# THE RELATIVE CLASS NUMBER ONE PROBLEM FOR FUNCTION FIELDS, I

#### KIRAN S. KEDLAYA

Abstract. We reduce the classification of finite extensions of function fields (of curves over finite fields) with the same class number to a finite computation; complete this computation in all cases except when both curves have base field  $\mathbb{F}_2$  and genus  $> 1$ ; and give a conjectural answer in the remaining cases. The conjecture will be resolved in subsequent papers.

#### 1. INTRODUCTION

The relative class number one problem for function fields (of curves over finite fields) is to classify finite extensions for which the relative class number equals 1, or equivalently the class numbers of the two function fields coincide. In this paper, we solve this problem in all cases except where both function fields have base field  $\mathbb{F}_2$ , and to reduce that case to a *feasible* finite computation. This extends work of numerous authors [\[2,](#page-12-0) [11,](#page-13-0) [18,](#page-13-1) [19,](#page-13-2) [22\]](#page-13-3) but our arguments are independent of these.

Before continuing, we introduce some terminology and notation. By a function field, we mean the field of rational functions on a curve over some finite field. Given a finite extension  $F'/F$  of function fields, we write  $C, C'$  for the curves corresponding to F, F';  $q_F, q_{F'}$  for the orders of the base fields of C, C';  $g_F, g_{F'}$  for the genera of C, C'; and  $h_F, h_{F'}$  for the class numbers of F, F'. We write  $J(C)$ ,  $J(C')$  for the Jacobians of C, C', so that  $\#J(C)(\mathbb{F}_{q_F}) = h_F$  and  $\#J(C')(\mathbb{F}_{q_{F'}}) = h_{F'}$ .

The *relative class number*  $h_{F'/F}$  is the ratio  $h_{F'}/h_F$ ; this can be interpreted as the order of a certain finite group (see below), and hence is an integer. This implies the following reduction: for  $E = F \cdot \mathbb{F}_{q_F}$ ,  $h_{F'/F} = 1$  if and only if  $h_{E/F} = h_{F'/E} = 1$ . We may thus focus on the cases where  $F' = E$ , in which case we say the extension  $F'/F$  is constant, and where  $E = F$ , in which case we say  $F'/F$  is purely geometric.

In the case of a constant extension, the equality  $h_{F'/F} = 1$  holds for trivial reasons when  $F' = F$  and when  $g_F = g_{F'} = 0$  (as in this case  $h_F = h_{F'} = 1$ ). Excluding these, we have the following result; see §[3](#page-3-0) for the proof.

<span id="page-0-0"></span>**Theorem 1.1.** Let  $F'/F$  be a constant extension of degree  $d > 1$  of function fields with  $g_F > 0$ ,  $q_{F'} > q_F$ , and  $h_{F'/F} = 1$ . Then  $(q_F, d, g_F, J(C))$  is one of

- $(2, 2, 1, 1.2.c), (2, 2, 2, 2.2.c).$   $(2, 2, 2, 2, 2.2.d.f), (2, 2, 3, 3.2.e. j.p),$  $(2, 2, 2, 2, 2.2.d.f), (2, 2, 3, 3.2.e. j.p),$  $(2, 2, 2, 2, 2.2.d.f), (2, 2, 3, 3.2.e. j.p),$  $(2, 2, 2, 2, 2.2.d.f), (2, 2, 3, 3.2.e. j.p),$  $(2, 2, 2, 2, 2.2.d.f), (2, 2, 3, 3.2.e. j.p),$
- $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$  $(2, 3, 1, 1.2.b), (2, 3, 1, 1.2.c), (3, 2, 1, 1.3.ad), (4, 2, 1, 1.4.ae),$

where  $J(C)$  is specified up to isogeny by an LMFDB label.

Date: 25 May 2022.

Thanks to Xander Faber for providing an early draft of [\[8\]](#page-13-4), Thomas Grubb for bringing [\[6\]](#page-13-5) to our attention, and Drew Sutherland for help with computing abelian extensions of function fields in Magma. The author was supported by NSF (grants DMS-1802161, DMS-2053473) and UC San Diego (Warschawski Professorship).

#### 2 KIRAN S. KEDLAYA

In the case of a purely geometric extension, the equality  $h_{F'/F} = 1$  holds for trivial reasons when  $F' = F$  and when  $g_F = g_{F'} \in \{0, 1\}$ . Moreover, when  $g_F \in$  $\{0,1\}$ , for any fixed pair of isomorphism classes of F and F', the existence of a single finite morphism  $F \to F'$  implies the existence of infinitely many more. It is thus natural to separate the cases  $g_F \leq 1$  and  $g_F > 1$ ; see §[6](#page-7-0) and §[8](#page-10-0) for the proofs.

