), we will instead enumerate values of $\Delta_4(f)$ in tandem with our enumeration of values of f, using a *monomial tree*, a data structure introduced in [1, §3.2].

In the computation described in [1], the discriminant polynomial has only 246 terms, and the corresponding monomial tree has 703 nodes and fits in 8KB of memory. In particular, the monomial tree easily fits in L1-cache, and there is very little overhead in recomputing it as required in a parallel computation (indeed, in the computation described in [1] each thread builds and maintains its own private monomial tree). In our case the discriminant polynomial Δ_4 is several orders of magnitude larger, and the implementation of the monomial tree merits further discussion, particular in view of the need to support a massively parallel computation that needs to be fault tolerant.

The monomial tree is based on data structure known in the computer science literature as a *trie* (or *prefix tree*). This data structure represents a set of (*key*, *value*) pairs using a tree whose paths correspond to keys with values stored at the leaves; in addition to supporting lookup operations, a trie allows one to efficiently enumerate all keys with a common prefix (it is commonly used to implement the auto-complete feature found in many user interfaces), but we will exploit it in a different way.

In a monomial tree, the keys are exponent vectors $e := (e_0, \dots, e_n)$ and the values are coefficients c_u. Each leaf of the tree represents a term $c_e a^e$ of a polynomial in the variables $a := (a_0, \dots, a_n)$. Two uninstantiated monomial trees for the polynomial

$$g(a_0, a_1, a_2) := a_0^3 a_2 + 3a_0^2 a_1^2 - 4a_0^2 a_1 a_2 - 5a_0 a_1^2 a_2 + 2a_1^4 + 7a_1^3 a_2$$

are shown in Figure 1 below.

We are free to choose any ordering of the variables, and there are thus many monomial trees that represent the same polynomial; in this case we prefer the tree on the right (both because it has fewer nodes, and because the maximum degree appearing at the top level is smaller). Once we fix an ordering of the variables, there is no need to actually identify the variable in each node, since this will be implied by its level in the tree; we only need to store the exponent. For polynomials that are fairly dense, such as Δ_4, we can make the exponent implicit as well by simply using an array of fixed size

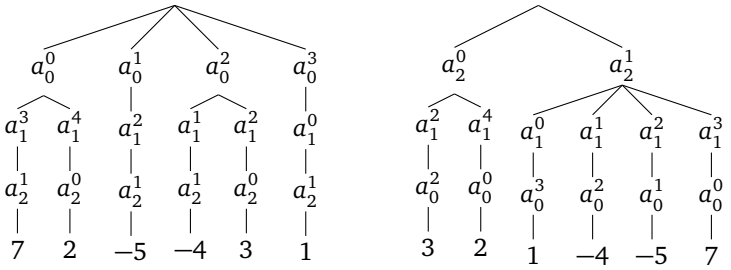


FIGURE 1. Two monomial trees for $g(a_0, a_1, a_2)$.

determined by the maximum degree of the variable in the next level, using null values to indicate the absence of a child of a given degree.

To evaluate a polynomial represented by a monomial tree we work from the bottom up (the opposite of the typical usage pattern for a trie). Using the monomial tree listed on the right in Figure 1, let us partially evaluate it by first making the substitution $a_0 = 2$, and then the substitution $a_1 = -1$; this yields monomial trees for the polynomials $g(2, a_1, a_2)$ and $g(2, -1, a_2)$, as shown in Figure 2.

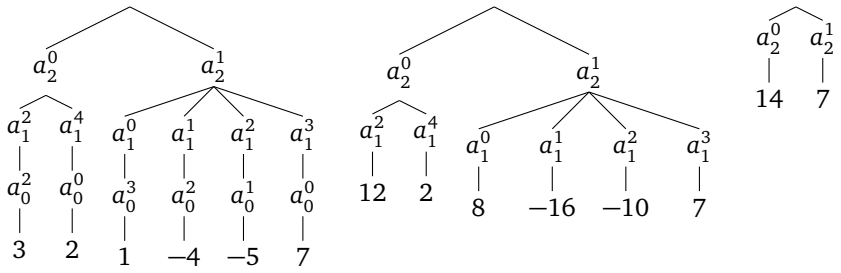


FIGURE 2. Monomial trees for $g(a_0, a_1, a_2)$, $g(2, a_1, a_2)$, and $g(2, -1, a_2)$.

With each substitution we evaluate nodes one level above the leaves (so $3a_0^2$ becomes 12 when we substitute $a_0 = 2$, for example), and sum siblings (this does not impact the first substitution, but $12a_1^2 + 2a_1^4$ becomes 14 when we substitute $a_1 = -1$, for example). We ultimately obtain a univariate polynomial in whichever variable we choose to put at the top of the tree; in this example that variable is a_2 and we have $g(2, -1, a_2) = 14 + 7a_2^1$, which we could then evaluate on any value of a_2 that we wish.

For the sake of illustration we have depicted the monomial tree as "shrinking" as we make these substitutions, but in reality substitutions are performed by updating auxiliary values attached to each node of the tree, the structure of which is not modified. At any point in the computation we can undo the most recent substitution by simply incrementing a *level pointer*, a variable that identifies the level of the tree where a variable substitution was most recently made (these are depicted as leaves in the diagrams above). More generally, we can immediately revert to any prefix of the variable substitutions that have been made by updating the level pointer; this feature is critical to the parallel implementation discussed in the next section.

One can thus view the monomial tree as an *arboreal stack*. The top of the stack is at the leaves, variable substitutions are "pushed" on to the stack by updating nodes at the current level, and we can "pop" any number of variable substitutions off the stack by updating the level pointer (which acts as a stack pointer).

For the discriminant polynomial Δ_4 there are $\binom{4+2}{2} = 15$ variables a_{ijk}, each corresponding to a possible coefficient of a monomial $x_0^i x_1^i x_2^k$ in a ternary quartic form. After accounting for the symmetries corresponding to permutations of x_0, x_1, x_2, there 15!/3! distinct monomial trees we could use to represent Δ_4, depending on how we choose to order the variables. The polynomial Δ_4 has total degree 27, but its degree in the variables a_{ijk} varies: it has degree 9 in $a_{400}, a_{040}, a_{004}$, degree 16 in $a_{211}, a_{121}, a_{112}$, and degree 12 in each of the remaining variables. One might expect that an optimal approach would have the variables sorted by degree (lowest at the top of the tree, highest at the bottom), but this is not quite true. After a lot of experimentation we settled on the following variable ordering (working from the top of tree down):

$$a_{400},\ a_{310},\ a_{301},\ a_{220},\ a_{202},\ a_{130},\ a_{040},\ a_{103},\ a_{004},\ a_{031},\ a_{013},\ a_{022},\ a_{211},\ a_{121},\ a_{112}.$$

This yields a monomial tree with a total of 246 798 264 nodes and level sizes as listed in Table 1 below.

a_{400}	10	a_{220}	1772	a_{040}	246759	a_{031}	11218852	a_{211}	50767957
a_{310}	67	a_{202}	8128	a_{103}	1197716	a_{013}	27045996	a_{121}	50767957
a_{301}	328	a_{130}	48856	a_{004}	3957952	a_{022}	50767957	a_{112}	50767957

TABLE 1. Levels in the monomial tree used for Δ_4.

Remark 3.1. As implied by the last four entries of Table 1, at the bottom several levels of the tree each node has only one child. Indeed, fixing the exponent for all but the 3 variables a_{211}, a_{121}, a_{112} of degree 16 uniquely determines a term in Δ_4. There does not appear to be an easy way to compute the exponents of a_{211}, a_{121}, a_{112} directly from the exponents of the other 12 variables, but such a function exists.

Our implementation uses 16 bytes of storage for each node in the monomial tree. This includes a 64-bit integer value to store substitution results modulo 2^{64} and a 32-bit integer that identifies the parent node by its index in an array that holds all the nodes in the tree; the total amount of memory required is about 4GB. Loading the terms of Δ_4 from a suitably prepared binary file and constructing the tree in memory takes less than 10 core-seconds on the machines we used (see the next section for details).

Modulo parallelization and optimizations discussed below, our strategy to enumerate ternary quartic forms with their discriminants is given by the following recursive algorithm, in which we use v_n to denote the variable a_{ijk} at level n of the tree, with $v_1 = a_{400}$ at the top and $v_{15} = a_{112}$ at the bottom, and view $\Delta_4 := \Delta_4(v_1, \ldots, v_{15})$ as a polynomial in these variables. After constructing the monomial tree T for Δ_4 as above, we invoke the following algorithm with $n = 15$ (the bottom of the tree).

Algorithm TERNARYQUARTICFORMENUMERATION(T,n)
Given a monomial tree T for Δ_4 and a level $n \in [1,15]$:

1. If $n = 1$ then
   a. Extract $g(v_1) = \Delta_4(v_1, c_2, \ldots, c_n) \bmod 2^{64}$ from T.
   b. For each integer c_1 in the coefficient interval $[-B_c, B_c]$:
      i. Compute $D \coloneqq g(c_1) \bmod 2^{64}$ with $-2^{63} \le D < 2^{63}$.
      ii. If $D = 0$ or $|D| > B_\Delta$ proceed to the next value of c_1.
      iii. Otherwise, compute $\Delta \coloneqq \Delta_4(c_1, \ldots, c_n) \in \mathbf{Z}$ using Sylvester's determinantal formula.
      If $|\Delta| \le B_\Delta$, output the ternary quartic form defined by $c_1, \ldots, c_{15}$ with discriminant Δ.
2. Otherwise, for each integer c_n in the coefficient interval $[-B_c, B_c]$:
   a. Apply the substitution $v_n \leftarrow c_n$ to T.
   b. Recursively invoke TERNARYQUARTICFORMENUMERATION($T, n-1$).

We assume that in the process of applying the substitution $v_n \leftarrow c_n$ the value of c_n is stored in T so that it can be accessed later in step 1.a.iii if needed (so the data structure for T includes an auxiliary array that holds $c_1, \ldots c_n$). We now note the following optimizations and implementation details:

- We are interested in $\mathrm{PGL}_3(\mathbf{Z})$-isomorphism classes of ternary quartic forms represented by a form within our coefficient bounds. Permutations of variables and sign changes do not change the absolute value of the discriminant, so we can restrict our enumeration to $0 \le c_{15} \le c_{14} \le c_{13}$. This saves a factor of 48.

- In the recursive call at level n, we can completely ignore levels of the tree below n. In a parallel implementation, we can fork the execution at any level and divide the work among child processes that only need the upper part of the tree. As described in the next section, we forked at level $n = 10$, at which point the upper part of the tree fits in 700MB of memory.

- In our implementation we use loops, not recursion, and completely unwind the inner loop, making each integer value $c_1 \in [-B_c, B_c]$ fully explicit.

- With the coefficient bound $B_c = 9$ we only need to compute $g(c_1)$ for 19 values of c_1. This makes the finite differences approach of [19] that was used in [1] less attractive, as there is an initial setup cost and we cannot as easily take advantage of the fact that the values of c_1 (and their powers) are known at compile time. Instead, we write $g_1(v_1) = g_0 + v_1 h_1(v_1^2) + h_2(v_1^2)$, with $\deg h_1, \deg h_2 \le 4$. We then have $g(0) = g_0$, and for $c_1 \in [1, B_c]$ we compute,

  $$g(c_1) = g_0 + c_1 h_1(c_1^2) + h_2(c_1^2), \quad g(-c_1) = g_0 - c_1 h_1(c_1^2) + h_2(c_1^2),$$

  reusing the values of $c_1 h_1(c_1^2)$ and $h_2(c_1^2)$, and taking advantage of the fact that all the powers of c_1 are known at compile time.

The last point is crucial, as most of the time will be spent in the inner loop evaluating $g(c_1)$. For the 9 values $c_1 = 0, \pm 1, \pm 2, \pm 4, \pm 8$ we can compute $g(c_1)$ using only 64-bit

additions/subtractions and bit shifts, and for the remaining $c_1 \in [-B_c, B_c]$ we use an average of four 64-bit multiplications and six 64-bit additions.

With $B_c = 9$, benchmarking shows that on average we spend less than 22 clock cycles computing each value of $g(c_1)$ and comparing the result with 0 and B_Δ (steps 1.b.ii and 1.b.iii of the algorithm), which is consistent with the operation counts above. Overall, the average time per iteration of the inner loop is about 33 clock cycles; this includes the cost of maintaining the monomial tree T, performing variable substitutions, iterating values of c_n, extracting the coefficients of $g(v_1)$ from T, and time spent computing $\Delta_4(c_1, \ldots, c_n) \in \mathbf{Z}$ using Sylvester's formula and multi-precision arithmetic (but step 1.b.iii is executed so rarely that its impact is negligible).

Remark 3.2. Another advantage of unrolling the inner loop so that powers of c_1 are available at compile time (thereby turning polynomial evaluation into a dot product), is that the multiplications can be performed in parallel. Although we did not take direct advantage of this in our implementation, it allows the compiler to minimize instruction latency via pipelining. The AVX-512 instruction set supported on newer Intel CPUs (Knights Landing and Skylake) provides SIMD instructions that support simultaneous 8-way 64-bit multiplication and 8-way 64-bit additive reduction, which in principle should reduce the cost of evaluating $g(c_1)$ by close to a factor of 4. At the time we performed the computations described in this article these newer processors were not yet widely available, but we plan to exploit this feature in future computations.

4. Distributed parallel implementation

We performed our computations using preemptible compute instances on Google's Compute Engine [13], which is part of the Google Cloud Platform (GCP). We used the `n1-highcpu-32` virtual machine type, each instance of which has 32 virtual CPUs (vCPUs) and 28.8GB memory; the 32 vCPUs correspond to hyperthreads running on 16 physical cores. This machine type is widely available on all GCP regions (geographical areas) and generally offers an optimal price/performance ratio for CPU intensive tasks.

With preemptible compute instances, computations are not allowed to run for more than 24 hours, and the computation may be halted by GCP at any time. Preempted computations can be restarted if and when the computational resources become available, and the restarted instance will have access to any information that was saved to disk, so in our implementation of the TernaryQuarticFormEnumeration algorithm we incorporated a checkpointing facility that tracks the current state of progress by writing the values of $c_{15}, c_{14}, \ldots, c_m$ to disk at regular intervals (we used $m = 7$). To restart we simply read the most recently checkpointed values of $c_{15}, \ldots, c_m$, rebuild the monomial tree, perform the corresponding variable substitutions $v_n = c_n$, and resume where we left off (restarting typically takes 10-15 seconds).

To efficiently distribute the computation across multiple instances using the coefficient bound $B_c = 9$ we divide the work into $\binom{B_c+3}{3}(2B_c+1)^2 = 79\,420$ jobs. Each job is given a fixed set of integers $(c_{15}, c_{14}, c_{13}, c_{12}, c_{11})$, with $0 \le c_{15} \le c_{14} \le c_{13} \le B_c$ and $c_{12}, c_{11} \in [-B_c, B_c]$ (the constraints on c_{15}, c_{14}, c_{13} come from the symmetry optimization noted above), and then proceeds to enumerate the $(2B_c+1)^{10} = 19^{10} \approx 10^{12.79}$

values of the integers $c_{10}, \ldots, c_1$ with $|c_n| \le B_c$. Based on the GCP resource quotas available to us, we assigned 2 jobs to each 32-vCPU instance, allowing us to use a total of up to 39 710 preemptible instances at any one time, each equipped with 32 virtual CPUs.

To utilize the 32 virtual CPUs on each instance in parallel, after constructing the monomial tree and applying substitutions using the values of $c_{15}, \ldots, c_{11}$ assigned to the job, we fork the process into 32 child processes. As noted in the previous section, after performing this substitutions the relevant part of the monomial tree (levels $n \le 10$) only requires 700MB of memory, allowing each child process to have a private copy of this portion of the tree while staying within our 28.8GB memory footprint. Each child process then iterates over values of c_{10}, c_9, c_8 as usual, but only proceeds to $c_7, \ldots, c_1$ when $(2B_c+1)^2 c_{10} + (2B_c+1)c_9 + c_8 \equiv i \mod 32$, where $i \in [0, 31]$ is an integer that distinguishes the child process among its 32 siblings.

With this approach it takes a typical 32-vCPU instance between 3000 and 4000 seconds of wall time to complete one job (just under an hour, on average). The physical machine types vary, but most of the machines we used were either 2.5GHZ Intel Xeon E5v2 (Ivy Bridge) CPUs or 2.2GHz Intel Xeon E5v4 (Broadwell) CPUs. The total time to complete all 79,420 jobs was about 290 vCPU-years.

Remark 4.1. One might assume 2 vCPUs = 1 core, but with our computational load vCPUs do substantially better than this. It is difficult to make an exact comparison due to the variety of machines used, but none of our GCP CPUs had a clock speed above 2.5GHz and the majority were 2.2GHz. If one estimates the total number of vCPU clock cycles ($\approx 10^{19.33\pm 0.3}$) and divides by the number of ternary quartic forms processed ($\approx 10^{17.69}$), the average throughput is 44 ± 3 vCPU clock cycles per form, versus 33 clock cycles for a single thread on an idle core. One explanation for this is that while 22 of the 33 average clock cycles represent processor bound low latency arithmetic operations in the inner loop that are unlikely to benefit from hyperthreading, the remainder are spent on memory bound activity (maintaining the monomial tree), which can be overlapped with processor bound activity by another vCPU.

We ran the computations described above on Sunday June 11, 2017, distributing the work across 24 GCP zones located in 9 regions (4 in North America, 2 in Europe, and 3 in Asia). We run the computation in two stages, one in the morning and one in the afternoon, each involving approximately 20 000 preemptible 32-vCPU instances. Figure 3 shows the CPU utilization over the course of the day; each color represents one of the 24 zones we used. As can be seen in the chart, our CPU utilization peaked around 9:00, at which point we were utilizing the equivalent of 580,000 vCPUs at full capacity (the total number of active vCPUs was well over 600,000, but not all were running at full capacity at the same time, due to preemption and startup/restart latency).

5. Identifying isomorphism class representatives

With coefficient bound $B_c = 9$ and discriminant bound $B_\Delta = 10^7$, the enumeration of ternary quartic forms described in the previous sections produces a list of more than 10^7 forms $f(x, y, z)$. But our goal is to construct a list of smooth plane quartic curves $C_f : f(x, y, z) = 0$ that we distinguish only up to isomorphism over $\mathbf{Q}$. The coefficient

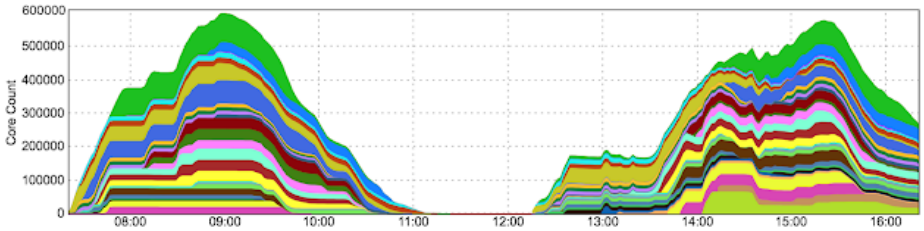


FIGURE 3. vCPU utilization on GCP

constraints that we added to optimize the search eliminate some obvious isomorphisms (at least for curves where the coefficients of xyz^2, xy^2z, x^2yz are distinct), and in some cases this does result in a unique isomorphism class representative appearing in our enumeration. But in the vast majority of cases it does not. Indeed, among the 1378 forms $f(x,y,z)$ we identified with absolute discriminant $|\Delta_4(f)| = 3^9 5^2$, only two $\mathbf{Q}$-isomorphism classes of curves are represented:

$$x^3z + x^2z^2 + xy^3 - xz^3 + y^3z = 0, \qquad x^3z + y^4 + 2y^3z - yz^3 = 0,$$

and in general, among the more than ten million curves we found, only 82 241 distinct $\mathbf{Q}$-isomorphism classes are represented. Our goal in this section is to briefly explain how we efficiently reduced our initial list of more than 10^7 ternary quartic forms to a list of 82 241 unique $\mathbf{Q}$-isomorphism class representatives.

We first note that this computation cannot be easily accomplished using any of the standard computer algebra packages. Even if one of them supported reliable isomorphism testing of smooth plane curves over $\mathbf{Q}$ (to the author's knowledge, none do), pairwise isomorphism testing is expensive and we would need to perform hundreds of millions of such tests. We want a strategy that can be applied in bulk and efficiently reduce a large set of smooth plane curves to a subset of unique isomorphism class representatives.

Given an equation $f(x,y,z)$ in our list S of ternary quartic forms satisfying the coefficient bound B_c and discriminant bound B_Δ, let S_f denote the set of ternary quartic forms g for which C_g is $\mathbf{Q}$-isomorphic to C_f. The set S_f is finite, and if we could efficiently compute it, our problem would be solved. Rather than computing S_f, we will compute successively larger subsets of it and use them to reduce the size of S by removing all elements of $S \cap S_f$ distinct from f (or distinct from a chosen representative of S_f that we happen to like better than f).

Let us fix the following set of generators for $\mathrm{GL}_3(\mathbf{Z})$:

$$A_1 := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2 := \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_3 := \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_4 := \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

These induce invertible linear transformations

$$A_1 : f(x,y,z) \mapsto f(x+y,y,z), \qquad A_2 : f(x,y,z) \mapsto f(y,-x,z),$$
$$A_3 : f(x,y,z) \mapsto f(-x,y,z), \qquad A_4 : f(x,y,z) \mapsto f(-z,x,y),$$

which do not change the $\mathbf{Q}$-isomorphism class of the curve $f(x,y,z)=0$ or its absolute discriminant. (This means we will not detect isomorphisms $f(x,y,z)\mapsto f(ax,y,z)$ with $a\neq\pm1$, but these change the discriminant by a^{36}, which will push the discriminant well beyond our discriminant bound). Let $\|f\|$ denote the maximum of the absolute values of the coefficients of f; note that $\|f\|$ is preserved by A_2,A_3,A_4, but not A_1. The following algorithm performs a breadth-first search of the Cayley graph of $\mathrm{GL}_3(\mathbf{Z})$ with respect to our generators, subject to the restriction that it only explores paths $1,M_1,\dots M_n\in\mathrm{GL}_3(\mathbf{Z})$ in the graph for which $\|M_i(f)\|\leq b$ for $1\leq i\leq n$.

Algorithm BOUNDEDISOMORPHISMCLASSENUMERATION(f,b)
Given a ternary quartic form $f(x,y,z)$ and a bound $b\geq\|f\|$, compute $S_{f,b}\subseteq S_f$ as follows:

1. Let $U:=\{f\}$ and $V:=\{f\}$.
2. Let $W:=\{\}$, and for $g\in V$:
   a. If $\|A_1(g)\|\leq b$ then set $W\leftarrow W\cup\{A_1(g)\}$.
   b. Set $W\leftarrow W\cup\{A_2(g),A_3(g),A_4(g)\}$.
3. Set $V\leftarrow\{g:g\in W \text{ and } g\notin U\}$.
4. If V is empty then output $S_{f,b}:=U\cup\{-g:g\in U\}$ and terminate.
5. Set $U\leftarrow U\cup V$ and return to step (2).

Our strategy is to start with $b=B_c$ and for each $f\in S$ remove every element of $S_{f,b}$ from S except for f, and then increase b and repeat. With $b=B_c$ and our initial set of over ten million forms S an efficient implementation of the algorithm above takes only ten minutes and reduces the number of curves to around 125 000. The algorithm becomes slower as b increases, but even with $b=B_c^2=81$ it takes just eight core-hours, yielding a list of 82 241 curves that appear to be non-isomorphic.

We are now left with the task of trying to prove that the remaining set of curves S are all non-isomorphic. Here again we adopt a bulk strategy and compute two sets of invariants for every $f\in S$. First we use the Magma package [26] which implements the algorithms described in [21] to compute the Dixmier-Ohno invariants of C_f; these uniquely identify the $\overline{\mathbf{Q}}$-isomorphism class of C_f. Second, we compute a vector of point counts of C_f modulo all primes $p\leq 256$ of good reduction for C_f, using the `smalljac` software package described in [19]. Both computations are quite fast; it takes only a few minutes to do this for all 82 241 of our candidate curves.

We now define an equivalence relation on S by defining C_f and C_g to be equivalent if and only if their normalized Dixmier-Ohno invariants coincide and their point counts at all common primes $p\leq 256$ of good reduction coincide. The resulting equivalence classes partition S into 82 239 singleton sets and the following pair of curves with absolute discriminant 324 480:

$$C_f: x^3y+x^3z+x^2y^2-2x^2yz-4x^2z^2-4xy^3+xz^3+2y^4-2yz^3+z^4=0,$$
$$C_g: x^4+x^3y+2x^3z+4x^2y^2-xy^3-2xy^2z+y^4+3y^3z+5y^2z^2+4yz^3+2z^4=0.$$

These curves both have good reduction modulo 7 but are not isomorphic as curves over $\mathbf{F}_7$, as can be verified by exhaustively checking all possible isomorphisms, or by using the algorithm of [21] to reconstruct unique $\mathbf{F}_7$-isomorphism class representatives

of all twists with these Dixmier-Ohno invariants and verifying that C_1 and C_2 are isomorphic to distinct representatives. As observed by one of the referees, these curves are isomorphic over $\mathbf{Q}(i)$ via the maps $(x : y : z) \mapsto (z : ix : (1-i)x/2 - y)$ and $(iy : (1+i)y/2 + z : -x) \leftarrow\!\shortmid (x : y : z)$.

6. Examples

We conclude with a list of the curves $f(x,y,z) = 0$ that we found with absolute discriminants less than 10^4:

$\lvert\Delta\rvert$	$f(x,y,z)$
2940	$x^3y + x^3z + x^2y^2 + 3x^2yz + x^2z^2 - 4xy^3 - 3xy^2z - 3xyz^2 - 4xz^3$ $+2y^4 + 3y^2z^2 + 2z^4$
4727	$x^3z + x^2z^2 + xy^3 - xy^2z + y^2z^2 - yz^3$
5835	$x^4 + 2x^3y + 2x^3z - 4x^2y^2 + 2x^2yz - 4x^2z^2 - xy^3 - xz^3 + 2y^4$ $-3y^3z + 5y^2z^2 - 3yz^3 + 2z^4$
5978	$x^3z + x^2y^2 + x^2yz + xy^3 + xy^2z + xyz^2 + xz^3 + y^3z + y^2z^2$
6050	$x^3z + x^2y^2 + xy^3 - xy^2z - 2xz^3 - y^2z^2 - z^4$
6171	$x^3z + x^2yz + x^2z^2 - xy^3 + xy^2z + xz^3 - y^2z^2 + yz^3$
6608	$x^3z + x^2yz + x^2z^2 + xy^3 - 3xy^2z - 4xz^3 - y^4 + 2y^3z + 2z^4$
7376	$x^3z + x^2y^2 + x^2z^2 + xy^3 + xyz^2 + y^3z + yz^3$
8107	$x^3z + x^2yz + x^2z^2 + xy^3 + xyz^2 + y^3z + y^2z^2 + yz^3$
8233	$x^3z + x^2yz + x^2z^2 + xy^3 - xy^2z + y^4 - y^3z - yz^3$
8325	$x^3z + x^2y^2 - 2x^2z^2 + y^3z - 2y^2z^2 + z^4$
8471	$x^3z + x^2y^2 - x^2z^2 + xy^3 - xy^2z + xyz^2 - xz^3 + y^3z - y^2z^2$
9607	$x^3z + x^2yz + x^2z^2 - xy^3 + xyz^2 + y^2z^2 + yz^3$

Table 2. Smooth plane quartics over $\mathbf{Q}$ of small discriminant.

Of the 13 absolute discriminants listed in Table 2, exactly one is prime, 8233, which arises for the curve

$$C_1 \colon x^3z + x^2yz + x^2z^2 + xy^3 - xy^2z + y^4 - y^3z - yz^3 = 0.$$

As noted in the introduction, in a similar search of hyperelliptic curves of genus 3, the smallest prime absolute discriminant that appears is also 8233, for the hyperelliptic curve

$$C_2 \colon y^2 + (x^4 + x^3 + x^2 + 1)y = x^7 - 8x^5 - 4x^4 + 18x^3 - 3x^2 - 16x + 8.$$

We used the average polynomial-time algorithms described in [15, 16, 17] to compute Frobenius traces at every prime $p \neq 8233$ up to 2^{28} for both curves and found that they coincide in every case. This is compelling evidence that the Jacobians of the two curves are isogenous. Computation of their period matrices by Nils Bruin suggest that they are related by an isogeny whose kernel is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^4 \times \mathbf{Z}/4\mathbf{Z}$. In principle, one can use trace computations to prove or disprove the existence of an isogeny via a Faltings-Serre argument (see [4, Thm. 2.1.5] for an effective algorithm), but we have not attempted to do so.

We have confirmed that the Jacobians of these curves are generic in the sense that their Mumford-Tate groups are as large as possible (all of GSp_6). In genus 3 this is equivalent to having no extra endomorphisms over $\overline{\mathbf{Q}}$ (type I in Albert's classification), see [23, §2.3], and to having large Galois image (open in $\mathrm{GSp}_6(\hat{\mathbf{Z}})$), see [6]. To prove this it is enough to show that for some prime ℓ the image of the Galois representation given by the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the ℓ-torsion subgroup of $\mathrm{Jac}(C_i)$ contains $\mathrm{Sp}_6(\mathbf{Z}/\ell\mathbf{Z})$: from the proof of [28, Lem. 2.4] the image of the ℓ-adic representation must then contain $\mathrm{Sp}(\mathbf{Z}_\ell)$, which in turn implies that the Mumford-Tate group is GSp_6.

Taking $\ell = 5$, if we compute the characteristic polynomial of Frobenius at the primes $p = 31, 41$ and reduce modulo $\ell = 5$ we obtain

$$\bar{f}_{31}(t) := t^6 + t^4 + 3t^3 + t^2 + 1 \qquad \text{and} \qquad \bar{f}_{41}(t) := t^6 + 4t^4 + 2t^3 + 4t^2 + 1,$$

A computation in Magma shows that among the maximal subgroups of $\mathrm{Sp}_6(\mathbf{Z}/5\mathbf{Z})$ (ten, up to conjugacy), none contain a pair of elements that realize these two characteristic polynomials; see the Magma scripts in [27] for details. This proves that the mod-5 Galois image contains $\mathrm{Sp}_6(\mathbf{F}_5)$; as argued above, this implies that the Mumford-Tate groups of the Jacobians of the curves C_1 and C_2 are both maximal, and the curves are thus generic.

References

[1] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus 2 curves over the rational numbers*, in *Algorithmic Number Theory (ANTS XII)*, LMS J. Comput. Math. **19** (2016), 235–254. 1, 3, 3

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265. 2.2

[3] George Boole, *Notes on linear transformation*, Cambridge Math. J. **4** (1845), 167–171. 2.1

[4] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaria, John Voight, and David S. Yuen, *On the paramodularity of typical abelian surfaces*, arXiv:1805.10873. 6

[5] David Cox, John Little, and Donal O'Shea, *Using algebraic geometry*, Springer, 1998. 2.1

[6] Anna Cadoret and Ben Moonen, *Integral and adelic aspects of the Mumford-Tate conjecture*, J. Inst. Math. Jussieu (2018), 1–22. 6

[7] John E. Cremona, *The elliptic curve database for conductors to 130000*, in *Algorithmic Number Theory (ANTS VII)* (F. Hess, S. Pauli, M. Pohst eds.), LNCS **4076**, Springer, 2006, 11–29. 1

[8] Jacques Dixmier *On the projective invariants of plane quartic curves*, Adv. in Math. **64** (1987), 279–304. 2.2

[9] Andreas-Stephan Elsenhans, *Explicit computation of invariants of plane quartic curves*, J. Symbolic Comput. **68** (2015), 109–115. 2.2

[10] Jean-Marc Fontaine *Il n'y a pas de variété abélienne sur* $\mathbf{Z}$, Invent. Math. **81** (1985), 515–538. 1

[11] Israel M. Gelfand, Mikhail M. Kapranov, Andrei V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Birkhäuser, 1994. 2, 2.3, 2, 2.1, 2.1, 2.6

[12] Martine Gerard and David R. Kohel, *Classification of genus 3 curves in special strata of the moduli space*, in *Algorithmic Number Theory (ANTS VII)*, F. Hess, S. Pauli, and M. Pohst. (eds), LNCS **4076**, Springer, 2006, 346–360. 2.2

[13] Google LLC, *Google Compute Engine Documentation*, available at `https://cloud.google.com/compute/docs/`, accessed June 2017. 4

[14] David Harvey, Maike Massierer, and Andrew V. Sutherland *Computing L-series of geometrically hyperelliptic curves of genus three*, in *Algorithmic Number Theory (ANTS XII)*, LMS J. Comput. Math. **19** (2016), 220-234. 1.1

[15] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, in *Algorithmic Number Theory (ANTS XI)*, LMS J. Comput. Math. **17** (2014), 257–273. 6

[16] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*, in *Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures* (D. Kohel and I. E. Shparlinski eds.), Contemporary Math. **663**, AMS, 127–148. 6

[17] David Harvey and Andrew V. Sutherland, *Counting points on smooth plane quartics in average polynomial time*, in preparation. 6

[18] Everett W. Howe, *Infinite families of pairs of curves over Q with isomorphic Jacobians*, J. London Math. Soc. **72** (2005), 327–350. 1

[19] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, in *Algorithmic Number Theory (ANTS VIII)* (A. J. van der Poorten, A. Stein eds.), LNCS **5011**, Springer, 2008, 312–326. 3, 5

[20] Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta, Jeroen Sijsling, *Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields*, in *Algorithmic Number Theory (ANTS XI)*, LMS J. Comput. Math. **17** (2014), 128–147. 2.2

[21] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Reconstructing plane quartics from the invariants*, arXiv:1606.05594. 2.2, 5

[22] The LMFDB Collaboration, *The L-functions and modular forms database*, available at `http://www.lmfdb.org`. 1

[23] Ben Moonen and Yuri Zharin, *Hodge classes on abelian varieties of low dimension*, Math. Ann. **315** (1999), 711–733. 6

[24] Toshiaki Ohno, *The graded ring of invariants of ternary quartics I*, unpublished 2007 preprint, available at `https://www.win.tue.nl/~aeb/math/ohno-preprint.2007.05.15.pdf`. 2.2

[25] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **86** (1967), 1022–1046. 2.2

[26] Jeroen Sijsling, *A Magma package for reconstructing plane quartics from Dixmier-Ohno invariants*, GitHub repository, available at `https://github.com/JRSijsling/quartic_reconstruction`. 2.2, 5

[27] Andrew V. Sutherland, Data and Magma scripts related to *A database of nonhyperelliptic genus 3 curves over* **Q**, available at `https://math.mit.edu/~drew`. 1, 2.6, 2.1, 2.2, 6

[28] David Zywina, *An explicit Jacobian of dimension 3 with maximal Galois action*, arXiv:1508.07655. 6

COUNTING POINTS ON GENUS-3 HYPERELLIPTIC CURVES WITH EXPLICIT REAL MULTIPLICATION

SIMON ABELARD, PIERRICK GAUDRY, AND PIERRE-JEAN SPAENLEHAUER

Abstract. We propose a Las Vegas probabilistic algorithm to compute the zeta function of a genus-3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, with explicit real multiplication by an order $\mathbb{Z}[\eta]$ in a totally real cubic field. Our main result states that this algorithm requires an expected number of $\widetilde{O}((\log q)^6)$ bit-operations, where the constant in the $\widetilde{O}()$ depends on the ring $\mathbb{Z}[\eta]$ and on the degrees of polynomials representing the endomorphism η. As a proof-of-concept, we compute the zeta function of a curve defined over a 64-bit prime field, with explicit real multiplication by $\mathbb{Z}[2\cos(2\pi/7)]$.

1. Introduction

Since the discovery of Schoof's algorithm [25], the problem of computing efficiently zeta functions of curves defined over finite fields has attracted a lot of attention, as its applications range from the construction of cryptographic curves to testing conjectures in number theory. We focus on the problem of computing the zeta function of a hyperelliptic curve $\mathcal{C}$ of genus 3 defined over a finite field $\mathbb{F}_q$ using ℓ-adic methods, in the spirit of Schoof's algorithm and its generalizations [23, 18, 2]. Although these methods are polynomial with respect to $\log q$, the exponents in the best known complexity bounds grow quickly with the genus. Another line of research is to use p-adic methods [19, 24, 8, 15], which are polynomial in the genus but exponential in the size of the characteristic of the underlying finite field. Variants of these methods [20, 16, 17] allow to count the points of a curve defined over the rationals modulo many primes in average polynomial time, which is especially relevant when experimenting with the Sato-Tate conjecture.

The aim of this paper is to show — both with theoretical proofs and practical experiments — that the complexity of ℓ-adic methods for genus-3 hyperelliptic curves can be dramatically decreased as soon as an explicitly computable non-integer endomorphism $\eta \in \mathrm{End}(\mathrm{Jac}(\mathcal{C}))$ is known. More precisely, we say that a curve $\mathcal{C}$ has *explicit real multiplication* by $\mathbb{Z}[\eta]$ if the subring $\mathbb{Z}[\eta] \subset \mathrm{End}(\mathrm{Jac}(\mathcal{C}))$ is isomorphic to an order in a totally real cubic number field, and if we have explicit formulas describing $\eta(P - \infty)$ for some fixed base point ∞ and a generic point P of C. By explicit formulas, we mean polynomials $(\eta_i^{(u)}(x,y))_{i\in\{0,1,2,3\}}$ and $(\eta_i^{(v)}(x,y))_{i\in\{0,1,2,3\}}$ in $\mathbb{F}_q[x,y]$, such that, when $\mathcal{C}$ is given in odd-degree Weierstrass form, the Mumford coordinates of $\eta((x,y)-\infty)$ are $\left\langle \sum_{i=0}^{3} \eta_i^{(u)}(x,y)X^i, \sum_{i=0}^{2} \left(\eta_i^{(v)}(x,y)/\eta_3^{(v)}(x,y)\right)X^i \right\rangle$, where (x,y) is the generic point of the curve. In cases where $\mathcal{C}$ does not have an odd-degree Weierstrass model, we can work in an extension of degree at most 8 of the base field in order to ensure the existence of a rational Weierstrass point.

The influence of real multiplication on the complexity of point counting was investigated for genus 2 curves in [12], where the authors decrease the complexity

14 Jun 2018 07:45:01 PDT
Version 3 - Submitted to Open Book Series

from $\widetilde{O}((\log q)^8)$ [14] to $\widetilde{O}((\log q)^5)$. For genus 2 curves, another related active line of research is to mimic the improvement of Elkies and Atkin by using modular polynomials [3]. However, the main difficulty of this method is to precompute the modular polynomials, which are much larger than their genus 1 counterparts.

Our main result is the following theorem.

Theorem 1. *Let $\mathcal{C}$ be a genus-3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$ having explicit real multiplication by $\mathbb{Z}[\eta]$, where $\eta \in \mathrm{End}(\mathrm{Jac}(C))$. We assume that $\mathcal{C}$ is given by an odd-degree Weierstrass equation $Y^2 = f(X)$. The characteristic polynomial of the Frobenius endomorphism on the Jacobian of $\mathcal{C}$ can be computed with a Las Vegas probabilistic algorithm in expected time bounded by $c\,(\log q)^6(\log\log q)^k$, where k is an absolute constant and c depends only on the degrees of the polynomials $\eta_i^{(u)}$ and $\eta_i^{(v)}$ and on the ring $\mathbb{Z}[\eta]$.*

In this paper, we use the notation $\widetilde{O}()$ as a shorthand for complexity statements hiding poly-logarithmic terms: the complexity in the theorem would be abbreviated $\widetilde{O}((\log q)^6)$. We insist on the fact that all the $O()$ and the $\widetilde{O}()$ notation used throughout the paper should be understood up to a multiplicative constant which may depend on the ring $\mathbb{Z}[\eta]$ and on the degrees of the polynomials $\eta_i^{(u)}$ and $\eta_i^{(v)}$. There are natural families of curves for which these degrees are bounded by an absolute constant and for which $\mathbb{Z}[\eta]$ is fixed: reductions at primes (of good reduction) of a hyperelliptic curve with explicit RM defined over a number field.

As in Schoof's algorithm and its generalizations in [23, 18, 2], the ℓ-adic approach consists in computing the characteristic polynomial of the Frobenius endomorphism by computing its action on the ℓ-torsion of the Jacobian of the curve for sufficiently many ℓ. In order to prove the claimed complexity bound, we consider primes $\ell \in \mathbb{Z}$ such that $\ell\mathbb{Z}[\eta]$ splits as a product $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ of prime ideals. Computing the kernels of endomorphisms α_i in each $\mathfrak{p}_i$ provides us with an algebraic representation of the ℓ-torsion $\mathrm{Jac}(\mathcal{C})[\ell] \subset \mathrm{Ker}\,\alpha_1 + \mathrm{Ker}\,\alpha_2 + \mathrm{Ker}\,\alpha_3$. Then, we compute from this representation integers $a, b, c \in \mathbb{Z}/\ell\mathbb{Z}$ such that the sum $\pi + \pi^\vee$ of the Frobenius endomorphism and its dual equals $a + b\eta + c\eta^2 \bmod \ell$. Once enough modular information is known, the values of a, b, c such that $\pi + \pi^\vee = a + b\eta + c\eta^2$ are recovered via the Chinese Remainder Theorem and the coefficients of the characteristic polynomial of the Frobenius can be directly expressed in terms of a, b and c. In fact, in practice we do not have to restrict to split primes: any partial factorization of $\ell\mathbb{Z}[\eta]$ provides some modular information on $a, b, c \bmod \ell$. We give an example with a ramified prime in Section 7.1; but on the theoretical side, considering non-split primes does not improve the asymptotic complexity.

The cornerstone of the complexity analysis is the cost of the computation of the kernels of the endomorphisms. This is achieved by solving a polynomial system. Using resultant-based elimination techniques and degree bounds on Cantor's polynomials, we prove that we can solve these equations in time quadratic in the number of solutions, which leads to the claimed complexity bound. For practical computations, we replace the resultants by Gröbner bases and we retrieve modular information only for small ℓ to speed up an exponential collision search which can be massively run in parallel. Although using Gröbner basis seems to be more efficient in practice, we do not see any hope of proving with rigorous arguments that it is asymptotically competitive.

14 Jun 2018 07:45:01 PDT
Version 3 - Submitted to Open Book Series

As a proof-of-concept, we have implemented our algorithm and we provide experimental results. In particular, we were able to compute the zeta function of a genus 3 hyperelliptic curve with explicit RM defined over $\mathbb{F}_p$ with $p = 2^{64} - 59$. To our knowledge the largest genus-3 computation that had be achieved previously was the computation of the zeta function of a general hyperelliptic curve defined over $\mathbb{F}_p$ with $p = 2^{61} - 1$, done by Sutherland [27] using p-adic methods.

Examples of curves with RM are given by modular curves. For instance, the genus-3 curve $y^2 = x^7 + 3x^6 + 2x^5 - x^4 - 2x^3 - 2x^2 - x - 1$ is a quotient of $X_0(284)$ and therefore has real multiplication by an element of $\mathbb{Q}[x]/(x^3 - 3x - 1)$. This follows from the properties of the Hecke operators as explained in [26, Chapter 7]. Based on this theory, algorithms for constructing such curves are explained in [11]; however the explicit expression for the real endomorphism is not given. We expect that tracking the Hecke correspondences along their construction, and using techniques like in [29] to reconstruct the rational fractions describing the real endomorphism could solve this question. In any case, these are only isolated points in the moduli space. Larger families are obtained from cyclotomic covering. This line of research has produced several families of hyperelliptic genus-3 curves having explicit RM by $\mathbb{Z}[2\cos(2\pi/7)]$. In particular, explicit such families are given in [22] and [28], and explicit formulas for their RM endomorphism are obtained in [21]. We use the 1-dimensional family of curves from [28, Theorem 1 with $p = 7$] for our experiments. Other families of genus-3 curves (but not necessarily hyperelliptic) with RM have been made explicit in [6, Chapter 2], following [10]. We would like to point out that within the moduli space of complex polarized abelian varieties of dimension 3, those with RM by a fixed order in a cubic field form a moduli space of codimension 3 [4, Sec. 9.2]. Since Jacobians of hyperelliptic curves form a codimension 1 space, we would expect the moduli space of hyperelliptic curves of genus 3 with RM by a given cubic order to have dimension 2.

We finally briefly mention how our algorithm and analysis could be extended in several directions. First, the complexity analysis leads, with small modifications, to a point-counting algorithm for general genus-3 hyperelliptic curves (i.e. without RM) with complexity in $\widetilde{O}((\log q)^{14})$. Second, if the curve is not hyperelliptic, the main difficulty is to define analogues of Cantor's division polynomials and get bounds on their degrees. Without them, it is still possible to use an explicit group law to derive a polynomial system for the kernel of an endomorphism, but getting a proof for its degree would require to take another path than what we did. Still, the complexities with or without RM are expected to remain the same for plane quartics as for genus-3 hyperelliptic curves. Third, if we go to higher genus hyperelliptic curves with RM, the main difficulty to extend our approach is in the complexity estimate of the polynomial system solving, because resultant-based approaches are not competitive when the number of variables grows, and a tedious analysis like in [1] seems to be necessary.

The article is organized as follows. Section 2 gives a bird-eye view of our algorithm, along with a complexity analysis relying on the technical results detailed in Sections 3 to 6. Practical experiments are presented in Section 7.

Acknowledgements. We are grateful to Benjamin Smith for fruitful discussions and to Allan Steel for his help with memory issues with Magma. We also wish to thank anonymous referees for their comments which helped improve the paper.

2. Overview of the algorithm

Let $\mathcal{C}$ be a genus-3 hyperelliptic curve over a finite field $\mathbb{F}_q$ with explicit RM, and let η be the given explicit endomorphism. We denote by μ_0, μ_1, μ_2 the coefficients of the minimal polynomial $T^3 + \mu_2 T^2 + \mu_1 T + \mu_0$ of η over $\mathbb{Q}$.

2.1. **Bounds.** The characteristic polynomial of the Frobenius endomorphism π is of the form $\chi_\pi(T) = T^6 - \sigma_1 T^5 + \sigma_2 T^4 - \sigma_3 T^3 + q\sigma_2 T^2 - q^2\sigma_1 T + q^3$, and Weil's bounds give

$$|\sigma_1| \leq 6\sqrt{q}, \quad |\sigma_2| \leq 15q, \quad |\sigma_3| \leq 20q^{3/2}.$$

In order to take advantage of the explicit RM, we consider the endomorphism $\psi = \pi + \pi^\vee$, for which we can derive the real Weil's polynomial $\chi_\psi(T) = T^3 - \sigma_1 T^2 + (\sigma_2 - 3q)T - (\sigma_3 - 2q\sigma_1)$, which corresponds to the characteristic polynomial of ψ viewed as an element of the real subfield of $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q}$. The endomorphism ψ belongs to the ring of integers of $\mathbb{Q}(\eta)$. The ring $\mathbb{Z}[\eta]$ might be a proper suborder of the ring of integers, so let us call Δ its index, so that ψ can be written $\psi = a + b\eta + c\eta^2$, where a, b, c are rationals with a denominator that divides Δ. By computing formally the characteristic polynomial of $a + b\eta + c\eta^2$ in $\mathbb{Q}(\eta)$ and by equating it with the expression for the real Weil's polynomial $\chi_\psi(T)$, we obtain a direct way to compute σ_1, σ_2 and σ_3 in terms of a, b, c:

$$\begin{aligned}
\sigma_1 &= 3\,a - b\,\mu_2 - 2\,c\,\mu_1 + c\,\mu_2^2\ , \\
\sigma_2 - 3q &= 3\,a^2 - 2\,a\,b\,\mu_2 + 2\,a\,c\,(\mu_2^2 - 2\mu_1) + b^2\,\mu_1 + 3\,b\,c\,\mu_0 - b\,c\,\mu_1\,\mu_2 - \\
&\qquad c^2\,(2\,\mu_0\,\mu_2 + \mu_1^2)\ , \\
\sigma_3 - 2q\sigma_1 &= a^3 - a^2\,b\,\mu_2 + a^2\,c\,(\mu_2^2 - 2\mu_1) + a\,b^2\,\mu_1 + a\,b\,c\,(3\,\mu_0 - \mu_1\,\mu_2) + \\
&\qquad a\,c^2\,(\mu_1^2 - 2\,\mu_0\,\mu_2) - b^3\,\mu_0 + b^2\,c\,\mu_0\,\mu_2 - b\,c^2\,\mu_0\,\mu_1 + c^3\,\mu_0^2\ .
\end{aligned} \tag{1}$$

In Section 4, it is shown that the coefficients a, b and c can be bounded in $O(\sqrt{q})$. More precisely, we denote by C_{abc} a constant that depends only on η such that their absolute values are bounded by $C_{abc}\sqrt{q}$. Since these bounds are much smaller than the bounds for σ_1, σ_2, σ_3, it makes sense to design an algorithm that reconstruct these coefficients of ψ instead of the coefficients of χ_π as in the classical Schoof algorithm, and this is what we are going to do later on.

Another important bound that we need concerns the size of small elements that can be found in ideals of $\mathbb{Z}[\eta]$. Let ℓ be a prime that splits completely in $\mathbb{Z}[\eta]$, so that we can write $\ell = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where the $\mathfrak{p}_i$'s are distinct prime ideals of norm ℓ. In Section 5, it is shown that each $\mathfrak{p}_i$ contains a non-zero element $\alpha_i = a_i + b_i\eta + c_i\eta^2$, where a_i, b_i and c_i are integers and are bounded in absolute value by $O(\ell^{1/3})$.

2.2. **Algorithms.** The general RM point counting algorithm is Algorithm 1. We give a description of it, allowing some black-box primitives that will be detailed in dedicated sections. As mentioned above, we will work with the a, b, c coefficients of the ψ endomorphism. More precisely, we compute their values modulo sufficiently many completely split primes ℓ until we can deduce their values from the bounds of Lemma 5 by the Chinese Remainder Theorem, taking into account their potential denominator Δ. Then the coefficients of χ_π are deduced by Equations (1).

We now explain how the algorithm works for a given split ℓ. First its decomposition as a product of prime ideals $\ell\mathbb{Z}[\eta] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ is computed, and for each prime ideal $\mathfrak{p}_i$, a non-zero element α_i of $\mathfrak{p}_i$ is found with a small representation $\alpha_i = a_i + b_i\eta + c_i\eta^2$ as in Lemma 6. In fact, $\mathfrak{p}_i$ is not necessarily principal and α_i need not generate $\mathfrak{p}_i$. The kernel of α_i is denoted by $J[\alpha_i]$ and it contains a subgroup G_i isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, since the norm of α_i is a multiple of ℓ. The

two-element representation $(\ell, \eta - \lambda_i)$ of the ideal $\mathfrak{p}_i$ implies that λ_i is an eigenvalue of η regarded as an endomorphism of $J[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^6$.

On $G_i \subset J[\alpha_i]$, the endomorphism η acts as the multiplication by λ_i. Therefore, $\psi = a + b\eta + c\eta^2$ also acts as a scalar multiplication on this 2-dimensional space, and we write $k_i \in \mathbb{Z}/\ell\mathbb{Z}$ the corresponding eigenvalue: for any D_i in G_i, we have $\psi(D_i) = k_i D_i$. On the other hand, from the definition of ψ, it follows that $\psi\pi = \pi^2 + q$. Therefore, if such a D_i is known, we can test which value of $k_i \in \mathbb{Z}/\ell\mathbb{Z}$ satisfies

$$k_i\pi(D_i) = \pi^2(D_i) + qD_i. \tag{2}$$

Since ℓ is a prime and D_i is of order exactly ℓ, this is also the case for $\pi(D_i)$. Finding k_i can then be seen as a discrete logarithm problem in the subgroup of order ℓ generated by $\pi(D_i)$; hence the solution is unique. Equating the two expressions for ψ, we get explicit relations between a, b, c modulo ℓ:

$$a + b\lambda_i + c\lambda_i^2 \equiv k_i \bmod \ell.$$

Therefore we have a linear system of three equations in three unknowns, the determinant of which is the Vandermonde determinant of the λ_i, which are distinct by hypothesis. Hence the system can be solved and it has a unique solution modulo ℓ.

Data: q an odd prime power, and $f \in \mathbb{F}_q[X]$ a monic squarefree polynomial of degree 7 such that the curve $Y^2 = f(X)$ has explicit RM by $\mathbb{Z}[\eta]$.
Result: The characteristic polynomial $\chi_\pi \in \mathbb{Z}[T]$ of the Frobenius endomorphism on the Jacobian J of the curve.
$R \leftarrow 1$;
while $R \leq 2\,\Delta\, C_{abc}\sqrt{q} + 1$ **do**
  Pick the next prime ℓ that satisfies conditions (C1) to (C4);
  Compute the ideal decomposition $\ell\,\mathbb{Z}[\eta] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, corresponding to the eigenvalues λ_1, λ_2, λ_3 of η in $J[\ell]$;
  for $i \leftarrow 1$ **to** 3 **do**
    Compute a small element α_i of $\mathfrak{p}_i$ as in Lemma 6;
    Compute a non-zero element D_i of order ℓ in $J[\alpha_i]$;
    Find the unique $k_i \in \mathbb{Z}/\ell\mathbb{Z}$ such that $k_i\pi(D_i) = \pi^2(D_i) + qD_i$;
  end
  Find the unique triple (a, b, c) in $(\mathbb{Z}/\ell\mathbb{Z})^3$ such that $a + b\lambda_i + c\lambda_i^2 = k_i$, for i in $\{1, 2, 3\}$;
  $R \leftarrow R \cdot \ell$;
end
Reconstruct (a, b, c) using the Chinese Remainder Theorem ;
Deduce χ_π from Equations (1).

Algorithm 1: Overview of our RM point-counting algorithm

It remains to show how to construct a divisor D_i in G_i, i.e. an element of order ℓ in the kernel $J[\alpha_i]$. Since an explicit expression of η as an endomorphism of the Jacobian of $\mathcal{C}$ is known, an explicit expression can be deduced for α_i, using the explicit group law. The coordinates of the elements of this kernel are solutions of a polynomial system that can be directly derived from this expression of α_i. Using standard techniques, it is possible to find the solutions of this system in a finite

extension of the base field (of degree bounded by the degree of the ideal generated by the system, i.e. in $O(\ell^2)$), from which divisors in $J[\alpha_i]$ can be constructed. Multiplying by the appropriate cofactor, we can reach all the elements of G_i; but we stop as soon as we get a non-trivial one.

We summarize the conditions that must be satisfied by the primes ℓ that we work with:

(C1) ℓ must be different from the characteristic of the base field;
(C2) ℓ must be coprime to the discriminant of the minimal polynomial of η;
(C3) there must exist $\alpha_i \in \mathfrak{p}_i$ as in Lemma 6 with norm non-divisible by ℓ^3 for $i \in \{1, 2, 3\}$;
(C4) the ideal $\ell\mathbb{Z}[\eta]$ must split completely.

The first 3 conditions eliminate only a finite number of ℓ's that depends only on η, while the last one eliminate a constant proportion. The condition (C3) implies that there is a unique subgroup G_i of order ℓ^2 in $J[\alpha_i]$ (our description of the algorithm could actually be adapted to handle the cases where this is not true).

Algorithm 1 is a very natural extension of the one described in [12] for genus 2 curves with RM. Already in [12], the action of the real endomorphism $\psi = \pi + \pi^\vee$ is studied on subspaces $J[\mathfrak{p}_i]$ of the ℓ-torsion, and the corresponding eigenvalues are collected and used to reconstruct information modulo ℓ. In genus 3, we have 3 such 2-dimensional subspaces and eigenvalues to compute and recombine instead of 2 in genus 2. The main differences between the present work and [12] are the way the ℓ-torsion elements are constructed with polynomial systems and the bounds on the coefficients of ψ. In both cases, going from dimension 2 to 3 is not immediate.

2.3. **Complexity analysis.** The field $\mathbb{Q}(\eta)$ is of degree 3, so its Galois group has order at most 6 and by Chebotarev's density theorem the density of primes that split completely is at least $1/6$. Therefore the main loop is done $O(\log q/\log\log q)$ times, with primes ℓ that are in $O(\log q)$. All the steps that take place in the number field take a negligible time. For instance, a small generator like in Lemma 6 can be found by exhaustive search: only $O(\ell)$ trials are needed since we are searching over all elements of the form $a + b\eta + c\eta^2$, with $|a|, |b|, |c|$ in $O(\ell^{1/3})$.

The bottleneck of the algorithm is the computation of a non-zero element of order ℓ in the kernel $J[\alpha_i]$ of α_i. This part will be treated in detail in Section 3, where it is shown to be feasible in $\widetilde{O}(\ell^4)$ operations in $\mathbb{F}_q$. The output is a divisor D_i of order ℓ in $J[\alpha_i]$ that is defined over an extension field $\mathbb{F}_{q^\delta}$, where δ is in $O(\ell^2)$.

In order to check Equation (2), we first need to compute $\pi(D_i)$ and $\pi^2(D_i)$ which amounts to raising the coordinates to the q-th power. The cost is in $\widetilde{O}(\ell^2 \log q)$ operations in $\mathbb{F}_q$. Then, each Jacobian operation in the group generated by $\pi(D_i)$ costs $\widetilde{O}(\ell^2)$ operations in the base field, and we need $O(\sqrt{\ell})$ of them to solve the discrete logarithm problem given by Equation (2). The overall cost of finding k_i, once D_i is known is therefore $\widetilde{O}(\ell^2(\sqrt{\ell} + \log q))$ operations in $\mathbb{F}_q$.

Finally, the amount of work performed for each ℓ is $\widetilde{O}(\ell^2(\ell^2 + \log q))$ operations in the base field $\mathbb{F}_q$. Summing up for all the primes, and taking into account the cost of the operations in $\mathbb{F}_q$, we obtain a global bit-complexity of $\widetilde{O}((\log q)^6)$.

3. Computing kernels of endomorphisms

3.1. **Modelling the kernel computation by a polynomial system.** Let α be an explicit endomorphism of degree $O(\ell^2)$ on the Jacobian of $\mathcal{C}$, which satisfies the properties of Lemma 6. In particular, α vanishes on a subspace of $J[\ell]$. We want to compute a triangular polynomial system that describes the kernel $J[\alpha]$ of α. This will provide us with a nice description of a subgroup of the ℓ-torsion on which we will be able to test the action of $\psi = \pi + \pi^\vee$ and deduce a, b, c such that $\psi = a + b\eta + c\eta^2 \bmod \ell$.

We first model $J[\alpha]$ by a system of polynomial equations that we will then put in triangular form. To do so, we consider a generic divisor $D = P_1 + P_2 + P_3 - 3\infty$, where P_i is an affine point of $\mathcal{C}$ of coordinates (x_i, y_i). We then write $\alpha(D) = 0$, i.e $\alpha(P_1 - \infty) + \alpha(P_2 - \infty) = -\alpha(P_3 - \infty)$. Generically, we expect each $\alpha(P_i - \infty)$ to be of weight 3, and we write $\langle u_i, v_i\rangle$ for its Mumford form. We derive our equations by computing the Mumford form $\langle u_{12}, v_{12}\rangle$ of $\alpha(P_1 - \infty) + \alpha(P_2 - \infty)$ and then writing coefficient-wise the conditions $u_{12} = u_3$ and $v_{12} = -v_3$. The case where the genericity conditions are not satisfied is discussed at the end of the section.

Similarly to the Schoof-Pila algorithm, we define polynomials — which are equivalent to Cantor's division polynomials — by the formulas

$$u_{12}(X) = X^3 + \sum_{i=0}^{2} \frac{\tilde{d}_i(x_1, x_2, y_1, y_2)}{\tilde{d}_3(x_1, x_2)} X^i, \quad v_{12}(X) = \sum_{i=0}^{2} \frac{\tilde{e}_i(x_1, x_2, y_1, y_2)}{\tilde{e}_3(x_1, x_2)} X^i,$$
$$u_3(X) = X^3 + \sum_{i=0}^{2} \frac{d_i(x_3)}{d_3(x_3)} X^i, \quad v_3(X) = y_3 \sum_{i=0}^{2} \frac{e_i(x_3)}{e_3(x_3)} X^i.$$

Lemma 2. *For any $i \in \{1, 2, 3\}$, the degrees of $\tilde{d}_i$, $\tilde{e}_i$, d_i and e_i are in $O(\ell^{2/3})$.*

Proof. Let us first remark that the $\tilde{d}_i$'s and $\tilde{e}_i$'s are obtained after adding two divisors $\langle u_1, v_1\rangle$ and $\langle u_2, v_2\rangle$ such that the coefficients of the u_i and v_i are respectively the d_j/d_3 and $y_i e_j/e_3$ evaluated at x_i. Thus, since this application of the group law involves a number of operations that is bounded independently of ℓ and q, the degree stays within a constant multiplicative factor, which is captured by the $O()$. Therefore it is enough to prove the result for the d_i's and e_i's.

Since the endomorphism α satisfies the properties of Lemma 6, it is a linear combination of 1, η and η^2 with coefficients of size $O(\ell^{1/3})$. Using the same argument about the group law, we can further reduce our proof to the case where $\alpha = n\eta^k$, with $k \in \{0, 1, 2\}$ and n an integer in $O(\ell^{1/3})$. But once again, η^k does not depend on ℓ so that, provided we can prove that Cantor's n-division polynomials have degrees in $O(n^2)$, we have proven that $n\eta^k(P - \infty) = \eta^k(n(P - \infty))$ have coefficients whose degrees are in $O(n^2)$, and then so does $\alpha(P - \infty)$. This quadratic bound on the degrees of Cantor's division polynomials is proven in Lemma 8 of Section 6 and the result follows. □

3.2. **Solving the system with resultants.** Typical tools for solving a polynomial system are the F4 algorithm, methods based on geometric resolution, or homotopy techniques. To obtain reasonable complexity bounds, they all require some knowledge of the properties of the system, and this might be hard to prove. Since we have a system in essentially 3 variables (in fact, there are six variables $x_1, x_2, x_3, y_1, y_2, y_3$, but the y_i variables can be directly eliminated by using the equation defining the curve), we prefer to stick to an approach based on resultants. It ends up having a

complexity that is quasi-quadratic in the degree of the ideal, which is the best that can be hoped for anyway for all of the advanced techniques, and the complexity analysis requires only elementary tools. A complication that can occur with resultants is that $\mathrm{Res}_x(f,g)$ is identically zero when f and g have a nonconstant GCD. This is not a problem in our case since we can divide polynomials f and g by their GCD, by factoring them at the cost of $O(\max(\deg(f),\deg(g))^\omega)$ field operations — where $\omega \leq 3$ is the exponent of linear algebra — using the bivariate recombination methods in [5] (the trivariate case can be reduced to the bivariate case by using the techniques in [31, Sec. 21.2]). In what follows, the complexities of computing the resultants are larger than $O(\max(\deg(f),\deg(g))^\omega)$, so we can forget about this complication. We also note that since the system is symmetric with respect to x_1 and x_2, it may be possible to decrease the degrees by rewriting the system in terms of elementary symmetric polynomials in x_1 and x_2; however, we do not consider this symmetrization process in the analysis since it may only win a constant factor in the complexity.

Following our modelling, the equality of the u-coordinates gives three equations

$$\forall i \in \{0,1,2\}, \quad \tilde{d}_i(x_1,x_2,y_1,y_2)d_3(x_3) = \tilde{d}_3(x_1,x_2)d_i(x_3), \tag{3}$$

of degree $O(\ell^{2/3})$ in the x_i's. By computing resultants with the equations $y_i^2 = f(x_i)$, we derive three equations $E_i(x_1,x_2,x_3)=0$ whose degrees are still in $O(\ell^{2/3})$.

We then eliminate x_1 by computing 3 trivariate resultants R_i (between the two equations E_j with $j \neq i$). We get three equations $R_i(x_2,x_3)=0$ of degrees $O(\ell^{4/3})$ within a complexity in $\widetilde{O}(\ell^{10/3})$ field operations, as proven in Lemma 4 below.

Then, we compute bivariate resultants S_i (between the two equations R_j with $j \neq i$) to eliminate x_2. From Lemma 3, we get three univariate equations $S_i(x_3)=0$ of degree bounded by $O(\ell^{8/3})$ for a complexity in $\widetilde{O}(\ell^4)$ field operations. And we compute the polynomial $S(x_3)$ as the GCD of the $S_i(x_3)$, which belongs to the ideal defined by our original system.

The bound on the degree of S is much larger than ℓ^2-1, the expected degree of the kernel. Although we can expect the actual degree to be in $O(\ell^2)$, we need to add the constraints coming from the v-coordinates to be able to prove it.

The polynomial system coming from $v_{12} = -v_3$ has the same characteristics as the one coming from the u-coordinates. Therefore, we can proceed in a similar way and deduce, at a cost of $\widetilde{O}(\ell^4)$ operations another univariate polynomial $\tilde{S}(x_3)$ belonging to the ideal. Now, since all the original equations have been taken into account all common roots of S and $\tilde{S}$ will correspond to a solution of the original system for which we know that there are $O(\ell^2)$ solutions. Therefore taking the squarefree part of the GCD of S and $\tilde{S}$ yields a polynomial of degree $O(\ell^2)$.

This univariate polynomial can be factored at a cost of $\widetilde{O}(\ell^4)$ operations in $\mathbb{F}_q$ with standard algorithms [30] (there exist asymptotically faster algorithms, but we already fit in our target complexity). We then deal with each irreducible factor in turn, until one is found that leads to a genuine solution of the original system. Let δ be the degree of such an irreducible factor $\phi(x_3)$. In the field extension $\mathbb{F}_{q^\delta} = \mathbb{F}_q[x_3]/\phi(x_3)$, we have by construction a root x_3 of ϕ. We then solve again the original polynomial system where x_3 is instantiated with this root. This system is bivariate in x_1 and x_2 and there are $O(1)$ solutions, that possibly live in another finite extension $\mathbb{F}_{q^{\delta'}}$ of $\mathbb{F}_{q^\delta}$. Since the degrees of the bivariate polynomials are in $O(\ell^{2/3})$, by Lemma 3, this system solving costs $\widetilde{O}(\ell^2)$ operations in $\mathbb{F}_{q^\delta}$.

A solution obtained in this way must be checked, because it could come from a vanishing denominator that has been cleared when constructing the system or from non-generic situations. But given a set of candidate coordinates for a D_i element of $J[\alpha_i]$, it is cheap to check that this is indeed an element of the Jacobian and that it is killed by α_i. Also, if α_i is not a generator of $\mathfrak{p}_i$, it is necessary to check the order of D_i: if this is a multiple of ℓ, then multiplying D_i by the cofactor gives an order-ℓ element. But it is also possible to get an unlucky element of small order coprime to ℓ, and then we have to take another solution of the system.

Since an operation in $\mathbb{F}_{q^\delta}$ requires a number of operations in $\mathbb{F}_q$ that is quasi-linear in δ, and since the sum of all the degrees δ of the irreducible factors of $\mathrm{GCD}(S, \tilde{S})$ is in $O(\ell^2)$, the amortized cost is $\widetilde{O}(\ell^4)$ operations in $\mathbb{F}_q$ to deduce a divisor D_i in $J[\alpha_i]$.

3.3. **Complexity of bi- and tri-variate resultants.** In this section, the algorithms work by evaluation / interpolation, which requires to have enough elements in the base field. Were it not the case, we simply take a field extension $\mathbb{F}_{q^\delta}$ of $\mathbb{F}_q$, that will add a factor $\widetilde{O}(\delta)$ to the complexity. The complexity of the algorithms will be polynomial in the number of evaluation points, therefore, the final complexity will be logarithmic in δ, so that the cost of taking a field extension will be hidden in the $\widetilde{O}()$ notation. We will therefore not mention this potential complication further.

Another difficulty is that an evaluation / interpolation strategy assumes that the points of evaluation are generic enough, so that all the degrees after evaluation are generic. This is again guaranteed by taking a large enough base field. Still, the algorithm remains a Monte-Carlo one. However, the ultimate goal is to construct kernel elements, which is an easily verified property. Turning this into a Las Vegas algorithm can therefore be done with standard techniques.

Lemma 3. [30, Thm. 6.22 and Cor. 11.21] *Let $P(x, y)$ and $Q(x, y)$ be two polynomials whose degrees in x and y are bounded by d_x and d_y respectively. Then, $R(y) = \mathrm{Res}_x(P, Q)$ can be computed in $\widetilde{O}(d_x^2 d_y)$ field operations, and the degree of R is bounded by $2d_x d_y$.*

Lemma 4. *Let $P(x, y, z)$ and $Q(x, y, z)$ be two polynomials whose degrees in each variable are bounded by d. Then, $R(y, z) = \mathrm{Res}_x(P, Q)$ can be computed in $\widetilde{O}(d^5)$ field operations, and the degree of R in each variable is bounded by $2d^2$.*

Proof. The Sylvester matrix has at most $2d$ columns and its entries are bivariate polynomials whose degrees in y and z are bounded by d. Thus, its determinant is a polynomial whose degrees in y and z are bounded by $2d^2$.

We first perform a Kronecker substitution by considering $\tilde{P}(x, y) = P(x, y, y^{2d^2+1})$ and $\tilde{Q}(x, y) = Q(x, y, y^{2d^2+1})$, which are polynomials of degrees $\leq d$ in x and $\leq 2d^3 + d$ in y. Note that the choice to replace z by y^{2d^2+1} is made to be able to invert the Kronecker substitution after the resultant computation.

Next, we compute $\tilde{R}(y) = \mathrm{Res}_x(\tilde{P}(x, y), \tilde{Q}(x, y))$. By Lemma 3, it is a univariate polynomial of degree at most $4d^4 + 2d^2$ and can be computed in $\widetilde{O}(d^5)$ operations. We can then invert the Kronecker substitution to get $R(y, z)$, which can be done in time linear in the number of monomials, that is in $O(d^4)$. □

3.4. **Non-generic situations.** Our analysis assumes in the first place that the ℓ-torsion elements are generic in a rather strong sense, see e.g. [1, Def. 11] for

details. This is expected to be the case with overwhelming probability, when the base field is large enough and the curve is taken at random in a large family. However, to obtain a proven complexity we must also consider the cases where there exist ℓ-torsion elements that are non-generic. We follow the strategy of [1] where another polynomial system is designed and solved for each non-generic situation, for instance the fact that an ℓ-torsion divisor is of weight less than 3, or that some points involved in the modelling are not distinct while they generically are. We do not give all the details, but the number of polynomial systems to consider is bounded by a constant, and each of these polynomial systems describes a situation that is smaller than the generic one in the sense that it has either less variables or a lower degree, so that the complexity bound is maintained.

4. Bounds on the coefficients of ψ

The system of equations (1) giving σ_1, σ_2 and σ_3 in terms of a, b, c is homogeneous if we put weight $1/2$ to a, b, c and σ_1, weight 1 to q and σ_2, weight $3/2$ to σ_3, and weight 0 to μ_0, μ_1, and μ_2 so any polynomial in a reduced Gröbner basis of the corresponding ideal will have the same property. Computing such a Gröbner basis with the lexicographical ordering $a > b > c > \sigma_1 > \sigma_2 > \sigma_3 > \mu_0 > \mu_1 > \mu_2 > q$ (we did this computation with the Magma V2.23-4 software), we get a polynomial Ψ_c of degree 6 in c that does not involve a or b, and which has the following form:

$$\Psi_c(q, c, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2) = D(\mu_0, \mu_1, \mu_2)^3\, c^6 + \textstyle\sum_{i=0}^{5} \psi_c^{(i)}(q, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2)\, c^i,$$

where $D(\mu_0, \mu_1, \mu_2) = -27\,\mu_0^2 + 18\,\mu_0\mu_1\mu_2 - 4\,\mu_0\mu_2^3 - 4\,\mu_1^3 + \mu_1^2\mu_2^2$ is the discriminant of the polynomial $T^3 + \mu_2\,T^2 + \mu_1\,T + \mu_0$.

By computing Gröbner bases for other lexicographical orderings (with $a > c > b > \sigma_1 > \sigma_2 > \sigma_3 > \mu_0 > \mu_1 > \mu_2 > q$ and $b > c > a > \sigma_1 > \sigma_2 > \sigma_3 > \mu_0 > \mu_1 > \mu_2 > q$ respectively), we obtain that polynomials of the following form also belong to the ideal generated by the polynomials in the system of equations (1):

$$\Psi_b(q, b, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2) = D(\mu_0, \mu_1, \mu_2)^3\, b^6 + \textstyle\sum_{i=0}^{5} \psi_b^{(i)}(q, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2)\, b^i,$$
$$\Psi_a(q, a, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2) = D(\mu_0, \mu_1, \mu_2)^3\, a^6 + \textstyle\sum_{i=0}^{5} \psi_a^{(i)}(q, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2)\, a^i.$$

The polynomials $\psi_a^{(i)}$, $\psi_b^{(i)}$ and $\psi_c^{(i)}$ are homogeneous of weighted degree $3 - i/2$ with respect to the grading given above.

Lemma 5. *The absolute values of the coefficients a, b, c of $\psi = a + b\eta + c\eta^2$ are bounded above by $O(q^{1/2})$.*

Proof. First, we consider the equation $\Psi_c = 0$. We write $c = \widetilde{c}\,q^{1/2}$, $\sigma_1 = \widetilde{\sigma_1}\,q^{1/2}$, $\sigma_2 = \widetilde{\sigma_2}\,q$, $\sigma_3 = \widetilde{\sigma_3}\,q^{3/2}$. Since $\psi_c^{(i)}$ is homogeneous and has weighted degree $3 - i/2$, there is a polynomial $\theta_c^{(i)}(\widetilde{\sigma_1}, \widetilde{\sigma_2}, \widetilde{\sigma_3}, \mu_0, \mu_1, \mu_2)$ such that

$$\psi_c^{(i)}\,(q, \sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2) \cdot c^i = q^3 \widetilde{c}^{\,i}\, \theta_c^{(i)}(\widetilde{\sigma_1}, \widetilde{\sigma_2}, \widetilde{\sigma_3}, \mu_0, \mu_1, \mu_2). \tag{4}$$

Weil's bounds imply that $|\widetilde{\sigma_i}| = O(1)$ for $i \in \{1, 2, 3\}$. Therefore, for all $i \in \{0, \ldots, 5\}$, we obtain that $|\theta_c^{(i)}(\widetilde{\sigma_1}, \widetilde{\sigma_2}, \widetilde{\sigma_3}, \mu_0, \mu_1, \mu_2)| = O(1)$. For fixed $\mu_0, \mu_1, \mu_2 \in \mathbb{Q}$ such that $\mu_0 + \mu_1 T + \mu_2 T^2 + T^3$ is the minimal polynomial of a totally real algebraic number, the discriminant $D(\mu_0, \mu_1, \mu_2)$ must be nonzero. Equations $\Psi_c = 0$ and (4) imply the following inequality:

$$|\widetilde{c}|^6 - \sum_{i=0}^{5} \frac{|\theta_c^{(i)}(\widetilde{\sigma_1}, \widetilde{\sigma_2}, \widetilde{\sigma_3}, \mu_0, \mu_1, \mu_2)|}{|D(\mu_0, \mu_1, \mu_2)|^3} |\widetilde{c}|^i \leq 0.$$

Then $|\widetilde{c}|$ must be smaller or equal to the largest root of this polynomial inequality, which can itself be bounded, for instance, with Cauchy's bound

$$|\widetilde{c}| \leq 1 + \max_{0\leq i\leq 5}\left\{\frac{|\theta_c^{(i)}(\widetilde{\sigma_1},\widetilde{\sigma_2},\widetilde{\sigma_3},\mu_0,\mu_1,\mu_2)|}{|D(\mu_0,\mu_1,\mu_2)|^3}\right\},$$

which shows that $|\widetilde{c}| = O(1)$, and hence $|c| = O(q^{1/2})$. The proof for the bounds on $|a|$ and $|b|$ are similar, using the equations $\Psi_a = 0$ and $\Psi_b = 0$. □

5. Small elements in ideals of $\mathbb{Z}[\eta]$

We first recall that we consider only primes ℓ that do not divide the discriminant of the minimal polynomial of η (Condition (C2)). Hence, if $\mathbb{Z}[\eta]$ is not the maximal order of $\mathbb{Q}(\eta)$, this has no consequence on the factorization properties of ℓ.

Lemma 6. *For any prime ℓ that splits completely in $\mathbb{Z}[\eta]$, each prime ideal $\mathfrak{p}_i$ above ℓ contains a non-zero element α_i of the form $\alpha_i = a_i + b_i\eta + c_i\eta^2$, where $|a_i|$, $|b_i|$ and $|c_i|$ are integers in $O(\ell^{1/3})$, and the norm of α_i is in $O(\ell)$.*

Proof. The coefficients of the elements of the ideal $\mathfrak{p}_i$ represented by polynomials in η form a lattice. Applying Minkowski's bound to this lattice, we obtain the existence of a non-zero element $\alpha_i = a_i + b_i\eta + c_i\eta^2$ in $\mathfrak{p}_i$ for which the L_2-norm of (a_i, b_i, c_i) is in $O(\ell^{1/3})$. From this bound on the L_2-norm, we derive a bound on the L_∞-norm, and finally on the norm of α_i as an algebraic number. At each step, the constant hidden in the $O()$ gets worse but still depends only on $\mathbb{Z}[\eta]$. □

For any given η, it is not difficult to make the constants in the $O()$ fully explicit. We do it in the particular case of $\mathbb{Z}[\eta_7]$, with $\eta_7 = 2\cos(2\pi/7)$, which is the RM used in our practical experiments. Since $\mathbb{Z}[\eta_7]$ is a principal ring, a more direct approach leads to bounds for a generator that are tighter than what would be obtained by a naive application of the previous lemma.

Lemma 7. *Every ideal $\mathfrak{p}_i$ of norm ℓ in $\mathbb{Z}[\eta_7]$ has a generator α_i of the form $a_i + b_i\eta_7 + c_i\eta_7^2$, where $a_i, b_i, c_i \in \mathbb{Z}$ satisfy*

$$|a_i| < 2.415\cdot\ell^{1/3}; \quad |b_i| < 1.850\cdot\ell^{1/3}; \quad |c_i| < 1.764\cdot\ell^{1/3}.$$

Proof. By abuse of notation, we identify $\mathbb{Q}(\eta_7)$ with the algebraic number field $\mathbb{Q}[X]/(X^3 + X^2 - 2X - 1)$ and we let σ_1, σ_2, σ_3 be the three real embeddings of $\mathbb{Q}(\eta_7)$ in $\mathbb{R}$. Let $\epsilon_1 = 1 - \eta_7^2$ and $\epsilon_2 = 1 + \eta_7$ be a pair of fundamental units, and let μ_i be a generator of $\mathfrak{p}_i$. The logarithmic embedding $\varphi : x \mapsto (\log|\sigma_1(x)|, \log|\sigma_2(x)|, \log|\sigma_3(x)|)$ sends the set of generators of $\mathfrak{p}_i$ to the lattice generated by $\varphi(\epsilon_1)$ and $\varphi(\epsilon_2)$ translated by $\varphi(\mu_i)$. Solving a CVP for the projection of $\varphi(\mu_i)$ on the plane where the 3 coordinates sum-up to zero, we deduce a unit ξ_i such that $\alpha_i = \xi_i\mu_i$ is a generator whose real embeddings are bounded by

$$|\sigma_1(\alpha_i)| \leq 2.247\cdot\ell^{1/3}, \quad |\sigma_2(\alpha_i)| \leq 1.803\cdot\ell^{1/3}, \quad |\sigma_3(\alpha_i)| \leq 2.247\cdot\ell^{1/3}.$$

Writing $\alpha_i = a_i + b_i\eta_7 + c_i\eta_7^2$, the real embeddings can also be expressed as $(\sigma_1(\alpha_i), \sigma_2(\alpha_i), \sigma_3(\alpha_i))^T = V\cdot(a_i, b_i, c_i)^T$, where V is the Vandermonde matrix of $(\sigma_1(\eta_7), \sigma_2(\eta_7), \sigma_3(\eta_7))$. A numerical evaluation of its inverse allows to translate the bounds on $\sigma_1(\alpha_i)$, $\sigma_2(\alpha_i)$, $\sigma_3(\alpha_i)$ into the claimed bounds on a_i, b_i, c_i. □

6. Bounding the degrees of Cantor's division polynomials in genus 3

The purpose of this section is to prove the following lemma on the Cantor's division polynomials, which are explicit formulas for the endomorphism corresponding to scalar multiplication [7].

Lemma 8. *In genus 3, the degrees of Cantor's ℓ-division polynomials are bounded by $O(\ell^2)$.*

In [7], there are exact formulas for the degrees of the leading and the constant coefficients d_3 and d_0. However, there is no formula or bounds for the degrees of the other coefficients of the ℓ-division polynomials. Still, our proof strongly relies on [7] and we do not try to make it standalone: we assume that the reader is familiar with this article and all references to expressions, propositions or definitions in this proof are taken from this paper.

For a polynomial P whose coefficients are themselves univariate polynomials, we denote by $\operatorname{maxdeg}(P)$ the maximum of the degrees of its coefficients.

We first prove a bound on the degrees of the coefficients of the quantities α_r and γ_r defined in [7], from which the wanted bounds will follow. The key tools are the recurrence formulas (8.31) and (8.33) that relate quantities at index r to quantities at index around $r/2$, in a similar fashion as for the division polynomials of elliptic curves. More precisely, the following lemma shows that when the index r is (roughly) doubled, $\operatorname{maxdeg}\alpha_r$ and $\operatorname{maxdeg}\gamma_r$ are roughly multiplied by 4, which leads to the expected quadratic growth.

Lemma 9. *Let $\ell \geq 12$, and assume that for all $i \leq (\ell+9)/2$ the degrees $\operatorname{maxdeg}\alpha_i$ and $\operatorname{maxdeg}\gamma_i$ are bounded by C, then $\operatorname{maxdeg}\alpha_\ell$ and $\operatorname{maxdeg}\gamma_\ell$ are bounded by $4C + 36\ell + 108$.*

Proof. We first deal with the bound on $\operatorname{maxdeg}\gamma_\ell$. Let us consider r and s around $\ell/2$ such that $\ell = r + s - 5$: we take either $r = s - 3 = \ell/2 + 1$ if ℓ is even, or $r = s - 4 = (\ell + 1)/2$ otherwise.

From Equations (8.30) and (8.31), the degree of $\gamma_\ell[h]\psi_{s-r}\psi_{r-2}\psi_{s-2}\psi_{r-1}\psi_{s-1}$ is that of the determinant of the matrix $\mathcal{E}_{rs}[h]$ defined by:

$$\mathcal{E}_{rs}[h] = \begin{pmatrix} \alpha_{r-3}\alpha_s[0] & \alpha_{r-3}\alpha_s[1] & \psi_{r-3}\psi_s & \gamma_{r-3}\gamma_s[h] \\ \alpha_{r-2}\alpha_{s-1}[0] & \alpha_{r-2}\alpha_{s-1}[1] & \psi_{r-2}\psi_{s-1} & \gamma_{r-2}\gamma_{s-1}[h] \\ \alpha_{r-1}\alpha_{s-2}[0] & \alpha_{r-1}\alpha_{s-2}[1] & \psi_{r-1}\psi_{s-2} & \gamma_{r-1}\gamma_{s-2}[h] \\ \alpha_r\alpha_{s-3}[0] & \alpha_r\alpha_{s-3}[1] & \psi_r\psi_{s-3} & \gamma_r\gamma_{s-3}[h] \end{pmatrix}.$$

Therefore we have an expression for the degrees of the coefficients of γ_ℓ in terms of objects at index around r and s:

$$\deg\gamma_\ell[h] \leq \deg\det\mathcal{E}_{rs}[h] - \deg(\psi_{r-2}\psi_{s-2}\psi_{r-1}\psi_{s-1}).$$

In this last formula, the factor ψ_{s-r} has been omitted, because $s-r$ is either 3 or 4, and by (8.17) this has non-negative degree in any case. Thus, we simply bounded it below by 0 in the previous inequality. Before entering a more detailed analysis, we use Equation (8.8) to rewrite the first column with expressions for which we have exact formulas for the degree:

$$\mathcal{E}_{rs}[h] = \begin{pmatrix} \psi_{r-4}\psi_{s-1} & \alpha_{r-3}\alpha_s[1] & \psi_{r-3}\psi_s & \gamma_{r-3}\gamma_s[h] \\ \psi_{r-3}\psi_{s-2} & \alpha_{r-2}\alpha_{s-1}[1] & \psi_{r-2}\psi_{s-1} & \gamma_{r-2}\gamma_{s-1}[h] \\ \psi_{r-2}\psi_{s-3} & \alpha_{r-1}\alpha_{s-2}[1] & \psi_{r-1}\psi_{s-2} & \gamma_{r-1}\gamma_{s-2}[h] \\ \psi_{r-1}\psi_{s-4} & \alpha_r\alpha_{s-3}[1] & \psi_r\psi_{s-3} & \gamma_r\gamma_{s-3}[h] \end{pmatrix}.$$

The determinant of $\mathcal{E}_{rs}[h]$ is the sum of products of 4 ψ factors and 4 α or γ factors. The degrees of the former are explicitly known, while by hypothesis we have upper bounds on the latter, since all the indices are at most $(\ell+9)/2$. We can then deduce an upper bound on the degree of this determinant. All the ψ_i have indices with i in the range $[r-4, s]$ (remember that $r \leq s$), and since their degrees increases with the indices, we can upper bound the degree of the products of the four ψ factors by $4 \deg \psi_s$. Therefore we have

$$\deg \det \mathcal{E}_{rs}[h] \leq 4(\deg \psi_s + C).$$

In order to deduce an upper bound on $\operatorname{maxdeg} \gamma_\ell$, it remains to get a lower bound on the degree of the $\deg(\psi_{r-2}\psi_{s-2}\psi_{r-1}\psi_{s-1})$ term, and again by monotonicity of the degree in the index, we lower bound it by $4 \deg \psi_{r-2}$. So finally, we get

$$\operatorname{maxdeg} \gamma_\ell \leq 4C + (\deg \psi_s^4 - \deg \psi_{r-2}^4).$$

Using (8.16) and (8.17), we deduce that for all k, we have $\deg(\psi_k^2) = 3(k^2-9)$ and substituting this value and the expression of $r-2$ and s in term of ℓ, we obtain

$$\deg \psi_s^4 - \deg \psi_{r-2}^4 = \begin{cases} 30\ell + 90 & \text{if } \ell \text{ is even,} \\ 36\ell + 108 & \text{if } \ell \text{ is odd,} \end{cases}$$

and the result follows for $\operatorname{maxdeg} \gamma_\ell$.

The proof for $\operatorname{maxdeg} \alpha_\ell$ follows the same line. Using the matrix $\mathcal{F}_{rs}[h]$ defined in (8.32) in a similar way as we used the matrix $\mathcal{E}_{rs}[h]$ and with the help of the formula (8.33), we end up with the following bounds

$$\operatorname{maxdeg} \alpha_\ell \leq \begin{cases} 4C + 30\ell - 30 & \text{if } \ell \text{ is even,} \\ 4C + 36\ell - 36 & \text{if } \ell \text{ is odd,} \end{cases}$$

which are stricter than our target.

Finally, the bound $\ell \geq 12$ is necessary to ensure that the quantities r and s are at least 5, as required in [7] to apply the formulas (8.31) and (8.33). □

We can now finish the proof of Lemma 8. We define two sequences $(\ell_i)_{i\geq 0}$ and $(C_i)_{i\geq 0}$ as follows: let $\ell_0 = 12$ and let C_0 be a bound on the degrees of the coefficients of all the α_i and γ_i for $i \leq \ell_0$. Then for all $i \geq 1$, we define the sequences inductively by

$$\begin{cases} \ell_{i+1} = 2\ell_i - 9 \\ C_{i+1} = 4C_i + 36\ell_{i+1} + 108. \end{cases}$$

By Lemma 9, for all i and all $\ell \leq \ell_i$, the degrees $\operatorname{maxdeg} \alpha_\ell$ and $\operatorname{maxdeg} \gamma_\ell$ are bounded by C_i. The expression $\ell_i = (\ell_0 - 9)2^i + 9 = 3 \cdot 2^i + 9$ can be derived directly from the definition and substituted in the recurrence formula of C_{i+1} to get $C_{i+1} = 4C_i + 216 \cdot 2^i + 432$. This recurrence can be solved by setting $\Gamma_i = C_i + 108 \cdot 2^i + 144$, so that $\Gamma_{i+1} = 4\,\Gamma_i$, and we obtain $C_i = (C_0 + 252)\,4^i - 108 \cdot 2^i - 144$. Finally, for any ℓ, we select the smallest i such that $\ell \leq \ell_i$. This value of i is $\lceil \log_2((\ell-9)/3) \rceil$. The corresponding bound for $\operatorname{maxdeg} \alpha_\ell$ and $\operatorname{maxdeg} \gamma_\ell$ is then C_i, which grows like $O(\ell^2)$ (and we remark that the effect of the ceiling can make the constant hidden in the $O()$ expression grow by a factor at most 3).

Using the expression (8.10), we have $\operatorname{maxdeg} \delta_\ell \leq \operatorname{maxdeg} \alpha_\ell + \operatorname{maxdeg} \gamma_\ell$, and therefore the bound $O(\ell^2)$ also applies to the degrees of the coefficients of δ_ℓ. And using the formula (8.13), the same holds as well for the coefficients of ϵ_ℓ / y.

This concludes the proof of Lemma 8.

7. Experimental results

In order to evaluate the practicality of our algorithm, we have tested it on one of the families of genus-3 hyperelliptic curves having explicit RM given in [28, Theorem 1]. Formulas for their RM endomorphisms are described in [21]: for $t \neq \pm 2$, the curve $\mathcal{C}_t$ with equation

$$y^2 = x^7 - 7x^5 + 14x^3 - 7x + t,$$

admits an endomorphism given in Mumford representation by

$$\eta_7(x, y) = \langle X^2 + 11\, xX/2 + x^2 - 16/9, y\rangle.$$

The fact that this expression has degree 2 while one would generically expect a degree 3 is no accident: it comes from the construction in [28] of the endomorphism as a sum of two automorphisms on a double cover of the curve. We have $\eta_7^3 + \eta_7^2 - 2\eta_7 - 1 = 0$, so that the ring $\mathbb{Z}[\eta_7]$ is isomorphic to the ring of integers $\mathbb{Z}[2\cos(2\pi/7)]$ of the real subfield of the cyclotomic field $\mathbb{Q}(e^{2i\pi/7})$. All the numerical data in this section have been obtained for the parameter $t = 42$, on the prime field $\mathbb{F}_p$ with $p = 2^{64} - 59$.

In our practical computations, the main differences with the theoretical description are the following: we use Gröbner basis algorithms instead of resultants, we consider also small non-split primes ℓ and small powers, and we finish the computation with a parallel collision search. The source code for our experiments is available at `https://members.loria.fr/SAbelard/RMg3.tgz`.

7.1. Computing modular information with Gröbner basis.

Although the polynomial system resolution using resultants has a complexity in $\widetilde{O}(\ell^4)$, the real cost for small values of ℓ is already pretty large. In the resolution method described in Section 3.2, each bivariate resultant is computed by evaluation / interpolation and hence requires the computation of many univariate resultants. We illustrate this by counting the number of univariate resultants to perform and their degrees for the main step of the resolution (the part that reaches the peak complexity). We also measure the cost of such resultant computations using the NTL 10.5.0 and FLINT 2.5.2 libraries, both linked against GMP 6, when the base field is $\mathbb{F}_{2^{64}-59}$. These costs do not include the evaluation / interpolation steps which might also be problematic for large instances, because they are hard to parallelize.

ℓ	#res	Deg	Cost (NTL)	Cost (FLINT)
13	525M	16,000	1,850 days	735 days
29	12.8G	80,000	310,000 days	190,000 days

We were more successful with the direct approach using Gröbner basis that we now describe. For computing the kernel of a given endomorphism, we computed a Gröbner basis of the system (3) with some small modifications. First, we observe that the only occurrences of y_1 and y_2 are within the monomial y_1y_2. Consequently, we can remove one variable by replacing each occurrence of y_1y_2 by a fresh variable y. Next, we need to make the system 0-dimensional by encoding the fact that $d_3(x_3)$ and $\widetilde{d_3}(x_1, x_2)$ are nonzero. This is done by introducing another fresh variable t and by adding the polynomial $S(x_1, x_2, x_3)t - 1$ to the system, where $S(x_1, x_2, x_3)$ is the squarefree part of $d_3(x_3)\widetilde{d_3}(x_1, x_2)$. Finally, since each polynomial is symmetric with respect to the transposition of the variables x_1 and x_2, we can rewrite the equations using the symmetric polynomials $s_1 = x_1 + x_2$ and $s_2 = x_1\, x_2$. This

divides by two the degree in x_1 and x_2 of the equations. We end-up with a system in 5 variables.

The whole construction can be slightly modified to compute the pre-image of a given divisor by the endomorphism: to model $\alpha(D) = Q$, we write $D = P_1 + P_2 + P_3 - 3\infty$ and solve for $\alpha(P_1 - \infty) + \alpha(P_2 - \infty) = Q - \alpha(P_3 - \infty)$. In that case, the variable y_3 gets involved in all the equations, so that we get a system in 6 variables.

For $\ell = 2$, the 2-torsion elements are easily deduced from the factorization of f, and by computing a pre-image of a 2-torsion divisor, we got a point in $J[4]$ from which we could deduce $a, b, c \bmod 4$. Dividing again by 2 was too costly, due to the fact that the 4-torsion point was in an extension of degree 4. For $\ell = 3$, which is an inert prime, we ran the kernel computation for the multiplication-by-3 endomorphism, without using the RM property. The norm being 27, this is the largest modular computation that we performed (and the most costly in terms of time and memory). The prime $\ell = 7$ ramifies in $\mathbb{Z}[\eta_7]$ as the cube of the ideal generated by $\alpha_7 = -2 - \eta_7 + \eta_7^2$. The kernel of α_7 can be computed but it yields only one linear relation in $a, b, c \bmod 7$. Dividing the kernel elements by α_7 would give more information, but again, this computation did not finish due to the field extension in which the divisors are defined. The first split prime is $\ell = 13$. We use the following small generators: $(13) = (2-\eta_7-2\eta_7^2)(-2+2\eta_7+\eta_7^2)(3+\eta_7-\eta_7^2)$, which seem to produce the polynomial systems with the smallest degrees. For instance, the apparently smaller element $1 + \eta_7^2$ of norm 13 yields equations of much higher degrees $7, 71, 72, 73, 72$. The next split prime is 29, which would maybe have been feasible, but was not necessary for our setting. In the following table, we summarize the data for these systems, that were obtained with Magma V2.23-4 on a Xeon E7-4850v3 at 2.20GHz, with 1.5 TB RAM.[1]

mod ℓ^k	#var	degree of each eq.	time	memory	$a, b, c \bmod \ell^k$
2	—	—	—	—	$0, 0, 0$
4 (inert^2)	6	$7, 7, 14, 15, 15, 10$	1 min	negl.	$2, 2, 2$
3 (inert)	5	$7, 53, 54, 55, 26$	14 days	140 GB	$1, 2, 1$
$7 = \mathfrak{p}_1^3$	5	$7, 35, 36, 37, 36$	3.5h	6.6 GB	$a + 2b + 4c \equiv 2$
$13 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	5	$7, 44, 45, 46, 52$	3×3 days	41 GB	$12, 10, 9$
$29 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	5	$7, 92, 93, 94, 100$	$>3\times2$ weeks	>0.8 TB	—

7.2. **Parallel collision search for RM curves.** The classical square-root-complexity search in genus 3 requires $O(q)$ group operations [9]. For RM curves, this can be improved by searching for the coefficients a, b, c of $\psi = \pi + \pi^\vee$ in $\mathbb{Z}[\eta]$. This readily yields a complexity in $O(q^{3/4})$, using the equation $aD + b\eta(D) + c\eta^2(D) = (q+1)D$, that must be satisfied for any rational divisor D. While a baby-step giant-step approach is immediate to design, it needs $O(q^{3/4})$ space and this is the bottleneck. A low-memory, parallel version of this search can be obtained with the algorithm of [13], where the details are given only for a 2-dimensional problem, while here this is a 3-dimensional problem. But we did not hit any surprise when adapting the parameters to our case. Also, just like in [13], including some anterior

[1]The F4 algorithm can be highly sensitive to the modelling of the problem and we refer to the source code. In particular, thanks to serendipity, we saved a factor greater than 12 in the runtime for $\ell = 7, 13$ by forgetting to take the squarefree part of the saturation polynomial. We have no explanation for this phenomenon.

modular knowledge is straightforward: if a, b, c are known modulo m, the expected time is in $O(q^{3/4}/m^{3/2})$.

We wrote a dedicated C implementation with a few lines of assembly to speed-up the additions and multiplications in $\mathbb{F}_p$, taking advantage of the special form of p. This implementation performs $10.7M$ operations in the Jacobian per second using 32 (hyperthreaded) threads of a 16-core bi-Xeon E5-2650 at 2 GHz. We used the knowledge of ψ modulo 156 but not of the known relation modulo 7 for simplicity (there is no obstruction to using it and saving an additional $7^{1/2}$ factor).

After computing about 190,000 chains of average length 32,000,000, we got a collision, from which we deduced

$$\psi = 2551309006 + 2431319810\ \eta_7 - 847267802\ \eta_7^2,$$

and the coefficients of the characteristic polynomial χ_π of the Frobenius are then

$$\sigma_1 = 986268198, \quad \sigma_2 = 35389772484832465583, \quad \sigma_3 = 109560528621042368187702122 44.$$

The number of group operations that were done is slightly less than 43 $(p^{3/4}/156^{3/2})$. This factor 43 is close to the average that we observed in our numerous experiments with smaller sizes. Scaled on a single (physical) core, we can estimate the cost of this collision search to be 105 core-days.

References

[1] Simon Abelard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. Improved complexity bounds for counting points on hyperelliptic curves, 2017. To appear in *Foundations of Computational Mathematics*, ArXiv preprint 1710.03448.

[2] Leonard M. Adleman and Ming-Deh Huang. Counting points on curves and Abelian varieties over finite fields. *Journal of Symbolic Computation*, 32(3):171–189, 2001.

[3] Sean Ballentine, Aurore Guillevic, Elisa Lorenzo García, Chloe Martindale, Maike Massierer, Benjamin Smith, and Jaap Top. Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. In *Algebraic Geometry for Coding Theory and Cryptography*, pages 63–94. Springer Verlag, 2017.

[4] Christina Birkenhake and Herbert Lange. *Complex Abelian varieties*, volume 302. Springer Science & Business Media, 2013.

[5] Alin Bostan, Grégoire Lecerf, Bruno Salvy, Éric Schost, and Bernd Wiebelt. Complexity issues in bivariate polynomial factorization. In *Proceedings of ISSAC 2004*, pages 42–49. ACM, 2004.

[6] Ivan Boyer. *Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication réelle ou complexe*. PhD thesis, Paris 7, 2014.

[7] David G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Journal fur die reine und angewandte Mathematik*, 447:91–146, 1994.

[8] Robert Carls and David Lubicz. A p-adic quasi-quadratic time point counting algorithm. *International Mathematics Research Notices*, 2009(4):698–735, 2009.

[9] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory*, pages 21–76. AMS/International Press, 1998. Proceedings of a Conference in Honor of A.O.L. Atkin.

[10] Jordan S. Ellenberg. Endomorphism algebras of Jacobians. *Advances in Mathematics*, 162:243–271, 2001.

[11] Gerhard Frey and Michael Müller. Arithmetic of modular curves and applications. In B. Heinrich Matzat, Gert-Martin Greuel, and Gerhard Hiss, editors, *Algorithmic Algebra and Number Theory*, pages 11–48. Springer Verlag, 1999.

[12] Pierrick Gaudry, David Kohel, and Benjamin Smith. Counting points on genus 2 curves with real multiplication. In *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 504–519. Springer Verlag, 2011.

[13] Pierrick Gaudry and Éric Schost. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm. In *ANTS-VI*, volume 3076 of *LNCS*, pages 208–222. Springer Verlag, 2004.

[14] Pierrick Gaudry and Éric Schost. Genus 2 point counting over prime fields. *Journal of Symbolic Computation*, 47(4):368–400, 2012.
[15] Michael C. Harrison. An extension of Kedlaya's algorithm for hyperelliptic curves. *Journal of Symbolic Computation*, 47(1):89–101, 2012.
[16] David Harvey. Counting points on hyperelliptic curves in average polynomial time. *Annals of Mathematics*, 179(2):783–803, 2014.
[17] David Harvey and Andrew V. Sutherland. Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II. In *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, volume 663 of *Contemporary Mathematics*, pages 127–148. AMS, 2016.
[18] Ming-Deh Huang and Doug Ierardi. Counting points on curves over finite fields. *Journal of Symbolic Computation*, 25(1):1–21, 1998.
[19] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan mathematical society*, 16(4):323–338, 2001.
[20] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *ANTS-VIII*, volume 5011 of *LNCS*, pages 312–326. Springer Verlag, 2008.
[21] David R. Kohel and Benjamin A. Smith. Efficiently computable endomorphisms for hyperelliptic curves. In *ANTS VII*, volume 4076 of *LNCS*, pages 495–509. Springer Verlag, 2006.
[22] Jean-François Mestre. Familles de courbes hyperelliptiques à multiplications réelles. In *Arithmetic algebraic geometry*, pages 193–208. Springer, 1991.
[23] Jonathan Pila. Frobenius maps of Abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.
[24] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *Journal of the Ramanujan mathematical society*, 15(4):247–270, 2000.
[25] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985.
[26] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Iwanami Shoten and Princeton University Press, 1971.
[27] Andrew Sutherland. Gallery of Jacobians. https://math.mit.edu/~drew/ZetaFunctions.html.
[28] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math*, 43(5):1055–1064, 1991.
[29] Paul van Wamelen. Proving that a genus 2 curve has complex multiplication. *Mathematics of Computation*, 68(228):1663–1677, 1999.
[30] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013. Third edition.
[31] Richard Zippel. *Effective polynomial computation*. Springer Verlag, 1993.

Université de Lorraine, CNRS, Inria
Email address: simon.abelard@loria.fr

Email address: pierrick.gaudry@loria.fr

Email address: pierre-jean.spaenlehauer@loria.fr

FAST JACOBIAN ARITHMETIC FOR HYPERELLIPTIC CURVES OF GENUS 3

ANDREW V. SUTHERLAND

ABSTRACT. We consider the problem of efficient computation in the Jacobian of a hyperelliptic curve of genus 3 defined over a field whose characteristic is not 2. For curves with a rational Weierstrass point, fast explicit formulas are well known and widely available. Here we address the general case, in which we do not assume the existence of a rational Weierstrass point, using a balanced divisor approach.

