ENUMERATING HYPERELLIPTIC CURVES OVER FINITE FIELDS IN QUASILINEAR TIME

EVERETT W. HOWE

Abstract. We present an algorithm that, for every fixed genus g, will enumerate all hyperelliptic curves of genus g over a finite field k of odd characteristic in quasilinear time; that is, the time required for the algorithm is $\widetilde{O}(q^{2g-1})$, where $q = \#k$. Such an algorithm already exists in the case $g = 2$, thanks to work of Mestre and Cardona and Quer, and in the case $g = 3$, thanks to work of Lercier and Ritzenthaler. Experimentally, it appears that our new algorithm is about two orders of magnitude faster in practice than ones based on their work.

1. Introduction

There are many circumstances in which one may want to enumerate all hyperelliptic curves of a given genus over a given finite field. One may wish to determine whether a hyperelliptic curve with certain special properties exists — for instance, with a certain number of points [14, p. 393], or a certain zeta function, or a certain a-number [7, §4], or some other property of interest — and explicit enumeration allows for a direct search. Or perhaps one may wish to gather data about all hyperelliptic curves of a given genus over a given finite field — for example, in order to compute the distribution of the number of points on such curves, as in [1], or to determine experimental results [18] that can inspire future theorems [11].

In this paper we present, for every fixed genus $g > 1$, an algorithm to calculate a list of all hyperelliptic curves of genus g over a given finite field of odd characteristic.[1]

Theorem 1.1. *Fix an integer $g > 1$. Together, the algorithms we present in Section 7 provide a method for computing a complete list of hyperelliptic curves of genus g over $\mathbf{F}_q$ for odd prime powers q, with each curve appearing exactly once up to isomorphism. The algorithms take time $\widetilde{O}(q^{2g-1})$ and space $O(q^{2g-1})$.*

From [3, Proposition 7.1] and from the fact that a generic hyperelliptic curve has automorphism group of order 2, we see that there are roughly $2q^{2g-1}$ hyperelliptic curves of genus g over $\mathbf{F}_q$, so our algorithm runs in quasilinear time.

We also present an apparently new explicit enumeration of all monic irreducible homogeneous bivariate quartics over a finite field k of odd characteristic, up to the natural action of $\mathrm{PGL}_2(k)$ (see Section 2), which may be of independent interest.

Date: 20 June 2024.

2020 *Mathematics Subject Classification.* Primary 11G20; Secondary 11Y16, 14G15, 14H10, 14H25.

Key words and phrases. Hyperelliptic curve, finite field.

[1] Hyperelliptic curves in characteristic 2 are different from those in other characteristics in some basic ways, and, as we discuss later, there already exists an efficient algorithm for enumerating them.

Submitted to Algor. Num. Th. Symp.

Theorem 1.2. *Given an odd prime power q, let γ be a nonzero element of $\mathbf{F}_{q^4}$ whose multiplicative order is $2(q^2-1)$ and let ρ be an element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$ with $\rho^2 \in \mathbf{F}_q$. Let S_4 be the union of the two sets*

$$\left\{(\gamma^i - 1)/(\gamma^i + 1) \mid i \text{ odd}, \ 1 \le i \le (q+1)/2\right\}$$

and

$$\left\{\rho(\gamma^i - 1)/(\gamma^i + 1) \mid i \text{ odd}, \ 1 \le i \le (q-1)/2\right\}.$$

Then the homogenized minimal polynomials of the elements of S_4 provide a complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic irreducible homogeneous bivariate quartics over $\mathbf{F}_q$.

We prove this in Section 3. Also, here and elsewhere, when we say we have a "complete set of unique representatives" for an action of a group on a set, we mean that we have a set of orbit representatives that contains exactly one member from each orbit.

Briefly, there are two main ideas behind the algorithms that give us Theorem 1.1. The first is that there is an easy way to tell whether two irreducible homogeneous polynomials in $\mathbf{F}_q[x,y]$ lie in the same orbit under the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ — see Theorem 4.2. We use this fact to reduce the problem of getting a list of all hyperelliptic curves *without* duplicates in quasilinear time to the problem of getting a list of hyperelliptic curves with a *bounded number* of duplicates in quasilinear time. The second is that if one understands the cosets of $\mathrm{PGL}_2(\mathbf{F}_q)$ in $\mathrm{PGL}_2(\mathbf{F}_{q^2})$, and if one has a list of orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ acting on irreducible homogenous polynomials of degree n in $\mathbf{F}_{q^2}[x,y]$, then one can get a list of orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on irreducible homogenous polynomials of degree $2n$ in $\mathbf{F}_q[x,y]$ — see Section 7.4. The point of this observation is that the number of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ orbits of irreducible degree-n polynomials over $\mathbf{F}_{q^2}$ is on the order of q^{2n-6}, while the number of $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of degree-$2n$ polynomials over $\mathbf{F}_q$ is roughly q^{2n-3}, so the former is easier to compute than the latter.

The algorithm for enumerating hyperelliptic curves that we present is designed for simplicity of argument, rather than for efficiency of computation. In Section 8 we describe modifications that will make the algorithm more efficient, and in Section 9 we present even more details and timings for the case of genus 2 and genus 3.

An obvious issue with our algorithm, as we present it here, is that it requires $O(q^{2g-1})$ space. This is because our initial computations often produce some duplicate entries, and we eliminate these duplicates by collecting all the output, computing some invariants, and then discarding entries whose invariants have already been seen. In a followup paper [9], we show how it is possible to modify the techniques presented here in order to get a quasilinear time algorithm for computing genus-g hyperelliptic curves over $\mathbf{F}_q$ that only requires $O(\log q)$ space. Our implementation of the genus-2 case of the algorithm from the present paper uses a basic version of the ideas from [9], and it would not be hard to modify the genus-2 code we provide in [10] so that it requires only $O(q)$ space.

We start by considering various reductions, special cases, and lemmas. In Section 2 we show that enumerating hyperelliptic curves of genus g over a finite field k of odd characteristic can be reduced to enumerating Galois-stable sets of $2g+2$ elements of $\mathbf{P}^1(\overline{k})$ up to the natural action of $\mathrm{PGL}_2(k)$. The rest of the paper is therefore concerned mostly with the latter problem, which we solve for all finite fields, not just those of odd characteristic. In Section 3 we prove Theorem 1.2,

as well as similar results for quartics with one or two irreducible quadratic factors and generalizations to characteristic 2. In Section 4 we introduce an invariant for $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of monic irreducible homogeneous bivariate polynomials of degree $n \geq 4$ over $\mathbf{F}_q$, and we use it to provide a very straightforward algorithm for giving a complete set of unique representatives for these orbits in time $\widetilde{O}(q^{n-2})$. In Sections 5 and 6 we give an explicit enumeration of a complete set of unique representatives for the cosets of $\mathrm{PGL}_2(\mathbf{F}_q)$ in $\mathrm{PGL}_2(\mathbf{F}_{q^p})$ for primes p. The case $p = 2$ is the key result needed for the most difficult case of our algorithm to enumerate hyperelliptic curves. In Section 7 we use the results of the earlier sections to present a collection of algorithms that, together, give a complete set of unique representatives for the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of Galois stable sets of $2g+2$ elements of $\mathbf{P}^1(\overline{\mathbf{F}}_q)$. We close with Sections 8 and 9, described above.

For many of our algorithms we require an easily computable total ordering of the elements of $\mathbf{F}_q$ or of polynomials in $\mathbf{F}_q[x]$ or in $\mathbf{F}_q[x,y]$. We will always denote such an ordering by "$<$" and we leave the reader to choose their favorite one. Also, if the proof of a proposition is clear, we indicate that the proof will be skipped by including an end-of-proof mark in the statement of the result.

Acknowledgements. I am grateful to the referees for ANTS, who provided helpful feedback that improved this paper.

2. Hyperelliptic curves and Weierstrass points

We begin by setting some general notation. Given a finite field k, let R be the graded polynomial ring $k[x,y]$, with the grading given by the degree. For each n let R_n be the set of homogeneous polynomials in R of degree n and let R_{hom} be the union of the R_n. We say that $f \in R_{\mathrm{hom}}$ is *monic* if $f(x,1)$ is monic as a univariate polynomial, and we say that f is *separable* if in $\overline{k}[x,y]$ it can be written as a constant times a product of distinct monic linear factors. We say that $\alpha \in \overline{k}$ is a *root* of f if $f(\alpha,1) = 0$, and that $[\alpha:\beta] \in \mathbf{P}^1(\overline{k})$ is a *zero* of f if $f(\alpha,\beta) = 0$.

We also define a left action of $\mathrm{PGL}_2(k)$ on $R_{\mathrm{hom}}/k^\times$ as follows. If Γ is an element of $\mathrm{PGL}_2(k)$ represented by a matrix $M := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and if f lies in R_{hom}, we define $\Gamma(f \bmod k^\times)$ to be the class in $R_{\mathrm{hom}}/k^\times$ of $f(dx-by, -cx+ay)$.

Every class of $R_{\mathrm{hom}}/k^\times$ contains a unique monic element, and we define an action of $\mathrm{PGL}_2(k)$ on the monic elements of R_{hom} by writing $\Gamma(f) = g$ when g is the monic element of $\Gamma(f \bmod k^\times)$. If Γ is represented by a matrix $M := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and if $\Gamma(f) = g$, then $f(dx-by,-cx+ay) = eg(x,y)$ for some $e \in k^\times$, and if we choose a different matrix to represent Γ, then the constant e will be multiplied by an nth power. When n is even, the class of e in $k^\times/k^{\times 2}$ therefore depends only on Γ, and we denote this square class by $s_{\Gamma,f}$.

Given a separable polynomial $f \in R_{\mathrm{hom}}$, we let $\mathrm{Zeros}(f)$ denote the set of zeros of f in $\mathbf{P}^1(\overline{k})$, so that $\mathrm{Zeros}(f)$ consists of the roots of f under the usual inclusion $\overline{k} \subset \mathbf{P}^1(\overline{k})$ given by $\alpha \mapsto [\alpha:1]$, together with $\infty := [1:0] \in \mathbf{P}^1(\overline{k})$ if f is divisible by y. For every integer $n \geq 0$ we let $\mathrm{Sym}^n(k)$ denote the set of all Galois-stable sets of n distinct points in $\mathbf{P}^1(\overline{k})$, so that the natural action of $\mathrm{PGL}_2(k)$ on $\mathbf{P}^1(\overline{k})$ leads to an action of $\mathrm{PGL}_2(k)$ on $\mathrm{Sym}^n(k)$. We see that Zeros gives us a bijection between the set of monic separable polynomials in R_n and the set $\mathrm{Sym}^n(k)$, and we check that $\mathrm{Zeros}(\Gamma(f)) = \Gamma(\mathrm{Zeros}(f))$ for all $f \in R_{\mathrm{hom}}$.