<span id="page-1-0"></span>**Theorem 1.2.** Let  $F'/F$  be a purely geometric extension of degree d of function fields with  $g_F \leq 1$ ,  $g_{F'} > g_F$ , and  $h_{F'/F} = 1$ . Then  $(q_F, g_F, g'_F, J(C), J(C'))$ appears in Table [3.](#page-14-0) (Note that the tuple does not always uniquely determine  $F'.$ )

When  $g_F = 0$ , Theorem [1.2](#page-1-0) recovers the solution of the *absolute class number* one problem for function fields [\[20,](#page-13-6) [35,](#page-13-7) [25,](#page-13-8) [31\]](#page-13-9).

<span id="page-1-1"></span>**Theorem 1.3.** Let  $F'/F$  be a purely geometric extension of degree d of function fields with  $g_{F'} > g_F > 1$  and  $h_{F'/F} = 1$ .

- (a) If  $q_F > 2$ , then  $q_F \in \{3, 4\}$ ,  $(g_F, g'_F) \in \{(2, 3), (2, 4), (3, 5)\}$ ,  $F'/F$  is  $(Ga-F')$ lois) cyclic, and  $(q_F, g_F, g_{F'} , F)$  appears in Table [4.](#page-14-1) In each listed case, the tuple uniquely determines F'.
- (b) If  $q_F = 2$ , then  $g_F \le 7$  and  $g_{F'} \le 13$ . The isogeny classes of  $J(C)$  and the Prym variety A (see below) form one of 208 pairs listed in Table [7.](#page-16-0)
- (c) If  $q_F = 2$ , then assuming that  $F'/F$  is cyclic, there are exactly 61 tuples  $(d, g_F, g_{F'}, F)$  with  $g_F \notin \{6, 7\}$ , and at least 3 with  $g_F \in \{6, 7\}$ ; see Tables [5](#page-14-2) and [6.](#page-15-0) In each listed case, the tuple uniquely determines  $F'$ .

In Theorem  $1.3(c)$ , there are only two cases  $(3.2.a b.a.c. and 5.2.b.c.e.i.)$  $(3.2.a b.a.c. and 5.2.b.c.e.i.)$  $(3.2.a b.a.c. and 5.2.b.c.e.i.)$  where F is not uniquely specified by  $d, g_F, g_{F'}$ ,  $J(C)$ . The scarcity of such examples reflects that curves with isogenous Jacobians can typically be distinguished by the L-functions of their abelian covers [\[4\]](#page-12-1).

By our earlier reduction, we recover the following corollary.

**Corollary 1.4.** Let  $F'/F$  be an extension of degree d of function fields with  $g_{F'}$  $g_F$  and  $h_{F'/F} = 1$  which is neither constant nor purely geometric. Then  $q_F = 2$ ,  $q_{F'} = 4$ , and  $(g_F, g_{F'}, J(C), J(C')) \in \{(0, 1, 0, 1.4 \text{ae}), (1, 2, 1.2 \text{c}, 2.4 \text{ae-1})\}.$ 

We now summarize the techniques used to prove Theorem [1.1,](#page-0-0) Theorem [1.2,](#page-1-0) and Theorem [1.3.](#page-1-1) The extension  $F'/F$  induces an injective morphism f from  $J(C)$  to the Weil restriction of  $J(C')$  from  $\mathbb{F}_{q_F}$ , to  $\mathbb{F}_{q_F}$ , and  $h_{F'/F}$  can be interpreted as the order of the group  $A(\mathbb{F}_{q_F})$  where A is the cokernel of f; we call A the Prym variety of the covering  $C' \to \tilde{C}$ . We restrict options for C and C' using the structure of simple abelian varieties of order 1 over  $\mathbb{F}_q$ : for  $q \geq 5$  there are none; for  $q = 3, 4$ there are only elliptic curves; for  $q = 2$  there is an infinite series described in work of Madan–Pal [\[23\]](#page-13-10) and Robinson [\[29\]](#page-13-11).

The severe restrictions on A impose constraints in turn on the number of rational points on  $C$  and  $C'$  over various finite extensions of their base fields. In the constant case, the restrictions lead quickly to Theorem [1.1](#page-0-0) because the zeta function of  $C'$ is uniquely determined by the zeta function of C and the degree of the extension. By contrast, in the purely geometric case there is no obvious way to predict the zeta function of  $C'$  from that of  $C$ ; we instead argue that  $C$  is forced to have many rational points, which for  $g_F \gg 0$  will violate a "linear programming" bound [\[30,](#page-13-12) Part II]. This yields effective upper bounds on  $g_F$  and  $g_{F'}$ ; we then obtain a list of candidates for the Weil polynomials of  $F$  and  $F'$  by an exhaustion in SAGEMATH (as described in [\[12\]](#page-13-13), and later used in LMFDB as per [\[7\]](#page-13-14)). There is a loose parallel

here with the Serre–Lauter method for refining upper bounds on rational points on curves over finite fields [\[16\]](#page-13-15).