1. INTRODUCTION

Like elliptic curves, Jacobians of hyperelliptic curves over finite fields are an important source of finite abelian groups in which the group operation can be made fully explicit and efficiently computed. This has given rise to many cryptographic applications, including Diffie-Hellman key exchange and pairing-based cryptography, and has also made it feasible to experimentally investigate various number-theoretic questions related to the L-series of abelian varieties over number fields, including analogs of the Birch and Swinnerton-Dyer conjecture, the Koblitz-Zywina conjecture, the Lang-Trotter conjecture, and the Sato-Tate conjecture, each of which was originally formulated for elliptic curves but has a natural generalization to abelian varieties of higher dimension. They can also be used to study analogs of the Cohen-Lenstra heuristics [5] and related questions in arithmetic statistics that were originally formulated for quadratic number fields but have a natural analog for quadratic function fields [1, 9].

Thanks to work by many authors, there are several algorithms available for Jacobian arithmetic in genus 2 that have been heavily optimized (primarily with a view toward cryptographic applications). For hyperelliptic curves of genus $g > 2$, fully general algorithms have been developed only in the last decade, and fast explicit formulas are typically available only for curves that have a rational Weierstrass point. This simplifying assumption makes it easier to encode elements of the Jacobian using unique representatives of their divisor class as described by Mumford [27] and later exploited by Cantor [3], who gave the first fully explicit algorithm for computing in the Jacobian of a hyperelliptic curve with a rational Weierstrass point.

But most hyperelliptic curves do not have a rational Weierstrass point. Over finite fields the proportion of such curves is roughly $1/(2g)$, and over a number field the proportion is zero (as an asymptotic limit taken over curves of increasing height). In particular, many arithmetically interesting examples of hyperelliptic curves do not have

The author was supported by NSF grants DMS-1115455 and DMS-1522526, and Simons Foundation grant 550033.

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

any rational Weierstrass points. This includes, for example, all 19 of the modular curves $X_0(N)$ that are hyperelliptic.[1]

In this article we treat hyperelliptic curves of genus $g = 3$ over fields whose characteristic is not 2. Our formulas are based on the *balanced divisor* approach introduced by David J. Mireles Morales in his thesis [26] and presented by Galbraith, Harrison, and Mireles Morales in [10]. The basic idea is to represent divisors of degree zero as the difference of an effective divisor of degree g and an effective divisor D_∞ whose support is "balanced" over two points at infinity (see §3 for further details). This is one of two approaches to generalizing Cantor's algorithm; the other is to work in what is known as the *infrastructure* of a "real" hyperelliptic curve [22, 36]. These two approaches were analyzed in [21] (using formulas in [7, 10]), which concluded that in genus 2, and even genus in general, the balanced divisor approach is more efficient [21, §8]. When the genus is odd, however, the divisor D_∞ cannot be perfectly balanced; genus 3 thus presents an interesting test case for the balanced divisor approach.

Another reason to be particular interested in the genus 3 case, and the main motivation for this work, is that group computations in the Jacobian play a small but crucial role in efficiently computing the L-series of a genus 3 curve. Recall that for a curve $C/\mathbf{Q}$ we may define its L-series as an Euler product

$$L(C,s) := \prod_p L_p(p^{-s})^{-1},$$

where $L_p \in \mathbf{Z}[T]$ is an integer polynomial of degree at most $2g$; for primes p of good reduction (all but finitely many), the degree is exactly $2g$ and $L_p(T)$ is the numerator of the zeta function

$$Z_{C_p}(T) := \exp\left(\sum_{r=1}^{\infty} \#C_p(\mathbf{F}_{p^r})\frac{T^r}{r}\right) = \frac{L_p(T)}{(1-T)(1-pT)},$$

where C_p denotes the reduction of C modulo p. Using the average polynomial-time algorithm described in [16, 18, 19], for hyperelliptic curves of genus g one can simultaneously compute $L_p(T) \bmod p$ at all primes $p \le N$ of good reduction in time $\tilde{O}(g^3 N \log^3 N)$. In principle one can use a generalization of the algorithm in [16] to compute $L_p(T)$ modulo higher powers of p sufficient to determine $L_p \in \mathbf{Z}[T]$ (in genus 3, computing $L_p(T) \bmod p^2$ suffices for $p > 144$), but this requires a more intricate implementation and is much more computationally intensive than computing $L_p(T) \bmod p$.

Alternatively, as described in [6, 20], for curves of genus 3 one can use $\tilde{O}(p^{1/4})$ group operations in the Jacobian of C_p and its quadratic twist to uniquely determine $L_p \in \mathbf{Z}[T]$. Within the practical range of computation (where $N \le 2^{32}$, say), the cost of doing this is negligible compared to the cost of computing $L_p(T) \bmod p$, *provided that the group operations can be performed efficiently*. This is the goal of the present work.

The algorithms we describe here played a key role in [17], which generalizes the algorithm of [19] to treat genus 3 curves that are hyperelliptic over $\overline{\mathbf{Q}}$, but not necessarily

[1] This follows from results of Ogg [31, 32], who both determined the N for which $X_0(N)$ is hyperelliptic and gave a criterion for rational Weierstrass points on $X_0(N)$ that allows one to rule out the existence of any such points on the hyperelliptic $X_0(N)$.

over **Q** (they may be degree-2 covers of pointless conics). The output of this algorithm is $L_p(T)L_p(-T) \bmod p$, and, as explained in [19, §7], one can again use $\tilde{O}(p^{1/4})$ group operations in the Jacobian to uniquely determine $L_p \in \mathbf{Z}[T]$ given this information. As can be seen in Table 1 of [17], which shows timings obtained using a preliminary version of the formulas presented in this article, the time spent on group operations is negligible compared to the time spent computing L-polynomials modulo p (less than one tenth). This was not true of initial attempts that relied on a generic implementation of the balanced divisor approach included in Magma [2], which has not been optimized for hyperelliptic curves of genus 3. For the application in [17], the primary use of our addition formulas occurs as part of a baby-steps giant-steps search in which field inversions can easily be combined by taking steps in parallel [20, §4.1]. The incremental cost of a field inversion is then just three field multiplications, making affine coordinates preferable to projective coordinates (by a wide margin); we thus present our formulas in affine coordinates, although they can be readily converted to projective coordinates if desired.

The explicit formulas we obtain are nearly as fast as the best known formulas for genus 3 hyperelliptic curves that have a rational Weierstrass point [4, 8, 14, 13, 23, 29, 30, 39], which have been extensively optimized.[2] Our formulas for addition/doubling have a cost of **I+79M**/**I+82M**, versus **I+67M**/**I+68M** for the fastest known formulas for genus 3 hyperelliptic curves with a rational Weierstrass point [29, 30], where **I** denotes a field inversion and **M** denotes a field multiplication. This performance gap is comparable to that seen in genus 2, where the fastest addition formulas for curves without a rational Weierstrass point cost **I+28M**/**I+32M** [10], versus **I+24M**/**I+27M** [24] for genus 2 curves with a rational Weierstrass point.

Contemporaneous with our work, Rezai Rad [**?**] has independently obtained formulas for genus 3 hyperelliptic curves without a rational Weierstrass point using a modified infrastructure approach that exploits a map from the infrastructure to the Jacobian whose image consists of balanced divisors, obtaining a cost of **I+75M**/**I+86M** (for affine coordinates in odd characteristic). This raises the interesting question of whether it is possible to integrate the faster addition formula in [**?**] with the faster doubling formula presented here.

2. Background

We begin by recalling some basic facts about hyperelliptic curves and their Jacobians.

2.1. **Hyperelliptic curves.** A (smooth, projective, geometrically integral) curve C over a field k is said to be *hyperelliptic* if its genus g is at least 2 and it admits a 2-1 morphism $\phi : C \to \mathbf{P}^1$ (the *hyperelliptic map*). The map ϕ determines an automorphism $P \to \overline{P}$ of C, the *hyperelliptic involution*, which fixes the fibers of ϕ and acts trivially only at ramification points. The fixed points of the hyperelliptic involution are precisely the *Weierstrass points* of C (the points P for which there exists a non-constant function on C

[2] Indeed, our addition formula uses exactly the same number of field inversions and multiplications as the formula in [4, Alg. 14.52] for genus 3 curves with a rational Weierstrass point in odd characteristic (but as noted above, this formula has since been improved).

with a pole of order less than $g+1$ at P and no other poles). The Riemann-Hurwitz formula implies that a hyperelliptic curve of genus g has exactly $2g+2$ Weierstrass points. Some authors require the hyperelliptic map ϕ to be defined over k (rationally hyperelliptic), while others only require it to be defined over $\overline{k}$ (geometrically hyperelliptic); we shall assume the former. When k is a finite field the distinction is irrelevant because $\mathbf{P}^1_k$ has no non-trivial twists (these would be genus 0 curves with no rational points, which do not occur over finite fields).

Provided $\mathrm{char}(k) \neq 2$, which we henceforth assume, every hyperelliptic curve C/k has an affine model of the form

$$y^2 = f(x),$$

with $f \in k[x]$ separable of degree $2g+1$ or $2g+2$. The hyperelliptic map ϕ sends each affine point (x,y) on C to $(x:1)$ on $\mathbf{P}^1$, and the hyperelliptic involution swaps (x,y) and $(x,-y)$. The projective closure of the model $y^2 = f(x)$ has a singularity on the line $z=0$ (points on this line are said to lie *at infinity*); the curve C is obtained by desingularization. Equivalently, C is the smooth projective curve with function field $k(C) := k[x,y]/(y^2 - f(x))$; the field $k(C)$ is a quadratic extension of the rational function field $k(x) \simeq k(\mathbf{P}^1)$, and the inclusion map $\phi^*\colon k(\mathbf{P}^1) \hookrightarrow k(C)$ corresponds to the hyperelliptic map ϕ.

When $\deg f = 2g+1$, the model $y^2 = f(x)$ has a unique rational point at infinity that is also a Weierstrass point. Conversely, if C has a rational Weierstrass point, we can obtain a model of the form $y^2 = f(x)$ with $\deg f = 2g+1$ by moving this point to infinity. We can then make f monic via the substitutions $x \mapsto \mathrm{lc}(f)x$ and $y \mapsto \mathrm{lc}(f)^g y$, after dividing both sides of $y^2 = f(x)$ by $\mathrm{lc}(f)^{2g}$.

If C does not have a rational Weierstrass point then we necessarily have $\deg f = 2g+2$, and there are either 0 or 2 rational points at infinity, depending on whether the leading coefficient of f is a square in $k^\times$ or not. Provided that C has some rational point P, moving this point to infinity ensures that there are two rational points at infinity (the other is $\overline{P} \neq P$). This makes the leading coefficient of f a square, and we can then make f monic by replacing y with $\sqrt{\mathrm{lc}(f)}y$ and dividing through by $\mathrm{lc}(f)$.

In summary, if C is a hyperelliptic curve with a rational point then it has a model of the form $y^2 = f(x)$ with f monic of degree $2g+1$ or $2g+2$. The former is possible if and only if C has a rational Weierstrass point and the later can always be achieved provided that C has a rational point that is not a Weierstrass point. If k is a finite field of cardinality q, the Weil bound $\#C(k) \geq q+1-2g\sqrt{q}$ guarantees that C has a rational point whenever $q > 4g^2$, and it is guaranteed to have a rational point that is not a Weierstrass point when $q > 4g^2+2g+2$. For $g=3$ this means that if k is a finite field of odd characteristic and cardinality at least 47, then C has a model of the form $y^2 = f(x)$ with f monic of degree 8; in what follows, we shall assume that the hyperelliptic curves C we work with have such a model.

Remark 2.1. In the literature, hyperelliptic curves with a model $y^2 = f(x)$ that has two rational points at infinity are sometimes called "real" hyperelliptic curves (those with one rational point at infinity are called "imaginary"). We avoid this abuse of terminology as it refers to the model and is not an intrinsic property of the curve. As noted

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

above, in the setting of interest to us every hyperelliptic curve can be viewed as a "real" hyperelliptic curve.

2.2. **Divisor class groups of hyperelliptic curves.** The *Jacobian* of a curve C/k of genus g is an abelian variety $\mathrm{Jac}(C)$ of dimension g that is canonically determined by C; see [25] for a formal construction. Describing $\mathrm{Jac}(C)$ as an algebraic variety is difficult, in general, but we are only interested in its properties as an abelian group. Provided that C has a k-rational point, then by [25, Thm. 1.1], we may functorially identify the group $\mathrm{Jac}(C)$ with the *divisor class group* $\mathrm{Pic}^0(C)$, the quotient of the group $\mathrm{Div}^0(C)$ of divisors of degree 0 by its subgroup of principal divisors. We recall that a *divisor* on C can be defined as a formal sum $D = \sum n_P P$ over points $P \in C(\overline{k})$ with only finitely n_P nonzero; the *degree* of D is $\deg(D) := \sum n_P$. A divisor is said to be *principal* if it is of the form $\mathrm{div}(\alpha) := \sum_P \mathrm{ord}_P(\alpha)P$ for some function $\alpha \in k(C)$; such divisors necessarily have degree 0.

We are interested in the k-rational points of $\mathrm{Jac}(C)$. Under our assumption that C has a k-rational point, these correspond to divisor classes $[D]$ of k-rational divisors $D \in \mathrm{Div}^0(C)$ (this means $D = \sum n_P P$ is fixed by $\mathrm{Gal}(\overline{k}/k)$, even though the points P in its support need not be). In order to describe the divisor classes $[D]$ explicitly, we now assume that C is a hyperelliptic curve that has a rational point, and fix a hyperelliptic map $\phi : C \to \mathbf{P}^1$. We say that a point P on C is *affine* if it lies above an affine point $(x : 1)$ on $\mathbf{P}^1$ and we call P a point *at infinity* if lies above the point $(1 : 0)$ on $\mathbf{P}^1$.

Recall that a divisor $D = \sum n_P P$ is *effective* if $n_P \geq 0$ for all P; an effective divisor can always be written as $\sum_i P_i$, where the P_i need not be distinct.

Definition 2.2. An effective divisor $D = \sum P_i$ on a hyperelliptic curve C is *semi-reduced* if $P_i \neq \overline{P}_j$ for any $i \neq j$; a semi-reduced divisor whose degree does not exceed the genus of C is said to be *reduced*.

Lemma 2.3. *Let C/k be a hyperelliptic curve that has a rational point. Every rational divisor class $[D]$ in $\mathrm{Pic}^0(C)$ can be represented by a divisor whose affine part is semi-reduced.*

Proof. By adding a suitable principal divisor to D if necessary, we can assume the affine part D_0 of D is effective. If D_0 is not semi-reduced it can be written as $D_1 + \overline{D}_1 + D_2$ with D_2 rational and semi-reduced; if we now take a principal divisor E on $\mathbf{P}^1$ with affine part $\phi_* D_1$ and subtract $\phi^* E$ from D we obtain a linearly equivalent rational divisor with affine part D_2 (here $\phi : C \to \mathbf{P}^1$ is the hyperelliptic map). □

Let us now fix a model $y^2 = f(x)$ for our hyperelliptic curve C that has a rational point at infinity. A semi-reduced affine divisor $D = \sum P_i$ can be compactly described by its *Mumford representation* $\mathrm{div}[u, v]$: let $P_i = (x_i, y_i)$, define $u(x) := \prod_i (x - x_i)$, and let v be the unique polynomial of degree less than $\deg u$ for which $f - v^2$ is divisible by u. As explained in [27, §1], this amounts to requiring that $v(x_i) = y_i$ with multiplicity equal to the multiplicity of P_i in D; when the x_i are distinct v can be computed via Lagrange interpolation in the usual way. If D is a rational divisor, then $u, v \in k[x]$.

Conversely, suppose we are given $u, v \in k[x]$ with u monic, $\deg v < \deg u$, and $f - v^2$ is divisible by u. Write $u(x) = \prod_i (x - x_i)$, define $P_i := (x_i, v(x_i))$; the affine points P_i lie

in $C(\bar{k})$ because $u|(f-v^2)$ implies $f(x_i)-v(x_i)^2$ is divisible by $u(x_i)=0$, and therefore $v(x_i)^2=f(x_i)$. We now define

$$\operatorname{div}[u,v] := \sum_i P_i.$$

The effective divisor $\operatorname{div}[u,v]$ is rational, since $u,v \in k[x]$, and it is semi-reduced: if $P_i = \overline{P}_j$ then we must have $x_i = x_j$ and $v(x_i) = -v(x_j) = -v(x_i) = 0$; if $i \neq j$ then x_i is a double root of u and of v, and therefore also a double root of f, but this is impossible since f is separable. There is thus a one-to-one correspondence between semi-reduced affine divisors and Mumford representations $\operatorname{div}[u,v]$, and $\operatorname{div}[u,v]$ is rational if and only if $u,v \in k[x]$.

Let us now fix an effective divisor D_∞ of degree g supported on rational points at infinity; if C has one rational point P_∞ at infinity we may take $D_\infty = gP_\infty$, and if C has two rational points P_∞ and $\overline{P}_\infty$ at infinity we may take $D_\infty = \lceil g/2 \rceil P_\infty + \lfloor g/2 \rfloor \overline{P}_\infty$.

Proposition 2.4. *Let C be a hyperelliptic curve of genus g and let D_∞ be an effective divisor of degree g supported on rational points at infinity. Each rational divisor class in $\operatorname{Pic}^0(C)$ can be uniquely written as $[D_0 - D_\infty]$, where D_0 is an effective rational divisor of degree g whose affine part is reduced.*

Proof. See Proposition 1 in [10], which follows from Propositions 3.1 and 4.1 of [33] (provided the support of D_∞ is rational, which we have assumed). □

Remark 2.5. When g is even it is not actually necessary for the points at infinity to be rational; the divisor $D_\infty = (g/2)(P_\infty + \overline{P}_\infty)$ will be rational in any case. Indeed, as astutely observed in [10], when C has even genus and no rational Weierstrass points, it is computationally advantageous to work with a model for C that does not have rational points at infinity. But this will not work when the genus is odd because we do need D_∞ to be rational (Proposition 2.4 is false otherwise).

3. Hyperelliptic divisor class arithmetic using balanced divisors

In this section we summarize the general formulas for Jacobian arithmetic using balanced divisors. Our presentation is based on [10], but we are able to make some simplifications by being more specific about our choice of D_∞ and unraveling a few definitions (we also introduce some new notation). We refer the reader to [10, 26] for details and proofs of correctness. In the next section we specialize these formulas to the case $g = 3$ and optimize for this case.

Let us first fix a model $y^2 = f(x)$ for a hyperelliptic curve C/k of genus g with rational points $P_\infty := (1:1:0)$ and $\overline{P}_\infty := (1:-1:0)$ at infinity (in weighted projective coordinates), and let us define $D_\infty := \lceil g/2 \rceil P_\infty + \lfloor g/2 \rfloor \overline{P}_\infty$. This implies that f is monic of degree $2g+2$; as noted above, this can be assumed without loss of generality if C has any rational points that are not Weierstrass points. The case where C has a rational Weierstrass point is better handled by existing algorithms in any case, so the only real constraint we must impose is that C have a rational point.[3] The assumption

[3] The assumption that C has a rational point is required by any algorithm that represents rational elements of $\operatorname{Pic}^0(C)$ using rational divisors (even though this is not always explicitly stated in the literature). As

that $\mathrm{char}(k) \neq 2$ is made purely for the sake of convenience, the algorithms in [10, 26] work in any characteristic.

Proposition 2.4 implies that we can uniquely represent each rational divisor class in $\mathrm{Pic}^0(C)$ by a triple (u, v, n), where $\mathrm{div}[u, v]$ is a rational reduced affine divisor in Mumford notation (so $u, v \in k[x]$ satisfy $\deg v < \deg u$, with u a monic divisor of $f - v^2$) with $\deg u \leq g$, and n is an integer with $0 \leq n \leq g - \deg u$). The triple (u, v, n) corresponds to the divisor

$$\mathrm{div}[u, v, n] := \mathrm{div}[u, v] + nP_\infty + (g - \deg u - n)\overline{P}_\infty - D_\infty.$$

Whenever we write $\mathrm{div}[u, v, n]$ we assume that u, v, n are as above. In this notation

$$\mathrm{div}[1, 0, \lceil g/2 \rceil] = \mathrm{div}[1, 0] + \lceil g/2 \rceil P_\infty + (g - 0 - \lceil g/2 \rceil)\overline{P}_\infty - D_\infty = 0,$$

is the unique representative of the trivial divisor class in $\mathrm{Pic}^0(C)$.

At intermediate steps in our computations we shall need to work with divisors whose affine parts are semi-reduced but not reduced. Given a semi-reduced affine divisor $\mathrm{div}[u, v]$ with $\deg u \leq 2g$ and an integer n with $0 \leq n \leq 2g - \deg u$, we define

$$\mathrm{div}[u, v, n]^* := \mathrm{div}[u, v] + nP_\infty + (2g - \deg u - n)\overline{P}_\infty - 2D_\infty,$$

and whenever we write $\mathrm{div}[u, v, n]^*$ we assume that u, v, n are as above (in particular, $\deg u + n \leq 2g$).

We begin by precomputing the unique monic polynomial V for which $\deg(f - V^2) \leq g$. This auxiliary polynomial is determined by the top $g + 1$ coefficients of f and will be needed in what follows.

Algorithm PRECOMPUTE
Given $f(x) = x^{2g+2} + f_{2g+1}x^{2g+1} + \cdots + f_1 x + f_0$, compute the monic $V(x)$ for which $\deg(f - V^2) \leq g$.

1. Set $V_{g+1} := 1$.
2. For $i = g, g-1, \ldots, 0$ compute $c := f_{g+1+i} - \sum_{j=i+1}^{g+1} V_j V_{g+1+i-j}$ and set $V_i := c/2$.
3. Output $V(x) := x^{g+1} + V_g x^g + \cdots + V_1 x + V_0$.

We now give the basic algorithm for composition, which is essentially the same as the first step in Cantor's algorithm [3]. In all of our algorithms, when we write $a \bmod b$ with $a, b \in k[x]$ and b nonzero, we denote the unique polynomial of degree less than $\deg b$ that is congruent to a modulo b (the zero polynomial if $\deg b = 0$), and for any divisors $D_1, D_2 \in \mathrm{Div}(C)$ we write $D_1 \sim D_2$ to denote linear equivalence (meaning that $D_1 - D_2$ is principal).

Algorithm COMPOSE
Given $\mathrm{div}[u_1, v_1, n_1]$ and $\mathrm{div}[u_2, v_2, n_2]$, compute $\mathrm{div}[u_3, v_3, n_3]^*$ such that

$$\mathrm{div}[u_1, v_1, n_1] + \mathrm{div}[u_2, v_2, n_2] \sim \mathrm{div}[u_3, v_3, n_3]^*.$$

1. Use the Euclidean algorithm to compute monic $w := \gcd(u_1, u_2, v_1 + v_2) \in k[x]$ and $c_1, c_2, c_3 \in k[x]$ such that $w = c_1 u_1 + c_2 u_2 + c_3(v_1 + v_2)$.

observed in [34, p. 287], without this assumption a rational divisor class need not contain any rational divisors.

2. Let $u_3 \coloneqq u_1u_2/w^2$ and let $v_3 \coloneqq (c_1u_1v_2 + c_2u_2v_1 + c_3(v_1v_2 + f))/w \bmod u_3$.
3. Output $\operatorname{div}[u_3, v_3, n_1 + n_2 + \deg w]^*$.

To reduce the divisor $\operatorname{div}[u_3, v_3, n_3]^*$ output by COMPOSE to the unique representative of its divisor class we proceed in two steps. The first is to repeatedly apply the algorithm below to obtain a divisor whose affine part is semi-reduced with degree at most $g+1$.

Algorithm REDUCE
Given $\operatorname{div}[u_1, v_1, n_1]^*$ with $\deg u_1 > g+1$, compute $\operatorname{div}[u_2, v_2, n_2]^*$ with $\deg u_2 \le \deg u_1 - 2$ such that

$$\operatorname{div}[u_1, v_1, n_1]^* \sim \operatorname{div}[u_2, v_2, n_2]^*.$$

1. Let u_2 be $(f - v_1^2)/u_1$ made monic and let $v_2 \coloneqq -v_1 \bmod u_2$.
2. If $\deg v_1 = g+1$ and $\operatorname{lc}(v_1) = 1$ then let $\delta \coloneqq \deg u_1 - (g+1)$;
   else if $\deg v_1 = g+1$ and $\operatorname{lc}(v_1) = -1$ then let $\delta \coloneqq g + 1 - \deg u_2$;
   else let $\delta \coloneqq (\deg u_1 - \deg u_2)/2$.
3. Output $\operatorname{div}[u_2, v_2, n_1 + \delta]^*$.

REDUCE decreases the degree of the affine part of its input by at least 2, so at most $\lfloor (g-1)/2 \rfloor$ calls to REDUCE suffice to reduce the output of COMPOSE to a linearly equivalent divisor whose affine part has degree at most $g+1$. Having obtained a divisor $\operatorname{div}[u, v, n]^*$ with $\deg u \le g+1$, we need to compute the unique representative of its divisor class. Now if $\lceil g/2 \rceil \le n \le \lceil 3g/2 \rceil - \deg u$, then $\deg u \le g$ and

$$\operatorname{div}[u, v, n]^* = \operatorname{div}[u, v] + (n - \lceil g/2 \rceil)P_\infty + (\lceil 3g/2 \rceil - \deg u - n)\overline{P}_\infty + D_\infty - 2D_\infty,$$

so we can simply take $\operatorname{div}[u, v, n - \lceil g/2 \rceil]$ as our unique representative. The following algorithm "adjusts" $\operatorname{div}[u, v, n]^*$ until n is within the desired range; it can be viewed as composition with a principal divisor supported at infinity followed by reduction.

Algorithm ADJUST
Given $\operatorname{div}[u_1, v_1, n_1]^*$ with $\deg u_1 \le g+1$ compute $\operatorname{div}[u_2, v_2, n_2]$ such that

$$\operatorname{div}[u_1, v_1, n_1]^* \sim \operatorname{div}[u_2, v_2, n_2].$$

1. If $n_1 \ge \lceil g/2 \rceil$ and $n_1 \le \lceil 3g/2 \rceil - \deg u_1$ then output $\operatorname{div}[u_1, v_1, n_1 - \lceil g/2 \rceil]$ and terminate.
2. If $n_1 < \lceil g/2 \rceil$, let $\hat{v}_1 \coloneqq v_1 - V + (V \bmod u_1)$, let u_2 be $(f - \hat{v}_1^2)/u_1$ made monic, let $v_2 \coloneqq -\hat{v}_1 \bmod u_2$, and let $n_2 \coloneqq n_1 + g + 1 - \deg u_2$.
3. If $n_1 \ge \lceil g/2 \rceil$, let $\hat{v}_1 \coloneqq v_1 + V - (V \bmod u_1)$, let u_2 be $(f - \hat{v}_1^2)/u_1$ made monic, let $v_2 \coloneqq -\hat{v}_1 \bmod u_2$, and let $n_2 \coloneqq n_1 + \deg u_1 - (g+1)$.
4. Output ADJUST$(\operatorname{div}[u_2, v_2, n_2]^*)$.

The polynomial u_2 computed in step 2 or 3 of ADJUST has degree at most g (this is guaranteed by $\deg(f - V^2) \le g$ and $\deg v_1 < \deg u_1$). If $\deg u_1 \le g$ then ADJUST either terminates or outputs a value for n_2 that is strictly closer to the desired range than n_1, and if $\deg u_1 = g+1$ then ADJUST outputs a divisor whose affine part has strictly lower degree with n_2 no further from the desired range than n_1. Thus it always makes progress, and the total number of non-trivial calls to ADJUST (those that do not terminate in step 1) is at most $\lceil g/2 \rceil + 1$.

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

We now give the general algorithm for adding rational divisor classes.

Algorithm ADDITION
Given $\mathrm{div}[u_1, v_1, n_1]$ and $\mathrm{div}[u_2, v_2, n_2]$, compute $\mathrm{div}[u_3, v_3, n_3] \sim \mathrm{div}[u_1, v_1, n_1] + \deg[u_2, v_2, n_2]$.

1. Set $\mathrm{div}[u, v, n]^* \leftarrow \textsc{Compose}(\mathrm{div}[u_1, v_1, n_1], \mathrm{div}[u_2, v_2, n_2])$.
2. While $\deg u > g + 1$, set $\mathrm{div}[u, v, n]^* \leftarrow \textsc{Reduce}(\mathrm{div}[u, v, n]^*)$.
3. Output $\textsc{Adjust}(\mathrm{div}[u, v, n]^*)$.

Note that ADDITION is fully general; the supports of its inputs may overlap, and it can be used with hyperelliptic curves of any genus, so long as the curve has a model with two rational points at infinity (always true over a sufficiently large finite field).

Let us now analyze the behavior of ADDITION in the typical case (which will be overwhelmingly dominant when k is a large finite field). We generically expect divisors to have affine parts of degree g, and even when the two inputs to ADDITION coincide, we expect the GCD computed in step 1 of COMPOSE to be trivial.

More specifically, we expect the following to occur in a typical call to ADDITION:

- The inputs will satisfy $\deg u_1 = \deg u_2 = g$, $\deg v_1 = \deg v_2 = g - 1$, and $n_1 = n_2 = 0$.
- The divisor $\mathrm{div}[u, v, n]^*$ output by COMPOSE will have $\deg u = 2g$, $\deg v = 2g - 1$, and $n = 0$.
- Each call to REDUCE will reduce the affine degree by 2 and increase n by 1.
- The input to ADJUST will have $\deg u = g + 1$ if g is odd, $\deg u = g$ if g is even, and $n = \lfloor g/2 \rfloor$.
- If g is even ADJUST will simply set n to 0 and return. If g is odd ADJUST will reduce the degree of u from $g + 1$ and increase n by 1 in the initial call, and then set n to 0 and return.

It is worth comparing this to Cantor's algorithm for hyperelliptic curves with a rational Weierstrass point, which instead uses a model $y^2 = f(x)$ for C with $\deg f = 2g + 1$. If we remove the steps related to maintaining the integers n, all of which have negligible cost, the algorithms COMPOSE and REDUCE are identical to those used in Cantor's algorithm; the only difference is that in Cantor's algorithm there is no analog of ADJUST. But note that in the typical odd genus case, Cantor's algorithm will need to call REDUCE when $\deg u$ reaches $g + 1$, and this is essentially equivalent to calling ADJUST in the typical odd genus case.

In summary, the asymptotic complexity of ADDITION in the typical case is effectively identical to that of Cantor's algorithm; the only meaningful difference is that the degree of the curve equation is $2g + 2$ rather than $2g + 1$, and this increases the complexity of various operations by a factor of $1 + O(1/g)$.

We conclude this section with an algorithm to compute the additive inverse of a divisor class.[4]

Algorithm NEGATION

[4] We correct a typo that appears in step 4 of the Divisor Inversion algorithms given in [10] and [26] (m_1 should be n_1).

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

Given $\mathrm{div}[u_1, v_1, n_1]$, compute $\mathrm{div}[u_2, v_2, n_2] \sim -\mathrm{div}[u_1, v_1, n_1]$.

1. If g is even, output $\mathrm{div}[u_1, -v_1, g - \deg u_1 - n_1]$ and terminate.
2. If $n_1 > 0$, output $\mathrm{div}[u_1, -v_1, g - \deg u_1 - n_1 + 1]$ and terminate.
3. Output $\textsc{Adjust}(\mathrm{div}[u_1, -v_1, \lceil 3g/2 \rceil - \deg u_1 + 1]^*)$.

Perhaps surprisingly, negation is the one operation that is substantially more expensive when the genus is odd (it is trivial when the genus is even). In the typical case we will have $n_1 = 0$ and the call to ADJUST will need to perform a reduction step.

4. Explicit formulas in genus 3

We now specialize to the case $g = 3$ and give explicit straight-line formulas for the two most common cases of ADDITION: adding divisors with affine parts of degree 3 and disjoint support, and doubling a divisor with affine part of degree 3. We also give a formula for NEGATION in the typical case.

We assume the curve equation is $y^2 = f(x)$ where $f(x) = \sum_{i=0}^{8} f_i x_i$ is monic of degree 8 (so $f_8 = 1$); we also assume that $f_7 = 0$, which can be achieved via the linear substitution $x \to x - f_7/8$. This implies that our precomputed monic polynomial $V = \sum_{i=0}^{4} V_i x^i$ with $\deg(f - V^2) \le 3$ has $V_3 = 0$.

4.1. **Addition in the typical case.** Unraveling the execution of ADDITION in the typical case for $g = 3$ with $\deg u_1 = \deg u_2 = 3$, and $\gcd(u_1, u_2) = 1$ yields the following algorithm.

Algorithm TYPICALADDITION (preliminary version)
Given $\mathrm{div}[u_1, v_1, 0]$ and $\mathrm{div}[u_2, v_2, 0]$ with $\deg u_1 = \deg u_2 = 3$ and $\gcd(u_1, u_2) = 1$, compute

$$\mathrm{div}[u_5, v_5, n_5] \sim \mathrm{div}[u_1, v_1, 0] + \mathrm{div}[u_2, v_2, 0].$$

1. Compute $c_1, c_2 \in k[x]$ such that $c_1 u_1 + c_2 u_2 = 1$.
2. Compute $u_3 \coloneqq u_1 u_2$ and $v_3 \coloneqq (c_1 u_1 v_2 + c_2 u_2 v_1) \bmod u_3$ (we have $\deg u_3 = 6$ and $n_3 = 0$).
3. Let u_4 be $(f - v_3^2)/u_3$ made monic, and let $v_4 \coloneqq -v_3 \bmod u_4$ (we have $\deg u_4 = 4$ and $n_4 = 1$).
4. Let $\hat{v}_4 \coloneqq v_4 - V + (V \bmod u_4)$, let u_5 be $(f - \hat{v}_4^2)/u_4$ made monic, and let $v_5 \coloneqq -\hat{v}_4 \bmod u_5$.
5. Output $\mathrm{div}[u_5, v_5, 3 - \deg u_5]$.

As first proposed by Harley in [12, 15] for genus 2 curves and subsequently exploited and generalized by many authors, the straight-line program obtained by unrolling the loop in Cantor's algorithm [3] in the typical case can be optimized in two ways. The first is to avoid the GCD computation in step 1 by applying the Chinese remainder theorem to the ring $k[x]/(u_3) = k[x]/(u_1 u_2) \simeq k[x]/(u_1) \times k[x]/(u_2)$ to compute

$$v_3 = \big((v_2 - v_1) u_1^{-1} \bmod u_2\big) u_1 + v_1.$$

where u_1^{-1} denotes the inverse of u_1 modulo u_2 (here we use $\gcd(u_1, u_2) = 1$). This expression for v_3 has degree at most 5, which is less than $\deg u_3 = 6$, so there is no need to reduce modulo $u_1 u_2$.

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

The second optimization is to combine composition with the reduction step, in which we compute u_4 as $(f - v_3^2)/u_3$ made monic and $v_4 := -v_3 \bmod u_4$. If we put $\tilde{s} := (v_2 - v_1)u_1^{-1} \bmod u_2$, then u_4 is

$$\frac{f - (\tilde{s}u_1 + v_1)^2}{u_1 u_2} = \frac{(f - v_1^2)/u_1 - \tilde{s}(\tilde{s}u_1 + 2v_1)}{u_2}$$

made monic. All the divisions are exact and u_4 has degree at most 4, so we only need know the top 3 coefficients of $w := (f - v_1^2)/u_1 = x^5 - u_{12}x^4 + (f_6 + u_{12}^2 - u_{11})x^3 + \cdots$, which do not depend on v_1 (here we have used $f_7 = 0$). To simplify matters we assume $\deg s = 2$ (which will typically be true), so that $\deg u_4 = 4$. If we let s be $\tilde{s}$ made monic and put $c := 1/\operatorname{lc}(\tilde{s})$ and $z := su_1$, then

$$u_4 = (s(z + 2cv_2) - c^2 w)/u_2 \qquad \text{and} \qquad v_4 = -v_1 - c^{-1}(z \bmod u_4).$$

These optimizations are exactly the same as those used to obtain existing explicit formulas that optimize Cantor's algorithm for hyperelliptic curves of genus 3 with a rational Weierstrass point using Harley's approach; see [39, Alg. 3], for example. We now discuss a further optimization that is specific to the balanced divisor approach. Rather than computing v_4, we may proceed directly to the computation of $\hat{v}_4 := v_4 - V + (V \bmod u_4)$, which is needed to compute u_5 as $(f - \hat{v}_4^2)/u_4$ made monic. Now V and u_4 are monic of degree 4, so $-V + (V \bmod u_4) = -u_4$ does not depend on V, and

$$\tilde{v}_4 := -\hat{v}_4 = u_4 - v_4 = u_4 + v_1 + c^{-1}(z \bmod u_4)$$

is a monic polynomial of degree 4 that we may use to compute u_5 as $(f - \tilde{v}_4^2)/u_4$ made monic and $v_5 = \tilde{v}_4 \bmod u_5$.

There is a notable difference here with the formulas used for genus 3 hyperelliptic curves with a rational Weierstrass point, where the corresponding expression $(f - v_4^2)/u_4$ is already monic, since $\deg v_4 \le 3$. But $(f - \tilde{v}_4^2)/u_4$ is not monic; its leading coefficient is $-2\tilde{v}_{43}$, where $\tilde{v}_{43}$ denotes the cubic coefficient of $\tilde{v}_4$. Expanding the equations for $u_4, v_4, \tilde{v}_4$ above yields the identity

$$\tilde{v}_{43} = u_{12} - u_{22} + c + 2s_1 + c^{-1}(u_{21} + s_1(s_1 - u_{22}) - s_0). \tag{1}$$

We now give an optimized version of TypicalAddition that forms the basis of our explicit formula.

Algorithm TypicalAddition
Given $\operatorname{div}[u_1, v_1, 0]$ and $\operatorname{div}[u_2, v_2, 0]$ with $\deg u_1 = \deg u_2 = 3$ and $\gcd(u_1, u_2) = 1$, compute

$$\operatorname{div}[u_5, v_5, n_5] \sim \operatorname{div}[u_1, v_1, 0] + \operatorname{div}[u_2, v_2, 0].$$

1. Compute $w := (f - v_1^2)/u_1$, and $\tilde{s} := (v_2 - v_1)u_1^{-1} \bmod u_2$.
2. Compute $c := \operatorname{lc}(\tilde{s})^{-1}$ and $s = c\tilde{s}$ and $z := su_1$ (require $\deg s = 2$).
3. Compute $u_4 := (s(z + 2cv_1) - c^2 w)/u_2$ and $\tilde{v}_4 := v_1 + u_4 + c^{-1}(z \bmod u_4)$.
4. Compute $u_5 := (2\tilde{v}_{43})^{-1}(\tilde{v}_4^2 - f)/u_4$ and $v_5 := \tilde{v}_4 \bmod u_5$ (require $\tilde{v}_{43} \neq 0$).
5. Output $\operatorname{div}[u_5, v_5, 3 - \deg u_5]$.

When expanding TypicalAddition into an explicit formula there are several standard optimizations that one may apply. These include the use of Karatsuba and Toom

style polynomial multiplication, fast algorithms for exact division, the use of Bezout's matrix for computing resultants, and Montgomery's method for combining field inversions. The last is particular relevant to us, as we require three inversions: the inverse of the resultant $r := \mathrm{Res}(u_1, u_2)$ used to compute $u_1^{-1} \bmod u_2$, as well as the inverses of $\mathrm{lc}(\tilde{s})$ and $\tilde{v}_{43}$. We may use equation (1) to calculate $\tilde{v}_{43}$ earlier than it is actually needed so that we can invert all three quantities simultaneously using Montgomery's trick: compute $(r\,\mathrm{lc}(\tilde{s})\tilde{v}_{43})^{-1}$ using one field inversion, and then use multiplications to obtain the desired inverses. We omit the details of these well-known techniques and refer the interested reader to [39, IV].

An explicit formula that implements TypicalAddition appears in the Supplementary Materials section. It includes a single exit point where we may revert to the general Addition algorithm if any of our requirements for typical divisors are not met: it verifies the assumptions $\gcd(u_1, u_2) = 1$, $\deg s = 2$, and $\tilde{v}_{43} \neq 0$. This makes it unnecessary to verify $\gcd(u_1, u_2) = 1$ before applying the formula.

We give field operation counts for each step in the form $[i\mathbf{I} + m\mathbf{M} + a\mathbf{A}]$, where i denotes the number of field inversions, m is the number of field multiplications (including squarings), and a is the number of additions or subtractions of field elements. The count a includes multiplications by 2, and also divisions by 2, which can be efficiently implemented using a bit-shift (possibly preceded by an integer addition) and costs no more than a typical field addition. The divisions by 2 arise primarily in places where we have used Toom-style multiplications and could easily be removed if one wished to adapt the formula to characteristic 2 by switching to Karatsuba.

The total cost of the formula for TypicalAddition is **I+79M+127A**; this is within 10 or 20 percent of the **I+67M+108A** cost of the best known formula for addition on genus 3 hyperelliptic curves with a rational Weierstrass point [30] (the exact ratio depends on the cost of field inversions relative to multiplications).[5] Aside from increasing the degree of f, the main difference in the two formulas is the need to compute and invert $\hat{v}_{43}$, and to then multiply by this inverse to make u_5 monic. By comparison, the cost of a naïve implementation of the unoptimized version of TypicalAddition that uses standard algorithms for multiplication, division with remainder, and GCD (as in [11, Ch. 1], for example), in which we do not count multiplications or divisions by 1, is **5I+275M+246A** (c.f. [28, p. 445]). Our optimizations thus improve performance by a factor of 4 or 5, in terms of the cost of field operations. In practice the speedup is better than this, closer to 6× when working over word-sized finite fields. This is due largely to the removal of almost all conditional logic from the explicit formula.

4.2. **Doubling in the typical case.** When doubling a divisor the inputs to Addition are identical, but the GCD computed in Compose is still trivial in the typical case where $\gcd(u_1, v_1) = 1$ with $\deg u_1 = 3$. The divisor $\mathrm{div}[u_3, v_3, n_3]$ output by Compose will have $u_3 = u_1^2$ and $v_3 = (c_1 u_1 v 1 + c_3(v_1^2 + f)) \bmod u_1^2$, where $c_1 u_1 + 2c_3 v_1 = 1$. In this situation we have $v_3 \equiv v_1 \bmod u_1$, and since both $\mathrm{div}[u_1, v_1]$ and $\mathrm{div}[u_3, v_3]$ are Mumford representations of semi-reduced divisors, we have $u_1 | (v_1^2 - f)$ and $u_1^2 | (v_3^2 - f)$. We may thus view v_1 as a square root of f modulo u_1, and we may view v_3 as a "lift" of

[5] The formula in [30] contains some typographical errors; see [8, p. 25] for a clean version.

this square root from $k[x]/(u_1)$ to $k[x]/(u_1^2)$. Rather than computing v_3 as in COMPOSE, as suggested in [12] we may instead compute it using a single u_1-adic Newton iteration:

$$v_3 := v_1 - \frac{v_1^2 - f}{2v_1} \bmod u_1^2.$$

If we put $w := (f - v_1^2)/u_1$ and define $\tilde{s} := w(2v_1)^{-1} \bmod u_1$, where $(2v_1)^{-1}$ denotes the inverse of $2v_1$ modulo u_1 (here we use $\gcd(u, v_1) = 1$), then $v_3 = v_1 + \tilde{s}u_1$, and u_4 is

$$\frac{f - (v_1 + \tilde{s}u_1)^2}{u_1^2} = \frac{w - 2v_1\tilde{s}}{u_1} - \tilde{s}^2$$

made monic. We now proceed as in §4.1. We assume $\deg \tilde{s} = 2$, let s be $\tilde{s}$ made monic, and define $c := \mathrm{lc}(\tilde{s})^{-1}$ and $z := su_1$. We then have

$$u_4 = s^2 - (c^2 w - 2cv_1 s)/u_1 \qquad \text{and} \qquad v_4 = -v_1 - c^{-1}(z \bmod u_4),$$

and

$$\tilde{v}_4 := -\hat{v}_4 = u_4 - v_4 = u_4 + v_1 + c^{-1}(z \bmod u_4)$$

is a monic polynomial of degree 4 that we may use to compute u_5 as $(f - \tilde{v}_4^2)/u_4$ made monic and $v_5 = \tilde{v}_4 \bmod u_5$. The polynomial $(f - \tilde{v}_4^2)/u_4$ has leading coefficient $-2\tilde{v}_{43}$, and expanding the equations for $u_4, v_4, \tilde{v}_4$ yields the identity

$$\tilde{v}_{43} = 2s_1 + c + c^{-1}(s_1(s_1 - u_{12}) - s_0 + u_{11}). \tag{2}$$

This leads to the following optimized formula for doubling a typical divisor.

Algorithm TYPICALDOUBLING
Given $\mathrm{div}[u_1, v_1, 0]$ with $\deg u_1 = 3$ and $\gcd(u_1, v_1) = 1$, compute

$$\mathrm{div}[u_5, v_5, n_5] \sim 2\,\mathrm{div}[u_1, v_1, 0].$$

1. Compute $\overline{w} := (f - v_1^2)/u_1 \bmod u_1$, and $\tilde{s} := \overline{w}(2v_1)^{-1} \bmod u_1$.
2. Compute $c := \mathrm{lc}(\tilde{s})^{-1}$, and $s := c\tilde{s}$ and $z := su_1$ (require $\deg s = 2$).
3. Compute $u_4 := (c^2 w - 2csv_1)/u_1 - s^2$ and $\tilde{v}_4 := v_1 + u_4 + c^{-1}(z \bmod u_4)$.
4. Compute $u_5 := (2\tilde{v}_{43})^{-1}(\tilde{v}_4^2 - f)/u_4$ and $v_5 := \tilde{v}_4 \bmod u_5$ (require $\tilde{v}_{43} \neq 0$).
5. Output $\mathrm{div}[u_5, v_5, 3 - \deg u_5]$.

An explicit formula that implements TYPICALDOUBLING appears in the Supplementary Materials section. In terms of field operations, its total cost is **I+82M+127A**, which may be compared with **I+68M+102A** for the best known formula for a genus 3 curve with a rational Weierstrass point [30], and **5I+285M+258A** for the unoptimized cost of doubling a typical divisor.

4.3. **Negation in the typical case.** Finally, we consider the case of negating a typical divisor $\mathrm{div}[u_1, v_1, 0]$ with $\deg u_1 = 3$, which amounts to computing $\mathrm{ADJUST}(\mathrm{div}[u_1, -v_1, 3]^*)$. Let

$$\tilde{v}_1 := v_1 - V + (V \bmod u_1) = -x_4 + \tilde{v}_{12}x^2 + \tilde{v}_{11}x + \tilde{v}_{10}$$

(here we have used $V_3 = 0$). We wish to compute u_2 as $(f - \tilde{v}_1^2)/u_1$ made monic and $v_2 := \tilde{v}_1 \bmod u_2$. The polynomial $(f - \tilde{v}_1)^2/u_1$ has degree 3 and leading coefficient $f_6 + 2\tilde{v}_{12}$, where

$$\tilde{v}_{12} = v_{12} + u_{12}^2 - u_{11}.$$

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

We thus obtain the following algorithm.

Algorithm TYPICALNEGATION
Given $\operatorname{div}[u_1, v_1, 0]$ with $\deg u_1 = 3$, compute $\operatorname{div}[u_2, v_2, n_2] \sim -\operatorname{div}[u_1, v_1, 0]$.

1. Compute $\tilde{v}_1 := v_1 - V + (V \bmod u_1)$.
2. Compute $u_2 := (f_6 + 2\tilde{v}_{12})^{-1}(f - \tilde{v}_1^2)/u_1$ and $v_2 := \tilde{v}_1 \bmod u_2$ (require $f_6 + 2\tilde{v}_{12} \neq 0$).
3. Output $\operatorname{div}[u_2, v_2, 0]$.

REFERENCES

[1] Jeffrey D. Achter, *Results of Cohen-Lenstra type for quadratic function fields*, in *Computational Arithmetic Geometry*, Contemporary Mathematics **463**, American Mathematical Society (2008), 1–7.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system I: The user language*, Journal of Symbolic Computation **24** (1997), 235–265.

[3] David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101.

[4] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of elliptic and hyperelliptic cryptography*, Discrete Mathematics and Its Applications **34**, Chapman and Hall/CRC, 2005

[5] Henri Cohen and Hendrik W. Lenstra, Jr., *Heuristics on class groups*, in *Number theory* (New York, 1982), Lecture Notes in Mathematics **1052**, Springer, 1984, 26–36.

[6] Noam D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in *Computational Perspectives on Number Theory, Proceedings of a Conference in Honor of A.O.L. Atkin*, Studies in Advanced Mathematics **7**, American Mathematical Society, 1995, 21–76.

[7] Stefan Erickson, Michael J. Jacobson Jr. and Andreas Stein, *Explicit formulas for real hyperelliptic curves of genus 2 in affine representation*, Adv. Math. Commun. **5** (2011), 623–666.

[8] Xinxin Fan, Thomas Wollinger, and Guang Gong, *Efficient explicit formulae for genus 3 hyperelliptic curve cryptosystems*, Technical Report CACR 2006-37, Centre for Applied Cryptographic Research, available at `http://cacr.uwaterloo.ca/techreports/2006/cacr2006-38.pdf`.

[9] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, in *Théories des nombres* (Quebec, 1987), de Gruyter, 1989, 227–239.

[10] Steven G. Galbraith, Michael Harrison, and David J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, in *Algorithmic Number Theory 8th International Symposium (ANTS-VIII)*, A.J. van der Poorten and A. Stein (eds.), Lecture Notes in Computer Science **5011**, Springer, 2008, 342–356.

[11] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 3rd ed., Cambridge University Press, 2013.

[12] Pierrick Gaudry and Robert Harley, *Counting points on hyperelliptic curves over finite fields*, in *Algorithmic Number Theory 4th International Symposium (ANTS IV)*, W. Bosma (ed.), Lecture Notes in Computer Science **1838**, Springer, 2000, 313–332.

[13] Masaki Gonda, Kazuto Matsuo, Kazumaro Aoki, Jinhui Chao, Shigeo Tsujii, *Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementations*, in *The 2004 Symposium on Cryptography and Information Security, Sendai Japan*, IEICE Transactions of Fundamentals of Electronics, Communications, and Computer Science, 2005, 89–96.

[14] Cyril Guyot, Kiumars Kaveh, and Vijay M. Patankar, *Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus 3*, J. Ramanujan Math. Soc. **19** (2004), 75–115.

[15] Robert Harley, Addenda to [12], available at `http://cristal.inria.fr/~harley/hyper`, 2000.

[16] David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Annals of Mathematics **179** (2014), 783–803.

[17] David Harvey, Maike Massierer, and Andrew V. Sutherland *Computing L-series of geometrically hyperelliptic curves of genus three*, in *Algorithmic Number Theory 12 International Symposium (ANTS XII)*, LMS J. Comput. Math. **19** (2016), 220–234.

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

[18] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, in *Algorithmic Number Theory 11th International Symposium (ANTS XI)*, LMS Journal of Computation and Mathematics **17** (2014), 257–273.

[19] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663**, American Mathematical Society, 127–148.

[20] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, in *Algorithmic Number Theory 8th International Symposium (ANTS VIII)*, Lecture Notes in Computer Science **5011**, Springer, 2008, 312–326.

[21] Michael J. Jacobson, Jr., Monireh Rezai Rad, and Renate Scheidler, *Comparison of scalar multiplication on real hyperelliptic curves*, Adv. Math. Comm. **8** (2014), 389–406.

[22] Michael J. Jacobson, Renate Scheidler, and Andreas Stein, *Cryptographic protocols on real hyperelliptic curves*, Adv. Math. Comm. **2** (2007), 197–221.

[23] Junichi Kuroki, Masaki Gonda, Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *Fast genus three hyperelliptic curve cryptosystems*, in *The 2002 Symposium on Cryptography and Information Security (SCIS 2002)*, Shirahama, Japan.

[24] Tanja Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Appl. Algebra Engr. Comm. Comput. **15** (2005), 295–328.

[25] James S. Milne, *Jacobian varieties*, in *Arithmetic Geometry*, G. Cornell and J.H. Silverman (eds.), Springer, 1986, 167–212.

[26] David J. Mireles Morales, *Efficient arithmetic on hyperelliptic curves with real representation*, PhD Thesis, University of London, 2008.

[27] David Mumford, *Tata Lectures on Theta II*, Birkhaüser, 2007 (reprint of the 1984 edition).

[28] Koh-ichi Nagao, *Improving group law algorithms for Jacobians of hyperelliptic curves*, in *Algorithmic Number Theory 4th International Symposium (ANTS IV)*, W. Bosma (ed.), Lecture Notes in Computer Science **1838**, Springer, 2000, 439–447.

[29] Jun Nyukai, *A fast addition algorithms on hyperelliptic curves* (in Japanese), technical report, available at `http://ir.c.chuo-u.ac.jp/repository/search/binary/p/3114/s/1893/`, 2006.

[30] Jun Nyukai, Kazuto Matsuo, Jinhui Chao, and Shigeo Tujii, *On the resultant computation in the Harley algorithms on hyperelliptic curves* (in Japanese), Technical Report ISEC2006-5, IEICE Japan, 2006.

[31] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.

[32] Andrew P. Ogg, *On the Weierstrass points of $X_0(N)$*, Illinois J. Math. **22** (1978), 31–35.

[33] Sachar Paulus and Hans-Georg Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp. **68** (1999), 1233-1241.

[34] Bjorn Poonen, *Computational aspects of curves of genus at least 2*, in *Algorithmic Number Theory 2nd International Symposium (ANTS II)*, Lecture Notes in Computer Science **1122**, Springer, 2005, 283–306.

[35] Monireh Rezai Rad, *A complete evaluation of arithmetic in real hyperelliptic curves*, Ph.D. thesis, University of Calgary, 2016.

[36] Renate Scheidler, Andreas Stein, and Hugh C. Williams, *Key-exchange in real quadratic congruence function fields*, Des. Codes Cryptography **7** (1996), 153–174.

[37] Andrew V. Sutherland, *Order computations in generic groups*, PhD thesis, Massachusetts Institute of Technology, 2007.

[38] Andrew V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Mathematics of Computation **80** (2011), 477–500.

[39] Thomas Wollinger, Jan Pelzl, and Christof Paar, *Cantor versus Harley: Optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems*, IEEE Transactions on Computers **54** (2005), 861–872.

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

Supplementary material

The explicit formulas presented on the following pages were typeset using latex source generated by an automated script that reads an executable version of verified source code; they should thus be free of the typos that unfortunately plague many of the formulas one finds in the literature. Magma source code for the formulas and an implementation of all the algorithms in this article and code to test their correctness can be found at

https://math.mit.edu/~drew/BalancedDivisor.m

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

TypicalAddition: $\mathrm{div}[u_5,v_5,n_5] \sim \mathrm{div}[u_1,v_1,0]+\mathrm{div}[u_2,v_2,0]$ with $\gcd(u_1,u_2)=1$.
1. Compute $r := \mathrm{Res}(u_1,u_2)$ and $i(x) = i_2x^2+i_1x+i_0 := ru_1^{-1} \bmod u_2$ (and $w_0 := u_{11}-u_{12}$). **[15M+12A]**
$t_1 := u_{10}-u_{20}$; $t_2 := u_{11}-u_{21}$; $w_0 := u_{12}-u_{22}$; $t_3 := t_2-u_{22}w_0$; $t_4 := t_1-u_{21}w_0$; $t_5 := u_{22}t_3-t_4$; $t_6 := u_{20}w_0+u_{21}t_3$; $i_0 := t_4t_5-t_3t_6$; $i_1 := w_0t_6-t_2t_5$; $i_2 := w_0t_4-t_2t_3$; $r := t_1i_0-u_{20}(t_3i_2+w_0i_1)$;
2. Compute $q(x) = q_2x^2+q_1x+q_0 := r(v_2-v_1)u_1^{-1} \bmod u_2$. **[10M+30A]**
$t_1 := v_{20}-v_{10}$; $t_2 := v_{11}-v_{21}$; $t_3 := v_{12}-v_{22}$; $t_4 := t_2i_1$; $t_5 := t_1i_0$; $t_6 := t_3i_2$; $t_7 := u_{22}t_6$; $t_8 := t_4+t_6+t_7-(t_2+t_3)(i_1+i_2)$; $t_9 := u_{20}+u_{22}$; $t_{10} := (t_9+u_{21})(t_8-t_6)$; $t_{11} := (t_9-u_{21})(t_8+t_6)$; $q_0 := t_5-u_{20}t_8$; $q_1 := t_4-t_5+(t_{11}-t_{10})/2-t_7+(t_1-t_2)(i_0+i_1)$; $q_2 := t_6-q_0-t_4+(t_1-t_3)(i_0+i_2)-(t_{10}+t_{11})/2$;
3. Compute $t_1 := rq_2\tilde{v}_{43}$ via (1), and $w_1 := c^{-1} = q_2/r$, $w_2 := c = r/q_2$, $w_3 := c^2$, $w_4 := (2\tilde{v}_{43})^{-1}$. Then compute $s(x) = x^2+s_1x+s_0 := c(v_2-v_1)u_1^{-1} \bmod u_2$ and $\tilde{v}_{43}$. **[I+18M+6A]**
$t_1 := (r+q_1)^2+q_2(rw_0+q_2u_{21}-q_1u_{22}-q_0)$; $t_2 := 2t_1$; $t_3 := rq_2$; If $t_2 = 0$ or $t_3 = 0$ then abort (revert to Addition). $t_4 := 1/(t_2t_3)$; $t_5 := t_2t_4$; $t_6 := rt_5$; $w_1 := t_5q_2^2$; $w_2 := rt_6$; $w_3 := w_2^2$; $w_4 := t_3^2t_4$; $s_0 := t_6q_0$; $s_1 := t_6q_1$; $\tilde{v}_{43} := t_1t_5$;
4. Compute $z(x) = x^5+z_4x^4+z_3x^3+z_2x^2+z_1x+z_0 := su_1$. **[4M+15A]**
$t_6 := s_0+s_1$; $t_1 := u_{10}+u_{12}$; $t_2 := t_6(t_1+u_{11})$; $t_3 := (t_1-u_{11})(s_0-s_1)$; $t_4 := u_{12}s_1$; $z_0 := u_{10}s_0$; $z_1 := (t_2-t_3)/2-t_4$; $z_2 := (t_2+t_3)/2-z_0+u_{10}$; $z_3 := u_{11}+s_0+t_4$; $z_4 := u_{12}+s_1$;
5. Compute $u_4(x) = x^4+u_{43}x^3+u_{42}x^2+u_{41}x+u_{40} := (s(z+2cv_1)-c^2(f-v_1^2)/u_1)/u_2$. **[14M+31A]**
$u_{43} := z_4+s_1-u_{22}$; $t_0 := s_1z_4$; $t_1 := u_{22}u_{43}$; $u_{42} := z_3+t_0+s_0-w_3-u_{21}-t_1$; $t_2 := u_{21}u_{42}$; $t_3 := (u_{21}+u_{22})(u_{42}+u_{43})-t_1-t_2$; $t_4 := 2w_2$; $t_5 := t_4v_{12}$; $t_6 := s_0z_3$; $t_7 := (s_0+s_1)(z_3+z_4)-t_0-t_6$; $u_{41} := z_2+t_7+t_5+w_3u_{12}-u_{20}-t_3$; $u_{40} := z_1+s_1(t_5+z_2)+t_6+t_4v_{11}-w_3(f_6+u_{12}^2-u_{11})-u_{20}u_{43}-t_2-u_{22}u_{41}$;
6. Compute $\tilde{v}_4(x) = x^4+\tilde{v}_{43}x^3+\tilde{v}_{42}x^2+\tilde{v}_{41}x+\tilde{v}_{40} := -\hat{v}_4 = v_1+u_4+c^{-1}(z \bmod u_4)$. **[6M+10A]**
$t_1 := u_{43}-z_4+w_2$; $\tilde{v}_{40} := v_{10}+w_1(z_0+u_{40}t_1)$; $\tilde{v}_{41} := v_{11}+w_1(z_1-u_{40}+u_{41}t_1)$; $\tilde{v}_{42} := v_{12}+w_1(z_2-u_{41}+u_{42}t_1)$;
7. Compute $u_5(x) = x^3+u_{52}x^2+u_{51}x+u_{50} := (2\tilde{v}_{43})^{-1}(\tilde{v}_4^2-f)/u_4$. **[9M+17A]**
$u_{52} := \tilde{v}_{43}/2+w_4(2\tilde{v}_{42}-f_6)-u_{43}$; $u_{51} := w_4(2(\tilde{v}_{41}+\tilde{v}_{43}\tilde{v}_{42})-f_5)-u_{52}u_{43}-u_{42}$; $u_{50} := w_4(\tilde{v}_{42}^2+2(\tilde{v}_{40}+\tilde{v}_{43}\tilde{v}_{41})-f_4)-u_{51}u_{43}-u_{52}u_{42}-u_{41}$;
8. Compute $v_5(x) = v_{52}x^2+v_{51}x+v_{50} := \tilde{v}_4 \bmod u_5$. **[3M+6A]**
$t_1 := u_{52}-\tilde{v}_{43}$; $v_{50} := \tilde{v}_{40}+t_1u_{50}$; $v_{51} := \tilde{v}_{41}-u_{50}+t_1u_{51}$; $v_{52} := \tilde{v}_{42}-u_{51}+t_1u_{52}$;
9. Output $\mathrm{div}[u_5,v_5,3-\deg u_5]$. **[Total: I+79M+127A]**

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

TYPICALDOUBLING: $\mathrm{div}[u_5, v_5, n_4] \sim 2\,\mathrm{div}[u_1, v_1, 0]$ with $\gcd(u_1, v_1) = 1$.
1. Compute $r := \mathrm{Res}(u_1, v_1)$ and $i(x) = i_2x^2 + i_1x + i_0 := rv_1^{-1} \bmod u_1$ ($w_0 := v_{11} - u_{12}v_{12}$). **[15M+9A]**
$w_0 := v_{11} - u_{12}v_{12}$; $t_2 := v_{10} - u_{11}v_{12}$; $t_3 := u_{12}w_0 - t_2$; $t_4 := u_{10}v_{12} + u_{11}w_0$; $i_0 := w_0t_4 - t_2t_3$; $i_1 := v_{11}t_3 - v_{12}t_4$; $i_2 := v_{11}w_0 - v_{12}t_2$; $r := v_{10}i_0 - u_{10}(w_0i_2 + v_{12}i_1)$;
2. Compute $p(x) = p_2x^2 + p_1x + p_0 := \overline{w} := (f - v_1^2)/u_1 \bmod u_1$ ($w_1 := u_{12}^2$, $w_2 := w_1 + f_6$). **[11M+24A]**
$w_1 := u_{12}^2$; $t_2 := 2u_{10}$; $t_3 := 3u_{11}$; $w_2 := w_1 + f_6$; $t_5 := 2t_2 - f_5$; $t_6 := 2u_{12}$; $t_7 := t_3 - w_2$; $p_2 := f_5 + t_6(t_7 - w_1) - t_2$; $p_1 := f_4 + u_{12}t_5 - v_{12}^2 - u_{11}(2f_6 - t_3) - w_1(t_7 + t_3)$; $p_0 := f_3 - u_{11}(w_1t_6 - t_5) - t_2w_2 - u_{12}p_1 - 2v_{11}v_{12}$;
3. Compute $q(x) = q_2x^2 + q_1x + q_0 := r((f - v_1^2)/u_1)v_1^{-1} \bmod u_1$. **[10M+28A]** ($w_3 := u_{10} + u_{11} + u_{12}$, $w_4 := u_{10} - u_{11} + u_{12}$)
$t_1 := i_1p_1$; $t_2 := i_0p_0$; $t_3 := i_2p_2$; $t_4 := u_{12}t_3$; $t_5 := (i_1 + i_2)(p_1 + p_2) - t_1 - t_3 - t_4$; $t_6 := u_{10}t_5$; $t_7 := u_{10} + u_{12}$; $w_3 := t_7 + u_{11}$; $w_4 := t_7 - u_{11}$; $t_{10} := w_3(t_3 + t_5)$; $t_{11} := w_4(t_5 - t_3)$; $q_0 := t_2 - t_6$; $q_1 := t_4 + (i_0 + i_1)(p_0 + p_1) + (t_{11} - t_{10})/2 - t_1 - t_2$; $q_2 := t_1 + t_6 + (i_0 + i_2)(p_0 + p_2) - t_2 - t_3 - (t_{10} + t_{11})/2$;
4. Compute $t_3 := 2rq_2\tilde{v}_{43}$ via (2), and $w_5 := 1/c$, $w_6 := c, w_7 := 1/\tilde{v}_{43}$. **[I+17M+7A]** Then compute $s(x) = x^2 + s_1x + s_0 := q/(2r)$ made monic and $\tilde{v}_{43}$.
$t_0 := 2r$; $t_1 := t_0^2$; $t_2 := q_2^2$; $t_3 := t_1 - q_0q_2 + q_1(2t_0 + q_1 - q_2u_{12}) + t_2u_{11}$; If $q_2 = 0$ or $t_3 = 0$ then abort (revert to ADDITION). $t_4 := 1/(t_0q_2t_3)$; $t_5 := t_3t_4$; $t_6 := t_0t_5$; $w_5 := t_2t_5$; $w_6 := t_1t_5$; $w_7 := t_1t_2t_4$; $s_0 := t_6q_0$; $s_1 := t_6q_1$; $\tilde{v}_{43} := t_3t_5$;
5. Compute $z(x) = x^5 + z_4x^4 + z_3x^3 + z_2x^2 + z_1x + z_0 := su_1$. **[4M+12A]**
$t_1 := w_3(s_0 + s_1)$; $t_2 := w_4(s_0 - s_1)$; $t_3 := u_{12}s_1$; $z_0 := s_0u_{10}$; $z_1 := (t_1 - t_2)/2 - t_3$; $z_2 := (t_1 + t_2)/2 - z_0 + u_{10}$; $z_3 := u_{11} + s_0 + t_3$; $z_4 := u_{12} + s_1$;
6. Compute $u_4(x) = x^4 + u_{43}x^3 + u_{42}x^2 + u_{41}x + u_{40} := s^2 - (c^2(f - v_1^2)/u_1 - 2csv_1)/u_1$. **[9M+14A]**
$t_1 := v_{12}w_6$; $t_2 := w_6^2$; $u_{43} := 2s_1$; $u_{42} := 2s_0 + s_1^2 - t_2$; $u_{41} := 2(s_0s_1 + u_{12}t_2 + t_1)$; $u_{40} := s_0^2 + 2(w_0w_6 + s_1t_1) - t_2(w_2 + 2(w_1 - u_{11}))$;
7. $\tilde{v}_4(x) = \tilde{v}_{43}x^3 + \tilde{v}_{42}x^2 + \tilde{v}_{41}x + \tilde{v}_{40} := -\hat{v}_4 = v_1 + u_4 + c^{-1}(z \bmod u_4)$. **[6M+10A]**
$t_1 := u_{43} - z_4 + w_6$; $\tilde{v}_{40} := v_{10} + w_5(z_0 + u_{40}t_1)$; $\tilde{v}_{41} := v_{11} + w_5(z_1 - u_{40} + u_{41}t_1)$; $\tilde{v}_{42} := v_{12} + w_5(z_2 - u_{41} + u_{42}t_1)$;
8. $u_5(x) = x^3 + u_{52}x^2 + u_{51}x + u_{50} := (2\tilde{v}_{43})^{-1}(\tilde{v}_4^2 - f)/u_4$. **[7M+17A]**
$u_{52} := \tilde{v}_{43}/2 + w_7(\tilde{v}_{42} - f_6/2) - u_{43}$; $u_{51} := \tilde{v}_{42} + w_7(\tilde{v}_{41} - f_5/2) - u_{52}u_{43} - u_{42}$; $u_{50} := \tilde{v}_{41} + w_7((\tilde{v}_{42}^2 - f_4)/2 + \tilde{v}_{40}) - u_{51}u_{43} - u_{52}u_{42} - u_{41}$;
9. $v_5(x) = v_{52}x^2 + v_{41}x + v_{50} := \tilde{v}_4 \bmod u_5$. **[3M+6A]**
$t_1 := u_{52} - \tilde{v}_{43}$; $v_{50} := \tilde{v}_{40} + t_1u_{50}$; $v_{51} := \tilde{v}_{41} - u_{50} + t_1u_{51}$; $v_{52} := \tilde{v}_{42} - u_{51} + t_1u_{52}$;
10. Output $\mathrm{div}[u_5, v_5, 3 - \deg u_5]$. **[Total: I+82M+127A]**

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

TYPICALNEGATION: $\mathrm{div}[u_2, v_2, 0] \sim -\mathrm{div}[u_1, v_1, 0]$.
1. Compute $\tilde{v}_1(x) = -x^4 + \tilde{v}_{12}x^2 + \tilde{v}_{11}x + \tilde{v}_{10} := v_1 - V + (V \bmod u_1)$. **[3M+5A]**
$\tilde{v}_{12} := v_{12} - u_{11} + u_{12}^2$; $\tilde{v}_{11} := v_{11} - u_{10} + u_{11}u_{12}$; $\tilde{v}_{10} := v_{10} + u_{10}u_{12}$;
2. Compute $u_2(x) = x^3 + u_{22}x^2 + u_{21}x + u_{20} := (f_6 + 2\tilde{v}_{12})^{-1}(f - \tilde{v}_1^2)/u_1$. **[I+8M+14A]**
$t_1 := 2\tilde{v}_{12}$; $\quad t_2 := f_6 + t_1$; If $t_1 = 0$ then abort (revert to NEGATION). $t_3 := 1/t_2$; $u_{22} := t_3(f_5 + 2\tilde{v}_{11}) - u_{12}$; $u_{21} := t_3(f_4 + 2\tilde{v}_{10} - \tilde{v}_{12}^2) - u_{11} - u_{12}u_{22}$; $u_{20} := t_3(f_3 - t_1\tilde{v}_{11}) - u_{10} - u_{11}u_{22} - u_{12}u_{21}$;
3. Compute $v_2(x) = v_{22}x^2 + v_{21}x + v_{20} := \tilde{v}_1 \bmod u_2$. **[3M+5A]**
$v_{22} := \tilde{v}_{12} - u_{22}^2 + u_{21}$; $v_{21} := \tilde{v}_{11} - u_{21}u_{22} + u_{20}$; $v_{20} := \tilde{v}_{10} - u_{20}u_{22}$;
4. Output $\mathrm{div}[u_2, v_2, 0]$. **[Total: I+14M+24A]**

9 Jun 2018 14:25:56 PDT
Version 3 - Submitted to Open Book Series

CONSTRUCTING PICARD CURVES WITH COMPLEX MULTIPLICATION USING THE CHINESE REMAINDER THEOREM

SONNY ARORA AND KIRSTEN EISENTRÄGER

Abstract. We give a new algorithm for constructing Picard curves over a finite field with a given endomorphism ring. This has important applications in cryptography since curves of genus 3 allow one to work over smaller fields than the elliptic curve case. For a sextic CM-field K containing the cube roots of unity, we define and compute certain class polynomials modulo small primes and then use the Chinese Remainder Theorem to construct the class polynomials over the rationals. We also give some examples.

1. Introduction

For cryptographic protocols whose security relies on the difficulty of the discrete log problem, one often wants to find a group whose order is divisible by a large prime. One option for the group is the group of points of an elliptic curve over a finite field, or more generally, the group of points on the Jacobian of a curve over a finite field. Thus, we are interested in the problem of finding curves over finite fields whose Jacobian has a given number of points.

For elliptic curves, Atkin and Morain showed in [3] that one can use the theory of complex multiplication to solve this problem. The approach taken in [3] involves computing the Hilbert class polynomial with respect to an imaginary quadratic field by evaluating modular j-invariants at certain values. An alternate method to construct the Hilbert class polynomial, taken in [9] and [1], is to compute the polynomial modulo several small primes and then reconstruct the polynomial using the Chinese Remainder Theorem. In the genus 2 case, analogous to the construction of the Hilbert class polynomial, one wishes to construct the so-called Igusa class polynomials. In this case, one can again use a Chinese Remainder Theorem approach to construct the Igusa class polynomials as shown in [11], [12].

If one wishes to construct genus 3 curves with a given number of points, less is known. Genus 3 curves fall into two classes: hyperelliptic curves and non-hyperelliptic plane quartics. One difficulty in the case of genus 3 curves is that there is no theory of invariants which works for all genus 3 curves. However, invariants do exist for the classes of hyperelliptic curves and non-hyperelliptic plane quartics separately. By making restrictions on the type of genus 3 curves considered, algorithms for constructing genus 3 curves with complex multiplication have been presented in [36], [23], [25], [4], and [20]. All these papers take a complex analytic approach to

The first author was partially supported by National Science Foundation grants DMS-1056703 and CNS-1617802. The second author was partially supported by National Science Foundation awards DMS-1056703 and CNS-1617802, and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0541.

4 Jun 2018 06:44:41 PDT
Version 3 - Submitted to Open Book Series

constructing genus 3 curves similar to the method in [3]. The papers [36], [4] deal with constructing hyperelliptic genus 3 curves with complex multiplication. The paper [23] and its improvement [25] deal with constructing Picard curves with complex multiplication, while [20] deals with constructing plane quartics defined over $\mathbb{Q}$ with complex multiplication. Due to the numerous improvements to the Chinese Remainder theorem approach in the elliptic curve case [5], [33], it is of interest to try to implement a Chinese Remainder Theorem approach for the construction of genus 3 curves. This is the aim of this paper.

As in [23], we will restrict our attention to Picard curves. These are genus 3 curves of the form $y^3 = f(x)$ where $\deg(f) = 4$ and f has no repeated roots over the algebraic closure. One advantage to using these curves is that it is very simple to generate representatives for all isomorphism classes of Picard curves over a finite field. Also, if K is a sextic CM-field that contains the cube roots of unity, then, by [23, Lemma 1], all simple, principally polarized abelian varieties of dimension 3 with complex multiplication by $\mathcal{O}_K$ arise as the Jacobians of Picard curves, so we can use Picard curves in a CRT approach.

1.1. **Statement of theorem.** Let K be a sextic CM-field containing the cube roots of unity. Fix a primitive CM-type Φ on the field K. Our first step will be to define suitable class polynomials for (K, Φ). For this we will require invariants for Picard curves.

We work with the set of invariants for Picard curves j_1, j_2, j_3 defined in [22]. They are discussed in more detail in Section 3.

We now wish to introduce class polynomials for Picard curves. Recall, the Hilbert class polynomial for an imaginary quadratic field K has as roots the j-invariants of elliptic curves with complex multiplication by the full ring of integers $\mathcal{O}_K$ of K. Analogous to this situation, we would like the class polynomials we define, for a sextic CM-field K containing the cube roots of unity, to have as roots the invariants of Picard curves with complex multiplication by $\mathcal{O}_K$. A complication that does not arise in the genus 1 case is that we will need to restrict to Picard curves whose Jacobian has a given primitive CM-type on K. In genus 2, a restriction on the CM-type for class polynomials was discussed in [26].

We would like our class polynomials to be defined over $\mathbb{Q}$. This will allow us to multiply by a large enough integer to clear denominators and hence use the Chinese remainder theorem on the resulting polynomials modulo various primes. For an abelian variety A of CM-type (K, Φ) and for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, A^σ is of type $(K, \sigma\Phi)$. Thus, we define class polynomials for $i = 1, ..., 3$ as follows:

$$H_i^\Phi := \prod (X - j_i(C)),$$

where the product runs over all isomorphism classes of Picard curves $C/\mathbb{C}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ of type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. These polynomials will be defined over $\mathbb{Q}$. Should one want to re-construct a Picard curve $C/\mathbb{C}$ such that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$ from the roots of the class polynomials, it is more convenient to work with a different set of class polynomials, introduced in [14] in the genus 2 setting. This is discussed more in Section 4.

We have the following theorem:

Theorem 1.1. *The following algorithm takes as input a sextic CM-field K containing the cube roots of unity and a primitive CM-type Φ on K. Assuming the*

4 Jun 2018 06:44:41 PDT
Version 3 - Submitted to Open Book Series

bound B in Theorem 5.4 is known, the algorithm outputs the class polynomials H_i^Φ, where $i = 1, ..., 3$, corresponding to the type (K, Φ)

(i) Construct a set of rational primes S which satisfy
  (a) $2 \notin S$
  (b) Each $p \in S$ splits completely in K
  (c) Each $p \in S$ splits completely into principal ideals in K^*, the reflex field for the type (K, Φ).
  (d) $\prod_{p \in S} p > B$ where B is the bound in Theorem 5.4.

(ii) Form the class polynomials H_i^Φ modulo p for every $p \in S$. Let $H_{i,p} := H_i^\Phi \mod p$. Then

$$H_{i,p} = \prod (X - j_i(C)),$$

where the product is over all $\overline{\mathbb{F}}_p$-isomorphism classes of Picard curves that arise as the reduction of a Picard curve over $\mathbb{C}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ of type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(iii) Form the polynomials H_i^Φ from the $H_{i,p}$, $p \in S$, using the Chinese Remainder Theorem.

We review background from the theory of complex multiplication in Section 2 and prove some results we will need. In Section 3 we review invariants of Picard curves. In Section 4, we discuss reducing class polynomials modulo primes. In Section 5 we show how to compute H_i^Φ modulo a prime p and we prove Theorem 1.1. Section 6 discusses the endomorphism ring computation, and in Section 7 we give some examples.

2. Results from complex multiplication

Definition 2.1 (CM-type)**.** *Let K be a CM-field of degree $2g$ and let Ω be an algebraically closed field of characteristic 0. Denote by $\mathrm{Hom}(K, \Omega) = \{\phi_1, \phi_2, ..., \phi_{2g}\}$ the set of embeddings of K into Ω. Furthermore, let ρ denote the automorphism inducing complex conjugation on K. Then any subset of these embeddings Φ satisfying the disjoint union $\Phi \sqcup \rho \circ \Phi = \mathrm{Hom}(K, \Omega)$ is called a CM-type on K.*

2.1. Injectivity of the reduction map.

Definition 2.2. *Let A be an abelian variety over a field k with complex multiplication by the maximal order $\mathcal{O}_K$ in a CM-field K, and let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. A surjective homomorphism $\lambda_\mathfrak{a} : A \to A^\mathfrak{a}$, to an abelian variety $A^\mathfrak{a}$, is an $\mathfrak{a}$-multiplication if every homomorphism $a : A \to A$ with $a \in \mathfrak{a}$ factors through $\lambda_\mathfrak{a}$, and $\lambda_\mathfrak{a}$ is universal for this property, in the sense that, for every surjective homomorphism $\lambda' : A \to A'$ with the same property; there is a homomorphism $\alpha : A' \to A^\mathfrak{a}$, necessarily unique, such that $\alpha \circ \lambda' = \lambda_\mathfrak{a}$.*

For abelian varieties A and B defined over a number field and with good reduction modulo a prime $\mathfrak{P}$, the next proposition gives a condition under which A and B will be isomorphic provided that their reductions modulo $\mathfrak{P}$ are isomorphic. The fact that the conditions below are sufficient for an isomorphism to lift was given for dimension 2 in [11, Theorem 2]. Here we give a general proof of this fact.

Proposition 2.3. *Let (A, ι), (B, ι') be simple, abelian varieties of type (K, Φ) defined over a number field k. Furthermore, assume that $\mathfrak{P}$ is a prime of k such that A and B have good reduction modulo $\mathfrak{P}$ and denote by $\tilde{A}$ and $\tilde{B}$ their reductions*

modulo $\mathfrak{P}$ respectively. If $\tilde{A}$ and $\tilde{B}$ are simple with endomorphism ring isomorphic to $\mathcal{O}_K$ and $\gamma : \tilde{A} \to \tilde{B}$ is an isomorphism over $\overline{\mathbb{F}}_p$, then A and B are isomorphic over $\overline{k}$.

Proof. As $(A, \iota), (B, \iota')$ have the same type then, by [30, Chapter II, Proposition 16], they are isogenous via an $\mathfrak{a}$-multiplication, which we denote by $\lambda_\mathfrak{a}$. After possibly taking a field extension and picking a prime above $\mathfrak{P}$, we can assume that $\lambda_\mathfrak{a}$ and all endomorphisms are defined over k. The reduction $\tilde{\lambda_\mathfrak{a}}$ is also an $\mathfrak{a}$-multiplication [28, Proposition 7.30]. Define an embedding $\tilde{\iota} : \mathcal{O}_K \to \mathrm{End}(\tilde{A})$ by $\tilde{\iota}(a) = \widetilde{\iota(a)}$. This map is an isomorphism. Let $a \in \mathcal{O}_K$ be such that $\tilde{\iota}(a) = \gamma^{-1} \circ \tilde{\lambda_\mathfrak{a}} \in \mathrm{End}(\tilde{A})$. As $\tilde{\iota}(a)$ factors through $\tilde{\lambda_\mathfrak{a}}$, $a \in \mathfrak{a}$ by [28, Corollary 7.24]. Also, $\iota(a)$ must factor through the $\mathfrak{a}$-multiplication, $\lambda_\mathfrak{a}$, that is, $\iota(a) = \gamma_1 \circ \lambda_\mathfrak{a}$ for γ_1 some isogeny from B to A.

Reducing modulo $\mathfrak{P}$, $\tilde{\iota}(a) = \tilde{\gamma_1} \circ \tilde{\lambda_\mathfrak{a}}$. As $\lambda_\mathfrak{a}$ is surjective, this implies $\gamma^{-1} = \tilde{\gamma_1}$. Similarly, we can find a γ_2 such that $\tilde{\gamma_2} = \gamma$. Then $\tilde{\gamma_1} \circ \tilde{\gamma_2} = \gamma^{-1} \circ \gamma = id$. As the reduction map is injective, $\gamma_1 \circ \gamma_2 = id$ and $\gamma_2 \circ \gamma_1 = id$, thus A and B are isomorphic. □

2.2. **The congruence relation.** Let $(A, \iota)/\mathbb{C}$ be of type (K, Φ) with $\mathrm{End}(A) \cong \mathcal{O}_K$. Denote by (K^*, Φ^*) the reflex of (K, Φ). Let k be a field of definition for (A, ι). As the Hilbert class field H of K^* is a field of definition for (A, ι) (see [15, Proposition 2.1]), we may assume that $k \subseteq H$. Take L to be a Galois extension of $\mathbb{Q}$ containing the field of definition k and the field K. Recall k contains K^* by [24, Chapter III, Theorem 1.1]. Let $\mathfrak{P}$ be a prime of k at which A has good reduction. Let $\mathfrak{P}_{K^*}$ be the prime of K^* below $\mathfrak{P}$. Pick a prime $\mathfrak{P}_L$ of L above $\mathfrak{P}$ and write Φ_L^{-1} for the set of elements ψ of $\mathrm{Gal}(L/\mathbb{Q})$ such that $(\psi^{-1})_{|K} \in \Phi$.

Let $\pi \in \mathcal{O}_K$ be such that $\tilde{\iota}(\pi)$ is the $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{P})$-th power Frobenius on the reduction $\tilde{A}$. In Section 5 we will use the following proposition, which is an easy consequence of the Shimura-Taniyama congruence relation, to obtain a bijection between abelian varieties with CM by $\mathcal{O}_K$ of type Φ and abelian varieties over a finite field satisfying certain properties.

Proposition 2.4. *Assume that p splits completely in K and splits completely into principal ideals in K^*. Also, let M be the Galois closure of the compositum of K and K^* and let $\mathfrak{P}_M$ be a prime above $\mathfrak{P}_{K^*}$. Write Φ_M^{-1} for the set of elements γ of $\mathrm{Gal}(M/\mathbb{Q})$ such that $(\gamma^{-1})_{|K} \in \Phi$. Then $\pi\mathcal{O}_M = \prod_{\gamma \in \Phi_M^{-1}} (\mathfrak{P}_M)^\gamma$.*

Proof. As p splits completely into principal ideals in K^*, p splits completely in the Hilbert class field H of K^*. Thus, as mentioned above, p splits completely in the field of definition k. Therefore, $f(\mathfrak{P}_L/\mathfrak{P}) = 1$, and by [24, Chapter 3, Thm 3.3] we obtain

$$\pi\mathcal{O}_L = \prod_{\psi \in \Phi_L^{-1}} \mathfrak{P}_L^\psi \mathcal{O}_L.$$

Using the splitting conditions on p and intersecting with $\mathcal{O}_M$ on both sides, we get the desired result. □

Thus the CM-type determines the ideal generated by Frobenius. We will also need a version of this statement over $\mathbb{Q}_p$. Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Let

$$H_w = \{\phi \in \mathrm{Hom}(K, \overline{\mathbb{Q}}_p) : \ \phi \text{ factors through } K \to K_w\},$$

where K_w is the completion of K at the place w.

4 Jun 2018 06:44:41 PDT
Version 3 - Submitted to Open Book Series

Proposition 2.5. *Let (A, ι) be an abelian variety with CM by the full ring of integers $\mathcal{O}_K$ and of CM-type Γ. Moreover, assume (A, ι) has a model over the p-adic integers $\mathbb{Z}_p$. If p splits completely in K, $\Gamma = \{\phi : \phi \in H_v, \text{ where } v \mid \pi\mathcal{O}_K\}$.*

Proof. By [34, Lemme 5], $\dfrac{v(\pi)}{v(q)} = \dfrac{Card(\Gamma \cap H_v)}{[K_v : \mathbb{Q}_p]}$. If p splits completely in K, then $[K_v : \mathbb{Q}_p] = 1$ for all $v \mid p$ and $q = p$. This gives $v(\pi) = Card(\Gamma \cap H_v)$.

Also, as p splits completely in K, there is only one embedding $K \to K_v$ for every $v \mid p$. Thus $Card(H_v) = 0$ or 1, and $Card(\Gamma \cap H_v) = 1$ if and only if $v(\pi) = 1$. □

3. Invariants of Picard curves

In this section, we discuss invariants for Picard curves. Recall, if $y^3 = f(x)$ where $\deg(f) = 4$ and f has no repeated roots over the algebraic closure, then this defines a smooth curve known as a *Picard curve*. Assume L is a field of characteristic not 2 or 3, and let C be a Picard curve over L. We can express the curve C in the form $y^3 = x^4 + g_2x^2 + g_3x + g_4$. This is called the *normal form* of the curve [18, Appendix 1, Definition 7.6].

As in [22, Section 1], we define the following three invariants for a Picard curve in normal form as $j_1 := g_2^3/g_3^2, j_2 := g_2g_4/g_3^2, j_3 := g_4^3/g_3^4$.

We can write down a model for the curve with given invariants as follows:

Case 1: If $j_1 \neq 0$, then $C : y^3 = x^4 + j_1x^2 + j_1x + j_1j_2$.

Case 2: If $j_1 = 0, j_3 \neq 0$, then $C : y^3 = x^4 + j_3^2x + j_3^3$.

Case 3: If $j_1 = 0, j_2 = 0, j_3 = 0$, then $C : y^3 = x^4 + x$.

If $g_3 = 0$, then C is a double cover of an elliptic curve (see [22, Lemma 2.1] and [22, Theorem 2.4]). Thus the invariants for a Picard curve C whose Jacobian is simple are always defined. This gives us the following proposition.

Proposition 3.1. *Let C be a Picard curve over a field L of characteristic not 2 or 3 with $\mathrm{Jac}(C)$ simple. Assume that the three invariants $j_i(C)$ are defined over a subfield k of L. Then C has a model as a Picard curve over k.*

Goren and Lauter showed that for genus 2 curves which have CM by a given primitive, quartic, CM-field K one can bound the primes occurring in the denominators of the Igusa class polynomials in terms of a value depending on K [16]. They obtain this bound by relating the primes occurring in the denominators to primes of bad reduction of the curves. For genus 3 curves with CM by a sextic CM-field K, a bound on the primes of bad reduction in terms of a value depending on K was obtained in [8] and [21]. A bound on the primes occurring in the denominators of the above invariants of Picard curves was obtained in [22].

We will need the following condition for Picard curves.

Proposition 3.2. *Let $K = \mathbb{Q}(\mu)$ be a sextic CM-field, Φ a primitive CM-type on K and p be a rational prime that splits completely in K. Let C be a genus 3 curve defined over a number field M with CM by the maximal order $\mathcal{O}_K$ of K and with type Φ. Let $\mathfrak{P}$ be a prime of M above p. Then C has potential good reduction at $\mathfrak{P}$. Moreover, if C is a Picard curve then $v_{\mathfrak{P}}(j_i(C)) \geq 0$ for all invariants j_i.*

Proof. Assume C has geometrically bad reduction modulo a prime $\mathfrak{P}$ of M above the rational prime p. After possibly extending M, we may assume that C has a stable model over M and $\mathrm{Jac}(C)$ has good reduction over M. The stable reduction

$\tilde{C}$ has at least 2 irreducible components [8, Proposition 4.2]. $\widetilde{\mathrm{Jac}(C)}$ is isomorphic as a polarized abelian variety to the product of the Jacobians of the irreducible components of $\tilde{C}$. That is, $\widetilde{\mathrm{Jac}(C)}$ is isomorphic as a principally polarized abelian variety to $E \times A$ [8, Corollary 4.3], where E is an elliptic curve and A is a two-dimensional principally polarized abelian variety. However, as p splits completely in K, the reduction modulo $\mathfrak{P}$ of $\mathrm{Jac}(C)$ must be simple with CM by K by [30, Chapter 3, Theorem 2]. By [32, Theorem 1.2]s $\widetilde{\mathrm{Jac}(C)}$ is ordinary, so $\mathrm{End}(\widetilde{\mathrm{Jac}(C)}) \otimes \mathbb{Q}$ is unchanged after base extension by [35, Theorem 7.2]. Therefore $\widetilde{\mathrm{Jac}(C)}$ is geometrically simple as the endomorphism ring tensored with $\mathbb{Q}$ is a field. This is a contradiction, so C must have potential good reduction.

Now assume that C is a Picard curve and that $v_{\mathfrak{P}}(j_i(C)) < 0$ for some j_i. After possibly extending M, we may assume that $\mathrm{Jac}(C)$ has good reduction modulo $\mathfrak{P}$. Then the reduction of $\mathrm{Jac}(C)$ modulo $\mathfrak{P}$ has two non-trivial abelian subvarieties by [22, Lemma 2.1]. However, as p splits completely in K, we again obtain a contradiction. □

Remark 3.3. It was pointed out to the authors by some of the anonymous referees and by Marco Streng that a similar condition to the above proposition was given in [20, Proposition 4.1] when the field $K/\mathbb{Q}$ is cyclic Galois.

Remark 3.4. To generate representatives for all distinct isomorphism classes, we use the invariants described in [23, Section 4]. To see that this enumerates all isomorphism classes of Picard curves with no repetitions see [18, Appendix 1, Section 7.5].

4. Reduction of class polynomials

Fix a sextic CM-field K containing the cube roots of unity and a primitive CM-type Φ on K. In the introduction we defined class polynomials H_i^{Φ} for $i = 1, ..., 3$,

$$H_i^{\Phi} := \prod (X - j_i(C)),$$

where the product runs over all isomorphism classes of Picard curves defined over $\mathbb{C}$ whose Jacobian has complex multiplication by $\mathcal{O}_K$ and of type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Remark 4.1. If one wants to use the class polynomials above to construct Picard curves over $\mathbb{C}$ with $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$, then one needs to match up the roots of the three polynomials to obtain a triple of roots (j_1, j_2, j_3) that corresponds to such a curve. In genus 2, alternate class polynomials were proposed based on Lagrange interpolation that prescribe which roots of the second and third Igusa class polynomials to choose once the first has been chosen [14, Section 3]. These polynomials only work if the first Igusa class polynomial has simple roots. For a discussion of resolving this issue in genus 2 see [31, Chapter III, Section 5].

We will show that under suitable restrictions on the prime p, the reduction modulo p of these polynomials H_i^{Φ} is

$$H_{i,p} := \prod (X - j_i(C)),$$

where the product runs over all $\overline{\mathbb{F}}_p$-isomorphism classes of Picard curves C which arise as the reduction of Picard curves over $\mathbb{C}$ that have complex multiplication by $\mathcal{O}_K$ and type $\sigma\Phi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

First we describe when a principally polarized abelian variety is the Jacobian of a Picard curve.

In the following, whenever we assume that a field F contains the cube roots of unity, it is also implied that F does not have characteristic 3.

Lemma 4.2. *Let $(A, \mathcal{C})$ be a simple, principally polarized abelian variety of dimension 3 over a perfect field H which contains the cube roots of unity. In addition, assume $(A, \mathcal{C})$ has complex multiplication by K with $\mathbb{Q}(\zeta_3) \subset K$. Then $(A, \mathcal{C})$ is geometrically the Jacobian of a Picard curve C which has a model over H.*

Proof. By [23, Lemma 1], $(A, \mathcal{C})$ is the Jacobian of a Picard curve C after we base change to a finite extension L of H. After possibly another finite extension, we may assume L is Galois over H. Let $\sigma \in \mathrm{Gal}(L/H)$, then $\mathrm{Jac}(C^\sigma) \cong_L \mathrm{Jac}(C)^\sigma$. As $\mathrm{Jac}(C)$ has a model over H, $\mathrm{Jac}(C^\sigma) \cong_L \mathrm{Jac}(C)$.

Hence by Torelli's theorem, $C \cong_L C^\sigma$. So $j_i(C) = j_i(C^\sigma) = j_i(C)^\sigma$, $i = 1, ..., 3$. Therefore the invariants $j_i(C)$ are defined over H. As the invariants $j_i(C)$ are defined over H, Proposition 3.1 implies that C has a model over H. □

Before we discuss reductions of our class polynomials, we need the following.

Proposition 4.3. *$H_1^\Phi, H_2^\Phi, H_3^\Phi$ are polynomials defined over $\mathbb{Q}$.*

Proof. Every abelian variety with CM by K has a model over a number field. Thus, by [29, Theorem 4], the curve C is also defined over a number field. So if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is an automorphism, then the tuple of invariants $j_i(C)^\sigma$ corresponds to the curve C^σ. But if $\mathrm{Jac}(C)$ has CM-type (K, Φ) under some embedding $\iota : K \hookrightarrow \mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q}$, then $\mathrm{Jac}(C^\sigma)$ has CM-type $(K, \sigma\Phi)$ by [24, Chapter 3, Theorem 1.2]. The number of roots of the H_i^Φ is finite as there are only finitely many principally polarized abelian varieties with endomorphism ring isomorphic to $\mathcal{O}_K$ of type $\sigma\Phi$ [24, Chapter 3, Corollary 2.7], so the H_i^Φ are polynomials defined over $\mathbb{Q}$. □

We will use the abbreviation p.p.a.v. for a principally polarized abelian variety. For a CM-field K of degree $2g$ over $\mathbb{Q}$, let

$$\mathrm{CM}_{K,\Phi} = \{\mathbb{C}\text{-isomorphism classes of simple p.p.a.v. with CM by } \mathcal{O}_K \text{ of type } \Phi\}.$$

The abelian varieties in this set are of dimension g. By [15, Proposition 2.1], every p.p.a.v. $(A, \mathcal{C})$ representing an isomorphism class in $\mathrm{CM}_{K,\Phi}$ has a model over the Hilbert class field H of the reflex field K^* which has good reduction modulo any prime $\mathfrak{P}$ of H. By [28, Chapter II, Proposition 6.7], the reduction of the polarization $\mathcal{C}$ is a polarization on the reduced variety $\tilde{A}$. If p splits completely into principal ideals in K^* then p splits completely into principal ideals in H. Thus, the reduction $(A_\mathfrak{P}, \mathcal{C}_\mathfrak{P})$ of $(A, \mathcal{C})$ modulo $\mathfrak{P}$ has a model over $\mathbb{F}_p$. Denote by $\widetilde{\mathrm{CM}}_{K,\Phi}$ the set of $\overline{\mathbb{F}}_p$-isomorphism classes occurring in this way. That is,

$$\widetilde{\mathrm{CM}}_{K,\Phi} = \{\overline{\mathbb{F}}_p\text{-isomorphism classes of p.p.a.v.'s } (A_\mathfrak{P}, \mathcal{C}_\mathfrak{P})/\mathbb{F}_p \mid (A, \mathcal{C}) \in \mathrm{CM}_{K,\Phi}\}.$$

Proposition 4.4. *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If $\Phi\gamma = \sigma\Phi$ for some $\gamma \in Aut(K/\mathbb{Q})$, then $CM_{K,\Phi}$ and $CM_{K,\sigma\Phi}$ are equal. Otherwise, $CM_{K,\Phi}$ and $CM_{K,\sigma\Phi}$ are disjoint.*

Proof. For the first statement see [31, Pg 22]. The second statement follows from [31, Chapter I, Lemma 5.6]. □

For a sextic CM-field K containing the cube roots of unity, define:

$$\mathcal{C}^{\Phi} := \{\text{Picard curves } C \text{ over } \mathbb{C} \mid \mathrm{Jac}(C) \in \mathrm{CM}_{K,\Phi}\}/\text{isomorphism over } \mathbb{C},$$

and

$$\widetilde{\mathcal{C}^{\Phi}} := \{\text{Picard curves } C \text{ over } \mathbb{F}_p \mid \mathrm{Jac}(C) \in \widetilde{\mathrm{CM}}_{K,\Phi}\}/\text{isomorphism over } \overline{\mathbb{F}}_p.$$

Let $p > 3$ be a rational prime that splits completely in K and splits completely into principal ideals in K^*.

Proposition 4.5. *The reduction of the polynomials H_i^{Φ} modulo a prime satisfying the above conditions gives $H_i^{\Phi} \mod p \equiv \prod(X - j_i(C))$, where the product is over all C such that C is in $\widetilde{\mathcal{C}^{\sigma\Phi}}$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

Proof. As p splits completely into principal ideals in K^*, the reflex field for (K, Φ), it splits completely in H. Let $\mathfrak{P}$ be a prime of H above p. By [15, Proposition 2.1], $\mathrm{Jac}(C)$ is defined over H for any curve C in $\mathcal{C}^{\Phi}$. Then C itself also has a model over H by Proposition 4.2. C has potential good reduction by Proposition 3.2, so let L be a finite extension over which C obtains good reduction. Furthermore, let $\mathfrak{P}_L$ be a prime above $\mathfrak{P}$. Thus, the reduction $C_{\mathfrak{P}_L}$ of C modulo $\mathfrak{P}_L$ will be defined over possibly a finite extension of $\mathbb{F}_p$. However, as the invariants of C belong to H, the invariants of $C_{\mathfrak{P}_L}$ belong to $\mathbb{F}_p$ so $C_{\mathfrak{P}_L}$ has a model over $\mathbb{F}_p$. Thus, we get a map from $\mathcal{C}^{\Phi}$ to $\widetilde{\mathcal{C}^{\Phi}}$. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let K_σ^* be the reflex field for the type $(K, \sigma\Phi)$. One can check that the reflex fields K^* and K_σ^* are isomorphic over $\mathbb{Q}$. Therefore, p splits completely into principal ideals in the reflex field of K_σ^*, so we also get a map from $\mathcal{C}^{\sigma\Phi}$ to $\widetilde{\mathcal{C}^{\sigma\Phi}}$ induced by reduction modulo $\mathfrak{P}_L$. It remains to show that the reduction map induces a bijection. Taking Jacobians of elements in $\mathcal{C}^{\Phi}$ and $\widetilde{\mathcal{C}^{\Phi}}$ gives bijective maps into $\mathrm{CM}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\Phi}$ respectively.

The map $\mathrm{CM}_{K,\Phi}$ to $\widetilde{\mathrm{CM}}_{K,\Phi}$ induced by reduction modulo $\mathfrak{P}$ is injective by Proposition 5.2. By definition, the map from $\mathrm{CM}_{K,\Phi}$ to $\widetilde{\mathrm{CM}}_{K,\Phi}$ is surjective, so it follows that $\mathcal{C}^{\Phi}$ is in bijection with the set $\widetilde{\mathcal{C}^{\Phi}}$ under the reduction map. The sets $\mathrm{CM}_{K,\Phi}$ and $\mathrm{CM}_{K,\sigma\Phi}$ are either equal or distinct by Proposition 4.4. The elements in $\widetilde{\mathrm{CM}}_{K,\Phi}$ are simple with CM by $\mathcal{O}_K$ by Proposition 5.1. Thus, the sets $\widetilde{\mathrm{CM}}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\sigma\Phi}$ are equal if and only if $\mathrm{CM}_{K,\Phi}$ and $\mathrm{CM}_{K,\sigma\Phi}$ are equal by Proposition 2.3. Therefore, bijectivity of the map from $\mathcal{C}^{\Phi}$ to $\widetilde{\mathcal{C}^{\Phi}}$ suffices to prove the proposition. □

5. Computing H_i^{Φ} modulo p

Let (K, Φ) be a primitive CM-type. Denote by (K^*, Φ^*) the reflex of (K, Φ). Let H be the Hilbert class field of K^* and M the normal closure of the compositum of K and K^*. Let L be the Galois closure of the compositum of H and M over $\mathbb{Q}$. Take p to be a rational prime which splits completely into principal ideals in K^* and splits completely in K. Denote by $\mathfrak{P}$ a prime of H above p, $\mathfrak{P}_L$ a prime of L above $\mathfrak{P}$ and $\mathfrak{P}_M$ a prime of M below $\mathfrak{P}_L$. Denote by Φ_M^{-1} the set of elements ψ_i of $\mathrm{Gal}(M/\mathbb{Q})$ such that $(\psi_i^{-1})_{|K} \in \Phi$.

5.1. **An equivalent definition of $\widetilde{\mathrm{CM}}_{K,\Phi}$.** In this subsection, we give an equivalent definition of $\widetilde{\mathrm{CM}}_{K,\Phi}$ in terms of a condition on the Frobenius of the abelian varieties in $\widetilde{\mathrm{CM}}_{K,\Phi}$. This new definition is more suitable for computations. In

particular, we will use it in computing the set $\widetilde{\mathcal{C}^{\Phi}}$ which occurs in the description of the class polynomials H_i^{Φ} modulo p in Theorem 4.5. For a CM-field K with $[K:\mathbb{Q}] = 2g$, recall the definitions of $\mathrm{CM}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\Phi}$ from Section 4.

We will now define a set $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ which we will show is equal to the set $\widetilde{\mathrm{CM}}_{K,\Phi}$. The main tool that allows us to give this equivalent description will be the Shimura-Taniyama Congruence relation, specifically the statement in Proposition 2.4, which relates the CM-type of an abelian variety defined over a number field with CM to the ideal generated by Frobenius of the reduction of the abelian variety modulo $\mathfrak{P}$. In genus 2, this idea was used in [26] to describe the set we refer to as $\widetilde{\mathrm{CM}}_{K,\Phi}$.