Our goal in this paper is to produce an algorithm to enumerate hyperelliptic curves of a given genus g over finite fields k of odd characteristic. As a first step, we reduce this problem to the problem of computing representatives for all $\mathrm{PGL}_2(k)$ orbits of $\mathrm{Sym}^n(k)$, where $n = 2g + 2$.

Let k be a finite field of odd characteristic and let C be a hyperelliptic curve over k, that is, a curve of genus $g > 1$ with a degree-2 map to a curve of genus 0. Every genus-0 curve over a finite field is isomorphic to $\mathbf{P}^1$, and since our k has odd characteristic C can be written in the form $z^2 = \tilde{f}$, where $\tilde{f} \in k[x]$ is a separable polynomial of degree $2g+1$ or $2g+2$. We can rewrite this as a model $z^2 = f(x, y)$ in weighted projective space by homogenizing $\tilde{f}$ into a polynomial $f \in R_{2g+2}$; here we give the coordinates x and y weight 1 and the coordinate z weight $g + 1$. Then the map $[x : y : z] \mapsto [x : y]$ gives the double cover $C \to \mathbf{P}^1$, and the points of $\mathbf{P}^1$ that ramify in this map are exactly the elements of $\mathrm{Zeros}(f)$. If C_1 and C_2 are two hyperelliptic curves, given by equations $z^2 = f_1$ and $z^2 = f_2$, then every isomorphism from C_1 to C_2 can be written in the form

$$[x : y : z] \mapsto [ax + by : cx + dy : ez],$$

where $ad - bc$ and e are nonzero, and where

$$e^2 f_1(x, y) = f_2(ax + by, cx + dy); \tag{1}$$

see [17, Corollary 7.4.33]. Then $e^2 f_1(dx - by, -cx + ay) = (ad - bc)^{2g+2} f_2(x, y)$, so we see that $f_2 \bmod k^\times = \Gamma(f_1 \bmod k^\times)$, where $\Gamma \in \mathrm{PGL}_2(k)$ is the element represented by the matrix $M := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. Thus, if C_1 and C_2 are isomorphic, the element Γ of $\mathrm{PGL}_2(k)$ takes the ramification points of $C_1 \to \mathbf{P}^1$ to the ramification points of $C_2 \to \mathbf{P}^1$. Conversely, if $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{PGL}_2(k)$ takes the ramification points of $C_1 \to \mathbf{P}^1$ to the ramification points of $C_2 \to \mathbf{P}^1$, then there is an $e \in \overline{k}$, with $e^2 \in k$, that makes (1) hold. If e lies in k, we have an isomorphism between C_1 and C_2; if e does not lie in k, we have an isomorphism between C_1 and the *quadratic twist* of C_2, that is, the curve $y^2 = \nu f_2$, where ν is a nonsquare in k. (In general, a *twist* of a curve C over a finite field k is another curve over k that becomes isomorphic to C when the base field is extended to an algebraic closure of k. Twists of C correspond to elements of the cohomology set $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}_{\overline{k}} C)$ — see [21, §III.1.3] — and by "the quadratic twist" of a hyperelliptic curve we mean the twist corresponding to the cocycle that sends the Frobenius element of $\mathrm{Gal}(\overline{k}/k)$ to the hyperelliptic involution. Note that sometimes the quadratic twist may in fact be the trivial twist.)

Thus, we have a map from the set of isomorphism classes of genus-g hyperelliptic curves over k to the set of $\mathrm{PGL}_2(k)$ orbits of $\mathrm{Sym}^n(k)$, where $n = 2g + 2$. This map is clearly surjective, and the $\mathrm{PGL}_2(k)$ orbit of an element A of $\mathrm{Sym}^n(k)$ has at most two preimages in the set of isomorphism classes of hyperelliptic curves: the isomorphism classes of $y^2 = f$ and of $y^2 = \nu f$, where f is the unique monic polynomial with $\mathrm{Zeros}(f) = A$ and where ν is a nonsquare in k. (We say "at most two" preimages because, as we noted above, these two curves may be isomorphic to one another.)

Whether an element A of $\mathrm{Sym}^n(k)$ has one or two preimages is easy to determine: Let $f \in R_n$ be the unique monic polynomial with $\mathrm{Zeros}(f) = A$. Compute all elements Γ of $\mathrm{PGL}_2(k)$ that take the set A to itself; at worst this takes time $O(n(n-1)(n-2))$, and since n is fixed in our context, this is $O(1)$ operations. For each such Γ compute the element $s_{\Gamma,f}$ of $k^\times/k^{\times 2}$. If any of these elements is

nontrivial, then the curve $y^2 = f$ is isomorphic to its twist $y^2 = \nu f$. (Compare to [20, Lemma 1.2].)

This shows that if we can compute a complete set of unique representatives for the orbits of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on $\mathrm{Sym}^{2g+2}(\mathbf{F}_q)$ in time $\widetilde{O}(q^{2g-1})$, we can also compute a complete set of unique representatives for the hyperelliptic curves of genus g over $\mathbf{F}_q$ in time $\widetilde{O}(q^{2g-1})$. Thus, for the rest of this paper we focus on enumerating the $\mathrm{PGL}_2(k)$ orbits of $\mathrm{Sym}^n(k)$, for $n = 2g+2$. In particular, for our application to enumerating hyperelliptic curves we only need to consider even n that are at least 6. The algorithms that we present for the latter problem work for all finite fields, not just those of odd characteristic.

Remark 2.1. Over a finite field $\mathbf{F}_q$ of characteristic 2 there are still roughly $2q^{2g-1}$ hyperelliptic curves of genus g, but it is much easier to enumerate them in quasi-linear time than it is in odd characteristic, because the ramification divisor of the hyperelliptic structure map $C \to \mathbf{P}^1$ is supported on at most $g+1$ points. Enumerating the possible ramification divisors up to the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ in time $\widetilde{O}(q^{2g-1})$ is therefore much simpler than in odd characteristic, and enumerating the curves with a given ramification divisor is relatively straightforward. The algorithm of Xarles [24] follows this outline; it has been implemented by him in genus 4, by Dragutinović [6] in genus 5, and by Huang, Kedlaya, and Lau [12] in genus 6.

3. Results for quartic polynomials

In this section we prove Theorem 1.2. We also prove similar results that give complete sets of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on monic homogeneous quartics that have one or two irreducible quadratic factors, and we state generalizations to finite fields of characteristic 2. We begin with an elementary lemma.

Lemma 3.1. *Let k be a field and let a, b, c, and d be distinct elements of $\mathbf{P}^1(k)$. Then there is a unique element of $\mathrm{PGL}_2(k)$ that swaps a with b and c with d, and this element is an involution.*

Proof. An element of $\mathrm{PGL}_2(k)$ is determined by where it sends three distinct elements of $\mathbf{P}^1(k)$, so the uniqueness is automatic, and we need only prove existence. By using the action of $\mathrm{PGL}_2(k)$, we see that it suffices to prove the lemma in the case where $a = \infty$, $b = 0$, and $c = 1$. Then the element $\left[\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right]$ of $\mathrm{PGL}_2(k)$ is an involution that swaps a with b and c with d. □

Corollary 3.2. *Let q be a prime power and let α, β, γ, and δ be distinct elements of $\overline{\mathbf{F}}_q$ such that $\{\{\alpha,\beta\},\{\gamma,\delta\}\} = \{\{\alpha^q,\beta^q\},\{\gamma^q,\delta^q\}\}$. Then there is a unique element of $\mathrm{PGL}_2(\mathbf{F}_q)$ that swaps α with β and γ with δ, and this element is an involution.*

Proof. Let $\Gamma \in \mathrm{PGL}_2(\overline{\mathbf{F}}_q)$ be the involution that swaps α with β and γ with δ. Then $\Gamma^{(q)}$, by which we mean the element of $\mathrm{PGL}_2(\overline{\mathbf{F}}_q)$ obtained by taking a representative matrix for Γ and replacing all of its entries by their qth powers, is also an involution that swaps α with β and γ with δ, because of the equality of sets in our hypothesis. By the uniqueness property in Lemma 3.1, it follows that $\Gamma^{(q)} = \Gamma$ in $\mathrm{PGL}_2(\overline{\mathbf{F}}_q)$, from which we see that Γ actually lies in $\mathrm{PGL}_2(\mathbf{F}_q)$. □

Proof of Theorem 1.2. First we show that every monic irreducible quartic in $\mathbf{F}_q[x]$ can be transformed into one of the quartics in the statement of the theorem; this

is equivalent to showing that every irreducible quartic has a root in $\mathbf{F}_{q^4}$ that can be moved by $\mathrm{PGL}_2(\mathbf{F}_q)$ to an element of the set S_4 from the theorem.

In the statement of the theorem we chose an element ρ of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$ with $\rho^2 \in \mathbf{F}_q$. Let $\nu = \rho^2$, so that ν is a nonsquare in $\mathbf{F}_q$.

Let f be an irreducible quartic in $\mathbf{F}_q[x]$, let α be a root of f in $\mathbf{F}_{q^4}$, and set $\alpha_1 := \alpha$, $\alpha_2 := \alpha_1^q$, $\alpha_3 := \alpha_2^q$, and $\alpha_4 := \alpha_3^q$. By Corollary 3.2 there is a unique involution Γ in $\mathrm{PGL}_2(\mathbf{F}_q)$ that swaps α_1 with α_3 and α_2 with α_4. We refer to this as the involution associated to f.

Let Φ be an element of $\mathrm{PGL}_2(\mathbf{F}_q)$. Then the involution associated to $\Phi(f)$ is $\Phi\Gamma\Phi^{-1}$. Since every involution in $\mathrm{PGL}_2(\mathbf{F}_q)$ is conjugate either to $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & \nu \\ 1 & 0 \end{smallmatrix}\right]$, we can choose Φ so that $\Phi\Gamma\Phi^{-1}$ is one of these two standard involutions. Now we replace f with $\Phi(f)$, α with $\Phi(\alpha)$, and Γ with $\Phi\Gamma\Phi^{-1}$.

Suppose $\Gamma = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. The subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ that stabilizes Γ under conjugation is

$$H_1 := \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \;\middle|\; a^2 \neq b^2 \right\} \cup \left\{ \begin{bmatrix} -a & -b \\ b & a \end{bmatrix} \;\middle|\; a^2 \neq b^2 \right\}.$$

We would like to apply an element of H_1 to α, and if necessary replace α with one of its conjugates, to put α into a standard form. We accomplish this by considering the function $\mathbf{P}^1(\mathbf{F}_{q^4}) \to \mathbf{P}^1(\mathbf{F}_{q^4})$ given by applying the element $\Psi := \left[\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right]$ of $\mathrm{PGL}_2(\mathbf{F}_q)$. Since Ψ conjugates Γ to the involution $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, we see that $\Psi(\alpha)^{q^2} = -\Psi(\alpha)$. This shows that $\Psi(\alpha)^{q^2-1} = -1$, so the multiplicative order of $\Psi(\alpha)$ is even and divides $2(q^2-1)$. It follows that we may write $\Psi(\alpha) = \gamma^i$ for some odd integer i with $0 < i < 2(q^2-1)$.