To complete the proofs, we identify candidates for  $C$  with a given zeta function using data from LMFDB [\[21\]](#page-13-16), which includes a table of genus-4 curves by Xarles [\[36\]](#page-13-17), plus a similar table of genus-5 curves computed by Dragutinović  $[6]$ . We then make a computation of abelian extensions of function fields in Magma.

The relative class number one problem is now reduced to the following.

<span id="page-2-0"></span>**Conjecture 1.5.** Let  $F'/F$  be a purely geometric extension of degree  $d > 1$  with  $q_F = 2$ ,  $g_F > 1$ , and  $h_{F'/F} = 1$ . Then F appears in one of Tables [5](#page-14-2) or [6](#page-15-0)

By Theorem [1.3,](#page-1-1) this further reduces to the following two logically independent statements, which will be addressed in subsequent work [\[14,](#page-13-18) [15\]](#page-13-19).

- Any extension as in Conjecture [1.5](#page-2-0) is cyclic. This will follow from Theo-rem [1.3\(](#page-1-1)b) by extending the argument for  $q_F > 2$  (see Lemma [8.2\)](#page-10-1).
- Table [6](#page-15-0) is complete in genera 6 and 7. This will follow from a limited census based on Mukai's descriptions of canonical curves of these genera [\[27,](#page-13-20) [28\]](#page-13-21); the entries in Table [6](#page-15-0) come from a preliminary version of this census.

We have not considered the relative class number m problem for  $m > 1$ , as in [\[20\]](#page-13-6). This would require adapting Lemma [5.6](#page-6-0) to abelian varieties over  $\mathbb{F}_2$  of order m. For each  $m$  it is known that there are infinitely many simple abelian varieties of order m over  $\mathbb{F}_2$  [\[13\]](#page-13-22), but it seems hopeless to give a complete classification; a better approach might be modeled on the use of resultants to prove statements about small algebraic integers (see [\[33\]](#page-13-23) for recent progress in this direction).

All computations in SageMath and Magma are documented in Jupyter notebooks available from a GitHub repository [\[17\]](#page-13-24); the computations take under 2 hours on a single CPU (Intel i5-1135G7@2.40GHz) and generate an Excel spreadsheet of the 208 pairs of Weil polynomials in Theorem [1.3\(](#page-1-1)b). We use LMFDB labels for isogeny classes of abelian varieties over finite fields, formatted as links into the site.

## 2. Abelian varieties of order 1

We say that an abelian variety A over a finite field  $\mathbb{F}_q$  has order 1 if we have  $#A(\mathbb{F}_q) = 1$ ; that is, the group of  $\mathbb{F}_q$ -rational points of A is trivial. Recall that  $#A(\mathbb{F}_q) = P(1)$  where  $P(T) \in \mathbb{Z}[T]$  is the Weil polynomial associated to A.

<span id="page-2-2"></span>**Lemma 2.1.** Let A be a simple abelian variety of order 1 over some finite field  $\mathbb{F}_q$ .

- (a) We must have  $q \leq 4$ .
- (b) If  $q \in \{3, 4\}$ , then A is an elliptic curve with Weil polynomial  $T^2 qT + q$ .
- (c) If  $q = 2$ , then each root  $\alpha$  of the Weil polynomial of A satisfies

(2.2) 
$$
\alpha^2 + (\eta - 1)\alpha - 2\eta = 0
$$

<span id="page-2-1"></span>for some root of unity  $\eta$ . The roots of unity  $\eta$  of order n give rise to two irreducible Weil polynomials if  $n = 7,30$  and one otherwise. The resulting A is ordinary unless n is a power of 2, in which case it has p-rank 0.

*Proof.* This follows from [\[23,](#page-13-10) Theorem 4], [\[29\]](#page-13-11) (for the second assertion of (c)), [\[5,](#page-12-2) Lemma 5.1] (for the description in  $(2.2)$ ), and [\[5,](#page-12-2) Lemma 4.3] (for the *p*-rank).  $\Box$ 

We deduce some consequences for the Frobenius traces of abelian varieties of order 1; for  $q = 2$  we establish a stronger result later (Lemma [5.6\)](#page-6-0). For A an abelian variety over a finite field  $\mathbb{F}_q$  and n a positive integer, let  $T_{A,q^n}$  be the trace of the  $q^n$ -power Frobenius on A; we also write  $T_{C,q^n}$  in case  $A = J(C)$ .