With notation as above, denote by $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ the set of all $\overline{\mathbb{F}}_p$-isomorphism classes of ordinary, simple, principally polarized abelian varieties $(A, \mathcal{C})$ of dimension g defined over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ satisfying the following condition: For $(A, \mathcal{C})$ a representative of an $\overline{\mathbb{F}}_p$ class as above, there exists an embedding ι of $K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ such that, under this embedding, the element π for which $\iota(\pi)$ is the Frobenius endomorphism on A satisfies

$$\pi\mathcal{O}_M = \prod_{\phi \in \Phi_M^{-1}} \mathfrak{P}_M^{\phi}. \tag{5.1}$$

Recall, in the beginning of the section, we fixed a prime $\mathfrak{P}_L$ of L above the prime $\mathfrak{P}$ of H and define $\mathfrak{P}_M = \mathfrak{P}_L \cap M$. One can easily check that $\widetilde{\mathrm{CM}}_{K,\Phi}$ does not depend on the choice of $\mathfrak{P}_L$ above $\mathfrak{P}$. We now wish to show that the sets $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ and $\widetilde{\mathrm{CM}}_{K,\Phi}$ are equal. First we show

Proposition 5.1. *Every element in $\widetilde{CM}_{K,\Phi}$ is ordinary, geometrically simple with endomorphism ring isomorphic to $\mathcal{O}_K$.*

Proof. Let $(A, \mathcal{C})$ be a representative of a class in $\mathrm{CM}_{K,\Phi}$ such that it has good reduction modulo $\mathfrak{P}$ as above. Let $A_{\mathfrak{P}}$ be the reduction of A modulo $\mathfrak{P}$. The reduction map gives an inclusion $\mathrm{End}(A) \hookrightarrow \mathrm{End}(A_{\mathfrak{P}})$ [24, Theorem 3.2], thus, $\mathcal{O}_K$ embeds into $\mathrm{End}(A_{\mathfrak{P}})$. By [30, Chapter 3, Theorem 2], the abelian variety $A_{\mathfrak{P}}$ is simple and $\mathrm{End}(A_{\mathfrak{P}}) = \mathcal{O}_K$. Also, $A_{\mathfrak{P}}$ is ordinary by [32, Theorem 1.2]. Thus, $\mathrm{End}(A_{\mathfrak{P}}) \otimes \mathbb{Q}$ is unchanged after base extension by [35, Theorem 7.2]. Hence $A_{\mathfrak{P}}$ is geometrically simple as the endomorphism ring tensored with $\mathbb{Q}$ is a field. □

The following two results are a generalization to arbitrary dimension of the dimension 2 case treated in [11, Theorem 2].

Proposition 5.2. *The reduction map $CM_{K,\Phi} \to \widetilde{CM}_{K,\Phi}$ is injective.*

Proof. Every element in $\widetilde{\mathrm{CM}}_{K,\Phi}$ is simple with CM by $\mathcal{O}_K$ by Proposition 5.1. Thus, the proposition follows from applying Proposition 2.3. □

Theorem 5.3. *With notation as above, the set $\widetilde{CM}_{K,\Phi}$ is equal to the set $CM^{Fr}_{K,\Phi}$.*

Proof. We first show that $\widetilde{\mathrm{CM}}_{K,\Phi} \subset \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. Let $(A, \mathcal{C})$ be a representative of a class in $\widetilde{\mathrm{CM}}_{K,\Phi}$. By Proposition 5.1, A is ordinary and geometrically simple with $\mathrm{End}(A) \cong \mathcal{O}_K$. As we remarked above, p splits completely into principal ideals in K^*, so the Frobenius of A satisfies Equation 5.1 by Proposition 2.4. Hence $\tilde{A} \in \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. This shows $\widetilde{\mathrm{CM}}_{K,\Phi} \subset \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. It remains to show the reverse inclusion.

To do this, we will show that the two sets have the same cardinality. Both sets are finite as there are only finitely many isomorphism classes of principally polarized abelian varieties defined over $\mathbb{F}_p$. We know from the previous proposition that $\mathrm{CM}_{K,\Phi} \to \widetilde{\mathrm{CM}}_{K,\Phi}$ is an injection. Thus, we have the inequality of cardinalities: $|\mathrm{CM}_{K,\Phi}| \leq |\widetilde{\mathrm{CM}}_{K,\Phi}| \leq |\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}|$.

It suffices to show $|\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}| \leq |\mathrm{CM}_{K,\Phi}|$. Therefore, we will show that there is an injective map from $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ into $\mathrm{CM}_{K,\Phi}$. We define the map as follows: Let $(A_0, \mathcal{C}_0)$ be an abelian variety representing a class in $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$. Since A_0 is ordinary, we can consider its Serre-Tate canonical lift [27, Pgs 172-173, Theorem 3.3] to $\mathbb{Z}_p$ which we will call $(A, \mathcal{C})$.

As $(A_0, \mathcal{C}_0) \in \mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ we have $\pi\mathcal{O}_M = \prod_{\phi_\alpha \in \Phi_M^{-1}} (\mathfrak{P}_M)^{\phi_\alpha}$. Let $\{\psi_w\}$ be the set of all embeddings of M into $\overline{\mathbb{Q}}_p$ induced by completion at a prime $\mathfrak{P}_w$ for $\mathfrak{P}_w \mid \pi\mathcal{O}_M$. By Proposition 2.5, the embeddings induced by completion at primes occurring in the decomposition of the ideal generated by π give the CM-type of A. Under some embedding $\rho : \mathbb{Q}_p \hookrightarrow \mathbb{C}$, we can verify that $\rho(A)$ has type $(K, \sigma\Phi)$ for some $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$. By [37, Theorem 7], modifying ρ by an automorphism of $\mathbb{C}$, we can arrange that $\rho(A)$ has CM-type (K, Φ). As the choice of ρ does not depend on A, this gives us the injection from $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ to $\mathrm{CM}_{K,\Phi}$. Hence $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi} = \widetilde{\mathrm{CM}}_{K,\Phi}$. □

5.2. **Correctness proof for the main algorithm.** We must now show that the Chinese Remainder Theorem may be used to reconstruct the class polynomials from sufficiently many of the $H_{i,p}$. This is accomplished by the following whose proof is identical to that of [11, Theorem 3]:

Theorem 5.4. *Let M be the least common multiple of the denominators of the class polynomials and let N be the maximum absolute value of the coefficients of the class polynomials. Let $B = 2NM$. Then if S is a set of primes satisfying the conditions in Theorem 1.1, we can use the Chinese remainder theorem on the polynomials $\{H_{i,p}\}_{p \in S}$, i from 1 to 3, to reconstruct the polynomials H_i^Φ.*

Remark 5.5. A definition of class polynomials for Picard curves and a bound on the primes occurring in the denominators are given in [21, Theorem 1.3], and the class polynomials we define divide them. In genus 2, bounds on the denominators of the Igusa class polynomials were obtained in [17].

Proof of Theorem 1.1. Using Theorem 4.5, we see that $H_{i,p} := \prod (X - j_i(C))$, where the product runs over representatives for elements in $\widetilde{\mathcal{C}^{\sigma\Phi}}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We can enumerate all $\overline{\mathbb{F}}_p$ isomorphism classes of Picard curves defined over $\mathbb{F}_p$ using the invariants discussed in Remark 3.4. We can check whether a curve is in $\widetilde{\mathcal{C}^\Phi}$ by checking whether $\mathrm{Jac}(C)$ is in $\mathrm{CM}^{\mathrm{Fr}}_{K,\Phi}$ by Theorem 5.3. This involves checking that $\mathrm{Jac}(C)$ has complex multiplication by $\mathcal{O}_K$ which can be accomplished using the algorithm of Section 6. We then perform the CRT step using Theorem 5.4. □

6. Endomorphism ring computation

The algorithm of Theorem 1.1 requires us to check whether certain genus 3 curves C have complex multiplication by a sextic CM-field K. An algorithm for checking whether the Jacobian of an ordinary genus 2 curve (i.e. a curve whose Jacobian is ordinary) has complex multiplication by the full ring of integers of a primitive quartic CM-field K was presented, under certain restrictions on the field K, in [11].

Improvements to this algorithm were presented in [12] and [26]. We generalize these methods to the genus 3 case.

Theorem 6.1. *The following algorithm takes as input a sextic CM-field K and an ordinary genus 3 curve C over a field $\mathbb{F}_p$ where p splits completely in K. The algorithm outputs* **true** *if* $\mathrm{Jac}(C)$ *has endomorphism ring the full ring of integers* $\mathcal{O}_K$ *and* **false** *otherwise:*

(i) Compute a list of all possible characteristic polynomials of Frobenius for ordinary, simple, abelian varieties with complex multiplication by K. Output false if the characteristic polynomial of $\mathrm{Jac}(C)$ *is not in this list.*
(ii) Compute a basis for $\mathcal{O}_K$.
(iii) For each element α of the basis in the previous step, use Proposition 6.2 to determine if it is an endomorphism. If it is not, output false.
(iv) Output true.

The values for Frobenius in Step i) satisfy $\pi\overline{\pi} = p$ with $\pi \in \mathcal{O}_K$, i.e. $N_{K/K^+}(\pi) = p$ where K^+ is the maximal totally real subfield of K. This relative norm equation can be used to find all such values of π. By the Honda-Tate theorem, every such π will arise as the Frobenius of some abelian variety A over $\mathbb{F}_p$. If the characteristic polynomial of π is irreducible, then A is simple and $\mathbb{Q}(\pi) \cong K$. If p does not divide the middle coefficient of the characteristic polynomial of Frobenius, then A is ordinary [19, Definition 3.1]. By [34, Pg 97, Exemple b], the endomorphism ring of A is an order in K.

6.1. **Determining if an element is an endomorphism.** Our approach in this subsection follows closely that of [12, Section 3] and [26, Section 4] for genus 2. We discuss some changes which are required for genus 3. To determine if $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$, we wish to check, for some $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\alpha_1, ..., \alpha_6$, whether each α_i is an endomorphism. As $\mathbb{Z}[\pi]$ is an order in K, for every $\alpha \in \mathcal{O}_K$, we can write

$$\alpha = P_\alpha(\pi)/n := (a_0 + a_1\pi + ... + a_5\pi^5)/n. \tag{6.1}$$

for some integer n. The next proposition lets us check if $\alpha \in \mathcal{O}_K$ is an endomorphism of $\mathrm{Jac}(C)$:

Proposition 6.2. *Let C be an ordinary curve of genus 3 over $\mathbb{F}_p$ with* $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = K$*, and suppose p splits completely in K. Let $\alpha = P_\alpha(\pi)/n \in \mathcal{O}_K$ with $n = \prod \ell_i^{e_i}$. Then α is an endomorphism of* $\mathrm{Jac}(C)$ *if and only if $P_\alpha(\pi)$ is zero on the $\ell_i^{e_i}$-torsion for $\ell_i \neq p$.*

Proof. By [12, Lemma 3.2], it suffices to check that each $P_\alpha(\pi)/\ell_i^{d_i}$ is an endomorphism. If ℓ_i is coprime to p, then by [11, Corollary 9], we can check whether $P_\alpha(\pi)/\ell_i^{d_i}$ is an endomorphism by determining if $P_\alpha(\pi)$ is zero on the $\ell_i^{d_i}$-torsion.

It remains to handle the case where $\ell_i = p$. For a group A, denote the p-primary part of A by A_p. Write $[\mathcal{O}_K : \mathbb{Z}[\pi]] = [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] \cdot [\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]]$. It is not hard to see that $[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]]$ is a power of p (See [12, Corollary 3.6].) As p splits completely in K, one can show, $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, thus $|(\mathcal{O}_K/\mathbb{Z}[\pi])_p| = |(\mathbb{Z}[\pi, \overline{\pi}]/\mathbb{Z}[\pi])_p|$. This follows from an argument similar to [12, Proposition 3.7].

But this implies for any $\beta \in \mathcal{O}_K$, if $p^k\beta \in \mathbb{Z}[\pi]$ then $\beta \in \mathbb{Z}[\pi, \overline{\pi}]$. Thus, any such element is an endomorphism. □

6.2. **Computing the ℓ^d-torsion and arithmetic.** The algorithm of Couveignes [10] shows how to compute the ℓ^d-torsion. Couveignes' method works for a very general class of curves. However, we instead use some algorithms specific to Picard curves. For a Picard curve C/k, where k is a finite field, Couveignes' method requires the ability to choose random points in $\mathrm{Jac}(C)(k)$. This is easy to do if we represent elements of $\mathrm{Jac}(C)(k)$ as formal sums of points on C. However, to do arithmetic on $\mathrm{Jac}(C)(k)$, it is easier to represent elements as ideals in the affine coordinate ring of C. Thus, we need to be able to switch between the two representations. First, we recall the following consequence of the Riemann-Roch theorem:

Proposition 6.3. *For C a Picard curve and P_∞ the point at infinity for the affine model described above, for any degree 0 divisor D there is a unique effective divisor E of minimal degree $0 \leq m \leq 3$ such that $E - mP_\infty$ is equivalent to D.*

Proof. As Picard curves are non-singular with a k-rational point, the proof follows from [13, Theorem 1]. □

We will call such a unique divisor above the reduced representation of D. So to find a random point in $\mathrm{Jac}(C)(k)$, we can just pick at most 3 random points on C.

A reduced divisor D for which all points in the effective part E lie in the same $\mathrm{Gal}(\overline{k}/k)$-orbit will be called an **irreducible** divisor. Every degree 0 divisor can be expressed as a sum of irreducible divisors.

We can also represent points on $\mathrm{Jac}(C)$ as elements of a particular class group. Denote by $R = k[x,y]/\langle y^3 - f(x)\rangle$ the coordinate ring of C. By [13, Proposition 2], R is the integral closure of $k[x]$ in $k(C)$.

Given an irreducible divisor P we can associate to it a prime ideal $\mathfrak{P}$ of R. We can extend this to a map ρ from effective divisors to ideals of R as:

$$\rho\left(\sum n_i P_i\right) := \prod \mathfrak{P}_i^{n_i},$$

with the P_i irreducible divisors and the $\mathfrak{P}_i$ the corresponding primes of R.

Proposition 6.4. *For C a Picard curve over k and R the coordinate ring of C described above, the map ρ induces an isomorphism $\mathrm{Jac}(C)(k) \to \mathrm{Cl}(R)$, where $\mathrm{Cl}(R)$ is the class group of R.*

Proof. This follows from applying [13, Proposition 3]. □

We refer to the image of a reduced divisor under the map ρ as a reduced ideal.

Proposition 6.5. *Given a reduced divisor D, there is an algorithm to find generators $u(x), w(x,y)$ for the ideal $\rho(D)$. Moreover, given an ideal I of R in the form $I = \langle u(x), w(x,y)\rangle$, we can compute $\rho^{-1}(I)$.*

Proof. As a reduced divisor is a sum of irreducible divisors, it suffices to associate to an irreducible divisor Q the corresponding prime ideal. We can associate a prime ideal $\mathfrak{P}$ in R by first considering the polynomial $u = \prod(x - x_i)$, where the product is over all x-coordinates of points in Q. We then take a polynomial $w(x,y)$ such that the set of common roots of u, w is exactly the set of points of Q. If the x_i are all distinct, then we take the polynomial $w = y - v(x)$, where $v(x)$ is the polynomial interpolating the points in Q. If the roots of $u(x)$ are not distinct, then we can construct w in a way similar to the interpolation polynomial. In the case where

there are two distinct x-coordinates x_1, x_2, let y_1 and y_2 be polynomials whose roots are the y-coordinates corresponding to x_1 and x_2, respectively. Then

$$w(x,y) := \frac{x-x_2}{x_1-x_2}y_1(y) + \frac{x-x_1}{x_2-x_1}y_2(y).$$

If there is only a single x-coordinate, then we can write $w(x,y) = \prod(y-y_i)$, where the y_i are the y-coordinates in the Galois orbit. The corresponding prime ideal in R is then the ideal generated by u and w.

We will now show how to explicitly find the inverse of ρ. Let $D = \prod \mathfrak{P}_i^{n_i}$ be the ideal decomposition of D. Write $\mathfrak{P}_i = \langle u(x), w(x,y)\rangle$. We can find the set of common zeroes of $\mathfrak{P}_i$ by finding all roots x_n of $u(x)$ and all roots $y_{n,m}$ of $w(x_n, y)$. Then the divisor $(\mathfrak{P}_i)$ equals $\sum(x_n, y_{n,m})$. Thus we have constructed the inverse of the map ρ on a prime divisor $\mathfrak{P}$. By linearity, we can explicitly find the inverse of any reduced ideal D . □

There are several algorithms which perform arithmetic on $\mathrm{Jac}(C)(k)$ using the representation of points on $\mathrm{Jac}(C)(k)$ as ideals in the class group, for example, [13], [2]. In particular, we will use the algorithm of [2] for the examples we compute. To add two elements P, Q of $\mathrm{Jac}(C)(k)$, one multiplies the corresponding ideals to get an ideal D. One then wishes to get a reduced ideal D', to have a unique representative for the point D. The algorithm of [2] gives a function g such that $D' = D + (g)$. The function g is necessary for the computation of the Weil pairing in the algorithm of Couveignes for computing torsion.

7. Examples

All examples were run on a computer with 4 Intel Xeon quad-core processors and 64 GB of RAM.

Let $K = K^+(\zeta_3)$, where K^+ is obtained by adjoining to $\mathbb{Q}$ a root of $x^3 - x^2 - 2x + 1$. We can verify that K is Galois with Galois group $\mathbb{Z}/6\mathbb{Z}$ and choose a primitive CM-type on K. All types on K are equivalent, so our choice does not matter. We count the expected degree of our class polynomials using [30, Pg 112, Note 3]. This is equivalent to counting the number of elements in the *polarized class group* (see [6]), for which there is a function in the AVIsogenies package [7]. We find that the degree of the class polynomials for K as above is 1. The first four primes satisfying the conditions of Theorem 1.1 are $13, 43, 97, 127$. For $p = 127$, our algorithm took 7 hours and 9 minutes of clock time and found one Picard curve in $\widetilde{\mathcal{C}^\Phi}$, that is, one Picard curve whose Jacobian is in $\mathrm{CM}_{K,\Phi}^{\mathrm{Fr}}$: $y^3 = x^4 + 75x^2 + 37x + 103$.

The Picard curve $\mathbb{C}$ with CM by $\mathcal{O}_K$, for K as above, was computed in [23]. However, the authors could not verify that the curve they produce has CM by $\mathcal{O}_K$. Our output agrees with the result of their paper reduced modulo 127. Furthermore, assuming the curve they compute is correct, we get a bound as in Theorem 5.4 for the denominators and size of coefficients in the class polynomials H_i^Φ. In particular, $N = 2^{12}$ and $M = 7$ work for the values in Theorem 5.4. Using these values, we can run the CRT algorithm of 1.1 to construct the class polynomials H_i^Φ defined over $\mathbb{Q}$. The algorithm took 8 hours, 55 minutes to run. We only need to reduce modulo the 4 primes $13, 43, 97, 127$. Our result agrees with the result of [23, 25]. Thus, our algorithm can compute the class polynomials H_i^Φ given that one can compute the bound in Theorem 5.4. If we compare the algorithms on the small

example we computed above, the algorithm in [25] performs much faster: it was able to compute the class polynomials in seconds. However, since there are no known bounds, yet, on the denominators of the class polynomials, no complexity analysis has been done for our algorithm or the algorithms in [23, 25]. So it is not clear how they would compare asymptotically.

Now let $K = K^+(\zeta_3)$, where K^+ is the field obtained by adjoining to $\mathbb{Q}$ a root of $x^3 + x^2 - 3x - 1$. This field is non-Galois, and the Galois group of the normal closure over $\mathbb{Q}$ is $S_3 \times \mathbb{Z}/2\mathbb{Z}$. We also pick a CM-type Φ on K. We compute that we expect our class polynomials to have degree 3 using the polarized class group. We pick $p = 67$, which satisfies the conditions of Theorem 1.1. Our algorithm ran in 2 hours and 23 minutes, and we got 3 Picard curves over $\mathbb{F}_p$ whose Jacobians lie in $\mathrm{CM}^{\mathrm{Fr}}_{K,\sigma\Phi}$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$y^3 = x^4 + 8x^2 + 64x + 61, \quad y^3 = x^4 + 62x^2 + 25x + 6, \quad y^3 = x^4 + 54x + 54.$$

Acknowledgments

The authors would like to thank Yuri Zarhin for helpful discussions. We thank the anonymous referees for several helpful suggestions. We thank Marco Streng for valuable feedback on an earlier version of this paper and for pointing out additional references.

References

[1] Amod Agashe, Kristin Lauter, and Ramarathnam Venkatesan. Constructing elliptic curves with a known number of points over a prime field. *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, 41:1–17, 2004.

[2] Seigo Arita. An addition algorithm in Jacobian of C_{ab} curves. *Discrete Applied Mathematics*, 130(1):13–31, 2003.

[3] A Oliver L Atkin and François Morain. Elliptic curves and primality proving. *Mathematics of computation*, 61(203):29–68, 1993.

[4] Jennifer S Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016.

[5] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic number theory*, pages 282–295. Springer, 2008.

[6] Gaetan Bisson. Computing endomorphism rings of abelian varieties of dimension two. *Mathematics of Computation*, 84(294):1977–1989, 2015.

[7] Gaetan Bisson, Robert Cosset, and Damien Robert. Avisogenies (abelian varieties and isogenies). *Magma package for explicit isogenies between abelian varieties, http://avisogenies.gforge.inria.fr*, 2010.

[8] Irene Bouw, Jenny Cooley, Kristin Lauter, Elisa Lorenzo García, Michelle Manes, Rachel Newton, and Ekin Ozman. Bad reduction of genus three curves with complex multiplication. In *Women in Numbers Europe*, pages 109–151. Springer, 2015.

[9] Jinhui Chao, Osamu Nakamura, Kohji Sobataka, and Shigeo Tsujii. Construction of secure elliptic cryptosystems using CM tests and liftings. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 95–109. Springer, 1998.

[10] Jean-Marc Couveignes. Linearizing torsion classes in the Picard group of algebraic curves over finite fields. *Journal of Algebra*, 321(8):2085–2118, 2009.

[11] Kirsten Eisenträger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. *Arithmetic, Geometry and Coding Theory (AGCT-10), Séminaires et Congrès 21*, pages 161–176, 2009.

[12] David Freeman and Kristin Lauter. Computing endomorphism rings of Jacobians of genus 2 curves over finite fields. *Algebraic geometry and its applications*, 5:29–66, 2008.

[13] Steven Galbraith, Sachar Paulus, and Nigel Smart. Arithmetic on superelliptic curves. *Mathematics of computation*, 71(237):393–405, 2002.

[14] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The 2-adic cm method for genus 2 curves with application to cryptography. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 114–129. Springer, 2006.
[15] Eyal Z Goren. On certain reduction problems concerning Abelian surfaces. *Manuscripta mathematica*, 94(1):33–44, 1997.
[16] Eyal Z Goren and Kristin E Lauter. Class invariants for quartic CM fields. In *Annales de l'institut Fourier*, volume 57, pages 457–480, 2007.
[17] Eyal Z Goren and Kristin E Lauter. Genus 2 curves with complex multiplication. *International Mathematics Research Notices*, 2012(5):1068–1142, 2012.
[18] Rolf-Peter Holzapfel. *The ball and some Hilbert problems*. Birkhäuser, 1995.
[19] Everett W Howe. Principally polarized ordinary abelian varieties over finite fields. *Transactions of the American Mathematical Society*, 347(7):2361–2401, 1995.
[20] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbf{Q}$ with complex multiplication. *arXiv preprint arXiv:1701.06489*, 2017.
[21] Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Rachel Newton, Ekin Ozman, and Marco Streng. A bound on the primes of bad reduction for CM curves of genus 3. *arXiv preprint arXiv:1609.05826*, 2018.
[22] Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng. Primes dividing invariants of CM Picard curves. *arXiv preprint arXiv:1801.04682*, 2018.
[23] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Mathematics of computation*, 74(249):499–518, 2005.
[24] Serge Lang. *Complex multiplication*, volume 255. Springer-Verlag, New York, 1983.
[25] Joan-C. Lario and Anna Somoza. A note on Picard curves of CM-type. *arXiv preprint arXiv:1611.02582*, 2016.
[26] Kristin Lauter and Damien Robert. Improved CRT algorithm for class polynomials in genus 2. *Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X)*, pages 437–461, 2013.
[27] William Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Lecture Notes in Mathematics, Vol. 264. Springer-Verlag, 1972.
[28] James S Milne. Complex multiplication. *Available at http://www.jmilne.org/math/.*, 2006.
[29] Frans Oort and Kenji Ueno. Principally polarized Abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci Univ. Tokyo Sect. IA Math*, 1973.
[30] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*. Princeton University Press, 1998.
[31] Marco Streng. *Complex multiplication of Abelian surfaces*. Mathematical Institute, Faculty of Science, Leiden University, 2010.
[32] Ken-ichi Sugiyama. On a generalization of Deuring's results. *Finite Fields and Their Applications*, 26:69–85, 2014.
[33] Andrew V Sutherland. Accelerating the CM method. *LMS Journal of Computation and Mathematics*, 15:172–204, 2012.
[34] John Tate. Classes d'isogénie des variétés Abéliennes sur un corps fini (d'après T. Honda). In *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*, pages 95–110. Springer, 1971.
[35] William C Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'cole Normale Suprieure*, 2(4):521–560, 1969.
[36] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *Journal-Ramanujan Mathematical Society*, 16(4):339–372, 2001.
[37] Paul B Yale. Automorphisms of the complex numbers. *Mathematics Magazine*, 39(3):135–141, 1966.

Department of Mathematics, The Pennsylvania State University, University, Park, PA 16802, USA
E-mail address: sza149@psu.edu

Department of Mathematics, The Pennsylvania State University, University, Park, PA 16802, USA
E-mail address: eisentra@math.psu.edu

GENERATING SUBGROUPS OF RAY CLASS GROUPS WITH SMALL PRIME IDEALS

BENJAMIN WESOLOWSKI

Abstract. Explicit bounds are given on the norms of prime ideals generating arbitrary subgroups of ray class groups of number fields, assuming the Extended Riemann Hypothesis. These are the first explicit bounds for this problem, and are significantly better than previously known asymptotic bounds. Applied to the integers, they express that any subgroup of index i of the multiplicative group of integers modulo m is generated by prime numbers smaller than $16(i \log m)^2$, subject to the Riemann Hypothesis. Two particular consequences relate to mathematical cryptology. Applied to cyclotomic fields, they provide explicit bounds on generators of the relative class group, needed in some previous work on the shortest vector problem on ideal lattices. Applied to Jacobians of hyperelliptic curves, they allow one to derive bounds on the degrees of isogenies required to make their horizontal isogeny graphs connected. Such isogeny graphs are used to study the discrete logarithm problem on said Jacobians.

1. Introduction

1.1. **Motivation.** In 1990, Bach [1] computed explicit bounds for the norms of prime ideals generating the class groups of number fields, assuming the Extended Riemann Hypothesis (henceforth, ERH). These bounds made explicit the earlier work of Lagarias, Montgomery and Odlyzko [11], and have proved to be a crucial tool in the design and analysis of many number theoretic algorithms. However, these bounds do not tell anything about the norms of prime ideals generating any particular subgroup of the class group. Indeed, a generating set for the full group might not contain any element of the subgroup.

Let K be a number field of degree n, and let Δ be the absolute value of its discriminant. The results of [11] show that the class group $\mathrm{Cl}(K)$ is generated by prime ideals of norm bounded by $O((\log \Delta)^2)$. Now, let H be an arbitrary subgroup of the class group $\mathrm{Cl}(K)$. Some asymptotic bounds on the norm of prime ideals generating H have already been computed in [10] by analysing spectral properties of the underlying Cayley graphs. They are of the form $O((n[\mathrm{Cl}(K) : H] \log \Delta)^{2+\varepsilon})$, for an arbitrary $\varepsilon > 0$. Taking H to be the full class group reveals a clear gap with the bounds of [11]. The explicit bounds provided in the present paper eliminate this gap, as they are asymptotically $O(([\mathrm{Cl}(K) : H] \log \Delta)^2)$.

Situations where proper subgroups of class groups have to be considered already arose in two distinct regions of mathematical cryptology. One is related to lattice-based cryptography. Cryptographic schemes based on ideal lattices are typically instantiated over the ring of integers $\mathcal{O}_K$ of a cyclotomic field K. The field K has a Hermitian vector space structure induced by its Minkowski embedding, and ideals of $\mathcal{O}_K$ are also lattices in this vector space. It was shown in [3, 4, 5] that in principal ideals of $\mathcal{O}_K$, an unusually short vector can be found in quantum polynomial time,

14 Jun 2018 08:13:39 PDT
Version 4 - Submitted to Open Book Series

under some heuristic assumptions (this short vector is actually a generator of the ideal). This led to the break of a multitude of cryptographic schemes using principal ideals (including [4, 8, 14, 20]).

A recent result [6] shows how to extend the algorithm to find short vectors in arbitrary ideals of $\mathcal{O}_K$, by transferring the problem to a principal ideal. Let n be the degree of K, K_0 the maximal real subfield of K, and $\mathrm{Cl}^-(K)$ the relative class group (i.e., the kernel of the norm map $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$). The transferring method of [6] crucially relies on the assumption that $\mathrm{Cl}^-(K)$ is generated by a small number (polynomial in $\log n$) of prime ideals of small norm (polynomial in n) and all their Galois conjugates. On one hand, very little is known about the structure of $\mathrm{Cl}^-(K)$, and it seems difficult to prove that it can always be generated by such a small number of Galois orbits of ideals (yet there is convincing numerical evidence; see [19] for the case where K has prime conductor). On the other hand it can be shown, assuming ERH, that the constraint on the norms can be satisfied, and the present work provides the best asymptotic bounds, and the first explicit ones (see Theorem 1.2 and Remark 2).

The second situation is related to hyperelliptic curves. Let $\mathscr{A}$ be the Jacobian of a hyperelliptic curve over a finite field $\mathbf{F}_q$. Isogeny graphs around $\mathscr{A}$ are a central tool to study the difficulty of the underlying discrete logarithm problem (see for instance [7, 9, 10, 21]). When $\mathscr{A}$ is ordinary and absolutely simple — as required for applications in cryptography — its endomorphism algebra is a complex multiplication field K (with maximal real subfield K_0) and its endomorphism ring is isomorphic to an order $\mathcal{O}$ in K. Any abelian variety isogenous to $\mathscr{A}$ has the same endomorphism algebra, and an isogeny that also preserves the endomorphism ring is called a *horizontal* isogeny. The horizontal isogeny graphs of $\mathscr{A}$ are closely related to Cayley graphs of the kernel $\mathscr{P}(\mathcal{O})$ of the norm map

$$N_{K/K_0} : \mathrm{Cl}(\mathcal{O}) \longrightarrow \mathrm{Cl}^+(\mathcal{O} \cap K_0),$$

where $\mathrm{Cl}^+(\mathcal{O} \cap K_0)$ is the narrow class group of $\mathcal{O} \cap K_0$. More precisely, for any bound $B > 0$, there is a graph isomorphism between

(1) the Cayley graph of $\mathscr{P}(\mathcal{O})$ with generators the ideals of prime norm smaller than B, and
(2) the isogeny graph consisting of all principally polarizable abelian varieties isogenous to $\mathscr{A}$ and with same endomorphism ring, and all isogenies between them of prime degree smaller than B.

When the Jacobian $\mathscr{A}$ is an elliptic curve, the situation is well understood since $K_0 = \mathbf{Q}$, hence $\mathscr{P}(\mathcal{O}) = \mathrm{Cl}(K)$. As a result, Bach's bounds have successfully been used to analyse various algorithms dealing with elliptic curve isogenies. In higher genus however, $\mathscr{P}(\mathcal{O})$ is typically a proper subgroup of the class group, and Bach's bounds are not sufficient to obtain connected isogeny graphs. New explicit bounds guaranteeing the connectedness are provided in Theorem 1.4.

1.2. **Setting.** Throughout this paper, K denotes a number field of degree n, with r_1 embeddings into $\mathbf{R}$ and $2r_2$ embeddings into $\mathbf{C}$. Let $\mathscr{I}(K)$ denote the group of fractional ideals of the ring of integers $\mathcal{O}_K$. A modulus $\mathfrak{m}$ of K is a formal product of a finite part $\mathfrak{m}_0$ (an ideal in $\mathcal{O}_K$), and an infinite part $\mathfrak{m}_\infty$ (a subset of the set of real embeddings of K). Then, $\mathscr{I}_\mathfrak{m}(K)$ denotes the subgroup generated by ideals coprime to $\mathfrak{m}_0$.

The notion of ray class group can now be recalled. Let $P_{K,1}^{\mathfrak{m}}$ be the subgroup of $\mathscr{I}_{\mathfrak{m}}(K)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$ where $\mathrm{ord}_{\mathfrak{p}}(\alpha-1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$ for all primes $\mathfrak{p}$ dividing $\mathfrak{m}_0$, and $\imath(\alpha) > 0$ for all $\imath \in \mathfrak{m}_\infty$. The *ray class group* of K modulo $\mathfrak{m}$ is the quotient

$$\mathrm{Cl}_{\mathfrak{m}}(K) = \mathscr{I}_{\mathfrak{m}}(K)/P_{K,1}^{\mathfrak{m}}.$$

For any ideal $\mathfrak{a}$ such that $(\mathfrak{a}, \mathfrak{m}) = 1$, let $[\mathfrak{a}]_{\mathfrak{m}}$ denote its class in $\mathrm{Cl}_{\mathfrak{m}}(K)$. The *narrow class group* of K is the group $\mathrm{Cl}_{\mathfrak{m}}(K)$ where $\mathfrak{m}$ is the set of all the real embeddings.

Our main tools to study these groups will be ray class characters. We call a *ray class character modulo* $\mathfrak{m}$ what Neukirch [16, Def. VII.6.8] calls a (generalised) Dirichlet character modulo $\mathfrak{m}$, that is a Größencharakter $\chi : \mathscr{I}_{\mathfrak{m}}(K) \to \mathbf{C}^\times$ that factors through the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ via the canonical projection.

1.3. **Main theorem.** Let K be a number field of degree n, and $\mathfrak{m}$ a modulus on K. Consider any subgroup H of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$, and any character χ that is not trivial on that subgroup. The main theorem generalizes [1] by providing explicit bounds on the smallest prime ideal $\mathfrak{p}$ whose class is in H and such that $\chi(\mathfrak{p}) \neq 1$. Note that all statements containing the mention (ERH) assume the Extended Riemann Hypothesis (recalled in Section 2). The following theorem is proved in Section 3.

Theorem 1.1 (ERH)**.** *Let K be any number field, and Δ the absolute value of the discriminant of K. Let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Let H be any subgroup of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$. Let χ be a ray class character modulo $\mathfrak{m}$ that is not trivial on H. Then there is a prime ideal $\mathfrak{p}$ such that $(\mathfrak{p}, \mathfrak{m}_0) = 1$, the class of $\mathfrak{p}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is in the subgroup H, $\chi(\mathfrak{p}) \neq 1$, $\deg(\mathfrak{p}) = 1$ and*

$$N(\mathfrak{p}) \leq \left([\mathrm{Cl}_{\mathfrak{m}}(K) : H]\,(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\right)^2,$$

where $\omega(\mathfrak{m}_0)$ denotes the number of distinct prime ideals dividing $\mathfrak{m}_0$.

Remark 1. When H is the full group and $n \geq 2$, the above bound can be compared to Bach's bound $N(\mathfrak{p}) \leq 18(\log(\Delta^2 N(\mathfrak{m}_0)))^2$ given by [1, Th. 4]. Let us put the expression of Theorem 1.1 in a comparable form. From [1, Lem. 7.1], we have

$$|\mathfrak{m}_\infty| \leq n \leq \frac{\log(\Delta N(\mathfrak{m}_0)) + 3/2}{\log(2\pi) - \psi(2)} \leq 0.71\log(\Delta N(\mathfrak{m}_0)) + 1.07,$$

where ψ is the logarithmic derivative of the gamma function. Moreover, we have the bound $\omega(\mathfrak{m}_0) \leq \log(\Delta N(\mathfrak{m}_0))/\log 2$. The bound of Theorem 1.1 becomes $N(\mathfrak{p}) \leq (5.62\log(\Delta N(\mathfrak{m}_0)) + 5.52)^2$. Whenever $\Delta N(\mathfrak{m}_0) < 12$, the corresponding ray class group is trivial, so we can suppose that $\log(\Delta N(\mathfrak{m}_0)) \geq \log(12) \geq 2.48$. These estimates lead to

$$N(\mathfrak{p}) \leq (5.62 + 5.52/2.48)^2\,(\log(\Delta N(\mathfrak{m}_0)))^2 \leq 62(\log(\Delta N(\mathfrak{m}_0)))^2. \tag{1.1}$$

Even in this form, direct comparison with [1, Lem. 7.1] is not obvious. With the unrefined estimate $\Delta^2 N(\mathfrak{m}_0) \leq (\Delta N(\mathfrak{m}_0))^2$, Bach's bound becomes $N(\mathfrak{p}) \leq 72(\log(\Delta N(\mathfrak{m}_0)))^2$. The constant factor is slightly worse than in the bound (1.1), but this comparison does not do justice to either theorem.

14 Jun 2018 08:13:39 PDT
Version 4 - Submitted to Open Book Series

1.4. **Consequences.** In Section 4, a series of notable consequences is derived from Theorem 1.1. Foremost, it allows us to obtain sets of small prime ideals generating any given subgroup of a ray class group. This is made precise in the following theorem.

Theorem 1.2 (ERH)**.** *Let K be any number field, and Δ the absolute value of the discriminant of K. Let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Let $\mathfrak{h}$ be any ideal in K. Let H be a non-trivial subgroup of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$. Then H is generated by the classes of the prime ideals in*

$$\{\mathfrak{p} \text{ prime ideal in } K \mid (\mathfrak{p}, \mathfrak{h}\mathfrak{m}_0) = 1, [\mathfrak{p}]_\mathfrak{m} \in H, \deg(\mathfrak{p}) = 1 \text{ and } N(\mathfrak{p}) < B\},$$

where $B = \left([\mathrm{Cl}_\mathfrak{m}(K) : H]\,(2.71 \log(\Delta N(\mathfrak{h}\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{h}\mathfrak{m}_0)) + 4.13\right)^2$, and $[\mathfrak{p}]_\mathfrak{m}$ denotes the class of $\mathfrak{p}$ in $\mathrm{Cl}_\mathfrak{m}(K)$.

Remark 2. In particular, Theorem 1.2 implies that the relative class group of a cyclotomic field K of degree n and discriminant Δ is generated by ideals of prime norm smaller than $(2.71 h_{K_0} \log \Delta + 4.13)^2$, where h_{K_0} is the class number of the maximal real subfield of K. This is an important improvement for [6] over the previously known bound $O((h_{K_0} n \log \Delta)^{2+\varepsilon})$ derived from [10].

Applying Theorem 1.1 to Dirichlet characters, one can obtain new results on subgroups of the multiplicative group $(\mathbf{Z}/m\mathbf{Z})^\times$. Let m be a positive integer, and H a non-trivial subgroup of $G = (\mathbf{Z}/m\mathbf{Z})^\times$. It is already known that, assuming GRH, H contains a prime number smaller than $O(([G : H] \log m)^2)$ (see [2, 13]). But these bounds do not provide a generating set for H: they only guarantee the existence of one such prime number. The following theorem gives a set of generators of H, whose norms are also asymptotically $O(([G : H] \log m)^2)$.

Theorem 1.3 (ERH)**.** *Let m be a positive integer, and H a non-trivial subgroup of $G = (\mathbf{Z}/m\mathbf{Z})^\times$. Then H is generated by the set of prime numbers p such that $p \bmod m \in H$ and $p \leq 16\,([G : H] \log m)^2$.*

Finally, we derive bounds on the degrees of cyclic isogenies required to connect all isogenous principally polarizable abelian varieties over a finite field sharing the same endomorphism ring.

Theorem 1.4 (ERH)**.** *Let $\mathscr{A}$ be a principally polarized, absolutely simple, ordinary abelian variety over a finite field $\mathbf{F}_q$, with endomorphism algebra K and endomorphism ring isomorphic to an order $\mathcal{O}$ in K. Let K_0 be the maximal real subfield of K, and $\mathfrak{f}$ the conductor of $\mathcal{O}$. For any $B > 0$, let $\mathscr{G}(B)$ be the isogeny graph whose vertices are the principally polarizable varieties isogenous to $\mathscr{A}$ and with the same endomorphism ring, and whose edges are isogenies connecting them, of prime degree smaller than B. Then, if $\mathcal{O}_0 = \mathcal{O} \cap K_0$ is the ring of integers of K_0, the graph*

$$\mathscr{G}\left(26\left(h^+_{\mathcal{O}_0} \log(\Delta N(\mathfrak{f}))\right)^2\right)$$

is connected, with Δ the absolute value of the discriminant of K, and $h^+_{\mathcal{O}_0}$ the narrow class number of $\mathcal{O}_0$.

Remark 3. In particular, the above holds in dimension 2, where *principally polarized* translates to *Jacobian of a genus 2 hyperelliptic curve* (see [15, Th. 4.1]).

14 Jun 2018 08:13:39 PDT
Version 4 - Submitted to Open Book Series

1.5. **Notation.** An inequality such as $x \leq y$ between complex numbers means that the relation holds between the real parts. The function log denotes the natural logarithm.

2. Ray class characters

This section summarizes the definitions, notations and facts related to ray class characters that will be used throughout the paper.

Recall that a ray class character modulo $\mathfrak{m}$ is a Größencharakter $\chi : \mathscr{I}_{\mathfrak{m}}(K) \to \mathbf{C}^{\times}$ that factors through the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ (via the canonical projection). A character is *principal* if it takes only the value 1. Let $\delta(\chi)$ be 1 if χ is principal and 0 otherwise. A ray class character is *primitive modulo* $\mathfrak{m}$ if it does not factor through $\mathrm{Cl}_{\mathfrak{m}'}(K)$ for any modulus $\mathfrak{m}'$ smaller[1] than $\mathfrak{m}$. The conductor $\mathfrak{f}_\chi$ of χ is the smallest modulus $\mathfrak{f}$ such that χ is the restriction of a ray class character modulo $\mathfrak{f}$. Let $\beta_\chi = |\mathfrak{f}_\infty|$ be the number of infinite places in the conductor $\mathfrak{f}$. From [16, Prop. 6.9], any ray class character χ is the restriction of a primitive ray class character of modulus $\mathfrak{f}_\chi$, which is also primitive as a Größencharakter.

The Hecke L-function associated to a character χ modulo $\mathfrak{m}$ is defined as

$$L_\chi(s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

for $\mathfrak{Re}(s) > 1$, where the sum is taken over all ideals of $\mathcal{O}_K$. Note that χ is implicitly extended to all ideals by defining $\chi(\mathfrak{a}) = 0$ whenever $(\mathfrak{a}, \mathfrak{m}_0) \neq 1$. When χ is the trivial character on $\mathscr{I}(K)$, we obtain the Dedekind zeta function of K, $\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$. These L-functions are extended meromorphically on the complex plane with at most a simple pole at $s = 1$, which occurs if and only if χ is principal. Let R_χ be the set of zeros of L_χ on the critical strip $0 < \mathfrak{Re}(s) < 1$. The ERH implies that all Hecke L-functions are zero-free in the half-plane $\mathfrak{Re}(s) > 1/2$.

We will make an extensive use of the logarithmic derivatives L'_χ/L_χ. When $\mathfrak{Re}(s) > 1$, they admit the absolutely convergent representation

$$\frac{L'_\chi}{L_\chi}(s) = -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\chi(\mathfrak{a})}{N(\mathfrak{a})^s}, \tag{2.1}$$

where Λ is the von Mangoldt function (i.e., $\Lambda(\mathfrak{a}) = \log N(\mathfrak{p})$ if $\mathfrak{a}$ is a power of a prime ideal $\mathfrak{p}$, and 0 otherwise). The residues of L'_χ/L_χ when χ is primitive modulo $\mathfrak{m}$ are summarised in Table 1, which comes from [1, p. 361] (with the observation that β in [1] coincides with $\beta_\chi = |\mathfrak{m}_\infty|$ for characters χ which are primitive modulo $\mathfrak{m}$).

Let ψ be the logarithmic derivative of the gamma function, and for any ray class character χ on K, define

$$\psi_\chi(s) = \frac{r_1 + r_2 - \beta_\chi}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2 + \beta_\chi}{2}\psi\left(\frac{s+1}{2}\right) - \frac{n \log \pi}{2}. \tag{2.2}$$

[1] A modulus $\mathfrak{m}'$ is (strictly) smaller than $\mathfrak{m}$ if $\mathfrak{m}'_0 \mid \mathfrak{m}_0$, $\mathfrak{m}'_\infty \subseteq \mathfrak{m}_\infty$ and $\mathfrak{m}' \neq \mathfrak{m}$.

TABLE 1. Residues of the logarithmic derivative of Hecke L-functions, when χ is a primitive ray class character ([1, p. 361]).

place	**residue of ζ_K'/ζ_K**	**residue of L_χ'/L_χ**
1	-1	0
$\rho \in R_1$	1	0 if $\rho \notin R_\chi$, 1 otherwise
$\rho \in R_\chi$	0 if $\rho \notin R_1$, 1 otherwise	1
0	$r_1 + r_2 - 1$	$r_1 + r_2 - \beta_\chi$
$-2n+1, n \in \mathbf{N}_{>0}$	r_2	$r_2 + \beta_\chi$
$-2n, n \in \mathbf{N}_{>0}$	$r_1 + r_2$	$r_1 + r_2 - \beta_\chi$

The main reason to introduce these functions is the following formula: for any complex number s, if χ is primitive then

(2.3)
$$-\mathfrak{Re}\frac{L_\chi'}{L_\chi}(s) = \frac{1}{2}\log(\Delta N(\mathfrak{f}_\chi)) + \mathfrak{Re}\left(\delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \sum_{\rho \in R_\chi}\frac{1}{s-\rho} + \psi_\chi(s)\right).$$

A proof can be found in [12, Lem. 5.1].

3. Proof of the main theorem

Throughout this section, consider a ray class character χ modulo $\mathfrak{m}$ that is not trivial on a given subgroup H of $G = \mathrm{Cl}_\mathfrak{m}(K)$.

3.1. **Outline of the proof.** For any $0 < a < 1$, $x > 0$, and ideal $\mathfrak{a}$, let

$$P(\mathfrak{a}, x) = \Lambda(\mathfrak{a})\left(\frac{N(\mathfrak{a})}{x}\right)^a \log\left(\frac{x}{N(\mathfrak{a})}\right).$$

Let us start by recalling a lemma that is the starting point of the original proof of Bach's bounds.

Lemma 3.1 ([1, Lem. 4.2])**.** *For $0 < a < 1$ and any character η,*

$$\sum_{N(\mathfrak{a})<x}\eta(\mathfrak{a})P(\mathfrak{a}, x) = \frac{-1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\cdot\frac{L_\eta'}{L_\eta}(s)ds.$$

Bach then considers the difference between two instances of this equality at $\eta = 1$ and at $\eta = \chi$, and proves the bounds by estimating the right-hand side as $x + O(\sqrt{x})$, while the left-hand side is zero if the character is trivial on all prime ideals of norm smaller than x; therefore such an x cannot be too large.

The proof of Theorem 1.1 follows the same strategy. It exploits the series of lemmata provided in [1, Sec. 5], interlacing them with a game of characters of G/H in order to account for the new condition $[\mathfrak{a}]_\mathfrak{m} \in H$. Consider the group of characters of the quotient G/H, namely $\widehat{G/H} = \mathrm{Hom}(G/H, \mathbf{C}^\times)$. Given any character $\theta \in \widehat{G/H}$, let θ^* be the primitive ray class character such that $\theta^*(\mathfrak{a}) = \theta([\mathfrak{a}]_\mathfrak{m}H)$ whenever $(\mathfrak{a}, \mathfrak{m}_0) = 1$. For any $\theta \in \widehat{G/H}$, write L_θ for the L-function of θ^*. For any ray class character η and any $\theta \in \widehat{G/H}$, let η_θ denote the primitive character inducing the product $\eta\theta^*$.

Lemma 3.2. *Let $\mathfrak{a}$ be any ideal in K. Let $\mathfrak{n}_0$ be the largest divisor of $\mathfrak{m}_0$ coprime to $\mathfrak{a}$, and $\mathfrak{n} = \mathfrak{n}_0\mathfrak{m}_\infty$. Let $\pi : \mathrm{Cl}_\mathfrak{m}(K) \to \mathrm{Cl}_\mathfrak{n}(K)$ be the natural projection. Then,*

$$\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = \begin{cases} [\mathrm{Cl}_\mathfrak{n}(K) : \pi(H)] & \text{if } [\mathfrak{a}]_\mathfrak{n} \in \pi(H), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\Theta_\mathfrak{a} = \{\theta \in \widehat{G/H} \mid \theta^*(\mathfrak{a}) \neq 0\} = \{\theta \in \widehat{G/H} \mid (\mathfrak{f}_{\theta^*}, \mathfrak{a}) = 1\}$. This set is naturally in bijection with the group X of characters of $\mathrm{Cl}_\mathfrak{n}(K)/\pi(H)$. We obtain

$$\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = \sum_{\theta \in \Theta_\mathfrak{a}} \theta^*(\mathfrak{a}) = \sum_{\nu \in X} \nu([\mathfrak{a}]_\mathfrak{n}) = \begin{cases} [\mathrm{Cl}_\mathfrak{n}(K) : \pi(H)] & \text{if } [\mathfrak{a}]_\mathfrak{n} \in \pi(H), \\ 0 & \text{otherwise.} \end{cases}$$

□

Lemma 3.3. *For any $0 < a < 1$, we have*

$$\mathscr{S}_\mathfrak{m}(x) + \mathscr{S}_H(x) = \frac{-1}{[G:H]} \sum_{\theta \in \widehat{G/H}} I(x, \theta),$$

where

$$\mathscr{S}_H(x) = \sum_{\substack{N(\mathfrak{a}) < x \\ [\mathfrak{a}]_\mathfrak{m} \in H}} (1 - \chi(\mathfrak{a}))\, P(\mathfrak{a}, x),$$

$$\mathscr{S}_\mathfrak{m}(x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) \neq 1}} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))\, P(\mathfrak{a}, x), \text{ and}$$

$$I(x, \theta) = \frac{1}{2\pi i} \int_{2 - i\infty}^{2 + i\infty} \frac{x^s}{(s+a)^2} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}} \right)(s) ds.$$

Proof. From Lemma 3.2, for any ray class character η, we have

$$\sum_{\substack{N(\mathfrak{a}) < x \\ [\mathfrak{a}]_\mathfrak{m} \in H}} \eta(\mathfrak{a}) P(\mathfrak{a}, x) = \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) = 1}} \frac{\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a})}{[G:H]} \eta(\mathfrak{a}) P(\mathfrak{a}, x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) = 1}} \eta_\theta(\mathfrak{a}) P(\mathfrak{a}, x).$$

Subtracting two instances of this equality, for $\eta = 1$ and $\eta = \chi$, we get

$$\mathscr{S}_H(x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{N(\mathfrak{a}) < x} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))\, P(\mathfrak{a}, x) - \mathscr{S}_\mathfrak{m}(x),$$

and conclude by applying Lemma 3.1. □

Lemma 3.4. *For $0 < a < 1$, and with the notation from Lemma 3.3,*

$$\frac{x}{(a+1)^2} = [G:H](\mathscr{S}_H(x) + \mathscr{S}_\mathfrak{m}(x)) + \sum_{\theta \in \widehat{G/H}} \big(I_{1/2}(x, \theta) + I_0(x, \theta) + I_-(x, \theta) \big)$$

where

$$I_-(x,\theta) = (\beta_{\chi_\theta} - \beta_\theta) \sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2 x^k},$$

$$I_{1/2}(x,\theta) = \sum_{\rho \in R_\theta} \frac{x^\rho}{(\rho+a)^2} - \sum_{\rho \in R_{\chi_\theta}} \frac{x^\rho}{(\rho+a)^2}, \text{ and}$$

$$I_0(x,\theta) = \frac{\log x}{x^a}\left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(-a) + \frac{1}{x^a}\left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(-a) + (\beta_{\chi_\theta} - \beta_\theta)\left(\frac{1}{a^2} - \frac{1}{x(a-1)^2}\right) - \frac{\delta(\theta)}{a^2}.$$

Recall that for any character η, R_η is the set of zeros of L_η on the strip $0 < \mathfrak{Re}(s) < 1$.

Proof. This lemma is an analogue of [1, Lem. 4.4]. Evaluating each integral $I(x,\theta)$ by residue using Table 1 yields

$$I(x,\theta) = I_{1/2}(x,\theta) + I_0(x,\theta) + I_-(x,\theta) - \frac{\delta(\theta)x}{(a+1)^2}.$$

The residue calculations can be justified as in the proof of [12, Th. 28]. The result follows from Lemma 3.3. □

3.2. **Explicit estimates.** This section adopts the notation from Lemma 3.3 and Lemma 3.4. The remainder of the proof consists in evaluating each term in the formula of Lemma 3.4. More precisely, we bound the quantities

(1) $I_{1/2}$ in Lemma 3.7,
(2) I_0 in Lemma 3.9,
(3) $\mathscr{S}_{\mathfrak{m}}$ in Lemma 3.10,
(4) $\mathscr{S}_H$ in Lemma 3.12

Remains the quantity I_-, which is easy to bound thanks to [1, Lem. 5.1]. All these estimates are combined in Lemma 3.11. Let

$$\mathscr{R}(a,\chi) = \sum_{\theta \in \widehat{G/H}} \left(\sum_{\rho \in R_\theta} \frac{1}{|\rho+a|^2} + \sum_{\rho \in R_{\chi_\theta}} \frac{1}{|\rho+a|^2} \right).$$

We bound that quantity in Lemma 3.6, but first, we need the following lemma.

Lemma 3.5. *For $\mathfrak{Re}(s) > 1$, we have*

$$\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s) \leq 0.$$

Proof. Equation (2.1) yields

$$\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s) = -\sum_{\theta \in \widehat{G/H}} \sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})(\chi_\theta(\mathfrak{a}) + \theta^*(\mathfrak{a}))}{N(\mathfrak{a})^s}$$
$$= -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})}{N(\mathfrak{a})^s} \sum_{\theta \in \widehat{G/H}} (\chi_\theta(\mathfrak{a}) + \theta^*(\mathfrak{a})).$$

Fix an ideal $\mathfrak{a}$. If $\chi_\theta(\mathfrak{a}) = 0$ for all θ, Lemma 3.2 implies that

$$\sum_{\theta \in \widehat{G/H}} (\chi_\theta(\mathfrak{a}) + \theta^*(\mathfrak{a})) \geq 0.$$

Now suppose that there exists an $\eta \in \widehat{G/H}$ such that $\chi_\eta(\mathfrak{a}) \neq 0$. The fact that any given character is induced by a unique primitive character implies that for any $\theta \in \widehat{G/H}$, we have $\chi_\theta(\mathfrak{a}) = \chi_\eta(\mathfrak{a}) \left(\theta\eta^{-1}\right)^* (\mathfrak{a})$. Indeed, if $\left(\theta\eta^{-1}\right)^* (\mathfrak{a}) \neq 0$, the equality follows from the fact that χ_θ is the primitive character inducing $\chi_\eta \cdot \left(\theta\eta^{-1}\right)^*$, and if $\left(\theta\eta^{-1}\right)^* (\mathfrak{a}) = 0$, then one must have $\chi_\theta(\mathfrak{a}) = 0$ because $\left(\theta\eta^{-1}\right)^*$ is the primitive character inducing χ_θ/χ_η. We deduce that

$$\sum_{\theta \in \widehat{G/H}} (\chi_\theta(\mathfrak{a}) + \theta^*(\mathfrak{a})) = \chi_\eta(\mathfrak{a}) \sum_{\theta \in \widehat{G/H}} \left(\frac{\theta}{\eta}\right)^* (\mathfrak{a}) + \sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = (\chi_\eta(\mathfrak{a}) + 1) \sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}),$$

whose real part is non-negative (using again Lemma 3.2). □

Lemma 3.6 (ERH)**.** *Let $0 < a < 1$. The sum $\mathscr{R}(a, \chi)$ is at most*

$$\frac{2[G:H]}{2a+1}\Bigg(\log(\Delta N(\mathfrak{m}_0)) + n(\psi(a+1) - \log(2\pi)) \\ - \frac{|\mathfrak{m}_\infty|}{2}\left(\psi\left(\frac{a+1}{2}\right) - \psi\left(\frac{a+2}{2}\right)\right)\Bigg) + \frac{2}{2a+1}\left(\frac{1}{a+1} + \frac{1}{a}\right).$$

Proof. Writing $\sigma = 1 + a$, we have $\frac{2a+1}{|\rho+a|^2} = \frac{1}{\sigma-\rho} + \frac{1}{\sigma-\bar{\rho}}$ for any $\mathfrak{Re}(\rho) = 1/2$ (as observed in [1, Lemma 5.5]), so for any ray class character η

$$\sum_{\rho \in R_\eta} \frac{1}{|\rho + a|^2} = \frac{1}{2a+1} \sum_{\rho \in R_\eta} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \bar{\rho}}\right).$$

As in [12, Lem. 5.1], we get from Equation (2.3) that

$$\sum_{\rho \in R_\eta} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \bar{\rho}}\right) = 2\mathfrak{Re}\frac{L'_\eta}{L_\eta}(\sigma) + \log(\Delta N(\mathfrak{f}_\eta)) + 2\delta(\eta)\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1}\right) + 2\psi_\eta(\sigma).$$

Then, $\mathscr{R}(a, \eta)$ is at most

$$\frac{1}{2a+1} \sum_{\theta \in \widehat{G/H}} \Bigg(2\mathfrak{Re}\left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(\sigma) + \log(\Delta^2 N(\mathfrak{f}_\theta \mathfrak{f}_{\chi_\theta})) \\ + 2\delta(\theta)\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1}\right) + 2(\psi_\theta(\sigma) + \psi_{\chi_\theta}(\sigma))\Bigg). \tag{3.1}$$

From Lemma 3.5, we have $\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(\sigma) \leq 0$, and the corresponding term can be discarded from the expression in (3.1). Also, with $\alpha_{\chi_\theta} = r_1 - \beta_{\chi_\theta}$,

$$\begin{aligned} 2\left(\psi_\theta(\sigma) + \psi_{\chi_\theta}(\sigma)\right) &= (n + \alpha_{\chi_\theta} - \beta_\theta)\psi\left(\frac{a+1}{2}\right) + (n - \alpha_{\chi_\theta} + \beta_\theta)\psi\left(\frac{a+2}{2}\right) - 2n\log\pi \\ &= 2n(\psi(a+1) - \log(2\pi)) + (\alpha_{\chi_\theta} - \beta_\theta)\left(\psi\left(\frac{a+1}{2}\right) - \psi\left(\frac{a+2}{2}\right)\right) \\ &\leq 2n(\psi(a+1) - \log(2\pi)) - |\mathfrak{m}_\infty|\left(\psi\left(\frac{a+1}{2}\right) - \psi\left(\frac{a+2}{2}\right)\right), \end{aligned}$$

where the first equality uses the expression (2.2) and the second one follows from the duplication formula $(\psi(z/2)+\psi((z+1)/2)=2(\psi(z)-\log 2))$. □

Lemma 3.7 (ERH)**.** *For $0<a<1$ and $x\geq 1$, $\sum_{\theta\in\widehat{G/H}}|I_{1/2}(x,\theta)|\leq\sqrt{x}\cdot\mathscr{R}(a,\chi)$.*

Proof. From the ERH, for any ray class character η, and any zero $\rho\in R_\eta$ of L_η on the critical strip, we have $\mathfrak{Re}(\rho)\leq 1/2$. Therefore $|x^\rho|=|x|^{\mathfrak{Re}(\rho)}\leq\sqrt{x}$. □

Lemma 3.8. *For any s,*

$$\begin{aligned}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s)=&\sum_{\rho\in R_\theta}\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)-\sum_{\rho\in R_{\chi_\theta}}\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)\\&-\frac{\beta_{\chi_\theta}-\beta_\theta}{2}\left(\psi\left(\frac{s}{2}\right)-\psi\left(\frac{s+3}{2}\right)-\psi(1)+\psi\left(\frac{3}{2}\right)\right)\\&-\frac{\beta_{\chi_\theta}-\beta_\theta}{s+1}+\delta(\theta)\left(\frac{3}{2}-\frac{1}{s}-\frac{1}{s-1}\right)+\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(2),\end{aligned}$$

and

$$\begin{aligned}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(s)=&\sum_{\rho\in R_{\chi_\theta}}\frac{1}{(s-\rho)^2}-\sum_{\rho\in R_\theta}\frac{1}{(s-\rho)^2}\\&-\frac{\beta_{\chi_\theta}-\beta_\theta}{4}\left(\psi'\left(\frac{s}{2}\right)-\psi'\left(\frac{s+3}{2}\right)\right)\\&+\frac{\beta_{\chi_\theta}-\beta_\theta}{(s+1)^2}+\delta(\theta)\left(\frac{1}{s^2}+\frac{1}{(s-1)^2}\right).\end{aligned}$$

Proof. This is essentially the same proof as [1, Lem. 5.2], with an additional use of the recurrence relations $\psi(z)=\psi(z+1)-1/z$ and $\psi'(z)=\psi'(z+1)+1/z^2$. □

Lemma 3.9 (ERH)**.** *Let $0<a<1$ and $x\geq 1$. Then,*

$$\begin{aligned}\sum_{\theta\in\widehat{G/H}}I_0(x,\theta)\leq&\frac{(2+a)\log x+1}{x^a}\cdot\mathscr{R}(a,\chi)+\frac{[G:H]|\mathfrak{m}_\infty|}{a^2}-\frac{1}{a^2}\\&+\frac{\log x}{x^a}\left(\frac{3}{2}+\frac{1}{a}+\frac{1}{a+1}\right)+\frac{1}{x^a}\left(\frac{1}{a^2}+\frac{1}{(a+1)^2}\right)\\&+\frac{[G:H]|\mathfrak{m}_\infty|}{x}\left(\frac{1}{(1-a)^2}-\frac{\log x}{(a-1)x^{a-1}}-\frac{1}{(a-1)^2x^{a-1}}\right).\end{aligned}$$

Proof. For any $0<a<1$, Lemma 3.8 implies that

$$\sum_{\theta\in\widehat{G/H}}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(-a)\leq(2+a)\cdot\mathscr{R}(a,\chi)+\frac{3}{2}+\frac{1}{a}+\frac{1}{a+1}-\sum_{\theta\in\widehat{G/H}}\frac{\beta_{\chi_\theta}-\beta_\theta}{1-a},$$

and

$$\sum_{\theta\in\widehat{G/H}}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(-a)\leq\mathscr{R}(a,\chi)+\frac{1}{a^2}+\frac{1}{(a+1)^2}+\sum_{\theta\in\widehat{G/H}}\frac{\beta_{\chi_\theta}-\beta_\theta}{(1-a)^2}.$$

We used the facts that $\psi\left(\frac{-a}{2}\right)-\psi\left(\frac{3-a}{2}\right)-\psi(1)+\psi\left(\frac{3}{2}\right)\geq 0$, and $\psi'\left(\frac{-a}{2}\right)-\psi'\left(\frac{3-a}{2}\right)\geq 0$, which are easily derived from the recurrence relations $\psi(z)=\psi(z+1)-1/z$ and $\psi'(z)=\psi'(z+1)+1/z^2$, and the monotonicity of ψ and ψ'. From [1,

Lem. 5.3], for any $0 < a < 1$, we have $\left(\frac{\log x}{(a-1)x^{a-1}} + \frac{1}{(a-1)^2x^{a-1}} - \frac{1}{(1-a)^2}\right) \leq 0$, therefore

$$\sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{x} \left(\frac{\log x}{(a-1)x^{a-1}} + \frac{1}{(a-1)^2x^{a-1}} - \frac{1}{(1-a)^2}\right)$$
$$\leq \frac{[G:H]|\mathfrak{m}_\infty|}{x} \left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right).$$

The result follows by applying these estimates to $I_0(x, \theta)$ (as defined in Lemma 3.4). □

Lemma 3.10. *For any $0 < a < 1$,*

$$\mathscr{S}_{\mathfrak{m}}(x) \leq \frac{2\log x}{ea}\omega(\mathfrak{m}_0) \leq \frac{2\log x}{ea\log 2}\log(N(\mathfrak{m}_0)),$$

where $\omega(\mathfrak{m}_0)$ is the number of distinct prime ideals dividing $\mathfrak{m}_0$.

Proof. We have

$$\mathscr{S}_{\mathfrak{m}}(x) = \frac{1}{[G:H]} \sum_{\substack{N(\mathfrak{a})<x \\ (\mathfrak{a},\mathfrak{m})\neq 1}} \left(\sum_{\theta \in \widehat{G/H}} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))\right) P(\mathfrak{a}, x) \leq \sum_{\substack{N(\mathfrak{a})<x \\ (\mathfrak{a},\mathfrak{m})\neq 1}} 2P(\mathfrak{a}, x),$$

and the result follows from [1, Lem. 5.7]. □

Lemma 3.11 (ERH)**.** *For any $0 < a < 1$, the fraction $\sqrt{x}/(a+1)^2$ is at most*

$$[G:H]\left(s_1(x)\log(\Delta N(\mathfrak{m}_0)) + s_5(x)n + s_4(x)|\mathfrak{m}_\infty| + s_3(x)\omega(\mathfrak{m}_0) + \frac{\mathscr{S}_H(x)}{\sqrt{x}}\right) + s_2(x),$$

where

$$s_1(x) = \frac{2}{2a+1}\left(1 + \frac{(2+a)\log x + 1}{x^{a+1/2}}\right),$$
$$s_2(x) = s_1(x)\left(\frac{1}{a} + \frac{1}{a+1}\right) + \frac{\log x}{x^{a+1/2}}\left(\frac{3}{2} + \frac{1}{a} + \frac{1}{a+1}\right) + \frac{1}{x^{a+1/2}}\left(\frac{1}{a^2} + \frac{1}{(a+1)^2}\right),$$
$$s_3(x) = \frac{2\log x}{ea\sqrt{x}},$$
$$s_4(x) = \frac{1}{(a-2)^2x^{5/2}} - \frac{s_1(x)}{2}\left(\psi\left(\frac{a+1}{2}\right) - \psi\left(\frac{a+2}{2}\right)\right) + \frac{1}{a^2\sqrt{x}}$$
$$+ \frac{1}{x^{3/2}}\left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right),$$
$$s_5(x) = s_1(x)(\psi(a+1) - \log(2\pi)).$$

Proof. As in [1, Lem. 5.1], we have $0 \leq \sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2x^k} \leq \frac{1}{(a-2)^2x^2}$. We deduce that $I_-(x,\theta) \leq \frac{|\beta_{\chi_\theta} - \beta_\theta|}{(a-2)^2x^2} \leq \frac{|\mathfrak{m}_\infty|}{(a-2)^2x^2}$. Together with Lemma 3.7, the bound from Lemma 3.4 becomes

$$\frac{\sqrt{x}}{(a+1)^2} \leq \frac{[G:H]|\mathfrak{m}_\infty|}{(a-2)^2x^{5/2}} + \mathscr{R}(a,\chi) + \frac{1}{\sqrt{x}} \sum_{\theta \in \widehat{G/H}} I_0(x,\theta) + [G:H]\frac{\mathscr{S}_H(x) + \mathscr{S}_{\mathfrak{m}}(x)}{\sqrt{x}}.$$

The result then follows from Lemma 3.6, Lemma 3.9 and Lemma 3.10. □

Lemma 3.12. *Suppose that $\chi(\mathfrak{p}) = 1$ for all prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) < x$, $[\mathfrak{p}]_{\mathfrak{m}} \in H$, and $\deg(\mathfrak{p}) = 1$. Then, for any $0 < a < 1$,*

$$\mathscr{S}_H(x) \leq \frac{2n}{ea} \sum_{m<\sqrt{x}} \Lambda(m).$$

Proof. We start as in [1, Lem. 5.7] by observing that when $t \geq 1$, the function $t^{-a}\log t$ is bounded above by $1/ea$. We deduce

$$\mathscr{S}_H(x) = \sum_{\substack{N(\mathfrak{a})<x \\ [\mathfrak{a}]_{\mathfrak{m}} \in H}} (1-\chi(\mathfrak{a}))\, P(\mathfrak{a}, x) \leq \frac{2}{ea} \sum_{\substack{N(\mathfrak{a})<x \\ [\mathfrak{a}]_{\mathfrak{m}} \in H \\ \chi(\mathfrak{a})\neq 1}} \Lambda(\mathfrak{a}). \tag{3.2}$$

Fix a prime ideal $\mathfrak{p}$ (above a rational prime p) of norm smaller than x and consider the contribution of its powers to the above sum. First suppose that $\deg(\mathfrak{p}) > 1$. Then,

$$\sum_{\substack{N(\mathfrak{p}^k)<x \\ [\mathfrak{p}^k]_{\mathfrak{m}} \in H \\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \leq \sum_{N(\mathfrak{p}^k)<x} \deg(\mathfrak{p})\Lambda(p^k) \leq \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k).$$

Now suppose that $\deg(\mathfrak{p}) = 1$, and let ℓ be the smallest integer such that $[\mathfrak{p}^\ell]_{\mathfrak{m}} \in H$. If $\ell = 1$, then $\chi(\mathfrak{p}^k) = 1$ for any integer k, so the contribution of $\mathfrak{p}$ is zero. Suppose that $\ell \geq 2$. Then,

$$\sum_{\substack{N(\mathfrak{p}^k)<x \\ [\mathfrak{p}^k]_{\mathfrak{m}} \in H \\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \leq \sum_{N(\mathfrak{p}^{k\ell})<x} \Lambda(\mathfrak{p}^{k\ell}) \leq \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k).$$

Summing over all rational primes p and ideals $\mathfrak{p}$ above p, we obtain

$$\sum_p \sum_{\mathfrak{p}|p} \sum_{\substack{N(\mathfrak{p}^k)<x \\ [\mathfrak{p}^k]_{\mathfrak{m}} \in H \\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \leq \sum_p \sum_{\mathfrak{p}|p} \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k) \leq n \sum_{m<\sqrt{x}} \Lambda(m).$$

We conclude by applying this inequality to Equation (3.2). □

Lemma 3.13. *For any $x > 0$,*

$$\lim_{a\to 1} \left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2 x^{a-1}} \right) = \frac{(\log x)^2}{2}.$$

Proof. A simple application of l'Hôpital's rule yields

$$\begin{aligned} &\lim_{a\to 1} \left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2 x^{a-1}} \right) \\ &= \lim_{b\to 0} \left(\frac{x^b - b\log x - 1}{b^2 x^b} \right) = \lim_{b\to 0} \left(\frac{x^b \log x - \log x}{bx^b(b\log(x) + 2)} \right) \\ &= \lim_{b\to 0} \left(\frac{(\log x)^2}{b^2(\log x)^2 + 4b\log x + 2} \right) = \frac{(\log x)^2}{2}. \end{aligned}$$

□

14 Jun 2018 08:13:39 PDT
Version 4 - Submitted to Open Book Series

3.3. **Proof of Theorem 1.1.** Let x be the norm of the smallest prime ideal $\mathfrak{p}$ such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$, $\deg(\mathfrak{p}) = 1$ and $\chi(\mathfrak{p}) \neq 1$. First suppose that $x \leq 95$, and consider the quantity

$$B = \big([G : H]\,(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\big)^2.$$

We want to show that $x \leq B$.

Suppose $n = 1$. For the ray class group G not to be trivial, one must have either $|\mathfrak{m}_\infty| = 1$ and $N(\mathfrak{m}_0) \geq 3$, in which case

$$B \geq \big(2.71\log(3) + 1.29 + 1.38 + 4.13\big)^2 = 95.59\cdots \geq x,$$

or $|\mathfrak{m}_\infty| = 0$ and $N(\mathfrak{m}_0) \geq 5$, in which case

$$B \geq \big(2.71\log(5) + 1.38 + 4.13\big)^2 = 97.44\cdots \geq x.$$

Suppose $n = 2$. Suppose that $\Delta N(\mathfrak{m}_0) \geq 8$. Then

$$B \geq (2.71\log(8) + 4.13)^2 = 95.36\cdots \geq x.$$

Now, one must investigate the cases where $\Delta N(\mathfrak{m}_0) \leq 7$. All quadratic fields with a discriminant of absolute value at most 7 have a trivial (narrow) class group. Therefore, one must have $N(\mathfrak{m}_0) \geq 2$. There is only one quadratic field of discriminant of absolute value at most 3, namely $\mathbf{Q}(\sqrt{-3})$. It has discriminant of absolute value 3 and no ideal of norm 2, so the condition $\Delta N(\mathfrak{m}_0) \leq 7$ is impossible.

Suppose $n > 2$. From [1, Lem. 7.1], we get

$$\log(\Delta N(\mathfrak{f})) \geq n(\log(2\pi) - \psi(2)) - \frac{3}{2} \geq 2.74,$$

and we deduce

$$B \geq (2.71 \cdot 2.74 + 4.13)^2 = 133.52\cdots \geq x.$$

It remains to consider the case $x > 95$. From Lemma 3.12 and [18, Th. 12],

$$\mathscr{S}_H(x) \leq \frac{2n}{ea} \sum_{m<\sqrt{x}} \Lambda(m) \leq \frac{2nC\sqrt{x}}{ea},$$

where $C = 1.03883$. We now apply Lemma 3.11 with $a \to 1$. From Lemma 3.13 (applied to the term s_4), and the facts that for $x \geq 95$, $\big(s_5(x) + \frac{2C}{ea}\big)$ is negative, and s_1, s_2, s_3 and s_4 are decreasing, we get

$$\begin{aligned} x &\leq 2^4\big([G : H]\,(s_1(95)\log(\Delta N(\mathfrak{m}_0)) + s_4(95)|\mathfrak{m}_\infty| + s_3(95)\omega(\mathfrak{m}_0)) + s_2(95)\big)^2 \\ &\leq \big([G : H]\,(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\big)^2, \end{aligned}$$

which proves the theorem. □

4. Consequences

With Theorem 1.1 at hands, we can now derive a few important consequences. The first of them, Theorem 1.2, asserts that a subgroup H of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ is always generated by ideals of bounded prime norm.

4.1. **Proof of Theorem 1.2.** Recall that K is a number field, Δ is the absolute value of the discriminant of K, and $\mathfrak{m}$ is a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Also, $\mathfrak{h}$ is an ideal in K, and H is a non-trivial subgroup of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$. Let

$$B = \left([G:H]\left(2.71\log(\Delta N(\mathfrak{h}\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{h}\mathfrak{m}_0)\right) + 4.13\right)^2,$$
$$\mathscr{N} = \{\mathfrak{p} \in \mathscr{I}_{\mathfrak{m}}(K) \mid \mathfrak{p} \text{ is prime}, (\mathfrak{p},\mathfrak{h}) = 1, [\mathfrak{p}]_{\mathfrak{m}} \in H, \deg(\mathfrak{p}) = 1 \text{ and } N(\mathfrak{p}) < B\},$$

and N the subgroup of H generated by $\mathscr{N}$. By contradiction, suppose $N \neq H$. Then, there is a non-trivial character of H that is trivial on N. Since G is abelian, this character on H extends to a character on G, thereby defining a ray class character χ modulo $\mathfrak{m}$ that is not trivial on H. From Theorem 1.1, there is a prime ideal $\mathfrak{p} \in \mathscr{I}_{\mathfrak{h}\mathfrak{m}}(K)$ such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$, $\chi(\mathfrak{p}) \neq 1$, $\deg(\mathfrak{p}) = 1$ and $N(\mathfrak{p}) \leq B$. All these conditions imply that $\mathfrak{p} \in \mathscr{N} \subseteq N$, whence $\chi(\mathfrak{p}) = 1$, a contradiction. □

The next consequence, Theorem 1.3, is a specialization of Theorem 1.2 to the field of rational numbers, and asserts that a subgroup H of a group of the form $(\mathbf{Z}/m\mathbf{Z})^\times$ is generated by prime numbers bounded polynomially in the subgroup index and $\log(m)$.

4.2. **Proof of Theorem 1.3.** Recall that m is a positive integer, and H is a non-trivial subgroup of $G = (\mathbf{Z}/m\mathbf{Z})^\times$. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0 = m\mathbf{Z}$ and $\mathfrak{m}_\infty$ is the real embedding of $\mathbf{Q}$. Then, $\mathrm{Cl}_{\mathfrak{m}}(\mathbf{Q})$ is isomorphic to $G = (\mathbf{Z}/m\mathbf{Z})^\times$. An isomorphism is given by the map sending the class of $a\mathbf{Z}$ to $a \bmod m$. The subgroup H of $(\mathbf{Z}/m\mathbf{Z})^\times$ corresponds to a subgroup H' of $\mathrm{Cl}_{\mathfrak{m}}(\mathbf{Q})$ through this isomorphism. From Theorem 1.2, H' is generated by prime numbers smaller than

$$B = \left([G:H]\left(2.71\log(m) + 1.29 + 1.38\omega(m)\right) + 4.13\right)^2,$$

and so is H. If H is the full group, then the theorem follows from [1, Th. 3]; and for $m \leq 11000$, the result is easy to check by an exhaustive computation. So we can assume that $m/|H| \geq 2$ and $m > 11000$. From [1, Lem. 6.4],

$$\frac{\omega(m)}{\log m} \leq \frac{\mathrm{li}(\log m) + 0.12\sqrt{\log m}}{\log m} \leq \frac{\mathrm{li}(\log 11000) + 0.12\sqrt{\log 11000}}{\log 11000} \leq 0.67,$$

where li is the logarithmic integral function. We get

$$B \leq \left([G:H]\log(m)\left(2.71 + \frac{1.29 + 4.13/2}{\log 11000} + 1.38 \cdot 0.67\right)\right)^2,$$

and we conclude by computing the constant. □

The third consequence is a bound on the degrees of the cyclic isogenies required to connect all isogenous principally polarizable abelian varieties over a finite field sharing the same endomorphism ring.

4.3. **Proof of Theorem 1.4.** Recall that $\mathscr{A}$ is a principally polarized, absolutely simple, ordinary abelian variety over a finite field $\mathbf{F}_q$, with endomorphism algebra K and endomorphism ring isomorphic to an order $\mathcal{O}$ in K. The field K_0 is the maximal real subfield of K, and $\mathfrak{f}$ is the conductor of $\mathcal{O}$. For any $B > 0$, $\mathscr{G}(B)$ is the isogeny graph whose vertices are the principally polarizable varieties isogenous to $\mathscr{A}$ and with the same endomorphism ring, and whose edges are isogenies connecting

them, of prime degree (therefore cyclic) smaller than B. By the theory of complex multiplication, the graph $\mathscr{G}(B)$ is isomorphic to the Cayley graph of

$$\mathscr{P}(\mathcal{O}) = \ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^+(\mathcal{O} \cap K_0))$$

with set of generators the classes of ideals of prime norm smaller than B (see [10, Sec. 2.5] for a detailed discussion on this isomorphism). Let $g \geq 2$ be the dimension of $\mathscr{A}$, and $n = 2g$ the degree of its endomorphism algebra K. The natural map $\pi : \mathrm{Cl}_{\mathfrak{f}}(K) \to \mathrm{Cl}(\mathcal{O})$ is a surjection (see for instance [10, Sec. 2.2]), so it is sufficient to find a generating set for $H = \pi^{-1}(\mathscr{P}(\mathcal{O}))$. From [10, Lem. 2.1], we have the inequality

$$[\mathrm{Cl}_{\mathfrak{f}}(K) : H] \leq [\mathrm{Cl}(\mathcal{O}) : \mathscr{P}(\mathcal{O})] \leq h^+_{\mathcal{O}_0}.$$

From Theorem 1.2, $\mathscr{G}(B)$ is connected for

$$B = \left(2.71 + 1.38\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} + \frac{4.13}{\log(\Delta N(\mathfrak{f}))}\right)^2 \left(h^+_{\mathcal{O}_0} \log(\Delta N(\mathfrak{f}))\right)^2, \tag{4.1}$$

and it remains to show that the constant factor in this expression is at most 26. First, we need a lower bound on the quantity $\log(\Delta N(\mathfrak{f}))$. From [17, Tab. 3], if $n = 4$, $\log(\Delta N(\mathfrak{f})) \geq 4\log(3.263) \geq 4.73$ (this result assumes ERH). For $n \geq 6$, [1, Lem. 7.1] implies

$$\log(\Delta N(\mathfrak{f})) \geq n(\log(2\pi) - \psi(2)) - \frac{3}{2} \geq 6.99.$$

Therefore for any degree $n \geq 4$, we have $\log(\Delta N(\mathfrak{f})) \geq 4.73$. Now, for $n = 2$, smaller values of $\log(\Delta N(\mathfrak{f}))$ are possible. One can easily check that the constant factor in the expression (4.1) is at most 26 for all pairs $(\Delta, N(\mathfrak{f}))$ such that $\log(\Delta N(\mathfrak{f})) < 4.73$ by an exhaustive computation. There are however five exceptions: when the field is $\mathbf{Q}(\sqrt{-1})$, and $N(\mathfrak{f}) \in \{1, 2\}$, when the field is $\mathbf{Q}(\sqrt{-3})$, and $N(\mathfrak{f}) \in \{1, 3\}$, and when the field is $\mathbf{Q}(\sqrt{5})$, and $N(\mathfrak{f}) = 1$. Since $\mathfrak{f}$ is the conductor of an order in a quadratic field, it is generated by an integer, so $N(\mathfrak{f})$ must be a square. This discards the cases $N(\mathfrak{f}) \in \{2, 3\}$. When $N(\mathfrak{f}) = 1$, the order $\mathcal{O}$ is the ring of integers, which has a trivial (narrow) class group for $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt{5})$.

Then, irrespective of the value of n, we can assume in the rest of the proof that $\log(\Delta N(\mathfrak{f})) \geq 4.73$. If $\omega(\mathfrak{f}) \leq 5$, then

$$\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} \leq \frac{5}{4.73} \leq 1.06.$$

If $\omega(\mathfrak{f}) > 5$, then $N(\mathfrak{f}) \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^{\omega(\mathfrak{f})-5}$, and

$$\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} \leq \frac{\omega(\mathfrak{f})}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^{\omega(\mathfrak{f})-5})} \leq \frac{5}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11)} + \frac{1}{\log(13)} \leq 1.06.$$

Then,

$$\left(2.71 + \frac{1.38 \cdot \omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} + \frac{4.13}{\log(\Delta N(\mathfrak{f}))}\right)^2 \leq (2.71 + 1.38 \cdot 1.06 + 4.13/4.73)^2 \leq 26,$$

which concludes the proof. □

Acknowledgements

The author wishes to thank Arjen K. Lenstra and Rob Granger, as well as the anonymous referees, for their helpful feedback. Part of this work was supported by the Swiss National Science Foundation under grant number 200021-156420.

References

1. E. Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), no. 191, 355–380. MR 91m:11096
2. Eric Bach and Jonathan P. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comput. **65** (1996), 1717–1735.
3. J.-F. Biasse and F. Song, *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, 2016, pp. 893–902.
4. P. Campbell, M. Groves, and D. Shepherd, *Soliloquy: A cautionary tale*, ETSI 2nd Quantum-Safe Crypto Workshop, 2014, Available at `http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`.
5. R. Cramer, L. Ducas, C. Peikert, and O. Regev, *Recovering short generators of principal ideals in cyclotomic rings*, pp. 559–585, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
6. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski, *Short Stickelberger class relations and application to Ideal-SVP*, Advances in Cryptology – EUROCRYPT 2017 (Jean-Sébastien Coron and Jesper Buus Nielsen, eds.), Springer International Publishing, 2017, pp. 324–348.
7. S. D. Galbraith, F. Hess, and N. P. Smart, *Extending the GHS Weil descent attack*, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (London, UK), EUROCRYPT '02, Springer-Verlag, 2002, pp. 29–44.
8. S. Garg, C. Gentry, and S. Halevi, *Candidate multilinear maps from ideal lattices*, EUROCRYPT, 2013, pp. 1–17.
9. D. Jao, S. D. Miller, and R. Venkatesan, *Expander graphs based on GRH with an application to elliptic curve cryptography*, J. Number Theory **129** (2009), no. 6, 1491 – 1504.
10. D. Jetchev and B. Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem*, Cryptology ePrint Archive, Report 2017/053, 2017, `http://eprint.iacr.org/2017/053`.
11. J.C. Lagarias, H.L. Montgomery, and A.M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Inventiones mathematicae **54** (1979), 271–296 (eng).
12. J.C. Lagarias and A.M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.
13. Y. Lamzouri, X. Li, and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Mathematics of Computation **84** (2015), no. 295, 2391–2412.
14. A. Langlois, D. Stehlé, and R. Steinfeld, *GGHLite: More efficient multilinear maps from ideal lattices*, Advances in Cryptology–EUROCRYPT 2014, Springer, 2014, pp. 239–256.
15. D. Maisner and E. Nart, *Abelian surfaces over finite fields as jacobians*, Experiment. Math. **11** (2002), 321337.
16. J. Neukirch and N. Schappacher, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin, New York, Barcelona, 1999.
17. A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results*, Journal de théorie des nombres de Bordeaux **2** (1990), no. 1, 119–141 (eng).
18. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics **6** (1962), no. 1, 64–94.
19. R. Schoof, *Minus class groups of the fields of the ℓ-th roots of unity*, Mathematics of Computation of the American Mathematical Society **67** (1998), no. 223, 1225–1245.
20. N. P. Smart and F. Vercauteren, *Fully homomorphic encryption with relatively small key and ciphertext sizes*, Public Key Cryptography, 2010, pp. 420–443.
21. B. Smith, *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*, Journal of Cryptology **22** (2009), no. 4, 505–529.

École Polytechnique Fédérale de Lausanne, EPFL IC LACAL, Switzerland

ON THE CONSTRUCTION OF CLASS FIELDS

CLAUS FIEKER, TOMMY HOFMANN, AND CARLO SIRCANA

Abstract. Class field theory is an important tool in number theory. We discuss improvements to the computation of ray class groups, congruence subgroups and class fields, which are fundamental building blocks of constructive class field theory. As an application and to illustrate the power of our new techniques, we find new fields with minimal discriminant having prescribed Galois group and signature.

1. Introduction

Class field theory of algebraic number fields is one of the main achievements of algebraic number theory in the first half of the 20th century. Building upon Kummer theory, it gives a complete description of abelian extensions of a number field K in terms of objects "inside" K. As a corollary, one obtains a fairly simple parametrization of all abelian extensions of K, similar to the parametrization of abelian extensions of $\mathbf{Q}$ provided by the theorem of Kronecker–Weber. With a growing interest in algorithmic aspects of algebraic number theory and the availability of computational resources, the existence theorem of class field theory was made constructive, resulting in efficient algorithms for working with ray class groups and constructing class fields, see [Has64, DP95, DP98, Poh99, CDyDO96, CDyDO98, Coh99, CS08].

The aim of this paper is to describe new methods for computing class fields with an emphasis on the problem of tabulating extensions of number fields. While the overall strategy is the same as in [CDyDO98] and [DP95], we show how the individual steps can be improved tremendously. The theoretical improvements are accompanied by an efficient implementation allowing computations in situations which were out of reach before. To illustrate this, we have computed new minimal discriminants of number fields with various Galois groups. For a number field K denote by d_K the absolute discriminant of K. If G is a transitive permutation group of degree n and $r \in \mathbf{Z}$, $0 \leq r \leq n$, we set $d_0(n, r, G)$ to be the smallest value of $|d_K|$, where $[K : \mathbf{Q}] = n$, K has r real embeddings, and if L is the Galois closure of K over $\mathbf{Q}$, then $\mathrm{Gal}(L/\mathbf{Q}) \cong G$.

We let C_n denote the cyclic group of order n, D_n denote the dihedral group of order $2n$ and S_n denote the symmetric group on n letters. Using our algorithm we obtain the following minimal discriminants.

Theorem 1. *The following hold:*

(1) $d_0(30, 1, D_{15}) = 239^7$,
(2) $d_0(30, 3, D_5 \times C_3) = 7^{12} \cdot 17^6$,
(3) $d_0(30, 5, S_3 \times C_5) = 2^{10} \cdot 11^{13}$,
(4) $d_0(36, 36, C_9 \rtimes C_4) = 1129^{27}$,
(5) $d_0(36, 0, C_9 \rtimes C_4) = 3^{88} \cdot 29^{27}$.

5 Jun 2018 07:51:59 PDT
Version 2 - Submitted to Open Book Series

In all five cases the value of the minimal possible discriminant was not known (see the database of Klüners–Malle [KM01] for the first three cases).

Finally, note that we only consider the problem of computing abelian extensions of arbitrary number fields K, with a focus on normal extensions. For various base fields, there are special methods, for example complex multiplication in case K is imaginary quadratic or (conjectural) Stark units for totally real fields.

2. Class field theory and enumeration of abelian extensions

In this section, we briefly recall the main theorem of class field theory and its application to the construction of number fields or complete tables of number fields with specific properties. We refer the reader to [Jan96] or [Lan94] for a detailed description of the topic.

Let K be a number field with ring of integers $\mathcal{O}_K$. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we denote by $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation. A *modulus* $\mathfrak{m}$ of K is a pair $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ consisting of a non-zero ideal $\mathfrak{m}_0$ of $\mathcal{O}_K$ and a set of real embeddings of K. In this case we also write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$. For a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ we define $I_\mathfrak{m}$ to be the group of fractional ideals of K generated by the prime ideals not dividing $\mathfrak{m}_0$. Moreover, for $x \in K$ we define $x \equiv 1 \bmod \mathfrak{m}$ if and only if $v_\mathfrak{p}(x-1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{m}_0$ and $\sigma(x) > 0$ for $\sigma \in \mathfrak{m}_\infty$. We define the *ray group* $P_\mathfrak{m} = \{xK \mid x \equiv 1 \bmod \mathfrak{m}\} \subseteq I_\mathfrak{m}$ and call the finite abelian group $\mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/P_\mathfrak{m}$ the *ray class group* of K modulo $\mathfrak{m}$. A subgroup $P_\mathfrak{m} \subseteq A \subseteq I_\mathfrak{m}$ is called a *congruence subgroup* modulo $\mathfrak{m}$. By abuse of notation, we will also call $\overline{A} = A/P_\mathfrak{m}$ a congruence subgroup. The smallest modulus $\mathfrak{n}$ with $I_\mathfrak{m} \cap P_\mathfrak{n} \subseteq A$ is the *conductor* of A.

Let L/K be an abelian extension. Then for every prime ideal $\mathfrak{p}$ of K, which is not ramified in L/K, there exists a unique morphism $\mathrm{Frob}_{\mathfrak{p},L/K} \in \mathrm{Gal}(L/K)$ with $x^{\mathrm{N}(\mathfrak{p})} \equiv x \bmod \mathfrak{p}\mathcal{O}_L$ for all $x \in \mathcal{O}_L$. We call $\mathrm{Frob}_{\mathfrak{p},L/K}$ the *Frobenius automorphism* of $\mathfrak{p}$. If $\mathfrak{m}$ is a modulus divisible by the prime ideals ramifying in L/K, there exists a unique morphism $\psi_{L/K}\colon I_\mathfrak{m} \longrightarrow \mathrm{Gal}(L/K)$, called the *Artin map*, such that $\psi_{L/K}(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p},L/K}$ for all non-zero prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}_0$. Any modulus $\mathfrak{f}$ such that $\varphi_{L/K}$ factors through $\mathrm{Cl}_\mathfrak{f}$ is called an *admissible modulus* of L/K. The smallest modulus with this property is called the *conductor* of L/K.

Theorem 2. *If L/K is an abelian extension of conductor $\mathfrak{f}$, then there exists a congruence subgroup $A_\mathfrak{f} \subseteq \mathrm{Cl}_\mathfrak{f}$ of conductor $\mathfrak{f}$ such that the Artin map induces an isomorphism $\psi_{L/K}\colon \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f} \to \mathrm{Gal}(L/K)$. If $A_\mathfrak{f}$ is a congruence subgroup of conductor $\mathfrak{f}$, then there exists an abelian extension L/K such that the Artin map induces an isomorphism $\psi_{L/K}\colon \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f} \to \mathrm{Gal}(L/K)$.*

Now assume that K is a number field, G an abelian group and $X \in \mathbf{R}_{>0}$. We fix an algebraic closure $\overline{K}$ of K. For a finite extension L/K we set $d_{L/K} = \mathrm{N}(\mathfrak{d}_{L/K})$ to be the norm of the relative discriminant. To find

$$\{K \subseteq L \subseteq \overline{K} \mid \mathrm{Gal}(L/K) \cong G \text{ and } d_{L/K} \leq X\},$$

we can proceed as follows:

(1) Find a set F containing all possible conductors $\mathfrak{f}$.
(2) For every conductor $\mathfrak{f} \in F$ compute the ray class group $\mathrm{Cl}_\mathfrak{f}$ and all subgroups $A \subseteq \mathrm{Cl}_\mathfrak{f}$ of conductor $\mathfrak{f}$ with $\mathrm{Cl}_\mathfrak{f}/A \cong G$.
(3) Let L be an abelian extension of K corresponding to a pair $(\mathfrak{f}, A)$ of step (2). If $d_{L/K} \leq X$, compute a defining equation for L.

We discuss Step (2) in Section 3 and Step (3) in Section 4. In many applications, one is only interested in field extensions with specific properties. While sieving after Step (3) is always possible, it is not an optimal strategy since the computation of the defining equation is usually the most expensive step. Very often, the situation allows one to make improvements already in Step (2) or (3). For example, since the ramification of L/K is intimately connected to the conductor of this extension, restrictions on the ramification allow us to reduce the set of possible conductors in Step (1). In other common situations, K itself is a normal extension of some subfield K_0 and one is only interested in extensions L/K with Galois group G, such that also L/K_0 is normal. We will address the latter problem in Section 5.

3. Quotients of Ray Class Groups

Let K be an algebraic number field and suppose that we are searching for abelian extensions of K with Galois group of exponent n. As described in Section 2, the fields we are looking for correspond to congruence subgroups H of ray class groups $\mathrm{Cl}_\mathfrak{m}$ with conductor $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, such that $\mathrm{Cl}_\mathfrak{m}/A$ is of exponent n, that is, to subgroups A with $\mathrm{Cl}_\mathfrak{m}^n \subseteq A \subseteq \mathrm{Cl}_\mathfrak{m}$. Therefore we do not need the whole group $\mathrm{Cl}_\mathfrak{m}$, but only the quotient $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^n$.

Recall that the standard algorithm (see [CDyDO96]) to compute the ray class group $\mathrm{Cl}_\mathfrak{m}$ relies on the following exact sequence:

$$\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl} \longrightarrow 0, \tag{1}$$

where $\mathcal{O}_K^\times$ are the units of $\mathcal{O}_K$ and Cl is the class group of K. In particular, if $\{u_i\}, \{m_i\}, \{c_i\}$ are generators of the groups $\mathcal{O}_K^\times$, $(\mathcal{O}_K/\mathfrak{m})^\times$ and Cl respectively, then we can choose as generators of $\mathrm{Cl}_\mathfrak{m}$ the union of the images of the m_i and preimages of the c_i. Computing the relations between the generators of Cl and $(\mathcal{O}_K/\mathfrak{m})^\times$ requires the computation of generators of principal ideals and of discrete logarithms in $(\mathcal{O}_K/\mathfrak{m})^\times$. To get the relations for the generators coming from $\mathcal{O}_K^\times$, we also have to compute discrete logarithms in $(\mathcal{O}_K/\mathfrak{m})^\times$. Note that the latter problem can be expensive. For every prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}_0$, computing the discrete logarithm in $(\mathcal{O}_K/\mathfrak{m})^\times$ requires the computation of a discrete logarithm in the multiplicative group $(\mathcal{O}_K/\mathfrak{p})^\times$ of the residue field. This quickly becomes a bottleneck in case $\mathrm{N}(\mathfrak{p}) - 1$ is hard to factor or divisible by large primes.

To avoid these problems, we show how to directly construct the quotient $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^n$ of the ray class group. For clarity of the exposition, we will only consider the case when n is a prime power, that is $n = p^s$ for some prime $p \in \mathbf{Z}_{>0}$. Indeed, if n factors as $n = \prod_{i=1}^r p_i^{e_i}$, we get

$$\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^n \cong \prod_{i=1}^r \mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{p_i^{e_i}}.$$

While for finite abelian groups, the functor $A \mapsto A/p^sA$ is in general only right exact, we can use the exact sequence (1) together with the following lemma to construct the quotient directly.

Lemma 3. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of finite abelian groups of exponents e_1, e_2 and e_3 respectively. Let $p \in \mathbf{Z}_{>0}$ be a prime number and $k \in \mathbf{Z}_{>0}$ with $k \geq v_p(e_i)$ for $i = 1, 2, 3$. Then the sequence*

$$0 \to A/p^kA \to B/p^kB \to C/p^kC \to 0$$

is exact.

Now let $\tilde{n} = p^{\tilde{s}}$ with $\tilde{s} = v_p(\#(\mathcal{O}_K/\mathfrak{m})^\times) + v_p(\#\mathrm{Cl})$. The lemma shows that we can construct $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{\tilde{n}}$ by working only with $\mathrm{Cl}/\mathrm{Cl}^{\tilde{n}}$ and with $(\mathcal{O}_K/\mathfrak{m})^\times/(\mathcal{O}_K/\mathfrak{m})^{\times\tilde{n}}$ (by applying it to $1 \to (\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{O}_K^\times) \to \mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl} \to 1$). In particular, the number of generators of the quotient can be smaller than the number of generators of the entire class group. Since for every generator we have to perform expensive operations, this improves performance.

The lemma also affects the construction of the multiplicative group. Let $\mathfrak{q}$ be a prime ideal divisor of $\mathfrak{m}_0$ and $l = v_\mathfrak{q}(\mathfrak{m}_0)$. Recall that by [Coh00, Proposition 4.2.4] we have

$$(\mathcal{O}_K/\mathfrak{q}^l)^\times \cong (\mathcal{O}_K/\mathfrak{q})^\times \times (1+\mathfrak{q})/(1+\mathfrak{q}^l).$$

We distinguish two cases:

- If $l = 1$, we need to compute a generator of $U/\tilde{n}U$, where $U = (\mathcal{O}_K/\mathfrak{q})^\times$. This is much easier than the computation of a generator of the whole group U, which would require the factorization of $\#U = N(\mathfrak{q})-1$. We can assume that $p \mid N(\mathfrak{q})-1$, otherwise $\mathfrak{m}$ can not be the conductor of such an extension ([Coh00, Prop. 3.3.21]). Let $e = v_p(N(\mathfrak{q})-1)$. Finding a generator of the group $U/\tilde{n}U$ is equivalent to finding an element of U of order divisible by p^e. Such an element can be found by picking random elements with high probability. Indeed, let g be an element of U and let $s = (N(\mathfrak{q})-1)/p^e$. Then g is a generator of $U/\tilde{n}U$ if $g^{sp^{e-1}}$ is not trivial. The probability of finding an element of order divisible by p^e is $\phi(p^e)/p^e = (p-1)/p$, which is always greater than $1/2$.
- If $l > 1$, then $p \nmid N(\mathfrak{q})-1$ and we can avoid computing the multiplicative group of the residue field altogether, since its order is not divisible by p.

Since in this way we have constructed the quotient $V = \mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{\tilde{n}}$, as a final step we just have to compute V/nV.

4. Ray class fields

Let L/K be an abelian extension of degree n and suppose that we have computed an admissible modulus $\mathfrak{f} = \mathfrak{f}_0\mathfrak{f}_\infty$ of L/K divisible only by the ramifying primes, and a congruence subgroup $A_\mathfrak{f}$ such that the Artin map induces an isomorphism $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f} \to \mathrm{Gal}(L/K)$. Furthermore we assume that we have computed an explicit isomorphism $\Psi\colon \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f} \to \mathbf{Z}/n\mathbf{Z}$. While various invariants can be computed from only $\mathfrak{f}$ and $A_\mathfrak{f}$, finding explicit defining equations for the extension L/K is sometimes relevant, for example when constructing towers of number fields. This problem is usually solved using either Hecke's theorem or the Artin map, see [Coh00, Section 5.5.5] for a comparison of both methods. Here we follow in principle the Artin map approach, but we show how to improve it significantly. We will repeatedly make use of the following key result from [Fie01, Section 3], see also [Coh00, Section 5.4.1].

Proposition 4. *Assume that K contains the n-th roots of unity and $L = K(\sqrt[n]{\alpha})$ is a Kummer extension. Then, for almost all prime ideals $\mathfrak{p}$ of K, we can efficiently find $k \in \mathbf{Z}$ with $\mathrm{Frob}_\mathfrak{p}(\sqrt[n]{\alpha}) = \zeta_n^k \sqrt[n]{\alpha}$ doing only computations in K.*

4.1. **Reduction to the prime power case.** Using the Fundamental Theorem of Finite Abelian Groups, we may decompose $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$ into a product of cyclic groups of prime power order. Accordingly, L/K is the compositum of linear disjoint

cyclic extensions of K of prime power degree. Thus, from now on we assume that $\mathrm{Gal}(L/K) \cong \mathbf{Z}/\ell^m\mathbf{Z}$ is a cyclic extension of prime power degree $n = \ell^m$ for some prime ℓ.

4.2. **Using Kummer theory.** Let $E = K(\zeta_n)$ and $F = LE = L(\zeta_n)$. Then F/E is again an abelian extension and, since $\mathrm{N}_{E/K}(P_{\mathfrak{f}\mathcal{O}_E}) \subseteq P_{\mathfrak{f}}$, we know that the lift $\mathfrak{f}_E = \mathfrak{f}\mathcal{O}_E$ is an admissible modulus for the abelian extension F/E by [Jan96, Chapter III, Section 3]. Our aim is to find a defining equation for the field extension F/E, which is now a Kummer extension. To this end, we compute Cl_E and a finite set S of primes of E containing the infinite primes such that

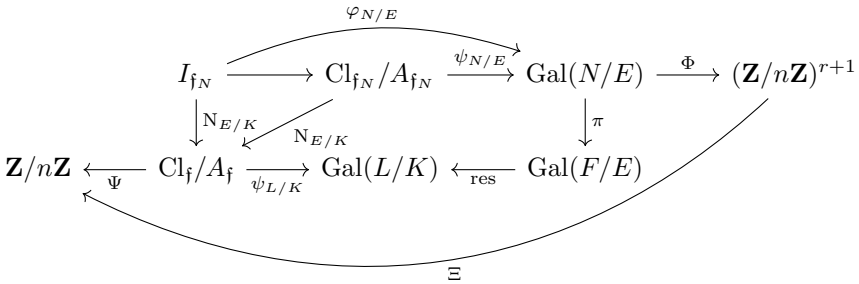
(1) F/E is unramified outside of S, that is, S contains all primes dividing $\mathfrak{f}_E$,
(2) $\mathrm{Cl}_E/\mathrm{Cl}_E^n$ is generated by the classes of the finite primes in S,
(3) S contains all finite primes dividing $n = \ell^m$.