Let

$$H_1' := \Psi H_1 \Psi^{-1} = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \;\middle|\; a \in \mathbf{F}_q^\times \right\} \cup \left\{ \begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix} \;\middle|\; a \in \mathbf{F}_q^\times \right\}.$$

Then applying an element of H_1 to α corresponds to applying an element of H_1' to $\Psi(\alpha)$, and the elements of H_1' either multiply $\Psi(\alpha)$ by an element of $\mathbf{F}_q^\times$ or replace $\Psi(\alpha)$ with its inverse times an element of $\mathbf{F}_q^\times$. Since the elements of $\mathbf{F}_q^\times$ are the powers of $\gamma^{2(q+1)}$, these two actions show that there is a $\Phi' \in H_1'$ such that $\Phi'(\Psi(\alpha)) = \gamma^i$ for an odd integer i with $0 < i < q+1$. If we let $\Phi = \Psi^{-1}\Phi'\Psi \in H_1$ and replace α with $\Phi(\alpha)$, we find that $\Psi(\alpha) = \gamma^i$ for this i.

Finally, replacing α with α^q has the effect of replacing i with iq. If we write $i = 2h+1$ we see that

$$iq \equiv 2hq + q \equiv -2h + q \equiv -(2h+1) + (q+1) \equiv q + 1 - i \bmod 2(q+1),$$

so by replacing α with its conjugate α^q, if necessary, and then modifying the new α by an element of H_1, we find that we may assume that $0 < i \leq (q+1)/2$.

We see that every irreducible quartic whose associated involution is $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ has a root in the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of $\Psi^{-1}(\gamma^i) = (\gamma^i - 1)/(\gamma^i + 1)$, for some odd i with $0 < i \leq (q+1)/2$. Moreover, from our analysis it is clear that different values of i in this range produce quartics in distinct $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits.

Next, suppose the involution associated with a quartic f is $\Gamma = \left[\begin{smallmatrix} 0 & \nu \\ 1 & 0 \end{smallmatrix}\right]$. The subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ that stabilizes Γ under conjugation is

$$H_\nu := \left\{ \begin{bmatrix} a & b\nu \\ b & a \end{bmatrix} \;\middle|\; a^2 \neq \nu b^2 \right\} \cup \left\{ \begin{bmatrix} -a & -b\nu \\ b & a \end{bmatrix} \;\middle|\; a^2 \neq \nu b^2 \right\}.$$

As before, we would like to apply an element of H_ν to α, and if necessary replace α with one of its conjugates, to put α into a standard form. This time we consider the function $\mathbf{P}^1(\mathbf{F}_{q^4}) \to \mathbf{P}^1(\mathbf{F}_{q^4})$ given by applying the element $\Psi := \left[\begin{smallmatrix} 1 & \rho \\ -1 & \rho \end{smallmatrix}\right]$ of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$, where ρ is the element of $\mathbf{F}_{q^2}$ chosen in the statement of the theorem and $\nu = \rho^2$. Then Ψ conjugates Γ to the involution $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, and once again we have $\Psi(\alpha)^{q^2} = -\Psi(\alpha)$. As before, we see that $\Psi(\alpha)^{q^2-1} = -1$, so $\Psi(\alpha)$ has multiplicative order dividing $2(q^2-1)$. Once again we may write $\Psi(\alpha) = \gamma^i$ for some odd integer i with $0 < i < 2(q^2-1)$.

Let $H'_\nu := \Psi H_\nu \Psi^{-1}$ and let N be the kernel of the norm map from $\mathbf{F}_{q^2}^\times$ to $\mathbf{F}_q^\times$. We check that

$$H'_\nu = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \;\middle|\; a \in N \right\} \cup \left\{ \begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix} \;\middle|\; a \in N \right\}.$$

Then applying an element of H_ν to α corresponds to applying an element of H'_ν to $\Psi(\alpha)$, and the elements of H'_ν either multiply $\Psi(\alpha)$ by an element of N or replace $\Psi(\alpha)$ with its inverse times an element of N.

The elements of N are the powers of $\gamma^{2(q-1)}$, so arguing as before we find that we may replace α with $\Phi(\alpha)$ for some $\Phi \in H_\nu$ so that $\Psi(\alpha) = \gamma^i$ for an odd i with $0 < i < q-1$. We check that $\Psi(\alpha^q) = 1/\Psi(\alpha)^q$, so replacing α with α^q has the effect of replacing i with $-iq$. If we write $i = 2h-1$ we see that

$$-iq \equiv -2hq + q \equiv -2h + q \equiv (-2h+1) + (q-1) \equiv q - 1 - i \bmod 2(q-1),$$

so by replacing α with its conjugate α^q, if necessary, we find that we may assume that $0 < i \leq (q-1)/2$.

We see that every irreducible quartic whose associated involution is $\left[\begin{smallmatrix} 0 & \nu \\ 1 & 0 \end{smallmatrix}\right]$ has a root in the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of $\Psi^{-1}(\gamma^i) = \rho(\gamma^i - 1)/(\gamma^i + 1)$, for some odd i with $0 < i \leq (q-1)/2$, and different values of i in this range give irreducible quartics that are not equivalent to one another under the action of $\mathrm{PGL}_2(\mathbf{F}_q)$. □

Remark 3.3. For a separable quartic $f = x^4 + ax^3y + bx^2y^2 + cxy^3 + dy^4$, we let $j(f)$ denote the j-invariant of the Jacobian of the genus-0 curve $z^2 = f$. One can show that $j(f) = 256(b^2 - 3ac + 12d)^3/\Delta$, where Δ is the discriminant of f, and clearly $j(\Gamma(f)) = j(f)$ for all $\Gamma \in \mathrm{PGL}_2(\mathbf{F}_q)$, because the curve $z^2 = \Gamma(f)$ is geometrically isomorphic to $z^2 = f$. Using arguments from [8, §3], one can show that j takes different values on irreducible quartics that are not in the same $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit.

For products of two distinct irreducible quadratics, we have a similar result.

Theorem 3.4. *Given an odd prime power q, let ζ be a generator of $\mathbf{F}_{q^2}^\times$, let ρ be an element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$ with $\rho^2 \in \mathbf{F}_q$, and let $\nu = \rho^2$. Let*

$$S_{22} = \{\rho(\zeta^i - 1)/(\zeta^i + 1) \mid 0 < i \leq (q-1)/2\}$$

and let T_{22} be the set of homogenized minimal polynomials of the elements of S_{22}. Then the set $\{(x^2 - \nu y^2)g \mid g \in T_{22}\}$ is a complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the homogeneous quartics that factor into a product of two distinct monic irreducible quadratics.

Proof. Let f be a homogeneous quartic that factors into a product of two monic irreducible quadratics, so that the roots of f are α, $\overline{\alpha}$, β, and $\overline{\beta}$, for two elements α and β in $\mathbf{F}_{q^2}$ with conjugates $\overline{\alpha}$ and $\overline{\beta}$. We will show that there is a unique element

σ in S_{22} such that the set $\{\alpha, \overline{\alpha}, \beta, \overline{\beta}\}$ can be sent to $\{\rho, \overline{\rho}, \sigma, \overline{\sigma}\}$ by an element of $\mathrm{PGL}_2(\mathbf{F}_q)$. This will be enough to prove the theorem.

By replacing f with its image under an element of $\mathrm{PGL}_2(\mathbf{F}_q)$ we may assume that $\alpha = \rho$. The subgroup of $\mathrm{PGL}_q(\mathbf{F}_q)$ that fixes the set $\{\rho, \overline{\rho}\}$ is the group H_ν from the proof of Theorem 1.2. Let $\Psi := \left[\begin{smallmatrix} 1 & \rho \\ -1 & \rho \end{smallmatrix}\right]$. Arguing as in the proof of Theorem 1.2 we find that there is a unique element Γ of H_ν so that we can write $\Psi(\Gamma(\beta))$ as ζ^i for an integer i with $0 < i \le (q-1)/2$.

Since by Corollary 3.2 there is an element of $\mathrm{PGL}_2(\mathbf{F}_q)$ that swaps α and $\overline{\alpha}$ with β and $\overline{\beta}$, we would have gotten the same value of i if we had normalized β and $\overline{\beta}$ to be ρ and $\overline{\rho}$ at the beginning of our argument, instead of α and $\overline{\alpha}$. Thus the value of i we obtain truly depends only on the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of f.

This shows that we may assume that $\beta = \Psi^{-1}(\zeta^i)$ is an element of S_2, and different elements of S_2 correspond to different $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits. The theorem follows. □

Remark 3.5. If f is a homogeneous quartic in $\mathbf{F}_q[x, y]$ that can be factored into the product of two monic irreducible quadratics $x^2 + sxy + ty^2$ and $x^2 + uxy + vy^2$, we define

$$\mu(f) := \frac{(su - 2t - 2v)^2}{(s^2 - 4t)(u^2 - 4v)},$$

and we check that $j(f) = 64(\mu(f)+3)^3/(\mu(f)-1)^2$, where $j(f)$ is as in Remark 3.3. Note that $\mu(f)$ is a square, because the two factors in the denominator are the discriminants of the irreducible factors of f.

We leave it to the reader to check that for f of this form we have $\mu(\Gamma(f)) = \mu(f)$ for every $\Gamma \in \mathrm{PGL}_2(\mathbf{F}_q)$, so μ is an invariant of the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of such quartics. Given any square d in $\mathbf{F}_q$ other than 1, we check that a quartic $f := (x^2 - \nu y^2)(x^2 + uxy + vy^2)$ satisfies $\mu(f) = d$ if and only if (u, v) lies on a certain nonsingular conic. Nonsingular conics over finite fields have rational points not on the line at infinity, so there are values of u and v that give a quartic for which μ attains the value d. Since μ attains $(q-1)/2$ different values, μ must take different values on the $(q-1)/2$ orbits of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on products of irreducible quadratics.

One can show that μ is derived from a modular function that parametrizes pairs (E, P), where E is an elliptic curve and P is a point of order 2. For products $f_1 f_2$ of two irreducible quadratics, the elliptic curve is the Jacobian of the curve $C\colon z^2 = f_1 f_2$, and the point of order 2 is represented by the degree-0 divisor on C whose double is the divisor of f_1/f_2.

We also have a similar result for quartics with exactly one irreducible quadratic factor, which works in all characteristics.

Theorem 3.6. *Given a prime power q, let ζ be a generator of $\mathbf{F}_{q^2}^\times$. Let*

$$S_{211} = \{\zeta^i \mid 0 < i \le (q+1)/2\}$$

and let T_{211} be the set of homogenized minimal polynomials of the elements of S_{211}. Then the set $\{xyg \mid g \in T_{211}\}$ is a complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic separable homogeneous quartics that have exactly one irreducible quadratic factor.

Proof. The proof follows the same lines as that of Theorem 3.4, but is much simpler. We move the two rational roots of f to 0 and ∞, and then show that up to scaling

and inversion, every element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$ has a unique representative in S_{211}. We leave the details to the reader. □

Remark 3.7. The function μ defined in Remark 3.5 can be extended to monic separable quartics with exactly one irreducible quadratic factor; when the two zeros of f in $\mathbf{P}^1(\mathbf{F}_q)$ are finite we can use the same formula as before, and when $f = y(x - by)(x^2 + ux + v)$ we can define $\mu(f) = (u + 2b)^2/(u^2 - 4v)$. Once again, μ depends only on the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of its argument. On quartics of this type, the set of values attained by μ is the set of nonsquares in $\mathbf{F}_q$ together with 0. Thus, μ distinguishes $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of such quartics from one another.

Theorem 3.6 applies to all finite fields, while Theorems 1.2 and 3.4 require the characteristic to be odd. The following theorem generalizes the latter two results to characteristic 2. The proof is analogous to those of the earlier theorems, but is made much simpler by the fact that in this case every involution in $\mathrm{PGL}_2(\mathbf{F}_q)$ is conjugate to $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. We leave the details to the reader.

Theorem 3.8. *Let q be a power of 2, let A be the set of elements of $\mathbf{F}_q$ of absolute trace 1, and let ν be an element of A. Then the set*

$$\left\{(x^4 + x^2y^2) + a(x^2y^2 + xy^3) + a^2\nu y^4 \mid a \in A\right\}$$

is a complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic irreducible homogeneous quartics over $\mathbf{F}_q$, and the set

$$\left\{(x^2 + xy + \nu y^2)(x^2 + xy + ay^2) \mid a \in A, a \neq \nu\right\}$$

is a complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the homogeneous quartics over $\mathbf{F}_q$ that can be written as the product of two distinct monic irreducible quadratics. □

Remark 3.9. Theorems 1.2, 3.4, 3.6, and 3.8 lead to quasilinear-time algorithms to give complete sets of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the various types of quartics discussed in the theorems. The only difficulty is obtaining a primitive element ζ for $\mathbf{F}_{q^2}$ in Theorems 3.4 and 3.6 and an element γ of order $2(q^2-1)$ in $\mathbf{F}_{q^4}$ for Theorem 1.2. But primitive elements for $\mathbf{F}_{q^2}$ can be determined deterministically in time $O(q^{1/2+\varepsilon})$ for every $\varepsilon > 0$ (see [23]), and the γ required for Theorem 1.2 can be obtained by taking the square root in $\mathbf{F}_{q^4}$ of a primitive element for $\mathbf{F}_{q^2}$.

In quasilinear time we can also create a table of size $O(q)$ that we can use to invert the function μ, which gives us a way to compute the orbit representatives of quartics with one or two irreducible quadratic factors. The function μ does not reduce well modulo 2, but the function $(\mu - 1)/4$ does; the corresponding function takes a product $(x^2 + sxy + ty^2)(x^2 + uxy + vy^2)$ in characteristic 2 to $((t + v)^2 + (s + u)(sv + tu))/(su)^2$.

4. An invariant for irreducible polynomials over finite fields

In this section we define an easily computable invariant[2] for monic irreducible homogeneous bivariate polynomials of arbitrary degree $n \geq 4$ over a finite field $\mathbf{F}_q$

[2]Classically, an *invariant* on the set $R_n \subset k[x, y]$ of homogeneous bivariate polynomials of degree n is a function $R_n \to k$ that is constant on $\mathrm{PGL}_2(k)$ orbits. We use the term more generally here, and simply mean a function from R_n to *any* set that is constant on $\mathrm{PGL}_2(k)$ orbits.

under the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ mentioned in Section 2. The invariant is based on the classical *cross ratio*, which is the function that assigns to an ordered quadruple (P_1, P_2, P_3, P_4) of distinct elements of $\mathbf{P}^1(\overline{k})$ the element $\alpha \in \overline{k}$ for which $\Gamma(P_4) = [\alpha : 1]$, where Γ is the unique element of $\mathrm{PGL}_2(\overline{k})$ that sends P_1 to ∞, P_2 to 0, and P_3 to 1. It follows that the cross ratio is constant on the orbits of the diagonal action of $\mathrm{PGL}_2(\overline{k})$ on such quadruples, and takes distinct values on distinct orbits. (Compare to [5, Definition III.3.7] and the propositions following it.)

Definition 4.1. Let q be a prime power and let f be a monic irreducible homogeneous bivariate polynomial of degree $n \geq 4$ over $\mathbf{F}_q$. We define the *cross polynomial* $\mathrm{Cross}(f)$ of f as follows: Let $\alpha \in \mathbf{F}_{q^n}$ be a root of f, and let $\chi \in \mathbf{F}_{q^n}$ be the cross ratio of α, α^q, α^{q^2}, and α^{q^3}; that is,

$$\chi := \frac{(\alpha^{q^3} - \alpha^q)(\alpha^{q^2} - \alpha)}{(\alpha^{q^3} - \alpha)(\alpha^{q^2} - \alpha^q)}.$$

Then set $\mathrm{Cross}(f)$ to be the characteristic polynomial of χ over $\mathbf{F}_q$.

Note that the denominator of χ is nonzero, because the powers of α involved are four of the n distinct conjugates of α. Also, replacing α with one of its conjugates results in replacing χ with a conjugate, so the characteristic polynomial remains unchanged. Thus we see that $\mathrm{Cross}(f)$ is well-defined.

Theorem 4.2. *Let q be a prime power. Two monic irreducible homogenous polynomials in $\mathbf{F}_q[x, y]$ of degree at least 4 lie in the same orbit under the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ if and only if they have the same cross polynomial.*

Proof. Suppose f and g are irreducible homogenous polynomials in $\mathbf{F}_q[x, y]$ of degree at least 4. Suppose f and g lie in the same $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit, say $g = \Gamma(f)$ for some $\Gamma \in \mathrm{PGL}_2(\mathbf{F}_q)$. Then f and g have the same degree, which we denote by n. Let α be a root of f in $\mathbf{F}_{q^n}$ and let $\beta = \Gamma(\alpha)$. Then β is a root of g, and for every $i \geq 0$ we have $\beta^{q^i} = \Gamma(\alpha^{q^i})$. In particular, the cross ratio of α, α^q, α^{q^2}, and α^{q^3} is equal to the cross ratio of β, β^q, β^{q^2}, and β^{q^3}, so $\mathrm{Cross}(f) = \mathrm{Cross}(g)$.

Conversely, suppose f and g are two monic irreducible polynomials of degree at least 4 with $\mathrm{Cross}(f) = \mathrm{Cross}(g)$. Since a polynomial has the same degree as its cross polynomial, f and g have the same degree, say n. Since the cross polynomials are equal, there are roots α of f and β of g in $\mathbf{F}_{q^n}$ such that α, α^q, α^{q^2}, and α^{q^3} have the same cross ratio as β, β^q, β^{q^2}, and β^{q^3}. It follows that there is an element Γ of $\mathrm{PGL}_2(\mathbf{F}_{q^n})$ with $\Gamma(\alpha^{q^i}) = \beta^{q^i}$ for $0 \leq i \leq 3$. In particular, we have $\Gamma(x^q) = \Gamma(x)^q$ for three distinct values of x, namely α, α^q, and α^{q^2}, so Γ is fixed by Frobenius and therefore lies in $\mathrm{PGL}_2(\mathbf{F}_q)$. Thus, Γ takes every root of f to a root of g, so $\Gamma(f) = g$. □

As an application of this invariant, we give an algorithm for creating a table of orbit representatives for irreducible polynomials of degree $n \geq 4$ in time $\widetilde{O}(q^{n-2})$.

Algorithm 4.3. Inverting the cross polynomial function.

Input: A prime power q and an integer $n \geq 4$.

Output: A table, indexed by the values of the cross polynomials for irreducible polynomials of degree n, giving for each cross polynomial g an irreducible homogeneous $f \in \mathbf{F}_q[x, y]$ of degree n with $\mathrm{Cross}\, f = g$.

1. Construct a copy of $\mathbf{F}_{q^n}$ with an $\mathbf{F}_q$-basis $(\beta_1, \ldots, \beta_n)$ such that β_1 appears with nonzero coefficient in the representation of 1.
2. Set L to be the empty list.
3. For every $\alpha \in \mathbf{F}_{q^n}$ that does not lie in a proper subfield, and whose representation $(a_1, \ldots, a_n)$ on the given basis has $a_1 = 0$ and has $a_i = 1$ for the first i with $a_i \neq 0$, do:
   (a) Compute the homogenization f of the minimal polynomial of α.
   (b) Compute $\operatorname{Cross} f$.
   (c) Append the pair $(\operatorname{Cross} f, f)$ to L.
4. Sort L.
5. Delete every entry $(\operatorname{Cross} f, f)$ of L for which the value of $\operatorname{Cross} f$ appears earlier in the list.
6. Return L.

Proposition 4.4. *Algorithm 4.3 produces correct output and runs in time $\widetilde{O}(q^{n-2})$, measured in arithmetic operations in $\mathbf{F}_q$.*

Proof. First we note that every $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit contains an α as in step (3). We can see this because starting with an arbitrary $\alpha \in \mathbf{F}_{q^n}$, we can subtract an element of $\mathbf{F}_q$ to zero out the coefficient of β_1, and then we can scale by an element of $\mathbf{F}_q^\times$ so that the first nonzero coefficient is 1. It follows that every orbit will have a representative included in the output, and step (5) ensures that there is only one representative given for each orbit. Thus the output is correct. Now we analyze the timing.

For fixed n, Shoup's algorithm [22] can construct a finite field $\mathbf{F}_{q^n}$ in time $\widetilde{O}(\sqrt{q})$, and in polynomial time [15] we can find an embedding of our given $\mathbf{F}_q$ into this copy of $\mathbf{F}_{q^n}$, so step (1) can be done within the stated time bound. Because n is fixed, for each α the values of f and $\operatorname{Cross} f$ can be computed in time $O(1)$, so creating the list L takes time $O(q^{n-2})$. Finally, sorting a list of length $O(q^{n-2})$ takes time $\widetilde{O}(q^{n-2})$ (see [13, §5.2.3]). □

As we will see, for composite values of n there is an algorithm for producing a complete set of unique representatives for the $\mathrm{PGL}_2(k)$ orbits of irreducible homogeneous polynomials of degree n that runs in time $\widetilde{O}(q^{n-3})$; see Section 8.3. An algorithm of this time complexity that works for all n is given in [9].

5. Explicit coset representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ in $\mathrm{PGL}_2(\mathbf{F}_{q^2})$

As part of our algorithm, we will need to have a complete set of unique representatives for the right cosets of the subgroup $\mathrm{PGL}_2(\mathbf{F}_q)$ of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$. In this section we give an explicit set of such representatives.