We consider then the group U_S of S-units of E. By Dirichlet's unit theorem it is isomorphic to $\mu_E \times \mathbf{Z}^{\#S-1}$. Let $\varepsilon_0 \in \mathcal{O}_E^\times$ be a torsion unit with $\langle \varepsilon_0 \rangle = \mu_E$. Denoting $r = \#S - 1$, we can compute r elements $\varepsilon_1, \dots, \varepsilon_r \in E$ such that $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$ generate U_S. Since F/E is of exponent n and E contains the n-th roots of unity, by Kummer theory we know that $F = E(\sqrt[n]{W_F})$, where $W_F = E^\times \cap F^{\times n}$. By [CS08, Lemma 5.4] condition (1) implies that $W_F/E^{\times n} \subseteq (U_S \cdot E^{\times n})/E^{\times n}$ and therefore $E \subseteq F \subseteq N$, where $N = E(\sqrt[n]{U_S})$. Since F/E is a cyclic subextension of N/E, Kummer theory asserts that there exists an element $\alpha = \varepsilon_0^{n_0}\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ such that $F = E(\sqrt[n]{\alpha})$. Our aim is to determine such an element $\alpha \in U_S$ or, equivalently, suitable exponents $n_0, \dots, n_r \in \mathbf{Z}$.

Let $\mathfrak{f}_N$ be an admissible modulus for N/E and $\mathrm{Cl}_{\mathfrak{f}_N}/A_{\mathfrak{f}_N}$ be the corresponding quotient of the ray class group; the latter is isomorphic to $\mathrm{Gal}(N/E)$ via the Artin map. Since $N = E(\sqrt[n]{U_S}) = E(\sqrt[n]{\varepsilon_0}, \dots, \sqrt[n]{\varepsilon_r})$, the Galois group $\mathrm{Gal}(N/E)$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{r+1}$ via

$$\Phi \colon \sigma \longmapsto (\overline{m}_0, \dots, \overline{m}_r), \text{ where } \sigma(\sqrt[n]{\varepsilon_i}) = \zeta_n^{m_i} \cdot \sqrt[n]{\varepsilon_i} \text{ for } 0 \le i \le r.$$

We therefore get the following commutative diagram:



Since F is the fixed field of $\mathrm{Gal}(N/F) \subseteq \mathrm{Gal}(N/E)$, we want to search for elements $v_1, \dots, v_l \in (\mathbf{Z}/n\mathbf{Z})^{r+1}$ such that $\langle \Phi^{-1}(v_1), \dots, \Phi^{-1}(v_l) \rangle = \mathrm{Gal}(N/F)$, that is, $\langle v_1, \dots, v_l \rangle = \Phi(\mathrm{Gal}(N/F))$. Through diagram chasing, we see that

$$\begin{aligned} \mathrm{Gal}(N/F) = \ker(\pi) = \ker(\psi_{L/K}^{-1} \circ \mathrm{res} \circ \pi) &= \ker(\mathrm{N}_{E/K} \circ \psi_{N/E}^{-1}) \\ &= \psi_{N/E}(\ker(\mathrm{N}_{E/K})) \\ &= \Phi^{-1}(\ker(\Xi)). \end{aligned}$$

Thus it is sufficient to compute the kernel of the $\mathbf{Z}/n\mathbf{Z}$-linear map Ξ. Once we have generators for the kernel, we can read off exponents $n_0, \dots, n_r$ such that $\alpha = \varepsilon_0^{n_0} \cdots \varepsilon_r^{n_r}$ using linear algebra. The following lemma shows that it is not necessary to directly compute the map Ξ in order to find $\ker(\Xi)$ or $\Phi^{-1}(\ker(\Xi))$ respectively.

Lemma 5. *Let T be a finite set of finite primes $\mathfrak{q}$ of E such that $\mathfrak{q}$ does not divide $\mathfrak{f}_N$ and $(\mathrm{Frob}_\mathfrak{q})_{\mathfrak{q}\in T}$ generates $\mathrm{Gal}(N/E)$. For $M = (\Psi(\mathrm{N}_{E/K}([\mathfrak{q}])))_{\mathfrak{q}\in T} \in (\mathbf{Z}/m\mathbf{Z})^{\#T\times 1}$ the following holds: If $v_1, \dots, v_l \in (\mathbf{Z}/n\mathbf{Z})^{\#T}$ generate the right kernel $\ker(M)$, then*

$$\sum_{\mathfrak{q}\in T} v_{i,\mathfrak{q}} \cdot \Phi(\mathrm{Frob}_\mathfrak{q}) \quad 1 \le i \le l,$$

are generators for $\Phi(\mathrm{Gal}(N/F))$.

Remark 6. *This is quite different from the original approach in* [Fie01, Section 3]*. There, an admissible modulus $\mathfrak{f}_N$ was explicitly constructed using bounds due to Hasse* [Has67]*. This was then followed by the computation of a generating set for the kernel $\ker(\mathrm{N}_{E/K}) \subseteq \mathrm{Cl}_{\mathfrak{f}_N}$ and the application of $\psi_{N/E} \circ \Phi$. Since the valuations of $\mathfrak{f}_N$ obtained by Hasse can be very large, the necessary discrete logarithms in the ray class group $\mathrm{Cl}_{\mathfrak{f}_N}$ tended to be quite costly. We circumvent this by avoiding any computation with $\mathrm{Cl}_{\mathfrak{f}_N}$.*

4.3. **Descent to L/K.** Suppose now that we have found $\alpha \in E$ such that $F = E(\sqrt[n]{\alpha})$. We aim at finding a defining equation for L/K. As a first step, we compute $\mu \in F$ such that $F = K(\mu)$. Since $E(\sqrt[n]{\alpha}) = K(\zeta_n, \sqrt[n]{\alpha})$, we can find μ as $\mu = \sqrt[n]{\alpha} + k\zeta_n$ for a suitable $k \in \mathbf{Z}$. Note that k can be found by trying small elements in $\mathbf{Z}$. As the coefficients of the minimal polynomial f_L^μ of μ over L generate the cyclic extension L/K, it is sufficient to determine

$$f_L^\mu = \prod_{\sigma\in\mathrm{Gal}(F/L)} (X - \sigma(\mu)) \in L[X].$$

Hence the problem of finding a defining equation is reduced to the problem of computing an explicit description of $\mathrm{Gal}(F/L)$ on $\sqrt[n]{\alpha}$ and ζ_n. Since F/K is the compositum of E and L, it is abelian with admissible modulus $\mathfrak{f}_F = n\mathcal{O}_K \cap \mathfrak{f}_N$. Denote by $A_{\mathfrak{f}_F}$ the corresponding congruence subgroup of Cl_{f_F}. We have the following commutative diagram

$$\begin{array}{ccccc} & & \overset{\varphi_{F/K}}{\frown} & & \\ I_{\mathfrak{f}_F} & \longrightarrow & \mathrm{Cl}_{\mathfrak{f}_F}/A_{\mathfrak{f}_F} & \xrightarrow{\psi_{F/K}} & \mathrm{Gal}(F/K) \\ & \searrow & \downarrow & & \downarrow \mathrm{res} \\ \mathbf{Z}/n\mathbf{Z} & \xleftarrow[\Psi]{} & \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

First, note that we can easily compute a generating set for $\mathrm{Gal}(F/K)$. As the group $\mathrm{Gal}(E/K) = \mathrm{Gal}(K(\zeta_n)/K)$ is a subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$ and n is a prime power, we can find $r, s \in \mathbf{Z}$ such that $\mathrm{Gal}(E/K)$ is generated by $\zeta_n \mapsto \zeta_n^r$ and $\zeta_n \mapsto \zeta_n^s$. Using [Fie01, Lemma 4.1], we can determine extensions $f, g\colon F \to F$ of both morphisms, which together with $F \to F, \sqrt[n]{\alpha} \mapsto \zeta_n\sqrt[n]{\alpha}$ generate $\mathrm{Gal}(F/K)$. We now need to find $\mathrm{Gal}(F/L) = \ker(\mathrm{res}\colon \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K))$.

5 Jun 2018 07:51:59 PDT
Version 2 - Submitted to Open Book Series

Lemma 7. *Let T be a finite set of finite primes $\mathfrak{q}$ of K such that $\mathfrak{q}$ does not divide $\mathfrak{f}_F$ and $(\mathrm{Frob}_\mathfrak{q})_{\mathfrak{q}\in T}$ generates $\mathrm{Gal}(F/K)$. Let $M = (\Psi([\mathfrak{q}]))_{\mathfrak{q}\in T} \in (\mathbf{Z}/n\mathbf{Z})^{\#T\times 1}$. If $v_1,\dots,v_l \in (\mathbf{Z}/m\mathbf{Z})^{\#T}$ generate the right kernel $\ker(M)$, then*

$$\prod_{\mathfrak{q}\in T} (\mathrm{Frob}_\mathfrak{q})^{v_{i,\mathfrak{q}}} \quad 1 \le i \le l,$$

are generators for $\mathrm{Gal}(F/L)$.

To compute $\mathrm{Frob}_\mathfrak{q}$ in F/K, we can proceed as follows. Since we already know $\mathrm{Gal}(F/K)$, if we pick a prime $\mathfrak{p}$ of F lying over $\mathfrak{q}$, we can find $\mathrm{Frob}_\mathfrak{q}$ as the unique $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(\zeta_n) \equiv \zeta_n^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{q}$ and $\sigma(\sqrt[n]{\alpha}) \equiv (\sqrt[n]{\alpha})^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{q}$.

Remark 8. *If $n = \ell$ is prime, even fewer steps are necessary. Since $[K(\zeta_n) : K]$ is a divisor of $\ell - 1$, it is coprime to ℓ and thus $\mathrm{Gal}(F/L)$ is the unique subgroup of $\mathrm{Gal}(F/K)$ of order ℓ. If f is the lift of a generator of $\mathrm{Gal}(K(\zeta_n)/K)$ to $\mathrm{Gal}(F/K)$, then f^ℓ will be a generator of $\mathrm{Gal}(F/L)$.*

Remark 9. *In* [Fie01, Section 4]*, the set $\mathrm{Gal}(F/L)$ is also computed as the kernel of the restriction map* res: $\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$*. More precisely, $\mathrm{Gal}(F/L)$ is computed as the image of $\ker(\iota\colon \mathrm{Cl}_{\mathfrak{f}_F} \to \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}))$ under $\psi_{F/K}$. This is a costly operation due to discrete logarithms in ray class groups. In our approach this is circumvented by the use of the Artin map on sufficiently many prime ideals.*

4.4. **Reduction of generators.** In the computation of a defining polynomial of the class field, we find a generator of a Kummer extension. Depending on the situation, this is either the final result or this computation is followed by the descent. To improve the overall performance, it is beneficial to find a "small" generator for the Kummer extension. More precisely, let K be an algebraic number field; given $\alpha \in K^\times$, we want to find a "small" representative for $\alpha \cdot K^{\times n}$, that is, we want to find $\beta \in K^\times$ such that $\beta^n \cdot \alpha$ is "small". To this end, we will describe how to compute a so-called compact representation

$$\alpha = \alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}$$

with small elements $\alpha_i \in \mathcal{O}_K$. Once we have found this, α_0 will be a small representative in the coset of α modulo $K^{\times n}$.

Note that the notion of compact representations was used in [Thi95] in connection with the computation of units and principal ideal generators. Here we give a different algorithm for computing it. As the value of the presented algorithms comes from the practicality, we will refrain from giving precise statements about the size of the objects. Note that it is possible to obtain rigorous estimates using Remark 11 and 13.

The first step of a compact representation is a reduction at the finite places. We let $\alpha\mathcal{O}_K = \prod_{i=1}^l \mathfrak{p}_i^{n_i}$ be the prime ideal factorization of $\alpha\mathcal{O}_K$ and set $N = \max_i n_i$.

Algorithm 10. *Let $k = \lfloor \log_n(N) \rfloor$. The following steps return small (with respect to the T_2-norm) elements $\alpha_0,\dots,\alpha_k$ and $\mathfrak{a}$ of small norm with*

$$\alpha\mathcal{O}_K = (\alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}) \cdot \mathfrak{a}.$$

(1) *Define $\mathfrak{a}_{k+1} = 1$.*

(2) *For $j = k,\dots,0$ define $\mathfrak{b}_j = \prod_{i=1}^l \mathfrak{p}_i^{\lfloor (n_i \bmod n^{j+1})/n^j \rfloor}$.*

(3) *For* $j = k, \dots, 0$ *find* $\alpha_j \in (\mathfrak{a}_{j+1}^n \mathfrak{b}_j)^{-1}$ *such that the ideal* $\mathfrak{a}_j := \alpha_j^{-1} \mathfrak{a}_{j+1}^n \mathfrak{b}_j$ *has small norm.*
(4) *Return* $\alpha_0, \dots, \alpha_k$ *and* $\mathfrak{a} = \mathfrak{a}_0$.

Remark 11. *Finding* α_j *in Step (1) and (3) is the well known problem of finding small representatives in ideal classes. The solution involves computing a small basis of the inverse ideal using a lattice reduction. In case one uses LLL reduction (*[LLL82]*), the ideals* $\mathfrak{a}_j$ *will have a small norm bounded by* $O(2^{d^2}\sqrt{|d_K|})$ *(see also* [BFH17, 4.3]*).*

We now assume that we have an element $\alpha \in \mathcal{O}_K$ such that $|\mathrm{N}(\alpha)|$ is small and for which we want to compute a compact representation. To do so, we need the following notion. Let $\mathfrak{b}$ be a non-zero integral ideal of $\mathcal{O}_K$. We define

$$\lfloor \sqrt[n]{\mathfrak{b}} \rfloor = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(\mathfrak{b})}{n} \rfloor},$$

to be the n-th root of $\mathfrak{b}$. Here the product runs over all non-zero prime ideals of $\mathcal{O}_K$. Note that $\lfloor \sqrt[n]{\mathfrak{b}} \rfloor$ is an integral ideal such that $\lfloor \sqrt[n]{\mathfrak{b}} \rfloor^n$ divides $\mathfrak{b}$.

Let $\sigma_1, \dots, \sigma_d \colon K \to \mathbf{C}$ be the complex embeddings of K. For an element $v = (v_i)_{1 \le i \le d} \in \mathbf{R}^d$ we denote $\max_{1 \le i \le n} |v_i|$ by $\|v\|_\infty$. Recall that the $T_{2,v}$-norm is defined to be $T_{2,v}(\beta) = \sum_{i=1}^d v_i^2 |\sigma_i(\alpha)|^2$ for $\beta \in K$.

Algorithm 12 (Compact representation for elements of small norm)**.** *Let* $\alpha \in \mathcal{O}_K$ *with* $|\mathrm{N}(\alpha)|$ *small. The following steps return small elements* $\alpha_0, \dots, \alpha_k$ *such that*

$$\alpha = \alpha_0 \alpha_1^n \alpha_2^{n^2} \cdots \alpha_k^{n^k}.$$

(1) *Define* $v = (v_j)_{1 \le j \le d} = (\log(|\sigma_j(\alpha)|))_{1 \le j \le d} \in \mathbf{R}^d$, $k = \lfloor \log_n(\|v\|_\infty) \rfloor$ *so that* $n^k \le \|v\|_\infty \le n^{k+1}$. *We set* $\tilde{\alpha}_{k+1} = \alpha$.
(2) *For* $i = k, \dots, 1$, *we set* $w = (\exp(n^{-i} v_j))_{1 \le j \le d}$ *and then compute* $\mathfrak{b}_i = \lfloor \sqrt[n^i]{\tilde{\alpha}_{i+1} \mathcal{O}_K} \rfloor$. *Next, use lattice reduction to find an element* $\gamma_i \in \mathfrak{b}_i^{-1}$ *which is small with respect to* $T_{2,w}$, *set* $\alpha_i = \gamma_i^{-1}$ *and* $\tilde{\alpha}_i = \tilde{\alpha}_{i+1} \cdot \gamma_i^{n^i}$.
(3) *Define* $\alpha_0 = \tilde{\alpha}_1$ *and return* $\alpha_0, \dots, \alpha_k$.

Remark 13. *The size of the elements* $\gamma_1, \dots, \gamma_k$ *of the algorithm is bounded in* T_2*-norm in terms of* n *and* $\sqrt{d_{K/\mathbf{Q}}}$. *Assume that we are in the* i*-th iteration of the algorithm; using the same notations as in Algorithm 12, the element* $\gamma_i \in \mathfrak{b}_i^{-1}$ *obtained by the LLL-algorithm has small* $T_{2,w}$*-norm:*

$$T_{2,w}(\gamma_i) \le C \Big(d_{K/\mathbf{Q}}^{\frac{1}{2}} N(\mathfrak{b}_i)^{-1} \prod_{j=1}^d w_j \Big)^{\frac{2}{d}} \le C \Big(d_{K/\mathbf{Q}}^{\frac{1}{2}} N(\alpha)^{\frac{1}{n^i}} \Big)^{\frac{2}{d}},$$

where C *is the explicit constant of the reduction algorithm and the last inequality comes from the fact that* $(N(\mathfrak{b}_i)^{-1} \prod_{j=1}^d w_j)^{n^i} = N(\alpha) N(\mathfrak{b}_i)^{-n^i}$ *is integral, hence bounded by* $N(\alpha)$. *Clearly,* $\alpha \gamma_i^{n^i} \in \mathcal{O}_K$ *and we have the following bound on its size:*

$$\begin{aligned} T_2(\alpha \gamma_i^{n^i}) &= \sum_{s=1}^d \Big(w_s^{-2n^i} |\sigma_s(\alpha)|^2 \Big) \Big(w_s^{2n^i} |\sigma_s(\gamma_i^{n^i})|^2 \Big) = \sum_{s=1}^d w_s^{2n^i} |\sigma_s(\gamma_i^{n^i})^2| \\ &\le \Big(\sum_{s=1}^d w_s^2 |\sigma_s(\gamma_i)|^2 \Big)^{n^i} = T_{2,w}(\gamma_i)^{n^i} \le C^{n^i} N(\alpha)^{\frac{2}{d}} d_{K/\mathbf{Q}}^{\frac{n^i}{d}}. \end{aligned}$$

Thus

$$\|v\|_\infty \leq \log T_2(\alpha\gamma_i^{n^i}) \leq n^i \log\left(CN(\alpha)^{2/d} d_{K/\mathbf{Q}}^{1/d}\right).$$

Now, $w_i^{-1} = \exp(-n^{-i}v_i) \leq \exp(n^{-i}\|v\|_\infty) \leq CN(\alpha)^{2/l} d_{K/\mathbf{Q}}^{1/d}$ *and*

$$T_2(\gamma_i) \quad = \quad \sum_{s=1}^{d} w_s^{-2} w_s^2 |\sigma_s(\gamma_i)|^2 \leq \|w^{-1}\|_2^2 T_{2,w}(\gamma_k) \leq dC^3 d_{K/\mathbf{Q}}^{3/d} N(\alpha)^{\frac{4}{d}+\frac{2}{dn^i}}$$

is bounded as well.

Summarizing, to reduce an element $\alpha \in K$ modulo $K^{\times n}$, we first apply Algorithm 10 to obtain $\alpha_0, \ldots \alpha_k \in K$ and an ideal $\mathfrak{a}$ of bounded norm such that $\alpha\mathcal{O}_K = (\alpha_0\alpha_1^n\alpha_2^{n^2}\cdots\alpha_k^{n^k})\cdot\mathfrak{a}$. Thus the element $\tilde{\alpha}$ defined by

$$\tilde{\alpha} = \alpha(\alpha_0^{-1}\alpha_1^{-n}\cdots\alpha_k^{-n^k})$$

is an element of small norm. This is followed by an application of Algorithm 12 to $\tilde{\alpha}$, which yields $\tilde{\alpha}_0, \ldots, \tilde{\alpha}_l$ with

$$\tilde{\alpha} = \tilde{\alpha}_0\tilde{\alpha}_1^n\cdots\tilde{\alpha}_k^{n^k}.$$

Since

$$\alpha = \prod_{i=0}^{\max(k,l)} (\alpha_i\tilde{\alpha}_i)^{n^i},$$

(where we set $\alpha_i = 1$ and $\tilde{\alpha}_i = 1$ for $i > k$ and $i > l$ respectively), we see that $\alpha \equiv \alpha_0\tilde{\alpha}_0 \bmod K^{\times n}$. By construction, $\alpha_0\tilde{\alpha}_0$ is a small element.

4.5. **Computation of Galois groups.** Let L/K be an abelian extension of degree n, for which we have computed a polynomial $f \in K[X]$ with $L \cong K[X]/(f)$. Denote by $\gamma \in L$ a root of f in L. Our aim is to show how to compute $\mathrm{Gal}(L/K)$ using the objects which showed up during the computation of the defining polynomial f. By computing $\mathrm{Gal}(L/K)$, we mean the computation of the image of γ under the elements of $\mathrm{Gal}(L/K)$. As in Section 4 we may assume that L/K is cyclic. Recall that $F = L(\zeta_n) = K(\zeta_n)(\sqrt[n]{\beta}) = E(\sqrt[n]{\beta})$. By Galois theory, we know that the restriction $\mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)$ is an isomorphism. Moreover, since F/E is a Kummer extension with generator $\sqrt[n]{\beta}$, we have that

$$\mathrm{Gal}(F/E) = \langle \sigma\colon F \to F\colon \sqrt[n]{\beta} \mapsto \zeta_n\sqrt[n]{\beta}\rangle.$$

In particular, $\sigma|_L$ is a generator of $\mathrm{Gal}(L/K)$ and $a_0, \ldots, a_{n-1} \in K$ with

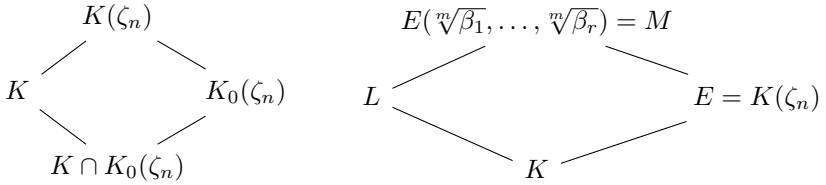
$$\sigma|_L(\gamma) = \sigma(\gamma) = \sum_{i=0}^{n-1} a_i\gamma^i$$

can be found using linear algebra.

Assume that K/K_0 and L/K_0 are normal extensions; this occurs frequently when constructing towers of normal extensions with more than two layers. In this case, it makes sense to compute for the "absolute" Galois group $\mathrm{Gal}(L/K_0)$. The naive way of computing $\mathrm{Gal}(L/K_0)$ would be to write L/K_0 as a simple extension and to find the roots of the defining polynomial. While this works well for small degrees, it quickly becomes unfeasible.

Alternatively, note that $\mathrm{Gal}(L/K_0) = \langle\sigma_1, \ldots, \sigma_r, \mathrm{Gal}(L/K)\rangle$, where $\sigma_1, \ldots, \sigma_r$ are extension of generators of $\mathrm{Gal}(K/K_0)$ to L. By the first part, we know how to compute generators of $\mathrm{Gal}(L/K)$, thus it is sufficient to show how to extend

an automorphism $\sigma \in \mathrm{Gal}(K/K_0)$ to an automorphism of $\mathrm{Gal}(L/K_0)$. Let ℓ be a prime dividing $[L : K]$ and denote by L_ℓ/K the largest subextension such that $[L : L_\ell]$ is coprime to ℓ. As $\mathrm{Gal}(L_\ell/K)$ is isomorphic to the ℓ-Sylow subgroup of $\mathrm{Gal}(L/K)$, also L_ℓ/K_0 is normal. Since L/K is the compositum of the linear disjoint L_ℓ/K, where ℓ divides $[L : K]$, we may assume that $L = L_\ell$ is an abelian ℓ-extension of K. In particular, L itself is the compositum of linear disjoint cyclic extensions $L_i = K(\gamma_i)$ of prime power degree ℓ^{m_i}. Recall that we have constructed the extension L_i/K by passing to the Kummer extension $L_i(\zeta_{\ell^{m_i}})/K(\zeta_{\ell^{m_i}})$, for which we computed an element $\beta_i \in K(\zeta_{\ell^{m_i}})$ with $L_i(\zeta_{\ell^{m_i}}) = K(\zeta_{\ell^{m_i}}, \sqrt[m_i]{\beta_i})$. For simplicity we assume that $m_i = m$ for all $i = 1, \dots, r$ and set $n = \ell^m$, $E = K(\zeta_n)$. We have the following lattices of number fields:



The idea is to extend $\sigma \in \mathrm{Gal}(K/K_0)$ to an automorphism of $M = E(\sqrt[n]{\beta_1}, \dots, \sqrt[n]{\beta_r})$ and then to restrict this to L. As the first step, we extend σ to $K(\zeta_n)$. Denote by K_1 the intersection $K_0(\zeta_n) \cap K$. Then $K(\zeta_n)/K_1$ is the compositum of the linear disjoint extensions K/K_1 and $K_0(\zeta_n)/K_1$. Thus it is straightforward to extend σ to an automorphism of $K(\zeta_n)$, which we also denote by σ.

In the next step, we extend σ to an automorphism $\hat{\sigma}$ of M by determining $\hat{\sigma}(\sqrt[n]{\beta_i})$ for all $i = 1, \dots, r$, using the Frobenius automorphisms. We now fix $i \in \{1, \dots, r\}$. Since M/E is a Kummer extension, there exist unique $1 \leq n_j \leq n$ and $\mu \in K(\zeta_n)$ such that

$$\hat{\sigma}(\sqrt[n]{\beta_i}) = \mu \cdot (\sqrt[n]{\beta_1})^{n_1} (\sqrt[n]{\beta_2})^{n_2} \cdots (\sqrt[n]{\beta_r})^{n_r}. \tag{2}$$

Our aim is to determine the n_j as well as μ. As $\hat{\sigma}$ extends σ, we may assume that $\hat{\sigma}(\sqrt[n]{\beta_i}) = \sqrt[n]{\sigma(\beta_i)}$. For a finite prime $\mathfrak{p}$ of E, unramified in M/E, there exist $e_\mathfrak{p}$, $e_{\mathfrak{p},1}, \dots, e_{\mathfrak{p},r} \in \mathbf{Z}/n\mathbf{Z}$ such that

$$\mathrm{Frob}_{\mathfrak{p},M/E}(\sqrt[n]{\beta_j}) = \mathrm{Frob}_{\mathfrak{p},E(\sqrt[n]{\beta_j})/E}(\zeta_n^{e_{\mathfrak{p},j}} \sqrt[n]{\beta_j}),$$
$$\mathrm{Frob}_{\mathfrak{p},M/E}(\sqrt[n]{\sigma(\beta_i)}) = \mathrm{Frob}_{\mathfrak{p},E(\sqrt[n]{\sigma(\beta_i)})/E}(\sqrt[n]{\sigma(\beta_i)}) = \zeta_n^{e_\mathfrak{p}} \sqrt[n]{\sigma(\beta_i)}.$$

Since $\mathrm{Frob}_{\mathfrak{p},M/E}(\mu) = \mu$, applying $\mathrm{Frob}_{\mathfrak{p},M/E}$ on (2) yields

$$\zeta_n^{e_\mathfrak{p}} = \zeta_n^{n_1 e_{\mathfrak{p},1}} \cdots \zeta_n^{n_r e_{\mathfrak{p},r}} \quad \text{that is,} \quad 0 = e_\mathfrak{p} - \sum_{i=1}^{r} n_i e_{\mathfrak{p},i} \text{ in } \mathbf{Z}/n\mathbf{Z}.$$

Thus, for each prime we get a linear equation over $\mathbf{Z}/n\mathbf{Z}$ of which $n_1, \dots, n_r$ is a solution. Since $\mathrm{Gal}(M/E)$ is generated by $\mathrm{Frob}_{\mathfrak{p},M/E}$, $\mathfrak{p}$ a finite prime of K, we know that for sufficiently many primes $(n_1, \dots, n_r)$ will be the unique solution of the simultaneous equations. Hence we can use Proposition 4 to compute $n_1, \dots, n_r$. Once this is done, we can recover μ by extracting an n-th root of

$$\frac{\sigma(\beta_i)}{\beta_1^{n_1} \cdots \beta_r^{n_r}} = \mu^n.$$

5. Invariant Subgroups

5.1. **Normal extensions.** Let K be a number field which is normal over the base field K_0 with Galois group $G = \mathrm{Gal}(K/K_0)$. In this section we describe how to compute abelian extensions of K, which are also normal over K_0.

The action of G on K extends to an action on the places of K and, in particular, on the set of moduli of K. Let $\mathfrak{m}$ be a modulus which is invariant under the action of G, that is, $\sigma(\mathfrak{m}) = \mathfrak{m}$ for every $\sigma \in G$. In this case G acts on the ray class group $\mathrm{Cl}_\mathfrak{m}$ by sending $[I]$ to $[\sigma(I)]$.

Remark 14. *Let L be an abelian extension of K with conductor $\mathfrak{m}$ and let $\sigma\colon L \to \overline{\mathbf{Q}}$ be an embedding. Then $\sigma(\mathfrak{m})$ is the conductor of $\sigma(L)$ over $\sigma(K)$. To see this it is enough to consider the compositum of the Artin map with σ.*

Proposition 15. *Let $\mathfrak{m}$ be a modulus of K which is invariant under the action of G. Every subgroup H of $\mathrm{Cl}_\mathfrak{m}$ which is invariant under the action of G corresponds to an abelian extension L/K, such that L/K_0 is normal. Conversely, let L be an abelian extension of K which is normal over K_0. Then the conductor $\mathfrak{f}$ of L/K as well as the corresponding congruence subgroup are invariant under the action of G.*

Proof. Firstly, we prove that if $\mathfrak{m}$ is an invariant modulus, the statement is true for $H = \{1\}$ and the corresponding extension L. Let σ be an embedding of L into $\overline{\mathbf{Q}}$ such that $\sigma|_{K_0} = \mathrm{id}$. Then $\sigma(K) = K$ since K is normal over K_0 and $\sigma(L)$ is an abelian extension of K with admissible modulus $\sigma(\mathfrak{m})$. As $\sigma(\mathfrak{m}) = \mathfrak{m}$, we get $\sigma(L) \subseteq L$ and thus L/K_0 is normal.

Now, let H be an invariant subgroup of $\mathrm{Cl}_\mathfrak{m}$ corresponding to an extension L and let F be the ray class field corresponding to $\{1\} < \mathrm{Cl}_\mathfrak{m}$. We want to show that L is normal over K_0, or, equivalently, that $\mathrm{Gal}(F/L)$ is normal in $\mathrm{Gal}(F/K_0)$. In this setting, we have the exact sequence

$$1 \to \mathrm{Gal}(F/K) \longrightarrow \mathrm{Gal}(F/K_0) \longrightarrow \mathrm{Gal}(K/K_0) \to 1$$

In particular, $\mathrm{Gal}(F/K_0)$ is generated by a set of generators of $\mathrm{Gal}(F/K)$ and preimages of generators of $\mathrm{Gal}(K/K_0)$. Obviously, $\mathrm{Gal}(F/L)$ is invariant under conjugation by elements of $\mathrm{Gal}(F/K)$ in $\mathrm{Gal}(F/K_0)$ since F/K is abelian. By the properties of the Artin map, $\mathrm{Cl}_\mathfrak{m} \simeq \mathrm{Gal}(F/K)$ and the action of G on $\mathrm{Cl}_\mathfrak{m}$ corresponds to conjugation in the group $\mathrm{Gal}(F/K_0)$. Since H is invariant, this means that $\mathrm{Gal}(F/L)$ is invariant under conjugation by generators of $\mathrm{Gal}(K/K_0)$ and therefore it is a normal subgroup.

On the other hand, let L be an abelian extension of K which is normal over K_0. The conductor being invariant follows from the observation above. Furthermore, we know that the field L corresponding to $\{1\} < \mathrm{Cl}_\mathfrak{f}$ is normal over K_0. Since L is normal, it corresponds to a normal subgroup of $\mathrm{Gal}(F/K_0)$, so it is invariant under conjugation by elements of this group. By the properties of the Artin map, the action of $\mathrm{Gal}(K/K_0)$ on $\mathrm{Gal}(F/K)$ is given by conjugation in $\mathrm{Gal}(F/K_0)$. Since L is normal, the corresponding subgroup is invariant. □

Consequently, if we are searching for abelian extensions of K which are also normal over K_0, we can restrict to invariant subgroups of the ray class groups.

5.2. **Computing invariant subgroups.** Let M be a finite abelian group of exponent n and G a finite group acting on M. We now describe how to compute the set of all G-invariant subgroups of M. While one could of course first compute the

set of all subgroups of M using a theorem of Butler [But94], the following example shows that this is in general not a useful approach.

Example 16. *We consider the abelian group $M = (\mathbf{Z}/25\mathbf{Z})^{11}$ with the symmetric group $G = S_{11}$ acting via $\sigma(a_1, \ldots, a_{11}) = (a_{\sigma(1)}, \ldots, a_{\sigma(11)})$ for $\sigma \in S_{11}$ and $(a_1, \ldots, a_{11}) \in M$. Then the number of subgroups of M with quotient isomorphic to $\mathbf{Z}/25\mathbf{Z}$ is* 119209287109375*, while only one of these subgroups is invariant.*

Denote by $\mathbf{Z}[G]$ the integral group ring of G. Since G-invariant subgroups of M are the same as $\mathbf{Z}[G]$-submodules of M and $n\mathbf{Z}$ acts trivially on M, it is sufficient to determine the $(\mathbf{Z}/n\mathbf{Z})[G]$-submodules of M.

By induction, it is enough to find all the irreducible $(\mathbf{Z}/n\mathbf{Z})[G]$-submodules of M. Since this task can be easily solved in case the exponent n of M is a prime number using the Meataxe (see [Par84] and [HEO05, Section 7.4]), we will focus on the non-prime case. As usual we can assume that the exponent n is a prime power: Indeed, for every prime number q dividing the order of M, the q-Sylow subgroup of M is invariant and they generate the whole group M. This means that every simple $(\mathbf{Z}/n\mathbf{Z})[G]$-submodule of M must be contained in one of the Sylow subgroups of M. As the q-Sylow subgroup of M is naturally a $(\mathbf{Z}/q^{v_q(n)}\mathbf{Z})[G]$-module, we may assume that $n = p^s$ is a prime power.

Proposition 17. *Let N be a simple $(\mathbf{Z}/p^s\mathbf{Z})[G]$-module. Then the exponent of N is p.*

Thus all minimal submodules are contained in the submodule $M_p = \{m \in M \mid pm = 0\}$, which is naturally an $\mathbf{F}_p[G]$-module. Thus to find the $(\mathbf{Z}/p^s\mathbf{Z})[G]$-submodules, we just have to apply the method for the prime case and iterate. In particular, we have an efficient algorithm to determine the G-invariant subgroups of an abelian group M.

Remark 18. *Assume we want to compute only G-invariant subgroups N of M such that the quotient M/N has exponent m. As mM itself is G-invariant, the group G also acts on M/mM and the G-invariant subgroups of M with quotient of exponent m correspond to the G-invariant subgroups of M/mM. In the situation where $M = \mathrm{Cl}_\mathfrak{m}$ is the ray class group, this implies that again it is sufficient to only compute the quotient $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^m$ instead of the whole ray class group.*

5.3. **Duality.** While the previous section provides a solution to the problem of finding G-invariant subgroups of M, it can be very inefficient if we are looking only for subgroups N with small index in M, since it can be necessary to repeat the procedure for finding minimal submodules multiple times.

In this case, we can use duality to translate the problem of finding submodules of small index into the one of finding submodules of small order. Recall that the dual group M^* of M is the group $\mathrm{Hom}_\mathbf{Z}(M, \mathbf{Z}/p^s\mathbf{Z})$, which is isomorphic to M. In practice, an isomorphism can be written explicitly after a choice of a basis. In our case, we assume that M has exponent p^s and is given in Smith normal form, that is, $M = \mathbf{Z}/p^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_w}\mathbf{Z}$ with $1 \leq n_1 \leq \cdots \leq n_w = s$. Let $e_1, \ldots, e_w$ be the canonical generators of M. Then we define elements of the dual

$$e_i^* \colon M \longrightarrow \mathbf{Z}/p^s\mathbf{Z}, \quad e_j \longmapsto \delta_{ij}\frac{p^s}{\mathrm{ord}(e_i)},$$

where δ_{ij} is the Kronecker delta and $\mathrm{ord}(e_i)$ denotes the order of e_i. The dual is again in Smith normal form with respect to this generating set.

Recall that every endomorphism φ of M induces a dual morphism

$$\varphi^*\colon M^* \longrightarrow M^*, \quad f \longmapsto f \circ \varphi.$$

In particular every element $g \in G$ acts on M^*, endowing M^* with the structure of a $(\mathbf{Z}/p^s\mathbf{Z})[G]$-module. The action of G on the dual group just defined preserves the inclusion-reversing correspondence existing between subgroups of M and subgroups of M^*. Given a subgroup H of M, define the orthogonal complement of H as

$$H^\perp = \{\varphi \in M^* \mid H \subseteq \ker(\varphi)\}.$$

Proposition 19. *There is an inclusion-reversing bijection between submodules of M and M^*:*

$$\begin{array}{ccc} \{(\mathbf{Z}/p^s\mathbf{Z})[G]\text{-submodules of } M\} & \longrightarrow & \{(\mathbf{Z}/p^s\mathbf{Z})[G]\text{-submodules of } M^*\}, \\ H & \longmapsto & H^\perp. \end{array}$$

Furthermore, for every submodule H of M, we have $H^\perp \simeq G/H$.

Thus if we want to search for submodules of small index, we can instead search for submodules of the dual module of small order and then use duality. In order to make this computationally effective, we need to understand how to obtain the action on the dual group M^* given the one on the group M. As above, we assume that M is given in Smith normal form with generators e_i and we consider the corresponding element of the dual e_i^*. Let $\varphi \in \mathrm{Aut}(M)$ be the automorphism of M induced by $g \in G$. We want to compute the matrix $A = (a_{ij})$ associated to φ^* with respect to the basis e_i^*. Note that by definition, $\varphi^*(e_i^*) = e_i^* \circ \varphi$. Let B be the matrix representing φ with respect to the elements e_i and let d_i be the valuation of the order of e_i at p . Then

$$\varphi^*(e_i^*)(e_j) = e_i^*(\varphi(e_j)) = e_i^*\Big(\sum_k b_{jk}e_k\Big) = b_{ji}e_i^*(e_i) = b_{ji}p^{s-d_i}.$$

On the other hand,

$$\varphi^*(e_i^*)(e_j) = \Big(\sum_k a_{ik}e_k^*\Big)(e_j) = a_{ij}e_j^*(e_j) = a_{ij}p^{s-d_j}.$$

Therefore, it is enough to choose a_{ij} satisfying the relation $a_{ij}p^{s-d_j} = b_{ji}p^{s-d_i}$.

6. Application: Fields with minimal discriminant

The algorithms outlined in the previous sections have been implemented in the number theory package Hecke [FHHJ17][1]. As an application, we used our implementation to find number fields K having Galois closure L over $\mathbf{Q}$ with prescribed Galois group and such that K has minimal discriminant among the fields with this property. We chose to consider the following cases:

- K of degree 15 with $\mathrm{Gal}(L/\mathbf{Q}) \simeq D_{15}$ and signature $(1, 7)$,
- K of degree 15 with $\mathrm{Gal}(L/\mathbf{Q}) \simeq D_5 \times C_3$ and signature $(3, 6)$,
- K of degree 15 with $\mathrm{Gal}(L/\mathbf{Q}) \simeq S_3 \times C_5$ and signature $(5, 5)$,
- K of degree 36 with $\mathrm{Gal}(L/\mathbf{Q}) \simeq C_9 \rtimes C_4$ and signatures $(36, 0)$, $(0, 18)$.

The computation took 12 hours on an Intel i7-4790 with 3.6 GHz. The results of the computation are given in Theorem 1.

[1]Available at `https://github.com/thofma/Hecke.jl`

6.1. **Nonnormal degree** 15 **extensions.** In this section, we consider number fields K of degree 15 over $\mathbf{Q}$ having Galois closure L over $\mathbf{Q}$ with Galois group $\mathrm{Gal}(L/\mathbf{Q}) \cong G \in \{D_{15}, D_5 \times C_3, S_3 \times C_5\}$. Our strategy is to compute the normal closure L (of degree 30) of K and then use the trace and norm to find the corresponding field K (as in Section 4.3). Since G has a normal cyclic subgroup of degree 15, we can construct L as a relative cyclic extension of degree 15 over a quadratic field F_2. A crucial point is the choice for bound on the discriminant of the Galois closure L given a bound on the field K of degree 15. Since L is the compositum of F_2 and K we have $d_{L/\mathbf{Q}} \leq d_{F_2/\mathbf{Q}}^{15} \cdot d_{K/\mathbf{Q}}^2$. Thus, we need to find a bound for the field F_2 given the one on K. For this, we have to distinguish the cases corresponding to the different groups.

- If $G = D_{15}$, we can apply [Coh00, Theorem 9.2.6] to obtain the bound $d_{F_2/\mathbf{Q}} \leq d_{K/\mathbf{Q}}^{1/7}$.
- If $G = D_5 \times C_3$, then K has an intermediate subfield K_1 of degree 5 and $d_{K_1/\mathbf{Q}} \leq d_{K/\mathbf{Q}}^{1/3}$ by the behaviour of the discriminant in towers of extensions. Now, the Galois closure of K_1 has Galois group D_5 and so we apply again [Coh00, Theorem 9.2.6] to obtain $d_{F_2/\mathbf{Q}} \leq d_{K_1/\mathbf{Q}}^{1/2} \leq d_{K/\mathbf{Q}}^{1/6}$.
- If $G = S_3 \times C_5$, we use the same strategy as in the case of $D_5 \times C_3$. Here K has an intermediate subfield K_1 of degree 3 whose Galois closure is an S_3-extension of $\mathbf{Q}$ and $d_{K_1/\mathbf{Q}} \leq d_{K/\mathbf{Q}}^{1/5}$. Therefore $d_{F_2/\mathbf{Q}} \leq d_{K_1/\mathbf{Q}} \leq d_{K/\mathbf{Q}}^{1/5}$.

Thus, we need to list the imaginary quadratic fields up to these bounds, since we are searching for fields K with non-real embeddings. By Proposition 15, the possible conductors are invariant under the action of the Galois group of F_2. For every possible conductor $\mathfrak{m}$, we need to search for invariant subgroups of index 15 in the group $R = \mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^{15}$. Before computing the defining equation, we check that the action of G on the quotient by any subgroup corresponds to the correct group extension. More precisely, let H be a congruence subgroup of $\mathrm{Cl}_{\mathfrak{m}}$ and let σ be the generator of $\mathrm{Gal}(F_2/\mathbf{Q})$. Then:

- for the D_{15}-extensions, σ must send every element of $\mathrm{Cl}_{\mathfrak{m}}/H$ to its inverse;
- for the $D_5 \times C_3$-extensions, σ must fix the 3-Sylow subgroup of $\mathrm{Cl}_{\mathfrak{m}}/H$ and act on the 5-Sylow by sending every element to its inverse;
- for the $S_3 \times C_5$-extensions, σ must fix the 5-Sylow subgroup of $\mathrm{Cl}_{\mathfrak{m}}/H$ and act on the 3-Sylow by sending every element to its inverse.

6.2. **Degree** 36 **extensions.** For $G = C_9 \rtimes C_4$, we construct these fields as a tower of a degree 4 normal field and a degree 9 field on top of it. In this example, the tools we developed in the previous sections are fundamental, since we are dealing with extensions having non-squarefree degree.

References

[BFH17] Jean-François Biasse, Claus Fieker, and Tommy Hofmann, *On the computation of the HNF of a module over the ring of integers of a number field*, J. Symbolic Comput. **80** (2017), no. part 3, 581–615.

[But94] Lynne M. Butler, *Subgroup lattices and symmetric functions*, Mem. Amer. Math. Soc. **112** (1994), no. 539, vi+160.

[CDyDO96] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Computing ray class groups, conductors and discriminants*, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 49–57.

[CDyDO98] ———, *Computing ray class groups, conductors and discriminants*, Math. Comp. **67** (1998), no. 222, 773–795.

[Coh99] Henri Cohen, *A survey of computational class field theory*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 1–13, Les XXèmes Journées Arithmétiques (Limoges, 1997).

[Coh00] ———, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[CS08] Henri Cohen and Peter Stevenhagen, *Computational class field theory*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 497–534.

[DP95] Mario Daberkow and Michael E. Pohst, *Computations with relative extensions of number fields with an application to the construction of Hilbert class fields*, Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ISSAC '95, Montreal, Canada, July 10–12, 1995, ACM Press, New York, NY, 1995, pp. 68–76.

[DP98] ———, *On the computation of Hilbert class fields*, J. Number Theory **69** (1998), no. 2, 213–230.

[FHHJ17] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson, *Nemo/Hecke: computer algebra and number theory packages for the Julia programming language*, ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2017, pp. 157–164.

[Fie01] Claus Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303.

[Has64] Helmut Hasse, *Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante - 47*, Acta Arithmetica **9** (1964), no. 4, 419–434.

[Has67] ———, *Vorlesungen über Klassenkörpertheorie*, Thesaurus Mathematicae, Band 6, Physica-Verlag, Würzburg, 1967.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.

[Jan96] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[KM01] Jürgen Klüners and Gunter Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196.

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534.

[Par84] Richard A. Parker, *The computer calculation of modular characters (the meataxe)*, Computational group theory (Durham, 1982), Academic Press, London, 1984, pp. 267–274.

[Poh99] Michael E. Pohst, *From class groups to class fields*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 103–119.

[Thi95] Christoph Thiel, *On the complexity of some problems in algorithmic algebraic number theory*, Ph.D. thesis, Universität des Saarlandes, 1995.

Claus Fieker, Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

E-mail address: fieker@mathematik.uni-kl.de

Tommy Hofmann, Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

E-mail address: thofmann@mathematik.uni-kl.de

Carlo Sircana, Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

E-mail address: sircana@mathematik.uni-kl.de

FAST MULTIQUADRATIC S-UNIT COMPUTATION AND APPLICATION TO THE CALCULATION OF CLASS GROUPS

JEAN-FRANÇOIS BIASSE AND CHRISTINE VAN VREDENDAAL

ABSTRACT. Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a real multiquadratic field and S be a set of prime ideals of L that does not contain any divisors of 2. In this paper, we present a heuristic algorithm for the computation of the S-class group and the S-unit group that runs in time $\text{Poly}(\log(\Delta), \text{Size}(S))e^{\tilde{O}(\sqrt{\ln d})}$ where $d = \max_{i \leq n} d_i$ and Δ is the discriminant of L. We use this method to compute the ideal class group of the maximal order $\mathcal{O}_L$ of L in time $\text{Poly}(\log(\Delta))e^{\tilde{O}(\sqrt{\log d})}$. When $\log(d) \leq \log(\log(\Delta))^c$ for some constant $c < 2$, these methods run in polynomial time. We implemented our algorithm using Sage 7.5.1.

1. INTRODUCTION

Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a real multiquadratic number field, and S be a set of prime ideals of L. The S-unit group U_S of L is the set of elements $\alpha \in L$ such that there is $\vec{e} \in \mathbb{Z}^{|S|}$ satisfying $\alpha\mathcal{O}_L = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}}$ where $\mathcal{O}_L$ is the maximal order of L. The computation of the S-unit group is a fundamental problem in computational number theory with many applications.

In this paper, we present an original algorithm for the computation of certain S-unit groups in real multiquadratic fields. The main motivation for the development of this algorithm is the computation of the ideal class group of $\mathcal{O}_L$. The computation of $\text{Cl}(\mathcal{O}_L)$ can be trivially deduced from the knowledge of an S-unit group where the classes of the elements of S generate $\text{Cl}(\mathcal{O}_L)$. The computation of the ideal class group is one of the four major tasks in computational number theory postulated by Zassenhaus [23, p. 2] (together with the computation of the unit group, the Galois group and the ring of integers). In 1968, Shanks [25, 26] proposed an algorithm relying on the baby-step giant-step method to compute the class number and the regulator of a quadratic number field in time $O\left(|\Delta|^{1/4+\epsilon}\right)$, or $O\left(|\Delta|^{1/5+\epsilon}\right)$ under the extended Riemann hypothesis [22]. Then, a subexponential strategy for the computation of the group structure of the class group of an imaginary quadratic field was described in 1989 by Hafner and McCurley [21]. The expected running time of this method is

$$L_\Delta(1/2, \sqrt{2} + o(1)) = e^{\left(\sqrt{2}+o(1)\right)\sqrt{\ln|\Delta| \ln\ln|\Delta|}}.$$

Buchmann [15] generalized this result to the case of infinite classes of number fields with fixed degree. Practical improvements to Buchmann's algorithm were presented in [19] by Cohen, Diaz Y Diaz and Olivier. Biasse [5] described an algorithm for computing the ideal class group and the unit group of $\mathcal{O} = \mathbb{Z}[\theta]$ in heuristic complexity bounded by $L_\Delta(1/3, c)$ for some $c > 0$ valid in certain classes of number

This work was supported by NIST under grant 60NANB17D184 and by the Simons Foundation under grant 430128.

fields. In [6, 9], Biasse and Fieker showed that there was a heuristic subexponential algorithm for the computation of the ideal class group in all classes of number fields. The methods of [9] can be specialized to the case of cyclotomic fields for a better asymptotic complexity [7]. The computation of the ideal class group is also the subject of study in the context of quantum computing. It was recently proved (under the GRH) by Biasse and Song that there is a quantum polynomial time algorithm for the computation of the ideal class group of an arbitrary field [13]. The most efficient practical implementations of algorithms for the computation of the ideal class group are either based on the quadratic sieve [12, 4, 11, 10] for quadratic fields and on the number field sieve [8] for number fields of higher degree.

The computation of S-units is also instrumental in the resolution of norm equations [27]. Indeed, it is the bottleneck of the resolution in x of $\mathcal{N}_{L/K}(x) = a$ for a given $a \in K$ where L/K is a Galois extension. This computational problem is closely related to Hilbert's 10th problem, for which there is no efficient *general* solution.

Contributions. Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a real multiquadratic number field, and S be a set of prime ideals of L that does not contain any ideals above 2. We define $d = \max_{i \leq n} d_i$ and $\Delta = \mathrm{disc}(L)$.

- We describe an algorithm for the computation of $\mathrm{Cl}(\mathcal{O}_L)$ in heuristic complexity $\mathrm{Poly}(\log(\Delta))e^{\tilde{O}(\sqrt{\log d})}$.
- We describe a heuristic algorithm for the computation of the S-class group and the S-unit group of L in time $\mathrm{Poly}(\log(\Delta), \mathrm{Size}(S))e^{\tilde{O}(\sqrt{\log d})}$.
- We report on the performance of an implementation of our algorithms.

Our recursive approach is based on the unit group computation of [3] which we extended to the more general problem of the computation of the S-unit group. In the case where d is small compared to Δ, our method for computing class groups, S-class groups and S-unit groups runs in heuristic polynomial time in $\log(\Delta)$ (and in the size of S) where $\log(x)$ is the bit size of the integer x. This is ensured when $\log(d) \leq \log(\log(\Delta))^c$ for some constant $c < 2$. For example, this is the case when the d_i are the first n consecutive primes. This is the first non-quantum algorithm that runs in polynomial time on infinite classes of number fields. The main ingredient of our recursion strategy is not restricted to multiquadratic fields. We can take advantage of computations in subfields whenever there are two different $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ of order two. General subfields might not enjoy the same general recursive structure as multiquadratic fields, but we expect that the reduction to the computation in subfields will improve the performance of class group algorithms. The application of these methods to more general fields was left for future work.

2. Preliminaries

2.1. **Number fields.** A number field K is a finite extension of $\mathbb{Q}$. Its ring of integers $\mathcal{O}_K$ has the structure of a lattice of degree $n = [K : \mathbb{Q}]$. A number field has $r_1 \leq n$ real embeddings $(\sigma_i)_{i \leq r_1}$ and $2r_2$ complex embeddings $(\sigma_i)_{r_1 < i \leq 2r_2}$ (coming as r_2 pairs of conjugates). The pair (r_1, r_2) is the signature of K. The field K is isomorphic to $\mathcal{O}_K \otimes \mathbb{Q}$. The norm of an element $x \in K$ is defined by $\mathcal{N}(x) = \prod_i \sigma_i(x)$. Let $(\alpha_i)_{i \leq n}$ such that $\mathcal{O}_K = \oplus_i \mathbb{Z}\alpha_i$, then the discriminant of K is $\Delta(K) := \det^2(T_2(\alpha_i, \alpha_j))$, where T_2 is defined by $T_2(x, x') := \sum_i \sigma_i(x)\overline{\sigma_i}(x')$. When there is no ambiguity, we simply denote it by Δ.

2.2. **Units of $\mathcal{O}_K$.** Elements $u \in \mathcal{O}_K$ that are invertible in $\mathcal{O}_K$ are called units. Equivalently, they are the elements $u \in K$ such that $(u) := (u)\mathcal{O}_K = \mathcal{O}_K$. The unit group of $\mathcal{O}_K$ where K is a real multiquadratic field has rank $r = n - 1$ and has the form $\mathcal{O}_K^* = \mu \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle$ where μ are roots of unity (torsion units) and the ϵ_i are non-torsion units. Such $(\epsilon_i)_{i \leq r}$ are called a system of fundamental units of $\mathcal{O}_K$. Units generate a lattice $\mathcal{L}$ of rank r in $\mathbb{R}^{r+1}$ via the embedding $x \in K \longmapsto \mathrm{Log}(x) := (\ln(|\sigma_1(x)|), \cdots, \ln(|\sigma_{r+1}(x)|))$. The volume R of $\mathcal{L}$ is an invariant of K called the regulator. The regulator R and the class number h satisfy $hR = \frac{|\mu|\sqrt{|\Delta|}}{2^{r_1}(2\pi)^{r_2}} \lim_{s \to 1} ((s-1)\zeta_K(s))$, where $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^s}$ is the usual ζ-function associated to K and $|\mu|$ is the cardinality of μ the group of torsion units. This allows us to derive a bound h^* in polynomial time under GRH that satisfies $h^* \leq hR < 2h^*$ ([2]).

2.3. **Multiquadratic fields.** In this paper, we focus on towers of quadratic extensions.

Definition 2.1. *Let $d_1, \ldots, d_n$ be squarefree integers that are multiplicatively independent modulo squares (i.e. they are independent in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$). Then $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ is called a multiquadratic field and $N := [L : \mathbb{Q}] = 2^n$. Its Galois group* $\mathrm{Gal}(L/\mathbb{Q}) := \{$*Automorphisms of L that fix $\mathbb{Q}\}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$.*

When $n = 1$, the field $L = \mathbb{Q}(\sqrt{d_1})$ is simply called a quadratic field. In this paper, we focus on real multiquadratic fields, that is, those that satisfy $\forall i \leq n,\ d_i > 0$. The discriminant of a real multiquadratic field is given to us by an explicit formula. This is useful for the computation of its maximal order.

Lemma 2.2. *Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ a multiquadratic field as given above and $\prod_{j=1}^{s} p_j^{m_j}$ with $p_1 < p_2 < \ldots < p_s$ be the factorization of $\prod_{i=1}^{n} d_i$. Then $\Delta(L) = (2^a p_1 \cdot p_2 \cdots p_s)^{2^{n-1}}$ where*

$$a = \begin{cases} 0 & d_i \equiv 1 \bmod 4\ (\forall\ 1 \leq i \leq n) \\ 2 & p_1 = 2 \text{ and } p_i \equiv 1 \bmod 4\ (\forall\ 2 \leq i \leq n) \text{ or} \\ & p_1 \neq 2 \text{ and } \exists\ i \text{ s.t. } p_i \equiv 3 \bmod 4 \\ 3 & \text{otherwise} \end{cases}$$

Proof. This follows from Theorem 2.1 of [24]. □

If we take $d_1, d_2, \ldots, d_n$ to be the first n primes, then their product is the primorial $p_n\# \approx e^{(1+o(1))n \log n}$. Combining this with Lemma 2.2 gives $\ln \Delta(L) \approx \frac{1}{2} N n \log n = \frac{1}{2} N \log N \log\log N$.

2.4. **Class groups.** Elements of the form $\frac{\mathfrak{I}}{d}$ where $\mathfrak{I} \subseteq \mathcal{O}_K$ is an ideal of the ring of integers of K and $d > 0$ are called fractional ideals. Ideals of $\mathcal{O}_K$ are also referred to as integral ideals. Fractional ideals have the structure of a $\mathbb{Z}$-lattice of degree $n = [K : \mathbb{Q}]$, and they form a multiplicative group $\mathcal{I}$. Elements of $\mathcal{I}$ admit a unique decomposition as a product of non-zero prime ideals of $\mathcal{O}_K$ (with possibly negative exponents). The norm of integral ideals is given by $\mathcal{N}(\mathfrak{I}) := [\mathcal{O}_K : \mathfrak{I}]$, which extends to fractional ideals by $\mathcal{N}(\mathfrak{I}/\mathfrak{J}) := \mathcal{N}(\mathfrak{I})/\mathcal{N}(\mathfrak{J})$. The norm of a principal (fractional) ideal agrees with the norm of its generator $\mathcal{N}(x\mathcal{O}_K) = |\mathcal{N}(x)|$. The principal fractional ideals $\mathcal{P}$ of K are a subgroup of $\mathcal{I}$ and the ideal class group of $\mathcal{O}_K$ is defined by $\mathrm{Cl}(\mathcal{O}_K) := \mathcal{I}/\mathcal{P}$. We denote by $[\mathfrak{a}]$ the class of a fractional $\mathfrak{a}$ in

$\mathrm{Cl}(\mathcal{O}_K)$ and by h the cardinality of $\mathrm{Cl}(\mathcal{O}_K)$ which is a finite group. Let $\mathfrak{a}, \mathfrak{b}$ be two fractional ideals of K. We have $[\mathfrak{a}] = [\mathfrak{b}]$ if and only if there is $\alpha \in K$ such that $\mathfrak{a} = (\alpha)\mathfrak{b}$. We also denote this property by $\mathfrak{a} \sim \mathfrak{b}$.

2.5. **How to compute class groups.** The best asymptotic algorithms to compute the ideal class group of $\mathcal{O}_K$ follow the general framework deriving from the algorithm of Hafner and McCurley [21] (subsequently generalized by Buchmann [15] and Biasse-Fieker [9]). Let $B > 0$ be a bound and define a factor base as $\mathcal{B} := \{\text{non-zero prime ideals } \mathfrak{p} \text{ with } \mathcal{N}(\mathfrak{p}) \leq B\}$. We refer to B as the *smoothness bound*. We compute a generating set of the lattice Λ of all the vectors $(e_1, \cdots, e_m) \in \mathbb{Z}^m$ with $m := |\mathcal{B}|$ such that $\exists \alpha \in K, \quad (\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$.

Definition 2.3 (relations)**.** *Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be a set of non-zero prime ideals of K. For each S-unit $\alpha \in K$ with $\vec{e} = (e_1, \ldots, e_s)$ such that $(\alpha) = \prod_i \mathfrak{p}_i^{e_i}$, we define the relation associated with α by $\mathcal{R}_{S,K}(\alpha) := (\alpha, \vec{e})$ The relations of K for the set S form a group denoted by $\mathcal{R}el_S(K)$.*

When $B > 12 \ln^2 |\Delta|$, the classes of ideals in $\mathcal{B}$ generate $\mathrm{Cl}(\mathcal{O}_K)$ under the GRH [1, Th. 4]. Therefore, $(\mathcal{B}, \Lambda)$ is a presentation of the group $\mathrm{Cl}(\mathcal{O}_K)$ and the search for a generating set of the relations $\mathcal{R}el_S(K)$ for $S = \mathcal{B}$ is equivalent to computing the group structure of $\mathrm{Cl}(\mathcal{O}_K)$. Indeed, the morphism

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{\varphi} & \mathcal{I} & \xrightarrow{\pi} & \mathrm{Cl}(\mathcal{O}_K) \\ (e_1, \ldots, e_m) & \longrightarrow & \prod_i \mathfrak{p}_i^{e_i} & \longrightarrow & \prod_i [\mathfrak{p}_i]^{e_i} \end{array},$$

is surjective, and the class group $\mathrm{Cl}(\mathcal{O}_K)$ is isomorphic to $\mathbb{Z}^m / \ker(\pi \circ \varphi) = \mathbb{Z}^m / \Lambda$.

2.6. **S-class groups and S-unit groups.** Let $S = \{\mathfrak{p}_1, \cdots \mathfrak{p}_s\}$ be a finite set of prime ideals of the number field K. We say that $x \in K$ is an S-integer if $v_{\mathfrak{p}}(x) \geq 0$ for all $\mathfrak{p} \notin S$. The set of S-integers is a ring denoted by $\mathcal{O}_{K,S}$. We define the S-unit group $U_{K,S}$ (or U_S if the field of definition is understood) as the elements $x \in K$ such that $v_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. The group of S-units is finitely generated: $U_S = \mu(K) \times \langle \eta_1 \rangle \times \cdots \langle \eta_{r+s} \rangle$ where $\mu(K)$ is the set of the roots of unity of K, and $\eta_1, \ldots, \eta_{s+r}$ are torsion free generators. The rank of its torsion-free part equals $r + s$ where r is the rank of the torsion free part of the unit group U_K. Let $\mathcal{I}_S$ be the group of fractional ideals of $\mathcal{O}_{K,S}$, and $\mathcal{P}_S$ its subgroup of principal ideals. We define the S-class group by $\mathrm{Cl}_S(\mathcal{O}_{K,S}) = \mathcal{I}_S / \mathcal{P}_S$.

3. S-units of quadratic fields

In this section, we assume that $L = \mathbb{Q}(\sqrt{d})$ for $d > 0$ a squarefree integer. The calculation of the S-unit group for S a set of prime ideals of L is done by using the approach of Simon [27, Sec. I.1.2]. Together with the subexponential strategy for computing the ideal class group derived from the Hafner-McCurley algorithm [21], the S-unit group of L can be computed in time $\mathrm{Poly}(\mathrm{Size}(S)) \cdot e^{\tilde{O}(\sqrt{\log d})}$. These algorithms have been extensively studied, in particular in [21, 15, 9, 27]. Therefore, we only give a brief sketch of the algorithm and will focus on the run time and the format of the output.

3.1. **Computing the class group.** First, let $B \in e^{\tilde{O}(\sqrt{\log d})}$ be a large enough smoothness bound such that the non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of L with norm less than B generate $\mathrm{Cl}(\mathcal{O}_L)$. Note that $k \in e^{\tilde{O}(\sqrt{\log d})}$. The computation of $\mathrm{Cl}(\mathcal{O}_L)$ starts with the collection of $\delta_1, \ldots, \delta_l$ for some $l \in \tilde{O}(k)$ such that for all $i \leq l$ there exist $(a_{i,1}, \ldots, a_{i,k})$ with $(\delta_i) = \prod_j \mathfrak{p}_j^{a_{i,j}}$. The δ_i and the $a_{i,j}$ are all polynomial size in $\log(d)$. Then there are unimodular matrices $U \in \mathrm{GL}_l(\mathbb{Z})$ and $V \in \mathrm{GL}_k(\mathbb{Z})$ such that

$$\mathrm{SNF}(A) = UAV = \left(\begin{array}{ccc} d_1 & & (0) \\ & \ddots & \\ (0) & & d_k \\ \hline & (0) & \end{array}\right),$$

where $\mathrm{SNF}(A)$ denotes the Smith Normal Form of A. The unimodular matrices U, V can be found in polynomial time [28] (in the dimension and the bit size of the entries of A), and their entries have polynomial size in the dimension of A and the bit size of its coefficients. This means that $\log(|U|), \log(|V|) \in e^{\tilde{O}(\sqrt{\log d})}$ where $|U|$ denotes a bound on the absolute values of the entries of U. Let $\mathcal{L} \subseteq \mathbb{Z}^k$ be the lattice generated by the rows of A. Then $\mathrm{Cl}(\mathcal{O}_L) \simeq \mathbb{Z}^k/\mathcal{L} \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_k\mathbb{Z}$. Let $\mathfrak{g}_j := \prod_{i \leq k} \mathfrak{p}_i^{v_{i,j}}$, we have $\mathrm{Cl}(\mathcal{O}_L) \simeq \langle [\mathfrak{g}_1] \rangle \times \ldots \times \langle [\mathfrak{g}_k] \rangle$. In addition, let $\beta_i := \prod_{j \leq l} \delta_j^{u_{i,j}}$, for $i \leq k$. We do not evaluate this product. We have $\mathfrak{g}_i^{d_i} = (\beta_i)$. Overall, the complexity of this calculation is in $e^{\tilde{O}(\sqrt{\log d})}$.

3.2. **Computing the S-unit group.** Let S be a set of primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ of L. To get the S-class group and the S-unit group we add extra relations to $\mathcal{L}$. More specifically, we need to identify the classes of $\mathrm{Cl}(\mathcal{O}_L)$ that are represented by a product of primes in S with the trivial class of $\mathrm{Cl}_S(\mathcal{O}_{L,S})$. The ideal class of each of the elements of S can be represented as a product of the classes of the $\mathfrak{g}_i$. In time $e^{\tilde{O}(\sqrt{\log d})}$ (and polynomial in $\log(\mathcal{N}(\mathfrak{q}_i))$), one can find polynomial size $x_1, \cdots, x_k$ and $\beta_{i+k} \in L$ such that $\mathfrak{q}_i = (\beta_{i+k}) \prod_j \mathfrak{p}_j^{x_j}$ with standard methods derived from [21]. Then for each j, $\mathfrak{p}_j = \prod_{i \leq k} \mathfrak{g}_i^{v'_{i,j}}$ where the $v'_{i,j}$ are the coefficients of V^{-1}, we readily find vectors $\vec{e}_i \in \mathbb{Z}^k$ with entries having polynomial size in k (that is in $e^{\tilde{O}(\sqrt{\log d})}$) such that $\mathfrak{q}_i = (\beta_{i+k}) \prod_{j \leq k} \mathfrak{g}_j^{e_{i,j}}$. The vectors $\vec{e}_i$ are precisely the new additions needed to expand $\mathcal{L}$. We get a new relation matrix

$$B = \left(\begin{array}{ccc} d_1 & & (0) \\ & \ddots & \\ (0) & & d_k \\ \hline & & \\ e_{1,1} & \ldots & e_{1,k} \\ \vdots & & \vdots \\ e_{s,1} & \ldots & e_{s,k} \end{array}\right).$$

As for the computation of $\mathrm{Cl}(\mathcal{O}_L)$, the SNF of B gives the elementary divisors of the cyclic decomposition of $\mathrm{Cl}_S(\mathcal{O}_{K,S})$. Meanwhile, let $\vec{w}_1, \cdots, \vec{w}_{1+s}$ be a basis for the left kernel of B (in general the dimension is $r+s$ where r is the rank of the unit group of L). This kernel is found in polynomial time in the dimension of B and the size of its entries, that is in time $\mathrm{Poly}(s) \cdot e^{\tilde{O}(\sqrt{\log d})}$. The entries of the kernel

vectors have size in $\text{Poly}(s) \cdot e^{\tilde{O}(\sqrt{\log d})}$, and $U_S = \mu \times \langle \gamma_1 \rangle \times \ldots \times \langle \gamma_{1+s} \rangle$ where $\mu = \{\pm 1\}$ are the torsion units of $\mathcal{O}_L$ and $\gamma_i := \prod_{j \leq k+s} \delta_j^{w_{i,j}}$.

Proposition 3.1. *Let $d > 0$ be a squarefree integer, $L = \mathbb{Q}(\sqrt{d})$ and S be a set of prime ideals of L with $|S| = s$. Then the S-unit group algorithm of* [27, Sec. I.1.2] *returns $l \in e^{\tilde{O}(\sqrt{\log d})}$ polynomial size elements $\delta_i \in L$ and $s+1$ vectors $\vec{c}_i$ with entries of size in $Poly(s) \cdot e^{\tilde{O}(\sqrt{\log d})}$ such that the $s+1$ elements $\gamma_i := \prod_{j \leq l} \delta_j^{c_{i,j}}$ generate the S-unit group of L. The overall complexity of this procedure is in $Poly(Size(S)) \cdot e^{\tilde{O}(\sqrt{\log d})}$ where the size of S is in $O(s \cdot \max_{\mathfrak{p} \in S} \log(\mathcal{N}(\mathfrak{p})))$.*

4. Recursive computation of S-units

Let S be a set of non-zero prime ideals in L that is invariant under the action of $\text{Gal}(L/\mathbb{Q})$ (that is, $\forall \mathfrak{p} \in S, \forall \sigma \in \text{Gal}(L/\mathbb{Q}), \mathfrak{p}^\sigma \in S$). In this section, we introduce a recursive method for finding a generating set of $\mathcal{R}el_S(L)$ which is the group of elements of the form $\mathcal{R}_{S,L}(\alpha) = (\alpha, \vec{e})$ such that $(\alpha) = \prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{e_i}$. Our strategy consists in deriving the S-unit group in L from that of three subfields of L. When we reach the leaves of this recursion tree, we use the methods of Section 3 for computing the S-unit group directly on the quadratic field.

4.1. High level description of the algorithms.

Let L be a multiquadratic number field and let σ, τ be two distinct non-trivial automorphisms of L. Let $\sigma\tau := \sigma \circ \tau$ and K_ℓ be the subfield of L fixed by $\ell \in \{\sigma, \tau, \sigma\tau\}$. Let S be a set of prime ideals of the ring of integers $\mathcal{O}_L$ of L stable by the action of $\text{Gal}(L/\mathbb{Q})$, and for each $\ell \in \{\sigma, \tau, \sigma\tau\}$ let us define $S_\ell := \{\mathfrak{p} \cap K_\ell \mid \mathfrak{p} \in S\}$. We recover a generating set of $\mathcal{R}el_S(L)$ from generating sets of $\mathcal{R}el_{S_\sigma}(K_\sigma)$, $\mathcal{R}el_{S_\tau}(K_\tau)$, and $\sigma(\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau}))$. Our result follows from two crucial observations:

(1) The subgroup U of $\mathcal{R}el_S(L)$ generated by the lifts of $\mathcal{R}el_{S_\sigma}(K_\sigma)$, $\mathcal{R}el_{S_\tau}(K_\tau)$, and $\sigma(\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau}))$ contains all the squares of relations in $\mathcal{R}el_S(L)$.
(2) There is an algorithm that efficiently produces elements of U that are square of relations in $\mathcal{R}el_S(L)$, and then computes their square root.

When the recursive tree reaches a quadratic subfield K_ℓ of L, it uses the subexponential algorithm of Simon [27, Sec. I.1.2] to return the S_ℓ-unit group. The high level description of this strategy is summarized in Algorithm 4.1. Note that the ring of integers $\mathcal{O}_L$ is part of the input. In general, the computation of $\mathcal{O}_L$ is as hard as the factorization of the discriminant of L, but in the particular case of multiquadratic fields, there is an efficient algorithm for this task [18].

4.2. Lifting relations.

To compute $\mathcal{R}el_S(L)$, we use relations from $\mathcal{R}el_{S_\sigma}(K_\sigma)$, $\mathcal{R}el_{S_\tau}(K_\tau)$, and $\sigma(\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau}))$ where $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$ and S_ℓ, K_ℓ are defined in Section 4.1. Therefore, given relations in a subfield K_σ of L, we need to be able to efficiently compute the corresponding relations in L.

Theorem 4.1. *Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a multiquadratic field. Let K_σ be the (multi)-quadratic subfield of L fixed by $\sigma \in \text{Gal}(L/\mathbb{Q})$, $S_\sigma = \{\mathfrak{p}_i\}_{i \leq s}$ where $\mathfrak{p}_i$ are prime ideals of K_σ, and $S = \{\mathfrak{P}_k \subset L \mid \exists i \leq s,\ \mathfrak{P}_k \cap K_\sigma = \mathfrak{p}_i\}$. Let $\mathcal{R}_{S_\sigma, K_\sigma}(\alpha) = (\alpha, \vec{e})$ be a relation in $\mathcal{R}el_{S_\sigma}(K_\sigma)$. Then $(\alpha, \vec{e}_L) := \mathcal{R}_{S,L}(\alpha) \in \mathcal{R}el_S(L)$ with $\vec{e}_L = (e_1\vec{f_1} | e_2\vec{f_2} | \ldots | e_s\vec{f_s})$, where $\vec{f_i}$ satisfy $\mathfrak{p}_i\mathcal{O}_L = \prod_{j \leq g_i} \mathfrak{P}_{k_{i,j}}^{f_{i,j}}$.*

Algorithm 4.1: High level description of recursive S-unit computation of L

Input: Real multiquadratic field L, ring of integers $\mathcal{O}_L$ of L, set of primes S of $\mathcal{O}_L$ stable under the action of $\mathrm{Gal}(L/\mathbb{Q})$

Result: A basis for $\mathcal{R}el_S(L)$.

```
if [L : Q] = 2 then
    Use the method of [27, Sec. I.1.2] to compute a basis Λ of Rel_S(L)
    return Λ
σ, τ ← distinct non-identity automorphisms of L
for ℓ ∈ {σ, τ, στ} do
    K_ℓ ← fixed field of ℓ
    Λ_ℓ ← basis of Rel_{S_ℓ}(K_ℓ)
Λ ← Λ_σ ∪ Λ_τ ∪ σ(Λ_στ)
Find a basis Λ_2 of the lattice of relations generated by Λ that are squares.
Λ_2 ← square roots of the elements in Λ_2.
Λ ← basis of the lattice generated by Λ ∪ Λ_2.
return Λ
```

Proof. Let $\alpha \in K_\sigma$ such that $(\alpha) = \prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{e_i}$. Each prime ideal $\mathfrak{p}_i \in K_\sigma$ factors as $\mathfrak{p}_i \mathcal{O}_L = \prod_{j \le g_i} \mathfrak{P}_{k_{i,j}}^{f_{i,j}}$, where the $\mathfrak{P}_{k_{i,j}}$ are the prime ideals of L such that $\mathfrak{P}_{k_{i,j}} \cap K_\sigma = \mathfrak{p}_i$ and the $f_{i,j}$ are the corresponding ramification indices. Therefore, we have

$$(\alpha)\mathcal{O}_L = \prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{e_i} \mathcal{O}_L = \prod_{\mathfrak{p}_i \in S} \prod_{j \le g_i} \mathfrak{P}_{k_{i,j}}^{e_i f_{i,j}}.$$

Thus $(\alpha, (e_1 \vec{f_1} | e_2 \vec{f_2} | \dots | e_s \vec{f_s}))$ is the relation corresponding to α in $\mathcal{R}el_S(L)$. □

Given the straightforward correspondence between $\mathcal{R}_{S_\sigma, K_\sigma}(\alpha) \in \mathcal{R}el_S(K_\sigma)$ and its lift in $\mathcal{R}el_S(L)$, we identify these two elements. The set $\mathcal{R}el_S(L)$ is also equipped with a natural group structure given by $(\alpha_1, \vec{e}_1) + (\alpha_2, \vec{e}_2) := (\alpha_1 \cdot \alpha_2, \vec{e}_1 + \vec{e}_2)$. We define the index of a subgroup U of $\mathcal{R}el_S(L)$ as that of the subgroup of U_S of the α such that there exists $\vec{e}$ with $(\alpha, \vec{e}) \in U$.

Lemma 4.2. *Let $L = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$ be a multiquadratic field and let S be a set of prime ideals of L that is invariant under the action of $\mathrm{Gal}(L/\mathbb{Q})$. Let $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ be two different non-identity isomorphisms, and define S_ℓ, K_ℓ of $\ell \in \{\sigma, \tau, \sigma\tau\}$ as in Section 4.1. Let U be the group generated by $\mathcal{R}el_{S_\sigma}(K_\sigma) \cup \mathcal{R}el_{S_\tau}(K_\tau) \cup \sigma(\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau}))$ where*

$$\sigma(\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau})) := \{\mathcal{R}_{S_\tau, K_\tau}(\sigma(\alpha)) \mid \exists \vec{e},\ (\alpha, \vec{e}) \in \mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau})\}$$

Then $(\mathcal{R}el_S(L))^2 \subseteq U \subseteq \mathcal{R}el_S(L)$, where $(\mathcal{R}el_S(L))^2$ denotes the relations of the form $(\alpha^2, 2\vec{e})$ where $(\alpha, \vec{e}) \in \mathcal{R}el_S(L)$.

Proof. From Theorem 4.1, we know that the relations in $\mathcal{R}el_{S_\sigma}(K_\sigma)$, $\mathcal{R}el_{S_\tau}(K_\tau)$ and $\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau})$ lift naturally to relations in $\mathcal{R}el_S(L)$. Moreover, σ maps elements of $K_{\sigma\tau}$ to K_τ, and since S is invariant under the action of σ, a relation is mapped to another relation (modulo a permutation of the coeficients of the exponent vector). So the action of σ on $\mathcal{R}el_{S_{\sigma\tau}}(K_{\sigma\tau})$ is well defined, and $U \subseteq \mathcal{R}el_S(L)$.

For the other inclusion, let $(\alpha, \vec{e}) \in \mathcal{R}el_S(L)$. For each $\ell \in \{\sigma, \tau, \sigma\tau\}$, $\alpha \cdot \ell(\alpha)$ decomposes as a product of ideals in S_ℓ. Therefore, there are vectors $\vec{e}_\ell$ such that

for each ℓ, $(\alpha \cdot \ell(\alpha), \vec{e}_\ell) \in \mathcal{R}el_{S_\ell}(K_\ell)$. Moreover,

$$\frac{\mathcal{N}_{L:K_\sigma}(\alpha)\mathcal{N}_{L:K_\tau}(\alpha)}{\sigma(\mathcal{N}_{L:K_{\sigma\tau}}(\alpha))} = \frac{\alpha \cdot \sigma(\alpha) \cdot \alpha \cdot \tau(\alpha)}{\sigma(\alpha \cdot \sigma\tau(\alpha))} = \alpha^2,$$

hence $(\alpha^2, 2\vec{e}) = (\sigma(\alpha), \vec{e}_\sigma) + (\tau(\alpha), \vec{e}_\tau) - \sigma((\sigma\tau)(\alpha), \vec{e}_{\sigma\tau})$ is a linear combination of relations in $\mathcal{R}el(K_\sigma), \mathcal{R}el(K_\tau)$ and $\sigma(\mathcal{R}el(K_{\sigma\tau}))$, so $(\mathcal{R}el(L))^2 \subseteq U$. □

4.3. **Representation of elements and square roots.** The lifting U of the relations in three different subfields yield a set of relations containing all the squares of the relations in $\mathcal{R}el_S(L)$. We need to solve two tasks:

(1) Identification of a generating set of the squares of U.
(2) For each square $(\alpha^2, 2\vec{e})$ found in (1): computation of $(\alpha, \vec{e})$.

***p*-th roots with saturation**. Let us identify $U \subseteq \mathcal{R}el_S(L)$ with the elements $\alpha \in U_S$ such that $\exists \vec{e}$, $(\alpha, \vec{e}) \in U$. Let $b > 0$ such that $(U_S : U) = b$. For any prime $p|b$ there is some $\alpha \in U_S \setminus U$ such that $\alpha^p \in U$. The saturation technique of Biasse and Fieker [8] can be used to find elements in U_S that are not in U. Let us fix the prime p. For any residue degree 1 prime ideal $\mathfrak{Q} \notin S$ with $Q := \mathcal{N}(\mathfrak{Q})$ such that $p|Q-1$ we define the map $\phi_\mathfrak{Q} : U \to \mathbb{F}_Q^*/(\mathbb{F}_Q^*)^p$ mapping S-units into the multiplicative group of the residue class field $\mathbb{F}_Q := \mathcal{O}_L/\mathfrak{Q}$ modulo p-th powers. The Cebotarev theorem [17] guarantees that if $\alpha \in U$ is not a p-th power, there will be some $\mathfrak{Q}$ such that $\phi_\mathfrak{Q}(\alpha)$ is non-trivial, i.e. α is not a p-th power modulo Q. To find p-th powers, we now simply intersect $\ker \phi_\mathfrak{Q}$ for sufficiently many $\mathfrak{Q}$. The elements $\alpha \in U/\left(\cap \ker \phi_\mathfrak{Q}\right)$ will have a p-th root in U_S but not in U. Suppose $(\alpha, \vec{e}) \in U$ with $\alpha \in U/\left(\cap \ker \phi_\mathfrak{Q}\right)$, then $(\sqrt[p]{\alpha}, \vec{e}/p)$ is a new relation that reduces the index of the lattice of currently found relations in $\mathcal{R}el_S(L)$.

Using quadratic characters for $p = 2$. When looking for square roots, we can use quadratic characters to find elements in elements $\alpha \in U/\left(\cap \ker \phi_\mathfrak{Q}\right)$ by following the approach of [3]. More specifically, in [3, Sec. 4.1], the map

$$\phi_\mathfrak{Q} : \mathbb{Z}[x_1, \ldots, x_n]/(x_1^2 - d_1, \ldots, x_n^2 - d_n) \simeq \mathbb{Z}\left[\sqrt{d_1}, \ldots, \sqrt{d_n}\right] \longrightarrow \mathbb{F}_Q,$$

where $\mathfrak{Q}$ is a residue degree 1 prime ideal and $Q = \mathcal{N}(\mathfrak{Q})$, is defined by $x_i \mapsto s_i$ where s_i is a square root of d_i modulo Q. Elements of U_S have non-negative valuation at $\mathfrak{Q}$ since it satisfies $\mathfrak{Q} \notin S$. We can use the characters defined in [3, Sec. 4.1] by $\chi_\mathfrak{Q}(\alpha) := \left(\frac{\phi_\mathfrak{Q}(\alpha)}{Q}\right) \in \{-1, 0, 1\}$. When α is a square, we have $\chi_\mathfrak{Q}(\alpha) = 1$. To find squares, we find the $\alpha \in U$ such that $\chi_{\mathfrak{Q}_i}(\alpha) = 1$ for $i \leq m$ where m is large enough. This boils down to the search for a kernel element of the linear map

$$\begin{array}{ccc} U_S & \xrightarrow{X} & \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z} \\ \alpha & \longrightarrow & \left(\log_{-1}\left(\chi_{\mathfrak{Q}_1}(\alpha)\right), \ldots, \log_{-1}\left(\chi_{\mathfrak{Q}_m}(\alpha)\right)\right) \end{array},$$

where for each $x \in \{-1, 1\}$, $\log_{-1}(x)$ denotes the discrete logarithm of x in base -1. If α is a square, then necessarily $X(\alpha) = (0, \ldots, 0)$. On the other hand, if $X(\alpha) = (0, \ldots, 0)$, there is a non-zero probability that α might not be a square. Given generators $\alpha_1, \cdots, \alpha_k$ of U, we can find a generating set of the squares of elements of U_S. This contains the squares of elements $\alpha_{k+1}, \ldots, \alpha_{k+l}$ of U_S such that $\alpha_1, \ldots, \alpha_{k+l}$ generate U_S. We obtain these squares by finding the kernel of the matrix $A = (X(\alpha_i)) \in \mathbb{Z}^{k \times m}$.

Representation of the elements. We compute S-units in the quadratic fields by directly applying the subexponential algorithm of [27, Sec. I.1.2]. As we saw in Section 3, the output of the computation in each quadratic field $K_l := \mathbb{Q}(\sqrt{d_l})$ for $l \leq 2^n := N$ is a set of $s+1$ elements γ_i that are represented by vectors of exponents $\vec{e}_i$ and k elements α_j such that $\gamma_i = \prod_{j \leq k} \delta_j^{e_{i,j}}$. The δ_j have polynomial size in $\log(d_i)$, while $k \in e^{\tilde{O}(\sqrt{\log(d_l)})}$ and the entries of $\vec{e}_i$ have size in $\mathrm{Poly}(s) \cdot e^{\tilde{O}(\sqrt{\log(d_l)})}$. In our algorithm these products are never evaluated in L. By linearity, one can evaluate $X(\gamma_i) = \sum_{j \leq k} e_{i,j} X(\delta_j)$ in time $k \cdot \mathrm{Poly}(\max_{i,j} \mathrm{Size}(e_{i,j})) \cdot \mathrm{Poly}(\max_i \mathrm{Size}(X(\delta_j)))$. As $\mathrm{Size}(X(\delta_j))$ is bounded by $m \cdot \max_i \log(\mathcal{N}(\mathfrak{Q}_i))$, the resulting complexity is in $\mathrm{Poly}(s, m, \log Q) \cdot e^{\tilde{O}\left(\sqrt{\log(d)}\right)}$ where $Q := \max_i \mathcal{N}(\mathfrak{Q}_i)$ and $d := \max_l d_l$.

When working in a subfield K of L of degree $N_\iota = 2^\iota$ for $2 \leq \iota \leq n$, we represent the elements $\alpha \in U_{K,S}$ as products of the γ_i^σ for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and $i \leq (s+1)N_\iota$ where $\gamma_{j+1}, \cdots, \gamma_{j+(s+1)}$ generate the S-unit group of the j-th quadratic subfield. Each lifting involves square roots. We do not evaluate the product of the γ_i, nor the square roots. To represent $\alpha \in U_{K,S}$, we use the vector $\vec{c} \in \mathbb{Z}^{N_\iota}$ such that $\alpha = \left(\prod_{i,\sigma} (\gamma_i^\sigma)^{c_i^\sigma}\right)^{\frac{1}{2^{\iota-1}}}$. Under this representation, the product of two elements, the image under a morphism $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and the computation of the square root are straightforward operations with complexity in $\mathrm{Poly}(s, N, C) \cdot e^{\tilde{O}\left(\sqrt{\log(d)}\right)}$ where C is an upper bound on the size of the coefficients of the exponent vectors $\vec{c}$. On the other hand, it is more delicate to compute $X(\alpha)$. For each $\mathfrak{Q}_i$, we can compute $\phi_{\mathfrak{Q}_i}\left(\prod_{i,\sigma} (\gamma_i^\sigma)^{c_i^\sigma}\right)$ in time $\mathrm{Poly}(s, N, \log Q) \cdot e^{\tilde{O}(\sqrt{\log d})}$. Evaluating a $2^{\iota-1}$-th root of this value in $\mathbb{F}_{Q_i}$ has the same complexity. However, there are $2^{\iota-1}$ different possible roots, and it is impossible to tell which one is the image of α under the map $\phi_{\mathfrak{Q}_i}$ without actually evaluating the product (and square roots) defining α (something we cannot afford for complexity reasons). To circumvent this, we choose the $Q_i := \mathcal{N}(\mathfrak{Q}_i)$ such that all of the different $2^{\iota-1}$-th roots in $\mathbb{F}_{Q_i}$ have the same Legendre symbol for $2 \leq \iota \leq n$. To do this, we need to ensure that -1 is a 2^{n-1}-th power in $\mathbb{F}_{Q_i}$. This is ensured when there is a primitive 2^n-th root of unity in $\mathbb{F}_{Q_i}$, or equivalently, when $2^n \mid Q_i - 1$.

Algorithm 4.2: S-UnitsGivenSubgroup(K , $\alpha_1, \ldots, \alpha_k$)

Input: Real multiquadratic field $K \subseteq \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$, $\alpha_1, \ldots, \alpha_k$ such that $U_{K,S}^2 \subseteq \langle \alpha_1, \ldots, \alpha_k \rangle$

Result: Generators of $U_{K,S}/\{\pm 1\}$

$\chi_1, \ldots, \chi_m \leftarrow$ characters defined by $\mathfrak{Q}_i$ with $2^n \mid \mathcal{N}(\mathfrak{Q}_i) - 1$ for $i \leq m$.

$A \leftarrow \left[\log_{-1}(\chi_i(\alpha_j))\right]_{i \leq m, j \leq k} \in \mathbb{F}_2^{m \times k}$.

$V \leftarrow$ Basis of the left kernel of A

for $i = 1, \ldots, \#V$ **do**

  $v_i \leftarrow \prod_j \alpha_j^{V_{ij}}$.

  $\beta_i \leftarrow \sqrt{v_i}$

return $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_{\#V}$

In the description of Algorithm 4.2, we identify field elements and their representation described above. As previously mentioned, all squares must map to elements

of LeftKernel(A), but there is a chance that elements from LeftKernel(A) do not arise as the map of a square in K. In this case, the element s_i calculated in Step 5 is not a square, and the (formal) square root computed in Step 6 does not correspond to any element in K. The probability of success of Algorithm 4.2 derives from a standard heuristic used for the computation of square roots in the Number Field Sieve algorithm [16, Sec. 8]. This argument was also used for computing units of multiquadratic fields in [3, Sec. 4.2]. Let $U := \langle \alpha_1, \ldots, \alpha_k \rangle / \{\pm 1\}$. The rank of $U/(U \cap K^2)$ is at most $s + r$ where r is the rank of the unit group of K and $s := |S|$. Therefore, the dual $\mathrm{Hom}\left(U/(U \cap K^2), \mathbb{F}_2\right)$ is an $\mathbb{F}_2$ vector space of dimension at most $r+s$. Assuming that $\log_{-1} \chi_{\mathfrak{Q}_1}, \cdots, \log_{-1} \chi_{\mathfrak{Q}_m}$ are independent uniform random elements of this dual, they span the dual with probability at least $1 - 1/2^{m-r-s}$ by [16, Lem. 8.2]. In that case, $X(\alpha) = 0$ implies $\alpha \in U \cap K^2$. Note that when we enforce the restriction, $2^n \mid Q_i - 1$ for $i \leq m$, elements divisible by 2 will always be in the kernel of the $\log_{-1} \chi_{\mathfrak{Q}_i}$, therefore the heuristic according to which the $\left(\log_{-1} \chi_{\mathfrak{Q}_i}\right)_{i \leq m}$ span the dual only makes sense when no element in U is divisible by 2, which is ensured when S does not contain any ideal above 2.

Heuristic 4.3. *Let K be a multiquadratic subfield of $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$, and let S be a set of prime ideals of K that does not contain any ideal above 2. Let $\alpha_1, \ldots, \alpha_k$ be elements generating $U^2_{K,S}$ and let $U := \langle \alpha_1, \ldots, \alpha_k \rangle / \{\pm 1\}$ Then morphisms of the form $\log_{-1} \chi_{\mathfrak{Q}_i}$ where $2^n \mid \mathcal{N}(\mathfrak{Q}_i) - 1$ are uniformly distributed in $\mathrm{Hom}\left(U/(U \cap K^2), \mathbb{F}_2\right)$.*

Proposition 4.4. *Let K be a multiquadratic subfield of $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$, and let S be a set of prime ideals of K that does not contain any ideal above 2. Let $\alpha_1, \ldots, \alpha_k$ be elements generating $U^2_{K,S}$. Let r be the rank of the unit group of K and let $s := |S|$. Then the run time of Algorithm 4.2 is in $Poly(s, m, N, C, \log Q) \cdot e^{\tilde{O}(\sqrt{\log d})}$ where m is the number of characters, $N = 2^n$, $Q = \max_{i \leq m} Q_i$, C is an upper bound on the bit size of the coefficients of the vectors defining the α_i and $d = \max_{i \leq n} d_i$. Algorithm 4.2 returns a generating set of $U_{K,S}$ with probability at least $1 - 1/2^{m-r-s}$ under Heuristic 4.3. Moreover, the size of the coefficients defining the β_i is bounded by kC.*

Remark 4.5. *The only subroutine that we have not formally analyzed is the creation of the $\chi_1, \ldots, \chi_m$. For that, we directly rely on the algorithm GoodPrime of [3]. It returns each prime in time $O(N)$. Thus, the calculation of $\chi_1, \ldots, \chi_m$ is in $O(mN)$.*

4.4. **Overall procedure.** We now have all the ingredients to specify the details of our recursive method to compute the S-unit group of $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ for a set of prime ideals S invariant under the action of the Galois group of L.

Theorem 4.6. *Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a real multiquadratic field of degree N and S be a set of prime ideals of L stable under $\mathrm{Gal}(L/\mathbb{Q})$ that does not contain any ideal above 2. Then under Heuristic 4.3, the elements $\beta_1, \ldots, \beta_{r+s}$ returned by Algorithm 4.3 generate the torsion free part of U_S with probability $1 - \frac{1}{2^N}$. The asymptotic complexity of Algorithm 4.3 is in $Poly(Size(S), \log(\Delta)) \cdot e^{\tilde{O}(\sqrt{\log d})}$ where $Size(S) = s \cdot \max_{\mathfrak{p} \in S} \log(\mathcal{N}(\mathfrak{p}))$, $\Delta = \mathrm{disc}(L)$, and $d := max_{i \leq n} d_i$.*

Proof. Algorithm 4.3 is called $3^n \in \mathrm{Poly}(N)$ times. The run time of Algorithm 4.3 is essentially ruled by that of Algorithm 4.2 and by the cost of Steps 12 and 14.

Algorithm 4.3: MQSunits for S stable under $\mathrm{Gal}(L/\mathbb{Q})$

Input: Real multiquadratic field L, ring of integers $\mathcal{O}_L$ of L, and set of prime ideals S of $\mathcal{O}_L$ stable under $\mathrm{Gal}(L/\mathbb{Q})$.

Result: A basis of the relations $\mathcal{R}el_S(L)$.

1 $S_0 \leftarrow \{p_1, \dots, p_s\}$ where $\forall i \leq s, \exists \mathfrak{p} \in S,\ p_i \mid \mathfrak{p}$.
2 **if** $[L : \mathbb{Q}] = 2$ **then**
3 $\Lambda \leftarrow$ basis of $\mathcal{R}el_S(L)$ using [27, Alg. I.1.2].
4 **return** Λ
5 $\sigma, \tau \leftarrow$ distinct non-identity automorphisms of L
6 **for** $\ell \in \{\sigma, \tau, \sigma\tau\}$ **do**
7 $K_\ell \leftarrow$ fixed field of ℓ
8 $S \leftarrow \{\mathfrak{p} \subseteq K_\ell \mid \exists e \in \mathbb{Z}, p \in S_0\ \ \mathcal{N}(\mathfrak{p}) = p^e\}$
9 $\Lambda_\ell \leftarrow \mathrm{MQSunits}(K_\ell, S)$
10 $\Lambda_U \leftarrow \Lambda_\sigma \cup \Lambda_\tau \cup \sigma(\Lambda_{\sigma\tau})$
11 $\Lambda := \{(\alpha_1, \vec{e}_1), \dots, (\alpha_k, \vec{e}_k)\} \leftarrow \mathrm{SunitGivenSubgroup}(L, \Lambda_U)$ (Alg. 4.2)
12 $A \leftarrow (\vec{e}_i)_{i \leq k}$. Compute $U \in \mathrm{GL}_k(\mathbb{Z})$ such that $UA = \begin{pmatrix} H \\ (0) \end{pmatrix}$ is the HNF of A
13 For $i = 1, \dots, s$: $\beta_i \leftarrow \prod_{j \leq k} \alpha_j^{U_{i,j}}$
14 Compute a basis $\vec{w}_1, \dots, \vec{w}_r$ of the left kernel of A
15 For $i = 1, \dots, r$: $\beta_{s+i} \leftarrow \prod_{j \leq k} \alpha_j^{w_{i,j}}$
16 **return** $(\beta_1, \vec{H}_1), \dots, (\beta_s, \vec{H}_s), (\beta_{s+1}, \vec{0}), \dots, (\beta_{s+r}, \vec{0})$

Moreover, the cost of the ideal arithmetic involved in the lifting of the relations is in $\mathrm{Poly}(\mathrm{Size}(S), \log(\Delta))$. The probablity of success of the overall algorithm is at least $\left(1 - \frac{1}{2^{m-r-s}}\right)^N \sim 1 - \frac{N}{2^{m-r-s}}$ where r is the rank of the unit group of L. Therefore, a choice of $m \in \mathrm{Poly}(N, s)$ can ensure that the probability of success is at least $1 - \frac{1}{2^N}$. With such a choice of m, we can also ensure that $Q \in \mathrm{Poly}(N, s)$. Finally, the bit size C of the coefficients of the representation of the elements in the relations only increase by a polynomial factor at every stage of the algorithm. In Algorithm 4.2, it gets multiplied by $k \leq 3(s + r)$, while in Steps 12 and 14, the coefficients of U and of the $\vec{w}_i$ are in $\mathrm{Poly}(s, \log(\Delta)) \cdot e^{\tilde{O}(\sqrt{\log d})}$. Moreover, the runtime of Steps 12 and 14 is also in $\mathrm{Poly}(s, \log(\Delta)) \cdot e^{\tilde{O}(\sqrt{\log d})}$, which proves the statement. □

The result of Algorithm 4.3 can be certified in polynomial time under the Generalized Riemann Hypothesis if the prime ideals in S generate the ideal class group of L. This is the case in all the applications that are considered in Section 5, including the computation of arbitrary S-unit groups. The only way Algorithm 4.3 can fail is if Algorithm 4.2 identifies non-squares as squares. If this is the case, then the set of relations returned by Algorithm 4.3 contains elements that are not in $\mathcal{R}el_S(L)$. Let $h_0 := \det(H)$ and R_0 be the volume of the lattice generated by $\mathrm{Log}(\beta_i)$ for $i = s + 1, \dots, s + r$. If the result is correct, then $h_0 = h$ the class number of $\mathcal{O}_L$ while $R_0 = R$ the regulator of L. If not, then $h_0 R_0 \leq \frac{1}{2} hR$ (i.e. $\mathcal{R}el_S(L)$ is a finite index subgroup of the output of Algorithm 4.3). An estimate for hR can be found in polynomial time under the GRH by using the mehods of [2].

Proposition 4.7. *Under the GRH, the result of Algorithm 4.3 can be certified in polynomial time if S includes a generating set of the ideal class group of $\mathcal{O}_L$.*

5. Applications of the S-unit computation algorithm

The S-unit group computation of Section 4 can be used to compute ideal class groups, S-class groups, and (arbitrary) S-unit groups.

5.1. Ideal class group computation.

As explained in Section 2.5, the computation of $\mathrm{Cl}(\mathcal{O}_L)$ can be done by searching for a basis of the relations between a generating set [1] of the classes of $\mathrm{Cl}(\mathcal{O}_L)$. Once such a generating set is found, then the strategy is the same as in [21], which was sketched in Section 3.

Algorithm 5.1: Computation of $\mathrm{Cl}(\mathcal{O}_L)$

Input: Ring of integers $\mathcal{O}_L$ of a real multiquadratic field L of degree N and discriminant Δ.
Result: Class group of $\mathcal{O}_L$.
1 Compute $S := \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq 3\ln^2\left(\Delta^2 \cdot 2^N\right),\ \mathfrak{p} \nmid 2\}$.
2 $(\alpha_1, \vec{H}_1), \ldots, (\alpha_s, \vec{H}_s), (\alpha_{s+1}, \vec{0}), \ldots, (\alpha_{s+r}, \vec{0}) \leftarrow$ output of Algorithm 4.3
3 $\mathrm{diag}(d_1, \ldots, d_s) \leftarrow \mathrm{SNF}(H)$
4 **return** $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z}$

Proposition 5.1. *Let $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ be a real multiquadratic field of degree N an discriminant Δ. Under the GRH, Algorithm 5.1 successfully returns the ideal class group of $\mathcal{O}_L$ with probability $1 - \frac{1}{2^N}$ in time Poly$(\log(\Delta)) \cdot e^{\tilde{O}(\sqrt{\log d})}$ where $d = \max_{i \leq n} d_i$. The result of Algorithm 5.1 can be certified in polynomial time in $\log(\Delta)$.*

Corollary 5.2. *When $d = \max_{i \leq n} d_i$ satisfies $\log(d) < \log(\log(\Delta))^c$ for some constant $c < 2$, then Algorithm 5.1 returns the ideal class group of $\mathcal{O}_L$ with probability $1 - \frac{1}{2^N}$ in polynomial time in $\log(\Delta)$.*

We showcase the effect of our algorithm on classes of multiquadratic fields with small d_i by the computation of the class group of the degree 128 multiquadratic field $L = \mathbb{Q}(\sqrt{5}, \sqrt{13}, \sqrt{17}, \sqrt{29}, \sqrt{37}, \sqrt{41}, \sqrt{53})$ and its subfields. We implemented Algorithm 5.1 and ran experiments on a single core of a HP ZBook 15 Mobile Workstation (Core i7 4800MQ - 16 GB RAM) and a single core of a AMD FX-8350 Vishera 4.0GHz CPU (32 GB RAM), both running version 7.5.1 of Sage [20]. For the low level multiquadratic arithmetic, we used the methods of [3]. For the Sage experiments the `class_group(proof = False)` method was used. Note that Sage's class group routine directly calls that of Pari/GP [29]. We also ran the class group routine of Magma V.2.23 on the same fields on an Intel Core i7-2600 CPU 3.40GHz with 8 GB of RAM (PC3). Magma [14] works at a higher level of rigour by only returning results that are at least certified under GRH (we ran the command `ClassGroup(K:Proof:="GRH")`). Therefore the comparison with Sage is not entirely relevant. In degree 64, the computation with Magma had to be terminated after 24h since it had exhausted the machine's memory. In the final version of the paper, all run times will be reported on the same architecture.

[1] We use [1, Th. 4] with $\mathfrak{f} = (2)\mathcal{O}_L$ to avoid primes dividing 2

Although slower for small degrees, our method is the only implementation that is able to compute the class group of multiquadratic fields of degree more than 32. We can see on Table 5.1 that the run time (in CPU seconds) of Algorithm 5.1 is consistent with a polynomial run time in $\log(\Delta)$. Our algorithm is parallelizable on several levels: subtrees of the recursion tree are independent, as well as computations modulo the $(Q_i)_{i\leq m}$. Therefore, we anticipate that a parallel version of our algorithm could reach degrees 256 and 512.

$[L:\mathbb{Q}]$	Alg. 5.1 (Vishera)	Magma (PC3)	Sage (Vishera)	$\mathrm{Cl}(\mathcal{O}_L)$
8	99.9	1.4	0.25	trivial
16	648	12	0.91	$C_4 \times C_4$
32	5027	3615	77.7	$C_2 \times C_4 \times C_8^4$
64	$4.0 \cdot 10^4$	·	$> 8.5 \cdot 10^5$	$C_2^9 \times C_4^3 \times C_8 \times C_{16}^4 \times C_{48} \times C_{240}$
128	$5.42 \cdot 10^5$	·	·	$C_2^{10} \times C_4^{16} \times C_8^{13} \times C_{16}^2 \times C_{48}^6 \times C_{96}^3 \times C_{48} \times C_{960}$

TABLE 5.1. Comparison of class group routine run time

5.2. **S-class group and S-unit group computation.** Algorithm 4.3 computes the S-unit group with the restriction that S contains all conjugates of any $\mathfrak{p} \in S$ under the action of $\mathrm{Gal}(L/\mathbb{Q})$. As shown in Section 3, the S-class group boils down to the search for the lattice of relations between the generators $(\mathfrak{g}_i)_{i\leq s_0}$ of $\mathrm{Cl}(\mathcal{O}_L)$ which we enlarge with new relations of the form $\mathfrak{q}_j \sim \prod_{i\leq s_0} \mathfrak{g}_i^{x_{i,j}}$. The SNF of this enlarged relation lattice gives the elementary divisors of the S-class group while its kernel reveal the S-unit group. Here, our only restriction on S is that it does not contain ideals above 2.

Algorithm 5.2: S-class group and S-unit group computation

Input: Real multiquadratic field L of degree N, ring of integers $\mathcal{O}_L$ of L, and a set S of prime ideals of $\mathcal{O}_L$ that does not contain ideals above 2.

Result: S-unit group and S-class group of L

Compute $S_0 := \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) \leq 3\ln^2\left(\Delta^2 \cdot 2^N\right),\ \mathfrak{p} \nmid 2\}$ for $\Delta = \mathrm{disc}(L)$

$S_0 \leftarrow S \cup \{\mathfrak{q}^\sigma \mid \mathfrak{q} \in S, \sigma \in \mathrm{Gal}(L/\mathbb{Q})\}$.

$(\alpha_1, \vec{H}_1), \ldots, (\alpha_{s_0}, \vec{H}_{s_0}), (\alpha_{s_0+1}, \vec{0}), \ldots, (\alpha_{s_0+r}, \vec{0}) \leftarrow$ output of Algorithm 4.3

Compute U, V such that $U \begin{pmatrix} H \\ (0) \end{pmatrix} V = \begin{pmatrix} \mathrm{SNF}(H) \\ (0) \end{pmatrix}$ with $\mathrm{SNF}(H) = \mathrm{diag}(d_i)_{i\leq s_0}$

For $j \leq s_0$, define $\mathfrak{g}_j := \prod_{i\leq s_0} \mathfrak{p}_i^{V_{i,j}}$ (here, $\mathrm{Cl}(\mathcal{O}_L) \simeq \bigoplus_{i\leq k} \langle [\mathfrak{g}_i] \rangle$)

$V' \leftarrow V^{-1}$ For each $j \leq s$, find $j_0 \leq s_0$ such that $\mathfrak{q}_j = \mathfrak{p}_{j_0}$

$\vec{x}_j \leftarrow (V'_{1,j_0}, \ldots, V'_{s_0,j_0})$ (here $\mathfrak{q}_j = \prod_{i\leq s_0} \mathfrak{g}_i^{x_{i,j_0}}$)

Let $M = \begin{pmatrix} H \\ (\vec{x}_i)_{i\leq s} \end{pmatrix}$

$\mathrm{diag}(d'_i)_{i\leq s_0} \leftarrow \mathrm{SNF}(M)$. Compute a basis $\vec{w}_1, \ldots, \vec{w}_s$ of the left kernel of M

For $i \leq s$ $\alpha'_i \leftarrow \prod_{j\leq s_0} \alpha_j^{w_{i,j}}$.

For $1 \leq i \leq r$: $\alpha'_{i+s} \leftarrow \alpha_{s_0+i}$ (the $(\alpha'_i)_{s<i\leq r+s}$ generate U_L)

return $\langle \alpha'_1 \rangle \times \ldots \times \langle \alpha'_{s+r} \rangle, \mathbb{Z}/d'_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d'_{s_0}$

Proposition 5.3. *Algorithm 5.2 is correct and returns the S-class group and the S-unit group with probability $1-\frac{1}{2^N}$ where $N = [L;\mathbb{Q}]$ in time $Poly(Size(S), \log(\Delta)) \cdot e^{\tilde{O}(\sqrt{\log d})}$ where $\Delta = \mathrm{disc}(L)$, and $d := max_{i\leq n} d_i$.*

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[2] E. Bach. Improved approximations for Euler products. In *Number Theory: CMS Proc.*, volume 15, pages 13–28. Amer. Math. Soc., Providence, RI, 1995.

[3] J. Bauch, D. Bernstein, H. de Valence, T. Lange, and C. van Vredendaal. Short generators without quantum computers: The case of multiquadratics. In J.-S. Coron and J. Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 27–59, 2017.

[4] J.-F. Biasse. Improvements in the computation of ideal class groups of imaginary quadratic number fields. *Adv. in Math. of Comm.*, 4(2):141–154, 2010.

[5] J.-F. Biasse. An L(1/3) algorithm for ideal class group and regulator computation in certain number fields. *Math. Comp.*, 83(288):2005–2031, 2014.

[6] J.-F. Biasse. Subexponential time relations in the class group of large degree number fields. *Advances in Mathematics of Communications*, 8(4):407–425, 2014.

[7] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin, and P. Kirchner. Computing generator in cyclotomic integer rings. In J.-S. Coron and J. Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 60–88, 2017.

[8] J.-F. Biasse and C. Fieker. Improved techniques for computing the ideal class group and a system of fundamental units in number fields. In *Algorithmic Number Theory, 10th International Symposium, ANTS-IX, San Diego CA, USA, July 9-13, 2012. Proceedings*, volume 1 of *Open Book Series*, pages 113–133. Mathematical Science Publishers, 2012.

[9] J.-F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17:385–403, 1 2014.

[10] J.-F. Biasse and M. Jacobson. Practical improvements to class group and regulator computation of real quadratic fields. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings*, volume 6197 of *Lecture Notes in Computer Science*, pages 50–65. Springer, 2010.

[11] J.-F. Biasse, M. Jacobson., and A. Silvester. Algebraic techniques for number fields. In *2nd International Conference on Symbolic Computation and Cryptography , SCC 2010, Egham, UK. Proceedings*, 2010.

[12] J.-F. Biasse, M. Jacobson, and A. Silvester. Security estimates for quadratic field based cryptosystems. In *ACISP*, volume 6168 of *Lecture Notes in Computer Science*, pages 233–247. Springer, 2010.

[13] J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In R. Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902. SIAM, 2016.

[14] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[15] J. Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In S. Goldstein, editor, *Séminaire de Théorie des Nombres, Paris 1988–1989*, pages 27–41, Boston, 1990. Birkhauser.

[16] J. Buhler, H. Lenstra, and C. Pomerance. Factoring integers with the number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.*, pages 50–94. Springer, Berlin, 1993.

[17] N. Cebotarev. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.*, 95:191–228, 1926.

[18] D. Chatelain. Bases des entiers des corps composs par des extensions quadratiques de $\mathbb{Q}$. *Ann. Univ. Besancon, Math.*, 6, 1973.
[19] H. Cohen, F. Diaz Y Diaz, and M. Olivier. Subexponential algorithms for class group and unit computations. *Journal of Symbolic Computation*, 24(3???4):433 – 441, 1997.
[20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5.1)*, 2017. http://www.sagemath.org.
[21] J. Hafner and K. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of American Mathematical Society*, 2:839–850, 1989.
[22] A. Lenstra. On the calculation of regulators and class numbers of quadratic fields. In *Journées arithmétiques*, pages 123–150. Cambridge Univ. Press, 1982.
[23] M. Pohst. *Algorithmic Methods in Algebra and Number Theory*. Number 1. Academic Press, 1987.
[24] B. Schmal. Diskriminanten, $\mathbb{Z}$-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern. *Archiv der Mathematik*, 52(3):245–257, Mar 1989.
[25] D. Shanks. Class number, a theory of factorization, and genera. In W. J. LeVeque and E. G. Straus, editors, *Proceedings of Symposia in Pure Mathematics*, volume 20, pages 415–440. American Mathematical Society, 1969.
[26] D. Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the 1972 Number Theory Conference*, pages 217–224. American Mathematical Society, 1972.
[27] D. Simon. *Équations dans les corps de nombres et discriminants minimaux*. PhD thesis, Université Bordeaux I, 1998.
[28] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Department of Computer Science, Swiss Federal Institute of Technology – ETH, 2000.
[29] The PARI Group, Univ. Bordeaux. *PARI/GP version* 2.9.4, 2018. available from http://pari.math.u-bordeaux.fr/.

University of South Florida, 4202 E Fowler Ave, Tampa, FL 33620, USA
E-mail address: biasse@usf.edu

Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
E-mail address: c.v.vredendaal@tue.nl

CYCLIC EXTENSIONS OF PRIME DEGREE AND THEIR p-ADIC REGULATORS

TOMMY HOFMANN AND YINAN ZHANG

Abstract. We present a conjecture on the distribution of the valuations of p-adic regulators of cyclic extensions of $\mathbb{Q}$ of odd prime degree. This is based on the observation of computational data of p-adic regulators of the 5 521 222 cyclic quintic and 329 708 cyclic septic extensions of $\mathbb{Q}$ for $2 < p < 100$ with discriminant up to 5×10^{31} and 10^{42} respectively, and noting that the observation matches the model that the entries in the regulator matrix are random elements with respect to the obvious restrictions.

1. Introduction

The class group and regulator of a number field are important invariants of the field, providing information about the multiplicative and unit group structure of the number field. These two invariants are intimately linked by the class number formula, and following the improvements to the class group algorithm by Buchmann [Buc90], can be computed together in the same algorithm. Despite various improvements to the algorithm, some in recent times, an efficient algorithm to compute the class group and regulator of arbitrary number fields remains elusive and a significant focus in computational number theory.

In [Leo62], Leopoldt introduced the p-adic regulator $R_p(K)$ of a number field K in his study of p-adic L-functions, and his conjecture states that it is non vanishing. While its classical counterpart, the regulator of a number field, is well defined for all finite extensions of $\mathbb{Q}$, the p-adic regulator is only unambiguous for totally real or CM number fields, and very little is known about the actual value of p-adic regulators.

Previous efforts on computing the p-adic regulators of number fields were predominantly focused on numerical verification of Leopoldt's conjecture, and significant practical difficulties with p-adic computations restricted efforts to compute its exact value. Indeed, this was noted by Panayi in his PhD thesis [Pan95], who was one of the first to compute $R_p(K)$ explicitly.

Research on the valuation of the p-adic regulator has also been limited. Examples of this include Schirokauer [Sch93, Prop. 3.8], who provided some heuristical arguments regarding the p-divisibility of the units, while Miki [Mik87] attempted to provide an upper bound on $v_p(R_p(K))$, and Hakkarainen provided a simple lower bound in his PhD thesis [Hak07], along with limited heuristics using the valuation of the class number and the class number formula.

Recent development by Fieker and Zhang [FZ16] in a p-adic class number algorithm for totally real abelian fields allowed relatively efficient computation of the p-adic regulator of these fields. This algorithm was used in [HZ16] to compute the

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

p-adic regulator of the almost 16 million cyclic cubic extensions of $\mathbb{Q}$ with discriminant less than 10^{16}, and from this experimental data, the authors were able to conjecture and provide heuristics on the distribution of the values of $v_p(R_p(K))$.

We continue this previous work by computing the p-adic regulator for a large number of cyclic quintic and septic extensions for $2 < p < 100$. Based on this new experimental data, we extend the previous heuristics to a conjecture for all cyclic extensions of $\mathbb{Q}$ with prime degree, as follows.

Fix an odd prime ℓ and let $\mathcal{K}$ be the set of all cyclic extensions of $\mathbb{Q}$ with degree ℓ inside a fixed algebraic closure of $\mathbb{Q}$. Note that such extensions are necessarily totally real. For a prime p let $\mathcal{K}_p^{\mathrm{un}}$ and $\mathcal{K}_p^{\mathrm{ram}}$ denote the set of all fields in $\mathcal{K}$ which are unramified and ramified at p, respectively. Note that $\mathcal{K}_p^{\mathrm{ram}} = \emptyset$ and $\mathcal{K} = \mathcal{K}_p^{\mathrm{un}}$ in case $p \not\equiv 1 \bmod \ell$ and $p \neq \ell$. For $D > 0$ we set $\mathcal{K}(D) = \{K \in \mathcal{K} \mid |d(K)| \leq D\}$, where $d(K)$ is the discriminant of K, $\mathcal{K}_p^{\mathrm{un}}(D) = \mathcal{K}_p^{\mathrm{un}} \cap \mathcal{K}(D)$, and $\mathcal{K}_p^{\mathrm{ram}}(D) = \mathcal{K}_p^{\mathrm{ram}} \cap \mathcal{K}(D)$. Let $\mathrm{ord}_\ell(p)$ be the multiplicative order of p modulo ℓ, and v_p be the p-adic valuation. Based on heuristics and numerical data, we make the following conjecture:

Conjecture 1. *Let $p \neq 2, \ell$ be a prime, $\mathrm{ord}_\ell(p) = m$, $\ell - 1 = mn$ and $\mathrm{T} \in \{\mathrm{un}, \mathrm{ram}\}$. Then $v_p(R_p(K)) \in m\mathbb{Z} + v_{\mathrm{T}}$ for all $K \in \mathcal{K}_p^{\mathrm{T}}$ and for $i \geq 0$ we have*

$$\lim_{D\to\infty} \frac{\#\{K \in \mathcal{K}_p^{\mathrm{T}}(D) \mid v_p(R_p(K)) = mi + v_{\mathrm{T}}\}}{\#\mathcal{K}_p^{\mathrm{T}}(D)} = \binom{i+n-1}{n-1} \frac{1}{p^{mi}} \left(1 - \frac{1}{p^m}\right)^n,$$

where $v_{\mathrm{un}} = \ell - 1$ and $v_{\mathrm{ram}} = (\ell - 1)/2$.

This paper is organised as follows: some basic definitions are recalled in §2. We then conjecture a link between the distribution of $v_p(R_p(K))$ and $v_p(\det(M))$, where M is an arbitrary matrix in a particular form, in §3 (see Conjecture 1′). So far this is similar to [HZ16, §1-3], but we diverge in §4 to obtain some results about solutions of linear equations in p-adic rings. Applying this to the factorisation of $\det(M)$, we obtain Conjecture 1 in §5. Finally, in §6, we provide the numerical data from our computations.

Acknowledgements. We would like to thank Pierre Guillot and Christian Wuthrich, who communicated to us a proof of Proposition 8. The first author was supported by Project II.2 of SFB-TRR 195 'Symbolic Tools in Mathematics and their Application' of the German Research Foundation (DFG).

2. Definition and notation

Let K be a number field of degree ℓ and p a prime. By $\mathbb{C}_p$ we denote the completion of an algebraic closure of $\mathbb{Q}_p$. By fixing an embedding from $\mathbb{C}_p$ into $\mathbb{C}$, any embedding of K into $\mathbb{C}_p$ can be considered as either real or complex, depending on the image of K in the composite embedding into $\mathbb{C}$. Note that for totally real or CM fields, whether an embedding from K to $\mathbb{C}_p$ is real or complex is independent of the choice of embedding from $\mathbb{C}_p$ to $\mathbb{C}$, but this is not well defined in general.

Let (r_1, r_2) be the signature of K and $r = r_1 + r_2 - 1$ the unit rank. Denote by $\tau_1, \ldots, \tau_{r_1}$ the real and by $\tau_{r_1+1}, \overline{\tau}_{r_1+1}, \ldots, \tau_{r_1+r_2}, \overline{\tau}_{r_1+r_2}$ the complex embeddings of K into $\mathbb{C}_p$. Let $\epsilon_1, \ldots, \epsilon_r$ be a set of independent units of K such that, modulo torsion, the index of $\langle \epsilon_1, \ldots, \epsilon_r \rangle$ in $\mathcal{O}_K^\times$ is coprime to p. Consider the submatrix formed by deleting one column of the matrix

$$(\delta_i \log_p(\tau_j(\epsilon_i)))_{i,j} \in \mathbb{C}_p^{r\times(r+1)},$$

where $\delta_i = 1$ for $1 \leq i \leq r_1$ and $\delta_i = 2$ if $r_1 + 1 \leq i \leq r_1 + r_2$, and $\log_p \colon \mathbb{C}_p^\times \to \mathbb{C}_p$ is the p-adic Iwasawa logarithm (see [Iwa72]). As each row sums to zero, the determinant of such a submatrix is independent of the column deleted up to a sign. The value of this determinant is also independent of the choice of the units $\epsilon_1, \ldots, \epsilon_r$ up to a p-adic unit, and is known as the p-adic regulator $R_p(K)$ of the number field K.

There is an alternate definition introduced by Iwasawa [Iwa72] and subsequently implemented in the algorithm by Fieker and Zhang [FZ16]. Instead of deleting a column in the matrix, one can add a row of 1's to it, and divide the determinant by ℓ. Again, due to each row summing to zero, the value of the determinant is unaffected. In [HZ16] it was noted that while this does have the disadvantage of calculating the determinant of a matrix one dimension higher than necessary, it is outweighed by leaving the structure of the original matrix intact.

If G is a compact group, we denote by μ_G the unique left Haar measure with $\mu_G(G) = 1$. In case no confusion can arise, we just write μ instead of μ_G. For two integers $n \in \mathbb{Z}_{\geq 1}$, $k \in \mathbb{Z}$ we denote by $k \bmod n$ the unique representative of $k + n\mathbb{Z}$ in the set $\{0, \ldots, n-1\}$.

3. p-adic regulators and regulator matrices

Let ℓ be a prime and denote by K a cyclic extension of $\mathbb{Q}$ of degree ℓ. We start by collecting basic facts about p-adic regulators, beginning with lower bounds, a special case of which was observed in [HZ16, Lemma 3.1].

Proposition 2. *For a prime $p \neq \ell$ we have*

$$v_p(R_p(K)) \geq \begin{cases} \frac{\ell-1}{2}, & \text{if } p \text{ is ramified in } K, \\ \ell - 1, & \text{if } p \text{ is unramified in } K. \end{cases}$$

Proof. By the theorem of Ax–Brumer (see [Bru67]) we know that Leopoldt's conjecture holds for abelian extensions of $\mathbb{Q}$ and in particular $R_p(K) \neq 0$. For a non zero prime ideal $\mathfrak{p} \mid p\mathcal{O}_K$ denote by $\nu_\mathfrak{p}$ the number of p-power roots of unity in the completion of K at $\mathfrak{p}$. By [Coa77, Appendix, Lemma 5] we know that

$$\frac{\ell \cdot p \cdot R_p(K)}{\Delta_K^{1/2}} \prod_{\mathfrak{p} \mid p\mathcal{O}_K} (\nu_\mathfrak{p} \cdot N(\mathfrak{p}))^{-1}$$

has non negative p-adic valuation. Using that $v_p(\nu_\mathfrak{p}) \geq 0$ we obtain

$$v_p(R_p(K)) \geq \frac{v_p(\Delta_K)}{2} - v_p(\ell) - v_p(p) + \frac{\ell}{e(p)},$$

where $e(p)$ is the ramification index of p in K. Since $K/\mathbb{Q}$ is cyclic of prime degree ℓ, we know that if p is ramified, then $e(p) = \ell$. Moreover, as p is tamely ramified, we have $v_p(\Delta_K) = \ell - 1$ ([Ser79, III.§7, Prop. 13]) □

Definition 3. *Let $R = \mathbb{Z}[X_1, \ldots, X_{\ell-1}]$ and set $X_0 = -\sum_{i=1}^{\ell-1} X_i$. We define $M_\ell = (m_{ij})_{1 \leq i,j \leq \ell} \in R^{\ell \times \ell}$ by*

$$m_{ij} = \begin{cases} 1, & \text{if } i = 1, \\ X_{(i+j-2) \bmod \ell}, & \text{otherwise.} \end{cases}$$

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

We call M_ℓ the generic regulator matrix of degree ℓ. Using the Haar measure μ on $\mathbb{Z}_p^{\ell-1}$ we define the random variable

$$P_{\ell,p}\colon \mathbb{Z}_p^{\ell-1} \longrightarrow \mathbb{R}_{\geq 0},\ (a_1,\dots,a_{\ell-1}) \longmapsto v_p(\det(M_\ell(a_1,\dots,a_{\ell-1}))),$$

where $M_\ell(a_1,\dots,a_{\ell-1})$ is obtained by setting $X_i = a_i$ in the matrix M_ℓ, so that for $i \in \mathbb{Z}_{\geq 0}$ we have $\operatorname{pr}(P_{\ell,p} = i) = \mu(\{a \in \mathbb{Z}_p^{\ell-1} \mid v_p(\det(M_\ell(a))) = i\})$.

The name of the generic regulator matrix is justified by the following result, which was also observed in [HZ16, Prop. 3.2] for $\ell = 3$.

Theorem 4. *Let $p \neq \ell$ be a prime. Then there exist $a \in \bar{\mathbb{Q}}_p^{\ell-1}$ such that $v_p(R_p(K)) = v_p(M_\ell(a))$. Moreover, if p is split in K, the vector a can be chosen in $\mathbb{Z}_p^{\ell-1}$.*

Proof. Let σ be a generator of $\operatorname{Gal}(K/\mathbb{Q})$ and $\tau\colon K \to \bar{\mathbb{Q}}_p$ a p-adic embedding. For $i \in \{1,\dots,\ell\}$ we define $\tau_i = \tau \circ \sigma^{i-1}$ and note that $\tau_1,\dots,\tau_\ell$ are the distinct p-adic embeddings of K. Due to [Mar96] there exists a p-Minkowski unit $\epsilon \in \mathcal{O}_K^\times$, that is, modulo torsion the subgroup $\langle \epsilon, \sigma(\epsilon),\dots,\sigma^{\ell-2}(\epsilon)\rangle$ of $\mathcal{O}_K^\times$ has index prime to p. Thus $v_p(R_p(K)) = v_p(\det((m_{ij})_{1\leq i,j\leq \ell}))$ where $m_{1j} = 1$ for $j \in \{1,\dots,\ell\}$ and $m_{ij} = \log_p(\tau_j(\sigma^{i-2}(\epsilon)))$ for $i \in \{2,\dots,\ell\}$, $j \in \{1,\dots,\ell\}$. Now $\tau_j(\sigma^{i-2}) = \sigma^{(i+j-2) \bmod \ell}$ and the claim follows by setting $a_i = \log_p(\sigma^{i-1}(\epsilon))$ for $i = 1,\dots,\ell-1$.

For the final statement first note that if p splits in K, then $\mathbb{Q}_p$ is a p-adic splitting field of K, that is, $\tau_i(\alpha) \in \mathbb{Q}_p$ for all $\alpha \in K$ and $i \in \{1,\dots,\ell\}$ and therefore $\tau_i(\epsilon) \in \mathbb{Z}_p$. □

Theorem 4 suggests that there could be a connection between the distribution of valuations of p-adic regulators and valuations of determinants of matrices of the form $M_\ell(a)$, where $a \in \bar{\mathbb{Q}}_p^{\ell-1}$ or $a \in \mathbb{Z}_p^{\ell-1}$ in case p is split. Based on numerical observations for the quintic and septic fields, similar to [HZ16, Conjecture 6], we conjecture that the distribution of the valuations of the p-adic regulators in cyclic ℓ-extensions matches that of the corresponding random variable $P_{\ell,p}\colon \mathbb{Z}_p^{\ell-1} \to \mathbb{R}, a \mapsto v_p(\det(M_\ell(a)))$ associated to the generic regulator matrix of degree ℓ. Although Theorem 4 supports this only in case p splits, numerical evidence suggests that it holds for all primes independent of the decomposition type. The lower bound of the regulator in the conjecture comes from Proposition 2.

Conjecture 1′. *For primes $2 < \ell$, $p \neq \ell$ and $\mathrm{T} \in \{\mathrm{un}, \mathrm{ram}\}$ the following hold:*

$$\lim_{D\to\infty} \frac{\#\{K \in \mathcal{K}_p^{\mathrm{T}}(D) \mid v_p(R_p(K)) = i + v_{\mathrm{T}}\}}{\#\mathcal{K}_p^{\mathrm{T}}(D)} = \operatorname{pr}(P_{\ell,p} = i).$$

where $v_{\mathrm{un}} = \ell - 1$ and $v_{\mathrm{ram}} = (\ell-1)/2$.

This is in agreement with the authors' previous work, since for the cubic case $\ell = 3$, Conjecture 1′ is equivalent to [HZ16, Conjecture 6]. Note that in the following it is shown that the value $\operatorname{pr}(P_{\ell,p}) = i$ on the right hand side of Conjecture 1′ can be computed explicitly (see Theorem 9), making it possible to gather numerical evidence for Conjecture 1′ by only investigating statistics of valuations of p-adic regulators of cyclic number fields (see Section 6).

While it may be possible to extend [HZ16, Lemma 4.8] and [HZ16, Lemma 4.9] to cover $\operatorname{pr}(P_{\ell,p} = i)$ when $\operatorname{ord}_\ell(p) = 1$ and $\operatorname{ord}_\ell(p) = \ell - 1$, respectively, this would be extremely tedious due to the increasing complexity of $\det(M_\ell(a))$ as ℓ grows, and it remains unclear whether such an approach could be adapted for arbitrary

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

values of ℓ. Furthermore, this leaves the case of $\mathrm{ord}_\ell(p) \neq 1, \ell-1$ unresolved, which only occurs when $\ell \geq 5$. For these reasons we need a different approach, and we start by obtaining some results about solutions of linear equations in p-adic rings.

4. Solutions of linear equations

Let ℓ be a prime and $M_\ell \in \mathbb{Z}[X_1, \ldots, X_{\ell-1}]$ the generic regular matrix of degree ℓ. To investigate the associated random variable $P_{\ell,p}$, where p is a prime, we will determine properties of the image of $\mathbb{Z}_p^{\ell-1}$ under the polynomial $\det(M_\ell) \in \mathbb{Z}[X_1, \ldots, X_{\ell-1}]$ using the following general setup.

Let $R \subseteq S$ be an extension of p-adic rings, that is, valuation rings of p-adic fields, such that the residue fields have cardinality p and q, respectively. We consider a system of k linear forms $f_1, \ldots, f_k \in S[X_1, \ldots, X_k]$ with k indeterminates. By $M \in S^{k\times k}$ we denote the unique matrix such that

$$\begin{pmatrix} f_1(a_1, \ldots, a_k) \\ f_2(a_1, \ldots, a_k) \\ \vdots \\ f_k(a_1, \ldots, a_k) \end{pmatrix} = M \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix}.$$

For the remainder of this section we assume that $\det(M) \in S^\times$.

Lemma 5. *For $v_1, \ldots, v_k \in \mathbb{Z}_{\geq 0}$ we have*

$$\mu(\{a \in S^k \mid v_p(f_i(a)) = v_i, i = 1, \ldots, k\}) = q^{-s}(1-q^{-1})^k$$

where $s = v_1 + \cdots + v_k$.

Proof. Let Y be the set $\{(b_1, \ldots, b_k) \in S^k \mid v_p(b_i) = v_i, i = 1, \ldots, k\}$. Then

$$\begin{aligned} \{a \in S^k \mid v_p(f_i(a)) = v_i\} &= \{a \in S^k \mid (f_1(a), \ldots, f_k(a)) \in Y\} \\ &= \{a \in S^k \mid M \cdot a \in Y\} \\ &= \{M^{-1}b \mid b \in Y\}. \end{aligned}$$

Since M is invertible and measure preserving, this implies that

$$\begin{aligned} \mu(\{a \in S^k \mid v_p(f_i(a)) = v_i,\ i = 1, \ldots, k\}) = \mu(Y) &= \prod_{i=1}^{k} q^{-v_i}(1-q^{-1}) \\ &= q^{-s}(1-q^{-1})^k. \end{aligned}$$

□

In our application, we will be mainly interested in counting solutions in R^k. While this seems rather difficult in general, we will see that in our case, the action of the associated Galois group of the p-adic fields on the set of polynomials $\{f_1, \ldots, f_k\}$ is of particular simple form, reflected in the following assumption: Assume that the field extension of the corresponding fraction fields of R and S is cyclic of degree d with Galois group $G = \langle\sigma\rangle$ and the system of linear forms $f_1, \ldots, f_k$ satisfies the following property: There exists a partition $\{f_1, \ldots, f_k\} = \bigcup_{i=1}^{l} F_i$ into disjoint sets F_i of cardinality d such that G acts transitively on each F_i. For $i \in \{1, \ldots, l\}$ we write $F_i = \{f_{i,1}, \ldots, f_{i,d}\}$. As G acts transitively we may order the polynomials such that $\sigma(f_{i,j}) = f_{i,(j+1) \bmod d}$ for all $i \in \{1, \ldots, l\}, j \in \{1, \ldots, d\}$.

Lemma 6. *Let $c = (c_{i,j})_{1\le i\le l, 1\le j\le d} = (c_{1,1}, \dots, c_{1,d}, c_{2,1}, \dots, c_{2,d}, \dots, c_{l,d}) \in S^k$ and $a = (a_1, \dots, a_k) \in S^k$ such that $M \cdot a = c$. Then $a \in R^k$ if and only if for each $1 \le i \le l$ we have $c_{i,j} = \sigma^{j-1}(c_{i,1})$ for $1 \le j \le d$.*

Proof. First assume that $a \in R^k$. We fix $1 \le i \le l$. Since $f_{i,1}(a) = c_{i,1}$ for all $1 \le j \le d$ we have

$$\sigma^{j-1}(c_{i,1}) = \sigma^{j-1}(f_{i,1}(a)) = (\sigma^{j-1}(f_{i,1}))(\sigma(a)) = f_{i,j}(a) = c_{i,j}.$$

Now assume that $c_{i,j} = \sigma^{j-1}(c_{i,1})$ for all $1 \le i \le l$, $1 \le j \le d$, that is, $\sigma(c_{i,j}) = c_{i,(j+1) \bmod d}$. Then

$$c_{i,(j+1) \bmod d} = \sigma(c_{i,j}) = \sigma(f_{i,j}(a)) = (\sigma(f_{i,j}))(\sigma(a)) = f_{i,(j+1) \bmod d}(\sigma(a)),$$

implying that also $\sigma(a)$ satisfies $M \cdot \sigma(a) = c$. Since M is invertible it follows that $a = \sigma(a)$, that is, $a \in R^k$. □

We can now determine the number of solutions with prescribed valuation in the subring R. Since the valuation of an element is invariant under σ, a necessary condition for the existence of solutions in R is that the valuations in every block F_i must be equal.

Proposition 7. *For $v_1, \dots, v_l \in \mathbb{Z}_{\ge 0}$ we have*

$$\mu(\{a \in R^k \mid v_p(f_{i,j}(a)) = v_i,\ i = 1, \dots, l,\ j = 1, \dots, d\}) = p^{-s}(1 - p^{-d})^l$$

where $s = d(v_1 + \cdots + v_l)$.

Proof. By defining

$$Y = \{(b_i, \sigma(b_i), \dots, \sigma^{d-1}(b_i))_{1\le i\le l} \mid (b_1, \dots, b_l) \in S^l,\ v_p(b_i) = v_i\} \subseteq S^k,$$

Lemma 6 shows that

$$\{a \in R^k \mid v_p(f_{i,j}(a)) = v_i,\ i = 1, \dots, l,\ j = 1, \dots, d\} = \{M^{-1}b \mid b \in Y\}.$$

The remainder of the proof is analogous to the proof of Lemma 5. □

5. Distribution for cyclic field of prime degree

Let K be a cyclic field of odd prime degree ℓ, and $p \ne 2, \ell$. Let M_ℓ be the generic regulator matrix of K. To find the associated random variable $P_{\ell,p}$ using the results from Section 4, we first need to determine the factorisation of $\det(M_\ell) \in \mathbb{Z}[X_1, \dots, X_{\ell-1}]$.

Proposition 8. *Denote by ζ a primitive ℓ-th root of unity and by $\sigma\colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Define $f_0 = X_0 + \zeta X_1 + \cdots + \zeta^{\ell-1} X_{\ell-1}$.*

(1) *We have*

$$\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(f_0) = (-1)^{(\ell-1)/2} \cdot \prod_{i=0}^{\ell-2} \sigma^i(f_0).$$

(2) *For $i \in \{1, \dots, \ell-2\}$ define $f_i = \sigma^i(f_0)$. The matrix $M \in \mathbb{Q}(\zeta)^{(\ell-1)\times(\ell-1)}$ defined by*

$$\begin{pmatrix} f_0 \\ \vdots \\ f_{\ell-2} \end{pmatrix} = M \begin{pmatrix} X_1 \\ \vdots \\ X_{\ell-1} \end{pmatrix}$$

satisfies $\det(M)^2 = (-1)^{(\ell-1)/2} \cdot \ell^{\ell-2}$.

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

Proof. (1): Recall that

$$M_\ell = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ X_1 & X_2 & X_3 & \cdots & X_{\ell-1} & X_0 \\ X_2 & X_3 & X_4 & \cdots & X_0 & X_1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ X_{\ell-1} & X_1 & X_2 & \cdots & X_{\ell-3} & X_{\ell-2} \end{pmatrix}.$$

As $X_0 = -X_1 - X_2 - \cdots - X_{\ell-1}$ we may treat X_0 as an indeterminate and proof the result for M_ℓ considered as an $\ell \times \ell$ matrix over $\mathbb{Z}[X_0, \ldots, X_{\ell-1}]$. By applying to M_ℓ the column transpositions $(i+1, \ell-(i-1))$, $i \in \{1, \ldots, \frac{\ell-1}{2}\}$, we see that $\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \det(N)$, where

$$N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ X_1 & X_0 & X_{\ell-1} & \cdots & X_3 & X_2 \\ X_2 & X_1 & X_0 & \cdots & X_4 & X_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ X_{\ell-1} & X_{\ell-2} & X_{\ell-3} & \cdots & X_1 & X_0 \end{pmatrix}.$$

On the other hand, the ciruclant matrix

$$N' = \begin{pmatrix} X_0 & X_{\ell-1} & X_{\ell-2} & \cdots & X_2 & X_1 \\ X_1 & X_0 & X_{\ell-1} & \cdots & X_3 & X_2 \\ X_2 & X_1 & X_0 & \cdots & X_4 & X_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ X_{\ell-1} & X_{\ell-2} & X_{\ell-3} & \cdots & X_1 & X_0 \end{pmatrix}.$$

has determinant $\det(N') = (X_0 + X_1 + \cdots + X_{\ell-1}) \cdot \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(f_0)$ (see [Dav79, 3.2]). Adding the last $\ell - 1$ rows of N' to the first row of N', we see that

$$\det(N') = (X_0 + X_1 + \cdots + X_{\ell-1}) \cdot \det(N).$$

This shows that

$$\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \det(N) = (-1)^{(\ell-1)/2} \cdot \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(f_0).$$

(2): As the matrix M is equal to $(\sigma^i(\zeta^j))_{0 \le i,j \le \ell-2}$ and $\{\zeta^j \mid j \in \{0, \ldots, \ell-2\}\}$ is an integral basis of the cyclotomic field $\mathbb{Q}(\zeta)$, we obtain $\det(M)^2 = \mathrm{disc}(\mathbb{Q}(\zeta)) = (-1)^{(\ell-1)/2} \cdot \ell^{\ell-2}$ (see [Lan94, IV.§1]). □

We can now apply the results of Section 4 to determine $P_{\ell,p}$.

Theorem 9. *Let* $\mathrm{ord}_\ell(p) = m$ *and* $\ell - 1 = mn$. *Then for* $i \in \mathbb{Z}_{\ge 0}$ *the following holds:*

$$\mathrm{pr}(P_{\ell,p} = mi) = \binom{i+n-1}{n-1} \frac{1}{p^{mi}} \left(1 - \frac{1}{p^m}\right)^n.$$

Proof. We use the same notation as in Proposition 8. Let $i \in \mathbb{Z}_{\ge 0}$ and $v_1, \ldots, v_n \in \mathbb{Z}_{\ge 0}$ such that $i = v_1 + \cdots + v_n$.

As $\mathrm{ord}_\ell(p) = m$ we know that $\mathbb{Z}_p \subseteq \mathbb{Z}_p[\zeta]$ is an extension of degree m. Using Proposition 8, by setting $F_k = \{f_j \mid j \equiv k \bmod m\}$, $k \in \{1, \ldots, n\}$, we find ourselves in the situation stated in Section 4, and Proposition 7 implies

$$\mu(\{a \in \mathbb{Z}_p^{\ell-1} \mid v_p(f_k(a)) = v_j,\ j = 1, \ldots, n,\ f_k \in F_j\}) = \frac{1}{p^{m(v_1+\cdots+v_n)}} \left(1 - \frac{1}{p^m}\right)^n.$$

As there are a total of $\binom{i+n-1}{n-1}$ choices of $(v_1, \dots, v_n)$ with $v_1 + \cdots + v_n = i$, we have

$$\begin{aligned}\mu(\{a \in \mathbb{Z}_p^{\ell-1} \mid v_p(\det(M(a))) = mi\} &= \sum_{v_1+\cdots v_n=i} \frac{1}{p^{m(v_1+\cdots+v_n)}} \left(1 - \frac{1}{p^m}\right)^n \\ &= \binom{i+n-1}{n-1} \frac{1}{p^{mi}} \left(1 - \frac{1}{p^m}\right)^n. \qquad \square\end{aligned}$$

In particular Conjecture 1 is just a reformulation of Conjecture 1′ using Theorem 9.

6. Numerical evidence

We have investigated Conjecture 1 (and 1′) numerically for $\ell \in \{5, 7\}$. Recall that Conjecture 1 states that for a prime $p \neq 2, \ell$ with $\operatorname{ord}_\ell(p) = m$, $\ell - 1 = mn$ and $\mathrm{T} \in \{\mathrm{un}, \mathrm{ram}\}$ we have $v_p(R_p(K)) \in m\mathbb{Z} + v_\mathrm{T}$ for all $K \in \mathcal{K}_p^\mathrm{T}$ and for $i \geq 0$ we have

$$\lim_{D\to\infty} \frac{\#\{K \in \mathcal{K}_p^\mathrm{T}(D) \mid v_p(R_p(K)) = i + v_\mathrm{T}\}}{\#\mathcal{K}_p^\mathrm{T}(D)} = \operatorname{pr}(P_{\ell,p} = i),$$

$$\lim_{D\to\infty} \frac{\#\{K \in \mathcal{K}_p^\mathrm{T}(D) \mid v_p(R_p(K)) = mi + v_\mathrm{T}\}}{\#\mathcal{K}_p^\mathrm{T}(D)} = \binom{i+n-1}{n-1} \frac{1}{p^{mi}} \left(1 - \frac{1}{p^m}\right)^n.$$

where $v_\mathrm{un} = \ell - 1$ and $v_\mathrm{ram} = (\ell - 1)/2$. As the right hand side of this equation is straight forward to calculate, only the limit on the left hand side had to be investigated. Thus to test our conjecture we needed both an algorithm to compute a large number of cyclic extensions and their p-adic regulators. We use an algorithm based on global class field theory as provided by Fieker in [Fie01] to obtain a list of cyclic quintic and septic extensions. For the computation of the p-adic regulators, we relied on the methods from Fieker and Zhang [FZ16]. A more detailed discussion of the algorithms can be found in these references.

6.1. **Cyclic quintic extensions.** We have computed the valuation of p-adic regulators for all cyclic quintic extensions with discriminant up to $5{\cdot}10^{31}$ for $2 < p < 100$, $p \neq \ell$. The computations were carried out using Magma [BCP97]. For these 5 521 222 fields, the values

$$\frac{\#\{K \in \mathcal{K}_p^\mathrm{T}(5 \cdot 10^{31}) \mid v_p(R_p(K)) = j\}}{\#\mathcal{K}_p^\mathrm{T}(5 \cdot 10^{31})}$$

are presented in Tables 1–4 and compared to the values as predicted by Conjecture 1. Note that in Table 1 and 2 for $p = 11$ the fields with $v_p(R_p(K)) \in \{11, 12, 13\}$ and $v_p(R_p(K)) \in \{9\}$ respectively have been omitted for brevity.

Moreover, the conjecture predicts that the valuations occur in an arithmetic progression with an initial value of $\ell - 1$ or $(\ell - 1)/2$ and common difference $\operatorname{ord}_\ell(p)$; indeed, no valuations not in this arithmetic progression were observed. For example, when $p = 13$ we have $\operatorname{ord}_5(13) = 4$, and the conjecture predicts that all valuations must be multiples of 4, and no valuation that is not a multiple of 4 were observed.

6.2. **Cyclic septic extensions.** The same computations as in the quintic case were carried out for all 329 708 cyclic septic extensions of discriminant $\leq 10^{42}$, see Tables 5–9. Again, no valuations not predicted by Conjecture 1 were observed in the computation.

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

TABLE 1. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p) = 1$ and p is unramified

p	$\#\mathcal{K}_p^{\mathrm{un}}(5 \cdot 10^{31})$	4	5	6	7	8	9	10
11	4 049 077	.68249	.24878	.05655	.01026	.00162	.237E-3	.326E-4
Conjecture 1		.68301	.24836	.05644	.01026	.00163	.237E-3	.323E-4
31	4 890 617	.87712	.11313	.00913	.567E-3	.331E-4	.204E-5	.204E-6
Conjecture 1		.87707	.11317	.00912	.588E-3	.332E-4	.171E-5	.830E-7
41	5 030 537	.90597	.08837	.00538	.253E-3	.115E-4	.198E-6	0
Conjecture 1		.90595	.08838	.00538	.262E-3	.112E-4	.437E-6	.160E-7
61	5 181 713	.93575	.06163	.00252	.849E-4	.173E-5	0	0
Conjecture 1		.93602	.06137	.00251	.824E-4	.236E-5	.620E-7	.152E-8
71	5 226 957	.94495	.05311	.00187	.549E-4	.765E-6	0	0
Conjecture 1		.94484	.05323	.00187	.527E-4	.130E-5	.293E-7	.619E-9

TABLE 2. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p) = 1$ and p is ramified

p	$\#\mathcal{K}_p^{\mathrm{ram}}(5 \cdot 10^{31})$	2	3	4	5	6	7	8
11	1 472 145	.68262	.24847	.05671	.01028	.00161	.247E-3	.319E-4
Conjecture 1		.68301	.24836	.05644	.01026	.00163	.237E-3	.323E-4
31	630 605	.87763	.11259	.00909	.629E-3	.428E-4	.158E-5	0
Conjecture 1		.87707	.11317	.00912	.588E-3	.332E-4	.171E-5	.830E-7
41	490 685	.90685	.08748	.00538	.258E-3	.142E-4	0	0
Conjecture 1		.90595	.08838	.00538	.262E-3	.112E-4	.437E-6	.160E-7
61	339 509	.93634	.06122	.00234	.854E-4	0	0	0
Conjecture 1		.93602	.06137	.00251	.824E-4	.236E-5	.626E-7	.152E-8
71	294 265	.94497	.05291	.00207	.407E-4	0	0	0
Conjecture 1		.94484	.05323	.00187	.527E-4	.130E-5	.293E-7	.619E-9

TABLE 3. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p) = 2$

p	$\#\mathcal{K}_p^{\mathrm{un}}(5 \cdot 10^{31})$	4	6	8	10
19	5 521 222	.99447	.00550	.210E-4	.181E-6
Conjecture 1		.99446	.00550	.228E-4	.845E-7
29	5 521 222	.99762	.00237	.507E-5	0
Conjecture 1		.99762	.00237	.423E-5	.670E-8
59	5 521 222	.99942	.570E-3	.362E-6	0
Conjecture 1		.99942	.574E-3	.247E-6	.947E-10
79	5 521 222	.99967	.324E-3	0	0
Conjecture 1		.99967	.320E-3	.769E-7	.164E-10
89	5 521 222	.99974	.252E-3	0	0
Conjecture 1		.99974	.252E-3	.478E-7	.804E-11

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

TABLE 4. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p) = 4$

p	$\#\mathcal{K}_p^{\mathrm{un}}(5 \cdot 10^{31})$	4	8	12	16
3	5 521 222	.98766	.01218	.142E-3	.181E-5
Conjecture 1		.98765	.01219	.150E-3	.185E-5
7	5 521 222	.99958	.413E-3	0	0
Conjecture 1		.99958	.416E-3	.173E-6	.722E-10
13	5 521 222	.99996	.354E-4	0	0
Conjecture 1		.99996	.350E-4	.122E-8	.429E-13
17	5 521 222	.99998	.110E-4	0	0
Conjecture 1		.99998	.119E-4	.143E-9	.171E-14
23	5 521 222	.99999	.271E-5	0	0
Conjecture 1		.99999	.357E-5	.127E-10	.456E-16
37	5 521 222	.99999	.126E-5	0	0
Conjecture 1		.99999	.533E-6	.284E-12	.151E-18
43	5 521 222	.99999	.181E-6	0	0
Conjecture 1		.99999	.292E-6	.855E-13	.250E-19
47	5 521 222	.99999	.181E-6	0	0
Conjecture 1		.99999	.204E-6	.419E-13	.860E-20
53	5 521 222	1	0	0	0
Conjecture 1		.99999	.126E-6	.160E-13	.203E-20
67	5 521 222	1	0	0	0
Conjecture 1		.99999	.496E-7	.246E-14	.122E-21
73	5 521 222	1	0	0	0
Conjecture 1		.99999	.352E-7	.123E-14	.436E-22
83	5 521 222	1	0	0	0
Conjecture 1		.99999	.210E-7	.443E-15	.935E-23
97	5 521 222	1	0	0	0
Conjecture 1		.99999	.112E-7	.127E-15	.144E-23

TABLE 5. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 1$ and p is unramified

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	7	8	9	10	11
29	273 289	.81036	.16753	.01990	.00204	.135E-3	.109E-4
Conjecture 1		.81014	.16761	.02022	.00186	.144E-3	.995E-5
43	289 489	.86861	.12041	.01034	.571E-3	.497E-4	.345E-5
Conjecture 1		.86833	.12116	.00986	.611E-3	.320E-4	.148E-5
71	304 141	.91805	.07774	.00400	.174E-3	.131E-4	0
Conjecture 1		.91841	.07761	.00382	.143E-3	.455E-5	.128E-6

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

TABLE 6. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 1$ and p is ramified

p	$\#\mathcal{K}_p^{\mathrm{ram}}(10^{42})$	3	4	5	6	7
29	56 419	.81070	.16575	.02164	.00171	.177E-3
Conjecture 1		.81014	.16761	.02022	.00186	.144E-3
43	40 219	.86861	.12041	.01034	.571E-3	.497E-4
Conjecture 1		.86833	.12116	.00986	.611E-3	.320E-4
71	25 567	.91977	.07713	.00297	.117E-3	0
Conjecture 1		.91841	.07761	.00382	.143E-3	.455E-5

TABLE 7. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 2$

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	8	10
13	329 708	.98216	.01766	.175E-3
Conjecture 1		.98235	.01743	.206E-3
41	329 708	.99814	.00184	.303E-5
Conjecture 1		.99821	.00178	.211E-5
83	329 708	. 99957	.421E-3	0
Conjecture 1		.99956	.435E-3	.126E-6
97	329 708	.99971	.288E-3	0
Conjecture 1		.99968	.318E-3	.677E-7

TABLE 8. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 3$

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	9
11	329 708	.99857	.00142
Conjecture 1		.99849	.00150
23	329 708	.99984	.157E-3
Conjecture 1		.99983	.164E-3
37	329 708	.99996	.363E-4
Conjecture 1		.99996	.394E-4

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	9
53	329 708	.99998	.151E-4
Conjecture 1		.99998	.134E-4
67	329 708	.99998	.121E-4
Conjecture 1		.99999	.664E-5
79	329 708	.99999	.303E-5
Conjecture 1		.99999	.405E-5

TABLE 9. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 6$

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	12
3	329 708	.99865	.00134
Conjecture 1		.99862	.00136
5	329 708	.99992	.758E-4
Conjecture 1		.99993	.639E-4
17	329 708	1	0
Conjecture 1		.99999	.414E-7
19	329 708	1	0
Conjecture 1		.99999	.212E-7
31	329 708	1	0
Conjecture 1		.99999	.112E-8

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	12
47	329 708	1	0
Conjecture 1		.99999	.927E-11
59	329 708	1	0
Conjecture 1		.99999	.237E-10
61	329 708	1	0
Conjecture 1		.99999	.194E-10
73	329 708	1	0
Conjecture 1		.99999	.660E-11
89	329 708	1	0
Conjecture 1		.99999	.201E-11

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bru67] Armand Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[Buc90] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, 1990.

[Coa77] John Coates. p-adic L-functions and Iwasawa's theory. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 269–353. Academic Press, London, 1977.

[Dav79] Philip J. Davis. *Circulant matrices*. John Wiley & Sons, New York-Chichester-Brisbane, 1979. A Wiley-Interscience Publication, Pure and Applied Mathematics.

[Fie01] Claus Fieker. Computing class fields via the Artin map. *Math. Comp.*, 70(235):1293–1303, 2001.

[FZ16] Claus Fieker and Yinan Zhang. An application of the p-adic analytic class number formula. *LMS J. Comput. Math.*, 19(1):217–228, 2016.

[Hak07] Tuomas Hakkarianen. *On the computation of class numbers of real abelian fields*. dissertation, University of Turku, 2007.

[HZ16] Tommy Hofmann and Yinan Zhang. Valuations of p-adic regulators of cyclic cubic fields. *J. Number Theory*, 169:86–102, 2016.

[Iwa72] Kenkichi Iwasawa. *Lectures on p-adic L-functions*. Princeton University Press, Princeton; University of Tokyo Press, Tokyo, 1972. Annals of Mathematics Studies, No. 74.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Leo62] Heinrich-Wolfgang Leopoldt. Zur Arithmetik in abelschen Zahlkörpern. *J. Reine Angew. Math.*, 209:54–71, 1962.

[Mar96] František Marko. On the existence of p-units and Minkowski units in totally real cyclic fields. *Abh. Math. Sem. Univ. Hamburg*, 66:89–111, 1996.

[Mik87] Hiroo Miki. On the Leopoldt conjecture on the p-adic regulators. *J. Number Theory*, 26(2):117–128, 1987.

[Pan95] Peter Panayi. *Computation of Leopoldt's p-adic regulator*. Phd thesis, University of East Anglia, 1995.

[Sch93] Oliver Schirokauer. Discrete logarithms and local units. *Philos. Trans. Roy. Soc. London Ser. A*, 345(1676):409–423, 1993.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

Tommy Hofmann, Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany
E-mail address: thofmann@mathematik.uni-kl.de

Yinan Zhang, Mathematical Sciences Institute, Australian National University, Canberra ACT 2601, Australia
E-mail address: yinan.zhang@anu.edu.au

13 Jun 2018 07:31:58 PDT
Version 5 - Submitted to Open Book Series

EXPLICIT COMPUTATIONS IN IWASAWA THEORY

REINIER BRÖKER, DAVID HUBBARD, AND LAWRENCE C. WASHINGTON

Abstract. We give two algorithms to compute layers of the anticyclotomic $\mathbf{Z}_3$-extension of an imaginary quadratic field. The first is based on complex multiplication techniques for nonmaximal orders; the second is based on Kummer theory. As an illustration of our results, we use the mirroring principle to derive results on the structure of class groups of nonmaximal orders.

1. Introduction

Let K be an imaginary quadratic field, with fixed algebraic closure $\overline{K}$, and for a fixed odd prime p, let $K^p \subset \overline{K}$ be the compositum of all $\mathbf{Z}_p$-extensions. The Galois group of K^p/K is isomorphic to $\mathbf{Z}_p^2$, and there are two "natural" $\mathbf{Z}_p$-extensions of K inside K^p. The *cyclotomic* $\mathbf{Z}_p$*-extension* K_p^{cycl} is the p-part of the extension $\bigcup_{n\geq 1} K(\zeta_{p^n}) \subset \overline{K}$. The extension $K_p^{\mathrm{cycl}}/\mathbf{Q}$ is procyclic. The *anticyclotomic* $\mathbf{Z}_p$*-extension* K_p^{anti} is implicitly defined by the property that $K_p^{\mathrm{anti}} \subset \overline{K}$ is the unique $\mathbf{Z}_p$-extension of K that is *prodihedral* over $\mathbf{Q}$, meaning that we have

$$\mathrm{Gal}(K_p^{\mathrm{anti}}/\mathbf{Q}) \cong \mathbf{Z}_p \rtimes \mathbf{Z}/2\mathbf{Z},$$

where the generator of $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$ acts by inversion on $\mathbf{Z}_p$.

The fields K_p^{cycl} and K_p^{anti} are linearly disjoint over K, and their compositum equals K^p. Since both have Galois group $\mathbf{Z}_p$, both extensions are unramified outside of p by [17, Prop. 13.2]. This article focuses on *explicitly computing* layers of K_3^{anti} for the case where 3 is ramified in K. By computing, we mean that on input of a positive integer k, we want to compute an irreducible polynomial $f \in K[x]$ of degree 3^k with

$$K_k = K[x]/(f(x)) \subset K_3^{\mathrm{anti}}.$$

The Galois group $\mathrm{Gal}(K_k/K)$ is cyclic of order 3^k.

Although we believe that most of our techniques can be generalized to arbitrary p and arbitrary splitting behavior of p, our restrictions to $p = 3$ and to the case that 3 ramifies in K allow us to highlight the technical considerations that arise in those cases. Furthermore, we can use the *mirror principle*, see Section 5, to obtain a criterion for when the 3-parts of certain class groups are cyclic.

The main result of this paper is that we have explicit algorithms to compute K_k. We use complex multiplication (CM) techniques in Sections 2 and 3, and Kummer techniques in 6. The CM technique works for any K; the Kummer technique is more restricted.

Previous attempts to compute initial layers of anticyclotomic $\mathbf{Z}_p$-extensions of an imaginary quadratic field include [3, 7, 12, 16]. These papers use a mix of class field theory and decomposition laws of primes.

1991 *Mathematics Subject Classification.* 11R23 (primary), 14K25 (secondary).

Perhaps not surprisingly, the *run times* of our algorithms are inherently exponential. Not only are the outputs of the algorithms polynomials of degree 3^k, but the CM approach computes, as intermediate step, a polynomial whose degree and logarithmic height of its coefficients are both $\widetilde{O}(|\operatorname{disc}(K)|^{1/2}3^k)$. For the Kummer approach, we need a polynomial of degree $O(3^k)$ over an auxilliary extension of degree $O(3^k)$; furthermore, the coefficients are themselves symmetric expressions in $O(3^k|\operatorname{disc}(K)|)$ terms.

Both approaches have their merits. Indeed, whereas the CM method requires the full class group of K as intermediate step, the Kummer method only looks at the prime 3. If the class group is large, then the Kummer method is better for small n. However, the Kummer method requires working over auxilliary extensions and this makes the method slower for larger n.

We detail various techniques we can use to reduce the size of the generating polynomial for K_k in Section 4. We illustrate our techniques with a variety of examples. All examples were done using the computer algebra package MAGMA [2] and the CM software package [10].

2. Anticyclotomic extension and ring class fields

Throughout this section, let $K = \mathbf{Q}(\sqrt{D})$ be a fixed imaginary quadratic field of discriminant D in which 3 is ramified. We let $\mathcal{O}$ be the maximal order of K. For any integer $k \geq 1$, the k-th layer K_k of the anticyclotomic $\mathbf{Z}_3$-extension of K is a generalized dihedral extension of $\mathbf{Q}$. Hence, by Bruckner's result (see [6] or [9, Thm. 9.18]), we know that K_k is contained in a *ring class field* for K. Since K_k is unramified outside 3, it follows that K_k is contained in a ring class field for an order $\mathcal{O}_N = \mathbf{Z} + 3^N\mathcal{O}$ of index 3^N for some $N \geq 1$.

In order to bound the exponent, we analyze ring class fields. We let H_N be the ring class field for the order $\mathcal{O}_N$. With this notation, H_0 is the Hilbert class field of K. The extension H_N/K is abelian and unramified outside 3. The Artin map gives an isomorphism $\operatorname{Pic}(\mathcal{O}_N) \xrightarrow{\sim} \operatorname{Gal}(H_N/K)$, with $\operatorname{Pic}(\mathcal{O}_N)$ the *Picard group* of $\mathcal{O}_N$. We have a natural exact sequence

$$1 \to (\mathcal{O}/3^N\mathcal{O})^*/\operatorname{Im}(\mathcal{O}^*)(\mathbf{Z}/3^N\mathbf{Z})^* \to \operatorname{Pic}(\mathcal{O}_N) \to \operatorname{Pic}(\mathcal{O}) \to 1,$$

where the last map is given by $[I] \mapsto [I \cdot \mathcal{O}]$. The kernel of the map $\operatorname{Pic}(\mathcal{O}_N) \to \operatorname{Pic}(\mathcal{O})$ is naturally isomorphic to $\operatorname{Gal}(H_N/H_0)$; the following lemma gives the structure of this group.

Lemma 2.1. *With the notation from the previous paragraph, we have*

$$\operatorname{Gal}(H_N/H_0) \cong \begin{cases} \mathbf{Z}/3^{N-1}\mathbf{Z} & \text{if } D = -3 \\ \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3^{N-1}\mathbf{Z} & \text{if } D \neq -3, D \equiv -3 \bmod 9 \\ \mathbf{Z}/3^N\mathbf{Z} & \text{if } D \equiv 3 \bmod 9 \end{cases}$$

for $N \geq 1$.

Proof. Let $\mathfrak{p} \mid (3)$ be the ideal of norm 3 in $\mathcal{O}$. We have $(\mathcal{O}/\mathfrak{p}^{2N})^* \cong (A/\mathfrak{p}^{2N})^*$, where A denotes the completion of $\mathcal{O}$ at $\mathfrak{p}$. The ring A is a tamely ramified quadratic extension of $\mathbf{Z}_3$, and it well-known that there are only *two* such rings up to isomorphism. For $D \equiv -3 \bmod 9$, we have $A = \mathbf{Z}_3[\sqrt{-3}] = \mathbf{Z}_3[\zeta_3]$, and $A = \mathbf{Z}_3[\sqrt{3}]$ for $D \equiv 3 \bmod 9$. We analyse both cases separately.

The unit group of $A = \mathbf{Z}_3[\zeta_3]$ equals

$$A^* = \langle -\zeta_3 \rangle \times (1 + \mathfrak{p}^2),$$

and $1+\mathfrak{p}^2$ is torsion free. Hence, $1+\mathfrak{p}^2$ is a free $\mathbf{Z}_3$-module of rank 2. We get

$$(A/3^NA)^* \cong \langle -\zeta_3\rangle \times (1+\mathfrak{p}^2)/(1+\mathfrak{p}^{2N}) \cong \mathbf{Z}/6\mathbf{Z} \times (\mathbf{Z}/3^{N-1}\mathbf{Z})^2,$$

and hence

$$(A/3^NA)^*/(\mathbf{Z}/3^N\mathbf{Z})^* \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3^{N-1}\mathbf{Z}.$$

For $A = \mathbf{Z}_3[\sqrt{3}]$, we have

$$A^* = \langle -1\rangle \times (1+\mathfrak{p}),$$

and since ζ_3 is not contained in A, the $\mathbf{Z}_3$-module $1+\mathfrak{p}$ is torsion free and hence a free rank 2 module. By iteratively applying the "cubing isomorphism" $1+\mathfrak{p}^k \xrightarrow{\sim} 1+\mathfrak{p}^{k+2}$ we see that

$$(A/3^NA)^* \cong \langle -1\rangle \times (1+\mathfrak{p})/(1+\mathfrak{p}^{2N}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3^N\mathbf{Z} \times \mathbf{Z}/3^{N-1}\mathbf{Z}$$

holds. Since the module $1+\mathfrak{p}$ is generated over $\mathbf{Z}_3$ by $1+3$ and $1+\sqrt{3}$, we get

$$(A/3^NA)^*/(\mathbf{Z}/3^N\mathbf{Z})^* \cong \mathbf{Z}/3^N\mathbf{Z}.$$

We have $\mathcal{O}^* = \{\pm 1\}$ for $D < -3$, and the only case where the local cube root of unity exists globally is $D = -3$. Quotienting by $\mathrm{Im}(\mathcal{O}^*)$ gives the lemma. □

For $D \equiv -3 \bmod 9$ with $D < -3$, we let $\alpha_N \in \mathcal{O}$ be an element that is congruent to $\zeta_3 \in A$ modulo 3^N. (As in the proof of Lemma 2.1, A denotes the completion of $\mathcal{O}$ at $\mathfrak{p}$.) This element α_N determines an *Artin symbol* $\left(\frac{\alpha_N}{H_N/H_0}\right) \in \mathrm{Gal}(H_N/H_0)$. We let H'_N be the fixed field of the order 3 subgroup $\langle\left(\frac{\alpha_N}{H_N/H_0}\right)\rangle$ and put

$$H_\infty = \begin{cases} \bigcup_{N\geq 1} H'_N/H_0 & \text{for } D \equiv -3 \bmod 9 \text{ and } D \neq -3 \\ \bigcup_{N\geq 1} H_N/H_0 & \text{otherwise.} \end{cases}$$

Theorem 2.2. *Let K_k be the k-th layer of the anticyclotomic $\mathbf{Z}_3$-extension of K. Then K_k is contained in the ring class field for the order $\mathcal{O}_{k+1} = \mathbf{Z} + 3^{k+1}\mathcal{O}$ of index 3^{k+1}.*

Proof. It is clear that $H_N/\mathbf{Q}$ is generalized dihedral. From the relation

$$\mathcal{O}_N \subseteq \mathcal{O}_M \Longrightarrow H_M \subseteq H_N$$

from class field theory, also known as the *Anordnungssatz* for ring class fields, and Lemma 2.1 we see that

$$\mathrm{Gal}(H_\infty/H_0) \cong \mathbf{Z}_3.$$

An inspection of the sizes in Lemma 2.1 now gives that the compositum K_kH_0 is contained in H_{k+1}. The theorem follows. □

The theory of *complex multiplication* provides us with a means of explicitly computing the extension H_N/K. This theory is usually only developed for *maximal* orders, but it generalizes to nonmaximal orders without too much difficulty. Indeed, by [9, Thm. 11.1] we know that

$$H_N = K[x]/(f_N(x)),$$

with $f_N \in \mathbf{Z}[x]$ the minimal polynomial of the j-invariant of the complex elliptic curve $\mathbf{C}/\mathcal{O}_N$. There are various algorithms to compute f_N; we refer to [1] and the references therein for an overview. However, since the proven upper bound $\widetilde{O}(|\operatorname{disc}(\mathcal{O}_N)^2|)$ (see e.g. [1, Section 5]) on the bit size of f_N is believed to be the actual size of f_N, these algorithms are inherently exponential. We will give various practical improvements in Section 4 to this basic approach.

13 Jun 2018 09:31:26 PDT
Version 3 - Submitted to Open Book Series

3. Selecting the right subfield

As before, let K be a fixed imaginary quadratic field in which 3 is ramified. We have seen that the k-th layer K_k of the anticyclotomic $\mathbf{Z}_3$-extension of K is contained in the ring class field H_{k+1}. In this section we explain a method to compute K_k as a subfield of H_{k+1}. To keep the sizes of the generating polynomials small, the examples given in this section already use the algorithmic improvements explained in Section 4. Magma code to compute the examples is available at [4].

We first assume that K has trivial 3-Hilbert class field. In this case, we have

$$[H_k : K_k] = \#\operatorname{Pic}(\mathcal{O}) \quad \text{for } D \equiv 3 \bmod 9$$

and K_k is the unique subfield of H_k that has degree 3^k over K. For $K = \mathbf{Q}(\sqrt{-3})$, K_k is the unique subfield of degree 3^k of H_{k+1}. For other $D \equiv -3 \bmod 9$, we proceed as follows. As in the discussion preceding Theorem 2.2, we let $\alpha_{k+1} \in \mathcal{O}$ be locally congruent to ζ_3 modulo 3^{k+1}. The fixed field H'_{k+1} of the automorphism $\left(\frac{\alpha_{k+1}}{H_{k+1}/H_0}\right)$ has a unique subfield of degree 3^k over K; this field is the field K_k that we are after.

Example 3.1. *The field $K = \mathbf{Q}(\sqrt{-21})$ has class group isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$. The index 4 subfield of the ring class field H_1 is generated by a root of $x^3 - 6x - 12$, but it is not part of the anticyclotomic $\mathbf{Z}_3$-extension.*

The index 4 subfield $\widetilde{K}_1$ of the ring class field H_2 is obtained by adjoining a root of

$$x^9 + 12x^6 + 81x^5 + 144x^4 + 30x^3 - 324x^2 - 504x - 336$$

to K. The Galois group $\widetilde{K}_1/K$ is isomorphic to $(\mathbf{Z}/3\mathbf{Z})^2$. To obtain the first layer, we compute that $\alpha_2 = 1 + \sqrt{-21}$ is locally congruent to ζ_3 modulo 9. We take the fixed field of the Artin symbol corresponding to α_2. We find that K_1 is generated by a root of

$$x^3 + 9x - 12$$

over K.

For the general case, we let $H_{0,3}$ be the 3-Hilbert class field of K. The extension H_∞/H_0 naturally defines a $\mathbf{Z}_3$-extension $H_{\infty,3}/H_{0,3}$. The sequence

$$1 \to \operatorname{Gal}(H_{\infty,3}/H_{0,3}) \to \operatorname{Gal}(H_{\infty,3}/K) \to \operatorname{Gal}(H_{0,3}/K) \to 1 \tag{1}$$

need not split in general. If it does split, then $H_{0,3}$ is *not* contained in the anticyclotomic $\mathbf{Z}_3$-extension and finding the layers proceeds as before. Determining whether the sequence splits is often easy. In Section 5, we will give a simple criterion (Theorem 5.1) under which $H_{0,3}$ is not contained in the anticyclotomic $\mathbf{Z}_3$-extension. Furthermore, the following examples show that it is computationally very easy to determine if $H_{0,3}$ lies in the anticyclotomic $\mathbf{Z}_3$-extension or not.

Example 3.2. *Fix $K = \mathbf{Q}(\sqrt{-87})$. The class group of $\mathcal{O}$ is cyclic of order 6. The order $\mathcal{O}_1$ of index 3 has cyclic Picard group of order 18. We may replace $H_{\infty,3}$ with $H_{1,3}$ in Sequence (1) to obtain the nonsplit sequence*

$$1 \to \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/9\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z} \to 1.$$

Hence, the 3-part of the Hilbert class field of K is the first layer of the anticyclotomic $\mathbf{Z}_3$-extension. Explicitly, we have

$$K_1 = K[x]/(x^3 - x^2 + 2x + 1).$$

The index 2 subfield of the ring class field for $\mathcal{O}_1$ gives the second layer of the anticyclotomic $\mathbf{Z}_3$ extension. It is generated by a root of

$$x^9 + 3x^8 + 6x^7 + 14x^6 + 9x^5 + 21x^4 + 6x^3 + 12x^2 + 3.$$

For $K = \mathbf{Q}(\sqrt{-771})$ we obtain the split sequence

$$1 \to \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z} \to 1$$

and the Hilbert class field is not contained in the anticyclotomic $\mathbf{Z}_3$-extension.

If the 3-part of $\mathrm{Pic}(\mathcal{O})$ is different from $\mathbf{Z}/3\mathbf{Z}$, the situation is slightly more involved. In the remainder of this section we explain how to split the 3-part $\mathrm{Pic}(\mathcal{O})_3$ into a part "inside" and a part "outside" of the anticyclotomic $\mathbf{Z}_3$-extension.

We let $S_{\max} \subseteq \mathrm{Pic}(\mathcal{O})_3$ be the largest subgroup (with respect to inclusion) for which the sequence

$$1 \to \mathrm{Gal}(H_{\infty,3}/H_{0,3}) \to \mathrm{Gal}(H_{\infty,3}/H_{0,3}^{S_{\max}}) \to S_{\max} \to 1$$

splits. Here, $H_{0,3}^{S_{\max}}$ is the fixed field of $H_{0,3}$ for $S_{\max}$. This fixed field is the largest subfield of $H_{0,3}$ that is contained in the anticyclotomic $\mathbf{Z}_3$-extension.

For ease of notation, we restrict to the case $D \equiv 3 \bmod 9$ so $H_{\infty,3}$ is the inverse limit of the 3-parts $\mathrm{Pic}(\mathcal{O}_N)_3$ of the ring class field for $\mathcal{O}_N$. Let $\langle \mathfrak{p} \rangle \subset \mathrm{Pic}(\mathcal{O})_3$ be a subgroup of 3-power order with $\mathfrak{p}$ coprime to 3. The ideal $\mathfrak{p} \cap \mathcal{O}_N$ is an invertible $\mathcal{O}_N$-ideal whose class in $\mathrm{Pic}(\mathcal{O}_N)_3$ maps to the class of $\mathfrak{p}$ in $\mathrm{Pic}(\mathcal{O})_3$. The other preimages are $(\mathfrak{p} \cap \mathcal{O}_N)I$, with I ranging over the kernel of $\mathrm{Pic}(\mathcal{O}_N)_3 \to \mathrm{Pic}(\mathcal{O})_3$. We compute the order inside $\mathrm{Pic}(\mathcal{O}_N)_3$ for each of the preimages of $\mathfrak{p}$, and check if one of those equals the order of $[\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O})_3$. If it does, the sequence

$$1 \to \mathrm{Gal}(H_{N,3}/H_{0,3}) \to \mathrm{Gal}(H_{N,3}/H_{0,3}^{\langle \mathfrak{p} \rangle}) \to \langle \mathfrak{p} \rangle \to 1$$

splits; otherwise it does not.

Example 3.3. *Fix $K = \mathbf{Q}(\sqrt{-6789})$. We have $\mathrm{Pic}(\mathcal{O}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ and $\mathrm{Pic}(\mathcal{O}_1) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z}$. The kernel of the map $\mathrm{Pic}(\mathcal{O}_1) \to \mathrm{Pic}(\mathcal{O})$ is generated by the class of the $\mathcal{O}_1$-ideal*

$$I = \mathcal{O}_1(9, 3\sqrt{-6789} - 3)$$

of norm 9. There are four subgroups of $\mathrm{Pic}(\mathcal{O})$ of index 3; elements of order 6 in these subgroups are ideals of norm 5, 7, 11 and 97, respectively. The ideal $\mathfrak{p}_5$ has order 6 in $\mathrm{Pic}(\mathcal{O})$, but $I^k(\mathfrak{p} \cap \mathcal{O}_1)$ has order 18 for $k = 0, 1, 2$. Likewise for $\mathfrak{p}_7$ and $\mathfrak{p}_{97}$. On the other hand, the ideal $(\mathfrak{p}_{11} \cap \mathcal{O}_1)$ has order 6.

The fixed field of H_0 under the subgroup of $\mathrm{Pic}(\mathcal{O})$ generated by $\mathfrak{p}_{11}$ (of order 6), $\mathfrak{p}_5^3$ (of order 2) and $\mathfrak{p}_2 = \mathcal{O}_1(2, 3\sqrt{-6789} + 1)$ (of order 2) equals the first layer K_1 of the anticyclotomic $\mathbf{Z}_3$-extension of K. To find a generating polynomial, we compute the maximal real subfield of H_0 using CM theory and compute its 4 degree 3 subfields $L_1, \ldots, L_4$. We now check whether the Artin symbol corresponding to $\mathfrak{p}_{11}$ acts trivially on KL_i/K. As expected, it does so for a unique field. In the end, we find that a root of

$$x^3 - x^2 + 8x + 124$$

generates K_1/K.

4. Practical improvements

The techniques described yield generating polynomials that are much larger than necessary. The reason for this is that the j-function is *not* the right function to use from a practical perspective to compute a ring class field. For every given discriminant, a suitably chosen *class invariant* can be used instead. The use of class invariants dates back to Weber's days, and modern treatments rely on *Shimura reciprocity*. We refer to [15, 13] for good descriptions and give the main result that we need.

Theorem 4.1. *Let $D < 0$ be a discriminant, and choose a quadratic generator τ for the imaginary order of discriminant D. Then there exists a modular function f of level $n > 1$ such that $f(\tau)$ generates the ring class field; furthermore, the minimal polynomial of $f(\tau)$ over $K = \mathbf{Q}(\sqrt{D})$ can be explicitly computed in time $\widetilde{O}(|D|)$.*

Proof. We refer to [13, Thm. 4] and [11, Cor. 3.1] for two classes of functions. □

The size of the generating polynomial for the ring class field depends on the choice of the function f in the theorem. To compute the 'reduction factor', we let $\Psi(j, f) = 0$ be the irreducible polynomial relation between j and f and put

$$r(f) = \frac{\deg_f(\Psi(f, j))}{\deg_j(\Psi(f, j))} \in \mathbf{Q}_{>0}.$$

As in [5, Sec. 4], we expect the logarithmic height of the coefficients of the minimal polynomial of $f(\tau)$ to be a factor $r(f)$ smaller than the corresponding coefficients for $j(\tau)$. By [5, Thm. 4.1], we have

$$r(f) \leq 800/7 \approx 114.28.$$

If 2 splits in $\mathcal{O}$, then the cube of the Weber-$\mathfrak{f}$ can be used. This function satisfies $(\mathfrak{f}^{24} - 16)^3 - j\mathfrak{f}^{24} = 0$ and has reduction factor $72/3 = 24$. If 2 is inert, we can use a suitably chosen *double η-quotient*. The exact reduction factor depends on the choice of the η-quotient; we refer to [11] for details. We can use the CM software package [10] by Enge to compute the necessary ring class fields. This package can select the modular function, so that only the discriminant D is required.

Example 4.2. *Let $K = \mathbf{Q}(\sqrt{-3})$. To obtain the first nontrival layer of the anticyclotomic $\mathbf{Z}_3$-extension, we compute the ring class field for the order $\mathcal{O}_2$. If we use the j-function, we obtain a cubic polynomial with constant term*

$$2^{45} \cdot 3 \cdot 5^9 \cdot 11^3 \cdot 23^3.$$

In this case, a suitably chosen double η-quotient yields a class invariant. Using the package [10]*, we obtain the polynomial*

$$x^3 - 12x^2 - 6x - 1.$$

We stress that by class invariants, we can only gain a *constant factor* in the size of the coefficients, and that our method is inherently exponential in $\log |D|$. To push the range of examples further, we can employ *lattice basis reduction*. Indeed, if we have computed a polynomial $f(x)$ that generates the ring class field, we can view the order defined by f as a *lattice* in Euclidean space. If the degree and the coefficients of f are not too big, we can compute a short basis for this lattice and obtain a "better" polynomial.

13 Jun 2018 09:31:26 PDT
Version 3 - Submitted to Open Book Series

Example 4.3. *For $K = \mathbf{Q}(\sqrt{-3})$, the polynomial $f \in \mathbf{Z}[x]$ for $\mathcal{O}_3$ given by Enge's program has coefficients in between -24930 and 29559. We view $\mathbf{Z}[x]/(f)$ as a lattice and after lattice basis reduction, we obtain the polynomial*

$$x^9 + 9x^6 + 27x^3 + 3.$$

Using the same technique, we find the polynomial

$$x^{27} + 27x^{24} + 324x^{21} + 1980x^{18} + 5022x^{15}$$

$$-8262x^{12} - 30348x^9 + 304236x^6 + 1365417x^3 + 3$$

for the third layer of the anticyclotomic $\mathbf{Z}_3$-extension.

5. Mirror principle

In this section we give an application of the *mirror principle* that relates the class groups of the imaginary quadratic field $\mathbf{Q}(\sqrt{D})$ and the real quadratic field $\mathbf{Q}(\sqrt{-D/3})$. This allows us to prove the following theorem that was alluded to in Example 3.2.

Theorem 5.1. *Let $D \equiv 3 \bmod 9$ be a negative discriminant, and assume that 3 does not divide the class number of the real quadratic field $\mathbf{Q}(\sqrt{-D/3})$. Then the 3-Hilbert class field of $K = \mathbf{Q}(\sqrt{D})$ is contained in the anticyclotomic $\mathbf{Z}_3$-extension of K.*

The proof of the theorem relies on the following lemma. The proof of this lemma is very similar to the proof of Scholz' mirror theorem [14].

Lemma 5.2. *Let $D \equiv 3 \bmod 9$ be a negative discriminant, and assume that 3 does not divide the class number of the real quadratic field $\mathbf{Q}(\sqrt{-D/3})$. Then, there exists exactly one degree 3 extension of $\mathbf{Q}(\sqrt{D})$ that is unramified outside 3 and dihedral over $\mathbf{Q}$.*

Proof. Let $K = \mathbf{Q}(\sqrt{D})$ and let L/K be a degree 3 extension that is unramified outside 3 and dihedral over $\mathbf{Q}$. The field L fits inside Diagram 1 below. This diagram also defines automorphisms τ, σ and φ. By abuse of notation, τ denotes both a generator of $\mathrm{Gal}(L/K)$ and its unique lift to $\mathrm{Gal}(L(\zeta_3)/V)$; likewise for σ and φ. Because $L(\zeta_3)/V$ is a Kummer extension, we can write $L(\zeta_3) = V(\sqrt[3]{\alpha})$ with $\alpha \in V$.

Any such $L(\zeta_3)$ will have φ acting trivially on the corresponding τ as well as have σ acting as -1 on τ. Our proof proceeds by showing that both the field of definition and the norm of α are very restricted.

First we show that α can be taken to lie in the real quadratic field $F = \mathbf{Q}(\sqrt{-D/3})$. The *Kummer pairing*

$$\langle \alpha \rangle / \langle \alpha^3 \rangle \times \langle \tau \rangle \to \mu_3$$

is Galois equivariant, and since σ acts on ζ_3 as -1 and on τ as -1, we see that σ acts as $+1$ on $\alpha \bmod (V^*)^3$. We deduce that $\sigma(\alpha) = \alpha \cdot \beta^3$ for some $\beta \in V^*$, and hence

$$N_{V/F}(\alpha) = \alpha\sigma(\alpha) \equiv \alpha^2 \bmod \text{cubes}.$$

Since α and α^2 generate the same extension, this shows that we may assume that α lies in F.

Since the extension $L(\zeta_3)/V$ is unramified outside 3, we have $(\alpha) = IJ^3$ for ideals I, J with I a product of primes lying over $(3) \subset \mathbf{Z}$. The assumption that

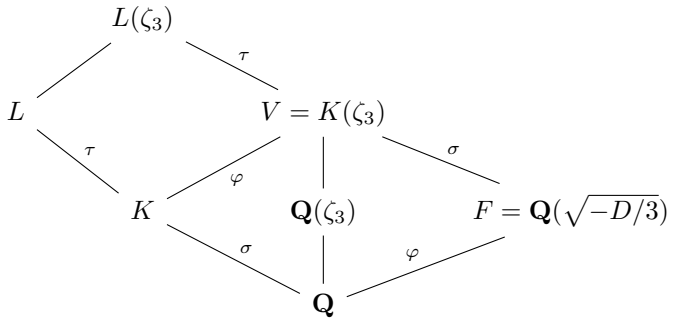


DIAGRAM 1. Diagram of fields for Lemma 5.2

.

3 does not divide the class number of F now implies that we may assume that α is 3-unit. Furthermore, the assumption $D \equiv 3 \bmod 9$ implies that 3 is inert in $\mathbf{Q}(\sqrt{-D/3})$. We get that α is a unit times 3^a for some a. Since $\varphi(\alpha)$ is congruent to α^{-1} modulo cubes, we must have $a \equiv 0 \bmod 3$. Therefore, we may take $\alpha = \pm\varepsilon$, with ε a fundamental unit of F. □

Proof of Theorem 5.1. Since K has a unique cubic extension that is unramified outside 3 and dihedral over $\mathbf{Q}$, the class group of $\mathcal{O}$ has 3-rank at most 1. We write $\mathrm{Pic}(\mathcal{O})_3 = \mathbf{Z}/3^n\mathbf{Z}$ for some $n \geq 0$. We need to prove that the 3-Hilbert class field $H_3(K)$ coincides with the n-th level K_n.

Suppose that we have $H_3(K) \cap K_n = K_k$ for some $k < n$. The Galois group of the compositum $H_3(K)K_n$ over K then has 3-rank 2. This means that there is more than one cubic extension of K contained in $H_3(K)K_n$. All these extensions are unramified outside 3 and dihedral over $\mathbf{Q}$ however; contradiction. □

Lemma 5.2 allows us to deduce a simple sufficient criterion for when the 3-parts $\mathrm{Pic}(\mathcal{O}_N)_3$ are cyclic.

Theorem 5.3. *Assume that* 3 *does not divide the class number of the real quadratic field* $\mathbf{Q}(\sqrt{-D/3})$. *For* $D \equiv 3 \bmod 9$, *the* 3*-part* $\mathrm{Pic}(\mathcal{O}_N)_3$ *is cyclic for all* $N \geq 0$.

Proof. By Theorem 5.1, the sequence

$$1 \to (\mathcal{O}/3^N\mathcal{O})^*/\operatorname{Im}(\mathcal{O}^*)(\mathbf{Z}/3^N\mathbf{Z})^* \to \mathrm{Pic}(\mathcal{O}_N)_3 \to \mathrm{Pic}(\mathcal{O})_3 \to 1$$

does not split for any N. Since the first and last term are cyclic, this means that the middle term is cyclic. □

6. Generators via Kummer theory

In computational class field theory, the 'standard' way to compute an abelian extension of prescribed conductor of a number field K depends on whether K has the appropriate roots of unity. If it does, we can use Kummer theory. If it does not, we adjoin the right root of unity ζ_n to K and compute the right abelian extension of $K(\zeta_n)$ first. Afterwards, we 'descend' down to K. We refer to [8] for a detailed description.

If K is imaginary quadratic, we can use complex multiplication techniques instead and bypass the general method. This is the technique we used in Section 2.

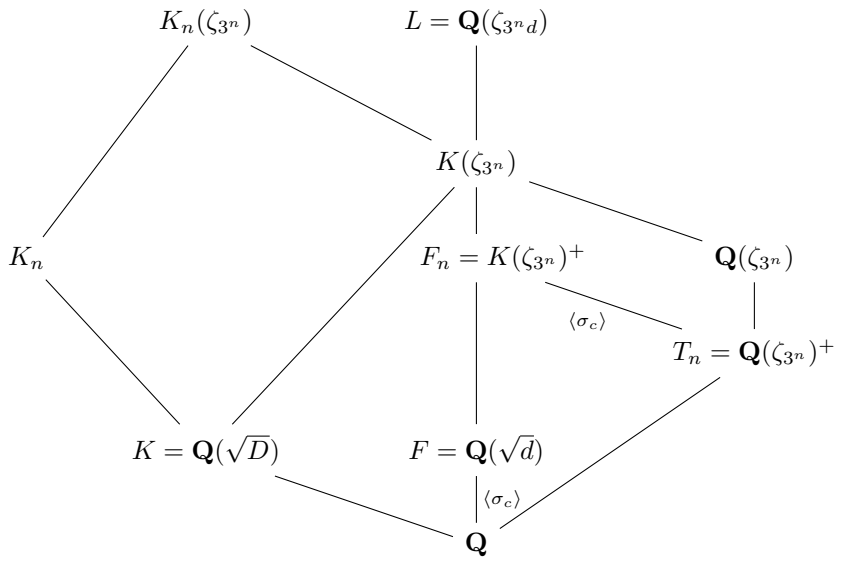


DIAGRAM 2. Diagram of fields for Section 6

.

However, we can make the Kummer theory approach very explicit in our setting. As before, $K = \mathbf{Q}(\sqrt{D})$ is an imaginary quadratic field in which 3 ramifies. Throughout this section, we assume 3 does not divide the class number of the real quadratic field $F = \mathbf{Q}(\sqrt{-D/3})$; we also assume that 3 remains inert in F. This last restriction is essential in Lemma 6.4; the split case appears to be much harder.

Theorem 6.1. *Assume that* 3 *ramifies in* $K = \mathbf{Q}(\sqrt{D})$ *and that* 3 *is inert in* $F = \mathbf{Q}(\sqrt{-D/3})$. *If, furthermore, 3 does not divide the class number of* F, *then the expression for* κ_n *given in Definition 6.7 gives a Kummer generator for* $K_n(\zeta_{3^n})/K(\zeta_{3^n})$ *for* $n \geq 1$.

Once we have computed κ_n, we can use the technique from [8, pp. 514–515] to descend from $K_n(\zeta_{3^n})/K(\zeta_{3^n})$ down to K_n/K.

Diagram 2 defines the various fields we will work in and explains the inclusion relations between them. In this diagram, the + notation indicates the maximal real subfield. We write $d = -D/3$, so that $F = \mathbf{Q}$ for $D = -3$ and F is real quadratic otherwise. If F is quadratic, we let χ be the associated quadratic character of conductor d.

All the base fields we consider are subfields of $L = \mathbf{Q}(\zeta_{3^n d})$; we identify $\mathrm{Gal}(L/\mathbf{Q})$ with $(\mathbf{Z}/3^n d\mathbf{Z})^*$ and for an integer b with $\gcd(b, 3d) = 1$, we let σ_b be the automorphism satisfying $\sigma_b(\zeta_{3^n d}) = \zeta_{3^n d}^b$. For $d \neq 1$, we fix an integer $c \equiv -1 \bmod 3^n$ with $\chi(c) = -1$; we identify $\mathrm{Gal}(F_n/T_n) \cong \mathrm{Gal}(F/\mathbf{Q}) \cong \langle\sigma_c\rangle$ in this case. (For $d = 1$, all statements about σ_c play no role and should be ignored.)

Lemma 6.2. *The class number of* F_n *is coprime to 3.*

Proof. By assumption, 3 remains inert in $F/\mathbf{Q}$. As the extension F_n/F has only one ramified prime and is totally ramified, the lemma follows from [17, Thm. 10.4]. □

The techniques of the proof of Lemma 5.2 shows that we may assume that the desired element κ_n lies in F_n. Furthermore, since the class number of F_n is coprime to 3, this proof also shows that κ_n is a 3-unit in F_n.

Furthermore, we claim that we may assume that σ_c inverts κ_n. To see this, note that $K(\zeta_{3^n d})/K$ is disjoint from K_∞/K, and σ_c therefore acts trivially on $\mathrm{Gal}(K_n(\zeta_{3^n})/K(\zeta_{3^n}))$. It also acts by inversion on ζ_{3^n}. Therefore, the Kummer pairing tells us that σ_c acts by inversion on κ_n modulo 3^n-th powers, i.e., we have $\kappa_n^{\sigma_c} = \kappa_n^{-1}\gamma^{3^n}$ for some γ. But then $\kappa_n^{1-\sigma_c} = \kappa_n^2\gamma^{-3^n}$ generates the same extension and is inverted by σ_c since $\sigma_c^2 = 1$ on $K(\zeta_{3^n})$.

Let E_n be the group of 3-units of F_n. Let E_n^- denote the subgroup consisting of elements that are inverted by σ_c, and E_n^+ denote those that are fixed (and hence lie in T_n). We will compute a valid κ_n as a product of suitably chosen 3-units in E_n^-. For $n \geq 1$, we define

$$\xi_n = \prod_{\substack{1 \leq a \leq 3^n d \\ a \equiv \pm 1 \bmod 3^n \\ (a,d)=1}} (1 - \zeta_{3^n d}^a)^{\chi(a)}.$$

The product is over values of a representing elements of $\mathrm{Gal}(L/T_n)$. We claim that ξ_n lies in F_n. Indeed, for $\sigma_b \in \mathrm{Gal}(L/F_n)$ we have $b \equiv \pm 1 \bmod 3^n$ and $\chi(b) = 1$. The computation

$$\sigma_b(\xi_n) = \prod_{\substack{1 \leq a \leq 3^n d \\ a \equiv \pm 1 \bmod 3^n \\ (a,d)=1}} (1 - \zeta_{3^n d}^{ab})^{\chi(a)} \qquad = \prod_{\substack{1 \leq a \leq 3^n d \\ a \equiv \pm 1 \bmod 3^n \\ (a,d)=1}} (1 - \zeta_{3^n d}^{a})^{\chi(a/b)} = \xi_n$$

gives $\xi_n \in F_n$.

Lemma 6.3. (a) $\xi_n \in E_n^-$.

(b) *The norm of ξ_n from F_n to F_{n-1} is ξ_{n-1}.*

Proof. For part (a), a simple computation shows that $\sigma_c(\xi_n) = \xi_n^{-1}$. If $d \neq 1$, every factor $1 - \zeta_{3^n d}^a$ is a unit, so ξ_n is a unit. If $d = 1$, then each factor is a 3-unit. Therefore, $\xi_n \in E_n^-$.

For (b), we note that the Galois conjugates of ζ_{3^n} for $L/\mathbf{Q}(\zeta_{3^{n-1}d})$ are $\zeta_{3^n}\zeta_3^i$ for $i = 0, 1, 2$. Therefore, the norm of the factor $(1 - \zeta_{3^n d}^a)$ is

$$\prod_{i=0,1,2} (1 - \zeta_{3^n d}^a \zeta_3^i) = (1 - \zeta_{3^n d}^{3a}) = (1 - \zeta_{3^{n-1} d}^a),$$

and the result folows. □

Lemma 6.4. *The $\sigma_j(\xi_n)$ for $\sigma_j \in Gal(F_n/F)$ are independent 3-units and generate a subgroup of E_n^- of index prime to 3.*

Proof. We need some preliminary work. Since keeping track of powers of 2 is irrelevant for what we do, for numbers a and b we use the notation $a \approx b$ to say that a/b is a power of 2, up to sign. When a, b are groups, $a \approx b$ means that a and b are subgroups of some larger group G with $[G : a]/[G : b]$ equal to a power of 2.

Since $\sigma_c^2 = 1$ on F_n, the identity $x^2 = x^{1-\sigma_c}x^{1+\sigma_c}$, implies

$$E_n \approx E_n^- \oplus E_n^+.$$

Let $\{u_1, \ldots, u_{3^{n-1}}\}$ be a basis for E_n^- and $\{v_1, \ldots v_{3^{n-1}-1}\}$ be a basis for E_n^+ mod $\{\pm 1\}$. The Galois group of $F_n/\mathbf{Q}$ is given by the elements σ_j and $\sigma_c\sigma_j$, where σ_j

runs through $\mathrm{Gal}(F_n/F)$. These can be used to calculate the regulator R_n of F_n, up to powers of 2. Let

$$R_n^- = (\log|\sigma_j(u_i)|_{j,i}) \quad \text{and} \quad R_n^+ = (\log|\sigma_j(v_i)|_{j,i}).$$

Then R_n, up to powers of 2, is the absolute value of the determinant of the matrix

$$\begin{pmatrix} R_n^- & R_n^+ \\ -R_n^- & R_n^+ \end{pmatrix}$$

with the last row deleted. Adding the top rows to the corresponding bottom rows yields a 0-block in the lower left and twice R_n^+ in the lower right. Therefore,

$$R_n \approx \det(R_n^-)\det(R_n^+).$$

Note that $\det(R_n^+)$ is, up to powers of 2, the regulator of T_n.

We define the regulator

$$R_{\xi_n} = |\det(\log|\sigma_j\sigma_i^{-1}\xi_n|)|, \qquad i,j \in \mathrm{Gal}(F_n/F)$$

of the $\mathrm{Gal}(F_n/F)$-conjugates of ξ_n. We claim that

$$\det(R_n^-) \approx \frac{h(F_n)R_{\xi_n}}{h(T_n)}.$$

holds. (Here, $h(\cdot)$ denotes the class number.) Since $R_{\xi_n}/\det(R_n^-)$ is the index in E_n^- of the subgroup generated by the conjugates of ξ_n, the lemma then follows from the observation that both T_n and F_n have class number coprime to 3.

The value R_{ξ_n} is a group determinant, and by [17, Lemma 5.26] we have

$$R_{\xi_n} = \pm\prod_{\psi}\sum_{j}\psi(\sigma_j)\log|\sigma_j\xi_n|,$$

where ψ ranges over the Dirichlet characters for $\mathrm{Gal}(F_n/F) \simeq \mathrm{Gal}(T_n/\mathbf{Q})$, and σ_j ranges over $\mathrm{Gal}(F_n/F)$.

We have

$$\sum_j \psi(j)\log|\sigma_j\xi_n| = \sum_j \psi(j)\sum_a \chi(a)\log|1-\zeta_{3^nd}^{aj}|,$$

where $1 \le a \le 3^nd$, $(a,d)=1$, $a \equiv \pm 1 \bmod 3^n$. This equals

$$\sum_{1\le a\le 3^nd,\,(a,3d)=1} \psi(a)\chi(a)\log|1-\zeta_{3^nd}^{a}|.$$

Recall that if ψ has conductor 3^m with $m \ge 1$, then

$$L(1,\overline{\psi\chi}) = -\frac{g(\overline{\psi\chi})}{3^md}\sum_{1\le a\le 3^md,\,(a,3d)=1}\psi(a)\chi(a)\log|1-\zeta_{3^md}^{a}|,$$

where $g(\overline{\psi\chi})$ is a Gauß sum. Since the values of $\psi(a)$ depend only on $a \bmod 3^m$, we have, for fixed a_0 with $3 \nmid a_0$,

$$\sum_{\substack{1\le a\le 3^nd \\ a\equiv a_0 \bmod 3^md}} \psi(a)\log|1-\zeta_{3^nd}^{a}| = \psi(a_0)\log|1-\zeta_{3^md}^{a_0}|,$$

where we have used the identity $\prod_{\omega^{3^{n-m}}=1}(1-\omega x) = 1-x^{3^{n-m}}$. Therefore,

$$\sum_j \psi(j)\log|\sigma_j\xi_n| = \frac{3^md}{g(\overline{\psi\chi})}L(1,\overline{\psi\chi}).$$

If ψ is trivial, then

$$\sum_j \log|\sigma_j \xi_n| = \log|\mathrm{Norm}_{F_n/F_1}\xi_n| = \log|\xi_1|$$

$$= \sum_{\substack{1\le a\le 3d\\(a,3d)=1}} \chi(a)\log|1-\zeta_{3d}^a|.$$

For fixed a_0,

$$\sum_{\substack{a\equiv a_0 \bmod d\\1\le a\le 3d,(a,3d)=1}} \log|1-\zeta_{3d}^a| = \log|1-\zeta_{3d}^{3a_0}| - \log|1-\zeta_{3d}^{3a_1}|,$$

where $3a_1 \equiv a_0 \pmod d$ and $1 \le 3a_1 \le 3d$. Therefore,

$$\sum_j \log|\sigma_j\xi_n| = \sum_{\substack{1\le a_0\le d\\(a_0,d)=1}} \chi(a_0)\log|1-\zeta_d^{a_0}| - \sum_{\substack{1\le a_1\le d\\(a_1,d)=1}} \chi(3a_1)\log|1-\zeta_d^{a_1}|$$

$$= (1-\chi(3))\frac{-d}{g(\chi)}L(1,\chi).$$

Using that 3 is inert in $F/\mathbf{Q}$, we compute $1-\chi(3)=2$.

From the analytic class number formula, we derive

$$\frac{h(F_n)R_n}{\sqrt{\mathrm{disc}(F_n)}}\,\frac{\sqrt{\mathrm{disc}(R_n)}}{h(T_n)R_n^+} \approx \prod_\psi L(1,\overline{\psi\chi}),$$

where h denotes the class number of the indicated field. By [17, Thm. 3.11 and Cor. 4.6], the Gauß sums, the discriminants, and the conductor $3^m d$ factors cancel, and we obtain

$$\det(R_n^-) \approx \frac{h(F_n)R_{\xi_n}}{h(T_n)}. \qquad \square$$

As a byproduct of the calculation with $\psi = 1$, we obtain the following:

Lemma 6.5. *If $d \neq 1$, then $\xi_1 = \epsilon_0^{-4h(F)}$, where $h(F)$ and ϵ_0 are the class number and fundamental unit of F. If $d = 1$ then $\xi_1 = 3$.*

Proof. Up to sign, the case $d \neq 1$ results from keeping track of the factors of 2. In the definition of ξ_1, we can pair the factors for a and $3d-a$ to see that ξ_1 is totally positive. When $d = 1$, the result follows directly from the definition of ξ_1. $\square$

We have almost done all the preparatory work to construct κ_n. Indeed, by Lemma 6.4 we know that κ_n is a product of Galois conjugates of ξ_n. To pin down the product, we need the following standard result.

Lemma 6.6. *Let $m \ge 1$. Let M be a number field, let ζ_m be a primitive m-th root of unity, and let $\alpha \in M(\zeta_m)^\times$. Let $M(\zeta_m, \alpha^{1/m})/M(\zeta_m)$ be a cyclic extension of degree m. Define a map*

$$\omega : \mathrm{Gal}(M(\zeta_m)/M) \to \mathbf{Z}/m\mathbf{Z}$$

by $\tau(\zeta_m) = \zeta_m^{\omega(\tau)}$. Then $F(\zeta_m, \alpha^{1/m})/M$ is Galois with abelian Galois group if and only if

$$\alpha^{\tau-\omega(\tau)} \in \left(M(\zeta_m)^\times\right)^m$$

holds for all $\tau \in \mathrm{Gal}(M(\zeta_m)/M)$.

Proof. The proof is a standard calculation with the Kummer pairing. See for instance the proof of [17, Thm. 14.7]. □

Choose $\tau \in \mathrm{Gal}(F_n/F)$ satisfying $\tau(\zeta_{3^n}) = \zeta_{3^n}^4$. We have

$$\kappa_n = \prod_{j=0}^{3^{n-1}-1} \tau^j(\xi_n)^{c_j},$$

for some integers c_j. Therefore, taking indices mod 3^{n-1}, we have

$$\kappa_n^\tau = \prod_{j=1}^{3^{n-1}} \tau^j(\xi_n)^{c_{j-1}}.$$

Lemma 6.6 says that $\kappa_n^{\tau-4}$ is a 3^n-th power, and since the elements $\tau^j(\xi_n)$ are multiplicatively independent, we must have

$$c_{j-1} - 4c_j \equiv 0 \pmod{3^n}, \qquad 1 \le j \le 3^{n-1}.$$

This implies that each c_j is uniquely determined mod 3^n by the value of c_0. Therefore, κ_n is uniquely determined up to an integral power and mod 3^n-th powers. Therefore, if we find $\kappa_n \in F_n$ such that

(1) $\kappa_n^{\tau-4}$ is a 3^nth power
(2) κ_n is not a cube in F_n,

then we have a Kummer generator for $K_n(\zeta_{3^n})/K(\zeta_{3^n})$.

For $i \ge 1$, define

$$B_i = \prod_{j=1}^{i-1} \left(\frac{1 + 4^{3^{j-1}} + 16^{3^{j-1}}}{3} \right).$$

Let

$$b_i = (1 - B_i)/3,$$

which is an integer for all $i \ge 1$. Finally, for $i \ge 2$, let

$$D_i(x) = \frac{3(b_i(x-1)-1) - (1 + x^{3^{i-1}} + x^{2\cdot 3^{i-1}})(b_{i-1}(x-1)-1)}{x-4}.$$

Note that the numerator of $D_i(x)$ evaluated at $x = 4$ is

$$3(3b_i - 1) - (1 + 4^{3^{i-1}} + 16^{3^{i-1}})(3b_{i-1} - 1) = 3(-B_i) + (1 + 4^{3^{i-1}} + 16^{3^{i-1}})B_{i-1} = 0,$$

so D_i has integer coefficients. For example, $D_2(x) = x - 1$.

Let

$$\delta_i = \xi_i^{D_i(\tau)} \text{ for } i \ge 2, \quad \beta_i = \xi_i^{b_i(\tau-1)-1} \text{ for } i \ge 1.$$

Then $\xi_i, \beta_i, \delta_i \in F_i$, and

$$\delta_i^{\tau-4} = \frac{\beta_i^3}{\beta_{i-1}}$$

for $i \ge 2$. Moreover,

$$\beta_1 = \xi_1^{b_1(\tau-1)-1} = \xi_1^{-1}.$$

Definition 6.7. *Let $\kappa_1 = \xi_1$, and for $n \ge 2$ let*

$$\kappa_n = \xi_1 \delta_2^3 \cdots \delta_n^{3^{n-1}} \in F_n \subset K(\zeta_{3^n}).$$

We have

$$\kappa_n^{\tau-4} = \xi_1^{-3}\frac{\beta_2^9}{\beta_1^3}\frac{\beta_3^{27}}{\beta_2^9}\cdots\frac{\beta_n^{3^n}}{\beta_{n-1}^{3^{n-1}}}$$

$$= \beta_n^{3^n}.$$

Lemma 6.8. *κ_n is not a cube in $K(\zeta_{3^n})$.*

Proof. The lemma is equivalent to ξ_1 not being a cube in $\mathbf{Q}(\zeta_{3^n})$. Our assumption $3 \nmid h(F)$ implies that $\xi_1 = \epsilon_0^{-4h(F)}$ is not a cube in F (when $d \neq 1$; the case $d = 1$ is trivial), so $x^3 - \xi_1$ generates a non-Galois cubic extension of F that must be disjoint from every abelian extension. Therefore, $\sqrt[3]{\xi_1} \notin K(\zeta_{3^n})$. □

Proof of Thm. 6.1. Lemma 6.8 implies that

$$K(\zeta_{3^n})(\sqrt[3^n]{\kappa_n})/K(\zeta_{3^n})$$

is cyclic of order 3^n. Since $\kappa_n^{\tau-4}$ is a 3^n-th power and κ_n is real, it is the desired Kummer generator for $K_n(\zeta_{3^n})/K(\zeta_{3^n})$. □

Example 6.9. *For $K = \mathbf{Q}(\sqrt{-3})$, we have $\kappa_1 = 3$ and hence $K_1 = \mathbf{Q}(\sqrt{-3}, 3^{1/3})$.*

To obtain the second layer, we compute $D_2(x) = x - 1$ and

$$\kappa_2 = 3\left(\frac{(1-\zeta_9^4)(1-\zeta_9^{-4})}{(1-\zeta_9)(1-\zeta_9^{-1})}\right)^3 = 3\left(\frac{1-\cos(8\pi/9)}{1-\cos(2\pi/9)}\right)^3.$$

We compute that κ_2 is a root of $x^3 - 1710x^2 + 513x - 27$, and $\kappa_2^{1/9}$ is therefore a root of

$$x^{27} - 1710x^{18} + 513x^9 - 27.$$

Having found the extension $K(\zeta_9)(\kappa_2^{1/9})/K(\zeta_9)$, we proceed as in [8, pp. 514–515] *to descend to the extension K_2/K. We compute that K_2 is generated over K by a root of*

$$x^9 - 59049x^3 + 4251528\sqrt{-3}.$$

Example 6.10. *Fix $K = \mathbf{Q}(\sqrt{-87})$. For the first layer, we compute that κ_1 is a root of $x^2 - 727x + 1$. Instead of following the descent procedure from* [8]*, we can also use the following argument to compute K_1/K. We replace x by x^3 and take the compositum with $x^2 + 3$ to obtain a degree 12 polynomial defining $K(\zeta_9)(\kappa_1^{1/3})/\mathbf{Q}$. This field has 7 subfields of degree 6. We test these fields pairwise for isomorphism, and compute that there is a unique field that is not isomorphic to another field. Hence, this is the unique field that is Galois over $\mathbf{Q}$ and must equal K_1. Applying lattice basis reduction to the default generator of $K_1/\mathbf{Q}$ gives the polynomial*

$$x^6 - 3x^5 + 13x^4 - 21x^3 + 43x^2 - 33x + 9.$$

To obtain K_2, we compute that κ_2 is a root of

$$\begin{aligned} x^6 &- 3298753006106830814034741x^5 + 859148927959860299001612714511680 6x^4 \\ &- 283203639684610111840656897778894161997 93x^3 \\ &+ 859148927959860299001612714511680 6x^2 \\ &- 3298753006106830814034741x + 1. \end{aligned}$$

The same technique as for K_1 gives that there are two subfields of $K_1(\zeta_9)(\kappa^{1/9})/\mathbf{Q}$ that are Galois over $\mathbf{Q}$. Since one of them is the known field K_1T_1, we select the field K_2 to be the other subfield that is Galois over $\mathbf{Q}$. A generating polynomial is given in Example 3.2.