Throughout this section, q is a prime power, ω is an element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$, and γ is a generator of the multiplicative group of $\mathbf{F}_{q^2}$.

An element of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ is determined by where it sends ∞, 0, and 1, and given any three distinct elements of $\mathbf{P}^1(\mathbf{F}_{q^2})$, there is an element of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ that sends ∞, 0, and 1 to those three elements. Thus, we may represent elements of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ by triples (ζ, η, θ) of pairwise distinct elements of $\mathbf{P}^1(\mathbf{F}_{q^2})$, indicating the images of ∞, 0, and 1. If Γ is an element of $\mathrm{PGL}_2(\mathbf{F}_q)$, then Γ sends the element (ζ, η, θ) of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ to $(\Gamma(\zeta), \Gamma(\eta), \Gamma(\theta))$.

Proposition 5.1. *Let B be the set $\{(\omega\gamma^i + \omega^q)/(\gamma^i + 1) \mid 0 \le i < q-1\}$. The following elements give a complete set of unique coset representatives for the left action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathrm{PGL}_2(\mathbf{F}_{q^2})$:*

(1) $(\infty, 0, 1)$;
(2) $\{(\infty, 0, \omega + a) \mid a \in \mathbf{F}_q\}$;
(3) $\{(\infty, \omega, \theta) \mid \theta \in \mathbf{F}_{q^2} \text{ with } \theta \ne \omega\}$;
(4) $\{(\omega, \omega^q, \theta) \mid \theta \in B\}$;
(5) $\{(\omega, \eta, \theta) \mid \eta \in B, \theta \in \mathbf{P}^1(\mathbf{F}_{q^2}) \text{ with } \theta \ne \omega \text{ and } \theta \ne \eta\}$.

To prove this proposition, we need the following lemma.

Lemma 5.2. *With notation as above, let G be the subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ that fixes the element ω. Then the set B from Proposition 5.1 is a complete set of unique representatives for the left action of G on $\mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \{\omega, \omega^q\}$.*

Proof. Let $r := \omega + \omega^q$ and let $s := \omega^{q+1}$. We check that the group G is equal to

$$G = \left\{ \begin{bmatrix} a & -sb \\ b & a - rb \end{bmatrix} \;\middle|\; [a:b] \in \mathbf{P}^1(\mathbf{F}_q) \right\}.$$

Let $\Phi := \left[\begin{smallmatrix} -1 & \omega^q \\ 1 & -\omega \end{smallmatrix}\right]$, so that Φ sends ω to ∞ and ω^q to 0. We compute that

$$\begin{aligned} \Phi G \Phi^{-1} &= \left\{ \begin{bmatrix} a - b\omega^q & 0 \\ 0 & a - b\omega \end{bmatrix} \;\middle|\; [a:b] \in \mathbf{P}^1(\mathbf{F}_q) \right\} \\ &= \left\{ \begin{bmatrix} (a - b\omega^q)/(a - b\omega) & 0 \\ 0 & 1 \end{bmatrix} \;\middle|\; [a:b] \in \mathbf{P}^1(\mathbf{F}_q) \right\}. \end{aligned}$$

By Hilbert 90, the set of values attained by $(a - b\omega^q)/(a - b\omega)$ is equal to the set of elements of $\mathbf{F}_{q^2}$ whose norms to $\mathbf{F}_q$ are equal to 1, and these elements are precisely the powers of γ^{q-1}. Thus, the action of $\Phi G \Phi^{-1}$ on $\mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \{\infty, 0\}$ is generated by multiplication by γ^{q-1}, and it is easy to see that the values $1, \gamma, \ldots, \gamma^{q-2}$ are orbit representatives for this action. Applying Φ^{-1} to these orbit representatives will give us orbit representatives for the action of G on $\mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \{\omega, \omega^q\}$, and we see that $\Phi^{-1}(\gamma^i) = (\omega\gamma^i + \omega^q)/(\gamma^i + 1)$. □

Proof of Proposition 5.1. Suppose we are given an element (ζ, η, θ) of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$. We will show how to modify it by elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ to put it into one of the forms listed in the proposition. In the course of this demonstration, it will become clear that the elements listed in the proposition do indeed lie in different $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits, because they are fixed by the following procedure.

Recall that ω is an element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$. Given a triple $\Gamma := (\zeta, \eta, \theta)$ representing an element of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$, we do the following:

(1) *If ζ lies in $\mathbf{P}^1(\mathbf{F}_q)$*: In this case, we can apply an element of $\mathrm{PGL}_2(\mathbf{F}_q)$ that moves ζ to ∞. Our element of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ can now be written (∞, η, θ), for some new values of η and θ. We can now only apply elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that fix ∞; that is, we are limited to the so-called $ax + b$ group.
   (a) *If η lies in $\mathbf{F}_q$*: In this case, we can use the $ax + b$ group to move η to 0. Our element of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ can now be written $(\infty, 0, \theta)$, for some new value θ. Now we can only apply elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that fix ∞ and 0; that is, we are limited to scalar multiplication.

(i) *If θ lies in $\mathbf{F}_q$*: In this case, we can scale θ so that it is equal to 1. We obtain the element $(\infty, 0, 1)$ listed in part (1) of the proposition, and no further action of $\mathrm{PGL}_2(\mathbf{F}_q)$ is possible.
(ii) *If θ does not lie in $\mathbf{F}_q$*: We can write $\theta = u\omega + v$ for elements u, v of $\mathbf{F}_q$, with u nonzero. There is a unique scaling that will put θ into the form $\omega + a$. We obtain an element from part (2) of the proposition.

(b) *If η does not lie in $\mathbf{F}_q$*: Using the $ax + b$ group, we can move η to ω. There is no further action of $\mathrm{PGL}_2(\mathbf{F}_q)$ that fixes ∞ and ω, so θ can be any element of $\mathbf{F}_{q^2}$ other than ω. This gives us an element from part (3) of the proposition.

(2) *If ζ does not lie in $\mathbf{P}^1(\mathbf{F}_q)$*: In this case, ζ is an element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$, and we can use the $ax + b$ subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ to move ζ to ω. The only elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that we can apply once we have fixed $\zeta = \omega$ are the elements of the group G from Lemma 5.2.

(a) *If η is equal to ω^q*: If $\eta = \omega^q$ then the action of G fixes η. We know that θ is different from both ω and ω^q, so by Lemma 5.2 we can use G to move θ to a unique element of the set B. This gives us an element from part (4) of the proposition.

(b) *If η is not equal to ω^q*: We can use G to move η to a unique element of B. Once we have normalized η in this way, there is no further action of $\mathrm{PGL}_2(\mathbf{F}_q)$ that fixes ω and η, so θ can be any element of $\mathbf{P}^1(\mathbf{F}_{q^2})$ other than ω and η. This gives us an element from part (5) of the proposition.

These cases enumerate all of the possibilities for our element (ζ, η, θ), so the proposition is proved. □

6. Explicit coset representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ in $\mathrm{PGL}_2(\mathbf{F}_{q^p})$

It is not necessary for proving our main theorem, but there is a result analogous to Proposition 5.1 for the cosets of $\mathrm{PGL}_2(\mathbf{F}_q)$ in $\mathrm{PGL}_2(\mathbf{F}_{q^p})$, where p is an odd prime. As before, we represent elements of $\mathrm{PGL}_2(\mathbf{F}_{q^p})$ as triples (ζ, η, θ) of distinct elements of $\mathbf{P}^1(\mathbf{F}_{q^p})$, indicating where the given element of $\mathrm{PGL}_2(\mathbf{F}_{q^p})$ sends ∞, 0, and 1.

Proposition 6.1. *Let q be a prime power and let p be an odd prime. Let C be a set of orbit representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathbf{F}_{q^p} \setminus \mathbf{F}_q$, let C_∞ be a set of orbit representatives for the action of the $ax + b$ subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathbf{F}_{q^p} \setminus \mathbf{F}_q$, and let $C_{\infty,0}$ be a set of orbit representatives for the multiplicative action of $\mathbf{F}_q^\times$ on $\mathbf{F}_{q^p} \setminus \mathbf{F}_q$.*

The following elements give a complete set of unique coset representatives for the left action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathrm{PGL}_2(\mathbf{F}_{q^p})$:

(1) $(\infty, 0, 1)$;
(2) $\{(\infty, 0, \theta) \mid \theta \in C_{\infty,0}\}$;
(3) $\{(\infty, \eta, \theta) \mid \eta \in C_\infty,\ \theta \in \mathbf{F}_{q^p} \text{ with } \theta \neq \eta\}$;
(4) $\{(\zeta, \eta, \theta) \mid \zeta \in C,\ \eta, \theta \in \mathbf{P}^1(\mathbf{F}_{q^p}) \text{ with } \eta \neq \zeta \text{ and } \theta \neq \zeta \text{ and } \theta \neq \eta\}$.

Proof. The proof is much like that of Proposition 5.1, but simpler. Suppose we are given an arbitrary (ζ, η, θ) in $\mathrm{PGL}_2(\mathbf{F}_{q^p})$. If ζ and η both lie in $\mathbf{P}^1(\mathbf{F}_q)$, we can

move them to ∞ and 0, and then we can only modify θ by scaling by elements of $\mathbf{F}_q^\times$. If θ lies in $\mathbf{F}_q$ we get case (1), and if not we get case (2).

If ζ lies in $\mathbf{P}^1(\mathbf{F}_q)$ but η does not, we move ζ to ∞ using $\mathrm{PGL}_2(\mathbf{F}_q)$. Then the only action of $\mathrm{PGL}_2(\mathbf{F}_q)$ we have left to us is the $ax+b$ subgroup. Since η lies in $\mathbf{F}_{q^p} \setminus \mathbf{F}_q$, we can use this subgroup to move η to an element of C_∞. Then θ can be arbitrary, as long as it is different from ∞ and from η. This gives us case (3).

If ζ does not lie in $\mathbf{P}^1(\mathbf{F}_q)$ then we can move ζ using $\mathrm{PGL}_2(\mathbf{F}_q)$ so that it lies in C, and there is no further action of $\mathrm{PGL}_2(\mathbf{F}_q)$ left available to us, because the only elements of $\mathbf{P}^1(\overline{\mathbf{F}}_q)$ with nontrivial $\mathrm{PGL}_2(\mathbf{F}_q)$ stabilizers lie in $\mathbf{P}^1(\mathbf{F}_{q^2})$. This gives us case (4). □

This result is useful because we can compute the sets of representatives we need.

Algorithm 6.2. Orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the elements of $\mathbf{F}_{q^n}$ that do not lie in proper subfields.

Input: A prime power q and an integer $n \geq 3$.

Output: A complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the the elements of $\mathbf{F}_{q^n}$ that do not lie in proper subfields.