Acknowledgements

We thank the referees for valuable suggestions on an earlier version of this paper.

References

1. Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter, *Computing Hilbert class polynomials*, Algorithmic number theory (Alfred J. van der Poorten and Andreas Stein, eds.), Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 282–295. MR 2467854
2. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
3. David Brink, *Prime decomposition in the anti-cyclotomic extension*, Math. Comp. **76** (2007), no. 260, 2127–2138. MR 2336287
4. Reinier Bröker, David Hubbard, and Lawrence C. Washington, *Magma code accompanying this paper*, Available at MSP site.
5. Reinier Bröker and Peter Stevenhagen, *Constructing elliptic curves of prime order*, Computational arithmetic geometry (Kristin E. Lauter and Kenneth A. Ribet, eds.), Contemp. Math., vol. 463, Amer. Math. Soc., 2008, pp. 17–28. MR 2459986
6. Gottfried Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr. **32** (1966), 317–326. MR 0217043
7. J. E. Carroll and H. Kisilevsky, *Initial layers of $\mathbf{Z}_l$-extensions of complex quadratic fields*, Compositio Math. **32** (1976), no. 2, 157–168. MR 0406970
8. Henri Cohen and Peter Stevenhagen, *Computational class field theory*, Algorithmic number theory: lattices, number fields, curves and cryptography (J. P. Buhler and P. Stevenhagen, eds.), Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 497–534. MR 2467555
9. David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. MR 3236783
10. Andreas Enge, `cm` — *complex multiplication of elliptic curves*, INRIA, 0.3 ed., March 2016, Distributed under GPL v3+; download from `http://cm.multiprecision.org/`.
11. Andreas Enge and Reinhard Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, J. Théor. Nombres Bordeaux **16** (2004), no. 3, 555–568. MR 2144957
12. Jae Moon Kim and Jangheon Oh, *Defining polynomial of the first layer of anti-cyclotomic $\mathbf{Z}_3$-extension of imaginary quadratic fields of class number 1*, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 3, 18–19. MR 2046261
13. Reinhard Schertz, *Weber's class invariants revisited*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 325–343. MR 1926005
14. Arnold Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203. MR 1581309
15. Peter Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory—its centenary and prospect (Tokyo, 1998) (Katsuya Miyake, ed.), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 161–176. MR 1846457
16. Yannick Van Huele, *On T-Semisimplicity of Iwasawa Modules and Some Computations with $\mathbf{Z}_3$-Extensions*, Ph.D. thesis, 2016, Thesis (Ph.D.)–University of Washington. MR 3597700
17. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575

Center for Communications Research, Princeton, NJ 08540, United States
E-mail address: `rmbroke@idaccr.org`

35 Holt Circle, Hamilton, NJ 08619, United States
E-mail address: `dhubbard@erols.com`

University of Maryland, College Park, MD 20742, United States
E-mail address: `lcw@math.umd.edu`

COUNTING ROOTS FOR POLYNOMIALS MODULO PRIME POWERS

QI CHENG, SHUHONG GAO, J. MAURICE ROJAS, AND DAQING WAN

ABSTRACT. Suppose p is a prime, t is a positive integer, and $f \in \mathbb{Z}[x]$ is a univariate polynomial of degree d with coefficients of absolute value $< p^t$. We show that for any *fixed* t, we can compute the number of roots in $\mathbb{Z}/(p^t)$ of f in deterministic time $(d \log p)^{O(1)}$. This fixed parameter tractability appears to be new for $t \geq 3$. A consequence for arithmetic geometry is that we can efficiently compute Igusa zeta functions Z, for univariate polynomials, assuming the degree of Z is fixed.

1. INTRODUCTION

Given a prime p, and a univariate polynomial $f \in \mathbb{Z}[x]$ of degree d with coefficients of absolute value $< p^t$, it is a basic problem to count the roots of f in $\mathbb{Z}/(p^t)$. Aside from its natural number theoretic relevance, counting roots in $\mathbb{Z}/(p^t)$ is closely related to error correcting codes [3] and factoring polynomials over the p-adic rationals $\mathbb{Q}_p$ [8, 4, 17], and the latter problem is fundamental in polynomial-time factoring over the rationals $\mathbb{Q}$ [23], the study of prime ideals in number fields [9, Ch. 4 & 6], elliptic curve cryptography [21], the computation of zeta functions [5, 22, 29, 6], and the detection of rational points on curves [27].

There is surprisingly little written about root counting in $\mathbb{Z}/(p^t)$ for $t \geq 2$: While an algorithm for counting roots of f in $\mathbb{Z}/(p^t)$ in time polynomial in $d \log p$ has been known in the case $t = 1$ for many decades (just compute the degree of $\gcd(x^p - x, f)$ in $\mathbb{F}_p[x]$), the case $t = 2$ was just solved in 2017 by some of our students [18]. The cases $t \geq 3$, which we solve here, appeared to be completely open (see also [28, 26, 14] for further background). One complication with $t \geq 2$ is that polynomials in $(\mathbb{Z}/(p^t))[x]$ do not have unique factorization, thus obstructing a simple use of polynomial gcd.

However, certain basic facts can be established quickly. For instance, the number of roots can be exponential in $\log p$. (It is natural to use $\log p$, among other parameters, to measure the size of a polynomial since it takes $O(dt \log p)$ bits to write down f.) The quadratic polynomial $x^2 = 0$, which has roots $0, p, 2p, \ldots, (p-1)p$ in $\mathbb{Z}/(p^2)$, is such an example. This is why we focus on computing the number of roots of f, instead of listing or searching for the roots in $\mathbb{Z}/(p^t)$.

Let $N_t(f)$ denote the number of roots of f in $\mathbb{Z}/(p^t)$ (setting $N_0(f) := 1$). The *Poincare series for* f is $P_f(x) := \sum_{t=0}^{\infty} N_t(f) x^t$. Assuming $P_f(x)$ is a rational function in x, one can reasonably recover $N_t(f)$ for any t via standard generating function techniques. That $P_f(x)$ is in fact a rational function of x (even for multivariate f) was first proved in 1974 by Igusa (in the course of deriving a new class of zeta functions [19]), applying resolution of singularities. Denef found a new proof (using p-adic cell decomposition [10]) leading to more algorithmic approaches later. While this in principle gives us a way to compute $N_t(f)$, there are few papers studying the computational complexity of Igusa zeta functions [30]. Our work here thus also contributes in the direction of arithmetic geometry by significantly improving [30], where P_f is computed in the special case where f is univariate and splits completely over $\mathbb{Q}$.

To better describe our results, let us start with a naive description of the first key idea: How do roots in $\mathbb{F}_p$ lift to roots in $\mathbb{Z}/(p^t)$? A simple root of f in $\mathbb{F}_p$ can be lifted uniquely to a root in $\mathbb{Z}/(p^t)$, according to the classical Hensel's lemma (see, e.g., [15]). But a root with multiplicity ≥ 2 in $\mathbb{F}_p$ can potentially be the image (under mod p reduction) of many roots in $\mathbb{Z}/(p^t)$, as illustrated by our earlier example $f(x) = x^2$. Or a root may not be liftable at all, e.g., $x^2 + p = 0$ has no roots mod p^2, even though it has a root mod p. More to the point, if one wants a fast deterministic algorithm, one can not assume that one has access to individual roots. This is because it is still an open problem to find the roots of univariate polynomials modulo p in deterministic polynomial time (see, e.g., [11, 16]).

Partially supported by NSF grant CCF-1409020, the American Institute of Mathematics, and MSRI (through REU grant DMS-1659138).

14 Jun 2018 19:35:42 PDT
Version 3 - Submitted to Open Book Series

Nevertheless, we have overcome this difficulty and found a way to keep track of how to correctly lift roots of any multiplicity.

Theorem 1.1. *There is a deterministic algorithm that computes the number of roots of f in $\mathbb{Z}/(p^t)$ in time $(d\log(p)+2^t)^{O(1)}$, where the implied constant in the big O notation is absolute.*

We prove Theorem 1.1 in Section 5. Note that Theorem 1.1 implies that if $t = O(\log\log p)$ then there is a deterministic $(d\log p)^{O(1)}$ algorithm to count the roots of f in $\mathbb{Z}/(p^t)$. We are unaware of any earlier algorithm achieving this complexity bound, even if randomness is allowed. It is worth noting that further speed-ups in terms of sparsity (e.g., polynomials with a fixed number of monomial terms) may be difficult to derive: Merely deciding the existence of roots in $\mathbb{F}_p$ or $\mathbb{Q}_p$ is already **NP**-hard (under **BPP**-reductions) with respect to the sparse encoding [1, 7]. An interesting open problem in this direction is then the following: If $c_1, c_2, c_3, a, b \in \{1, \ldots, p^2-1\}$ with $a < b < p^2 - p$, can one decide if $c_1 + c_2x^a + c_3x^b$ has a root in $\mathbb{Z}/(p^2)$ in time polynomial in $\log p$?

Our main technical innovations are the following:

- We use ideals in the ring $\mathbb{Z}_p[x_1, \ldots, x_k]$ of multivariate polynomials over the p-adic integers to keep track of the roots of f in $\mathbb{Z}/(p^t)$. More precisely, from the expansion
$$f(x_1 + px_2 + \cdots + p^k x_{k-1}) = g_1(x_1) + pg_2(x_1, x_2) + p^2 g_3(x_1, x_2, x_3) + \cdots$$
we build a collection of ideals in $\mathbb{Z}_p[x_1, \ldots, x_k]$, starting from $(g_1(x_1))$. We then decompose the ideals according to multiplicity type and rationality. This process produces a tree of ideals which ultimately encode the summands making up our final root count.
- The expansion above is not unique. (For example, adding p to g_1 and subtracting 1 from g_2 gives us another expansion.) However, we manage to keep most of our computations within $\mathbb{F}_p$, and maintain uniformity for the roots of our intermediate ideals, by using Teichmüller lifting (described in Section 4).

2. Overview of Our Approach

To count the number of roots in $\mathbb{Z}/(p^t)$ of $f \in \mathbb{Z}[x]$, our algorithm follows a divide-and-conquer strategy. First, partially factor f over $\mathbb{F}_p$ according to multiplicity and rationality as follows:

$$f = f_1 f_2^2 f_3^3 \cdots f_l^l F \pmod{p}, \tag{1}$$

where each $f_i \in \mathbb{F}_p[x]$ is monic and splits completely into a product of distinct linear factors over $\mathbb{F}_p$, the f_i are pairwise relatively prime, and F is free of linear factors in $\mathbb{F}_p[x]$. Such a factorization is classically known to be doable in deterministic polynomial-time (see, e.g., [2, pp. 170–171]). For an element $\alpha \in \mathbb{F}_p$, we call any element of its inverse image under the natural map $\mathbb{Z} \to \mathbb{F}_p$ a *lift* of α to $\mathbb{Z}$. Similarly, we can define a lift of α to $\mathbb{Z}_p$ or to $\mathbb{Z}/(p^t)$, and we can naturally extend this concept to polynomials in $\mathbb{F}_p[x]$ as well. The core of our algorithm counts how many roots of f in $\mathbb{Z}/(p^t)$ are lifts of roots of f_i in $\mathbb{F}_p$, for each i. For f_1, by Hensel's lifting lemma, the answer should be $\deg f_1$ for all t. For other f_i, however, Hensel's lemma will not apply, so we run our algorithm on the pair (f, m), where m is the lift of (a factor of) f_i to $\mathbb{Z}[x]$[1], for each $i \in \{2, \ldots, l\}$, to see how many lifts (to roots of f in $\mathbb{Z}/(p^t)$) are produced by the roots of the f_i in $\mathbb{F}_p$. The final count is then the summation of the results over all the f_i, since the roots of f in $\mathbb{Z}/(p^t)$ are partitioned by the roots of the f_i.

Remark 2.1. *If one instead uses a randomized factorization algorithm (e.g.,* [20]*) to find roots of f in $\mathbb{F}_p$ in polynomial time then one may assume* $\deg m = 1$*, and greatly simplify the analysis of our algorithm.*

[1]All factors of all f_i are ultimately exhausted.

Since $m|f$ (and in fact $m^2|f$) in $\mathbb{F}_p[x]$, we have $f(x) = 0 \pmod{(m(x), p)}$ and, in $\mathbb{Z}[x_1, x_2]$, we have the containment

$$f(x_1 + px_2) \in (m(x_1), p).$$

If we have the refined containment $f(x_1 + px_2) \in (m(x_1), p^t)$ then for any root r_1 of m in $\mathbb{Z}/(p^t)$, and any integer $0 \le r_2 < p^{t-1}$, $f(r_1 + pr_2) = 0 \pmod{p^t}$. Thus each root of m in $\mathbb{F}_p$ lifts to exactly p^{t-1} roots of f in $\mathbb{Z}/(p^t)$, and the counting problem for (f, m) is solved. Otherwise we can efficiently find an integer $s \in \{1, \ldots, t-1\}$ and a $g \in \mathbb{Z}[x_1, x_2]$ such that

$$f(x_1 + px_2) = p^s g(x_1, x_2) \pmod{(m(x_1), p^t)}, \tag{2}$$

where $\deg_{x_2} g \le t - 1$, $\deg_{x_1} g < \deg m$ and $g(x_1, x_2) \neq 0 \pmod{p, m(x_1)}$. Let

$$g(x_1, x_2) = \sum_{0 \le j < t} g_j(x_1) x_2^j.$$

Then either $g_j = 0 \pmod{p}$ or $\gcd(m(x_1), g_j(x_1)) = 1$ over $\mathbb{F}_p$. (Otherwise, we apply the algorithm to the pairs $(f, \gcd(m, g_j))$ and $(f, m/\gcd(m, g_j))$.)

If $s = 1$ then, since $m^2|f$ over $\mathbb{F}_p$, we must have

$$f(x_1 + px_2) = pg_0(x_1) \pmod{m(x_1), p^2}.$$

Since $\gcd(m, g_0) = 1$ over $\mathbb{F}_p$, none of the roots of m in $\mathbb{F}_p$ can be lifted to $\mathbb{Z}/p^2$. So from now on we assume that $1 < s < t$.

2.1. **The algorithm for $t = 3$.** The only interesting case is when $s = 2$.

Theorem 2.2. *The number of roots in $\mathbb{Z}/(p^3)$ of f that are lifts of roots of $m \pmod{p}$ is equal to p times the number of roots in $\mathbb{F}_p^2$ of the 2×2 polynomial system below:*

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \tag{3}$$

and thus the number of roots can be calculated in deterministic polynomial time.

Proof. To calculate the number of the roots, we run the Euclidean algorithm to compute the gcd of two polynomials:

$$g(x_1, x_2) \text{ and } x_2^p - x_2,$$

viewed as polynomials in x_2 over $\mathbb{F}_p[x_1]/(m(x_1))$. If we encounter a zero divisor of $\mathbb{F}_p[x_1]/(m(x_1))$ during the computation, then we have a nontrivial factorization of $m(x_1) = m_1 m_2$. We recursively count the $\mathbb{F}_p$ solutions of the equation system $m_1(x_1) = 0$ and $g(x_1, x_2) = 0$, and the system $m_2(x_1) = 0$ and $g(x_1, x_2) = 0$, output the sum of these two numbers.

Otherwise assume that the degree of the gcd (a monic polynomial in x_2) is n_2. The number of $\mathbb{F}_p$-roots of (3) equals to $n_2 \deg(m(x))$.

Since $m(x_1)$ has at most $\deg(m(x))$ many factors, and the Euclidean algorithm can be done in deterministic polynomial time, the theorem follows. ■

More details and generalization (to the Gröbner base computation) of the algorithm can be found in Section 6. Note that since $\deg_{x_2} g \le 2$ any root of m in $\mathbb{F}_p$ can be lifted to at most $2p$ roots in $\mathbb{Z}/(p^3)$.

Assume that $f \in \mathbb{Z}[x]$ is not divisible by p. The preceding ideas are formalized in the following algorithm:

Algorithm 1 The case $t = 3$

function COUNT($f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0 \pmod p$)
  Factor f as in (1).
  $count = \deg f_1$ ▷ Every root of f_1 can be lifted uniquely.
  Push $f_2, f_3, \ldots, f_l$ onto a stack S
  while $S \neq \emptyset$ **do**
    Pop a polynomial from the stack, find its lift to $\mathbb{Z}$ and denote it by m
    if $f(x_1 + px_2) = 0 \pmod{(m(x_1), p^3)}$ **then**
      $count \leftarrow count + p^2 \deg m$
    else
      Find s and g satisfying the conditions in Equation (2)
      if $\deg \gcd(m, g_j) > 0$ for some j **then**
        Push $\gcd(m, g_j)$ and $m/\gcd(m, g_j)$ onto the stack
      else
        if $s = 2$ **then**
          $count \leftarrow$ count $+p\cdot$(the number of the solutions of (3) in $\mathbb{F}_p^2$)
        end if
      end if
    end if
  end while
  return count
end function

2.2. **A Proposition for General t.** Let $r \in \mathbb{F}_p$ be any root of m, r' be the corresponding lifted root of m in $\mathbb{Z}_p$, and $a \in \mathbb{Z}_p$. We then have

$$f(r' + ap) = p^s g(r', a) \pmod{p^t}.$$

So $r' + ap$ is a root in $\mathbb{Z}/(p^t)$ for f if and only if

$$g(r', a) = 0 \pmod{p^{t-s}}.$$

The preceding argument leads us to the following result.

Proposition 2.3. *The number of roots in $\mathbb{Z}/(p^t)$ of f that are lifts of the roots of $m \pmod p$ is equal to p^{s-1} times the number of solutions in $(\mathbb{Z}/(p^{t-s}))^2$ of the 2×2 polynomial system (in the variables (x_1, x_2)) below:*

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \tag{4}$$

Since the root of m is liftable only when $s > 1$ (see the discussion at the beginning of the section), this yields the following dichotomy corollary:

Corollary 2.4. *If $m^2 | f$ in $\mathbb{F}_p[x]$, and $t \geq 2$, then any root of m in $\mathbb{F}_p$ is either not liftable to a root in $\mathbb{Z}/(p^t)$ of f, or can be lifted to at least p roots of f in $\mathbb{Z}/(p^t)$.*

3. From Taylor Series to Ideals

For any univariate polynomial m of degree n let us define

$$T_{m,j}(x, y) = \sum_{1 \leq i \leq j} \frac{y^{i-1}}{i!} \frac{d^i m}{(dx)^i}(x).$$

Note that if $m \in \mathbb{Z}[x]$ then $\frac{1}{i!}\frac{d^i m}{(dx)^i}(x)$, being a Taylor expansion coefficient, also lies in $\mathbb{Z}[x]$. So $T_{m,j}$ is an integral multivariate polynomial for any j. Since $T_{m,1}$ does not depend on y, we abbreviate $T_{m,1}(x,y)$ by $T_m(x)$. The following lemma follows from a simple application of Taylor expansion:

Lemma 3.1. *Let $m \in \mathbb{Z}[x]$ be a polynomial that is irreducible in $\mathbb{Z}[x]$ but splits completely, without repeated factors, into linear factors in $\mathbb{F}_p[x]$. Let $r \in \mathbb{F}_p$ be any root of m and let $r' \in \mathbb{Z}_p$ be the corresponding p-adic integer root of m. Then*

$$m(r' + ap) = apT_m(r) \pmod{p^2}.$$

To put it in another way, we have the following congruence:

$$m(x_1 + px_2) \equiv px_2T_m(x_1) \pmod{m(x_1), p^2}$$

in the ring $\mathbb{Z}[x_1, x_2]$.

That one can always associate an $r \in \mathbb{F}_p$ to a root $r' \in \mathbb{Z}_p$ as above is an immediate consequence of the classical Hensel's Lemma [15]. More generally, we have the following stronger result:

Lemma 3.2. *Let $m \in \mathbb{Z}[x]$ be a polynomial that is irreducible in $\mathbb{Z}[x]$ but splits completely, without repeated factors, into linear factors in $\mathbb{F}_p[x]$. Let $r \in \mathbb{F}_p$ be any root of m, and let $r' \in \mathbb{Z}_p$ be the corresponding p-adic integer root of m. Then for any positive integer u,*

$$m(r' + ap) = apT_{m,u-1}(r', ap) \pmod{p^u}.$$

Also, in the ring $\mathbb{Z}[x_1, x_2]$, we have

$$m(x_1 + px_2) = x_2pT_{m,\deg(m)}(x_1, px_2) \pmod{m(x_1)}.$$

Proof. By Taylor expansion:

$$\begin{aligned} m(r' + ap) &= m(r') + \sum_{1 \le i < u} \frac{(ap)^i}{i!}\frac{d^i m}{(dx)^i}(r') \pmod{p^u} \\ &= \sum_{1 \le i < u} \frac{(ap)^i}{i!}\frac{d^i m}{(dx)^i}(r') \pmod{p^u} \\ &= ap \sum_{1 \le i < u} \frac{(ap)^{i-1}}{i!}\frac{d^i m}{(dx)^i}(r') \pmod{p^u} \end{aligned}$$

As observed earlier, $\frac{1}{i!}\frac{d^i m}{(dx)^i}(x)$ is an integral polynomial (even when $i > p-1$), so we are done. ■

Note that in the setting of Lemma 3.2, $T_{m,u-1}(r', ap) \equiv T_m(r') \neq 0 \pmod{p}$.

The following theorem is a generalization of the preceding lemmas to ideals.

Theorem 3.3. *Let I be a ideal in $\mathbb{Z}_p[x_1, \ldots, x_{k-1}]$. Assume that $I \pmod{p}$ is a zero-dimensional radical ideal in $\mathbb{F}_p[x_1, \ldots, x_{k-1}]$ whose zero set in $\bar{F}_p^{k-1}$ lies in $\mathbb{F}_p^{k-1}$ and lifts to $\mathbb{Z}_p$. Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ satisfy $\deg_{x_k} f < p$. If $f(r_1, \ldots, r_k) \equiv 0 \pmod{p^s}$ for every $\mathbb{Z}_p$-root $(r_1, \ldots, r_{k-1})$ of I, and every integer r_k, then there must exist a polynomial $g(x_1, \ldots, x_k)$ such that*

$$f(x_1, \ldots, x_k) \equiv p^s g(x_1, \ldots, x_k) \pmod{I}.$$

Theorem 3.3 can be proved by induction on k. Lemma 3.2 is basically the special case of Theorem 3.3 when $s = 1, k = 2$, $I = (m(x_1))$ and $f(x_1, x_2) = m(x_1 + px_2)$. It is important in Theorem 3.3 that the ideal $I \pmod{p}$ be radical, just like in Lemma 3.2, where m is free of repeated factors over $\mathbb{F}_p$.

4. The Case $t = 4$ and the Need for Teichmüller Lifting.

Here we work on the case $t = 4$. Earlier, we saw that in the course of our algorithm, m is a lift of a factor of f_i to $\mathbb{Z}[x]$. In this section we will show the need for Teichmüller lifting. We start with

$$f(x_1 + px_2) = p^s g(x_1, x_2) \pmod{m(x_1), p^4},$$

where $1 < s < 4$. If $s = 3$ then we have the following root count, thanks to Proposition 2.3:

Theorem 4.1. *The number of roots in $\mathbb{Z}/(p^4)$ of f that are lifts of roots of $m \pmod p$ is equal to p^2 times the number of roots in $\mathbb{F}_p^2$ of the 2×2 polynomial system (in the variables (x_1, x_2)) below:*

$$\begin{aligned} m(x_1) &= 0 \\ g(x_1, x_2) &= 0 \end{aligned} \tag{5}$$

which can be calculated in deterministic polynomial time.

The most interesting subcase is thus $s = 2$. From Equation (3), we first build an ideal

$$(m(x_1), g(x_1, x_2)) \pmod p \subset \mathbb{F}_p[x_1, x_2].$$

The leading coefficient of $g(x_1, x_2)$, viewed as a polynomial in x_2, is assumed to be invertible in $\mathbb{F}_p[x_1]/(m(x_1))$. So g can be made monic (as a polynomial in x_2). So we may assume that the ideal is given as

$$(m(x_1), x_2^{n_2} + f_2(x_1, x_2)),$$

where $n_2 \leq 2$ and $\deg_{x_2} f_2 < n_2$. If (r, r_2) is a root in $\mathbb{F}_p$ of the ideal, and r_1 is the lift of r to the $\mathbb{Z}_p$-root of m, then $r_1 + pr_2$ is a solution of $f \pmod{p^3}$. We compute the rational component of the ideal, and find its radical over $\mathbb{F}_p$. In the process, we may factor m in $\mathbb{F}_p[x]$. If we lift naively a factor m_1 of m over $\mathbb{F}_p$, the p-adic roots of m_1 may not be p-adic roots of m. So how do we keep the information about p-adic roots of m, a polynomial with integer coefficients?

Our solution to this problem is to use Teichmüller lifting: Recall that for an element α in the prime field $\mathbb{F}/p$, the Teichmüller lifting of α is the unique p-adic integer $w(\alpha) \in \mathbb{Z}_p$ such that $w(\alpha) \equiv \alpha \mod p$ and $w(\alpha)^p = w(\alpha)$. If a is any integer representative of α, then the Teichmüller lifting of α can be computed via

$$w(\alpha) = \lim_{k \to \infty} a^{p^k}, \ w(\alpha) \equiv a^{p^t} \mod p^t.$$

Although the full Teichmüller lifting cannot be computed in finite time, we will see momentarliy how its mod p^t reduction can be computed in deterministic polynomial time.

Let us now review how the mod p^t reduction of the Teichmüller lift can be computed in deterministic polynomial time: If $m \in \mathbb{Z}[x]$ is a monic polynomial of degree $d > 0$ such that $m \mod p$ splits as a product of distinct linear factors

$$m(x) \equiv \prod_{i=1}^{d} (x - \alpha_i) \mod p, \ \alpha_i \in \mathbb{F}_p,$$

then the Teichmüller lifting of $m \mod p$ is defined to be the unique monic p-adic polynomial $\hat{m} \in \mathbb{Z}_p[x]$ of degree d such that the p-adic roots of $\hat{m}$ are exactly the Teichmüller lifting of the roots of $m \mod p$. That is,

$$\hat{m}(x) = \prod_{i=1}^{d} (x - w(\alpha_i)) \in \mathbb{Z}_p[x].$$

The Teichmüller lifting $\hat{m}$ can be computed without factoring $m \mod p$: Using the coefficients of m, one forms a $d \times d$ companion matrix M with integer entries such that $m(x) = \det(xI_d - M)$. Then, one can show that

$$\hat{m}(x) = \lim_{k \to \infty} \det(xI_d - M^{p^k}), \ \hat{m}(x) \equiv \det(xI_d - M^{p^t}) \mod p^t.$$

This construction and computation of Teichmüller lifting of a single polynomial $m(x) \pmod p$ can be extended to any triangular zero-dimensional radical ideal with only rational roots as follows.

Let I be a radical ideal of the form

$$I = (g_1(x_1), g_2(x_1, x_2), \ldots, g_k(x_1, \ldots, x_k)) \subset \mathbb{F}_p[x_1, \ldots, x_k],$$

having only rational roots, where $g_i \in \mathbb{Z}[x_1, \ldots, x_i]$ is a monic polynomial in x_i of the form

$$g_i(x_1, \ldots, x_i) = x_i^{n_i} + f_i(x_1, \ldots, x_i),\ n_i \geq 1$$

satisfying $\deg_{x_i} f_i < n_i$. Such a presentation of the ideal I is called *triangular form*. It is clear that such an I is a zero-dimensional complete intersection. Using the companion matrix of a polynomial, we can easily find $n_i \times n_i$ matrices $M_{i-1}(x_1, \ldots, x_{i-1})$ whose entries are polynomials with coefficients in $\mathbb{Z}$ such that

$$g_i(x_1, \ldots, x_i) \equiv \det(x_i I_{n_i} - M_i(x_1, \ldots, x_{i-1})) \pmod p,\ 1 \leq i \leq k.$$

Recursively define the polynomial $f_i \in (\mathbb{Z}/(p^t))[x_1, \ldots, x_i]$ for $1 \leq i \leq k$ such that

$$f_1(x_1) \equiv \det(x_1 I_{n_1} - M_0^{p^t}) \pmod{p^t},$$

$$f_2(x_1, x_2) \equiv \det(x_2 I_{n_2} - M_1(x_1)^{p^t}) \pmod{(p^t, f_1(x_1))},$$

$$\vdots$$

$$f_k(x_1, \ldots, x_k) \equiv \det(x_k I_{n_k} - M_{k-1}(x_1, \ldots, x_{k-1})^{p^t}) \pmod{(p^t, f_1, \ldots, f_{k-1})}.$$

The ideal $\hat{I} = (f_1, \ldots, f_k) \in (\mathbb{Z}/(p^t))[x_1, \ldots, x_i]$ is called the *Teichmüller lifting mod p^t of I*. It is independent of the choice of the auxiliary integral matrices M_i. The roots of $\hat{I}$ over $\mathbb{Z}/p^t\mathbb{Z}$ are precisely the Teichmüller liftings mod p^t of the roots of I over $\mathbb{F}_p$. In particular, each root $(r_1, \ldots, r_k)$ over $\mathbb{Z}/(p^t)$ of $\hat{I}$ satisfies the condition $r_i^p \equiv r_i \pmod{p^t}$.

We require that m be the Teichmüller lift of (a factor of) f_i at beginning of the algorithm. Then we compute the Teichmüller lift of the ideal $(m(x_1), x_2^{n_2} + f_2(x_1, x_2))$, which is an ideal in $\mathbb{Z}_p[x_1, x_2]$. We only need it modulo p^4. Denote the ideal by I_2. For every root (r_1, r_2) of I_2, $r_1 + pr_2$ is a solution of $f(x) = 0 \pmod{p^3}$. Namely, for any integer r_3, we have $f(r_1 + pr_2 + p^2 r_3) = 0 \pmod{p^3}$, since $f(x_1 + px_2) = 0 \pmod{I_2, p^3}$.

According to Theorem 3.3, there exists a polynomial $G \in \mathbb{Z}[x_1, x_2, x_3]$ such that

$$f(x_1 + px_2 + p^2 x_3) \equiv p^3 G(x_1, x_2, x_3) \pmod{I_2},$$

since $I_2 \pmod p$ is radical. We have

$$f(x_1 + px_2 + p^2 x_3) = g_1(x_1, x_2)p^3 x_3 + g_0(x_1, x_2)p^3 \pmod{(I_2, p^4)}.$$

Hence if (r_1, r_2) is a root of I_2, then $r_1 + pr_2 + p^2 r_3$ is a root of $f \pmod{p^4}$ iff (r_1, r_2, r_3) satisfies

$$g_1(r_1, r_2)r_3 + g_0(r_1, r_2) = 0.$$

Assume that $g_1 \not\equiv 0 \pmod{I_2, p}$. We count the number of rational roots of

$$(I_2, g_1(x_1, x_2)x_3 + g_0(x_1, x_2)) \pmod p \subset \mathbb{F}_p[x_1, x_2, x_3].$$

Multiplying the resulting count by p yields the number of roots of f in $\mathbb{Z}/(p^4)$.

5. Generalization to Arbitrary $t \geq 5$

We now generalize the idea for the case of $t = 4$ to counting roots in $\mathbb{Z}/(p^t)$ of $f(x)$ when $t \geq 5$ and f is not identically 0 mod p. (We can of course divide f by p and reduce t by 1 to apply our methods here, should $p|f$.) In the algorithm, we build a tree of ideals. At level k, the ideals belong to the ring $(\mathbb{Z}/(p^t))[x_1, \ldots, x_k]$. The root of the tree (level 0) is $\{0\} \subset \mathbb{Z}/(p^t)$, the zero ideal. At the next level the ideals are of the form $(m(x_1))$, where m is taken to be the Teichmüller lift of f_i in Equation (1). We study how the roots in $\mathbb{Z}_p$ of m can be lifted to roots of f in $\mathbb{Z}/(p^t)$.

Let $I_0, I_1, \ldots, I_k$ be the ideals in a path from the root to a leaf. We require:

- $I_0 = \{0\} \subset \mathbb{Z}/(p^t)$ and $I_i \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_i]$;
- $I_i = I_{i+1} \cap \mathbb{Z}/(p^t)[x_1, \ldots, x_i]$ for all $0 \leq i \leq k-1$;
- The ideal $I_i \pmod p$ in $\mathbb{F}_p[x_1, \ldots, x_i]$ is zero-dimensional, radical, and has only rational roots for all $i \in \{0, \ldots, k\}$; furthermore, I_i can be written in the form

$$\begin{aligned} &(I_{i-1}, x_i^{n_i} + f_i(x_1, \ldots, x_i)) \\ \subset &(\mathbb{Z}/(p^t))[x_1, \ldots, x_i] \end{aligned} \tag{6}$$

  where $\deg_{x_i} f_i < n_i$.
- The ideal I_i is the mod p^t reduction of the Teichmüller lift of the mod p reduction of I_i.

The basic strategy of the algorithm is to grow every branch of the tree until we reach a leaf whose ideal allows a trivial count of solutions. (In which case we output the count and terminate the branch.) Once all the branches terminate, we then compute the summation of the numbers on all the leaves as the output of the algorithm. The tree of ideals contains all necessary information about the solutions of $f \pmod{p^t}$ in the following sense:

- For any ideal I_i in the tree, there exists an integer $s \in \{i, \ldots, t\}$, such that if $(r_1, \ldots, r_i)$ is a solution of I_i in $(\mathbb{Z}/(p^t))^i$, then $r_1 + pr_2 + \cdots + p^{i-1}r_i + p^i r$ is a solution of $f(x) \pmod{p^s}$ for any integer r. Denote the maximum such s by $s(I_i)$.
- If $r \in \mathbb{Z}/(p^t)$ is a root of $f \pmod{p^t}$, then there exists a terminal leaf I_k in the tree such that
$$r \equiv r_1 + pr_2 + \cdots + p^{k-1}r_k \pmod{p^k}$$
for some root $(r_1, \ldots, r_k)(\mathbb{Z}/(p^t))^k$ of I_k.
- The root sets of ideals from distinct leaves are disjoint.

Suppose that at the end of a branch we have an ideal $I_k \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_k]$. The ideal $I_k \pmod p$ is zero-dimensional and radical in $\mathbb{F}_p[x_1, \ldots, x_k]$, with only rational roots. There are two termination conditions:

- If $s(I_k) = t$ then each root of I_k in $\mathbb{Z}_p^k$ produces exactly p^{t-k} roots of f in $\mathbb{Z}/(p^t)$. We can count the number of roots in $\mathbb{F}_p^k$ of I_k, multiply it by p^{t-k}, output the number, and terminate the branch.
- Let g be the polynomial satisfying
$$f(x_1 + px_2 + p^2x_3 + \cdots + p^{k-1}x_k + p^k x_{k+1}) \equiv p^{s(I_k)} g(x_1, \ldots, x_{k+1}) \pmod{I_k}.$$
Such a polynomial exists according to Theorem 3.3. If $g \pmod p$ is a constant polynomial in x_{k+1}, and its constant is an invertible element $\pmod{I_k, p}$, then the count on this leaf is zero.

Example 5.1. *Suppose $t = 2$. For the polynomials $x^2 = 0$ and $x^2 + p = 0$, the ideal (x_1) is a terminal leaf with count p for the former polynomial, and with count 0 for the latter.*

If none of the conditions hold then let

$$g = \sum_{j \leq t/k} g_j(x_1, \ldots, x_k) x_{k+1}^j \pmod p.$$

The degree bound t/k is due to the fact that p^{kj} divides any term in the monomial expansion of $f(x_1+px_2+\cdots+p^{k-1}x_k+p^kx_{k+1})$ that has a factor x_{k+1}^j. If any of g_j vanish at some rational root of I_k in $\mathbb{F}_p^k$ then this allows $I_k \pmod p$ to expressed as an intersection of simpler ideals. Otherwise, for the ideal $(I_k, g) \subset (\mathbb{Z}/(p^t))[x_1, \ldots, x_{k+1}]$, we compute its decomposition in $\mathbb{F}_p[x_1, \ldots, x_{k+1}]$ according to multiplicity type, find the radicals of the underlying ideals, and then lift them back to $(\mathbb{Z}/(p^t))[x_1, \ldots, x_{k+1}]$. They become the children of I_k. Note that if (I_k, g) does not have rational roots, it means that none of the roots of I_k can be lifted to solution of $f \pmod{p^{s+1}}$, and thus the branch terminates with count 0.

Proof of Theorem 1.1: If $p \leq d$ then factoring polynomials over $\mathbb{F}_p$ can be done in time polynomial in d by brute force, and all the ideals in the tree are maximal. The number of children that an ideal with distance k from the root can have is bounded from above by t/k or the degree of g. (More precisely, number of non-terminal child nodes is bounded from above by $t/(2k)$.) The complexity is determined by the size of the tree, which is bounded from above by $d\prod_{k=1}^{t}(t/k) = d\frac{t^t}{t!} < de^t$.

If $p > d$ then our upper bound above on the tree size still holds. Since we use Teichmüller lifting during the algorithm, the tree size will never decrease. The algorithm must stop once the tree size approaches the upper bound $\lfloor de^t \rfloor$. For each tree size change, we either create new children, or split a node. We need to compute in the ring $\mathbb{F}_p[x_1, \ldots, x_k]/I_k$. Observe that in (6), we must have $n_i < t/(i-1)$ for $i \geq 2$. So the ring is a vector space over $\mathbb{F}_p$ of dimension at most $d\prod_{i=2}^{t} n_i = d\frac{t^{t-1}}{(t-1)!} < de^t$. Theorem follows from the fact that each tree size change involves a number of bit operations at most polynomial in $de^t \log p$. ■

6. Computer Algebra Discussion

In this section, we explain how to split ideals over $\mathbb{F}_p$ into triangular form so that the Teichmüller lift to $\mathbb{Z}_p$ can be computed. We start with the one variable case: For any given ideal $I = (f(x)) \subset \mathbb{F}_p[x]$, we can split f into the following form

$$f = g_1^{d_1} \cdots g_t^{d_t} g_0$$

where $d_1 > \cdots > d_t > 0$, the polynomials $g_1, \ldots, g_t \in \mathbb{F}_p[x]$ are separable, pairwise co-prime and each splits completely over $\mathbb{F}_p$, and g_0 has no linear factors in $\mathbb{F}_p[x]$. Such a factorization can be computed deterministically in time polynomial in $\log(p)\deg(f)$. Note that, for $1 \leq i \leq t$, each root of g_i has multiplicity d_i in I. This means that we can count the number of $\mathbb{F}_p$-rational roots of I, and their multiplicities, in polynomial time. Also, the rational part of I (i.e., excluding the factor g_0) is decomposed into t factors $g_1, \ldots, g_t$.

Now we show how to go from k variables to $k+1$ variables for any $k \geq 1$. Suppose $J = (g_1, \ldots, g_k) \subset \mathbb{F}_p[x_1, \ldots x_k]$ has triangular form:

$$\begin{aligned} g_1 &= x_1^{n_1} + r_1(x_1), \\ g_2 &= x_2^{n_2} + r_2(x_1, x_2), \\ &\vdots \\ g_k &= x_k^{n_k} + r_k(x_1, x_2, \ldots, x_k), \end{aligned}$$

where g_i is monic in x_i (i.e., $\deg_{x_i} r_i < n_i$) for $1 \leq i \leq k$. We further assume that J is radical and splitting completely over $\mathbb{F}_p$ — that is, J has $n_1 n_2 \cdots n_k$ distinct solutions in $\mathbb{F}_p^k$. In particular, $g_1(x_1)$ has n_1 distinct roots in $\mathbb{F}_p$ and, for each root $a_1 \in \mathbb{F}_p$ of g_1, there are n_2 distinct $a_2 \in \mathbb{F}_2$ such that (a_1, a_2) is a root of $g_2(x_1, x_2)$. In general, for $1 \leq i < k$, each root $(a_1, \ldots, a_i) \in \mathbb{F}_p^i$ of $(g_1, \ldots, g_i)$ can be extended to n_{i+1} distinct solutions $(a_1, \ldots, a_i, a_{i+1}) \in \mathbb{F}_p^{i+1}$ of g_{i+1}. For convenience, any ideal with these properties is called a *splitting triangular ideal*.

Let $f \in \mathbb{F}_p[x_1, \ldots, x_k, x_{k+1}]$ be any nonzero polynomial which is monic in x_{k+1}, and let $I = (J, f)$ be the ideal generated by J and f in $\mathbb{F}_p[x_1, \ldots, x_k, x_{k+1}]$. We want to decompose I into splitting triangular ideals, together with their multiplicities. More precisely, we want to decompose I into the following form:

$$I = (J_1, h_1^{d_1}) \cap (J_2, h_2^{d_2}) \cap \cdots \cap (J_m, h_m^{d_m}) \cap (J_0, h_0), \tag{7}$$

where $J = J_1 \cap J_2 \cap \cdots \cap J_m \cap J_0$, $I_0 = (J_0, h_0)$ has no solutions in $\mathbb{F}_p^{k+1}$, and the ideals $I_i = (J_i, h_i) \subset \mathbb{F}_p[x_1, \ldots, x_k, x_{k+1}]$, $1 \le i \le m$, are splitting triangular ideals and are pairwise co-prime (i.e., any pair of distinct I_i have no roots in common).

To get the decomposition (7), we first compute

$$w := x_{k+1}^p - x_{k+1} \bmod G.$$

where $G = \{g_1, g_2, \ldots, g_k, f\}$ is a Gröbner basis under the lexicographical order with $x_{k+1} > x_k > \cdots > x_1$. Via the square-and-multiply method, w can be computed using $\mathrm{O}(\log(p)^3 n^2)$ bit operations where $n = \deg(f) \cdot n_1 \cdots n_k$ is the degree of the ideal I. Next we compute the Gröbner basis B of $\{g_1, g_2, \ldots, g_k, f, w\}$ (under lex order with $x_{k+1} > x_k > \cdots > x_1$), which is radical and completely splitting (hence all of its solutions are in $\mathbb{F}_p^{k+1}$ and are distinct). This mean that we get rid of the nonlinear part (J_0, h_0) in (7). The ideal (B) is now equal to the radical of the rational part of I. To decompose (B) into splitting triangular ideals, we view each polynomial in B as a polynomial in x_{k+1} with coefficient in $\mathbb{F}_p[x_1, \ldots, x_k]$. Let $t_0 = 0 < t_1 < \cdots < t_v$ be the distinct degrees of x_{k+1} among the polynomials in B. For $0 \le i \le v$, let B_i denote the set of the leading coefficient of all $g \in B$ with $\deg(g) \le t_i$. We then have a chain of ideals

$$J \subseteq (B_0) \subset (B_1) \subset \cdots \subset (B_{v-1}) \subset (B_v) = \mathbb{F}_p[x_1, \ldots, x_k]$$

with the following properties:

(i) $1 \in B_v$,
(ii) each B_i $(1 \le i \le v)$ is automatically a Gröbner basis under the lex order with $x_k > \cdots > x_1$ (one can remove some redundant polynomials from B_i),
(iii) for $0 \le i < v$, each solution of B_i that is not a solution of B_{i+1} can be extended to exactly t_{i+1} distinct solutions of I.

We can compute a Gröbner basis C_i for the colon ideal $(B_{i+1}) : (B_i)$ for $0 \le i < v$. These C_i give us the different components of J that have different numbers of solution extensions. Together with B, we get different components of (I, w). These components are completely splitting, but may not be in triangular form (as stated above). We again use the Gröbner basis structure to further decompose them until all are splitting triangular ideals (J_i, h_i). Note that computing Gröbner bases, for arbitrary ideals in $\mathbb{Q}[x_1, \ldots, x_n]$, has exponential worst-case complexity [25]. However, all of our ideals are of a special form, so their Gröbner bases can be computed deterministically in polynomial-time via the incremental method in [12] (see also [13]).

Finally, to get the multiplicity of each component (J_i, h_i), we compute the Gröbner basis for the ideal $(J_i, f, f^{(j)})$ where $f^{(j)}$ denotes the j-th derivative of f for $j = 1, 2, \ldots, \deg(f)$, until the Gröbner basis is 1. These ideals may not be in triangular form, so they may split further, but the total number of components is at most $\deg f$. Hence the total number of bit operations used is still polynomial in $\log(p) \deg(I)$.

Acknowledgements

We thank the anonymous referees for suggestions that helped improve our paper. We also gratefully acknowledge the support of the American Institute of Mathematics.

References

[1] Martíin Avendaño; Ashraf Ibrahim; J. Maurice Rojas; and Korben Rusek, *"Faster p-adic Feasibility for Certain Multivariate Sparse Polynomials,"* Journal of Symbolic Computation, special issue in honor of 60th birthday of Joachim von zur Gathen, vol. 47, no. 4, pp. 454–479 (April 2012).

[2] Eric Bach and Jeff Shallit, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[3] Jérémy Berthomieu; Grégoire Lecerf; and Guillaume Quintin, *"Polynomial root finding over local rings and application to error correcting codes,"* Applicable Algebra in Engineering, Communication, and Computing, December 2013, Volume 24, Issue 6, pp. 413–443.

[4] David G. Cantor and Daniel M. Gordon, *"Factoring polynomials over p-adic fields,"* Algorithmic number theory (Leiden, 2000), pp. 185–208, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[5] Wouter Castryck; Jan Denef; and Frederik Vercauteren, *"Computing Zeta Functions of Nondegenerate Curves,"* International Mathematics Research Papers, vol. 2006, article ID 72017, 2006.

[6] Antoine Chambert-Loir, *"Compter (rapidement) le nombre de solutions d'équations dans les corps finis,"* Séminaire Bourbaki, Vol. 2006/2007, Astérisque No. 317 (2008), Exp. No. 968, vii, pp. 39-90.

[7] Qi Cheng; Shuhong Gao; J. Maurice Rojas; and Daqing Wan, *"Sparse Univariate Polynomials with Many Roots Over a Finite Field,"* Finite Fields and their Applications, Vol. 46, July 2017, pp. 235–246.

[8] Alexander L. Chistov, *"Efficient Factoring [of] Polynomials over Local Fields and its Applications,"* in I. Satake, editor, Proc. 1990 International Congress of Mathematicians, pp. 1509–1519, Springer-Verlag, 1991.

[9] Henri Cohen, *A course in computational algebraic number theory,* Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[10] Jan Denef, *"Report on Igusa's local zeta function,"* Séminaire Bourbaki 1990/1991 (730-744) in Astérisque 201–203 (1991), pp. 359–386.

[11] Shuhong Gao, *"On the deterministic complexity of polynomial factoring"*, *Journal of Symbolic Computation*, 31 (2001), 19–36.

[12] Shuhong Gao, Yinhua Guan, and Frank Volny IV, *"A new incremental algorithm for computing Gröbner bases"*, the 35th International Symposium on Symbolic and Algebraic Computation (ISSAC), pp. 13–19, Munich, July 25–28, 2010.

[13] Shuhong Gao, Frank Volny IV, and Mingsheng Wang, *"A new framework for computing Gröbner bases"*, *Mathematics of Computation*, 85 (2016), no. 297, 449–465.

[14] Joachim von zur Gathen and Silke Hartlieb, *"Factoring Modular Polynomials,"* J. Symbolic Computation (1998) **26**, pp. 583–606.

[15] Fernando Q. Gouveêa, *p-adic Numbers,* Universitext, 2nd ed., Springer-Verlag, 2003.

[16] Bruno Grenet, Joris van der Hoeven and Grégoire Lecerf, *"Deterministic root finding over finite fields using Graeffe transforms,"* Applicable Algebra in Engineering, Communication and Computing, (2016) **27** , pp. 237–257.

[17] Jordi Guàrdia; Enric Nart; Sebastian Pauli, *"Single-factor lifting and factorization of polynomials over local fields,"* Journal of Symbolic Computation 47 (2012), pp. 1318–1346.

[18] Trajan Hammonds; Jeremy Johnson; Angela Patini; and Robert M. Walker, *"Counting Roots of Polynomials Over $\mathbb{Z}/p^2\mathbb{Z}$,"* Houston Journal of Mathematics, to appear. (Also available as Math ArXiv preprint `1708.04713` .)

[19] Jun-Ichi Igusa, *Complex powers and asymptotic expansions I: Functions of certain types*, Journal für die reine und angewandte Mathematik, 1974 (268–269): 110130.

[20] Kiran Kedlaya and Christopher Umans, *"Fast polynomial factorization and modular composition,"* SIAM J. Comput., 40 (2011), no. 6, pp. 1767–1802.

[21] Alan G. B. Lauder, *"Counting solutions to equations in many variables over finite fields,"* Found. Comput. Math. 4 (2004), no. 3, pp. 221–267.

[22] Alan G. B. Lauder and Daqing Wan, *"Counting points on varieties over finite fields of small characteristic,"* Algorithmic number theory: lattices, number fields, curves and cryptography, pp. 579-612, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

[23] Arjen K. Lenstra; Hendrik W. Lenstra (Jr.); Laszlo Lovász, *"Factoring polynomials with rational coefficients,"* Math. Ann. 261 (1982), no. 4, pp. 515–534.

[24] Michael Maller and Jennifer Whitehead, *"Efficient p-adic cell decomposition for univariate polynomials,"* J. Complexity *15* (1999), pp. 513-525.

[25] E. Mayr and A. Meyer, *"The Complexity of the Word Problem for Commutative Semigroups and Polynomial Ideals,"* Adv. Math. **46**, 305–329, 1982.

[26] Bernard R. McDonald, *Finite Rings with Identity,* Marcel Dekker, Inc., New York, 1974.

[27] Bjorn Poonen, *"Heuristics for the Brauer-Manin Obstruction for Curves,"* Experimental Mathematics, Volume 15, Issue 4 (2006), pp. 415–420.
[28] R. Raghavendran, *"Finite associative rings,"* Compositio Mathematica, tomme 21, no. 2 (1969), pp. 195–229.
[29] Daqing Wan, *"Algorithmic theory of zeta functions over finite fields,"* Algorithmic number theory: lattices, number fields, curves and cryptography, pp. 551–578, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.
[30] W. A. Zuniga-Galindo, *"Computing Igusa's Local Zeta Functions of Univariate Polynomials, and Linear Feedback Shift Registers,"* Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.6.

E-mail address: qcheng@ou.edu

School of Computer Science, University of Oklahoma, Norman, OK 73019

E-mail address: sgao@math.clemson.edu

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975

E-mail address: rojas@math.tamu.edu

TAMU 3368, College Station, TX 77843-3368

E-mail address: dwan@math.uci.edu

Department of Mathematics, University of California, Irvine, CA 92697-3875

FAST COEFFICIENT COMPUTATION FOR ALGEBRAIC POWER SERIES IN POSITIVE CHARACTERISTIC

ALIN BOSTAN, XAVIER CARUSO, GILLES CHRISTOL, AND PHILIPPE DUMAS

Abstract. We revisit Christol's theorem on algebraic power series in positive characteristic and propose yet another proof for it. This new proof combines several ingredients and advantages of existing proofs, which make it very well-suited for algorithmic purposes. We apply the construction used in the new proof to the design of a new efficient algorithm for computing the Nth coefficient of a given algebraic power series over a perfect field of characteristic p. It has several nice features: it is more general, more natural and more efficient than previous algorithms. Not only the arithmetic complexity of the new algorithm is linear in $\log N$ and quasi-linear in p, but its dependency with respect to the degree of the input is much smaller than in the previously best algorithm. Moreover, when the ground field is finite, the new approach yields an even faster algorithm, whose bit complexity is linear in $\log N$ and quasi-linear in $\sqrt{p}$.

1. Introduction

Given a perfect field k of characteristic $p > 0$, we address the following question: how quickly can one compute the Nth coefficient f_N of an algebraic power series

$$f(t) = \sum_{n \geq 0} f_n t^n \in k[[t]],$$

where N is assumed to be a large positive integer? This question was recognized as a very important one in complexity theory, as well as in various applications to algorithmic number theory: Atkin-Swinnerton-Dyer congruences, integer factorization, discrete logarithm and point-counting [10, 3].

As such, the question is rather vague; both the data structure and the computation model have to be stated more precisely. The algebraic series f will be specified in $k[[t]]$ as some root of a polynomial $E(t, y)$ in $k[t, y]$, of degree $d = \deg_y E \geq 1$ and of height $h = \deg_t E$. To do this specification unequivocally, we will make several assumptions. First, we assume that E is *separable*, that is E and its derivative $E_y = \partial E/\partial y$ are coprime in $k(t)[y]$. Second, we assume that E is *irreducible*[1] in $k(t)[y]$. Note that both assumptions are satisfied if E is assumed to be the minimal polynomial of f and that irreducibility implies separability as soon as we know that E has at least one root in $k[[t]]$. The polynomial E might have several roots in $k[[t]]$. In order to specify uniquely its root f, we further assume that we are given a nonnegative integer ρ together with $f_0, \ldots, f_{2\rho}$ in k such that

$$E(t, f_0 + f_1 t + \cdots + f_{2\rho} t^{2\rho}) \equiv 0 \pmod{t^{2\rho+1}},$$
$$E_y(t, f_0 + f_1 t + \cdots + f_{\rho} t^{\rho}) \not\equiv 0 \pmod{t^{\rho+1}}.$$

[1]The first assumption is not always implied by the second one, as exemplified by $E = y^p - t \in \mathbb{F}_p[t, y]$, and in general by any irreducible polynomial E in $k[t, y^p]$.

13 Jun 2018 06:16:17 PDT
Version 4 - Submitted to Open Book Series

In other words, the data structure used to represent f is the polynomial E together with the initial coefficients $f_0, \dots, f_{2\rho}$. (Actually $\rho+1$ coefficients are enough to ensure the uniqueness of f. However $2\rho+1$ coefficients are needed to ensure its existence; for this reason, we will always assume the coefficients of f are given up to index 2ρ.) We observe that it is always possible to choose ρ less than or equal to the t-adic valuation of the y-resultant of E and E_y, hence *a fortiori* $\rho \leq (2d-1)h$.

Under these assumptions, the classical Newton iteration [16] allows the computation of the first N coefficients of f in quasi-linear complexity $\tilde{O}(N)$. Here, and in the whole article (with the notable exception of Section 4), the algorithmic cost is measured by counting the number of basic arithmetic operations $(+, -, \times, \div)$ and applications of the Frobenius map $(x \mapsto x^p)$ and of its inverse $(x \mapsto x^{1/p})$ in the ground field k. The soft-O notation $\tilde{O}(\cdot)$ indicates that polylogarithmic factors in the argument are omitted. Newton's iteration thus provides a quasi-optimal algorithm to compute $f_0, \dots, f_N$. A natural and important question is whether faster alternatives exist for computing the coefficient f_N alone.

With the exception of the rational case ($d = 1$), where the Nth coefficient can be computed in complexity $O(\log N)$ by binary powering [13], the most efficient algorithm currently known to compute f_N in characteristic 0 has complexity $\tilde{O}(\sqrt{N})$ [9]. It relies on baby step / giant step techniques, combined with fast multipoint evaluation.

Surprisingly, in positive characteristic p, a radically different approach leads to a spectacular complexity drop to $O(\log N)$. However, the big-O term hides a (potentially exponential) dependency in p. The good behavior of this estimate with respect to the index N results from two facts. First, if the index N is written in radix p as $(N_{\ell-1} \dots N_1 N_0)_p$, then the coefficient f_N is given by the simple formula

$$f_N = [(\mathsf{S}_{N_{\ell-1}} \cdots \mathsf{S}_{N_1}\, \mathsf{S}_{N_0}\, f)(0)]^{p^\ell}, \tag{1}$$

where the S_r $(0 \leq r < p)$ are the *section* operators defined by

$$\mathsf{S}_r \sum_{n\geq 0} g_n t^n = \sum_{n\geq 0} g_{pn+r}^{1/p} t^n. \tag{2}$$

Note that for the finite field $\mathbb{F}_p$ the exponents p^ℓ in (1) and $1/p$ in (2) are useless, since the Frobenius map $x \mapsto x^p$ is the identity map in this case.

Second, by Christol's theorem [6, 7, 15], the coefficient sequence of an algebraic power series f over a perfect field k of characteristic $p > 0$ is *p-automatic*: this means that f generates a finite-dimensional k-vector space under the action of the section operators. Consequently, with respect to a fixed k-basis of this vector space, one can express f as a column vector C, the section operators S_r as square matrices A_r $(0 \leq r < p)$, and the evaluation at 0 as a row vector R. Formula (1) then becomes

$$f_N = [R A_{N_{\ell-1}} \cdots A_{N_1} A_{N_0} C]^{p^\ell}. \tag{3}$$

Since ℓ is about $\log N$, and since the size of the matrices A_r does not depend on N, formula (3) yields an algorithm of complexity $O(\log N)$. This observation (for any p-automatic sequence) is due to Allouche and Shallit [1, Cor. 4.5]. However, this last assertion hides the need to first find the linear representation $(R, (A_r)_{0\leq r<p}, C)$. As shown in [2, Ex. 5], already in the case of a finite prime field, translating the p-automaticity in terms of linear algebra yields matrices A_r whose size can be about

d^2hp^{2d}. Thus, their precomputation has a huge impact on the cost with respect to the prime number p.

In the particular case of a prime field $k = \mathbb{F}_p$, and under the assumption $E_y(0, f_0) \neq 0$, this was improved in [2] by building on an idea originally introduced by Christol in [6]: one can compute f_N in complexity $\tilde{O}((h+d)^5hp)+O((h+d)^2h^2 \log N)$. So far, this was the best complexity result for this task.

Contributions. We further improve the complexity result from [2] down to $\tilde{O}(d^2hp + d^\omega h) + O(d^2h^2 \log N)$ (Theorem 3.4, Section 3.2). Here ω is the exponent of matrix multiplication. In the case where k is a finite field, we propose an even faster algorithm, with bit complexity linear in $\log N$ and quasi-linear in $\sqrt{p}$ (Theorem 4.1, Section 4). It is obtained by blending the approach in Section 3.2 with ideas and techniques imported from the characteristic zero case [9]. All these successive algorithmic improvements are consequences of our main theoretical result (Theorem 2.2, Section 2.2), which can be thought of as an effective version of Christol's Theorem (and in particular reproves it).

2. Effective version of Christol's theorem

We keep the notation of the introduction. Christol's theorem is stated as follows.

Theorem 2.1 (Christol)**.** *Let $f(t)$ in $k[[t]]$ be a formal power series that is algebraic over $k(t)$, where k is a perfect field with positive characteristic. Then there exists a finite-dimensional k-vector space containing $f(t)$ and stable by the section operators.*

The aim of this section is to state and to prove an effective version of Theorem 2.1, on which our forthcoming algorithms will be built. Our approach follows the initial treatment by Christol [6], which is based on Furstenberg's theorem [14, Thm. 2]. For the application we have in mind, it turns out that the initial version of Furstenberg's theorem will be inefficient; hence we will first need to strengthen it, considering residues around the moving point $f(t)$ instead of residues at 0. Another new input we shall use is a globalization argument allowing us to compare section operators at 0 and at $f(t)$. This argument is formalized throught Frobenius operators and is closely related to the Cartier operator used in a beautiful geometric proof of Christol's theorem due to Deligne [11] and Speyer [18], and further studied by Bridy [5].

2.1. Frobenius and sections.

Recall that the ground field k is assumed to be a perfect field of prime characteristic p, for example a finite field $\mathbb{F}_q$, where $q = p^s$. Let $K = k(t)$ be the field of rational functions over k and let $L = K[y]/(E)$.

Since k is a perfect field, the Frobenius endomorphism $\mathsf{F} : k \to k$ defined by $x \mapsto x^p$ is an automorphism of k. It extends to a ring homomorphism, still denoted by F, from $L[t^{1/p}]$ to L which raises an element of $L[t^{1/p}] = L^{1/p}$ to the power p. This homomorphism is an isomorphism and its inverse writes

$$\mathsf{F}^{-1} = \sum_{r=0}^{p-1} t^{r/p}\, \mathsf{S}_r, \tag{4}$$

where each S_r, with $0 \leq r < p$, maps L onto itself.

The use in (4) of the same notation as in Formula (2) is not a mere coincidence. The algebraic series f provides an embedding of L into the field of Laurent series $k((t))$, which is the evaluation of an element $P(y)$ of L at the point $y = f(t)$. We

will call $\mathsf{eval}_f : L \to k((t))$ the corresponding map, which sends $P(y)$ to $P(f(t))$. The Frobenius operator extends from L to $k((t))$, and the same holds for the sections S_r $(0 \le r < p)$. These extensions are exactly those of Eq. (2). The S_r's in Eq. (4) then appear as global variants of the S_r's in Eq. (2). Moreover, global and local operators are compatible, in the sense that they satisfy

$$\mathsf{F} \circ \mathsf{eval}_f = \mathsf{eval}_f \circ \mathsf{F}, \quad \mathsf{S}_r \circ \mathsf{eval}_f = \mathsf{eval}_f \circ \mathsf{S}_r \,. \tag{5}$$

As for rational functions, the Frobenius operator and the section operators induce, respectively, a ring isomorphism F from $K[t^{1/p}]$ onto K and maps σ_r $(0 \le r < p)$ from K onto K such that $\mathsf{F}^{-1} = \sum_{r=0}^{p-1} t^{r/p}\, \sigma_r$. The operators F and S_r $(0 \le r < p)$ are not K-linear but only k-linear. More precisely, for any λ in $K[t^{1/p}]$, μ in K, and z in L,

$$\mathsf{F}(\lambda z) = \mathsf{F}(\lambda)\, \mathsf{F}(z) \quad \text{and} \quad \mathsf{S}_r(\mu z) = \sum_{s=0}^{p-1} t^{\lfloor \frac{r+s}{p} \rfloor} \sigma_s(\mu)\, \mathsf{S}_{r-s}(z). \tag{6}$$

In other words both F and F^{-1} are actually semi-linear.

2.2. **The key theorem.** Let $k[t,y]_{<h,<d}$ be the set of polynomials $P \in k[t,y]$ such that $\deg_t P < h$ and $\deg_y P < d$.

Theorem 2.2. *For $P \in k[t,y]_{<h,<d}$ and for $0 \le r < p$, there exists a (unique) polynomial Q in $k[t,y]_{<h,<d}$ such that*

$$\mathsf{S}_r\left(\frac{P}{E_y}\right) \equiv \frac{Q}{E_y} \pmod{E}. \tag{7}$$

The rest of this subsection is devoted to the proof of Theorem 2.2. Although mainly algebraic, the proof is based on the rather analytic remark that any algebraic function in $k(t)[f]$ can be obtained as the residue at $T = f$ of some rational function in $k(t,T)$ (see Lemma 2.3). This idea was already used in Furstenberg [14], whose work has been inspiring for us. The main new insight of our proof is the following: we replace several small branches around zero by a single branch around a moving point. In order to make the argument work, we shall need further to relate the behavior of the section operators around 0 and around the aforementioned moving point. This is where the reinterpretation of the S_r's in terms of Frobenius operators will be useful.

We consider the ring $\mathcal{H} = k((t))[[T]]$ of power series over $k((t))$. Its fraction field is the field $\mathcal{K} = k((t))((T))$ of Laurent series over $k((t))$. There is an embedding $k((t))[y] \to \mathcal{H}$ taking a polynomial in y to its Taylor expansion around f. Formally, it is simply obtained by mapping the variable y to $f+T$. It extends to a field extension $k((t))(y) \to \mathcal{K}$. We will often write $P(t, f+T)$ for the image of $P(t,y) \in k((t))(y)$ in $\mathcal{K}$. The field $\mathcal{K}$ is moreover endowed with a *residue map* $\mathrm{res} : \mathcal{K} \to k((t))$, defined by $\mathrm{res}\left(\sum_{i=v}^{\infty} a_i T^i\right) = a_{-1}$ (by convention, $a_{-1} = 0$ if $v > -1$). It is clearly $k((t))$-linear.

Lemma 2.3. *For any polynomial $P \in k((t))[y]$, the following equality holds:*

$$\mathrm{res}\left(\frac{P(t, f+T)}{E(t, f+T)}\right) = \frac{P(t,f)}{E_y(t,f)}.$$

Proof. Since f is a simple root of E, the series $E(t, f+T)$ has a simple zero at $T = 0$. This means that it can be written $E(t, f+T) = T \cdot q(T)$ with $q \in \mathcal{H}$, $q(0) \neq 0$. Taking the logarithmic derivative with respect to T gives

$$\frac{E_y(t, f+T)}{E(t, f+T)} = \frac{1}{T} + \frac{q'(T)}{q(T)},$$

akin to [14, Formula (15), p. 276], from which we derive

$$\frac{P(t, f+T)}{E(t, f+T)} = \frac{g(T)}{T} + g(T)\,\frac{q'(T)}{q(T)},$$

where $g(T) = P(t, f+T)/E_y(t, f+T)$. Since $E_y(t, f+T)$ does not vanish at $T = 0$, the series $g(T)$ has no pole at 0. Therefore, the residue of $g(T)/T$ is nothing but $g(0)$. Besides the residue of the second summand $g(T)\,q'(T)/q(T)$ vanishes. All in all, the residue of $P(t, f+T)/E(t, f+T)$ is $g(0) + 0 = P(t, f)/E_y(t, f)$. □

We now introduce analogues of section operators over $\mathcal{K}$. For this, we first observe that the Frobenius operator $x \mapsto x^p$ defines an isomorphism $\mathsf{F} : \mathcal{K}[t^{1/p}, T^{1/p}] \to \mathcal{K}$. Moreover $\mathcal{K}[t^{1/p}, T^{1/p}]$ is a field extension of $\mathcal{K}$ of degree p^2. A basis of $\mathcal{K}[t^{1/p}, T^{1/p}]$ over $\mathcal{K}$ is of course $(t^{r/p}\,T^{s/p})_{0 \leq r,s < p}$, but it will be more convenient for our purposes to use a different one. It is given by the next lemma.

Lemma 2.4. *The family $(t^{r/p}\,(f+T)^{s/p})_{0 \leq r,s < p}$ is a basis of $\mathcal{K}[t^{1/p}, T^{1/p}]$ over $\mathcal{K}$.*

Proof. For simplicity, we set $y = f+T \in \mathcal{K}$. We have:

$$\begin{pmatrix} 1 & y^{1/p} & \cdots & y^{(p-1)/p} \end{pmatrix} = \begin{pmatrix} 1 & T^{1/p} & \cdots & T^{(p-1)/p} \end{pmatrix} \cdot U$$

where U is the square matrix whose (i, j) entry (for $0 \leq i, j < p$) is $\binom{j}{i} f^{i/p}$. In particular, U is upper triangular and all its diagonal entries are equal to 1. Thus U is invertible and the conclusion follows. □

For r and s in $\{0, 1, \ldots, p-1\}$, we define the section operators $\mathsf{S}_{r,s} : \mathcal{K} \to \mathcal{K}$ by

$$\mathsf{F}^{-1} = \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} t^{r/p} (f+T)^{s/p}\ \mathsf{S}_{r,s}\,.$$

(These operations look like those used in [2, §3.2], but they are not exactly the same.) Clearly $\mathsf{S}_{r,0}$ extends the operator $\mathsf{S}_r : k((t)) \to k((t))$ defined by Eq. (2) and $\mathsf{S}_{r,s}(g_1^p g_2) = g_1\,\mathsf{S}_{r,s}(g_2)$ for all $g_1, g_2 \in \mathcal{K}$. We observe moreover that the $\mathsf{S}_{r,s}$'s stabilize the subrings $k((t))[y]$ and $k[t, y]$, since y corresponds to $f+T$.

Proposition 2.5. *The following commutation relation holds over $\mathcal{K}$:*

$$\mathsf{S}_r \circ \mathrm{res} = \mathrm{res} \circ \mathsf{S}_{r,p-1}\,.$$

Proof. Let us write $g \in \mathcal{K}$ as $g = \sum_{i=v}^{\infty} a_i T^i$ with $v \in \mathbb{Z}$ and $a_i \in k((t))$ for all $i \geq v$. Its image under F^{-1} can be expressed in two different ways as follows:

$$\mathsf{F}^{-1}(g) = \sum_{i=v}^{\infty} \mathsf{F}^{-1}(a_i)\,T^{i/p} = \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} t^{r/p} (f+T)^{s/p}\ \mathsf{S}_{r,s}(g).$$

We identify the coefficient in $T^{-1/p}$. For doing so, we observe that the terms obtained with $s < p-1$ do not contribute, while the contribution of the term

$t^{r/p}(f+T)^{(p-1)/p}\ \mathsf{S}_{r,p-1}(g)$ is the residue of $t^{r/p}\ \mathsf{S}_{r,p-1}(g)$. We then get

$$\mathsf{F}^{-1}(a_{-1}) = \sum_{r=0}^{p-1} \mathrm{res} \circ \mathsf{S}_{r,p-1}(g) \cdot t^{r/p}.$$

Going back to the definition of S_r, we derive $\mathsf{S}_r(a_{-1}) = \mathrm{res} \circ \mathsf{S}_{r,p-1}(g)$, from which the lemma follows. □

Proof of Theorem 2.2. Let $P \in k[t,y]$ and $0 \le r < p$. We set $Q = \mathsf{S}_{r,p-1}(PE^{p-1}) \in k[t,y]$. Combining Lemma 2.3 and Proposition 2.5, we derive the following equalities:

$$\begin{aligned}\mathsf{S}_r\left(\frac{P(t,f)}{E_y(t,f)}\right) &= \mathsf{S}_r \circ \mathrm{res}\left(\frac{P(t,f+T)}{E(t,f+T)}\right)\\ &= \mathrm{res} \circ \mathsf{S}_{r,p-1}\left(\frac{P(t,f+T)}{E(t,f+T)}\right) = \mathrm{res}\left(\frac{Q(t,f+T)}{E(t,f+T)}\right) = \frac{Q(t,f)}{E_y(t,f)}\end{aligned}$$

(compare with [2, §3.2]). The stability of $k[t,y]/E(t,y)$ under S_r follows using the fact that E is the minimal polynomial of f over $K = k(t)$. If we know in addition that P lies in $k[t,y]_{<h,<d}$ then $P\,E^{p-1}$ is in $k[t,y]_{<ph,\le p(d-1)}$ and, therefore, Q falls in $k[t,y]_{<h,<d}$ as well. Theorem 2.2 is proved. □

Remark 2.6. It is possible to slightly vary the bounds on the degree and the height, and to derive this way other stability statements. For example, starting from a polynomial $P(t,y)$ with $\deg_t P \le h$ and $\deg_y P \le d$, we have:

$$\mathsf{S}_r\,\frac{P(t,f)}{E_y(t,f)} = \frac{Q(t,f)}{E_y(t,f)}$$

with $\deg_t Q \le h$ and $\deg_y P < d$. Moreover $\deg_t Q < h$ provided that $r > 0$.

Another remark in this direction is the following: if P has degree at most $d-2$, the section $\mathsf{S}_{r,p-1}(PE^{p-1})$ has degree at most $d-2$ for any $r \in \{0,1,\ldots,p-1\}$. Indeed, PE^{p-1} has degree at most $pd-2 < p(d-1)+p-1$. In other words, the subspace $k[t,y]_{<h,\le d-2}$ is stable by the section operators S_r $(0 \le r < p)$.

3. Application to algorithmics

Theorem 2.2 exhibits an easy-to-handle finite dimensional vector space which is stable under the section operators. In this section, we derive from it two efficient algorithms that compute the Nth term of f in linear time in $\log N$. The first is less efficient, but easier to understand; we present it mainly for pedagogical purposes.

3.1. **First algorithm: modular computations.** The first algorithm we will design follows rather straightforwardly from Theorem 2.2. It consists of the following steps:

(1) we compute the matrix giving the action of the Frobenius F with respect to the "modified monomial basis" $\mathcal{B} = (y^j/E_y)_{0\le j\le d-1}$;
(2) we deduce the matrix of F^{-1} with respect to $\mathcal{B}$;
(3) we extract from it the matrices of the section operators S_r;
(4) we compute the Nth coefficient of f using Formula (1).

Let us be a bit more precise (though we will not give full details because we will design in §3.2 below an even faster algorithm). Let M be the matrix of F in the basis $\mathcal{B}$; its jth column contains the coordinates of the vector $\mathsf{F}(\frac{y^j}{E_y}) = \frac{y^{pj}}{E_y^p}$ in the basis

$$M = \begin{pmatrix} 1 + 2t^4 + 4t^5 + 3t^6 + 2t^7 + 2t^8 + 2t^{12} + 4t^{13} + 3t^{14} + t^{15} + 2t^{16} & \cdots \\ t + 2t^2 + 3t^3 + 4t^5 + 4t^6 + 3t^7 + 3t^8 + 3t^9 + t^{10} + 4t^{11} + t^{13} + 2t^{15} + t^{16} & \cdots \\ 1 + 2t + 3t^2 + 3t^5 + 2t^6 + 2t^7 + t^8 + t^9 + 3t^{10} + t^{11} + 3t^{12} + 3t^{14} + 4t^{15} + 3t^{16} & \cdots \\ 0 & \cdots \end{pmatrix} \pmod{t^{17}}$$

$$M^{-1} = \begin{pmatrix} 1 + 3t^4 + t^8 + t^{12} + t^{13} + t^{16} & t^4 + 2t^8 & t^8 + t^{12} & t^{12} \\ 2 + 2t + \cdots + t^9 + 3t^{12} & 3 + 2t + \cdots + 2t^{13} + t^{16} & 3 + 4t + t^5 + t^8 & 1 + 4t^4 + 3t^5 + 2t^9 + 2t^{12} \\ 4 + 2t + \cdots + 2t^9 + 4t^{12} & 4 + 2t + \cdots + +2t^9 + 4t^{12} & 1 + 2t + \cdots + 3t^{13} + t^{16} & 2 + 4t + \cdots + 4t^5 + 2t^8 \\ 0 & 0 & 0 & 1 + 4t + \cdots + 4t^{13} + t^{16} \end{pmatrix}$$

FIGURE 1. Frobenius and its inverse in the "modified monomial basis".

$\mathcal{B}$, which are also the coordinates of y^{pj}/E_y^{p-1} in the monomial basis $(1, y, \ldots, y^{d-1})$. It is easily seen that the matrix of F^{-1} with respect to $\mathcal{B}$ is $\mathsf{F}^{-1}(M^{-1})$, which is, by definition, the matrix obtained by applying F^{-1} to each entry of M^{-1}.

We now discuss the complexity of the computation of M^{-1}. Thanks to Theorem 2.2 and Eq. (4), we know that its entries are polynomials of degree at most $h(p-1)$. However, this bound is not valid for the entries of M. Indeed, in full generality, the latter are rational fractions whose numerators and denominators have degrees of magnitude dhp. In order to save the extra factor d, we rely on modular techniques: we choose a polynomial B of degree $h(p-1)+1$ and perform all computations modulo B. To make the method work, B must be chosen in such a way that both M and M^{-1} make sense modulo B, *i.e.* B must be coprime with the denominators of the entries of M. The latter condition discards a small number of choices, so that a random polynomial B will be convenient with high probability.

Using fast polynomial and matrix algorithms, the computation of M modulo B can be achieved within $\tilde{O}(d^2hp)$ operations in k, while the inversion of M modulo B requires $\tilde{O}(d^\omega hp)$ operations in k, where $\omega \in [2,3]$ is the matrix multiplication exponent. Since we count an application of $\mathsf{F}^{-1} : k \to k$ as a unique operation, the cost of the first two steps is $\tilde{O}(d^\omega hp)$ as well. The third step is free as it only consists in reorganizing coefficients. As for the evaluation of the formula (1), each application of S_r has a cost of $O(d^2h^2)$ operations in k. The total complexity of our algorithm is then $\tilde{O}(d^\omega hp) + O(d^2h^2 \log N)$ operations in k.

Remark 3.1. We do not need actually to apply the Frobenius inverse $\mathsf{F}^{-1} : k \to k$ since, at the end of the computation, we raise the last intermediate result at the power p^ℓ. The complexity $\tilde{O}(d^\omega hp) + O(d^2h^2 \log N)$ can then be reached even if we do not count an application of F^{-1} as a single operation.

A detailed example. Consider $k = \mathbb{F}_5$ and the polynomial

$$E = (t^4 + t + 1)y^4 + y^2 + y - t^4 \in k[t, y].$$

It admits a unique root f in $k[[t]]$ which is congruent to 0 modulo t.

The matrix M of the Frobenius F with respect to the basis $\mathcal{B} = (\frac{1}{E_y}, \frac{y}{E_y}, \frac{y^2}{E_y}, \frac{y^3}{E_y})$ writes $D^{-1} \cdot \widetilde{M}$, where D and the largest entry of $\widetilde{M}$ have degrees 55 and 39, respectively. However, by Theorem 2.2, we know that M^{-1} has polynomial entries of degree at most 16. Noticing that 0 is not a root of the resultant of E and E_y, we can compute M and its inverse modulo $B(t) = t^{17}$. The result of this computation is displayed partly on Figure 1. We observe that the maximal degree of the entries

of M^{-1} is 16 and reaches our bound $h(p-1)$ (which is then tight for this example). We furthermore observe that M is block triangular, as expected after Remark 2.6.

Let us now compute the images of $y \in L$ under the section operators. For this, we write $y = E_y^{-1} \cdot \big(4t^4 + 2y + 3y^2\big)$ in L. We then have to compute the product $M^{-1} \cdot (4t^4 \quad 2 \quad 3 \quad 0)^T$. As a result, we obtain:

$$\begin{pmatrix} t^4 + 4t^8 + 2t^{12} + 4t^{16} + 4t^{17} + 4t^{20} \\ t + 3t^4 + 2t^5 + t^8 + 3t^9 + 4t^{10} + 3t^{12} + 3t^{13} + 4t^{16} \\ 1 + 2t^2 + 3t^3 + 4t^4 + t^5 + t^6 + 4t^7 + 4t^8 + 3t^9 + 2t^{10} + 2t^{13} + 4t^{16} \\ 0 \end{pmatrix}.$$

Rearranging the terms, we finally find that

$$\begin{aligned}
\mathsf{S}_0(y) &= E_y^{-1} \cdot \big(4t^4 + (2t + 4t^2)y + (1 + t + 2t^2)y^2\big) \\
\mathsf{S}_1(y) &= E_y^{-1} \cdot \big(4t^3 + (1 + 4t^3)y + (t + 4t^3)y^2\big) \\
\mathsf{S}_2(y) &= E_y^{-1} \cdot \big((2t^2 + 4t^3) + 3t^2 y + (2 + 4t)y^2\big) \\
\mathsf{S}_3(y) &= E_y^{-1} \cdot \big(4t + (t + 3t^2)y + (3 + 4t + 2t^2)y^2\big) \\
\mathsf{S}_4(y) &= E_y^{-1} \cdot \big(1 + (3 + 3t)y + (4 + 3t)y^2\big).
\end{aligned}$$

To conclude this example, suppose that we want to compute the 70th coefficient of f. Applying Eq. (1), we find that it is equal to the constant coefficient of $\mathsf{S}_2\,\mathsf{S}_4\,\mathsf{S}_0\,f$. Therefore we have to compute $\mathsf{S}_2\,\mathsf{S}_4\,\mathsf{S}_0\,y$. Repeating twice what we have done before, we end up with

$$\mathsf{S}_2\,\mathsf{S}_4\,\mathsf{S}_0\,y = E_y^{-1} \cdot \big((2 + t^2) + (4 + 3t + 3t^3)y + (2 + 4t^2 + 2t^3)y^2\big).$$

Plugging $y = f$ in the above equality, we get $\mathsf{S}_2\,\mathsf{S}_4\,\mathsf{S}_0\,f = 2 + O(t)$, from which we conclude that $f_{70} = 2$.

Remark 3.2. In the above example, only the constant coefficient of f was needed to carry out the whole computation. This is related to the fact that $E_y(f(t))$ has t-adic valuation 0. More generally if $E_y(f(t))$ has t-adic valuation ρ, we will need the first $\rho+1$ coefficients of f since the final division by E_y will induce a loss of t-adic precision of ρ "digits". This does not change the complexity bound, since $\rho \leq \deg_t \operatorname{Res}_y(E, E_y) \in O(dh)$.

3.2. **Second algorithm: Hermite–Padé approximation.** For obvious reasons related to the size of the computed objects, we cannot hope to achieve a complexity lower than linear with respect to p using the approach of Section 3.1. However, the exponent on d still can be improved. In order to achieve this, we return to Theorem 2.2. The key idea is to leap efficiently from the polynomial P to the polynomial Q in Formula (7).

Let $P = \sum_{i=0}^{d-1} a_i(t)y^i$ in $k[t,y]_{<h,<d}$ and $0 \leq r < p$. By Theorem 2.2, there exists $Q = \sum_{i=0}^{d-1} b_i(t)y^i$ in $k[t,y]_{<h,<d}$ such that $\mathsf{S}_r(P/E_y) \equiv Q/E_y \pmod{E}$, or, equivalently,

$$\mathsf{S}_r\left(\sum_{i=0}^{d-1} a_i(t)\frac{f(t)^i}{E_y(t,f(t))}\right) = \sum_{j=0}^{d-1} b_j(t)\frac{f(t)^j}{E_y(t,f(t))}. \tag{8}$$

The algorithmic question is to recover efficiently the b_i's starting from the a_i's. Identifying coefficients in Eq. (8) yields a linear system over k in the coefficients of

the unknown polynomials b_i. This system has hd unknowns and an infinite number of linear equations. The point is that the following truncated version of Eq. (8)

$$\mathsf{S}_r\left(\sum_{i=0}^{d-1} a_i(t)\frac{f(t)^i}{E_y(t,f(t))}\right) \equiv \sum_{j=0}^{d-1} b_j(t)\frac{f(t)^j}{E_y(t,f(t))} \pmod{t^{2dh}} \tag{9}$$

is sufficient to uniquely determine Q. This is a direct consequence of the following.

Lemma 3.3. *If Q in $k[t,y]_{<h,<d}$ satisfies $\frac{Q}{E_y}(t,f(t)) \equiv 0 \pmod{t^{2dh}}$, then $Q = 0$.*

Proof. The resultant $r(t)$ of $E(t,y)$ and $Q(t,y)$ with respect to y is a polynomial of degree at most $d(h-1)+h(d-1)$. On the other hand, we have a Bézout relation

$$E(t,y)\,u(t,y) + Q(t,y)\,v(t,y) = r(t),$$

where $u(t,y)$ and $v(t,y)$ are bivariate polynomials in $k[t,y]$. By evaluating the previous equality at $y = f(t)$ it follows that

$$r(t) \equiv Q(t,f(t))\,v(t,f(t)) \equiv 0 \pmod{t^{2dh}}$$

holds in $k((t))$, and therefore $r = 0$. Thus E and Q have a non-trivial common factor; since E is irreducible, it must divide Q. But $\deg_y Q < \deg_y E$, so $Q = 0$. □

Solving Eq. (9) amounts to solving a *Hermite–Padé approximation* problem. In terms of linear algebra, it translates into solving a linear system over k in the coefficients of the unknown polynomials b_i. This system has dh unknowns and $N = 2dh$ linear equations. Moreover, it has a very special shape: it has a quasi-Toeplitz structure, with displacement rank $\Delta = O(d)$. Therefore, it can be solved using fast algorithms for structured matrices [17, 4] in $\tilde{O}(\Delta^{\omega-1}N) = \tilde{O}(d^\omega h)$ operations in k. These algorithms first compute a (quasi)-inverse of the matrix encoding the homogenous part of the system, using a compact data-structure called displacement generators (or, ΣLU representation); then, they apply it to the vector encoding the inhomogeneous part. The first step has complexity $\tilde{O}(\Delta^{\omega-1}N) = \tilde{O}(d^\omega h)$, the second step has complexity $\tilde{O}(\Delta N) = \tilde{O}(d^2 h)$.

In our setting, we will need to solve $\log N$ systems of this type, each corresponding to the current digit of N in radix p. An important feature is that these systems share the same homogeneous part, which only depends on the coefficients of the power series $s_j(t) = \frac{f^j}{E_y(t,f(t))}$ occurring on the right-hand side of (9). Only the inhomogeneous parts vary: they depend on the linear combination $\sum_{i=0}^{d-1} a_i(t)s_i(t)$. Putting these facts together yields Algorithm 1 and the following complexity result.

Theorem 3.4. *Let k be a perfect field with characteristic $p > 0$. Let $E(t,y)$ be an irreducible polynomial in $k[t,y]$ of height h and degree d. We assume that we are given a nonnegative integer ρ and a polynomial $\bar{f}(t)$ such that $E(t,\bar{f}(t)) \equiv 0 \pmod{t^{2\rho+1}}$ and $E_y(t,\bar{f}(t)) \not\equiv 0 \pmod{t^{\rho+1}}$.*

There there exists a unique series $f(t)$ congruent to $\bar{f}(t)$ modulo $t^{\rho+1}$ for which $E(t,f(t)) = 0$. Moreover, Algorithm 1 computes the Nth coefficient of f for a cost of $\tilde{O}(d^2hp + d^\omega h) + O(d^2h^2 \log N)$ operations in k.

Proof. The first assertion is Hensel's Lemma [12, Th. 7.3].

The precomputation of $s_j(t) = \frac{f(t)^j}{E_y(t,f(t))}$ modulo t^{2dhp} for $0 \le j < d$ can be performed using Newton iteration, for a total cost of $\tilde{O}(d^2hp)$ operations in k. As

Algorithm **Nth coefficient *via* Hermite-Padé.**

Input: A polynomial $E(t,y) = e_d(t)y^d + \cdots + e_0(t)$ and a truncation $g = f_0 + \cdots + O(t^{\rho+1})$ of a series f such that $E(t,g) = O(t^{\rho+1})$.
Output: The Nth coefficient f_N of the series f.

1. Precompute the first $2pdh$ coefficients of the series expansions s_j of $f(t)^j/E_y(t,f)$, $0 \le j < d$.
2. Precompute the quasi-inverse of the Toeplitz matrix corresponding to the Hermite–Padé approximation problem.
3. Expand $N = (N_{\ell-1} \dots N_0)_p$ with respect to the radix p.
4. Set $g = y \in L$ written as $E_y^{-1} \cdot \big(-de_0 - (d-1)e_1 y - \cdots - e_{d-1}y^{d-1}\big)$.
5. For $i = 0, 1, \dots, \ell - 1$,
   (1) write $g = P(t,f)/E_y(t,f)$ as a linear combination of the s_j's,
   (2) compute the section $\mathsf{S}_{N_i}(g)$ at precision $O(t^{2dh})$,
   (3) recover Q such that $\mathsf{S}_{N_i}(g) = Q/E_y$ by Hermite–Padé,
   (4) redefine g as Q/E_y
6. Replace y by $\bar{f}(t)$ in g and call $\bar{g}(t)$ the obtained result.
7. Expand $\bar{g}(t)$ at precision $O(t)$.
8. Set $\bar{g}_0$ to the constant coefficient of $\bar{g}(t)$.
9. Return $\bar{g}_0^{p^\ell}$.

Algorithm 1

explained above, this is enough to set up the homogeneous part of the quasi-Toeplitz system; its inversion has cost $\tilde{O}(d^\omega h)$.

Let us turn to the main body of the computation, which depends on the index N. For each p-digit $r = N_i$ of N, we first construct the inhomogeneous part of the system. For this, we extract the coefficients of t^{pj+r} in $\sum_{i=0}^{d-1} a_i(t)s_i(t)$, for $0 \le j < d$, for a total cost of $O(d^2h^2)$ operations in k. We then apply the inverse of the system to it, for a cost of $O(d^2h^2)$ (using a naive matrix vector multiplication[2]). This is done $\ell \approx \log N$ times. The other steps of the algorithm have negligible cost. □

4. Improving the complexity with respect to p

As shown in Theorem 3.4, Algorithm 1 has a nice complexity with respect to the parameters d, h and $\log N$: it is polynomial with small exponents. However, the complexity with respect to p is not that good, as it is exponential in $\log p$, which is the relevant parameter. Thus, when p is large (say $> 10^5$), Algorithm 1 runs slowly and is no longer usable.

For this reason, it is important to improve the complexity with respect to p. In this section, we introduce some ideas to achieve this. More precisely, our aim is to design an algorithm whose complexity with respect to p and N is $\tilde{O}(\sqrt{p}) \cdot \log N$, and remains polynomial in all other relevant parameters. In the current state of knowledge, it seems difficult to decrease further the exponent on p; indeed, the question addressed in this paper is related to other intensively studied questions

[2]One can actually achieve this step for a cost of $\tilde{O}(d^2h)$ operations in k using the quasi-Toeplitz structure; however this is not that useful since the cost of the previous step was already $O(d^2h^2)$.

(e.g., counting points *via* p-adic cohomologies) for which the barrier $\tilde{O}(\sqrt{p})$ has not been overcome yet.

Notations and assumptions. We keep the notation of previous sections. We make one additional hypothesis: *the ground field k is a finite field.* We assume that k is represented as $(\mathbb{Z}/p\mathbb{Z})[X]/\pi(X)$ where π is an irreducible monic polynomial over $\mathbb{Z}/p\mathbb{Z}$ of degree s. We choose a monic polynomial $\hat{\pi} \in \mathbb{Z}[X]$ of degree s lifting π. We set $W = \mathbb{Z}_p[X]/\hat{\pi}(X)$ where $\mathbb{Z}_p$ is the ring of p-adic integers.

The algorithm we are going to design is not algebraic in the sense that it does not only perform algebraic operations in the ground field k, but will sometimes work over W (or, more exactly, over finite quotients of W). For this reason, throughout this section, we will use bit complexity instead of algebraic complexity.

We use the notation $\mathrm{poly}(n)$ to indicate a quantity whose growth is at most polynomial in n. The precise result we will prove reads as follows.

Theorem 4.1. *Under the assumptions of Theorem 3.4 and the above extra assumptions, there exists an algorithm of bit complexity $\mathrm{poly}(dh)\tilde{O}(s\sqrt{p})\log N$ that computes the Nth coefficient of f.*

If p is bounded by a (fixed) polynomial in d and h, then Theorem 4.1 has been proved already. In the sequel, we will then always assume that $p \gg d, h$.

Overview of the strategy. We reuse the structure of Algorithm 1 but speed up the computation of the $\mathsf{S}_{N_i}(g)$'s. Precisely, in Algorithm 1, the drawback was the computation of the $\frac{f^j}{E_y(t,f)}$'s or, almost equivalently, the computation of $g = \frac{P(t,f)}{E_y(t,f)}$ at sufficient precision. However, only a few (precisely $2dh$) coefficients of g are needed, since we are only interested in one of its sections. A classical method for avoiding this overhead is to find a (small) recurrence on the coefficients on $g = \sum_{n=0}^{\infty} g_i t^i$ of the form:

$$b_r(i)g_{i+r} + b_{r-1}(i)g_{i+r-1} + \cdots + b_1(i)g_{i+1} + b_0(i)g_i = 0. \tag{10}$$

We then unroll it using matrix factorials (for which fast algorithms are available in the literature [9] Unrolling the recurrence is straightforward as soon as the leading coefficient $b_r(i)$ does not vanish. On the contrary, when $b_r(i) = 0$, the value of g_{i+r} cannot be deduced from the previous ones. Unfortunately, it turns out that $b_r(i)$ does sometimes vanish in our setting.

We tackle this issue by lifting everything over W and performing all computations over this ring. Divisions by p then become possible but induce losses of precision. We then need to control the p-adic valuation of the denominators, that are the p-adic valuations of the $b_r(i)$'s. We cannot expect to have a good control on them in full generality; even worse, we can build examples where $b_r(i)$ vanishes in W for some i. There exists nevertheless a good situation—the so-called *ordinary case*—where we can say a lot on the $b_r(i)$'s. With this extra input, we are able to lead our strategy to its end.

The general case reduces to the ordinary one using a change of origin, *i.e.* replacing t by $u+\alpha$ for some $\alpha \in k$. This change of origin does not seem to be harmless *a priori*. Indeed the Taylor expansion of g around α (the one we shall compute) has in general nothing to do with the Taylor expansion of g around 0 (the one we are interested in). The sections are nevertheless closely related (see Proposition 4.3). This "miracle" is quite similar to what we have already observed in Proposition 2.5 and again can be thought of as an avatar of the Cartier operator.

4.1. **From algebraic equations to recurrences.** We consider a bivariate polynomial $P(t,y) \in k[t,y]$ with $\deg_t P < h$ and $\deg_y P < d$. We fix moreover an integer r is the range $[0, p-1]$. Our aim is to compute $\mathsf{S}_r\big(\frac{P(t,f)}{E_y(t,f)}\big)$ at precision $O(t^{2dh})$. Set $g = \frac{P(t,f)}{E_y(t,f)}$ and write $g = \sum_{i=0}^{\infty} g_i t^i$. By definition $\mathsf{S}_r(g) = \sum_{j=0}^{\infty} g_{r+pj}^{1/p} t^j$, so that we have to compute the coefficients g_{r+pj} for $j < 2dh$.

We let L be the leading coefficient of $E(t,y)$ and R be the resultant of E and E_y. To begin with, we make the following assumption (which will be relaxed in §4.3):

(H1): Both L and R have t-adic valuation 0.

As explained above, we now lift the situation over W. We choose a polynomial $\hat{E} \in W[t,f]$ of bidegree (h,d) lifting E. We define $\hat{E}_t = \frac{\partial \hat{E}}{\partial t}$, $\hat{E}_y = \frac{\partial \hat{E}}{\partial y}$. The assumption **(H1)** implies that the series f lifts uniquely to a series $\hat{f} \in W[[t]]$ such that $\hat{E}(t,\hat{f}) = 0$. We define $\hat{L}$ as the leading coefficient of $\hat{E}(t,y)$ and set $\hat{R} = \mathrm{Res}(\hat{E}, \hat{E}_y)$. We introduce the ring $W_K = W[t, (\hat{L}\hat{R})^{-1}]$. By **(H1)**, W_K embeds canonically into $W[[t]]$. We pick a polynomial $\hat{P} \in W[t,y]$ lifting P such that $\deg_t \hat{P} < h$ and $\deg_y \hat{P} < d$. We set $\hat{g} = \hat{P}(t,\hat{f})$.

We now compute a linear differential equation satisfied by $\hat{g}$. For this, we observe that the derivation $\frac{\partial}{\partial t} : W[[t]] \to W[[t]]$ stabilizes the subring $W_L = W_K[\hat{f}]$. Indeed from the relation $\hat{E}(t,\hat{f}) = 0$, we deduce that $\frac{\partial \hat{f}}{\partial t} = -\frac{\hat{E}_t(t,\hat{f})}{\hat{E}_y(t,\hat{f})}$. Thus $\frac{\partial \hat{f}}{\partial t} \in W_L$ because $\hat{E}_y(t,\hat{f})$ is invertible in W_L thanks to **(H1)**. Using additivity and the Leibniz relation, we finally deduce that $\frac{\partial}{\partial t}$ takes W_L to itself. In particular, all the successive derivatives of $\hat{g}$ lie in W_L. On the other hand, we notice that W_L is free of rank d over W_K with basis $(1, \hat{f}, \ldots, \hat{f}^{d-1})$. Let M be the $d \times d$ matrix whose jth column (for $0 \le j < d$) contains the coordinates of $\frac{\partial^j \hat{g}}{\partial t^j}$ with respect to the above basis. Similarly let C be the column vector whose entries are the coordinates of $\frac{\partial^d \hat{g}}{\partial t^d}$. Let $\Delta_d = \det M$. We solve the system $MX = C$ using Cramer's formulae and find this way a linear differential equation of the form:

$$\Delta_d \frac{\partial^d \hat{g}}{\partial t^d} + \Delta_{d-1} \frac{\partial^{d-1} \hat{g}}{\partial t^{d-1}} + \cdots + \Delta_1 \frac{\partial \hat{g}}{\partial t} + \Delta_0 \hat{g} = 0,$$

where the other Δ_i's are defined as determinants as well. In particular, they all lie in W_K. Multiplying by the appropriate power of $\hat{L}\hat{R}$, we end up with a differential equation of the form:

$$\hat{a}_d \frac{\partial^d \hat{g}}{\partial t^d} + \hat{a}_{d-1} \frac{\partial^{d-1} \hat{g}}{\partial t^{d-1}} + \cdots + \hat{a}_1 \frac{\partial \hat{g}}{\partial t} + \hat{a}_0 \hat{g} = 0 \tag{11}$$

where the $\hat{a}_i$'s are polynomials in t. We can even be more precise. Indeed, following the above constructions, we find that all entries of M and C are rational functions whose degrees (of numerators and denominators) stay within $\mathrm{poly}(dh)$. We then deduce that the degrees of the $\hat{\Delta}_i$'s and $\hat{a}_i$'s are in $\mathrm{poly}(dh)$ as well. Furthermore, they can be computed for a cost of $\mathrm{poly}(dh)$ operations in k, that is $\mathrm{poly}(dh)\tilde{O}(s \log p)$ bit operations (recall that s denotes the degree of k over $\mathbb{F}_p$)

We write $\hat{g} = \sum_{i=0}^{\infty} \tilde{g}_i \frac{t^i}{i!}$. The differential equation (11) translates to a recurrence relation on the $\tilde{g}_i$'s of the form:

$$\forall n \ge r, \quad \tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \cdots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0 \tag{12}$$

where the $\tilde{b}_i$'s are polynomials in n over W whose degrees are in poly(dh). Moreover r is at most $d + \max_i \deg \hat{a}_i$. In particular, $r \in \text{poly}(dh)$. Finally it is easy to write down explicitly $\tilde{b}_0$: it is the constant polynomial with value $\hat{a}_d(0)$.

4.2. **The ordinary case.** In order to take advantage of Eq. (12), we make the following extra assumption, corresponding to the so-called *ordinary case*:

(H2): $\hat{a}_d(0)$ does not vanish modulo p.

Under **(H2)**, $\tilde{b}_0(n) = \hat{a}_d(0)$ is invertible in W and there is no obstruction to unrolling the recurrence (12). Let us be more precise. We recall that we want to compute the values of g_{r+pj} for j up to $2dh$. Clearly g_n is the reduction modulo p of $\frac{\tilde{g}_n}{n!}$. In order to get g_{r+pj}, we need to compute $\tilde{g}_{r+pj}$ modulo p^{v+1} where v is the p-adic valuation of $(r + 2dhp)!$. Under our assumption that p is large enough compared to d and h, we get $v = 2dh$. We will then work over the finite ring $W' = W/p^{2dh+1}W$.

We first compute the r first coefficients of $\hat{f}$ modulo p^{2dh+1} by solving the equation $\hat{E}(t, \hat{f}) = 0$ (using a Newton iteration for example). Since $r \in \text{poly}(dh)$, this computation can be achieved for a cost of poly(dh) operations in W', that is poly$(dh)\tilde{O}(s \log p)$ bit operations. We then build the companion matrix:

$$M(n) = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \frac{-\tilde{b}_r(n)}{\hat{a}_d(0)} & \frac{-\tilde{b}_{r-1}(n)}{\hat{a}_d(0)} & \cdots & \frac{-\tilde{b}_1(n)}{\hat{a}_d(0)} \end{pmatrix} \in (W'[n])^{r \times r}.$$

Obviously,

$$\begin{pmatrix} \tilde{g}_{n-r+1} & \tilde{g}_{n-r+2} & \cdots & \tilde{g}_n \end{pmatrix}^T = M(n) \cdot M(n-1) \cdots M(r) \cdot \begin{pmatrix} \tilde{g}_0 & \tilde{g}_1 & \cdots & \tilde{g}_{r-1} \end{pmatrix}^T,$$

and computing $\tilde{g}_n$ reduces to evaluating the matrix factorial $M(n) \cdot M(n-1) \cdots M(r)$. Using [9], the latter can be computed within poly$(dh)\tilde{O}(\sqrt{n})$ operations in W', that is poly$(dh)\tilde{O}(\sqrt{n} \cdot s \log p)$ bit operations. All in all, we find that the g_{r+pj}'s $(0 \leq j < 2dh)$ can all be computed for a cost of poly$(dh)\tilde{O}(s\sqrt{p})$ bit operations.

Plugging this input in Algorithm 1, we end up with an algorithm of bit complexity poly$(dh)\tilde{O}(s\sqrt{p}) \log N$. Theorem 4.1 is thus proved under the extra assumptions **(H1)** and **(H2)**.

4.3. **Reduction to the ordinary case.** We finally explain how **(H1)** and **(H2)** can be relaxed. The rough idea is to translate the origin at some point where these two hypotheses hold simultaneously.

The case of complete vanishing. Before proceeding, we need to deal with the case where the whole polynomial $\hat{a}_d$ vanishes modulo p. This case is actually very special; this is shown by the next lemma, whose proof relies on the fact that for a generic g, the minimal-order (homogeneous) linear differential equation over $k(t)$ satisfied by g has order exactly d [8].

Lemma 4.2. *For a generic $g \in L = k(t)[y]/E(t, y)$, the reduction of $\hat{a}_d$ modulo p does not vanish.*

We say that an element $g \in L$ is *good* if the corresponding $\hat{a}_d$ does not vanish modulo p. Lemma 4.2 ensures that goodness holds generically. It then holds with high probability since we have assumed that the ground field k has a large cardinality.

Consequently, even if we were unlucky and g was not good, we can produce with high probability a decomposition $g = g_1 + g_2$ where g_1 and g_2 are both good (just by sampling g_1 at random). Since moreover the section S_r is additive, we can recover $\mathsf{S}_r(g)$ as $\mathsf{S}_r(g_1) + \mathsf{S}_r(g_2)$.