1. Set L and M to be empty lists.
2. Construct a copy of $\mathbf{F}_{q^n}$ with an $\mathbf{F}_q$-basis $(\beta_1, \dots, \beta_n)$ such that β_1 appears with nonzero coefficient in the representation of 1.
3. If $n = 3$ return a list containing the single element β_2, and stop.
4. For every $\alpha \in \mathbf{F}_{q^n}$ that does not lie in a proper subfield, and whose representation $(a_1, \dots, a_n)$ on the given basis has $a_1 = 0$ and has $a_i = 1$ for the first i with $a_i \neq 0$, do:
   (a) Compute α^{q^i} for $i = 1, \dots, n-1$. If any of these conjugates is smaller than or equal to α under a fixed ordering $<$, continue on to the next value of α.
   (b) Compute the minimal polynomial f of α.
   (c) Find the (unique) irreducible factor g of $\mathrm{Cross}(f)$.
   (d) Append the pair (g, α) to L.
5. Sort L.
6. Delete every element (g, α) of L such that g appears as a first entry of an element earlier in the list.
7. For every (g, α) in L, do:
   (a) For $i = 0, \dots, \deg g - 1$, append the element α^{q^i} to M.
8. Return M.

Proposition 6.3. *Algorithm 6.2 produces a complete list of unique representatives for the orbits of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *acting on the elements of* $\mathbf{F}_{q^n}$ *that lie in no proper subfield. It runs in time* $\widetilde{O}(q^{n-2})$.

Proof. When $n = 3$, the group $\mathrm{PGL}_2(\mathbf{F}_q)$ acts transitively on $\mathbf{P}_{q^3} \setminus \mathbf{F}_q$, so step (3) gives correct output. For $n > 3$, Algorithm 6.2 is a variation on Algorithm 4.3. The only additional fact we must note is that there is an element of $\mathrm{PGL}_2(\mathbf{F}_q)$ that takes α to one of its nontrivial conjugates if and only if the cross polynomial of f is not irreducible, and that the order of each such element of $\mathrm{PGL}_2(\mathbf{F}_q)$ is equal to the exponent e such that $\mathrm{Cross}(f) = g^e$. Thus, the Galois orbit of α contains representatives of exactly $\deg g$ $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits. □

Algorithm 6.2 gives us a method to calculate the set C from Proposition 6.1. The sets C_∞ and $C_{\infty,0}$ can be computed in similar (but simpler) ways; we leave the details to the reader.

7. Enumerating $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit representatives for $\mathrm{Sym}^n(\mathbf{F}_q)$

In this section we present our algorithm for enumerating orbit representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathrm{Sym}^n(\mathbf{F}_q)$ in time $\widetilde{O}(q^{n-3})$, for n fixed and q varying. The algorithm consists of a number of different algorithms, each addressing a subset of elements of $\mathrm{Sym}^n(\mathbf{F}_q)$. The problem is trivial when $n \leq 3$, so we will always assume that $n \geq 4$, and for one case we will also demand that n be even. This is sufficient for our application to enumerating hyperelliptic curves of genus g, where $n = 2g + 2$ is even and at least 6. (See [9] for an algorithm that works for all n.)

Recall that an element of $\mathrm{Sym}^n(\mathbf{F}_q)$ is a set $A = \{\alpha_1, \ldots, \alpha_n\}$ of n distinct elements of $\mathbf{P}^1(\overline{\mathbf{F}}_q)$ that is stable under the action of the Galois group of $\overline{\mathbf{F}}_q$ over $\mathbf{F}_q$. An element of $\mathrm{Sym}^n(\mathbf{F}_q)$ is *primitive* if the degree of each extension $\mathbf{F}_q(\alpha_i)$ over $\mathbf{F}_q$ is equal to n. Every element A of $\mathrm{Sym}^n(\mathbf{F}_q)$ can be written in a unique way (up to order) as the union of a collection $\{A_i\}$ of primitive elements A_i of $\mathrm{Sym}^{m_i}(\mathbf{F}_q)$, for some sequence of integers m_i with $\sum m_i = n$. The sequence $(m_i)_i$, listed in non-increasing order, is the *Galois type* of A. If f is the monic homogeneous polynomial whose zero set is A, then $(m_i)_i$ is also the list of the degrees of the irreducible factors of f, and we also refer to this sequence as the Galois type of f. We will enumerate the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of $\mathrm{Sym}^n(\mathbf{F}_q)$ by enumerating each Galois type separately.

Let $M := (m_1, m_2, \ldots, m_r)$ be a Galois type for $\mathrm{Sym}^n(\mathbf{F}_q)$, so that $m_1 \geq m_2 \geq \cdots \geq m_r > 0$ and $n = m_1 + \cdots + m_r$. In the following subsections we show how to enumerate the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbits of the elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of this Galois type, based on the value of m_1.

7.1. **The case $m_1 = 1$.** Every element A of $\mathrm{Sym}^n(\mathbf{F}_q)$ of this Galois type is simply a collection of n distinct elements of $\mathbf{P}^1(\mathbf{F}_q)$. We can specify a standard form for such elements A by considering all possible choices of three distinct points a_i, a_j, and a_k in A, and using an element Γ of $\mathrm{PGL}_2(\mathbf{F}_q)$ to move those three points to ∞, 0, and 1, respectively. To this choice we associate the polynomial f of degree $n - 1$ defined by

$$f := y \prod_{\ell \neq i} (x - \Gamma(a_\ell) y) \,.$$

Our standard form for A is the smallest polynomial f obtained in this way, under an arbitrary total ordering $<$ of the monic homogeneous polynomials of degree n.

Our algorithm for enumerating orbit representatives of this Galois type is as follows.

Algorithm 7.1. Orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of Galois type $(1, 1, \ldots, 1)$.

Input: A prime power q and an integer $n \geq 4$.

Output: A complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic homogenous polynomials of degree n and Galois type $(1, 1, \ldots, 1)$.

1. Set L to be the empty list, and set $a_1 := \infty$, $a_2 := 0$, and $a_3 := 1$.
2. For every set $\{a_4, \ldots, a_n\}$ of distinct elements of $\mathbf{F}_q \setminus \{0, 1\}$ do:
   (a) Set $f := y \prod_{i=2}^{n} (x - a_i y)$.

(b) Set $F := \{\Gamma(f)\}$, where Γ ranges over the elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that send three elements of $\{a_i\}$ to ∞, 0, and 1.
(c) If f is the smallest element of F under the ordering $<$, append f to L.

3. Return L.

Proposition 7.2. *Algorithm 7.1 produces a complete set of unique representatives for the orbits of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *acting on the monic homogeneous degree-n polynomials of Galois type* $(1, 1, \ldots, 1)$. *It runs in time* $\widetilde{O}(q^{n-3})$, *measured in arithmetic operations in* $\mathbf{F}_q$. □

7.2. **The case $m_1 = 2$.** When $m_1 = 2$ the possible Galois types $(m_1, \ldots, m_r)$ consist of s values of 2 and t values of 1, where $2s + t = n$ and $s > 0$. We present two algorithms, one that applies when $t \geq 3$ and one that applies when $s \geq 2$. Since we are assuming throughout that $n \geq 4$, the only remaining case is when $s = 1$ and $t = 2$, but that situation is handled by Theorem 3.6.

Algorithm 7.3. Orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of Galois type of the form $(2, 2, \ldots, 2, 1, \ldots, 1)$, with s entries of 2 and t entries of 1, where $t \geq 3$.

Input: A prime power q, an integer $n \geq 4$, and integers s and t with $2s + t = n$ and $t \geq 3$.

Output: A complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic homogenous polynomials of degree n with the given Galois type.

1. Set L to be the empty list, and set $a_1 := \infty$, $a_2 := 0$, and $a_3 := 1$.
2. Create a list I_2 of the monic irreducible homogeneous quadratics over $\mathbf{F}_q$.
3. For every set $\{a_4, \ldots, a_t\}$ of distinct elements of $\mathbf{F}_q \setminus \{0, 1\}$ and every set $\{g_1, \ldots, g_s\}$ of distinct elements of I_2 do:
   (a) Set $f := y \prod_{i=2}^{t} (x - a_i y) \cdot \prod_{i=1}^{s} g_i$.
   (b) Set $F := \{\Gamma(f)\}$, where Γ ranges over the elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that send three elements of $\{a_i\}$ to ∞, 0, and 1.
   (c) If f is the smallest element of F under the ordering $<$, append f to L.
4. Return L.

Proposition 7.4. *Algorithm 7.3 produces a complete set of unique representatives for the orbits of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *acting on the monic homogeneous degree-n polynomials of Galois type* $(2, 2, \ldots, 2, 1, \ldots, 1)$, *with s entries of* 2 *and $t \geq 3$ entries of* 1. *It runs in time* $\widetilde{O}(q^{n-3})$, *measured in arithmetic operations in* $\mathbf{F}_q$. □

Algorithm 7.5. Orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of Galois type of the form $(2, 2, \ldots, 2, 1, \ldots, 1)$, with s entries of 2 and t entries of 1, where $s \geq 2$.

Input: A prime power q, an integer $n \geq 4$, and integers s and t with $2s + t = n$ and $s \geq 2$.

Output: A complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic homogenous polynomials of degree n with the given Galois type.

1. Set L to be the empty list.
2. Let I_1 be the set of polynomials $\{y\} \cup \{x - ay : a \in \mathbf{F}_q\}$.
3. Create a list I_2 of the monic irreducible homogeneous quadratics over $\mathbf{F}_q$.

4. For every pair (f_1, f_2) of irreducible quadratic factors obtained from Theorem 3.4 or Theorem 3.8, for every set $\{f_3, \dots, f_s\}$ of elements of I_2 such that the quadratics $f_1, \dots, f_s$ are distinct, and for every set $\{g_1, \dots, g_t\}$ of distinct elements of I_1, do:
   (a) Set $f := \prod_{i=1}^{s} f_i \cdot \prod_{i=1}^{t} g_i$.
   (b) Set $F := \{\Gamma(f)\}$, where Γ ranges over the elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that send a pair of elements of $\{f_i\}$ to the representative of their $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit, calculated using the table mentioned at the end of Remark 3.9.
   (c) If f is the smallest element of F under the ordering $<$, append f to L.
5. Return L.

Remark 7.6. The most direct way of implementing step (4)(b) involves computing the roots of various irreducible quadratics in a fixed copy of $\mathbf{F}_{q^2}$. From [15, Theorem 1.2], we know that this can be done in time polynomial in $\log q$.

Proposition 7.7. *Algorithm 7.5 produces a complete set of unique representatives for the orbits of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *acting on the monic homogeneous degree-n polynomials of Galois type* $(2, 2, \dots, 2, 1, \dots, 1)$*, with* $s \geq 2$ *entries of* 2 *and* t *entries of* 1*. It runs in time* $\widetilde{O}(q^{n-3})$*, measured in arithmetic operations in* $\mathbf{F}_q$*.* □

7.3. **The case** $3 \leq m_1 \leq n-1$**.** Let $(m_1, \dots, m_r)$ be a Galois type with $3 \leq m_1 \leq n-1$. When $m_1 > 3$ we will make use of the list of $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit representatives of irreducible polynomials of degree m_1 provided by Algorithm 4.3, which will not exceed our claimed time bound of $\widetilde{O}(q^{n-3})$ because $m_1 - 2 \leq n-3$. When $m_1 = 3$ we will use the fact that there is exactly one $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of irreducible degree-3 polynomials, so we can take our favorite irreducible polynomial of degree 3 as the sole orbit representative.