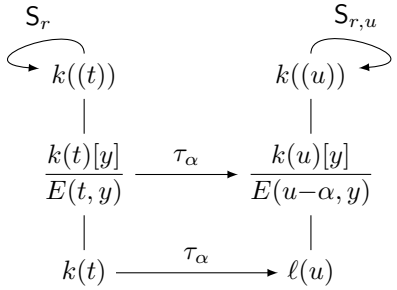
For this reason, in what follows we will assume safely that g is good.

Change of origin. Let $\hat{\alpha} \in W$ be such that $\hat{L}(\hat{\alpha}) \not\equiv 0 \pmod p$, $\hat{R}(\hat{\alpha}) \not\equiv 0 \pmod p$, $\hat{a}_d(\hat{\alpha}) \not\equiv 0 \pmod p$. Such an element exists (since k is assumed to be large) and can be found for a cost of $\mathrm{poly}(dh)$ operations in k (e.g., by enumerating its elements).

We denote by $\alpha \in k$ the reduction of $\hat{\alpha}$ modulo p and assume that $\alpha \neq 0$ (otherwise, we are in the ordinary case). We perform the change of variable $\tau_\alpha : t \mapsto u+\alpha$. Note that τ_α induces isomorphisms $k(t) \to k(u)$ and $k(t)[y]/E(t,y) \to k(u)[y]/E(u-\alpha, y)$. Furthermore, the polynomial $E(\alpha, y) = 0$ has d simple roots in an algebraic closure of k. Let $f_{\alpha,0}$ be one of them. By construction, $f_{\alpha,0}$ lies in a finite extension ℓ of k of degree at most d. Moreover, by Hensel's Lemma, $f_{\alpha,0}$ lifts uniquely to a solution:

$$f_\alpha = f_{\alpha,0} + f_{\alpha,1}u + \cdots + f_{\alpha,i}u^i + \cdots \in \ell[[u]]$$

to the equation $E(u-\alpha, y) = 0$. We emphasize that the morphism $k(t)[y]/E(t,y) \to k(u)[y]/E(u-\alpha,y)$ does *not* extend to a mapping $k((t)) \to \ell((u))$ sending f to f_α. The next diagram summarizes the previous discussion:



Here S_r and $\mathsf{S}_{r,u}$ refer to the section operators defined in the usual way. We observe that they stabilize the subfields $\frac{k(t)[y]}{E(t,y)}$ and $\frac{k(u)[y]}{E(u+\alpha,y)}$, respectively, since they can alternatively be defined by the relations:

$$\begin{aligned} &\text{over } \tfrac{k(t)[y]}{E(t,y)}: && \mathsf{F}^{-1} = \textstyle\sum_{r=0}^{p-1} t^{r/p}\,\mathsf{S}_r \\ &\text{over } \tfrac{k(u)[y]}{E(u-\alpha,y)}: && \mathsf{F}^{-1} = \textstyle\sum_{r=0}^{p-1} u^{r/p}\,\mathsf{S}_{r,u} \end{aligned} \tag{13}$$

where F is the Frobenius map (see also Eq. (4)).

Proposition 4.3. *The commutation* $\mathsf{S}_{p-1,u} \circ \tau_\alpha = \tau_\alpha \circ \mathsf{S}_{p-1}$ *holds over* $\frac{k(t)[y]}{E(t,y)}$.

Proof. Clearly τ_α commutes with the Frobenius because it is a ring homomorphism. From the relations (13), we then derive $\sum_{r=0}^{p-1} u^{r/p}\,\mathsf{S}_{r,u} \circ \tau_\alpha = \sum_{r=0}^{p-1} (u+\alpha)^{r/p}\,\tau_\alpha \circ \mathsf{S}_r$. Identifying the coefficients in $u^{\frac{p-1}{p}}$, we get the announced result. □

We emphasize that the other section operators $\mathsf{S}_{r,\star}$ (with $r < p-1$) *do not commute* with τ_α: the above phenomenon is specific to the index $p-1$. However, we can relate S_r and $\mathsf{S}_{p-1,u}$ as follows.

Corollary 4.4. *For all* $g \in \frac{k(t)[y]}{E(t,y)}$, *we have* $\mathsf{S}_r(g) = \tau_\alpha^{-1} \circ \mathsf{S}_{p-1,u} \circ \tau_\alpha(t^{p-1-r} g)$.

Proof. This follows from Proposition 4.3 and from $\mathsf{S}_r(g) = \mathsf{S}_{p-1}(t^{p-1-r} g)$. □

A modified recurrence. In order to use Corollary 4.4, we need to check that $\tau_\alpha(t^{p-1-r}g)$ fits the ordinary case. Recall the differential equation satisfied by $\hat{g}$,

$$\hat{a}_d\frac{\partial^d\hat{g}}{\partial t^d}+\hat{a}_{d-1}\frac{\partial^{d-1}\hat{g}}{\partial t^{d-1}}+\cdots+\hat{a}_1\frac{\partial\hat{g}}{\partial t}+\hat{a}_0\hat{g}=0.$$

We set $r'=p-1-r$ and $\hat{G}=t^{r'}\hat{g}$. Applying Leibniz formula to $\hat{g}=t^{-r'}\hat{G}$, we get:

$$\frac{\partial^j\hat{g}}{\partial t^j}=\sum_{i=0}^{j}(-1)^i\binom{j}{i}r'(r'+1)\cdots(r'+i-1)t^{-r'-i}\frac{\partial^j\hat{G}}{\partial t^{j-i}},$$

from which we derive the following differential equation satisfied by $\hat{G}$:

$$\sum_{0\le i\le j\le d}(-1)^i\hat{a}_j\binom{j}{i}r'(r'+1)\cdots(r'+i-1)t^{-r'-i}\frac{\partial^{j-i}\hat{G}}{\partial t^{j-i}}.$$

Reorganizing the terms and multiplying by $t^{r'+d}$, we end up with:

$$\sum_{j=0}^{d}\sum_{i=0}^{d-j}(-1)^i\hat{a}_{i+j}\binom{i+j}{i}r'(r'+1)\cdots(r'+i-1)t^{d-i}\frac{\partial^j\hat{G}}{\partial t^j}. \tag{14}$$

Set $W_{L,u}=W[u,y]/\hat{E}(u+\alpha,y)$ and define the ring homomorphism $\tau_{\hat{\alpha}}:W_L\to W_{L,u}$, $t\mapsto u+\hat{\alpha}$, $y\mapsto y$. Clearly $\tau_{\hat{\alpha}}$ lifts τ_α. Applying $\tau_{\hat{\alpha}}$ to Eq. (14) and noticing that $\frac{\partial}{\partial t}=\frac{\partial}{\partial u}$, we obtain:

$$\sum_{j=0}^{d}\sum_{i=0}^{d-j}(-1)^i\hat{\tau}_{\hat{\alpha}}(a_{i+j})\binom{i+j}{i}r'(r'+1)\cdots(r'+i-1)(u+\hat{\alpha})^{d-i}\frac{\partial^j\tau_{\hat{\alpha}}(\hat{G})}{\partial u^j}.$$

Conclusion. The leading term of the latest differential equation (obtained only with $j=d$ and $i=0$) is $\tau_{\hat{\alpha}}(\hat{a}_d)\,(u+\hat{\alpha})^d$. Its value at $u=0$ is then $\hat{a}_d(\hat{\alpha})\,\hat{\alpha}^d$, which is not congruent to 0 modulo p by assumption. Moreover the other coefficients are polynomials in u whose degrees stay within $\mathrm{poly}(dh)$. Therefore, we can apply the techniques of §4.2 and compute $\mathsf{S}_{p-1,u}(\tau_\alpha G)$ at precision $O(u^{2dh})$ for a cost of $\mathrm{poly}(dh)\tilde{O}(s\sqrt{p})$ bit operations. As explained in §3.2, we can reconstruct $\mathsf{S}_{p-1,u}(\tau_\alpha G)$ as an element of $k[u,y]/E(u+\alpha,y)$ for a cost of $\mathrm{poly}(dh)$ operations in k using Hermite–Padé approximations. Thanks to Corollary 4.4, it now just remains to apply τ_α^{-1} to get $\mathsf{S}_r(g)$. This last operation can be performed for a cost of $\mathrm{poly}(dh)$ operations in k as well. All in all, we are able to compute $\mathsf{S}_r(g)$ for a total bit complexity of $\mathrm{poly}(dh)\tilde{O}(s\sqrt{p})$. Repeating this process $\log N$ times, we obtain the complexity announced in Theorem 4.1.

References

[1] J.-P. Allouche and J. Shallit. The ring of k-regular sequences. *Theoret. Comput. Sci.*, 98(2):163–197, 1992.

[2] A. Bostan, G. Christol, and P. Dumas. Fast computation of the Nth term of an algebraic series over a finite prime field. In *ISSAC'16*, pages 119–126. ACM, 2016.

[3] A. Bostan, P. Gaudry, and É. Schost. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. *SIAM Journal on Computing*, 36(6):1777–1806, 2007.

[4] A. Bostan, C.-P. Jeannerod, and E. Schost. Solving structured linear systems with large displacement rank. *Theoret. Comput. Sci.*, 407(1-3):155–181, 2008.

[5] A. Bridy. Automatic sequences and curves over finite fields. *Algebra & Number Theory*, 11(3):685–712, 2017.

[6] G. Christol. Ensembles presque periodiques k-reconnaissables. *Theoret. Comput. Sci.*, 9(1):141–145, 1979.
[7] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France*, 108(4):401–419, 1980.
[8] D. V. Chudnovsky and G. V. Chudnovsky. On expansion of algebraic functions in power and Puiseux series. I. *J. Complexity*, 2(4):271–294, 1986.
[9] D. V. Chudnovsky and G. V. Chudnovsky. Approximations and complex multiplication according to Ramanujan. In *Ramanujan revisited (Urbana-Champaign, 1987)*, pages 375–472. 1988.
[10] D. V. Chudnovsky and G. V. Chudnovsky. Computer algebra in the service of mathematical physics and number theory. In *Computers in mathematics (Stanford, 1986)*, volume 125 of *Lecture Notes in Pure and Appl. Math.*, pages 109–232. 1990.
[11] P. Deligne. Intégration sur un cycle évanescent. *Invent. Math.*, 76(1):129–143, 1984.
[12] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, 1995.
[13] C. M. Fiduccia, An efficient formula for linear recurrences. *SIAM J. Comput.*, 14(1):106–112, 1985.
[14] H. Furstenberg. Algebraic functions over finite fields. *J. Algebra*, 7:271–277, 1967.
[15] T. Harase. Algebraic elements in formal power series rings. *Israel J. Math.*, 63(3):281–288, 1988.
[16] H. T. Kung and J. F. Traub. All algebraic functions can be computed fast. *J. Assoc. Comput. Mach.*, 25(2):245–260, 1978.
[17] V. Y. Pan. *Structured matrices and polynomials*. Birkhäuser Boston, Inc., Boston, MA; Springer-Verlag, New York, 2001. Unified superfast algorithms.
[18] D. Speyer. Christol's theorem and the Cartier operator. Blog post, 11 Feb 2010, Secret Blogging Seminar, `https://sbseminar.wordpress.com/2010/02/11/`.

Inria, France
E-mail address: `alin.bostan@inria.fr`

CNRS, France
E-mail address: `xavier.caruso@normalesup.org`

IMJ, France
E-mail address: `christol.gilles@gmail.com`

Inria, France
E-mail address: `philippe.dumas@inria.fr`

FASTER INTEGER MULTIPLICATION USING SHORT LATTICE VECTORS

DAVID HARVEY AND JORIS VAN DER HOEVEN

ABSTRACT. We prove that n-bit integers may be multiplied in $O(n \log n\, 4^{\log^* n})$ bit operations. This complexity bound had been achieved previously by several authors, assuming various unproved number-theoretic hypotheses. Our proof is unconditional and is based on a new representation for integers modulo a fixed modulus, which we call the θ-representation. The existence of such representations is ensured by Minkowski's theorem concerning lattice vectors in symmetric convex sets.

1. INTRODUCTION

Let $\mathsf{M}(n)$ denote the number of bit operations required to multiply two n-bit integers, where "bit operations" means the number of steps on a deterministic Turing machine with a fixed, finite number of tapes [21] (our results also hold in the Boolean circuit model). Let $\log^* x$ denote the iterated natural logarithm, i.e., $\log^* x := \min\{j \in \mathbb{N} : \log^{\circ j} x \leqslant 1\}$, where $\log^{\circ j} x := \log \cdots \log x$ (iterated j times). The main result of this paper is an algorithm achieving the following bound.

Theorem 1.1. *We have* $\mathsf{M}(n) = O(n \log n\, 4^{\log^* n})$.

The first complexity bound for $\mathsf{M}(n)$ of the form $O(n \log n\, K^{\log^* n})$ was established by Fürer [8, 9], for an unspecified constant $K > 1$. His algorithm reduces a multiplication of size n to many multiplications of size exponentially smaller than n, which are then handled recursively. The number of recursion levels is $\log^* n + O(1)$, and the constant K measures the "expansion factor" at each recursion level.

The first explicit value for K, namely $K = 8$, was given by Harvey, van der Hoeven and Lecerf [14]. Their method is somewhat different to Fürer, but still carries out an exponential size reduction at each recursion level. One may think of the constant $K = 8$ as being built up of three factors of 2, each coming from a different source.

The first factor of 2 arises from the need to perform both forward and inverse DFTs (discrete Fourier transforms) at each recursion level. This is a feature common to all of the post-Fürer algorithms, suggesting that significantly new ideas will be needed to do any better than $O(n \log n\, 2^{\log^* n})$.

The second factor of 2 arises from coefficient growth: a product of polynomials with k-bit integer coefficients has coefficients with at least $2k$ bits. This factor of 2 also seems difficult to completely eliminate, although Harvey and van der Hoeven have recently made some progress [13]: they achieve $K = 4\sqrt{2} \approx 5.66$ by arranging

Harvey was supported by the Australian Research Council (grants DP150101689 and FT160100219).

20 Jun 2018 14:52:56 PDT
Version 3 - Submitted to Open Book Series

that, in effect, the coefficient growth only occurs at every second recursion level. This was the best known unconditional value of K prior to the present paper[1].

The final factor of 2 occurs because the algorithm works over $\mathbb{C}$: when multiplying complex coefficients with say β significant bits, the algorithm first computes a full 2β-bit product, and then truncates to β bits. More precisely, after splitting the β-bit inputs into m exponentially smaller chunks, and encoding them into polynomials of degree m, the algorithm must compute the full product of degree $2m$, even though essentially only m coefficients are needed to resolve β significant bits of the product. Again, this factor of 2 has been the subject of a recent attack: Harvey has shown [10] that it is possible to work modulo a polynomial of degree only m, at the expense of increasing the working precision by a factor of $3/2$. This leads to an integer multiplication algorithm achieving $K = 6$.

Another way of attacking this last factor of 2 is to replace the coefficient ring $\mathbb{C}$ by a finite ring $\mathbb{Z}/q\mathbb{Z}$ for a suitable integer q. A Fürer-type complexity bound (with no attempt to optimise the value of K) was first obtained using this approach in [7]. By choosing q with some special structure, it may become possible to convert a multiplication modulo q directly into a polynomial multiplication modulo some polynomial of degree m, rather than $2m$. Three algorithms along these lines have been proposed.

First, Harvey, van der Hoeven and Lecerf suggested using *Mersenne primes*, i.e., primes of the form $q = 2^k - 1$, where k is itself prime [14, §9]. They convert multiplication in $\mathbb{Z}/q\mathbb{Z}$ to multiplication in $\mathbb{Z}[y]/(y^m - 1)$, where m is a power of two. Because k is not divisible by m, the process of splitting an element of $\mathbb{Z}/q\mathbb{Z}$ into m chunks is somewhat involved, and depends on a variant of the Crandall–Fagin algorithm [6].

Covanov and Thomé [5] later proposed using *generalised Fermat primes*, i.e., primes of the form $q = r^m + 1$, where m is a power of two and r is a small even integer. Here, multiplication in $\mathbb{Z}/q\mathbb{Z}$ is converted to multiplication in $\mathbb{Z}[y]/(y^m + 1)$. The splitting procedure consists of rewriting an element of $\mathbb{Z}/q\mathbb{Z}$ in base r, via fast radix-conversion algorithms.

Finally, Harvey and van der Hoeven [12] proposed using *FFT primes*, i.e., primes of the form $q = a \cdot 2^k + 1$, where a is small. They reduce multiplication in $\mathbb{Z}/q\mathbb{Z}$ to multiplication in $\mathbb{Z}[y]/(y^m + a)$ via a straightforward splitting of the integers into m chunks, where m is a power of two. Here the splitting process is trivial, as k may be chosen to be divisible by m.

These three algorithms all achieve $K = 4$, subject to plausible but unproved conjectures on the distribution of the relevant primes. Unfortunately, in all three cases, it is not even known that there are infinitely many primes of the required form, let alone that there exist a sufficiently high density of them to satisfy the requirements of the algorithm.

The main technical novelty of the present paper is a splitting procedure that works for an almost *arbitrary* modulus q. The core idea is to introduce an alternative representation for elements of $\mathbb{Z}/q\mathbb{Z}$: we represent them as expressions

[1]The main feature that the preprint [13] has in common with the present paper is that it inherits the overall algorithm structure (decompose into exponentially smaller DFTs and apply Bluestein's trick) from [14]. The main novelty of the present paper (use of θ-representations and short lattice vectors) does not appear in [13]. Besides integer multiplication, it is noteworthy to mention that [13] proves an analogous complexity bound for polynomial multiplication over finite fields, again with $K = 4$.

20 Jun 2018 14:52:56 PDT
Version 3 - Submitted to Open Book Series

$a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1}$, where θ is some fixed $2m$-th root of unity in $\mathbb{Z}/q\mathbb{Z}$, and where the a_i are small integers, of size roughly $q^{1/m}$. Essentially the only restriction on q is that $\mathbb{Z}/q\mathbb{Z}$ must contain an appropriate $2m$-th root of unity. We will see that Linnik's theorem is strong enough to construct suitable such moduli q.

In Section 2 we show that the cost of multiplication in this representation is only a constant factor worse than for the usual representation. The key ingredient is Minkowski's theorem on lattice vectors in symmetric convex sets. We also give algorithms for converting between this representation and the standard representation. The conversions are not as fast as one might hope — in particular, we do not know how to carry them out in quasilinear time — but surprisingly this turns out not to affect the overall complexity, because in the main multiplication algorithm we perform the conversions only infrequently.

Then in Sections 3 and 4 we prove Theorem 1.1, using an algorithm that is structurally very similar to [12]. We make no attempt to minimise the implied big-O constant in Theorem 1.1; our goal is to give the simplest possible proof of the asymptotic bound, without any regard for questions of practicality.

An interesting question is whether it is possible to combine the techniques of the present paper with those of [13] to obtain an algorithm achieving $K = 2\sqrt{2} \approx 2.83$. Our attempts in this direction have so far been unsuccessful. One might also ask if the techniques of this paper can be transferred to the case of multiplication of polynomials of high degree in $\mathbb{F}_p[x]$. However, this is not so interesting, because an unconditional proof of the bound corresponding to $K = 4$ in the polynomial case is already known [13]. One may finally wonder whether any algorithms along these lines may be useful for practical purposes. We refer to [18, 11, 15] for some recent work on this theme.

Throughout the paper we use the following notation. We write $\lg n := \lceil \log_2 n \rceil$ for $n \geqslant 2$, and for convenience put $\lg 1 := 1$. We define $\mathsf{M}_{\mathrm{SS}}(n) = Cn \lg n \lg\lg n$, where $C > 0$ is some constant so that the Schönhage–Strassen algorithm multiplies n-bit integers in at most $\mathsf{M}_{\mathrm{SS}}(n)$ bit operations [23]. This function satisfies $n\,\mathsf{M}_{\mathrm{SS}}(m) \leqslant \mathsf{M}_{\mathrm{SS}}(nm)$ for any $n, m \geqslant 1$, and also $\mathsf{M}_{\mathrm{SS}}(dm) = O(\mathsf{M}_{\mathrm{SS}}(m))$ for fixed d. An n-bit integer may be divided by an m-bit integer, producing quotient and remainder, in time $O(\mathsf{M}_{\mathrm{SS}}(\max(n, m)))$ [24, Ch. 9]. We may transpose an $n \times m$ array of objects of bit size b in $O(bnm \lg \min(n, m))$ bit operations [3, Appendix]. Finally, we occasionally use Xylouris's refinement of Linnik's theorem [25], which states that for any relatively prime positive integers a and n, the least prime in the arithmetic progression $p = a \pmod n$ satisfies $p = O(n^{5.2})$.

Acknowledgments. We wish to express our gratitude to the referees for their careful reading and their useful comments and suggestions.

2. θ-representations

In this section, fix an integer $q \geqslant 2$ and a power of two $m \geqslant 2$ such that

$$m \leqslant \frac{\log_2 q}{(\lg\lg q)^2}, \qquad \text{or equivalently,} \qquad q^{1/m} \geqslant 2^{(\lg\lg q)^2}, \tag{2.1}$$

and such that we are in addition given some $\theta \in \mathbb{Z}/q\mathbb{Z}$ with $\theta^m = -1$. (In Section 3, we will ensure that q and m are chosen so that a suitable θ exists.)

For a polynomial $F = F_0 + F_1 y + \cdots + F_{m-1} y^{m-1} \in \mathbb{Z}[y]/(y^m + 1)$, define $\|F\| := \max_i |F_i|$. This norm satisfies $\|FG\| \leqslant m\|F\|\|G\|$ for any $F, G \in \mathbb{Z}[y]/(y^m + 1)$.

Definition 2.1. Let $u \in \mathbb{Z}/q\mathbb{Z}$. A *$\theta$-representation for u* is a polynomial $U \in \mathbb{Z}[y]/(y^m + 1)$ such that $U(\theta) = u \pmod q$ and $\|U\| \leqslant mq^{1/m}$.

Example 2.2. Let $m = 4$ and

$$\begin{aligned} q &= 31415926535897932384628 33, \\ \theta &= 25425334315669044509227 35 \pmod q, \\ u &= 27182818284590452353602 88 \pmod q. \end{aligned}$$

(For reasons of legibility, the choice of q in this running example is somewhat smaller than what is required by (2.1).) The coefficients in a θ-representation must not exceed $mq^{1/m} \approx 5325341.46$. Two examples of θ-representations for u are

$$\begin{aligned} U(y) &= 3366162y^3 + 951670y^2 - 5013490y - 3202352, \\ U(y) &= -4133936y^3 + 1849981y^2 - 5192184y + 1317423. \end{aligned}$$

By (2.1), the number of bits required to store $U(y)$ is at most

$$m\big(\log_2(mq^{1/m}) + O(1)\big) = \lg q + O(m \lg m) = \left(1 + \frac{O(1)}{\lg \lg q}\right) \lg q,$$

so a θ-representation incurs very little overhead in space compared to the standard representation by an integer in the interval $0 \leqslant x < q$.

Our main tool for working with θ-representations is the *reduction algorithm* stated in Lemma 2.9 below. Given a polynomial $F \in \mathbb{Z}[y]/(y^m + 1)$, whose coefficients are up to about twice as large as allowed in a θ-representation, the reduction algorithm computes a θ-representation for $F(\theta)$ (up to a certain scaling factor, discussed further below). The basic idea of the algorithm is to precompute a nonzero polynomial $P(y)$ such that $P(\theta) = 0 \pmod q$, and then to subtract an appropriate multiple of $P(y)$ from $F(y)$ to make the coefficients small.

After developing the reduction algorithm, we are able to give algorithms for basic arithmetic on elements of $\mathbb{Z}/q\mathbb{Z}$ given in θ-representation (Proposition 2.15), a more general reduction algorithm for inputs of arbitrary size (Proposition 2.17), and algorithms for converting between standard and θ-representation (Proposition 2.18 and Proposition 2.21).

We begin with two results that generate certain precomputed data necessary for the main reduction step.

Lemma 2.3. *In $q^{1+o(1)}$ bit operations, we may compute a nonzero polynomial $P \in \mathbb{Z}[y]/(y^m + 1)$ such that $P(\theta) = 0 \pmod q$ and $\|P\| \leqslant q^{1/m}$.*

Proof. We first establish existence of a suitable $P(y)$. Let $\overline{\theta^i}$ denote a lift of θ^i to $\mathbb{Z}$, and consider the lattice $\Lambda \subset \mathbb{Z}^m$ spanned by the rows of the $m \times m$ integer matrix

$$A = \begin{pmatrix} q & 0 & 0 & & 0 \\ -\overline{\theta} & 1 & 0 & \cdots & 0 \\ -\overline{\theta^2} & 0 & 1 & & 0 \\ \vdots & & & \ddots & \\ -\overline{\theta^{m-1}} & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Every vector $(a_0, \ldots, a_{m-1}) \in \Lambda$ satisfies the equation $a_0 + \cdots + a_{m-1}\theta^{m-1} = 0 \pmod q$. The volume of the fundamental domain of Λ is $\det A = q$. The volume of

the closed convex symmetric set

$$\Sigma := \{(x_1, \ldots, x_m) \in \mathbb{R}^m : |x_1|, \ldots, |x_m| \leqslant q^{1/m}\}$$

is $(2q^{1/m})^m = 2^m q$, so by Minkowski's theorem (see for example [16, Ch. V, Thm. 3]), there exists a nonzero vector $(a_0, \ldots, a_{m-1})$ in $\Lambda \cap \Sigma$. The corresponding polynomial $P(y) := a_0 + \cdots + a_{m-1}y^{m-1}$ then has the desired properties.

To actually compute $P(y)$, we simply perform a brute-force search. By (2.1) there are at most $(2q^{1/m} + 1)^m \leqslant (3q^{1/m})^m = 3^m q < q^{1+o(1)}$ candidates to test. Enumerating them in lexicographical order, we can easily evaluate $P(\theta) \pmod q$ in an average of $O(\lg q)$ bit operations per candidate. □

Example 2.4. Continuing Example 2.2, the coefficients of $P(y)$ must not exceed $q^{1/m} \approx 1331335.36$. A suitable polynomial $P(y)$ is given by

$$P(y) = -394297y^3 - 927319y^2 + 1136523y - 292956.$$

Remark 2.5. The computation of $P(y)$ is closely related to the problem of finding an element of small norm in the ideal of the ring $\mathbb{Z}[\zeta_{2m}]$ generated by q and $\zeta_{2m} - \overline{\theta}$, where ζ_{2m} denotes a primitive $2m$-th root of unity.

Remark 2.6. The poor exponential-time complexity of Lemma 2.3 can probably be improved, by taking advantage of more sophisticated lattice reduction or shortest vector algorithms, but we were not easily able to extract a suitable result from the literature. For example, LLL is not guaranteed to produce a short enough vector [17], and the Micciancio–Voulgaris exact shortest vector algorithm [19] solves the problem for the Euclidean norm rather than the uniform norm. In any case, this has no effect on our main result.

Lemma 2.7. *Assume that $P(y)$ has been precomputed as in Lemma 2.3. Let r be the smallest prime exceeding $2m^2q^{1/m}$ such that $r \nmid q$ and such that $P(y)$ is invertible in $(\mathbb{Z}/r\mathbb{Z})[y]/(y^m+1)$. Then $r = O(m^2q^{1/m})$, and in $q^{1+o(1)}$ bit operations we may compute r and a polynomial $J \in \mathbb{Z}[y]/(y^m + 1)$ such that $J(y)P(y) = 1 \pmod r$ and $\|J\| \leqslant r$.*

Proof. Let $R \in \mathbb{Z}$ be the resultant of $P(y)$ (regarded as a polynomial in $\mathbb{Z}[y]$) and $y^m + 1$. The primes r dividing R are exactly the primes for which $P(y)$ fails to be invertible in $(\mathbb{Z}/r\mathbb{Z})[y]/(y^m+1)$. Therefore our goal is to find a prime $r > 2m^2q^{1/m}$ such that $r \nmid Rq$.

Since m is a power of two, y^m+1 is a cyclotomic polynomial and hence irreducible in $\mathbb{Q}[y]$. Thus y^m+1 and $P(y)$ have no common factor, and so $R \neq 0$. Also, we have $R = \prod_\alpha P(\alpha)$ where α runs over the complex roots of $y^m + 1$. These roots all lie on the unit circle, so $|P(\alpha)| \leqslant m\|P\| \leqslant mq^{1/m}$. From (2.1) we obtain $m \log_2 m < (\log_2 q/(\lg\lg q)^2) \log_2 \log_2 q \leqslant \log_2 q$ and so $|Rq| \leqslant (mq^{1/m})^m q = m^m q^2 < q^3$.

On the other hand, let $\vartheta(x) := \sum_{p \leqslant x} \log p$ (sum taken over primes) be the standard Chebyshev function. Combining Theorems 9, 10 and 18 of [22], one deduces the explicit estimate $x/4 < \vartheta(x) < 2x$ for all $x \geqslant 8$. Therefore

$$\sum_{2x < p \leqslant 20x} \log_2 p = \frac{1}{\log 2}(\vartheta(20x) - \vartheta(2x)) > x, \qquad x \geqslant 4.$$

Taking $x := m^2q^{1/m} \geqslant 4$, again by (2.1) we get

$$\sum_{2m^2q^{1/m} < p \leqslant 20m^2q^{1/m}} \log_2 p > m^2q^{1/m} > 3 \cdot 2^{(\lg\lg q)^2} \geqslant 3 \lg q \geqslant \log_2(q^3).$$

In particular, there must be at least one prime in the interval $2m^2q^{1/m} \leqslant r \leqslant 20m^2q^{1/m}$ that does not divide Rq.

To find the smallest such r, we first make a list of all primes up to $20m^2q^{1/m}$ in $(m^2q^{1/m})^{1+o(1)} < q^{1+o(1)}$ bit operations. Then for each prime r between $2m^2q^{1/m}$ and $20m^2q^{1/m}$, we check whether r divides q in $(\lg q)^{1+o(1)}$ bit operations, and attempt to invert $P(y)$ in $(\mathbb{Z}/r\mathbb{Z})[y]/(y^m+1)$ in $(m \lg r)^{1+o(1)} = (\lg q)^{1+o(1)}$ bit operations [24, Ch. 11]. □

Example 2.8. Continuing Example 2.2, we have $r = 42602761$ and

$$J(y) = 17106162y^3 + 6504907y^2 + 30962874y + 8514380.$$

Now we come to the main step of the reduction algorithm, which is inspired by Montgomery's method for modular reduction [20].

Lemma 2.9. *Assume that $P(y)$, r and $J(y)$ have been precomputed as in Lemmas 2.3 and 2.7. Given as input $F \in \mathbb{Z}[y]/(y^m+1)$ with $\|F\| \leqslant m^3(q^{1/m})^2$, we may compute a θ-representation for $F(\theta)/r \pmod q$ in $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations.*

Proof. We first compute the "quotient" $Q := FJ \pmod r$, normalised so that $\|Q\| \leqslant r/2$. This is done by means of Kronecker substitution [24, Ch. 8], i.e., we pack the polynomials $F(y)$ and $J(y)$ into integers, multiply the integers, unpack the result, and reduce the result modulo y^m+1 and modulo r. The packed integers have at most $m(\lg \|F\| + \lg r + \lg m)$ bits, where the $\lg m$ term accounts for coefficient growth in $\mathbb{Z}[y]$. By (2.1) and Lemma 2.7, this simplifies to $O(\lg q)$ bits, so the integer multiplication step costs $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations. This bound also covers the cost of the reductions modulo r.

Next we compute the product QP, again using Kronecker substitution, at a cost of $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations. Since $\|Q\| \leqslant r/2$ and $\|P\| \leqslant q^{1/m}$, we have $\|QP\| \leqslant \frac{1}{2}rmq^{1/m}$.

By construction of J we have $QP = F \pmod r$. In particular, all the coefficients of $F - QP \in \mathbb{Z}[y]/(y^m+1)$ are divisible by r. The last step is to compute the "remainder" $G := (F - QP)/r$; again, this step costs $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations. Since $r \geqslant 2m^2q^{1/m}$, we have

$$\|G\| \leqslant \frac{\|F\|}{r} + \frac{\|QP\|}{r} \leqslant \frac{m^3(q^{1/m})^2}{2m^2q^{1/m}} + \frac{mq^{1/m}}{2} \leqslant mq^{1/m}.$$

Finally, since $P(\theta) = 0 \pmod q$, and all arithmetic throughout the algorithm has been performed modulo y^m+1, we see that $G(\theta) = F(\theta)/r \pmod q$. □

Using the above reduction algorithm, we may give preliminary addition and multiplication algorithms for elements of $\mathbb{Z}/q\mathbb{Z}$ in θ-representation.

Lemma 2.10. *Assume that $P(y)$, r and $J(y)$ have been precomputed as in Lemmas 2.3 and 2.7. Given as input θ-representations for $u, v \in \mathbb{Z}/q\mathbb{Z}$, we may compute θ-representations for uv/r and $(u \pm v)/r$ in $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations.*

Proof. Let the θ-representations be given by $U, V \in \mathbb{Z}[y]/(y^m+1)$. We may compute $F_* := UV$ in $\mathbb{Z}[y]/(y^m+1)$ using Kronecker substitution in $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations, and $F_\pm := U \pm V$ in $O(\lg q)$ bit operations. Note that $\|F_*\| \leqslant m\|U\|\|V\| \leqslant m^3(q^{1/m})^2$, and $\|F_\pm\| \leqslant \|U\| + \|V\| \leqslant 2mq^{1/m} \leqslant m^3(q^{1/m})^2$, so we may apply Lemma 2.9 to obtain the desired θ-representations. □

20 Jun 2018 14:52:56 PDT
Version 3 - Submitted to Open Book Series

Example 2.11. Continuing Example 2.2, we walk through an example of computing a product of elements in θ-representation. Let

$$u = 14142135623730950488801689 \pmod q,$$
$$v = 17320508075688772935274463 \pmod q.$$

Suppose we are given as input the θ-representations

$$U(y) = 3740635y^3 + 3692532y^2 - 3089740y + 4285386,$$
$$V(y) = 4629959y^3 - 4018180y^2 - 2839272y - 3075767.$$

We first compute the product of $U(y)$ and $V(y)$ modulo $y^m + 1$:

$$F(y) = U(y)V(y) = 10266868543625y^3 - 37123194804209y^2 - 4729783170300y + 26582459129078.$$

We multiply $F(y)$ by $J(y)$ and reduce modulo r to obtain the quotient

$$Q(y) = 3932274y^3 - 14729381y^2 + 20464841y - 11934644.$$

Then the remainder

$$(F(y) - P(y)Q(y))/r = 995963y^3 - 1814782y^2 + 398819y + 777998$$

is a θ-representation for $uv/r \pmod q$.

The following precomputation will assist in eliminating the spurious $1/r$ factor appearing in Lemmas 2.9 and 2.10.

Lemma 2.12. *Assume that $P(y)$, r and $J(y)$ have been precomputed as in Lemmas 2.3 and 2.7. In $q^{1+o(1)}$ bit operations, we may compute a polynomial $D \in \mathbb{Z}[y]/(y^m + 1)$ such that $\|D\| \leqslant mq^{1/m}$ and $D(\theta) = r^2 \pmod q$.*

Proof. We may easily compute the totient function $\varphi(q)$ in $q^{1+o(1)}$ bit operations, by first factoring q. Since $(r, q) = 1$, we have $r^{-(\varphi(q)-2)} = r^2 \pmod q$. Repeatedly using the identity $r^{-i-1} = (r^{-i} \cdot 1)/r$, we may compute θ-representations for $r^{-1}, r^{-2}, \ldots, r^{-(\varphi(q)-2)}$ by successively applying Lemma 2.10. Here we notice that we may use $U = 1$ as the θ-representation for 1. □

Remark 2.13. Assuming the factorisation of q is known (which will always be the case in the application in Section 3), the complexity of Lemma 2.12 may be improved to $O(\mathsf{M}_{\mathrm{SS}}(\lg q) \lg q)$ bit operations by using a modified "repeated squaring" algorithm.

Example 2.14. Continuing Example 2.2, we may take

$$D(y) = -1918607y^3 - 3680082y^2 + 2036309y - 270537.$$

Henceforth we write $\mathcal{P}(q, m, \theta)$ for the tuple $(P(y), r, J(y), D(y))$ of precomputed data generated by Lemmas 2.3, 2.7, and 2.12. Given q, m and θ as input, the above results show that we may compute $\mathcal{P}(q, m, \theta)$ in $q^{1+o(1)}$ bit operations. With these precomputations out of the way, we may state complexity bounds for the main operations on θ-representations.

Proposition 2.15. *Assume that $\mathcal{P}(q, m, \theta)$ has been precomputed. Given as input θ-representations for $u, v \in \mathbb{Z}/q\mathbb{Z}$, we may compute θ-representations for uv and $u \pm v$ in $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations.*

Proof. For the product, we first use Lemma 2.10 to compute a θ-representation for $uv/r \pmod q$, and then we use Lemma 2.10 again to multiply by $D(y)$, to obtain a θ-representation for $(uv/r)(r^2)/r = uv \pmod q$. The sum and difference are handled similarly. □

Remark 2.16. We suspect that the complexity bound for $u \pm v$ can be improved to $O(\lg q)$, but we do not currently know how to achieve this. This question seems closely related to Remark 2.23 below.

Proposition 2.17. *Assume that $\mathcal{P}(q, m, \theta)$ has been precomputed. Given as input a polynomial $F \in \mathbb{Z}[y]/(y^m + 1)$ (with no restriction on $\|F\|$), we may compute a θ-representation for $F(\theta) \pmod q$ in time $O(\lceil m \lg \|F\| / \lg q \rceil \, \mathsf{M}_{\mathrm{SS}}(\lg q))$.*

Proof. Let $b := \lg \lceil q^{1/m} \rceil$ and $n := \lceil 2m \lg \|F\| / \lg q \rceil$, so that

$$2^{nb} \geqslant (q^{1/m})^n \geqslant (q^{1/m})^{2m \lg \|F\| / \lg q} = 2^{\lg \|F\| (2 \log_2 q / \lg q)} \geqslant 2^{\lg \|F\|}.$$

We may therefore decompose the coefficients of F into n chunks of b bits, i.e., we may compute polynomials $F_0, \ldots, F_{n-1} \in \mathbb{Z}[y]/(y^m + 1)$ such that $F = F_0 + 2^b F_1 + \cdots + 2^{(n-1)b} F_{n-1}$ and $\|F_i\| \leqslant 2^b \leqslant 2q^{1/m}$. (This step implicitly requires an array transposition of cost $O(bmn \lg m) = O(n \lg q \lg \lg q)$.) Now we use Proposition 2.15 repeatedly to compute a θ-representation for F via Horner's rule, i.e., first we compute a θ-representation for $2^b F_{n-1} + F_{n-2}$, then for $2^b(2^b F_{n-1} + F_{n-2}) + F_{n-3}$, and so on. Here we notice that 2^b is already in θ-representation, since $2^b \leqslant 2q^{1/m} \leqslant mq^{1/m}$. □

Proposition 2.18. *Assume that $\mathcal{P}(q, m, \theta)$ has been precomputed. Given as input an element $u \in \mathbb{Z}/q\mathbb{Z}$ in standard representation, we may compute a θ-representation for u in $O(m \, \mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations.*

Proof. Simply apply Proposition 2.17 to the constant polynomial $F(y) = u$, noting that $\|F\| \leqslant q$. □

Corollary 2.19. *Every $u \in \mathbb{Z}/q\mathbb{Z}$ admits a θ-representation.*

Remark 2.20. It would be interesting to have a direct proof of the corollary that does not rely on the reduction algorithm. A related question is whether it is possible to tighten the bound in the definition of θ-representation from $mq^{1/m}$ to $q^{1/m}$. We do not know whether such a representation exists for all $u \in \mathbb{Z}/q\mathbb{Z}$.

Proposition 2.21. *Given as input an element $u \in \mathbb{Z}/q\mathbb{Z}$ in θ-representation, we may compute the standard representation for u in $O(m \, \mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations.*

Proof. Let $U \in \mathbb{Z}[y]/(y^m + 1)$ be the input polynomial. The problem amounts to evaluating $U(\theta)$ in $\mathbb{Z}/q\mathbb{Z}$. Again we may simply use Horner's rule. □

Remark 2.22. In both Proposition 2.18 and Proposition 2.21, the input and output have bit size $O(\lg q)$, but the complexity bounds given are not quasilinear in $\lg q$. It is possible to improve on the stated bounds, but we do not know a quasilinear time algorithm for the conversion in either direction.

Remark 2.23. In the reduction algorithm, the reader may wonder why we go to the trouble of introducing the auxiliary prime r. Why not simply precompute an approximation to a *real* inverse for $P(y)$, i.e., the inverse in $\mathbb{R}[y]/(y^m + 1)$, and use this to clear out the *high-order bits* of each coefficient of the dividend? In

other words, why not replace the Montgomery-style division with the more natural Barrett-style division [1]?

The reason is that we cannot prove tight enough bounds on the size of the coefficients of this inverse: it is conceivable that $P(y)$ might accidentally take on a very small value near one of the complex roots of $y^m + 1$, or equivalently, that the resultant R in the proof of Lemma 2.7 might be unusually small. For the same reason, we cannot use a more traditional 2-adic Montgomery inverse to clear out the low-order bits of the dividend, because again $P(y)$ may take a 2-adically small value near one of the 2-adic roots of $y^m + 1$, or equivalently, the resultant R might be divisible by an unusually large power of 2.

3. Integer multiplication: the recursive step

In this section we present a recursive routine Transform with the following interface. It takes as input a (sufficiently large) power-of-two transform length L, a prime $p = 1 \pmod{L}$, a prime power $q = p^\alpha$ such that

$$\lg L \leqslant \lg q \leqslant 3 \lg L \lg\lg L, \tag{3.1}$$

a principal L-th root of unity $\zeta \in \mathbb{Z}/q\mathbb{Z}$ (i.e., an L-th root of unity whose reduction modulo p is a primitive L-th root of unity in the field $\mathbb{Z}/p\mathbb{Z}$), certain precomputed data depending on L, q and ζ (see below), and a polynomial $F \in (\mathbb{Z}/q\mathbb{Z})[x]/(x^L - 1)$. Its output is the DFT of F with respect to ζ, that is, the vector

$$\hat{F} := (F(1), F(\zeta), \ldots, F(\zeta^{L-1})) \in (\mathbb{Z}/q\mathbb{Z})^L.$$

The coefficients of both F and $\hat{F}$ are given in standard representation.

The precomputed data consists of the tuple $\mathcal{P}(q, m, \theta)$ defined in Section 2, where m and θ are defined as follows.

First, (3.1) implies that $\lg q \geqslant 2(\lg\lg L)^2 \lg\lg\lg L$ for sufficiently large L, so we may take m to be the unique power of two lying in the interval

$$\frac{\lg q}{(\lg\lg L)^2 \lg\lg\lg L} \leqslant m < \frac{2 \lg q}{(\lg\lg L)^2 \lg\lg\lg L}. \tag{3.2}$$

Observe that (2.1) is certainly satisfied for this choice of m (for large enough L), as (3.1) implies that $\lg\lg L \sim \lg\lg q$.

Next, note that $2m \mid L$, because (3.1) and (3.2) imply that $m = o(\lg L) = o(L)$; therefore we may take $\theta := \zeta^{L/2m}$, so that $\theta^m = \zeta^{L/2} = -1$.

We remark that the role of the parameter α is to give us enough control over the bit size of q, to compensate for the fact that Linnik's theorem does not give us sufficiently fine control over the bit size of p (see Lemma 3.5).

Our implementation of Transform uses one of two algorithms, depending on the size of L. If L is below some threshold, say L_0, then it uses any convenient base-case algorithm. Above this threshold, it reduces the given DFT problem to a collection of exponentially smaller DFTs of the same type, via a series of reductions that may be summarised as follows.

(i) Use the conversion algorithms from Section 2 to reduce to a transform over $\mathbb{Z}/q\mathbb{Z}$ where the input and output coefficients are given in θ-representation. (During steps (ii) and (iii) below, all elements of $\mathbb{Z}/q\mathbb{Z}$ are stored and manipulated entirely in θ-representation.)

(ii) Reduce the "long" transform of length L over $\mathbb{Z}/q\mathbb{Z}$ to many "short" transforms of exponentially small length $S := 2^{(\lg\lg L)^2}$ over $\mathbb{Z}/q\mathbb{Z}$, via the Cooley–Tukey decomposition.
(iii) Reduce each short transform from step (ii) to a product in $(\mathbb{Z}/q\mathbb{Z})[x]/(x^S-1)$, i.e., a cyclic convolution of length S, using Bluestein's algorithm.
(iv) Use the definition of θ-representation to reinterpret each product from (iii) as a product in $\mathbb{Z}[x,y]/(x^S-1, y^m+1)$, where the coefficients in $\mathbb{Z}$ are exponentially smaller than the original coefficients in $\mathbb{Z}/q\mathbb{Z}$.
(v) Embed each product from (iv) into $(\mathbb{Z}/q'\mathbb{Z})[x,y]/(x^S-1, y^m+1)$ for a suitable prime power q' that is exponentially smaller than q, and large enough to resolve the coefficients of the products over $\mathbb{Z}$.
(vi) Reduce each product from (v) to a collection of forward and inverse DFTs of length S over $\mathbb{Z}/q'\mathbb{Z}$, and recurse.

The structure of this algorithm is very similar to that of [12]. The main difference is that it is not necessary to explicitly split the coefficients into chunks in step (iv); this happens automatically as a consequence of storing the coefficients in θ-representation. In effect, the splitting (and reassembling) work has been shunted into the conversions in step (i).

We now consider each of the above steps in more detail. We write $\mathsf{T}(L,q)$ for the running time of Transform. We always assume that L_0 is increased whenever necessary to accommodate statements that hold only for large L.

Step (i) — convert between representations. Let $\mathsf{T}_{\mathrm{long}}(L,q)$ denote the time required to compute a DFT of length L over $\mathbb{Z}/q\mathbb{Z}$ with respect to ζ, assuming that the coefficients of the input F and the output $\hat{F}$ are given in θ-representation, and assuming that $\mathcal{P}(q,m,\theta)$ is known.

Lemma 3.1. *We have* $\mathsf{T}(L,q) < \mathsf{T}_{\mathrm{long}}(L,q) + O(L\lg L\lg q)$.

Proof. We first convert F from standard to θ-representation using Proposition 2.18; we then compute $\hat{F}$ from F (working entirely in θ-representation); at the end, we convert $\hat{F}$ back to standard representation using Proposition 2.21. By (3.1) and (3.2), the total cost of the conversions is

$$\begin{aligned} O(Lm\,\mathsf{M}_{\mathrm{SS}}(\lg q)) &= O\left(L\frac{\lg q}{(\lg\lg L)^2\lg\lg\lg L}\lg q\lg\lg q\lg\lg\lg q\right) \\ &= O\left(L\frac{\lg L\lg\lg L}{(\lg\lg L)^2\lg\lg\lg L}\lg q\lg\lg L\lg\lg\lg L\right) \\ &= O(L\lg L\lg q). \end{aligned}$$

□

Henceforth all elements of $\mathbb{Z}/q\mathbb{Z}$ are assumed to be stored in θ-representation, and we will always use Proposition 2.15 to perform arithmetic operations on such elements in $O(\mathsf{M}_{\mathrm{SS}}(\lg q))$ bit operations.

Step (ii) — reduce to short DFTs. Let $S := 2^{(\lg\lg L)^2}$. Given as input polynomials $F_1,\dots,F_{L/S} \in (\mathbb{Z}/q\mathbb{Z})[x]/(x^S-1)$ (presented sequentially on tape), let $\mathsf{T}_{\mathrm{short}}(L,q)$ denote the time required to compute the transforms $\hat{F}_1,\dots,\hat{F}_{L/S} \in (\mathbb{Z}/q\mathbb{Z})^S$ with respect to the principal S-th root of unity $\omega := \zeta^{L/S}$. (Here and below, we continue to assume that $\mathcal{P}(q,m,\theta)$ is known.).

Lemma 3.2. *We have* $\mathsf{T}_{\mathrm{long}}(L,q) < \frac{\lg L}{(\lg\lg L)^2}\,\mathsf{T}_{\mathrm{short}}(L,q) + O(L\lg L\lg q)$.

Proof. Let $d := \lfloor \lg L / \lg S \rfloor$, so that $\lg L = d \lg S + d'$ where $0 \leqslant d' < \lg S$. Applying the Cooley–Tukey method [4] to the factorisation $L = S^d 2^{d'}$, the given transform of length L may be decomposed into $d \sim \lg L/(\lg\lg L)^2$ layers, each consisting of L/S transforms of length S (with respect to ω), followed by d' layers, each consisting of $L/2$ transforms of length 2. Between each of these layers, we must perform $O(L)$ multiplications by "twiddle factors" in $\mathbb{Z}/q\mathbb{Z}$, which are given by certain powers of ζ. (For further details of the Cooley–Tukey decomposition, see for example [14, §2.3].)

The total cost of the twiddle factor multiplications, including the cost of computing the twiddle factors themselves, is

$$\begin{aligned} O((d+d')L\,\mathsf{M}_{\mathrm{SS}}(\lg q)) &= O\left(\left(\frac{\lg L}{(\lg\lg L)^2} + (\lg\lg L)^2\right) L \lg q \lg\lg q \lg\lg\lg q\right) \\ &= O\left(\frac{\lg L}{(\lg\lg L)^2} L \lg q \lg\lg L \lg\lg\lg L\right) = O(L \lg L \lg q). \end{aligned}$$

This bound also covers the cost of the length 2 transforms ('butterflies'), each of which requires one addition and one subtraction in $\mathbb{Z}/q\mathbb{Z}$.

In the Turing model, we must also account for the cost of rearranging data so that the inputs for each layer of short DFTs are stored sequentially on tape. The cost per layer is $O(L \lg S \lg q)$ bit operations, so $O(L \lg L \lg q)$ altogether (see [14, §2.3] for further details). □

Step (iii) — reduce to short convolutions. Given polynomials $G_1, \ldots, G_{L/S}, H \in (\mathbb{Z}/q\mathbb{Z})[x]/(x^S - 1)$ as input, let $\mathsf{M}_{\mathrm{short}}(L, q)$ denote the time required to compute the products $G_1 H, \ldots, G_{L/S} H$.

Lemma 3.3. *We have* $\mathsf{T}_{\mathrm{short}}(L, q) < \mathsf{M}_{\mathrm{short}}(L, q) + O(L(\lg\lg L)^2 \lg q)$.

Proof. We use Bluestein's method [2], which reduces the the problem of computing the DFT of $F \in (\mathbb{Z}/q\mathbb{Z})[x]/(x^S - 1)$ to the problem of computing the product of certain polynomials $G, H \in (\mathbb{Z}/q\mathbb{Z})[x]/(x^S - 1)$, plus $O(S)$ auxiliary multiplications in $\mathbb{Z}/q\mathbb{Z}$ (for further details see [14, §2.5]). Here G depends on F and ζ, but H depends only on ζ. The total cost of the auxiliary multiplications is

$$O((L/S) S\,\mathsf{M}_{\mathrm{SS}}(\lg q)) = O(L \lg q \lg\lg q \lg\lg\lg q) = O(L(\lg\lg L)^2 \lg q). \qquad \square$$

Step (iv) — reduce to bivariate products over $\mathbb{Z}$. Given as input polynomials $\tilde{G}_1, \ldots, \tilde{G}_{L/S}, \tilde{H} \in \mathbb{Z}[x, y]/(x^S - 1, y^m + 1)$, all whose of coefficients are bounded in absolute value by $mq^{1/m}$, let $\mathsf{M}_{\mathrm{bivariate}}(L, q)$ denote the cost of computing the products $\tilde{G}_1 \tilde{H}, \ldots, \tilde{G}_{L/S} \tilde{H}$.

Lemma 3.4. *We have* $\mathsf{M}_{\mathrm{short}}(L, q) < \mathsf{M}_{\mathrm{bivariate}}(L, q) + O(L(\lg\lg L)^2 \lg q)$.

Proof. We are given as input polynomials $G_1, \ldots, G_{L/S}, H \in (\mathbb{Z}/q\mathbb{Z})[x]/(x^S - 1)$. Since their coefficients are given in θ-representation, we may immediately reinterpret them as polynomials $\tilde{G}_1, \ldots, \tilde{G}_{L/S}, \tilde{H} \in \mathbb{Z}[x, y]/(x^S - 1, y^m + 1)$, with coefficients bounded by $mq^{1/m}$. By definition of θ-representation, we have $\tilde{H}(x, \theta) = H(x) \pmod q$, and similarly for the G_i.

After computing the products $\tilde{G}_i \tilde{H}$ for $i = 1, \ldots, L/S$, suppose that

$$(\tilde{G}_i \tilde{H})(x, y) = \sum_{j=0}^{S-1} A_{ij}(y) x^j, \qquad A_{ij} \in \mathbb{Z}[y]/(y^m + 1).$$

Then we have $(G_iH)(x) = (\tilde{G}_i\tilde{H})(x,\theta) = \sum_j A_{ij}(\theta)x^j \pmod q$ for each i. Therefore, to compute the desired products G_iH with coefficients in θ-representation, it suffices to apply Proposition 2.17 to each A_{ij}, to compute θ-representations for all of the $A_{ij}(\theta)$.

Let us estimate the cost of the invocations of Proposition 2.17. We have $\|A_{ij}\| \leqslant Sm(mq^{1/m})^2 = Sm^3(q^{1/m})^2$, so

$$\lg\|A_{ij}\| \leqslant \frac{2\lg q}{m} + \lg S + 3\lg m < \frac{2\lg q}{m} + (\lg\lg L)^2 + O(\lg\lg L).$$

From (3.2) we have $\frac{\lg q}{m} > \frac{1}{2}(\lg\lg L)^2 \lg\lg\lg L$, so for large L,

$$\lg\|A_{ij}\| < \left(2 + \frac{3}{\lg\lg\lg L}\right)\frac{\lg q}{m}. \tag{3.3}$$

The cost of applying Proposition 2.17 for all A_{ij} is thus

$$O\left((L/S)S\left\lceil\frac{m\lg\|A_{ij}\|}{\lg q}\right\rceil \mathsf{M}_{\mathrm{SS}}(\lg q)\right) = O(L\,\mathsf{M}_{\mathrm{SS}}(\lg q)) = O(L(\lg\lg L)^2\lg q). \quad \square$$

Step (v) — Reduce to bivariate products over $\mathbb{Z}/q'\mathbb{Z}$. Let p' be the smallest prime such that $p' = 1 \pmod S$; by Linnik's theorem we have $p' = O(S^{5.2})$. Put $q' := (p')^{\alpha'}$ where

$$\alpha' := \left\lceil \left(2 + \frac{4}{\lg\lg\lg L}\right)\frac{\lg q}{m} \Big/ \lg\lfloor p'/2\rfloor \right\rceil.$$

We have the following bounds for q'.

Lemma 3.5. *Let A_{ij} be as in the proof of Lemma 3.4, for $i = 1,\dots,L/S$ and $j = 0,\dots,S-1$. Then $q' \geqslant 4\|A_{ij}\|$ and*

$$\lg q' < \left(2 + \frac{O(1)}{\lg\lg\lg L}\right)\frac{\lg q}{m}.$$

Proof. In what follows, we frequently use the fact that $\frac{\lg q}{m} \asymp (\lg\lg L)^2\lg\lg\lg L$ (see (3.2)). Now, observe that $\log_2 q' = \alpha'\log_2 p' \geqslant \alpha'\lg\lfloor p'/2\rfloor$, so by (3.3),

$$\log_2 q' \geqslant \left(2 + \frac{4}{\lg\lg\lg L}\right)\frac{\lg q}{m} \geqslant \left(2 + \frac{3}{\lg\lg\lg L}\right)\frac{\lg q}{m} + 2 \geqslant \lg\|A_{ij}\| + 2.$$

Thus $q' \geqslant 4\|A_{ij}\|$. For the other direction, since $\lg p' \asymp \lg S = (\lg\lg L)^2$, we have

$$\lg q' \leqslant \alpha'\lg p' \leqslant \left[\frac{\left(2 + \frac{4}{\lg\lg\lg L}\right)\frac{\lg q}{m}}{\lg\lfloor p'/2\rfloor} + 1\right]\lg p' < \left(2 + \frac{O(1)}{\lg\lg\lg L}\right)\frac{\lg q}{m}\cdot\frac{\lg p'}{\lg\lfloor p'/2\rfloor},$$

and $\lg p'/\lg\lfloor p'/2\rfloor < 1 + O(1)/\lg p' < 1 + O(1)/(\lg\lg L)^2$. $\square$

Now, given as input polynomials $g_1,\dots,g_{L/S},h \in (\mathbb{Z}/q'\mathbb{Z})[x,y]/(x^S-1, y^m+1)$, let $\mathsf{M}'_{\mathrm{bivariate}}(L,q)$ denote the cost of computing the products $g_1h,\dots,g_{L/S}h$, where all input and output coefficients in $\mathbb{Z}/q'\mathbb{Z}$ are in standard representation.

Lemma 3.6. *We have $\mathsf{M}_{\mathrm{bivariate}}(L,q) < \mathsf{M}'_{\mathrm{bivariate}}(L,q) + O(L\lg q)$.*

Proof. We may locate p' by testing $S+1, 2S+1, \ldots$, in $S^{O(1)} = 2^{O((\lg\lg L)^2)} = O(L)$ bit operations, and we may easily compute α' and q' within the same time bound. Now, given as input $\tilde{G}_1, \ldots, \tilde{G}_{L/S}, \tilde{H} \in \mathbb{Z}[x,y]/(x^S - 1, y^m + 1)$, we first convert them (in linear time) to polynomials $g_1, \ldots, g_{L/S}, h \in (\mathbb{Z}/q'\mathbb{Z})[x,y]/(x^S - 1, y^m + 1)$, and then multiply them in the latter ring. The bound $q' \geqslant 4\|A_{ij}\|$ in Lemma 3.5 shows that the products over $\mathbb{Z}$ may be unambiguously recovered from those over $\mathbb{Z}/q'\mathbb{Z}$; again, this lifting can be done in linear time. □

Step (vi) — reduce to DFTs over $\mathbb{Z}/q'\mathbb{Z}$. In this step we will call TRANSFORM recursively to handle certain transforms of length S over $\mathbb{Z}/q'\mathbb{Z}$. To check that these calls are permissible, we must verify the precondition corresponding to (3.1), namely $\lg S \leqslant \lg q' \leqslant 3 \lg S \lg\lg S$. The first inequality is clear since $q' \geqslant p' > S$. The second inequality follows from (3.2), Lemma 3.5, and the observation that $\lg S \lg\lg S \geqslant (\lg\lg L)^2 \lg\lg\lg L$.

Lemma 3.7. *We have* $\mathsf{M}'_{\text{bivariate}}(L, q) < \left(\frac{2L}{S} + 1\right) m\, \mathsf{T}(S, q') + O(L(\lg\lg L)^2 \lg q)$.

Proof. We start by computing various data needed for the recursive calls. We may compute a primitive S-th root of unity in $\mathbb{Z}/p'\mathbb{Z}$ in $(p')^{O(1)} = O(L)$ bit operations, and then Hensel lift it to a principal S-th root of unity $\zeta' \in \mathbb{Z}/q'\mathbb{Z}$ in $(\lg p' \lg q')^{O(1)} = O(L)$ bit operations. For q (whence q' and S) sufficiently large, we have $\lg q' \geqslant \lg S > 2(\lg\lg S)^2 \lg\lg\lg S$. Just as before, this allows us to define m' to be the unique power of two in the interval

$$\frac{\lg q'}{(\lg\lg S)^2 \lg\lg\lg S} \leqslant m' < \frac{2 \lg q'}{(\lg\lg S)^2 \lg\lg\lg S}, \tag{3.4}$$

and set $\theta' := (\zeta')^{S/2m'}$. Using Lemmas 2.3, 2.7, and 2.12, we may compute $\mathcal{P}(q', m', \theta')$ in $(q')^{1+o(1)} = 2^{O((\lg\lg L)^2 \lg\lg\lg L)} = O(L)$ bit operations.

Now suppose we wish to compute the products $g_1 h, \ldots, g_{L/S} h$, for polynomials $g_1, \ldots, g_{L/S}, h \in (\mathbb{Z}/q'\mathbb{Z})[x,y]/(x^S - 1, y^m + 1)$. We use the following algorithm.

First we use TRANSFORM to transform all $L/S+1$ polynomials with respect to x, that is, we compute $g_i((\zeta')^j, y)$ and $h((\zeta')^j, y)$ as elements of $(\mathbb{Z}/q'\mathbb{Z})[y]/(y^m+1)$, for $i = 1, \ldots, L/S$ and $j = 0, \ldots, S-1$. Since TRANSFORM must be applied separately to every coefficient $1, y, \ldots, y^{m-1}$, the total number of calls is $(L/S+1)m$. Accessing the coefficient of each y^k also implies a number of array transpositions whose total cost is $O((L/S)Sm \lg m \lg q') = O(L \lg\lg L \lg q)$.

Next we compute the $(L/S)S = L$ pointwise products $g_i((\zeta')^j, y) h((\zeta')^j, y)$. Using Kronecker substitution, each such product in $(\mathbb{Z}/q'\mathbb{Z})[y]/(y^m + 1)$ costs $O(\mathsf{M}_{\text{SS}}(\lg q))$ bit operations, as $m(\lg q' + \lg m) = O(\lg q)$.

Finally, we perform $(L/S)m$ inverse transforms with respect to x. It is well known that these may be computed by the same algorithm as the forward transform, with ζ' replaced by $(\zeta')^{-1}$, followed by a division by S. The division may be accomplished by simply multiplying through by $S^{-1} \pmod{q'}$; this certainly costs no more than the pointwise multiplication step. □

Corollary 3.8. *We have* $\mathsf{T}(L, q) < \frac{\lg L}{(\lg\lg L)^2} \left(\frac{2L}{S} + 1\right) m\, \mathsf{T}(S, q') + O(L \lg L \lg q)$.

Proof. This follows immediately by chaining together Lemmas 3.1, 3.2, 3.3, 3.4, 3.6, and 3.7. □

Define

$$\mathsf{T}(L) := \max_q \frac{\mathsf{T}(L,q)}{L \lg L \lg q},$$

where the maximum is taken over all prime powers q satisfying (3.1). (For large L, at least one such q always exists. For example, take $\alpha := 1$ and take $q = p$ to be the smallest prime satisfying $p = 1 \pmod{L}$; then Linnik's theorem implies that (3.1) holds for this q.)

Proposition 3.9. *We have* $\mathsf{T}(L) < \left(4 + \frac{O(1)}{\lg\lg\lg L}\right) \mathsf{T}(2^{(\lg\lg L)^2}) + O(1)$.

Proof. Dividing the bound in Corollary 3.8 by $L \lg L \lg q$ yields

$$\frac{\mathsf{T}(L,q)}{L \lg L \lg q} < \left(2 + \frac{S}{L}\right) \frac{m \lg q'}{\lg q} \cdot \frac{\mathsf{T}(S,q')}{S \lg S \lg q'} + O(1).$$

Applying Lemma 3.5 and the estimate $S/L < O(1)/\lg\lg\lg L$ yields

$$\frac{\mathsf{T}(L,q)}{L \lg L \lg q} < \left(4 + \frac{O(1)}{\lg\lg\lg L}\right) \mathsf{T}(S) + O(1).$$

Taking the maximum over allowable q yields the desired bound. □

Corollary 3.10. *We have* $\mathsf{T}(L) = O(4^{\log^* L})$.

Proof. This follows by applying the "master theorem" [14, Prop. 8] to the recurrence in Proposition 3.9. Alternatively, it follows by the same method used to deduce [12, Cor. 3] from [12, Prop. 2]. The key point is that $2^{(\lg\lg L)^2}$ is dominated by a "logarithmically slow" function of L, such as $\Phi(x) := 2^{(\log\log x)^3}$ (see [14, §5]). □

Remark 3.11. When working with θ-representations, it is possible to multiply an element of $\mathbb{Z}/q\mathbb{Z}$ by any power of θ in linear time, by simply permuting the coefficients. In other words, we have available "fast roots of unity" in the sense of Fürer. Notice however that the algorithm presented in this section makes no use of this fact!

This raises the question of whether one can design an integer multiplication algorithm that uses these fast roots in the same way as in Fürer's original algorithm, instead of our appeal to Bluestein's trick. This is indeed possible, and one does obtain a bound of the form $O(n \lg n\, K^{\log^* n})$. In this algorithm, instead of the running time being dominated by the short transforms, it is dominated by the twiddle factor multiplications, just as in Fürer's algorithm. Unfortunately, this leads to a worse value of K, because of the implied constant in Proposition 2.15.

4. Integer multiplication: the top level

The only complication in building an integer multiplication algorithm on top of the Transform routine is ensuring that the precomputations do not dominate the complexity. We achieve this by means of a multivariate Kronecker-style splitting, as follows.

Proof of Theorem 1.1. Suppose that we wish to compute the product of two n-bit integers u and v, for some sufficiently large $n \geqslant 729$. Let $b := \lg n$ and $t := \lceil \lceil n/b \rceil^{1/6} \rceil$, so that $t^6 b \geqslant n$ and $t \leqslant n^{1/6}$. Decompose u into t^6 chunks of b bits,

say $u = u_0 + u_1 2^b + \cdots + u_{t^6-1} 2^{(t^6-1)b}$ where $0 \leqslant u_i < 2^b$ for each i, and similarly for v. Let

$$U(x_0, \ldots, x_5) := \sum_{i_0=0}^{t-1} \cdots \sum_{i_5=0}^{t-1} u_{i_0+ti_1+\cdots+t^5 i_5} x_0^{i_0} \cdots x_5^{i_5} \in \mathbb{Z}[x_0, \ldots, x_5],$$

so that $u = U(2^b, 2^{tb}, \ldots, 2^{t^5 b})$, and define $V(x_0, \ldots, x_5)$ similarly. We store multivariate polynomials in $\mathbb{Z}[x_0, \ldots, x_5]$ using the recursive dense representation. The product UV has degree less than $2t$ in each variable, so at most $64t^6$ terms altogether, and its coefficients are bounded by $2^{2b} t^6 \leqslant 2^{2b} n \leqslant 4n^3$. We may therefore reconstruct uv from UV using a straightforward overlap-add procedure (essentially, evaluating at $(2^b, 2^{tb}, \ldots, 2^{t^5 b})$) in $O(t^6 \lg n) = O(n)$ bit operations.

Now we consider the computation of UV. Let L be the unique power of two in the interval $2t \leqslant L < 4t$; then it suffices to compute the product UV in the ring $\mathbb{Z}[x_0, \ldots, x_5]/(x_0^L - 1, \ldots, x_5^L - 1)$.

For $i = 1, \ldots, 19$, let q_i be the least prime such that $q_i = 1 \pmod{L}$ and $q_i = i \pmod{23}$. Then the q_i are distinct, and by Linnik's theorem they satisfy $q_i = O(L^{5.2}) = O(t^{5.2}) = O(n^{0.9})$, so we may locate the q_i in $n^{0.9+o(1)}$ bit operations. They certainly satisfy (3.1), since $q_i \geqslant L$ and $\lg q_i \leqslant 5.2 \lg L + O(1) \leqslant 3 \lg L \lg \lg L$ for large L. Moreover, for large n we have $q_1 \cdots q_{19} > L^{19} \geqslant 2^{19} t^{19} \geqslant 2^{19} (n/\lg n)^{19/6} > 4n^3$, so to compute UV it suffices to compute $UV \pmod{q_i}$ for each i and then reconstruct UV by the Chinese remainder theorem. The cost of this reconstruction is $(\lg n)^{1+o(1)}$ bit operations per coefficient, so $(n/\lg n)(\lg n)^{1+o(1)} = n(\lg n)^{o(1)}$ altogether.

We have therefore reduced to the problem of computing a product in the ring $(\mathbb{Z}/q_i\mathbb{Z})[x_0, \ldots, x_5]/(x_0^L - 1, \ldots, x_5^L - 1)$ for each $i = 1, \ldots, 19$. To do this, we use Transform to perform forward DFTs of length L with respect to a suitable primitive L-th root of unity ζ_i in $\mathbb{Z}/q_i\mathbb{Z}$ (with the notations from Section 3, this means that we take $p = q = q_i$ and $\zeta = \zeta_i$) for each variable $x_0, \ldots, x_5$ successively; then we multiply pointwise in $\mathbb{Z}/q_i\mathbb{Z}$; finally we perform inverse DFTs and scale the results. The necessary precomputations for each prime q_i (finding ζ_i, m_i, θ_i, and computing $\mathcal{P}(q_i, m_i, \theta_i)$) require only $q_i^{1+o(1)} = n^{0.9+o(1)}$ bit operation per prime. Since one FFT-multiplication in $(\mathbb{Z}/q_i\mathbb{Z})[x_0, \ldots, x_5]/(x_0^L - 1, \ldots, x_5^L - 1)$ requires two direct multivariate transforms and one inverse multivariate transform, the total number of calls to Transform for each prime is $6 \cdot (2+1)L^5 = 18L^5$. The total cost of the pointwise multiplications is $n(\lg n)^{o(1)}$. By Corollary 3.10, this yields

$$\begin{aligned}
\mathsf{M}(n) &= O(L^5 \textstyle\sum_{i=1}^{19} \mathsf{T}(L, q_i)) + n(\lg n)^{o(1)} \\
&= O(L^6 \textstyle\sum_{i=1}^{19} \mathsf{T}(L) \lg L \lg q_i) + n(\lg n)^{o(1)} \\
&= O((n/\lg n) 4^{\log^* L} \lg n \lg n) + n(\lg n)^{o(1)} \\
&= O(n \lg n \, 4^{\log^* n}).
\end{aligned}$$

□

References

1. P. Barrett, *Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor*, Advances in cryptology—CRYPTO '86 (Santa Barbara, Calif., 1986), Lecture Notes in Comput. Sci., vol. 263, Springer, Berlin, 1987, pp. 311–323. MR 907099 (88i:94015)
2. L. I. Bluestein, *A linear filtering approach to the computation of discrete Fourier transform*, IEEE Transactions on Audio and Electroacoustics **18** (1970), no. 4, 451–455.

20 Jun 2018 14:52:56 PDT
Version 3 - Submitted to Open Book Series

3. A. Bostan, P. Gaudry, and É. Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator*, SIAM J. Comput. **36** (2007), no. 6, 1777–1806. MR 2299425 (2008a:11156)
4. J. W. Cooley and J. W. Tukey, *An algorithm for the machine calculation of complex Fourier series*, Math. Comp. **19** (1965), 297–301. MR 0178586
5. S. Covanov and E. Thomé, *Fast integer multiplication using generalized Fermat primes*, `http://arxiv.org/abs/1502.02800`, 2016.
6. R. Crandall and B. Fagin, *Discrete weighted transforms and large-integer arithmetic*, Math. Comp. **62** (1994), no. 205, 305–324. MR 1185244
7. A. De, P. P. Kurur, C. Saha, and R. Saptharishi, *Fast integer multiplication using modular arithmetic*, SIAM J. Comput. **42** (2013), no. 2, 685–699.
8. M. Fürer, *Faster integer multiplication*, STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing, ACM, New York, 2007, pp. 57–66. MR 2402428 (2009e:68124)
9. ———, *Faster integer multiplication*, SIAM J. Comput. **39** (2009), no. 3, 979–1005. MR 2538847 (2011b:68296)
10. D. Harvey, *Faster truncated integer multiplication*, `https://arxiv.org/abs/1703.00640`, 2017.
11. D. Harvey, J. van der Hoeven, and G. Lecerf, *Fast polynomial multiplication over* $\mathbb{F}_{2^{60}}$, Proc. ISSAC '16 (New York, NY, USA), ACM, 2016, pp. 255–262.
12. D. Harvey and J. van der Hoeven, *Faster integer multiplication using plain vanilla FFT primes*, `https://arxiv.org/abs/1611.07144`, to appear in Math. Comp., 2016.
13. ———, *Faster integer and polynomial multiplication using cyclotomic coefficient rings*, `https://arxiv.org/abs/1712.03693`, 2017.
14. D. Harvey, J. van der Hoeven, and G. Lecerf, *Even faster integer multiplication*, J. Complexity **36** (2016), 1–30. MR 3530637
15. J. van der Hoeven, R. Larrieu, and G. Lecerf, *Implementing fast carryless multiplication*, Proc. MACIS 2017, Vienna, Austria (Cham) (J. Blömer, I. S. Kotsireas, T. Kutsia, and D. E. Simos, eds.), Lect. Notes in Computer Science, Springer International Publishing, 2017, pp. 121–136.
16. S. Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723
17. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR 682664
18. C. Lüders, *Implementation of the DKSS algorithm for multiplication of large numbers*, Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2015, Bath United Kingdom, July 06 - 09, 2015, 2015, pp. 267–274.
19. D. Micciancio and P. Voulgaris, *A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations*, SIAM J. Comput. **42** (2013), no. 3, 1364–1391. MR 3504632
20. P. L. Montgomery, *Modular multiplication without trial division*, Math. Comp. **44** (1985), no. 170, 519–521. MR 777282 (86e:11121)
21. C. H. Papadimitriou, *Computational complexity*, Addison-Wesley Publishing Company, Reading, MA, 1994. MR 1251285 (95f:68082)
22. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR 0137689
23. A. Schönhage and V. Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR 0292344 (45 #1431)
24. J. von zur Gathen and J. Gerhard, *Modern computer algebra*, third ed., Cambridge University Press, Cambridge, 2013. MR 3087522
25. T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. **150** (2011), no. 1, 65–91. MR 2825574 (2012m:11129)

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
E-mail address: `d.harvey@unsw.edu.au`

CNRS, Laboratoire d'informatique, École polytechnique, 91128 Palaiseau, France
E-mail address: `vdhoeven@lix.polytechnique.fr`

20 Jun 2018 14:52:56 PDT
Version 3 - Submitted to Open Book Series

A NEW PERSPECTIVE ON THE POWERS OF TWO DESCENT FOR DISCRETE LOGARITHMS IN FINITE FIELDS

THORSTEN KLEINJUNG AND BENJAMIN WESOLOWSKI

Abstract. A new proof is given for the correctness of the powers of two descent method for computing discrete logarithms. The result is slightly stronger than the original work, but more importantly we provide a unified geometric argument, eliminating the need to analyse all possible subgroups of $\mathrm{PGL}_2(\mathbf{F}_q)$. Our approach sheds new light on the role of PGL_2, in the hope to eventually lead to a complete proof that discrete logarithms can be computed in quasi-polynomial time in finite fields of fixed characteristic.

1. Introduction

In this paper we prove the following result.

Theorem 1.1. *Given a prime power q, a positive integer d, coprime polynomials h_0 and h_1 in $\mathbf{F}_{q^d}[x]$ of degree at most two, and an irreducible degree ℓ factor I of $h_1 x^q - h_0$, the discrete logarithm problem in $\mathbf{F}_{q^{d\ell}} \cong \mathbf{F}_{q^d}[x]/(I)$ can be solved in expected time $q^{\log_2 \ell + O(d)}$.*

It was originally proven in [GKZ18] when $q > 61$, q is not a power of 4, and $d \geq 18$. Even though we eliminate these technical conditions, the main contribution is the new approach to the proof. The theorem represents the state of the art of provable quasi-polynomial time algorithms for the discrete logarithm problem (or DLP) in finite fields of fixed characteristic. The obstacle separating Theorem 1.1 from a full provable algorithm for DLP is the question of the existence of a good field representation: polynomials h_0, h_1 and I for a small d. A direction towards a full provable algorithm would be to find analogues of this theorem for other field representations, but this may require in the first place a good understanding of why Theorem 1.1 is true.

The integers q, d and ℓ, and the polynomials h_0, h_1 and I are defined as in the above theorem for the rest of the paper. The core of that result is Proposition 1.3 below, which essentially states that elements of $\mathbf{F}_{q^{d\ell}}$ represented by a *good* irreducible polynomial in $\mathbf{F}_{q^d}[x]$ of degree $2m$ can be rewritten as a product of *good* irreducible polynomials of degrees dividing m — a process called *degree two elimination*, first introduced for $m = 1$ in [GGMZ13].

Definition 1.2 (Traps and good polynomials)**.** An element $\tau \in \overline{\mathbf{F}}_q$ for which $[\mathbf{F}_{q^d}(\tau) : \mathbf{F}_{q^d}]$ is an even number $2m$ and $h_1(\tau) \neq 0$ is called

(1) a *degenerate trap root* if $\frac{h_0}{h_1}(\tau) \in \mathbf{F}_{q^{dm}}$,
(2) a *trap root of level* 0 if it is a root of $h_1 x^q - h_0$, or
(3) a *trap root of level* dm if it is a root of $h_1 x^{q^{dm+1}} - h_0$.

Analogously, a polynomial in $\overline{\mathbf{F}}_q[x]$ that has a trap root is called a *trap*. A polynomial is *good* if it is not a trap.

18 Jun 2018 05:54:53 PDT
Version 3 - Submitted to Open Book Series

Proposition 1.3 (Degree two elimination)**.** *Given an extension $k/\mathbf{F}_{q^d}$ of degree m such that $dm \geq 23$, and a good irreducible quadratic polynomial $Q \in k[x]$, there is an algorithm which finds a list of good linear polynomials $(L_0, \ldots, L_n)$ in $k[x]$ such that $n \leq q+1$ and*

$$Q \equiv h_1 L_0^{-1} \cdot \prod_{i=1}^{n} L_i \mod I,$$

and runs in expected polynomial time in q, d and m.

The difficulty of proving Theorem 1.1 lies mostly in Proposition 1.3. We recall briefly in Section 1.2 how the proposition implies the theorem. The main contribution of the present paper is a new proof of Proposition 1.3, which hopefully provides a better understanding of the degree two elimination method, the underlying geometry, and the role of traps. The action of PGL_2 on the polynomial $x^q - x$ became a crucial ingredient in the recent progress on the discrete logarithm problem for fields of small characteristic, since [Jou13] (and implicitly in [GGMZ13]). While the proof in [GKZ18] resorted to an intricate case by case analysis enumerating through all possible subgroups of $\mathrm{PGL}_2(\mathbf{F}_q)$, we provide a unified geometric argument, shedding new light on the role of PGL_2.

1.1. **Degree two elimination algorithm.** The key observation allowing degree two elimination is that a polynomial of the form $\alpha x^{q+1} + \beta x^q + \gamma x + \delta$ has a high chance to split completely over its field of definition. Furthermore, we have the congruence

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \equiv h_1^{-1}(\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1) \mod I, \tag{1.1}$$

and the numerator of the right-hand side has degree at most 3. Consider the $\overline{\mathbf{F}}_q$-vector space V spanned by x^{q+1}, x^q, x and 1 in $\overline{\mathbf{F}}_q[x]$, and the linear subspace

$$V_Q = \{\alpha x^{q+1} + \beta x^q + \gamma x + \delta \in V \mid \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \equiv 0 \mod Q\}.$$

As long as Q is a good irreducible polynomial, V_Q is of dimension two. The algorithm simply consists in sampling uniformly at random elements $f \in V_Q(k)$ (or equivalently in its projectivisation $\mathbf{P}^1_Q(k)$) until f splits completely over k into good linear polynomials $(L_1, \ldots, L_{\deg f})$. Since $f \in V_Q$, the polynomial Q divides the numerator of the right-hand side of (1.1), and the quotient is a polynomial L_0 of degree at most 1. The algorithm returns $(L_0, \ldots, L_{\deg f})$.

To prove that the algorithm terminates in expected polynomial time, we need to show that a random polynomial in $V_Q(k)$ has good chances to split into good linear polynomials over k. In this paper, we prove this by constructing a morphism $C \to \mathbf{P}^1_Q$ where C is an absolutely irreducible curve defined over k, such that the image of any k-rational point of C is a polynomial that splits completely over k. This construction is the object of Section 4. The absolute irreducibility implies that C has a lot of k-rational points, allowing us to deduce that a lot of polynomials in $\mathbf{P}^1_Q(k)$ split over k. This is done in Section 5.

1.2. **Proof of Theorem 1.1.** We briefly explain in this section how Proposition 1.3 implies Theorem 1.1. Consider the factor base

$$\mathfrak{F} = \{f \in \mathbf{F}_{q^d}[x] \mid \deg f \leq 1, f \neq 0\} \cup \{h_1\}.$$

First, the following proposition extends the degree two elimination to a full descent algorithm from any polynomial down to the factor base.

18 Jun 2018 05:54:53 PDT
Version 3 - Submitted to Open Book Series

Proposition 1.4. *Suppose $d \geq 23$. Given a polynomial $F \in \mathbf{F}_{q^d}[x]$, there is an algorithm that finds integers $(\alpha_f)_{f\in\mathfrak{F}}$ such that*

$$F \equiv \prod_{f\in\mathfrak{F}} f^{\alpha_f} \mod I,$$

and runs in expected time $q^{\log_2 \ell + O(d)}$.

Proof. This is essentially the *zigzag* descent presented in [GKZ18]. We recall the main idea for the convenience of the reader. First, one finds a good irreducible polynomial $G \in \mathbf{F}_{q^d}[x]$ of degree 2^e such that $F \equiv G \mod I$ (this can be done for $e = \lceil \log_2(4\ell+1)\rceil$, see [Wan97, Th. 5.1] and [GKZ18, Lem. 2]). Over the extension $\mathbf{F}_{q^{d2^{e-1}}}$, the polynomial G splits into 2^{e-1} good irreducible quadratic polynomials, all conjugate under $\mathrm{Gal}(\mathbf{F}_{q^{d2^{e-1}}}/\mathbf{F}_{q^d})$. Let Q be one of them, and apply the algorithm of Proposition 1.3 to rewrite Q in terms of linear polynomials $(L_0,\dots,L_n)$ in $\mathbf{F}_{q^{d2^{e-1}}}[x]$ and h_1. For any index i, let L'_i be the product of all the conjugates of L_i in the extension $\mathbf{F}_{q^{d2^{e-1}}}/\mathbf{F}_{q^d}$. Then,

$$F \equiv h_1^{2^{e-1}} L_0'^{-1} \cdot \prod_{i=1}^{n} L'_i \mod I,$$

and each L'_i factors into good irreducible polynomials of degree a power of 2 at most 2^{e-1}. The descent proceeds by iteratively applying this method to each L'_i until all the factors are in the factor base $\mathfrak{F}$. □

Then, as in [GKZ18, Sec. 2], the descent algorithm of Proposition 1.4 can be used to compute discrete logarithms, following ideas from [EG02] and [Die11]. To compute the discrete logarithm of an element h in base g, the idea is to collect relations between g, h, and elements of the factor base by applying the descent algorithm on $g^\alpha h^\beta$ for a few uniformly random exponents α and β (note that in practice one descent is usually sufficient, when complemented by an independent heuristic computation for the factor base elements).

That proves Theorem 1.1 for $d \geq 23$. To remove the condition on d, suppose that $d \leq 22$, and let $d' \leq 44$ be the smallest multiple of d larger than 22. Let I' be an irreducible factor of I in $\mathbf{F}_{q^{d'}}[x]$. The DLP can be solved in expected time $q^{\log_2(\deg I')+O(d')} = q^{\log_2 \ell + O(1)}$ in the field $\mathbf{F}_{q^{d'}}[x]/(I')$, and therefore also in the subfield $\mathbf{F}_{q^d}[x]/(I)$.

2. The action of PGL_2 on $x^q - x$

As already mentioned, a crucial fact behind degree two elimination is that a polynomial of the form $\alpha x^{q+1} + \beta x^q + \gamma x + \delta$ has a high chance to split completely over its field of definition. This fact is closely related to the action of 2×2 matrices on such polynomials.

Definition 2.1. We denote by $\star$ the action of invertible 2×2 matrices on univariate polynomials defined as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star f(x) = (cx+d)^{\deg f} f\left(\frac{ax+b}{cx+d}\right).$$

Consider the $\overline{\mathbf{F}}_q$-vector subspace V spanned by x^{q+1}, x^q, x, and 1 in $\overline{\mathbf{F}}_q[x]$. The above action induces an action of the group PGL_2 on the projective space $\mathbf{P}(V)$,

which we also write $\star$. Parameterizing the polynomials in $\mathbf{P}(V)$ as $\alpha x^{q+1} + \beta x^q + \gamma x + \delta$, let S be the quadratic surface in $\mathbf{P}(V)$ defined by the equation $\alpha\delta = \beta\gamma$. This surface is the image of the morphism

$$\psi : \mathbf{P}^1 \times \mathbf{P}^1 \longrightarrow \mathbf{P}(V) : (a, b) \longmapsto (x - a)(x - b)^q.$$

Note that to avoid heavy notation, everything is written affinely, but we naturally have $\psi(\infty, b) = (x - b)^q$, $\psi(a, \infty) = x - a$ and $\psi(\infty, \infty) = 1$. More generally, we say that $f(x) \in V$ has a root of degree n at infinity if f is of degree $q + 1 - n$. Now, the following lemma shows that apart from the surface S, the polynomials of $\mathbf{P}(V)$ form exactly one orbit for PGL_2.

Lemma 2.2. *We have* $\mathbf{P}(V) \setminus S = \mathrm{PGL}_2 \star (x^q - x)$.

Proof. First notice that both S and $\mathbf{P}(V) \setminus S$ are closed under the action of PGL_2. In particular, $\mathrm{PGL}_2 \star (x^q - x) \subseteq \mathbf{P}(V) \setminus S$. Let $f(x) \in \mathbf{P}(V) \setminus S$. Suppose by contradiction that $f(x)$ has a double root $r \in \mathbf{P}^1$, and let $g \in \mathrm{PGL}_2$ be a linear transformation sending 0 to r. The polynomial $g \star f(x)$ has a double root at 0, so has no constant or linear term, and must be of the form $\alpha x^{q+1} + \beta x^q$, so it is in S, a contradiction. Therefore $f(x)$ has $q + 1$ distinct roots. Let $g \in \mathrm{PGL}_2$ send 0, 1 and ∞ to three of these roots. Then, $g \star f(x)$ has a root at 0 and at ∞ so is of the form $\beta x^q + \gamma x$, and since it also has a root at 1, it can only be $x^q - x$. □

This result implies that most polynomials of $\mathbf{P}(V)$ are of the form $g \star (x^q - x)$, which splits completely over the field of definition of the matrix g.

3. The role of traps

Consider a finite field extension $k/\mathbf{F}_{q^d}$ of degree m. Let Q be an irreducible quadratic polynomial in $k[x]$ coprime to h_1. Let a_1 and a_2 be the roots of Q in $\overline{\mathbf{F}}_q$. The degree two elimination aims at expressing Q modulo $h_1 x^q - h_0$ as a product of linear polynomials. To do so, we study a variety $\mathbf{P}^1_Q \subset \mathbf{P}(V)$ parameterizing polynomials that can possibly lead to an elimination of Q (i.e., such that Q divides the right hand side of (1.1)). In this section, we define $\mathbf{P}^1_Q$ and show how the notion of traps and good polynomials determine how it intersects the surface S from Lemma 2.2.

Recall that V is the $\overline{\mathbf{F}}_q$-vector subspace V spanned by x^{q+1}, x^q, x, and 1 in $\overline{\mathbf{F}}_q[x]$. Consider the linear map

$$\varphi : V \longrightarrow \overline{\mathbf{F}}_q[x][h_1^{-1}] : \begin{cases} 1 & \longmapsto 1, \\ x & \longmapsto x, \\ x^q & \longmapsto h_0/h_1, \\ x^{q+1} & \longmapsto x h_0/h_1. \end{cases} \tag{3.1}$$

We want $\mathbf{P}^1_Q$ to parameterise the polynomials $f \in V$ such that $\varphi(f)$ is divisible by Q. For any $P \in \overline{\mathbf{F}}_q[x]$ coprime with h_1, write $\varphi_P = \pi_P \circ \varphi$ where $\pi_P : \overline{\mathbf{F}}_q[x][h_1^{-1}] \to \overline{\mathbf{F}}_q[x]/P$ is the canonical projection. We can now define $\mathbf{P}^1_Q$ as

$$\mathbf{P}^1_Q = \mathbf{P}(\ker \varphi_Q). \tag{3.2}$$

The variety $\mathbf{P}^1_Q$ is the intersection of the two planes $\mathbf{P}(\ker \varphi_{x-a_1})$ and $\mathbf{P}(\ker \varphi_{x-a_2})$.

Lemma 3.1. *If Q is not a degenerate trap, then $|(\mathbf{P}^1_Q \cap S)(\overline{\mathbf{F}}_q)| = 2$, and these two points are of the form $\psi(a_1, b_1)$ and $\psi(a_2, b_2)$, with $a_1 \neq a_2$ and $b_1 \neq b_2$.*

Proof. For $a \in \{a_1, a_2\}$, we have

$$\mathbf{P}(\ker \varphi_{x-a}) \cap S = \psi\left(\{a\} \times \mathbf{P}^1\right) \cup \psi\left(\mathbf{P}^1 \times \left\{\frac{h_0}{h_1}(a)^{1/q}\right\}\right).$$

Since the polynomial Q is irreducible, we have $a_1 \neq a_2$. Furthermore, assuming that Q is not a degenerate trap, we have $\frac{h_0}{h_1}(a_1) \notin k$, and thereby $\frac{h_0}{h_1}(a_1) \neq \frac{h_0}{h_1}(a_2)$. Therefore $\mathbf{P}^1_Q \cap S$ is equal to

$$\mathbf{P}(\ker \varphi_{x-a_1}) \cap \mathbf{P}(\ker \varphi_{x-a_2}) \cap S = \left\{\psi\left(a_1, \frac{h_0}{h_1}(a_2)^{1/q}\right), \psi\left(a_2, \frac{h_0}{h_1}(a_1)^{1/q}\right)\right\}.$$

□

In particular, when Q is not a degenerate trap, $\mathbf{P}^1_Q$ is exactly the line passing through the two points $s_1 = \psi(a_1, b_1)$ and $s_2 = \psi(a_2, b_2)$. We get a k-isomorphism $\mathbf{P}^1 \to \mathbf{P}^1_Q : \alpha \mapsto s_1 - \alpha s_2$. For this reason the two points s_1 and s_2 play a central role in the rest of the analysis, and the following proposition shows that they behave nicely when Q is a good polynomial.

Proposition 3.2. *Suppose Q is a good polynomial. Then, $(\mathbf{P}^1_Q \cap S)(\overline{\mathbf{F}}_q) = \{s_1, s_2\}$, where $s_1 = (x - a_1)(x - b_1)^q$, and $s_2 = (x - a_2)(x - b_2)^q$, and the roots a_1, a_2, b_1 and b_2 are all distinct.*

Proof. From Lemma 3.1, we can write $(\mathbf{P}^1_Q \cap S)(\overline{\mathbf{F}}_q) = \{s_1, s_2\}$ with $a_1 \neq a_2$ and $b_1 \neq b_2$. If $a_1 = b_2$ or $a_2 = b_1$, then Q divides $x^q h_1 - h_0$, a trap of level 0. Now, suppose $a_1 = b_1$ (the case $a_2 = b_2$ is similar). Since a_1 and a_2 are the two roots of Q, and Q divides $(x - a_1)(h_0 - a_1^q h_1)$, then a_2 is a root of $h_0 - a_1^q h_1$. We get that $h_0(a_2) = a_1^q h_1(a_2)$, so a_2 is a root of $h_1 x^{q^{dm+1}} - h_0$, a trap of level dm. □

4. Irreducible covers of $\mathbf{P}^1_Q$

In this section we suppose that Q is a good polynomial, and we consider the polynomials $s_1 = (x-a_1)(x-b_1)^q$ and $s_2 = (x-a_2)(x-b_2)^q$ as defined in Proposition 3.2, where a_1, a_2, b_1 and b_2 are all distinct. Consider the variety $\mathbf{P}^1_Q$ from (3.2).

Recall that our goal is to prove that a significant proportion of the polynomials of $\mathbf{P}^1_Q(k)$ splits completely over k. As mentioned in Section 1.1, our method consists in constructing a morphism $C \to \mathbf{P}^1_Q$ where C is an absolutely irreducible curve defined over k, such that the image of any k-rational point of C is a polynomial that splits completely over k. The absolute irreducibility is crucial as it implies that C has a lot of k-rational points. The idea is to consider the algebraic set

$$C = \{(u, r_1, r_2, r_3) \mid \text{the } r_i\text{'s are three distinct roots of } u\} \subset \mathbf{P}^1_Q \times \mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1,$$

and the canonical projection $C \to \mathbf{P}^1_Q$.

Proposition 4.1. *If $(u, r_1, r_2, r_3) \in C(k)$, then u splits completely over k.*

Proof. Suppose that (u, r_1, r_2, r_3) is a k-rational point of C. From Lemma 2.2, we get $u = g \star (x^q - x)$ where g is the matrix $g \in \mathrm{PGL}_2(k)$ sending the three points r_1, r_2 and r_3 to 0, 1 and ∞. In particular, the set of roots of u is $g^{-1}(\mathbf{P}^1(\mathbf{F}_q))$ which are all in $\mathbf{P}^1(k)$. □

In the rest of this section, we prove that C is absolutely irreducible (Proposition 4.6). The strategy is the following. Instead of considering directly C, which encodes three roots for each polynomial of $\mathbf{P}^1_Q$, we start with the variety

$$X = \{(u, r) \mid u(r) = 0\} \subset \mathbf{P}^1_Q \times \mathbf{P}^1,$$

which considers a single root for each polynomial. We can then "add" roots by considering fibre products. Recall that given two covers $\nu : Z \to Y$ and $\mu : Z' \to Y$, the geometric points of the fibre product $Z \times_Y Z'$ are pairs (z, z') such that $\nu(z) = \mu(z')$. In particular, the fibre product over the projection $X \to \mathbf{P}^1_Q$ is

$$\begin{aligned} X \times_{\mathbf{P}^1_Q} X &= \{((u_1, r_1), (u_2, r_2)) \mid u_1(r_1) = 0, u_2(r_2) = 0, u_1 = u_2\} \\ &\cong \{(u, r_1, r_2) \mid u(r_1) = 0, u(r_2) = 0\}. \end{aligned}$$

This product $X \times_{\mathbf{P}^1_Q} X$ contains a trivial component, the diagonal, corresponding to triples (u, r, r). The rest is referred to as the non-trivial part, and we prove that it is an absolutely irreducible curve (Corollary 4.3). Iterating this construction, the fibre product $(X \times_{\mathbf{P}^1_Q} X) \times_X (X \times_{\mathbf{P}^1_Q} X)$ (over the projection $X \times_{\mathbf{P}^1_Q} X \to X$ to the first component) encodes quadruples (u, r_1, r_2, r_3). Therefore the curve C naturally embeds into the non-trivial part of this product. We prove that this non-trivial part is itself an absolutely irreducible curve (Lemma 4.5).

Instead of the projection $X \to \mathbf{P}^1_Q$, we work with an isomorphic cover θ. It is easy to see that the canonical projection $X \to \mathbf{P}^1$ is an isomorphism, with inverse $r \mapsto (s_2(r)s_1 - s_1(r)s_2, r)$. Through the isomorphisms $X \cong \mathbf{P}^1$ and $\mathbf{P}^1_Q \cong \mathbf{P}^1$, this projection is isomorphic to the cover θ in the following commutative diagram (where, again, the morphisms are written affinely for convenience):

$$\begin{array}{ccccc} & & (u, r) & \longmapsto & u \\ (u, r) & & X & \longrightarrow & \mathbf{P}^1_Q \\ \downarrow & & \downarrow \wr & & \downarrow \wr \\ r & & \mathbf{P}^1 & \xrightarrow{\theta} & \mathbf{P}^1 \\ & & r & \longmapsto & s_1(r)/s_2(r). \end{array} \qquad \begin{array}{c} s_1 - \alpha s_2 \\ \downarrow \\ \alpha \end{array}$$

For convenience, consider θ as a cover $X_1 \to X_0$ where $X_0 = X_1 = \mathbf{P}^1$. As a first step, we study the induced fibre product $X_1 \times_{X_0} X_1$. It contains the diagonal Δ_1, isomorphic to X_1. We wish to show that $Y_2 = X_1 \times_{X_0} X_1 \setminus \Delta_1$ is absolutely irreducible. The second step consists in showing that $X_2 \times_{X_1} X_2 \setminus \Delta_2$ is also absolutely irreducible, where X_2 is a desingularisation of Y_2 and Δ_2 is the diagonal. The following lemma provides a general method used in both steps.

Lemma 4.2. *Let Y and Z be two absolutely irreducible, smooth, complete curves over k, and consider a cover $\eta : Z \to Y$. If there exists a point $a \in Z$ such that η is not ramified at a and $\#(\eta^{-1}(\eta(a))) = 2$, then $Z \times_Y Z \setminus \Delta$ is absolutely irreducible, where Δ is the diagonal component.*

Proof. By contradiction, suppose that $Z \times_Y Z \setminus \Delta$ is not absolutely irreducible, and can be decomposed as two components $A \cup B$. Let $\mathrm{pr} : Z \times_Y Z \to Z$ be the projection on the first factor. Since $Z \times_Y Z$ is complete, both A and B are

complete, so we have $\mathrm{pr}(A) = \mathrm{pr}(B) = \mathrm{pr}(\Delta) = Z$. Observe that $\mathrm{pr}^{-1}(a)$ consists of $\#(\eta^{-1}(\eta(a))) = 2$ points, so one of them must belong to two of the components A, B and Δ. That point must therefore be singular in $Z \times_Y Z$, contradicting the fact that η is not ramified at a (recall that a point $(z_1, z_2) \in Z \times_Y Z$ is singular if and only if η is ramified at both z_1 and z_2). □

Corollary 4.3. *The curve $Y_2 = X_1 \times_{X_0} X_1 \setminus \Delta_1$ is absolutely irreducible.*

Proof. First observe that θ is ramified only at b_1 and b_2 (as can be verified from the explicit formula $\theta(r) = s_1(r)/s_2(r)$). In particular, it is not ramified at a_1. Since $\#(\theta^{-1}(\theta(a_1))) = \#\{a_1, b_1\} = 2$, we apply Lemma 4.2. □

Lemma 4.4. *The desingularisation morphism $\nu : X_2 \to Y_2$ is a bijection between the geometric points.*

Proof. It is sufficient to prove that for any singular point P on Y_2, and $\varphi : \tilde{Y}_2 \to Y_2$ the blowing-up at P, the preimage $\varphi^{-1}(P)$ consists of a single smooth point. Up to a linear transformation of $X_1 = \mathbf{P}^1$, we can assume that s_1 and s_2 are of the form $s_1(x) = (x-1)x^q$ and $s_2(x) = x - a$, for some $a \neq 0, 1$. The intersection A of the curve Y_2 with the affine patch $\mathbf{A}^2 \subset \mathbf{P}^1 \times \mathbf{P}^1$ is then defined by the polynomial

$$f(x,y) = \frac{s_1(x)s_2(y) - s_1(y)s_2(x)}{x-y} = \frac{x^q(x-1)(y-a) - y^q(y-1)(x-a)}{x-y}.$$

It remains to blow up A at the singularity $(0,0)$ (which corresponds to (b_1, b_1) through the linear transformation), and check the required properties. This is easily done following [Har77, Ex. 4.9.1], and we include details for the benefit of the reader. Let $\psi : Z \to \mathbf{A}^2$ be the blowing-up of $\mathbf{A}^2$ at $(0,0)$. The inverse image of A in Z is defined in $\mathbf{A}^2 \times \mathbf{P}^1$ by the equations $f(x,y) = 0$ and $ty = xu$ (where t and u parameterize the factor $\mathbf{P}^1$). It consists of two irreducible components: the blowing-up $\tilde{A}$ of A at $(0,0)$ and the exceptional curve $\psi^{-1}(0,0)$. Suppose $t \neq 0$, so we can set $t = 1$ and use u as an affine parameter (since f is symmetric, the case $u \neq 0$ is similar). We have the affine equations $f(x,y) = 0$ and $y = xu$, and substituting we get $f(x, xu) = 0$, which factors as

$$f(x, xu) = x^{q-1}\frac{(x-1)(xu-a) - u^q(xu-1)(x-a)}{1-u}.$$

The blowing-up $\tilde{A}$ is defined on $t = 1$ by the equations $g(x,u) = f(x,xu)/x^{q-1} = 0$ and $y = xu$. It meets the exceptional line only at the point $u = 1$, which is non-singular. □

The projection $X_1 \times_{X_0} X_1 \to X_1$ on the first component induces another cover $\theta_2 : X_2 \to X_1$, through which we build the fibre product $X_2 \times_{X_1} X_2$. As above, it contains a diagonal component Δ_2 isomorphic to X_2.

Lemma 4.5. *The curve $Y_3 = X_2 \times_{X_1} X_2 \setminus \Delta_2$ is absolutely irreducible.*

Proof. Let $\nu : X_2 \to Y_2$ be the bijective morphism from Lemma 4.4. Since θ_1 is only ramified at b_1 and b_2, the cover θ_2 is ramified at most at the points $\nu^{-1}(b_i, b_i)$ and $\nu^{-1}(a_i, b_i)$ (for $i \in \{1, 2\}$). In particular, it is not ramified at $\nu^{-1}(b_1, a_1)$. Since $\#(\theta_2^{-1}(\theta_2(\nu^{-1}(b_1, a_1)))) = \#\{\nu^{-1}(b_1, a_1), \nu^{-1}(b_1, b_1)\} = 2$, we apply Lemma 4.2. □

Proposition 4.6. *The curve C is absolutely irreducible.*

Proof. Let $\nu : X_2 \to Y_2$ be the morphism from Lemma 4.4. It is an isomorphism away from the singularities of Y_2, so

$$C \longrightarrow Y_3 : (u, r_1, r_2, r_3) \longmapsto (\nu^{-1}(r_1, r_2), \nu^{-1}(r_1, r_3))$$

is a morphism. It is an embedding, and the result follows from Lemma 4.5. □

5. Counting split polynomials in $\mathbf{P}^1_Q$

Recall that we wish to prove Proposition 1.3 by showing that $\mathbf{P}^1_Q(k)$ contains a lot of polynomials that split into good polynomials over k. The results of Section 4 allow us to prove in Theorem 5.1 that a lot of polynomials in $\mathbf{P}^1_Q(k)$ do split. We then show in Proposition 5.2 that all these polynomials are coprime, which implies that bad polynomials cannot appear too often.

Theorem 5.1. *Let $k/\mathbf{F}_{q^d}$ be a field extension of degree m, and Q be a good irreducible quadratic polynomial in $k[x]$ coprime to h_1. If $dm \geq 23$, there are at least $\#k/2q^3$ polynomials in $\mathbf{P}^1_Q$ that split completely over the field k.*

Proof. Let $\Theta : Y_3 \to \mathbf{P}^1_Q$ be the cover resulting from the composition of the successive covers of Section 4. Let $S_3 = \Theta^{-1}(\mathbf{P}^1_Q \cap S)$. The embedding $C \to Y_3$ from Proposition 4.6 has image $Y_3 \setminus S_3$. The morphism

$$\mu : Y_3 \to \mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1 : (\nu^{-1}(r_1, r_2), \nu^{-1}(r_1, r_3)) \mapsto (r_1, r_2, r_3)$$

restricts to an embedding of $Y_3 \setminus S_3$. Let A be the intersection of $\mu(Y_3)$ with the affine patch $\mathbf{A}^3$. The curve A is a component of the (reducible) curve defined by the equations $\theta(r_1) = \theta(r_2)$ and $\theta(r_1) = \theta(r_3)$. Therefore A is of degree at most $4(q+1)^2$. If B is the closure of A in $\mathbf{P}^3$, then [Bac96, Th. 3.1] shows that

$$|\#B(k) - \#k - 1| \leq 16(q+1)^4\sqrt{\#k}.$$

Since Y_3 is complete, $\mu(Y_3)$ is closed, so all the points of $B \setminus A$ are at infinity, and there are at most $\deg(B) \leq 4(q+1)^2$ of them. Also, at most $2(q^3 - q)$ points of B are in $\mu(S_3)$ (because $\#S = 2$ and Θ is of degree $q^3 - q$). Therefore

$$\#C(k) = \#(Y_3 \setminus S_3)(k) \geq \#k + 1 - 16(q+1)^4\sqrt{\#k} - 4(q+1)^2 - 2(q^3 - q).$$

Since $q \geq 2$ and $dm \geq 23$, we get $\#C(k) \geq \#k/2$. From Proposition 4.1, and the fact that the map Θ is $q^3 - q$ to one, we get that at least $\#k/2q^3$ polynomials in $\mathbf{P}^1_Q$ split completely over k. □

Let φ be the morphism defined in (3.1).

Proposition 5.2. *Suppose Q is a good polynomial. For any two distinct polynomials f and g in $\mathbf{P}^1_Q(\overline{\mathbf{F}}_q)$, we have $\gcd(f, g) = 1$ and $\gcd(h_1\varphi(f), h_1\varphi(g)) = Q$.*

Proof. Let s_1 and s_2 be as in Proposition 3.2. They have no common root. Since f and g are distinct, all the polynomials of $\mathbf{P}^1_Q$ are of the form $\alpha f + \beta g$ for $(\alpha : \beta) \in \mathbf{P}^1$. Then, if r is a root of f and g, r is a root of all the polynomials of $\mathbf{P}^1_Q$. In particular, it is a root of both s_1 and s_2, a contradiction. This shows that $\gcd(f, g) = 1$.

Similarly, if a polynomial h divides $h_1\varphi(f)$ and $h_1\varphi(g)$, it must also divide both $h_1\varphi(s_1) = (x - a_1)(h_0 - b_1^q h_1)$, and $h_1\varphi(s_2) = (x - a_2)(h_0 - b_2^q h_1)$. Since $h_0 - b_1^q h_1$ and $h_0 - b_2^q h_1$ are coprime, h must divide Q. □

Proof of Proposition 1.3. As discussed in Section 1.1, it is sufficient to prove that a uniformly random element of $\mathbf{P}^1_Q(k)$ has a good probability to lead to an elimination into good polynomials. A polynomial $f \in \mathbf{P}^1_Q(k)$ leads to an elimination into good polynomials if f splits completely over k into good linear polynomials, and $\varphi(f)$ is itself a good polynomial.

Let A be the set of polynomials of $\mathbf{P}^1_Q(k)$ that split completely over k. From Theorem 5.1, A contains at least $q^{dm-3}/2$ elements. Trap roots τ occurring in A or $\varphi(A)$ must be roots of $h_1x^q - h_0$, or of $h_1x^{q^{dn+1}} - h_0$ for $n \mid m/2$, or satisfy $\frac{h_0}{h_1}(\tau) \in \mathbf{F}_{q^{dm/2}}$. There are at most $q^{\frac{dm}{2}+3}$ such trap roots. From Proposition 5.2, any trap root can only occur once in A and in $\varphi(A)$. So there are at most $2q^{\frac{dm}{2}+3}$ polynomials in A for which trap roots appear. Therefore the number of elements in A leading to a good reduction is at least

$$\frac{1}{2}q^{dm-3} - 2q^{\frac{dm}{2}+3} \geq \frac{1}{2}\left(q^{dm-3} - 4q^{dm-8}\right) \geq \frac{1}{4}q^{dm-3},$$

using $dm \geq 23$. Since $\mathbf{P}^1_Q(k)$ contains $q^{dm}+1$ elements, the probability of a random element to lead to a good elimination is $1/O(q^3)$. □

Acknowledgements

Part of this work was supported by the Swiss National Science Foundation under grant number 200021-156420.

References

[Bac96] Eric Bach, *Weil bounds for singular curves*, Applicable Algebra in Engineering, Communication and Computing **7** (1996), no. 4, 289–298.

[Die11] Claus Diem, *On the discrete logarithm problem in elliptic curves*, Compositio Mathematica **147** (2011), no. 1, 75–104.

[EG02] Andreas Enge and Pierrick Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arithmetica **102** (2002), 83–103.

[GGMZ13] Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel, *On the function field sieve and the impact of higher splitting probabilities*, Advances in Cryptology – CRYPTO 2013, Springer Berlin Heidelberg, 2013, pp. 109–128.

[GKZ18] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel, *On the discrete logarithm problem in finite fields of fixed characteristic*, Trans. Amer. Math. Soc. **270** (2018), no. 5, 3129–3145.

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Jou13] Antoine Joux, *A new index calculus algorithm with complexity* $L(1/4+o(1))$ *in small characteristic*, Selected Areas in Cryptography - SAC 2013, Lecture Notes in Computer Science, vol. 8282, Springer, 2013, pp. 355–379.

[Wan97] Daqing Wan, *Generators and irreducible polynomials over finite fields*, Mathematics of Computation **66** (1997), no. 219, 1195–1212.

École Polytechnique Fédérale de Lausanne, EPFL IC LACAL, Switzerland

HIGHER DIMENSIONAL SIEVING FOR THE NUMBER FIELD SIEVE ALGORITHMS

LAURENT GRÉMY

Abstract. Since 2016 and the introduction of the exTNFS (extended Tower Number Field Sieve) algorithm, the security of cryptosystems based on non-prime finite fields, mainly the paring and torus-based one, is being reassessed. The feasibility of the relation collection, a crucial step of the NFS variants, is especially investigated. It usually involves polynomials of degree one, i.e., a search space of dimension two. However, exTNFS uses bivariate polynomials of at least four coefficients. If sieving in dimension two is well described in the literature, sieving in higher dimension received significantly less attention. We describe and analyze three different generic algorithms to sieve in any dimension for the NFS algorithms. Our implementation shows the practicability of dimension four sieving, but the hardness of dimension six sieving.

1. Introduction

Nowadays, an important part of the deployed asymmetric cryptosystems bases its security on the hardness of two main number theory problems: the factorization of large integers and the computation of discrete logarithms in a finite cyclic group. In such a group $(G, \cdot)$ of order ℓ and generator g, the *discrete logarithm problem* (DLP) is, given $a \in G$, to find $x \in [0, \ell)$ such that $g^x = a$. Usual choices of group are groups of points on elliptic curves or multiplicative subgroups of finite fields.

In this article, we focus on discrete logarithms in finite fields of the form $\mathbb{F}_{p^n}$, where p is a prime and n is relatively small, namely the medium and large characteristics situation studied in [22]. Computing discrete logarithms in this type of field can affect torus-based [29, 36] or pairing-based [12] cryptography. The best known algorithm to achieve computations in such groups is the *number field sieve* (NFS) algorithm. It has a subexponential complexity, often expressed with the $L(\alpha)$ notation: $L_{p^n}(\alpha, c) = \exp\left[(c + o(1)) \log(p^n)^\alpha \log\log(p^n)^{1-\alpha}\right]$, where $\alpha = 1/3$ for all the variants of NFS. For the general setting in medium characteristic, the first $L(1/3)$ algorithm was reached with $c = 2.43$ [22], improved to 2.21 [4] and now to 1.93 with exTNFS [23], the same complexity as NFS in large characteristic. In some specific context, exTNFS even reaches a lower complexity. However, theoretical complexities are not enough to estimate what would cost a real attack, since practical improvements can be hidden in the $o(1)$ term [1, 30, 7]. Experimental results are then needed to assess the concrete limits of known algorithms.

On the practical side, there has been a lot of effort to compute discrete logarithms in prime fields, culminating in a 768-bit record [27]. Although the records for $\mathbb{F}_{p^2}$ are smaller than the ones in prime fields, the computations turned out to be

Laurent Grémy was supported by the ERC Starting Grant ERC-2013-StG-335086-LATTAC. His work was started in the CARAMBA team of Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France and completed in the AriC team.

faster than expected [4]. However, when n is a small composite and p fits for $\mathbb{F}_{p^n}$ to be in the medium characteristic case (typically $n = 6$ [16] and $n = 12$ [18]), the records are smaller, even with a comparable amount of time spent during the computation. A way to fill the gap between medium and large characteristics is to implement exTNFS, since the computations in medium characteristic were, until now, performed with a predecessor of exTNFS.

Since exTNFS is a relatively new algorithm, there remain many theoretical and practical challenges to be solved before a practical computation can be reached. One of the major challenges concerns the sieve algorithms which efficiently perform the relation collection, one of the most costly steps of NFS. However, if there exist sieve algorithms in dimension two and three, these sieves are not efficient for higher dimension and exTNFS needs to sieve in even dimension larger or equal to four.

Our contributions. We describe three new generic sieve algorithms which deal with any dimension, especially those addressed by exTNFS. Instantiating these algorithms in dimension two or three may allow to recover the existing sieve algorithms. Since these new sieves do not ensure completeness of the enumeration, unlike most of the existing sieve algorithms, we describe workarounds to ensure a trade-off between the completeness and the running time efficiency. Finally, we analyze some quality criteria of these sieve algorithms and show the feasibility of sieving in dimension four, but the hardness of dimension six sieving.

2. Overview of the NFS algorithms

Let ℓ be a large prime factor of the order $\Phi_n(p)$ of $\mathbb{F}_{p^n}^*$ that is coprime to $\Phi_k(p)$ for all prime factors k of n: the Pohlig–Hellman algorithm allows to reduce the DLP in $\mathbb{F}_{p^n}^*$ to the DLP in all its subgroups, especially the one of order ℓ. The NFS algorithms can be split into four main steps: *polynomial selection*, *relation collection*, *linear algebra* and *individual logarithm*. The first step defines in a convenient way the field $\mathbb{F}_{p^n}$. The next two steps find the discrete logarithms of a subset of *small to medium* elements of $\mathbb{F}_{p^n}$, where sizes of the elements will be defined later. The last step computes the discrete logarithm of a *large* element of $\mathbb{F}_{p^n}$. The overall complexity of NFS is dominated by the relation collection and the linear algebra.

2.1. **Polynomial selection.** Let $n = \eta\kappa$: the field $\mathbb{F}_{p^n}$ can be represented as a degree-κ extension of $\mathbb{F}_{p^\eta}$. Let h be an integer polynomial of degree η irreducible over $\mathbb{F}_p$ and ι be a root of h. Let $\mathbb{F}_{p^\eta}$ be defined by R/pR, where R is the ring $\mathbb{Z}[y]/h(y)$. There exist two ring homomorphisms from $R[x] = \mathbb{Z}[\iota][x]$ to $\mathbb{F}_{p^n}$: one of them involves a number field K_0 (respectively K_1) defined by f_0 (respectively f_1). The polynomials f_0 and f_1 are irreducible over R and share a common irreducible factor ϕ of degree κ modulo p. This setting allows to define $\mathbb{F}_{p^n} = \mathbb{F}_{(p^\eta)^\kappa} \approx (R/pR)[x]/\phi(x)$. This provides the commutative diagram of Figure 1. The different polynomial selections defining f_0 and f_1 are given in Figure 2.

2.2. **Relation collection.** Since the diagram of Figure 1 is the same for all the NFS variants, we use in the following the name NFS_η to cover all the variants (see Table 1 for their names) or NFS when the parameter η does not matter.

2.2.1. *Relation.* A relation in NFS is given by a polynomial $a(x, y)$ in $R[x]$ of degree μ in x, often set to $\mu = 1$ to reach the best complexity (see Table 1), and $\eta - 1$ in y. Since there are $t = (\mu + 1)\eta$ coefficients to define a polynomial a, the relation collection is done in *dimension* t. A polynomial a gives a relation when the ideal

18 May 2018 09:47:52 PDT
Version 5 - Submitted to Open Book Series

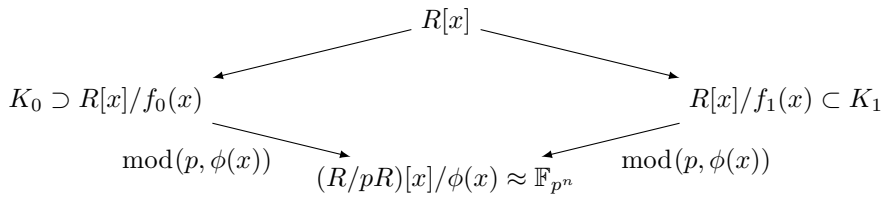


FIGURE 1. The NFS diagram to compute discrete logarithms in $\mathbb{F}_{p^n}$.

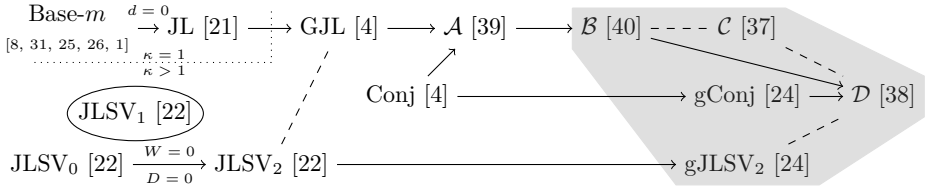


FIGURE 2. Polynomial selections: a link $a \to b$ means that a is a particular case of b (getting a from b is written if this is not explicit in the articles); a dashed link means that the selection strategies in a and b strongly resemble. Polynomial selections in the gray area allow to build polynomial with algebraic coefficients.

factorizations of a mapped in both number fields involve prime ideals of norms smaller than two $L(1/3)$ smoothness bounds B_0 and B_1 respectively: such ideals are elements of the so-called factor bases $\mathcal{F}_0$ and $\mathcal{F}_1$ respectively, see [22, 5, 23].

Since the factorization of a in prime ideals and the factorization of the norm of a are strongly linked, the relation collection looks for polynomials a of norms B_0-smooth in K_0 and B_1-smooth in K_1. To ensure the best probability of smoothness, the t coefficients $\boldsymbol{a}$ of a are taken into a *t-search space* $\mathcal{S}$ containing $L(1/3)$ elements. Since an upper bound of the norm of a involves its infinity norm [6], the search spaces are usually cuboids of form $\mathcal{S} = [S_0^m, S_0^M) \times [S_1^m, S_1^M) \times \cdots \times [S_{t-1}^m, S_{t-1}^M)$, where $\mathbf{0}$ is in $\mathcal{S}$, all the $[S_i^m, S_i^M)$ are integer intervals and $S_i^M = -S_i^m$, where i is in $[0, t)$. Theoretically, all the S_i^M are equal but practically, the skewness of the polynomials f_0 and f_1 must be taken into account [31, 25, 26, 1], implying a skew search space. Since $-a$ and a give the same relation, $S_{t-1}^m = 0$. By abuse of notation, we denote by a both the polynomial and the list $\boldsymbol{a}$ of its t coefficients.

	$\kappa = 1$	$\kappa \geq 1$
$\eta = 1$	NFS	NFS-HD
$\eta \geq 1$	TNFS	exTNFS

(A) Name of the NFS variants.

	$\kappa = 1$	$\kappa \geq 1$
$\eta = 1$		$\mu \geq 1$
$\eta \geq 1$	$\mu = 1$	

(B) Optimal degree.

TABLE 1. The different variants of NFS.

2.2.2. *Practical considerations.* To ensure the best running time for the relation collection, the polynomials f_0 and f_1 must be chosen carefully. However, the two

usual quality criteria, especially the α but also the Murphy-E functions [31], are only defined for NFS_1 and $\mu \leq 3$ [14]. Finding good polynomials for $\text{NFS}_{>1}$, even by settling for integer coefficients to define f_0 and f_1, is yet a challenge.

The goal of the relation collection is to produce more relations than the number of ideals in both factor bases. A classical algorithm, used to analyze theoretically NFS, tests the smoothness of the norms of a in $\mathcal{S}$ by using the *elliptic curve method* (ECM) algorithm. However, if this algorithm is almost memory-free, the practical running time of such a task is prohibitive.

Instead, the common practical way is to perform ECM only on promising polynomials a, i.e., polynomials whose norms have many small factors. Finding these small factors is efficiently performed thanks to arithmetic sieve algorithms. However, sieve algorithms need a huge memory-footprint, since they need to store the norms of all the elements of $\mathcal{S}$. This problem was tackled in [33], allowing moreover a high-level parallelization, by considering many subsets of polynomial: in one number field, say K_0, the factorization into prime ideals of these polynomials involved at least an enforced ideal of medium size. Let $\mathfrak{Q}$ be such an ideal, called special-$\mathfrak{Q}$. Polynomials a such that $\mathfrak{Q}$ appears into their ideal factorization in K_0 are elements of a lattice, called $\mathfrak{Q}$-lattice, a basis of which is given by the rows of the matrix $M_{\mathfrak{Q}}$. To consider only polynomials fitting into $\mathcal{S}$, sieves look for elements $\boldsymbol{c}$ in the intersection of the $\mathfrak{Q}$-lattice and a t-search space $\mathcal{H} = [H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \cdots \times [0, H_{t-1}^M)$: a is obtained from $\boldsymbol{c}M_{\mathfrak{Q}}$. If theoretically $\mathcal{H}$ should depend on $\mathfrak{Q}$, it is often the same for all the special-$\mathfrak{Q}$s. In this intersection, sieve algorithms remove the contribution of small ideals. Let $\mathfrak{R}$ be such an ideal of prime norm r. Except for a tiny number of such ideals, a basis of the $\mathfrak{R}$-lattice in the $\mathfrak{Q}$-lattice can be of the form

$$\begin{aligned}(1)\quad \{(r,0,0,\ldots,0),(\lambda_{0,\mathfrak{Q},\mathfrak{R}},1,0,0,\ldots,0),(\lambda_{1,\mathfrak{Q},\mathfrak{R}},0,1,0,0,\ldots,0),\ldots,\\ (\lambda_{t-2,\mathfrak{Q},\mathfrak{R}},0,0,\ldots,0,1)\} = \{\boldsymbol{b_0},\boldsymbol{b_1},\boldsymbol{b_2},\ldots,\boldsymbol{b_{t-1}}\},\end{aligned}$$

where the $\lambda_{i,\mathfrak{Q},\mathfrak{R}}$ are integers in $[0,r)$. Briefly, the different steps of the relation collection with the *special-$\mathfrak{Q}$-method* and sieving algorithms are as follows:

- For all the possible special-$\mathfrak{Q}$s
  1. For both sides i in $[0,1]$
     (a) Compute the norms $N_i[\boldsymbol{c}]$ of $a = \boldsymbol{c}M_{\mathfrak{Q}}$, where $\boldsymbol{c}$ is in $\mathcal{H}$.
     (b) For all the ideals $\mathfrak{R}$ to be sieved, enumerate the elements $\boldsymbol{c}$ in $\mathcal{H} \cap \Lambda_{\mathfrak{Q}\mathfrak{R}}$ and remove the contribution of $\mathfrak{R}$ from $N_i[\boldsymbol{c}]$.
  2. If both $N_0[\boldsymbol{c}]$ and $N_1[\boldsymbol{c}]$ are sufficiently small to have a chance to give a relation, factorize the norms of a and report a if a gives a relation.

However, if there exist generic sieve algorithms in any dimension (see Section 3), they are not very efficient when $t \geq 4$ that especially arises with $\text{NFS}_{>1}$. We propose algorithms for these cases in Section 4. Note that we will use the term sieve algorithms, but we only focus on the enumeration part of them, which is Step 1b without updating the array N_i. Step 1a is briefly addressed in Section 5.

2.3. **Linear algebra and individual logarithm.** Let θ_0 (respectively θ_1) be a root of f_0 (respectively f_1). Let a be a polynomial that gives a relation, i.e., $\langle a(\theta_k,\iota)\rangle = \prod_{\mathfrak{R}\in\mathcal{F}_k} \mathfrak{R}^{\text{val}_{\mathfrak{R}}(a(\theta_k,\iota))}$, where k is in $[0,1]$ and val denotes the valuation: the factorizations of the norms of a must be translated into such a factorization of ideals [9]. A relation can be transformed into a linear relation involving the virtual logarithms (vlog) of the ideals [42]. To be valid, this linear relation must

involve the Schirokauer maps ϵ_k [41], as $\sum_{\mathfrak{R}\in\mathcal{F}_0} \mathrm{val}_{\mathfrak{R}}(a(\theta_k,\iota))\,\mathrm{vlog}(\mathfrak{R}) + \epsilon_0(a) = \sum_{\mathfrak{R}\in\mathcal{F}_1} \mathrm{val}_{\mathfrak{R}}(a(\theta_k,\iota))\,\mathrm{vlog}(\mathfrak{R}) + \epsilon_1(a) \mod \ell$. In this equation, the virtual logarithms are unknowns, the valuations are small integers and the Schirokauer maps are large integers, close to ℓ. These large elements negatively impact the usual algorithms to solve sparse systems, but the cost of these heavy parts can be significantly decreased thanks to a modification of the block Wiedemann algorithm [10, 20, 13].

The last step of the computation is the computation of a large, say $L(1)$, unknown logarithm. This computation is achieved by rewriting the (virtual) logarithm of the target in terms of logarithms of smaller elements; these smaller elements are again rewritten in terms of smaller elements until the logarithm of the target has been rewritten using only the precomputed logarithms given by the relation collection and the linear algebra. This *descent step* uses different algorithms depending on the size of the rewritten element: the target is rewritten in elements up to $L(2/3)$ thanks to the so-called initial splitting (booting step) [34, 21, 2, 17, 45]; for elements in $[L(1/3), L(2/3))$, the special-$\mathfrak{Q}$-method is used. The theoretical analysis of [13, Appendix A.2] shows that the descent by special-$\mathfrak{Q}$ may be more efficient by considering polynomials of degree not restricted to $\mu = 1$.

3. A framework to study existing sieve algorithms

Let $\mathfrak{Q}$ be a special-$\mathfrak{Q}$ and $\mathfrak{R}$ be an ideal to be sieved such that the lattice $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ is given by a basis as in Equation (1)[1]. There exist different sieve algorithms proposed for NFS that allow to enumerate the elements in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and a search space $\mathcal{H}$. Their efficiency depends on the dimension of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and the density of the lattice in $\mathcal{H}$. This density is formally defined thanks to the *level* of a sieve algorithm in Definition 3.1, a key notion for the rest of the description and especially for Section 4. All the existing sieve algorithms used in NFS are reported in Table 2. These algorithms can be described by the following two-step algorithm. The vectors produced in Step 2 will be called *transition-vectors*:

(1) Compute an adapted set $\mathcal{B}$ of spanning vectors of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ with respect to $\mathcal{H}$.
(2) Start from $\mathbf{0}$ and use the vectors of $\mathcal{B}$ or a (often small) linear combination of them to enumerate elements in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $\mathcal{H}$.

Definition 3.1 (Level)**.** Let Λ be a lattice and $\mathcal{H}$ be a search space. The level of a sieve algorithm with respect to Λ and $\mathcal{H}$ is the minimal integer value $\ell < t$ such that the intersections of the cuboids $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \cdots \times [H_\ell^m, H_\ell^M) \times \{c_{\ell+1}\} \times \{c_{\ell+2}\} \times \cdots \times \{c_{t-1}\}$, where $(c_{\ell+1}, c_{\ell+2}, \ldots, c_{t-1})$ are in $[H_{\ell+1}^m, H_{\ell+1}^M) \times [H_{\ell+2}^m, H_{\ell+2}^M) \times \cdots \times [H_{t-1}^m, H_{t-1}^M)$, and the lattice Λ contains more than one element on average. In case $\mathcal{H}$ contains less than one element on average, $\ell = t - 1$.

3.1. Exhaustive sieve algorithms.

The first use of a sieve algorithm in an index calculus context is attributed to Schroeppel and was successfully used by Pomerance [35, 28]. They used the one-dimensional sieve of Eratosthenes as a factoring algorithm instead of a prime detecting one. It was extended to any dimension and called *line sieve*, see for example its use in dimension three in [44]. In dimension two, the line sieve is known to be inefficient when there is at most one element in a line, an intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $[H_0^m, H_0^M) \times \{c_1\}$ where c_1 is in $\mathbb{Z}$: the 0-level line sieve is used as a 1-level sieve algorithm. Pollard designed in this sense the *sieve by*

[1]Sieve algorithms can deal with other basis shapes of lattices, but this one occurs the most.

vectors [33], now subsumed by the *lattice sieve* of Franke and Kleinjung [11]. Based on this sieve algorithm, the *plane sieve* [14] and the *3-dimensional lattice sieve* [19] were proposed for similar densities in three dimensions. The plane sieve was turned into a generic sieve algorithm in CADO-NFS [43] (see Section 4.4).

The completeness of all these sieve algorithms comes from special procedures that compute transition-vectors. They are defined thanks to the *t-extended search spaces*: let k be in $[0, t)$ and $\mathcal{H}$ be a t-search space, the t-extended search space $\mathcal{H}_k$ is the set $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \cdots \times [H_k^m, H_k^M) \times \mathbb{Z}^{t-(k+1)}$.

Definition 3.2 (Transition-vector)**.** Let k be in $[0, t)$ and $\mathcal{H}$ be a t-search space. A k–transition-vector is an element $\boldsymbol{v} \neq \mathbf{0}$ of a lattice Λ such that there exist $\boldsymbol{c}$ and $\boldsymbol{d}$ in the intersection of Λ and the t-extended search space $\mathcal{H}_k$, where $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{v}$ is such that the $t - 1 - k$ last coordinates of $\boldsymbol{c}$ and $\boldsymbol{d}$ are equal and the coordinate $\boldsymbol{d}[k]$ is the smallest possible larger than $\boldsymbol{c}[k]$.

With such sieve algorithms, the small factors of both norms of all the considered polynomials a are known: this allows to be close to the expected number of relations at the end of the relation collection. But, the number of relations is not the only efficiency criterion of the relation collection. Indeed, in dimension two, the lattice sieve is used since it allows to maintain the same number of relations but decrease the time per relation. The same occurs in dimension three, switching from the line to the plane or the 3D-lattice sieves. However, these sieves have some drawbacks, highlighted when there is less than one element on average in each plane $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times \{c_2\}$, where c_2 is in $[H_2^m, H_2^M)$. The plane sieve is essentially the use of the lattice sieve on each plane: even if there is no element in a plane, the lattice sieve is used to report nothing instead of using it only on non empty planes. There is no alternative to avoid these useless uses without losing completeness. The 3D-lattice sieve does not have this drawback, but the procedure to generate the spanning list $\mathcal{B}$ and the one to enumerate seem difficult to analyze and may be costly for skewed lattices or skewed search spaces.

3.2. **Heuristic sieve algorithms.** Because of these drawbacks and especially the penalty in terms of running time, the designers of the plane sieve proposed a heuristic sieve algorithm, the *space sieve* [14]. Its use allows to decrease the running time by 45% for the 240 bits example of [14], while at the same time losing less than 6% of the relations. This corresponds to decrease the time per relation by 42%.

	Line sieve	Lattice sieve [11]	3-dimensional lattice sieve [19]	Plane sieve [14]	Space sieve [14]	This work
$t = 2$	✓	✓	✗	✗	✗	✓
$t = 3$	✓	✗	✓	✓	✓	✓
$t > 3$	✓	✗	✗	✓	✗	✓
Level	$\ell = 0$	$\ell = 1$	$\ell = 1$ and $\ell = 2$	$\ell = 1$	$\ell = 2$	Any
Completeness of enumeration	✓	✓	✓	✓	✗	✗

TABLE 2. Characteristics of the sieve algorithms proposed for NFS.

The space sieve focuses on enumerating a large portion of the elements instead of all of them, which is helpful for multiple reasons. First, all the sieve algorithms, both exhaustive and heuristic, allow to enumerate the t-extended search space $\mathcal{H}_{t-2}$

instead of the search space $\mathcal{H} = \mathcal{H}_{t-1}$. For exhaustive sieves, it implies that the spanning set $\mathcal{B}$ is qualitatively too accurate because it allows to generate transition-vectors that will never be used. If this accuracy implies a costly computation to find an adapted set $\mathcal{B}$, the time per relation can be drastically impacted. Secondly, completeness is not always useful, since this reports hits on polynomials a that will give relations or not: missing some hits may not affect the number of relations in some circumstances. Furthermore, if the computation can be completed, the expected gain in the time per relation must be considered to compare heuristic and exhaustive sieves, even if the relation collection misses some relations. Finally, in dimension larger than three, the use of heuristic sieve seems unavoidable: to the best of our knowledge, producing all the transition-vectors can only be computed by the exhaustive sieve algorithms, all of them being inefficient when there is less than one element in $[H_0^m, H_0^M) \times [H_1^m, H_1^M) \times [H_2^m, H_2^M) \times \{c_3\} \times \{c_4\} \times \cdots \times \{c_{t-1}\}$, where c_i is in $[H_i^m, H_i^M)$. Yielding to produce some transition-vectors can be done by computing Graver basis of the lattice: these transition-vectors may lead to build a generic exhaustive sieve algorithm from the heuristic one described in Section 4. However, computing Graver basis is often too costly in our context [15, 32].

In the following, we propose `globalntv`, `localntv` and `sparsentv`, three heuristic sieves which perform the enumeration in any dimensions and levels.

4. Sieve algorithms in higher dimensions

Using transition-vectors implies that the sieve enumerations are exhaustive. Since completeness is not the main target of `globalntv`, `localntv` and `sparsentv`, the vectors used in Step 2 of Section 3, called here *nearly-transition-vectors*, will be weakened by removing from Definition 3.2 the strong condition about $\boldsymbol{d}[k]$.

Definition 4.1 (Nearly-transition-vector)**.** Let k be in $[0, t)$ and $\mathcal{H}$ be a t-search space. A k–nearly-transition-vector is an element $\boldsymbol{v} \neq \boldsymbol{0}$ of a lattice Λ such that there exist $\boldsymbol{c}$ and $\boldsymbol{d}$ in the intersection of Λ and the t-extended search space $\mathcal{H}_k$, where $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{v}$ is such that the $t-1-k$ last coordinates of $\boldsymbol{c}$ and $\boldsymbol{d}$ are equal and the coordinate $\boldsymbol{d}[k]$ is larger than $\boldsymbol{c}[k]$.[2]

The three generic sieve algorithms will take place in a general framework, described by allowing the report of duplicated elements for simplicity in Algorithm 1. It is purposely vague, to be as general as possible: instantiation examples of **Initialization**, Step 1c and Step 1d will be given in the following.

The addition of a possible nearly-transition-vector (Step 1c) is likewise performed for all the three sieve algorithms. Like the addition of a 2–nearly-transition-vector in the space sieve [14], a loop iterate the list of k–nearly-transition-vectors, beforehand sorted by increasing coordinate k (see Section 4.3). We also choose to use the same fall-back strategy (Step 1d): this choice is justified in Section 4.2. Therefore, the difference between the three sieve algorithms only comes from the initialization processes, described in Section 4.1.

4.1. Initializations.

To define the three initialization processes, we introduce two new notions: the *shape* of the nearly-transition-vectors and the *skew-small-vectors*.

[2]Note that transition vectors of [14, Definition 5] are 2–nearly-transition-vectors.

Initialization: Call a procedure that returns nearly-transition-vectors with respect to a search space $\mathcal{H}$ and a lattice $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ described as in Equation (1). Set $\boldsymbol{c}$ to $\mathbf{0}$ and k to $t-1$.

Enumeration:

(1) While $\boldsymbol{c}[k] < H_k^M$:
   (a) Report $\boldsymbol{c}$.
   (b) If $k > 0$, call this enumeration procedure recursively with inputs $\boldsymbol{c}$ and $k-1$.
   (c) Find a k–nearly-transition-vector $\boldsymbol{v}$ from the one computed during **Initialization**, such that adding $\boldsymbol{v}$ to $\boldsymbol{c}$ lands in the extended search space $\mathcal{H}_{k-1}$ and $\boldsymbol{c}[k]$ is the smallest possible.
   (d) If there does not exist such a k–nearly-transition-vector $\boldsymbol{v}$, call a *fall-back strategy* that tried to produce a new element $\boldsymbol{c}$ in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$, and therefore a new k–nearly-transition-vector.
(2) Recover $\boldsymbol{c}$ as it was when the procedure was called.
(3) While $\boldsymbol{c}[k] \geq H_k^m$, perform Step 1a, Step 1b, Step 1c and Step 1d by considering $\boldsymbol{c} - \boldsymbol{v}$ instead of $\boldsymbol{c} + \boldsymbol{v}$.

ALGORITHM 1. Framework for `globalntv`, `localntv` and `sparsentv`.

4.1.1. *Preliminaries.* Even if the three initialization processes are different, the shapes of the nearly-transition-vectors are the same. The shape represents the expected magnitude of the coefficients of the nearly-transition-vectors with respect to a search space $\mathcal{H}$ and $\Lambda_{\mathfrak{Q}\mathfrak{R}}$. In this paragraph, the $O(j)$ notation will denote a value smaller or almost equal to j. Let us recall the shape of the transition-vectors of the ℓ-level sieve algorithms in three dimensions. Let I_i be the length of the interval $[H_i^m, H_i^M)$. When $\ell = 0$, the shape is equal to $(O(r), O(1), O(1))$; the one for $\ell = 1$ is $(O(I_0), O(r/I_0), O(1))$; the one for $\ell = 2$ is $(O(I_0), O(I_1), O(r/(I_0 I_1)))$. This shape is generalized, as $(I_0, I_1, \ldots, I_{\ell-1}, r/(I_0 \times I_1 \times \cdots \times I_{\ell-1}), 1, 1, \ldots, 1)$, given a level ℓ of a sieve algorithm and removing the $O(\cdot)$ for clarity.

The initialization processes of the three sieve algorithms does not ensure that the produced vectors are nearly-transition-vectors. They build skew-small-vectors, that are lattice vectors whose coefficients try to follow the shape. Even if Definition 4.2 will not capture it, skew-small-vectors are build to be almost nearly-transition-vectors: a k–skew-small-vector $\boldsymbol{v}$ is a k–nearly-transition-vector if $|\boldsymbol{v}[i]| < I_i$.

Definition 4.2 (Skew-small-vector)**.** Let k be in $[0, t)$. A k–skew-small-vector is an element $\boldsymbol{v} \neq \mathbf{0}$ of a lattice Λ such that there exist $\boldsymbol{c}$ and $\boldsymbol{d}$ in Λ, where $\boldsymbol{d} = \boldsymbol{c} + \boldsymbol{v}$ is such that the $t - 1 - k$ last coordinates of $\boldsymbol{c}$ and $\boldsymbol{d}$ are equal and the coordinate $\boldsymbol{d}[k]$ is larger than $\boldsymbol{c}[k]$.

4.1.2. *Three initialization processes.* The three initialization processes try to generate a large number of nearly-transition-vectors, given the level ℓ of the sieve algorithms. They begin by building a basis $\mathcal{B}$ of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ whose basis vectors are skew-small-vectors. Nearly-transition-vectors are afterwards build thanks to small linear combination of the basis vectors. The major difference between `globalntv` on the one hand, and `localntv` and `sparsentv` on the other is about the coefficients of the k–skew-small-vectors, where $k > \ell$. In `localntv` and `sparsentv`, the coordinate k is enforced to 1, and even to 0 for the coordinates $\ell + 1$ to $k - 1$ in `sparsentv`.

This comes from a crude interpretation of the magnitude of the coefficients given by the shape. To build the k–skew-small-vectors, where $k \leq \ell$ for `localntv` and `sparsentv` or all of them for `globalntv`, the initialization processes compute a skew basis of a (sub)lattice, that is a basis formed by skew-small-vectors. The basis $\mathcal{B}$ is build thanks to:

- a skew basis reduction of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{t-1}}\}$ for `globalntv`;
- a skew basis reduction of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ followed by, for k in $[\ell+1, t)$, a reduction of $\boldsymbol{b_k}$ by its closest vector in $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$ for `localntv`;
- a skew basis reduction of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ followed by, for k in $[\ell+1, t)$, a reduction of $\boldsymbol{b_k}$ by its closest vector in $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ for `sparsentv`.

To build possible nearly-transition-vectors, linear combinations of the skew basis vectors are performed, as well as computations of some vectors close to $\boldsymbol{b_k}$ in the corresponding sublattice instead of one for `localntv` and `sparsentv`. The patterns of the skew-small-vectors produced by the different initializations follow necessarily the ones reported in Table 3. Note that, when $\ell = t-2$, `localntv` and `sparsentv` have the same initialization processes. When $\ell = t-1$, the three initialization processes are the same.

k	`globalntv`	`localntv`	`sparsentv`
0	$(>0,0,0,0,0)$	$(>0,0,0,0,0)$	$(>0,0,0,0,0)$
1	$(\cdot,>0,0,0,0)$	$(\cdot,>0,0,0,0)$	$(\cdot,>0,0,0,0)$
2	$(\cdot,\cdot,>0,0,0)$	$(\cdot,\cdot,>0,0,0)$	$(\cdot,\cdot,>0,0,0)$
3	$(\cdot,\cdot,\cdot,>0,0)$	$(\cdot,\cdot,\cdot,1,0)$	$(\cdot,\cdot,\cdot,1,0)$
4	$(\cdot,\cdot,\cdot,\cdot,>0)$	$(\cdot,\cdot,\cdot,\cdot,1)$	$(\cdot,\cdot,\cdot,0,1)$

TABLE 3. Patterns of the k–skew-small-vectors, where $\ell = 2$ and $t = 5$.

4.2. **A common fall-back strategy.** At this step, all the additions to $\boldsymbol{c}$ in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$ of a k–nearly-transition-vector fail to land in $\mathcal{H}_{k-1}$. The additions of $\boldsymbol{v}$, a k–skew-small-vector, are necessarily out of $\mathcal{H}_{k-1}$. Since no k–skew-small-vector allows to stay in $\mathcal{H}_{k-1}$, a possible k–nearly-transition-vector must have some smaller coordinates. Vectors close to $\boldsymbol{c}+\boldsymbol{v}$ in the sublattice formed by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$ may allow from $\boldsymbol{c}+\boldsymbol{v}$ to obtain such a k–nearly-transition-vector. Let $\boldsymbol{e}$ be such a vector: subtract $\boldsymbol{e}$ to $\boldsymbol{c}+\boldsymbol{v}$ will shrink the k first coefficients of $\boldsymbol{c}+\boldsymbol{v}$. If $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ fits in the search space, $\boldsymbol{v}-\boldsymbol{e}$ is a new k–nearly-transition-vector. If not, set $\boldsymbol{c}$ to $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ and rerun this procedure, until $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ fits in $\mathcal{H}$ or its coordinate k is larger than H_k^M. The different steps of this fall-back strategy are, $\boldsymbol{c}$ in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$ and k in $[0, t)$:

(1) While $\boldsymbol{c}[k] < H_k^M$
  (a) For all k–skew-small-vectors $\boldsymbol{v}$
    (i) Compute some vectors close to $\boldsymbol{c}+\boldsymbol{v}$ in the sublattice generated by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$ and store them in the list E.
    (ii) For all $\boldsymbol{e}$ in E, return $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ if $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ is in $\mathcal{H}$.
  (b) Set $\boldsymbol{c}$ to one of the vector $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ computed previously.
(2) Return fail.

If this procedure does not fail, the new element in $\mathcal{H}$ is the output of this procedure and $\boldsymbol{v}-\boldsymbol{e}$ is the new k–nearly-transition-vector, computed by the difference

between the output and the input vectors of the fall-back procedure and inserted in the lists of k–nearly-transition-vectors and k–skew-small-vectors for further use.

This fall-back strategy is costly since it requires to solve a or multiple closest vector problem instances in Step 1(a)i, iterate all the k–skew-small-vectors and loop while H_k^M is not reached. The condition to use such a strategy must therefore be carefully studied. If $k \leq \ell$, the average number of elements with the same $(t-k-1)$th last coordinate is equal to one, from the Definition 3.1 of the level. If no precomputed k–nearly-transition-vectors allows to find a new element in $\mathcal{H}$, then, most likely, there do not exist such elements. However, if $k > \ell$, there are generically more chances that such an element exists. The fall-back strategy is therefore applied only when $k > \ell$. This condition must be study a little bit more carefully. If $\ell = t-1$, the $t-1$ first coordinates of $\boldsymbol{c}+\boldsymbol{v}$ out of $\mathcal{H}$ must be shrunk, where $\boldsymbol{v}$ is a ℓ–skew-small-vector. Therefore, when $k = t-1$, the close vector $\boldsymbol{e}$ is a linear combination of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{t-2}}\}$. Since this strategy allows to modify the maximal number of coordinates without changing the last non-zero one, the strategy allows to increase the chance to find a new element. Another strategy is proposed in Section 4.4, but is specific to `sparsentv`.

4.3. **Formal algorithms.** The pseudo-code of the addition of a nearly-transition-vector and the fall-back strategy are given respectively in Function `add` and in Function `fbadd`. They return an element in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $\mathcal{H}$ or an element out of $\mathcal{H}$ to stop the enumeration of a subset of $\mathcal{H}$. The lists T and S consist of t lists containing respectively nearly-transition-vectors and skew-small-vectors (e.g., k–nearly-transition-vectors are stored in $T[k]$). Each list $T[k]$ and $S[k]$ are sorted by increasing coordinate k. Given an element $\boldsymbol{c}$ of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and an integer i, the function `CVA` (Close Vectors Around a targeted element) returns a list of some lattice vectors close to $\boldsymbol{c}$ in the sublattice of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ generated by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_i}\}$.

```
FUNC. add(c, k, H, T, S, Λ_QR, ℓ)
  for v ∈ T[k] do
    if c + v ∈ H_{k-1} then return c + v;
  if k > ℓ or k = t − 1 then
    e ← fbadd(c, k, H, S, Λ_QR);
    if e ∈ H then
      T[k] ← T[k] ∪ {e − c};
      S[k] ← S[k] ∪ {e − c};
    c ← e;
  else
    c ← (H_0^M, H_1^M, ..., H_{t-1}^M);  // ∉ H
  return c;
```

```
FUNC. fbadd(c, k, H, S, Λ_QR)
while c[k] < H_k^M do
    L ← ∅;
    for v ∈ S[k] do
      E ← CVA(c + v, k − 1, Λ_QR);
      for e ∈ E do
        if c + v − e ∈ H then
          return c + v − e;
        L ← L ∪ {c + v − e};
    set c to an element of L;
return c;                          // ∉ H
```

4.4. **A specific fall-back strategy.** Unlike the previous fall-back strategy, we describe here a specific one which allows to recover all the sieve algorithms of Section 3. This specific fall-back strategy is designed for `sparsentv` by exploiting the specific patterns of the skew-small-vectors of `sparsentv`. It can be more costly but can report a larger number of elements. To completely recover exhaustive sieve algorithms, the k–skew-small-vectors used in the sieve algorithms must have their coordinate k equal to 1, when $k > \ell$.

When the fall-back strategy is called, the coefficient of $\boldsymbol{c}+\boldsymbol{v}$, where $\boldsymbol{c}$ is in $\Lambda_{\mathfrak{Q}\mathfrak{R}} \cap \mathcal{H}$ and $\boldsymbol{v}$ is a k–skew-small-vector, are shrunk with vectors close to $\boldsymbol{c}+\boldsymbol{v}$ in

the sublattice generated by $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_\ell}\}$ instead of $\{\boldsymbol{b_0}, \boldsymbol{b_1}, \ldots, \boldsymbol{b_{k-1}}\}$, to keep unchanged the coordinates $\ell+1$ to $t-1$ of $\boldsymbol{c}+\boldsymbol{v}$. Let $\boldsymbol{e}$ be a vector subtracted to $\boldsymbol{c}+\boldsymbol{v}$ to shrink its coefficients. If $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ fits in $\mathcal{H}$, a new element in the intersection of $\Lambda_{\mathfrak{Q}\mathfrak{R}}$ and $\mathcal{H}$ is found, as well as a new k–nearly-transition-vector.

If $k > \ell+1$, the coordinates $\ell+1$ to $k-1$ of $\boldsymbol{c}$ have not been modified, and therefore, some cuboids of dimension $\ell+1$ were not explored to try to find a new starting point: to explore them, this procedure must be called with inputs one of the vectors generated previously and $k-1$. If all the recursions fail to find a new element in the intersection of the lattice and the search space, $\boldsymbol{c}$ is set to $\boldsymbol{c}+\boldsymbol{v}-\boldsymbol{e}$ and this procedure is redone with inputs $\boldsymbol{c}$ and k, until a generated element fits in the $\mathcal{H}$ or its coordinate k is larger than H_k^M. The different steps of this generation are the same as the ones described in Section 4.2, except that after Step 1b, the following instruction is added:

(1) While $\boldsymbol{c_t}[k] < H_k^M$
    ...
    (c) If $k-1 > \ell$, use this fall-back procedure (additive or subtractive case) with $\boldsymbol{c}$ and $k-1$ as inputs and return the result if it does not fail.
(2) Return fail.

5. Analyzes of the generic sieves

Practical generic sieve algorithms are of two types: exhaustive for the levels $\ell = 0$ and $\ell = 1$, and heuristic for all levels[3]. For levels $\ell = 0$ and $\ell = 1$, using heuristic algorithms make almost no sense, since generically, the exhaustive algorithms are optimal in term of running time. For larger levels, the practical gain obtained by using the space sieve lets us expect an improvement since exhaustive sieves are not adapted to such levels. However, heuristic sieves do not ensure completeness of the enumeration: if substantially many relations are not reported, the time per relation can negatively be impacted and can eventually be worse than with exhaustive sieves.

To evaluate the practicability of the three new sieve algorithms, we analyze them practically thanks to a Sage implementation of the three sieves named `ntv.sage` (provided in CADO-NFS), mainly implemented to test accuracy of the enumeration processes, see Section 5.1. Even if the implementation is not optimized to test running time, we can extrapolate some tendency about the efficiency of the sieves, see Section 5.2. The practical experiments were done on random lattices[4] having the shape of Equation (1), whose volume is adapted to fit for the tested levels.

5.1. **Accuracy.**

The quality criteria to test accuracy reported in Table 4 are:

- the number of produced skew-small-vectors, adjusted thanks to the number of the small linear combinations and close vectors,
- the number of iterations of the while loop in the fall-back strategy and
- the relative error between the expected number of elements to be enumerated ($\#\mathcal{H}/r$) and the number of reported elements.

The relative error informs about the accuracy of the algorithm. A large relative error likely means that the nearly-transition-vectors have too large coordinates. A

[3]Combining the 3D-lattice sieve [19] and Section 4.4 may lead to obtain an 2-level exhaustive generic sieve algorithm, but we did not manage to fully implement the 3D-lattice sieve.

[4]From the point of view of a practical sieving procedure, lattices describing ideals of a same or different factor bases, or random lattices, are treated similarly.

few more linear combinations during the initialization may solve this problem. The criterion about the fall-back strategy informs about the global effort on discovering new nearly-transition-vectors or stopping regularly the enumeration process, as the number of generated skew-small-vectors about the global effort on the initialization. The combination of these three criteria is needed since, e.g., generating a huge amount of skew-small-vectors will decrease quantitatively the two other criteria by putting solely too much effort on the initialization.

Since the patterns of the skew-small-vectors of `localntv` and `sparsentv` are constrained, their relative errors are expected to be better (i.e., smaller) than the one with `globalntv`. Since the initialization is less under control with `globalntv`, the number of skew-small-vectors may be often (much) larger for `globalntv`; however, the number of calls to the fall-back strategy is expected to be lower.

	`globalntv` ($\ell = 2$)				`localntv` ($\ell = 2$)				`globalntv` ($\ell = 3$)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
# ssvs	40				41				40			
# fbs	0	2.0	61	3.1	0	3.0	61	4.3	0	12.0	65	20.0
rel. err.	0.0	2.6	95.7	10.1	0.0	1.2	96.7	5.8	0.0	0.0	75.0	2.0

(A) Experiments on 2^{14} lattices where $\mathcal{H} = [-2^6, 2^6)^3 \times [0, 2^6)$ ($t = 4$, $\#\mathcal{H} = 2^{27}$).

	`globalntv` ($\ell = 2$)				`localntv` ($\ell = 2$)				`sparsentv` ($\ell = 2$)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
# ssvs	364				69				37			
# fbs	0	5.0	712	18.3	0	9.0	591	20.0	0	13.0	332	22.0
rel. err.	0.0	1.5	36.1	6.4	0.0	1.6	50.0	5.6	0.0	2.0	49.0	5.9

(B) Experiments on 2^7 lattices where $\mathcal{H} = [-2^4, 2^4)^5 \times [0, 2^4)$ ($t = 6$, $\#\mathcal{H} = 2^{29}$).

	`globalntv` ($\ell = 3$)				`localntv` ($\ell = 3$)				`sparsentv` ($\ell = 3$)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
# ssvs	364				88				72			
# fbs	0	8.0	142	13.3	0	12.0	186	16.8	0	14.0	161	18.1
rel. err.	0.0	2.7	54.4	7.7	0.0	3.3	47.7	6.9	0.0	3.2	48.8	6.8

(C) Experiments on 2^7 lattices where $\mathcal{H} = [-2^4, 2^4)^5 \times [0, 2^4)$ ($t = 6$, $\#\mathcal{H} = 2^{29}$).

	`globalntv` ($\ell = 4$)				`localntv` ($\ell = 4$)				`globalntv` ($\ell = 5$)			
	min	med	max	mean	min	med	max	mean	min	med	max	mean
# ssvs	364				153				364			
# fbs	0	1.0	10	1.8	0	3.0	10	3.3	0	8.5	17	8.3
rel. err.	0.0	6.4	60	11.3	0.0	5.2	52.9	9.8	0.0	0.0	66.7	2.0

(D) Experiments on 2^7 lattices where $\mathcal{H} = [-2^4, 2^4)^5 \times [0, 2^4)$ ($t = 6$, $\#\mathcal{H} = 2^{29}$).

TABLE 4. Experiments on the three sieves: "# ssvs" corresponds to Criterion 5.1, "# fbs" to Criterion 5.1 and "rel. err." to Criterion 5.1.

The accuracy of the algorithms seems more than sufficient for the majority of the lattices, both in four and six dimensions. The maximal values of all the tables can be impressive, but occur only for a sufficiently small number of skewed lattices: since the enumeration in such lattices may be costly, it can be better to avoid them or at least, to be not too accurate.

In four dimensions, the accuracy is combined with a reasonable number of produced skew-small-vectors. The criteria do not help to determine which of the 2-level

`localntv` and `globalntv` is the most suitable algorithm. The running time estimations may help to decide. At level $\ell = 3$, the number of calls to the fall-back strategy can be an issue but may be under control in a careful implementation.

The situation is mitigated in dimension six. Except for the 2-level `sparsentv`, the number of skew-small-vectors is huge, which disqualify with this setting all the sieves at any level. In addition, the number of calls to the fall-back strategy at level $\ell = 2$ and $\ell = 3$ indicates that the produced nearly-transition-vectors are of poor quality. If dimension six sieving would be feasible, it will need more investigation; however, using cuboid search spaces is probably a too hard constraint that implies a hardness, or even an impossibility, for the sieving process. In addition, the initialization of the norms in higher dimensions implemented in CADO-NFS [43] is actually too slow for dimension larger than six by preserving a relative accuracy. It confirms the hardness of the relation collection above dimension four.

5.2. **Running time.** From the previous section, only four-dimensional sieving seems an option. We compare, at levels $\ell = 2$ and $\ell = 3$, the new sieves with the state-of-the-art sieve algorithms and also between themselves.

Comparison with the plane sieve. The 2-level `globalntv` and `localntv` are compared with the most efficient existing sieve algorithm, which is the (generalized) plane sieve. Our implementation of the plane sieve is incomplete: we implement the fall-back strategy of Section 4.4 without enforcing the coordinate k of the k–skew-small-vectors to be equal to 1. On 2^8 lattices, the average running time of `globalntv` (respectively `localntv`) is almost 4 (respectively 3) time faster than our generalized plane sieve. Since the accuracy of the two heuristic sieve algorithms is quite good, `globalntv` seems to be an alternative to the plane sieve.

Comparison of the new sieves. The 3-level `globalntv` is also compared with the 2-level `globalntv` and `localntv` on 2^{10} lattices. Unlike the previous comparisons, the results can be puzzling. Indeed, for lattices where the 3-level `globalntv` is expected to be efficient, the 2-level `localntv` is less than 1.5 time faster. Furthermore, the 2-level `localntv` is more than 3 time faster than the 2-level `globalntv`. Before explaining these results, we first remark that, in this situation, the three studied sieves algorithms share the same condition to use or not the fall-back strategy. The second remark comes from a detail of our implementation. Since accuracy is our main concern, Step 1b of the fall-back strategy in Section 4.2 sets $\boldsymbol{c}$ to one of the computed elements with the smallest coordinate k (i.e., the first element, since the list of k–nearly-transition-vectors is sorted by increasing coordinate k).

The 2-level `globalntv` and `localntv` produce more or less the same nearly-transition-vectors, despite different produced skew-small-vectors. The 3–skew-small-vectors are less numerous and have smaller coordinates with `localntv` than with `globalntv`. Then, if the for loop on the k–skew-small-vectors (Step 1a) fails to find an element in $\mathcal{H}$ in both sieves, and if the coordinate k of the first k–skew-small-vectors is the same for both sieves (this two situations often occur), `localntv` is faster than `globalntv`.

Between the 3-level `globalntv` and the 2-level `localntv`, the situation shares some of the observations made previously. However, this time, `globalntv` produces nearly-transition-vectors and skew-small-vectors of better quality than `localntv`: in some cases, `globalntv` is faster than `localntv`, but if the situations become the same as in the previous analysis, `localntv` stays faster. We believe that a careful study of the different parts (especially how the linear combinations can produce

useful vectors during the initialization of `globalntv` specialized in dimension four) of the algorithms will lead to an efficient implementation of the 3-level `globalntv`.

6. Conclusion

In this article we propose algorithms to sieve in any dimensions in the intersection of a lattice and a cuboid, which is one of the challenges we list to have a practical implementation of the $\text{NFS}_{>1}$ algorithms. These algorithms allow to report a large portion of the elements in the intersection, faster than the previous generic sieve algorithms. We provide a reference implementation of these algorithms, allowing us to highlight their advantages and drawbacks for the accuracy and efficiency of the enumeration, and demonstrate the practicability of these sieves for dimension four, and the hardness of sieving in dimension six and above.

In a near future, we plan to integrate these algorithms, specialized in dimension four, in the existing implementations of NFS_1 in CADO-NFS [43] and extend it to $\text{NFS}_{>1}$. It will help key size estimations for pairings [30, 3]. However, since a practical computation of the relation collection with $\text{NFS}_{>1}$ will be possible only with good polynomials f_0 and f_1, we also plan to study quality criteria for such NFS algorithms. Further work includes also enumeration in non-cuboid search space.

Acknowledgments. The authors are grateful to Pierrick Gaudry and Marion Videau for numerous discussions and reviews of preliminary versions of this work, as well as Aurore Guillevic and Shashank Singh for numerous discussions about NFS. We also thank Damien Stehlé and the referees whose remarks helped us to improve the presentation of our results.

References

1. S. Bai, C. Bouvier, A. Kruppa, and P. Zimmermann, *Better polynomials for GNFS*, Math. Comp. **85** (2016), no. 298, 861–873.
2. R. Barbulescu, *Algorithmes de logarithmes discrets dans les corps finis*, Ph.D. thesis, Université de Lorraine, 2013.
3. R. Barbulescu and S. Duquesne, *Updating key size estimations for pairings*, J. Cryptology **31** (2018), 1–39.
4. R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain, *Improving NFS for the discrete logarithm problem in non-prime finite fields*, EUROCRYPT 2015 (E. Oswald and M. Fischlin, eds.), LNCS, vol. 9056, Springer, 2015, pp. 129–155.
5. R. Barbulescu, P. Gaudry, and T. Kleinjung, *The Tower Number Field Sieve*, ASIACRYPT 2015 (T. Iwata and J. Cheon, eds.), LNCS, vol. 9453, Springer, 2015, pp. 31–55.
6. Y. Bistritz and A. Lifshitz, *Bounds for resultants of univariate and bivariate polynomials*, Linear Algebra and its Applications **432** (2010), no. 8, 1995–2005.
7. F. Boudot, *On Improving Integer Factorization and Discrete Logarithm Computation using Partial Triangulation*, Cryptology ePrint Archive, Report 2017/758, 2017.
8. J. Buhler, H. Lenstra, and C. Pomerance, *Factoring integers with the number field sieve*, The Development of the Number Field Sieve (A. Lenstra and H. Lenstra, eds.), Lecture Notes in Mathematics, vol. 1554, Springer, 1993, pp. 50–94.
9. H. Cohen, *A course in algorithmic algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, 2000, fourth printing.
10. D. Coppersmith, *Solving homogeneous linear equations over $GF(2)$ via block Wiedemann algorithm*, Math. Comp. **62** (1994), no. 205, 333–350.
11. J. Franke and T. Kleinjung, *Continued fractions and lattice sieving*, SHARCS 2005, 2005.
12. D. Freeman, M. Scott, and E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*, J. Cryptology **23** (2010), 224–280.
13. J. Fried, P. Gaudry, N. Heninger, and E. Thomé, *A Kilobit Hidden SNFS Discrete Logarithm Computation*, EUROCRYPT 2017 (J.-S. Coron and J. Nielsen, eds.), LNCS, vol. 10210, Springer, 2017, pp. 202–231.

14. P. Gaudry, L. Grémy, and M. Videau, *Collecting relations for the number field sieve in* $GF(p^6)$, LMS J. Comput. Math **19** (2016), no. A, 332–350.
15. J. Graver, *On the foundations of linear and integer linear programming I*, Mathematical Programming **9** (1975), no. 1, 207–226.
16. L. Grémy, A. Guillevic, F. Morain, and E. Thomé, *Computing discrete logarithms in* $GF(p^6)$, SAC 2017 (C. Adams and J. Camenisch, eds.), LNCS, vol. 10719, Springer, 2018, pp. 85–105.
17. A. Guillevic, *Faster individual discrete logarithms with the QPA and NFS variants*, Cryptology ePrint Archive, Report 2016/684, 2017.
18. K. Hayasaka, K. Aoki, T. Kobayashi, and T. Takagi, *An Experiment of Number Field Sieve for Discrete Logarithm Problem over* $GF(p^{12})$, Number Theory and Cryptography (M. Fischlin and S. Katzenbeisser, eds.), LNCS, vol. 8260, Springer, 2013, pp. 108–120.
19. ———, *A construction of 3-dimensional lattice sieve for number field sieve over* $\mathbb{F}_{p^n}$, Cryptology ePrint Archive, 2015/1179, 2015.
20. A. Joux and C. Pierrot, *Nearly sparse linear algebra and application to discrete logarithms computations*, Contemporary Developments in Finite Fields and Applications (A. Canteaut, G. Effinger, S. Huczynska, D. Panario, and L. Storme, eds.), World Scientific Publishing Company, 2016, pp. 119–144.
21. A. Joux and R. Lercier, *Improvements to the General Number Field Sieve for discrete logarithms in prime fields*, Math. Comp. **72** (2003), no. 242, 953–967.
22. A. Joux, R. Lercier, N. Smart, and F. Vercauteren, *The Number Field Sieve in the Medium Prime Case*, CRYPTO 2006 (C. Dwork, ed.), LNCS, vol. 4117, Springer, 2006, pp. 326–344.
23. T. Kim and R. Barbulescu, *Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case*, CRYPTO 2016 (M. Robshaw and J. Katz, eds.), LNCS, vol. 9814, Springer, 2016, pp. 543–571.
24. T. Kim and J. Jeong, *Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree*, PKC 2017 (S. Fehr, ed.), LNCS, vol. 10174, Springer, 2017, pp. 388–408.
25. T. Kleinjung, *On polynomial selection for the general number field sieve*, Math. Comp. **75** (2006), no. 256, 2037–2047.
26. ———, *Polynomial Selection*, Slides presented at the CADO workshop on integer factorization, 2008, `http://cado.gforge.inria.fr/workshop/slides/kleinjung.pdf`.
27. T. Kleinjung, C. Diem, A. Lenstra, C. Priplata, and C. Stahlke, *Computation of a 768-Bit Prime Field Discrete Logarithm*, EUROCRYPT 2017 (J.-S. Coron and J. Nielsen, eds.), LNCS, vol. 10210, Springer, 2017, pp. 185–201.
28. A. Lenstra, *General purpose integer factoring*, Topics in Computational Number Theory Inspired by Peter L. Montgomery (J. Bos and A. Lenstra, eds.), Cambridge University Press, 2017, pp. 116–160.
29. A. Lenstra and E. Verheul, *The XTR public key system*, CRYPTO 2000 (M. Bellare, ed.), LNCS, vol. 1880, Springer, 2000, pp. 1–19.
30. A. Menezes, P. Sarkar, and S. Singh, *Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-Based Cryptography*, Mycrypt 2016 (R. Phan and M. Yung, eds.), LNCS, vol. 10311, Springer, 2017, pp. 83–108.
31. B. Murphy, *Polynomial selection for the number field sieve integer factorisation algorithm*, Ph.D. thesis, The Australian National University, 1999.
32. S. Onn, *Theory and Applications of n-Fold Integer Programming*, Mixed Integer Nonlinear Programming (J. Lee and S. Leyffer, eds.), IMA, vol. 154, Springer, 2012, pp. 559–593.
33. J. Pollard, *The lattice sieve*, The Development of the Number Field Sieve (A. Lenstra and H. Lenstra, eds.), Lecture Notes in Mathematics, vol. 1554, Springer, 1993, pp. 43–49.
34. C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational Methods in Number Theory (H. Lenstra and R. Tijdeman, eds.), Mathematical Centre Tracts, vol. 154, Mathematish Centrum, 1982, pp. 89–139.
35. ———, *A Tale of Two Sieves*, Notices Amer. Math. Soc **43** (1996), 1473–1485.
36. K. Rubin and A. Silverberg, *Torus-based cryptography*, CRYPTO 2003 (D. Boneh, ed.), LNCS, vol. 2729, Springer, 2003, pp. 349–365.
37. P. Sarkar and S. Singh, *A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm*, ASIACRYPT 2016 (J. Cheon and T. Takagi, eds.), LNCS, vol. 10031, Springer, 2016, pp. 37–62.

38. ———, *A Generalisation of the Conjugation Method for Polynomial Selection for the Extended Tower Number Field Sieve Algorithm*, Cryptology ePrint Archive, Report 2016/537, 2016.
39. ———, *New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields*, EUROCRYPT 2016 (M. Fischlin and J.-S. Coron, eds.), LNCS, vol. 9665, Springer, 2016, pp. 429–458.
40. ———, *Tower number field sieve variant of a recent polynomial selection method*, Cryptology ePrint Archive, Report 2016/401, 2016.
41. O. Schirokauer, *Discrete logarithms and local units*, Philos. Trans. Roy. Soc. A **345** (1993), no. 1676, 409–423.
42. ———, *Virtual logarithms*, J. Algorithms **57** (2005), 140–147.
43. The CADO-NFS Development Team, *CADO-NFS, an implementation of the number field sieve algorithm*, 2018, development version, `http://cado-nfs.gforge.inria.fr/`.
44. P. Zajac, *Discrete logarithm problem in degree six finite fields*, Ph.D. thesis, Slovak University of Technology, 2008, `http://www.kaivt.elf.stuba.sk/kaivt/Vyskum/XTRDL`.
45. Y. Zhu, J. Zhuang, C. Lv, and D. Lin, *Improvements on the individual logarithm step in extended tower number field sieve*, Cryptology ePrint Archive, Report 2016/727, 2016.

Univ Lyon, CNRS, ENS de Lyon, Inria, Université Claude Bernard Lyon 1, LIP UMR 5668, F-69007 LYON, France
Email address: `firstname.lastname@ens-lyon.fr`

FAST TABULATION OF CHALLENGE PSEUDOPRIMES

ANDREW SHALLUE AND JONATHAN WEBSTER

Abstract. We provide a new algorithm for tabulating composite numbers which are pseudoprimes to both a Fermat test and a Lucas test. Our algorithm is optimized for parameter choices that minimize the occurrence of pseudoprimes, and for pseudoprimes with a fixed number of prime factors. Using this, we have confirmed that there are no PSW challenge pseudoprimes with two or three prime factors up to 2^{80}. In the case where one is tabulating challenge pseudoprimes with a fixed number of prime factors, we prove our algorithm gives an unconditional asymptotic improvement over previous methods.

1. Introduction

Pomerance, Selfridge, and Wagstaff famously offered \$620 for a composite n that satisfies

(1) $2^{n-1} \equiv 1 \pmod{n}$ so n is a base 2 Fermat pseudoprime,
(2) $(5 \mid n) = -1$ so n is not a square modulo 5, and
(3) $F_{n+1} \equiv 0 \pmod{n}$ so n is a Fibonacci pseudoprime,

or to prove that no such n exists. We call composites that satisfy these conditions PSW challenge pseudoprimes. In [PSW80] they credit R. Baillie with the discovery that combining a Fermat test with a Lucas test (with a certain specific parameter choice) makes for an especially effective primality test [BW80]. Perhaps not as well known is Jon Grantham's offer of \$6.20 for a Frobenius pseudoprime n to the polynomial $x^2 - 5x - 5$ with $(5 \mid n) = -1$ [Gra01]. Similar to the PSW challenge, Grantham's challenge number would be a base 5 Fermat pseudoprime, a Lucas pseudoprime with polynomial $x^2 - 5x - 5$, and satisfy $(5 \mid n) = -1$. Both challenges remain open as of this writing, though at least in the first case there is good reason to believe infinitely many exist [Pom84].

The largest tabulation to date of pseudoprimes of similar type is that of Gilchrist [Gil13], who found no Baillie-PSW pseudoprimes (a stronger version of the PSW challenge) up to $B = 2^{64}$. After first tabulating 2-strong pseudoprimes [Fei13, Nic12] using an algorithm due to Pinch [Pin00], he applied the strong Lucas test using the code of Nicely [Nic12]. Taking inspiration from tabulations of strong pseudoprimes to several bases [Jae93, Ble96, JD14, SW17], our new idea is to treat the tabulation as a two-base computation: a Fermat base and a Lucas base. In this way we exploit both tests that make up the definition.

Specifically, we improve upon [Pin00] in three ways:

- GCD computations replace factorizations of $b^n - 1$,

The first author was supported in part by Illinois Wesleyan University's Artistic and Scholarly Development grant and the second author was supported in part by Butler University's Holcomb Awards Committee.

18 Jun 2018 09:23:49 PDT
Version 5 - Submitted to Open Book Series

- sieving searches are done with larger moduli,
- fewer pre-products are constructed.

Other notable attempts to find a PSW challenge number involve construction techniques that result in a computationally infeasible subset-product problem [GA99, CG03]. The first of such attempts would have also found the number requested at the end of [Wil77] which is simultaneously a Carmichael number and a (P, Q)-Lucas pseudoprime for all pairs (P, Q) with $5 = P^2 - 4Q$ and $(5 \mid n) = -1$.

The new algorithm presented constructs n by pairing primes p with admissible pre-products k. In Section 6 we provide an unconditional proof of the running time. Unfortunately, the provable running time gets worse as the number of primes dividing k increases. Specifically, we prove the following.

Theorem 1. *There exists an algorithm which tabulates all PSW challenge pseudoprimes up to B with t prime factors, while using $\widetilde{O}(B^{1-\frac{1}{3t-1}})$ bit operations and space for $O(B^{\frac{3t-2}{4t-2}})$ words.*

The running time improves under a heuristic assumption that factoring plays a minimal role, to $\widetilde{O}(B^{1-\frac{1}{2t-1}})$ bit operations.

No PSW challenge pseudoprimes with two or three prime factors exist up to $B = 2^{80}$.

For the computation performed we chose 2 as the Fermat base and $(1, -1)$ as the Lucas base, but the algorithm as designed can handle arbitrary choices.

The rest of the paper is organized as follows. Section 2 establishes key definitions and notation, while Section 3 provides the theoretical underpinnings of the algorithm. The algorithm is presented in Section 4 along with a proof of correctness. The running time is analyzed in Sections 5 and 6. We conclude the paper with comments on our computation with $B = 2^{80}$.

2. Definitions and Notation

A *base b Fermat pseudoprime* is a composite n with $\gcd(n, b) = 1$ that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$.

Lucas sequences have many equivalent definitions. We state a few important ones and let the reader consult standard sources such as [Leh30] for a more thorough treatment. Let $P, Q \in \mathbb{Z}$ and α, β be the distinct roots of $f(x) = x^2 - Px + Q$, with $D = P^2 - 4Q$ the discriminant. Then the Lucas sequences are

$$U_n(P, Q) = (\alpha^n - \beta^n)/(\alpha - \beta) \quad \text{and } V_n(P, Q) = \alpha^n + \beta^n \ .$$

Equivalently, we may define these as recurrence relations, where

$$U_0(P, Q) = 0, \quad U_1(P, Q) = 1, \quad \text{and} \quad U_n(P, Q) = PU_{n-1}(P, Q) - QU_{n-2}(P, Q) \ .$$

and

$$V_0(P, Q) = 2, \quad V_1(P, Q) = P, \quad \text{and} \quad V_n(P, Q) = PV_{n-1}(P, Q) - QV_{n-2}(P, Q) \ .$$

We will use $\epsilon(n) = (D \mid n)$ for the Jacobi symbol and will frequently write U_n or V_n when the particular sequence is clear from context. It should be noted that the definition below

guarantees that n is odd so that the Jacobi symbol is well-defined. Often U_n is referred to as the Lucas sequence with parameters P and Q, but both V_n and U_n are needed for the "double-and-add" method for computing U_n using $O(\log n)$ arithmetic operations. For a more modern take on this classic algorithm see [JQ96].

A (P, Q)-*Lucas pseudoprime* is a composite n with $\gcd(n, 2QD) = 1$ such that $U_{n-\epsilon(n)} \equiv 0 \pmod{n}$.

Definition 1. We call a composite n a (b, P, Q)-challenge pseudoprime if it is simultaneously a base b Fermat pseudoprime, a (P, Q)-Lucas pseudoprime, and additionally satisfies $\epsilon(n) = -1$.

Note that $\epsilon(n) = -1$ means that D is not a square.

A PSW challenge pseudoprime is then a $(2, 1, -1)$-challenge pseudoprime in our notation. To get a Baillie-PSW pseudoprime, one replaces the Fermat test with a strong pseudoprime test and the Lucas test with a strong Lucas test. The Lucas parameters are chosen as $P = 1$ and $Q = (1 - D)/4$, where D is the first discriminant in the sequence $\{5, -7, 9, -11, \dots\} = \{(-1)^k(2k + 1)\}_{k\geq 2}$ for which $(D \mid n) = -1$.

We use $\ell_b(n)$ when $\gcd(b, n) = 1$ to denote the multiplicative order of b modulo n, i.e. the smallest positive integer such that $b^{\ell_b(n)} = 1 \mod n$. When $n = p$ is a prime, $\ell_b(p) \mid p - 1$ by Lagrange's Theorem since $p - 1$ is the order of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Given a prime p, there exists a least positive integer ω such that $U_\omega \equiv 0 \pmod{p}$. We call ω the rank of apparition of p with respect to the Lucas sequence (P, Q), and we denote it by $\omega(p)$. It is also well known that $U_{p-\epsilon(p)} \equiv 0 \pmod{p}$ and hence that $\omega(p) \mid p - \epsilon(p)$.

Throughout, we will use log to represent the natural logarithm.

The function $P(n)$ returns the largest prime factor of n, and for asymptotic analysis we often use $\widetilde{O}$, where $f = \widetilde{O}(g)$ means there are positive constants N, c such that $f(n) \leq g(n)(\log(4 + g(n)))^c$ for nonnegative functions $f(n)$ and $g(n)$ and for all $n \geq N$ [vzGG03, Definition 25.8].

3. Algorithmic Theory

The main idea of the tabulation comes from [Jae93, Ble96, JD14, SW17], but instead of tabulating pseudoprimes to many bases, we have just a Fermat base and a Lucas base. For the Fermat case we state known results for completeness, while for the Lucas case we state and prove the required results. We follow the notation in [SW17] when possible.

To find all (b, P, Q)-challenge pseudoprimes $n < B$, we construct n in factored form $n = p_1 p_2 \dots p_{t-1} p_t$ where t is the number of prime divisors of n and $p_i \leq p_{i+1}$. We call $k = p_1 p_2 \dots p_i$ for $i < t$ a pre-product. Subsection 3.1 states theorems limiting the number of pre-products that need to be considered. Subsection 3.2 shows that p_t may be found via a GCD computation when k is small and by a sieving search when k is large.

3.1. Conditions on $n = wk$.

We will frequently make use of the fact that if $\epsilon(n) = -1$ and $n = wk$ then $\epsilon(w) = -\epsilon(k)$ by the multiplicative property of the Jacobi symbol.

Proposition 1 (Theorem 3.20 of [Ble96])**.** *Let $k \geq 1$ be an integer and p a prime. If $n = kp^2$ is a Fermat pseudoprime for the base b then the following two conditions must be satisfied:*

(1) $b^{p-1} \equiv 1 \pmod{p^2}$,
(2) $b^{k-1} \equiv 1 \pmod{p^2}$.

Proposition 2. *Let $k \geq 1$ be an integer and p a prime. If $n = kp^2$ is a (P, Q)-Lucas pseudoprime with $\epsilon(n) = -1$ then the following two conditions must be satisfied:*

(1) $U_{p-\epsilon(p)} \equiv 0 \pmod{p^2}$,
(2) $U_{k-\epsilon(k)} \equiv 0 \pmod{p^2}$.

Proof. We start by noting that $\omega(p^2) \mid p\omega(p)$ and hence $\omega(p^2)$ divides $p(p-\epsilon(p))$ by the law of repetition [Leh30, Theorem 1.6]. In addition, $U_{n+1} \equiv 0 \pmod{n}$ by assumption so that $U_{n+1} \equiv 0 \pmod{p^2}$ and hence $\omega(p^2) \mid n+1$. With p relatively prime to $n+1$, it follows that $\omega(p^2)$ divides $\gcd(n+1, p-\epsilon(p))$, and we conclude that $\omega(p^2)$ divides $p-\epsilon(p)$, which proves the first congruence.

For the second congruence, if $k = 1$ then $U_{k-\epsilon(k)} = U_0$ and the congruence is satisfied. In the case $k > 1$, $\omega(p^2)$ divides $n+1 = kp^2+1 = kp^2 - \epsilon(k)$ and $p - \epsilon(p)$. Thus $\omega(p^2)$ divides

$$kp^2 - \epsilon(k) - k(p-1)(p+1) = kp^2 - \epsilon(k) - k(p^2-1) = k - \epsilon(k) \ .$$

It follows that $U_{k-\epsilon(k)} \equiv 0 \pmod{p^2}$. □

In the case $b = 2$, these primes are known as Weiferich primes and in the $(1, -1)$ case they are known as Wall-Sun-Sun primes. [CDP97] suggests the following heuristic argument to understand the rarity of these primes. Consider either $b^{p-1} - 1$ or $U_{p-\epsilon(p)}$ in a base p representation. The constant coefficient is zero by Fermat's Little Theorem and its analogue. The coefficient on p needs to be 0 to satisfy the above congruence and we expect this to happen with probability $1/p$. Summing over the reciprocal of primes gives an expected count of such primes up to x as being on the order of $\log \log x$. For challenge pseudoprimes, both congruences would have to be met simultaneously. The corresponding count from the expected values is now a sum of $1/p^2$ and the infinite sum converges. So we expect the count to be finite and we know of no examples of this behavior.

Either the Fermat case or the Lucas case can individually be checked up to a bound B in $O(B^{1/2})$ time and such primes may be then tested against the other condition. In the very unlikely scenario that such a prime does exist, we refer the reader to section 6 of [Pin00] in order to account for square factors dividing challenge pseudoprimes. Given how exceedingly rare we believe these are, we deal no further with square factors and assume a squarefree challenge pseudoprime.

Proposition 3. *Let $n = p_1 p_2 \dots p_t$ be a (b, P, Q)-challenge pseudoprime,*

$$L = \operatorname{lcm}(\ell_b(p_1), \dots, \ell_b(p_t)), \quad \textit{and} \quad W = \operatorname{lcm}(\omega(p_1), \dots, \omega(p_t)) \ .$$

Then $\gcd(L, W) \leq 2$, $\gcd(n, L) = 1$, *and* $\gcd(n, W) = 1$.

Proof. We have $b^{n-1} \equiv 1 \pmod{p_i}$ and hence $n \equiv 1 \pmod{\ell_b(p_i)}$. We also have $U_{n+1} \equiv 0 \pmod{p_i}$ and hence $n \equiv -1 \pmod{\omega(p_i)}$. So $\ell_b(p_i) \mid (n-1)$ and $\omega(p_i) \mid (n+1)$ and this holds for all $p_i \mid n$. Therefore, $L \mid (n-1)$ and $W \mid (n+1)$. Then $\gcd(L, W) \leq \gcd(n-1, n+1) \leq 2$. Since n is relatively prime to both $n+1$ and $n-1$, the other two gcds are as claimed. □

This is extremely useful in limiting the pre-products under consideration. For one, it means that most primes with $\epsilon(p) = 1$ need not be considered, since it is highly probable that $\gcd(\ell_b(p), \omega(p)) > 2$ when $\epsilon(p) = 1$. In private correspondence, Paul Pollack gave a heuristic argument suggesting around $\log(x)$ such primes up to x. We call k *admissible* if the primes dividing k satisfy the above proposition.

3.2. **Conditions on p_t given k.** Henceforth, we assume that $k = p_1 \dots p_{t-1}$ and that k is admissible.

Proposition 4. *If $n = kp$ is a (b, P, Q)-challenge pseudoprime then p is a divisor of*

$$\gcd(b^{k-1} - 1, U_{k-\epsilon(k)}).$$

Proof. Recall that $b^{n-1} \equiv 1 \pmod{n}$ and $U_{n+1} \equiv 0 \pmod{n}$. We rewrite $n-1 = kp-1 = k(p-1)+k-1$. Since $\ell_b(p)$ divides $(p-1)$ and $n-1$ we conclude $\ell_b(p) \mid k-1$. Thus, $p \mid b^{k-1} - 1$.

Similarly $n+1 = kp - \epsilon(p)\epsilon(k) = k(p-\epsilon(p)) + k\epsilon(p) - \epsilon(p)\epsilon(k) = k(p-\epsilon(p)) + \epsilon(p)(k-\epsilon(k))$. Since $\omega(p)$ divides $p - \epsilon(p)$ and $n+1$ we conclude $\omega(p) \mid (k - \epsilon(k))$. Thus, $p \mid U_{k-\epsilon(k)}$. □

Proposition 5. *If $n = kp$ is a (b, P, Q)-challenge pseudoprime then*

$$p \equiv \begin{cases} k^{-1} \pmod{L} \\ -k^{-1} \pmod{W} \end{cases},$$

where

$$L = \operatorname{lcm}(\ell_b(p_1), \dots, \ell_b(p_{t-1})), \quad \textit{and} \quad W = \operatorname{lcm}(\omega(p_1), \dots, \omega(p_{t-1})) \ .$$

Proof. Since $n = kp$ is a challenge pseudoprime, we have that $b^{kp-1} \equiv 1 \mod p_i$ where p_i is any prime factor of k, and so $\ell_b(p_i) \mid kp - 1$. Thus, $p \equiv k^{-1} \mod \ell_b(p_i)$. We also know that $\omega(n+1) \equiv 0 \mod n$, and hence that it is congruent to 0 modulo p_i. Thus, $\omega(p_i) \mid kp + 1$ so that $p \equiv -k^{-1} \mod \omega(p_i)$.

Now, $\ell_b(p_i) \mid kp - 1$ for all $p_i \mid k$ if and only if $L \mid kp - 1$. A similar statement holds for W, which completes the proof. □

4. Algorithm

Our basic strategy follows that found in [SW17]. Find all pseudoprimes with t prime factors for each $t \geq 2$ in turn. For a given t, we analyze all pre-products k with $t-1$ prime factors. The question for each pre-product is whether there exists a prime p such $n = kp$ is a challenge pseudoprime. For small pre-products, this question can be answered with a gcd computation. For large pre-products, we instead use a sieve.

Algorithm 1: Tabulating squarefree challenge pseudoprimes

Input : bound B, positive integer $b \geq 2$, Lucas sequence parameters (P, Q)
Output: list of $n \leq B$ which are (b, P, Q)-challenge pseudoprimes

```
Create an array of size √B with entry i containing the smallest prime factor of i;
for primes p ≤ √B do
    Compute ℓ_b(p), ω(p) and only keep prime p if gcd(ℓ_b(p), ω(p)) ≤ 2;
    Update pre-product list;
    for new pre-products k do
        if k ≤ X then
            do GCD step
        else
            do Sieve step
```

The above suggests storing all such primes up to $\sqrt{B}$ along with allowable pre-products, but space constraints would prohibit this strategy in practice. Construction of composite pre-products may be done with a combination of storing the 3-tuple $(p, \ell_b(p), \omega(p))$ for small primes and creating them on the fly for large primes, where the distinction is dependent upon space constraints. To efficiently create them, one may use an incremental sieve or a segmented sieve to generate factorizations of consecutive integers so that we may quickly compute $\ell_b(p)$ from the factorization of $p-1$ and $\omega(p)$ from the factorization of $p - \epsilon(p)$.

To tabulate Baillie-PSW pseudoprimes, one tabulates all pseudoprimes for each D in the sequence. Each discriminant performs a trial division so that successive computations will remove the next small prime from consideration, making the algorithm progressively more efficient.

4.1. **Algorithm Details and Correctness Proof.** We update the pre-product list as follows. For each existing admissible pre-product k', create a new pre-product $k = k'p$ and check that it is also admissible. Recall that $k = \prod p_i$ is admissible if $\gcd(L, W) \leq 2$ where $L = \operatorname{lcm}_i(\ell_b(p_i))$ and $W = \operatorname{lcm}_i(\omega(p_i))$.

The GCD step involves computing and then factoring $\gcd(b^{k-1} - 1, U_{k-\epsilon(k)})$. For each prime p dividing the gcd with $p > P(k)$, we build $n = kp$ and apply the Fermat test and the Lucas test to determine if it is a challenge pseudoprime. Importantly, both b^{k-1} and $U_{k-\epsilon(k)}$ can be computed using a standard "double-and-add" strategy at a cost of $O(\log k)$ arithmetic operations. With such large inputs, it is vital to use a gcd algorithm asymptotically faster than the Euclidean algorithm. The solution is a discrete fast Fourier transform method that requires $\widetilde{O}(n)$ operations on n-bit inputs [SZ04].

For the sieve step, we check primes p in the range $p_{t-1} < p < B/k$ that fall into the arithmetic progression given by Proposition 5. For each such prime, we again construct $n = kp$ and apply the tests directly to see if it is a challenge pseudoprime.

Theorem 2. *Algorithm 1 correctly tabulates all squarefree (b, P, Q)-challenge pseudoprimes up to B.*

Proof. Suppose that $n \leq B$ is a (b, P, Q)-challenge pseudoprime. Then we can write $n = p_1 \cdots p_t = kp_t$. By Proposition 3, $\gcd(L, W) \leq 2$, and this is true whether L, W are computed for each of the p_i separately, for k, or for n as a whole. Thus, limiting our pre-product list to admissible k is valid. Note that any prime $p \mid k$ satisfies $p \leq B^{1/2}$, so finding all primes up to $B^{1/2}$ is sufficient, if space intensive.

Given k, it follows from Propositions 4 and 5 that p_t is a divisor of $\gcd(b^{k-1} - 1, U_{k-\epsilon(k)})$ and that

$$p_t \equiv \begin{cases} k^{-1} \pmod{L} \\ -k^{-1} \pmod{W} \end{cases} .$$

Note that k^{-1} exists modulo L and modulo W because $\gcd(n, L) = \gcd(n, W) = 1$. Thus, the algorithm will find p_t either through the GCD step or the Sieve step.

Finally, there is no chance of false positives because each potential pseudoprime is subjected to the necessary Fermat and Lucas tests. □

5. Reciprocal sums involving order

The next two sections develop a proof of the asymptotic running time in the case where $t = 2$ or $t = 3$. This proof depends on finding upper bounds on the sum over primes

$$\sum_p \frac{1}{p \cdot \operatorname{lcm}(\ell_b(p), \omega(p))} .$$

Since such results are of independent interest, we spend some time here developing the appropriate theory. A general observation is that in order to bound a reciprocal sum of a function $f(n)$, it is not sufficient to know that $f(n)$ is usually large. Instead, we need a precise bound on how often $f(n) \leq y$ for a range of values y.

The first step is to prove a slight generalization of a known lemma. Our proof will follow closely the version found as Lemma 3 in [Mur88]. Let b be the base of the Fermat test, and let $\beta = \alpha/\bar{\alpha}$ where $\alpha, \bar{\alpha}$ are the roots of $x^2 - Px + Q$. In this context let D be the squarefree part of the discriminant of $x^2 - Px + Q$. Define Γ as the subgroup of the unit group of $\mathbb{Q}(\sqrt{D})$ generated by β, and let Γ_p be the reduction of Γ modulo p.

Lemma 1. *Let Γ be a rank 1 subgroup of $\mathbb{Q}(\sqrt{D})$, generated by β. Then there are $O(y^2)$ primes p such that $|\Gamma_p| \leq y$.*

Proof. Let n be a positive integer less than y, and consider $\beta^n - 1$. Since $\beta \in \mathbb{Q}(\sqrt{D})$, so is $\beta^n - 1$. Analyzing the numerator, it is straightforward to show that the numerator of $\beta^n - 1$ is at most c^n, where c is a constant depending on P and Q.

Now, define $S = \{\beta^n \ : \ 0 \leq n \leq y\}$. If $|\Gamma_p| \leq y$ then two elements of S are equal modulo p, i.e. $\beta^{n_1} = \beta^{n_2} \mod p$. Without loss of generality, assume $n_1 \geq n_2$ so that $m = n_1 - n_2$ is nonnegative. Then $\beta^{n_1 - n_2} = 1 \mod p$ and we denote $m = n_1 - n_2$, noting that $0 \leq m \leq y$. Then thinking of $\beta^m - 1$ as an element of $\mathbb{Q}(\sqrt{D})$, we have $\beta^m - 1 = \gamma_1 + \gamma_2\sqrt{D}$, and $\beta^{n_1 - n_2} = 1 \mod p$ implies p divides the numerators of the rational numbers γ_1 and γ_2.

For any given $m = n_1 - n_2 \leq y$, there are $O(m) = O(y)$ primes dividing the numerators of both γ_1 and γ_2, where the constant depends on the choice of β. Thus, the total number of primes with $|\Gamma_p| \leq y$ is $O(y^2)$. □

The next lemma will be essential in the analysis of the sieve step of Algorithm 1. The authors are very grateful to an anonymous referee for suggesting the usage of the Cauchy-Schwarz inequality, thus improving the bound from $\widetilde{O}(X^{-2/3})$ to $\widetilde{O}(X^{-1})$.

Lemma 2. *We have*

$$\sum_{\substack{X<p<B \\ \gcd(\ell_b(p),\omega(p))\leq 2}} \frac{1}{p \cdot \operatorname{lcm}(\ell_b(p), \omega(p))} = \widetilde{O}(X^{-1})$$

where the sum is over primes and the implicit logarithm factor depends on B, b, P, Q.

Proof. We first utilize the fact that $\gcd(\ell_b(p), \omega(p)) \leq 2$ for all primes in the sum, along with the Cauchy-Schwarz inequality to get the new upper bound

$$\sum_{X<p<B} \frac{2}{p \cdot \ell_b(p)\omega(p)} \leq \left(\sum_{X<p<B} \frac{1}{p \cdot \ell_b(p)^2} \right)^{1/2} \left(\sum_{X<p<B} \frac{1}{p \cdot \omega(p)^2} \right)^{1/2} .$$

To bound these new sums, we break into two pieces depending on whether $\ell_b(p)$ is greater or less than y (similarly, whether $\omega(p)$ is greater or less than y).

In the case where $\ell_b(p)$ is small we will use partial summation, and thus require a bound on the count of primes p with $\ell_b(p) \leq y$. By Murty-Srinivasan, Lemma 1, we know there are $O(y^2)$ primes with $\ell_b(p) \leq y$. Using partial summation, we then have

$$\sum_{\substack{X<p<B \\ \ell_b(p)\leq y}} \frac{1}{\ell_b(p)^2} = \frac{1}{y^2} \cdot O(y^2) - \int_1^y O(t^2) \cdot -2t^{-3} \, \mathrm{d}t = O(1) + O(\log y)$$

and so

$$\sum_{\substack{X<p<B \\ \ell_b(p)\leq y}} \frac{1}{p \cdot \ell_b(p)^2} \leq \frac{1}{X} \sum_{\substack{X<p<B \\ \ell_b(p)\leq y}} \frac{1}{\ell_b(p)^2} \leq O\left(\frac{\log y}{X}\right) .$$

In the case where $\ell_b(p)$ is large we bound as follows:

$$\sum_{\substack{X<p<B \\ \ell_b(p)> y}} \frac{1}{p \cdot \ell_b(p)^2} \leq \frac{1}{y^2} \sum_{X<p<B} \frac{1}{p} \leq O\left(\frac{\log B}{y^2}\right) .$$

Balancing the two cases gives $\sum_{X<p<B} 1/(p\ell_b(p)^2) = \widetilde{O}(X^{-1})$.

By Lemma 1, there are also at most $O(y^2)$ primes with $\omega(p) \leq y$. Using the same argument as above, we also have $\sum_{X<p<B} 1/(p\omega(p)^2) = \widetilde{O}(X^{-1})$. The result then follows. □

6. Algorithm Analysis

In this section we provide an asymptotic analysis of Algorithm 1. Recall the additional assumption that the squarefree part of D is not -1 or -3. First we find the cost of the GCD step.

Theorem 3. *The asymptotic cost of the* gcd *step for all $k \le X$ is $\widetilde{O}(X^2) + \widetilde{O}(B^{1/2}X^{3/2})$ bit operations and space for $\widetilde{O}(B^{1/2}X^{1/2})$ words.*

Proof. As noted above, for each pre-product $k \le X$ we need to compute $b^{k-1} - 1$ and $U_{k-\epsilon(k)}$ at a cost of $\widetilde{O}(k)$ bit operations, then apply a linear gcd algorithm to compute $g(k) = \gcd(b^{k-1} - 1, U_{k-\epsilon(k)})$ at a cost of $\widetilde{O}(k)$ bit operations.

In factoring $g(k)$ we do not need a complete factorization; rather we need to find all primes $p < B/k$ that divide $g(k)$. Using the polynomial evaluation method of Pollard and Strassen (see [vzGG03, Theorem 19.3]) this requires $\widetilde{O}((B/k)^{1/2} \cdot \log(g(k))) = \widetilde{O}((Bk)^{1/2})$ bit operations and $O((Bk)^{1/2})$ space.

The total cost in bit operations for all $k \le X$ is then

$$\sum_{k \le X} O(k) + \widetilde{O}(k) + \widetilde{O}((Bk)^{1/2}) = \widetilde{O}(X^2) + \widetilde{O}(B^{1/2}X^{3/2}) \ .$$

□

Next we find the cost of the Sieve step of Algorithm 1, broken down by the number of prime factors in the pre-product.

Theorem 4. *Restrict attention to the tabulation of (b, P, Q)-challenge pseudoprimes that are squarefree with $t \ge 3$ prime factors. Then the cost in bit operations of the Sieve step in Algorithm 1 is*

$$\widetilde{O}(X^{-1/(t-1)}B) \ .$$

Proof. By construction we have $n = kp_t$ where $k > X$ and p_t is the largest prime factor dividing n. Since k is admissible, $\gcd(\ell_b(p), \omega(p)) \le 2$ for all $p \mid k$.

Let k' denote k/p_{t-1}, the product of the smallest $t-2$ primes in the pre-product. It follows that $X < k < B^{1-1/t}$ and so $\frac{X}{k'} < p_{t-1} < \frac{B^{1-1/t}}{k'}$. As t increases, k' might become larger than X. In this case we use the alternate lower bound $p_{t-1} > X^{1/(t-1)}$. This lower bound is true because we construct k so that its prime factors are increasing, and thus if $p_{t-1} \le X^{1/(t-1)}$ then $k \le X$, a contradiction.

By Proposition 5 the size of the arithmetic progression to check for each pre-product k is $\frac{B}{k\mathrm{lcm}(L,W)}$, where L and W are computed from the primes dividing k. Then the total

cost in arithmetic operations for all pre-products with $t-1$ prime factors is

$$\sum_{X<k<B^{1-1/t}} \frac{B}{k\mathrm{lcm}(L,W)} \leq \sum_{k'\leq X^{1-\frac{1}{t-1}}} \sum_{\frac{X}{k'}<p_{t-1}<\frac{B^{1-1/t}}{k'}} \frac{B}{k'p_{t-1}\mathrm{lcm}(\ell_b(p_{t-1}),\omega(p_{t-1}))} + \sum_{X^{1-\frac{1}{t-1}}<k'<B^{1-\frac{2}{t}}} \sum_{X^{\frac{1}{t-1}}<p_{t-1}} \frac{B}{k'p_{t-1}\mathrm{lcm}(\ell_b(p_{t-1}),\omega(p_{t-1}))} .$$

For both sums the key tool will be Lemma 2. In the first case we have

$$\sum_{k'\leq X^{1-\frac{1}{t-1}}} \sum_{\frac{X}{k'}<p_{t-1}<\frac{B^{1-1/t}}{k'}} \frac{B}{k'p_{t-1}\mathrm{lcm}(\ell_b(p_{t-1}),\omega(p_{t-1}))} \leq \sum_{k'<X^{1-\frac{1}{t-1}}} \frac{B}{k'} \cdot \widetilde{O}\left(\frac{k'}{X}\right) = \widetilde{O}\left(\frac{B}{X^{\frac{1}{t-1}}}\right)$$

while in the second case we have

$$\sum_{X^{1-\frac{1}{t-1}}<k'<B^{1-\frac{2}{t}}} \sum_{X^{\frac{1}{t-1}}<p_{t-1}} \frac{B}{k'p_{t-1}\mathrm{lcm}(\ell_b(p_{t-1}),\omega(p_{t-1}))} \leq \sum_{X^{1-\frac{1}{t-1}}<k'<B^{1-\frac{2}{t}}} \frac{B}{k'} \cdot \widetilde{O}(X^{-\frac{1}{t-1}}) = \widetilde{O}\left(\frac{B}{X^{\frac{1}{t-1}}}\right) .$$

Since these arithmetic operations are on integers of size at most B, the result follows. □

Note that we are only utilizing the order statements for one prime in the pre-product; utilizing more seems quite difficult.

If the pre-product is prime and the pseudoprimes have two prime factors then the sum is easier to analyze, namely

$$\sum_{\substack{X<q<B \\ \gcd(\ell_b(q),\omega(q))\leq 2}} \frac{B}{q\mathrm{lcm}(\ell_b(q),\omega(q))}$$

which is $\widetilde{O}(B/X)$ by Lemma 2.

These two theorems form the main components of the analysis of Algorithm 1.

Theorem 5. *The worst-case asymptotic running time of Algorithm 1, when restricted to constructing pseudoprimes with t prime factors, is $\widetilde{O}(B^{1-\frac{1}{3t-1}})$ bit operations.*

The running time improves under a heuristic assumption that computing the gcd in the GCD step is more costly than factoring the gcd. The running time becomes $\widetilde{O}(B^{1-\frac{1}{2t-1}})$ bit operations when constructing (b,P,Q)-challenge pseudoprimes with t prime factors.

Proof. We balance the cost of the GCD step from Theorem 3 and the cost of the Sieve step from Theorem 4. The bottleneck in the GCD step is factoring, and balancing B/X with $B^{1/2}X^{3/2}$ gives $X = B^{1/5}$ and a running time with main term $B^{4/5}$ in the case $t = 2$. In practice, computing gcds was the bottleneck rather than factoring. If we assume this

holds in general, the cost of the GCD step is instead $\widetilde{O}(X^2)$. In the case $t = 2$, balancing X^2 with B/X gives $X = B^{1/3}$ and a running time with main term $B^{2/3}$.

For larger t, balancing $BX^{-\frac{1}{t-1}}$ with $B^{1/2}X^{3/2}$ gives $X = B^{\frac{t-1}{3t-1}}$ and a running time of $\widetilde{O}(B^{1-\frac{1}{3t-1}})$ bit operations. Under the heuristic assumption that the cost of the GCD step is instead $O(X^2)$, balancing with $BX^{-\frac{1}{t-1}}$ instead gives $X = B^{\frac{t-1}{2t-1}}$ and a running time of $\widetilde{O}(B^{1-\frac{1}{2t-1}})$.

Asymptotically smaller is the cost of finding all primes up to $B^{1/2}$. Applying the Fermat test and Lucas test to each composite constructed requires only $O(\log B)$ arithmetic operations per number on integers with $O(\log B)$ bits. □

7. Computational Notes and Conclusion

We implemented Algorithm 1 and verified there are no $(2, 1, -1)$-challenge pseudoprimes (i.e. PSW challenge pseudoprimes) with two or three prime factors less than 2^{80}. Since there are no primes up to 2^{40} which are simultaneously Weiferich and Wall-Sun-Sun, this claim includes composites with square factors.

If such a challenge pseudoprime with two prime factors were to be found, one of the primes would be admissible while satisfying $\epsilon(p) = 1$. This would be a surprising occurrence for the following reason. If $\epsilon(p) = 1$ then $\ell_b(p) \mid p - 1$ and $\omega(p) \mid p - 1$. Since $\ell_b(p)$ and $\omega(p)$ are usually large, it will usually happen that $\gcd(\ell_b(p), \omega(p)) > 2$. Thus it is notable that we found 7 admissible primes with $\epsilon(p) = 1$ while generating primes less than 2^{40}.

p	$\ell_2(p)$	$\omega(p)$
61681	40	1542
363101449	171436	1059
4278255361	80	6684774
4562284561	120	147934
4582537681	160453	1428
26509131221	748	14176006
422013019339	290442546	2906

One of the reasons the (b, P, Q) test is effective is because of conflicting divisibility conditions. The Fermat condition requires divisibility with respect to $n - 1$. The Lucas condition (with $\epsilon(n) = -1$) requires divisibility with respect to $n + 1$. Seemingly, this conflict will happen independent of the bases chosen. However, 2047 can be checked to be a $(2, 23, 131)$-challenge pseudoprime. The authors are curious how challenging such pseudoprimes are in general. Are there bases for which the subset-product method of construction makes the challenge only moderately challenging?

The authors also note the influence on this problem of the number sought at the end of [Wil77]. That number is simultaneously a Carmichael number, a Lucas pseudoprime to all sequences of a fixed discriminant, and has $\epsilon(n) = -1$, so it would certainly be a challenge pseudoprime. Williams shows that such a number has an odd number of prime factors, has more than three prime factors, and is not divisible by 3.

We conclude by offering our own rewards for exhibiting challenge pseudoprimes:

- \$20 for a $(2, 1, -1)$ challenge pseudoprime with an even number of prime factors,
- \$20 for a $(2, 1, -1)$ challenge pseudoprime with exactly three prime factors,
- \$6 for a $(2, 1, -1)$ challenge pseudoprime divisible by 3.

References

[Ble96] Daniel Bleichenbacher, *Efficiency and security of cryptosystems based on number theory*, Ph.D. thesis, Swiss Federal Institute of Technology Zurich, 1996.

[BW80] Robert Baillie and Samuel S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), no. 152, 1391–1417.

[CDP97] Richard Crandall, Karl Dilcher, and Carl Pomerance, *A search for wieferich and wilson primes*, Math. Comp. **66** (1997), 433–449.

[CG03] Zhuo Chen and John Greene, *Some comments on Baillie-PSW pseudoprimes*, Fibonacci Quart. **41** (2003), no. 4, 334–344.

[Fei13] Jan Feitsma, *Pseudoprimes*, http://www.janfeitsma.nl/math/psp2/index, 2013.

[GA99] Jon Grantham and Red Alford, *List of primes*, 1999, Available at http://pseudoprime.com/primes620.txt. Current as of 2/1/2018.

[Gil13] Jeff Gilchrist, *Pseudoprime enumeration with probabilistic primality tests*, http://gilchrist.ca/jeff/factoring/pseudoprimes.html, 2013.

[Gra01] Jon Grantham, *Frobenius pseudoprimes*, Math. Comp. **70** (2001), no. 234, 873–891.

[Jae93] Gerhard Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), no. 204, 915–926.

[JD14] Yupeng Jiang and Yingpu Deng, *Strong pseudoprimes to the first eight prime bases*, Math. Comp. (2014), 1–10 (electronic).

[JQ96] Marc Joye and Jean-Jacques Quisquater, *Efficient computation of full Lucas sequences*, Tech. Report CG-1996/3, Université Cathollque de Louvain, 1996, UCL Crypto Group Technical Report Series.

[Leh30] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448.

[Mur88] M. Ram Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59–67.

[Nic12] Thomas R. Nicely, *The Baillie-PSW primality test*, http://www.trnicely.net/misc/bpsw.html, 2012.

[Pin00] Richard G. E. Pinch, *The pseudoprimes up to* 10^{13}, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 459–473.

[Pom84] Carl Pomerance, *Are there counter-examples to the Baillie–PSW primality test*, 1984, item number 44 at https://www.math.dartmouth.edu/ carlp/. Current as of 6/4/2018.

[PSW80] Carl Pomerance, J. L. Selfridge, and Samuel S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), no. 151, 1003–1026.

[SW17] Jonathan Sorenson and Jonathan Webster, *Strong pseudoprimes to twelve prime bases*, Math. Comp. **86** (2017), no. 304, 985–1003.

[SZ04] Damien Stehlé and Paul Zimmermann, *A binary recursive gcd algorithm*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 411–425.

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, 2003.

[Wil77] H. C. Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bull. **20** (1977), no. 1, 133–143.