Algorithm 7.8. Orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of Galois type $(m_1, \dots, m_r)$, with $3 \leq m_1 \leq n-1$.

Input: A prime power q, an integer $n \geq 4$, and a Galois type with $3 \leq m_1 \leq n-1$.

Output: A complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic homogenous polynomials of degree n with the given Galois type.

1. Set L to be the empty list.
2. For each value of m_i in the set $\{m_2, \dots, m_r\}$, create a list I_{m_i} of the monic irreducible homogeneous polynomials of degree m_i.
3. If $m_1 > 3$, let L_1 be the output of Algorithm 4.3 associated to the inputs q and m_1 and let S be the list of orbit representatives of irreducible polynomials of degree m_1 obtained as the second elements of each pair on the list L_1.
4. If $m_1 = 3$ let S be the single-element list consisting of an arbitrary irreducible polynomial of degree 3.
5. For every element f_1 of S and every set of distinct polynomials $\{f_2, \dots, f_r\}$ with $f_i \in I_{m_i}$ do:
   (a) Set $f := \prod_{i=1}^{r} f_i$.
   (b) Let M_1 be the set of f_i of degree m_1 and set $F := \{\Gamma(f)\}$, where Γ ranges over the elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ that send an element of M to its associated orbit representative, obtained by computing its cross polynomial and using the lookup table L_1 if $m_1 > 3$ and by direct calculation if $m_1 = 3$.

(c) If f is the smallest element of F under the ordering $<$, append f to L.

6. Return L.

Remark 7.9. As in the similar situation in Algorithm 7.5, we can accomplish step (5)(b) by computing the roots of various irreducible polynomials of degree m in a fixed copy of $\mathbf{F}_{q^m}$, and [15, Theorem 1.2] shows that we can do this in time polynomial in $\log q$.

Proposition 7.10. *Algorithm 7.8 produces a complete set of unique representatives for the orbits of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *acting on the monic homogeneous degree-n polynomials of the given Galois type. It runs in time* $\widetilde{O}(q^{n-3})$*, measured in arithmetic operations in* $\mathbf{F}_q$*.*

Proof. The correctness of the algorithm is clear, because every $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of the given Galois type has a representative considered by the algorithm, and duplicates are prevented by steps (5)(b) and (5)(c).

For each m_i in step (2), the time required to compute the list I_{m_i} is $\widetilde{O}(q^{m_i})$, and since $m_i \le n - m_1 \le n - 3$ this is $\widetilde{O}(q^{n-3})$. The time required for step (3) is $\widetilde{O}(q^{m_1-2})$, and since $m_1 - 2 \le n - 3$, this is also $\widetilde{O}(q^{n-3})$. And in step (5), we consider $O(q^{n-3})$ tuples $(f_1, \dots, f_r)$, and each takes time $\widetilde{O}(1)$ to process. Thus, the total time required is as claimed. □

7.4. **The case $m_1 = n$.** This is the first and only case in which we will require n to be even. The case $n = 4$ is covered by Theorems 1.2 and 3.8, so we may assume that $n \ge 6$. Note that we cannot just apply Algorithm 4.3, because that takes time $\widetilde{O}(q^{n-2})$, and we want an algorithm that takes time $\widetilde{O}(q^{n-3})$.

Algorithm 7.11. Orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of Galois type (n), where $n \ge 6$ is even.

Input: A prime power q and an even integer $n \ge 6$.

Output: A complete set of unique representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on the monic irreducible homogenous polynomials of degree n.

1. If $n = 6$, let M be the list consisting of a single monic irreducible cubic homogeneous polynomial in $\mathbf{F}_{q^2}[x, y]$.
2. If $n = 8$, let M be the list consisting of the monic irreducible quartic homogeneous polynomials in $\mathbf{F}_{q^2}[x, y]$ given by Theorem 1.2 or Theorem 3.8 applied to the field $\mathbf{F}_{q^2}$.
3. If $n \ge 10$, use Algorithm 4.3 to create a list M of orbit representatives for the action of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ acting on the monic irreducible homogeneous polynomials of degree $n/2$ in $\mathbf{F}_{q^2}[x, y]$.
4. Let G be the list of coset representative for the left action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ from Proposition 5.1.
5. Let N be the list consisting of $\Gamma(f)$, for all $\Gamma \in G$ and f in M.
6. Let L be the list of all products $gg^{(q)}$ for $g \in N$, where the superscript (q) means to raise each coefficient of a polynomial to the qth power.
7. Let L' be the list of all pairs $(\mathrm{Cross}\, f, f)$ for $f \in L$.
8. Sort L', and then delete every entry $(\mathrm{Cross}\, f, f)$ where $\mathrm{Cross}\, f$ appears as the first element of an earlier entry in L'.
9. Let L'' be the list of second elements of the entries in L'.

10. Return L''.

Proposition 7.12. *Algorithm 7.11 produces a complete set of unique representatives for the orbits of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *acting on the monic irreducible homogeneous polynomials of degree* n*. It runs in time* $\widetilde{O}(q^{n-3})$*, measured in arithmetic operations in* $\mathbf{F}_q$*.*

Proof. To prove correctness, we must show that the list L'' consists of unique representatives for each $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit of irreducible polynomials of degree n over $\mathbf{F}_q$. First we show that it contains at least one representative from each orbit.

We know that every monic irreducible homogeneous polynomial f of degree n in $\mathbf{F}_q[x,y]$ can be written $gg^{(q)}$ for a monic irreducible homogeneous polynomial g in $\mathbf{F}_{q^2}[x,y]$ of degree $n/2$, and g is unique up to $g \leftrightarrow g^{(q)}$. If we can show that the list N contains an element in every orbit of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the left on the set S of monic irreducible homogeneous polynomials of degree $n/2$ in $\mathbf{F}_{q^2}[x,y]$, then that will show that L contains at least one element in every orbit of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the monic irreducible homogeneous polynomials of degree n in $\mathbf{F}_q[x,y]$. But since M is a list of representative for the orbits of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ acting on S, and since G consists of coset representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on $\mathrm{PGL}_2(\mathbf{F}_{q^2})$, this is clear. Thus, L contains a representative from each orbit of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the set of monic irreducible homogeneous polynomials of degree n in $\mathbf{F}_q[x,y]$. In fact, L contains at most two such representatives for each orbit, because of the uniqueness of g up to $g \leftrightarrow g^{(q)}$.

By construction (and by Theorem 4.2), the list L'' contains at most one representative from each orbit of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the irreducible polynomials. But we already saw that it contains at least one such representative. Therefore, it is a complete list of unique representatives.

The only thing left to check is that the algorithm runs in time $\widetilde{O}(q^{n-3})$. Steps (1) through (3) take time at most $\widetilde{O}((q^2)^{(n/2-2)}) = \widetilde{O}(q^{n-4})$. Step (4) takes time $O(q^3)$, and step (5) takes time $\widetilde{O}(q^{n-3})$ because there are $O(q^3)$ elements of G and $O(q^{n-6})$ elements of M. Steps (6) through (9) also take time $\widetilde{O}(q^{n-3})$, because the lists N, L, and L' contain $O(q^{n-3})$ elements. □

8. Additional efficiencies

In this section we mention a few ways that the algorithms in Section 7 can be improved. The asymptotic complexity of the revised algorithms is still $\widetilde{O}(q^{n-3})$, but the speedups in this section improve the algorithms by constant factors.

8.1. **Avoiding repeated orbits.** Several of our algorithms include a step to deal with elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ that can be normalized (in the manner of the particular algorithm) in several ways. This happens in steps (2)(b) and (c) of Algorithm 7.1, in steps (3)(b) and (c) of Algorithm 7.3, in steps (4)(b) and (c) of Algorithm 7.5, and in steps (5)(b) and (c) of Algorithm 7.8. In Algorithm 7.8, for example, this is needed when there is more than one occurrence of the number m_1 in the Galois type. The algorithm normalizes elements of $\mathrm{Sym}^n(\mathbf{F}_q)$ of the given Galois type (represented by monic homogeneous polynomials of degree n) by absorbing all of the action of $\mathrm{PGL}_2(\mathbf{F}_q)$ into one factor of degree m_1. If there is more than one such factor, there is more than one normalization of the same polynomial, and the algorithm has to identify the resulting repeated orbits and return only one of them.

(There is also more than one normalization if a factor of degree m_1 has nontrivial $\mathrm{PGL}_2(\mathbf{F}_q)$ stabilizer, but that is rare.)

The most straightforward way to avoid this situation is to handle Galois types with m_1 occurring more than once in a different way. For instance, if we are working with the Galois type $(4,4,3,1)$, instead of normalizing on the factors of degree 4 (for which there are two choices), we can instead normalize on the factor of degree 3. This technique can be used to handle every Galois type that includes at least one value of m that is at least 3 and that occurs just once in the type. Similarly, if the value 2 occurs in a type exactly twice, we can normalize the product of two irreducible quadratics.

If we have a Galois type with $m_1 \geq 3$ where this is impossible — for example, $(4,4,3,3)$ — we have another option. We use a modified version of Algorithm 4.3 where we skip step (5); this gives us a list of all monic irreducible polynomials of degree m_1, grouped by their cross polynomials. Then, in Algorithm 7.8, in step (5) we do not consider *all* sets of distinct polynomials $\{f_2, \dots, f_r\}$; instead, we demand that the cross polynomial of every f_i whose degree is equal to m_1 not appear earlier on the sorted list that that of f_1. If in fact all of the additional cross polynomials are different from the cross polynomial of f_1, the orbit representative we obtain will not be repeated unless the $\mathrm{PGL}_2(\mathbf{F}_q)$ stabilizer of f_1 is nontrivial, which is unusual (and easy to check). If some of the additional cross polynomials *are* the same as that of f_1, then we keep track of this orbit on a separate list, and deduplicate this (much smaller) list separately.

8.2. **Treating the Galois types $(n-1,1)$ and $(n-2,1,1)$ more efficiently.** Consider the Galois type $(n-1,1)$, corresponding to a product of a linear homogeneous polynomial with an irreducible homogeneous polynomial of degree $n-1$. Instead of absorbing all the $\mathrm{PGL}_2(\mathbf{F}_q)$ action into the choice of the irreducible polynomial of degree $n-1$, we can instead demand that the linear polynomial have its zero at ∞. Then we have to find representatives for irreducible homogeneous polynomials of degree $n-1$ up to the $ax+b$ group. We can accomplish this by modifying the technique of Algorithm 4.3: We construct a copy of $\mathbf{F}_{q^{n-1}}$, we choose a basis $(\beta_1, \dots, \beta_{n-1})$ such that β_1 appears with a nonzero coefficient in the representation of 1, and then we simply list the minimal polynomials of elements whose representation on the given basis begins $(0, \dots, 0, 1, \dots)$, with at least one 0 at the beginning and with the first nonzero element being 1. We can also take care to produce only one element from each Galois orbit at this stage, in order to avoid using cross polynomials to deduplicate the list later.

For the Galois type $(n-2,1,1)$, we look for orbit representatives of the form xyf for irreducible homogeneous f of degree $n-2$. We can modify f only by replacing (x,y) with (cx,y) or (cy,x), so we can construct a copy of $\mathbf{F}_{q^{n-2}}$ with basis $(\beta_1, \dots, \beta_{n-2})$, list the minimal polynomials of the elements whose representations on the given basis have their first nonzero element equal to 1, and then deduplicate as usual.

8.3. **More efficient computations of PGL_2 orbits of irreducibles.** In step (3) of Algorithm 7.8, we obtain a list of orbit representatives for irreducible polynomials of a given degree m by using Algorithm 4.3. If m is composite, we can use a more efficient algorithm based on the idea of Algorithm 7.11. Namely, if $m = pm'$, we can compute orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_{q^p})$ acting on irreducible polynomials

in $\mathbf{F}_{q^p}[x]$ of degree m', and then use Proposition 5.1 or Proposition 6.1 to list coset representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ in $\mathrm{PGL}_2(\mathbf{F}_{q^p})$. As in Algorithm 7.11, we can combine these two lists to get a complete list of unique orbit representatives for $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on irreducible polynomials of degree n.

In fact, what we have just shown is that if n is composite, we can compute a complete set of unique representatives for the orbits of $\mathrm{PGL}_2(\mathbf{F}_q)$ acting on the monic irreducible homogeneous polynomials of degree n in time $\widetilde{O}(q^{n-3})$. This leaves open the case when n is prime. In a followup paper [9], we explain a completely different technique that will produce these orbit representatives for prime n — indeed, for *odd* n — in time $\widetilde{O}(q^{n-3})$, but no longer deterministically, because the method relies on factoring polynomials of bounded degree in polynomial time.

9. Implementations for genus 2 and genus 3

We have implemented our algorithm for hyperelliptic curves of genus 2 and genus 3 in Magma [2]. Magma files with the implementations can be found in several places: in the ancillary files attached the the arXiv version of this paper, on the author's web page, and in the GitHub repository associated to this paper [10]. In addition to the improvements described in Section 8 and others of a similar nature, our code for the genus-2 case includes an improvement for the Galois type (6) that allows us to skip the deduplication step in Algorithm 7.11. The basic idea is to choose the irreducible cubic polynomial in step (1) of Algorithm 7.11 so that it lies in $\mathbf{F}_q[x,y]$ and so that its zeros are permuted by the order-3 element $\left[\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right]$ of $\mathrm{PGL}_2(\mathbf{F}_q)$, so that it is easier to keep track of which elements of $\mathrm{PGL}_2(\mathbf{F}_{q^2})$ in G give rise to homogeneous sextic polynomials $f \in \mathbf{F}_q[x,y]$ that lie in the same $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit. The details are too lengthy to include here, but are spelled out in the comments in the code, as well as in the followup paper [9]. Other improvements are described in the comments as well.

For our genus-3 implementation, we did not spend as much time optimizing, and there are very likely improvements that can be made.

We ran some timing experiments to compare our Magma code to the built-in Magma functions that implement the algorithms of Mestre [19] and Cardona and Quer [4] for genus-2 curves, and the algorithms of Lercier and Ritzenthaler [16] for genus-3 curves. We give some sample timings in Table 1, taken by running Magma (V2.28-8) on one core of an Apple M1 Max processor with 64GB RAM. For our algorithm, we divide our timings into two steps: computation of the $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit representatives of $\mathrm{Sym}^{2g+2}(\mathbf{F}_q)$ and computation of the isomorphism classes of curves. Our algorithm includes a computation of the automorphism groups of the curves, which gives us a consistency check, since the sum over all hyperelliptic curves of genus g over $\mathbf{F}_q$ of 1 over the size of the automorphism group is equal to q^{2g-1} [3, Proposition 7.1].

We compare our genus-2 timings to those of applying the Magma command

```
Twists(HyperellipticCurveFromG2Invariants([a,b,c]))
```

to all triples (a,b,c) of elements of $\mathbf{F}_q$ and then retrieving the polynomials that define the resulting curves. For $q > 127$ we estimate the time for the Magma builtin functions by running the above command on 10,000 random triples (a,b,c) and multiplying the time taken by $q^3/10^4$; these estimates are indicated with asterisks. We see that our genus-2 code is running approximately 90 times faster than Magma's internals.

TABLE 1. Sample timings (in seconds) to compute all hyperelliptic curves of genus 2 and 3 over $\mathbf{F}_q$. The second column gives timings for Magma's built-in routines for genus 2. The third through fifth columns give timings for the techniques of this paper: the third for computing $\mathrm{PGL}_2(\mathbf{F}_q)$ orbit representatives of $\mathrm{Sym}^6(\mathbf{F}_q)$, the fourth for computing genus-2 curves from these representatives, and the fifth for the total time for both. Similarly, the sixth through ninth columns give timings for computing genus-3 curves. Timings marked with an asterisk are estimates.

	Genus 2				Genus 3			
		This paper				This paper		
q	Magma	Sym^6	Curves	Total	Magma	Sym^8	Curves	Total
17	7.9	0.16	0.02	0.18	5274	20	1	21
31	52.7	0.77	0.06	0.83	99463*	304	14	318
59	327.1	3.85	0.25	4.10	2408665*	5932	479	6411
127	3308	36	2	38				
257	27448*	290	10	300				
509	211655*	2307	76	2384				

We compare our genus-3 timings to those of applying the Magma command

```
TwistedHyperellipticPolynomialsFromShiodaInvariants(S)
```

to all Shioda invariants with nonzero discriminants, obtained by applying

```
ShiodaAlgebraicInvariants(V : ratsolve := true)
```

to every element V of the 5-dimensional weighted projective space over $\mathbf{F}_q$ with weights $[2,3,4,5,6,7]$ and discarding those with discriminant 0. For $q = 31$ and $q = 59$ we estimate Magma's times as before. It appears that our genus-3 code is running several hundred times faster than Magma's internals.

For genus-2 curves over $\mathbf{F}_{509}$, our code spent 42.46% of the time on Galois type (6), 16.06% on type $(3,3)$, and 12.55% on type $(5,1)$, with the remaining 29% of the time divided among the remaining eight types. For genus-3 curves over $\mathbf{F}_{59}$, our code spent 26.49% of the time on Galois type $(7,1)$, 25.77% on type (8), 19.45% on type $(2,2,2,2)$, and 7.87% on type $(4,4)$, with the remaining 20% of the time divided among the remaining eighteen types.

We note that memory handling issues may have slowed the genus-3 computation for $q = 59$, which reemphasizes the point, made in the introduction, that it would be good to have a version of our algorithm for higher genera that requires less space. We have not yet implemented the low-memory algorithm from [9] to see whether that will help improve our timings for larger q.

REFERENCES

[1] Jonas Bergström, Everett W. Howe, Elisa Lorenzo García, and Christophe Ritzenthaler, *Refinements of Katz–Sarnak theory for the number of points on curves over finite fields*, Canad. J. Math. (2024), online, not yet assigned an issue.

[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). Software available at http://magma.maths.usyd.edu.au/. MR 1484478
[3] Bradley W. Brock and Andrew Granville, *More points than expected on curves over finite field extensions*, Finite Fields Appl. **7** (2001), no. 1, 70–91. MR 1803936
[4] Gabriel Cardona and Jordi Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Scientific Publishing, Hackensack, NJ, 2005, pp. 71–83. MR 2181874
[5] John B. Conway, *Functions of one complex variable*, second ed., Graduate Texts in Mathematics, vol. 11, Springer-Verlag, New York–Berlin, 1978, Available for digital loan. MR 503901
[6] Dušan Dragutinović, *Computing binary curves of genus five*, J. Pure Appl. Algebra **228** (2024), no. 4, Paper No. 107522, 19. MR 4642980
[7] Sarah Frei, *The a-number of hyperelliptic curves*, Women in numbers Europe II, Assoc. Women Math. Ser., vol. 11, Springer, Cham, 2018, pp. 107–116. MR 3882708
[8] Everett W. Howe, *Curves of medium genus with many points*, Finite Fields Appl. **47** (2017), 145–160. MR 3681085
[9] ———, *Enumerating places of* $\mathbf{P}^1$ *up to automorphisms of* $\mathbf{P}^1$ *in quasilinear time*, 2024, in preparation.
[10] ———, *everetthowe/hyperelliptic*, 2024, online GitHub repository, accessed March 2024.
[11] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 1, 239–289. MR 2514865
[12] Yongyuan Huang, Kiran S. Kedlaya, and Jun Bo Lau, *A census of genus 6 curves over* $\mathbf{F}_2$, 2024. arXiv:2402.00716 [math.AG]
[13] Donald E. Knuth, *The art of computer programming. Vol. 3: Sorting and searching*, second ed., Addison-Wesley, Reading, MA, 1998. MR 3077154
[14] Tetsuo Kodama, Jaap Top, and Tadashi Washio, *Maximal hyperelliptic curves of genus three*, Finite Fields Appl. **15** (2009), no. 3, 392–403. MR 2516433
[15] Hendrik W. Lenstra, Jr., *Finding isomorphisms between finite fields*, Math. Comp. **56** (1991), no. 193, 329–347. MR 1052099
[16] Reynald Lercier and Christophe Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra **372** (2012), 595–636. MR 2990029
[17] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Available for digital loan. MR 1917232
[18] Daniel Maisner and Enric Nart, *Abelian surfaces over finite fields as Jacobians*, Experiment. Math. **11** (2002), no. 3, 321–337, With an appendix by Everett W. Howe. MR 1959745
[19] Jean-François Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. MR 1106431 (92g:14022)
[20] Enric Nart, *Counting hyperelliptic curves*, Adv. Math. **221** (2009), no. 3, 774–787. MR 2511037
[21] Jean-Pierre Serre, *Cohomologie galoisienne*, fifth ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994. MR 1324577
[22] Victor Shoup, *New algorithms for finding irreducible polynomials over finite fields*, Math. Comp. **54** (1990), no. 189, 435–447. MR 993933
[23] Igor Shparlinski, *On finding primitive roots in finite fields*, Theoret. Comput. Sci. **157** (1996), no. 2, 273–275. MR 1389773
[24] Xavier Xarles, *A census of all genus 4 curves over the field with 2 elements*, 2020. arXiv:2007.07822 [math.AG]

Independent mathematician, San Diego, CA 92104, USA
Email address: however@alumni.caltech.edu
URL: http://ewhowe.com