<span id="page-3-2"></span>**Lemma 2.3.** Let A be a simple abelian variety of order 1 over  $\mathbb{F}_2$ . Choose  $\alpha, \eta$  as in  $(2.2)$  and assume that the order of  $\eta$  is not in  $\{1, 2, 7, 30\}$ . For

(2.4) 
$$
t_i = \text{Trace}_{\mathbb{Q}(\eta)/\mathbb{Q}}(\eta^i) = \frac{\phi(n)}{\phi(n/\gcd(n,i))}\mu\left(\frac{n}{\gcd(n,i)}\right)
$$

(where  $\mu$  is the Möbius function), we have

<span id="page-3-3"></span>
$$
T_{A,2} = \text{Trace}_{\mathbb{Q}(\eta)/\mathbb{Q}}(1-\eta) = \phi(n) - t_1
$$
  
\n
$$
T_{A,4} = \text{Trace}_{\mathbb{Q}(\eta)/\mathbb{Q}}(1+2\eta+\eta^2) = \phi(n) + 2t_1 + t_2
$$
  
\n
$$
T_{A,8} = \text{Trace}_{\mathbb{Q}(\eta)/\mathbb{Q}}(1+3\eta-3\eta^2-\eta^3) = \phi(n) + 3t_1 - 3t_2 - t_3
$$
  
\n
$$
T_{A,16} = \text{Trace}_{\mathbb{Q}(\eta)/\mathbb{Q}}(1+4\eta-2\eta^2+4\eta^3+\eta^4) = \phi(n) + 4t_1 - 2t_2 + 4t_3 + t_4.
$$

*Proof.* Our assumption on n ensures that  $\mathbb{Q}(\alpha)$  is a quadratic extension of  $\mathbb{Q}(\eta)$ . From [\(2.2\)](#page-2-1), we see that

$$
T_{A,2} = \text{Trace}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \text{Trace}_{\mathbb{Q}(\eta)/\mathbb{Q}}(1-\eta) = \phi(n) - t_1.
$$

Similarly, from [\(2.2\)](#page-2-1) we deduce that

$$
0 = \alpha^{4} + (-1 - 2\eta - \eta^{2})\alpha^{2} + 4\eta^{2}
$$
  
=  $\alpha^{6} + (-1 - 3\eta + 3\eta^{2} + \eta^{3})\alpha^{3} - 8\eta^{3}$   
=  $\alpha^{8} + (-1 - 4\eta + 2\eta^{2} - 4\eta^{3} - \eta^{4})\alpha^{4} + 16\eta^{4}$ ,

from which we read off the expressions for  $T_{A,4}, T_{A,8}, T_{A,16}$ .  $\Box$ 

<span id="page-3-5"></span>**Lemma 2.5.** Let A be an abelian variety of order 1 and dimension g over  $\mathbb{F}_q$ .

- (a) If  $q = 4$ , then  $T_{A,q} = 4g$ ,  $T_{A,q^2} = 8g$ .
- (b) If  $q = 3$ , then  $T_{A,q} = 3g$ ,  $T_{A,q^2} = 3g$ .
- (c) If  $q = 2$  and A is simple, then  $T_{A,2} + T_{A,4} \geq 2$ . This is strict if  $q \geq 4$ .

Proof. Parts (a) and (b) are apparent from Lemma [2.1.](#page-2-2) To check (c), we check for  $g \leq 6$  using LMFDB;<sup>[1](#page-3-1)</sup> see Table [2](#page-7-1) for the detailed results. For  $g > 6$ , Lemma [2.3](#page-3-2) and [\(2.4\)](#page-3-3) yield  $T_{A,2} + T_{A,4} = 2g + t_1 + t_2 \geq 2g - 1 - 2 \geq 2$ , as desired.  $\Box$ 

# 3. Constant extensions

<span id="page-3-0"></span>In this section, we prove Theorem [1.1.](#page-0-0) We recall a point from the introduction: for any abelian variety A over  $\mathbb{F}_q$  and any positive integer d, the Weil restriction of A from  $\mathbb{F}_{q^d}$  to  $\mathbb{F}_q$  is isogenous to the product of A with the "Prym variety" A'.

<span id="page-3-4"></span>**Lemma 3.1.** Let A be an abelian variety over  $\mathbb{F}_q$  such that  $#A(\mathbb{F}_q) = #A(\mathbb{F}_{q^d})$ for some prime  $d > 2$ . Then  $q = 2$ ,  $d = 3$ , and the Weil polynomial of every simple isogeny factor of A belongs to  $\{T^2 + T + 2, T^2 + 2T + 2\}.$ 

*Proof.* Since  $[A(\mathbb{F}_{q^d}) : A(\mathbb{F}_q)] = \#A'(\mathbb{F}_q)$  is an integer, the hypothesis that  $\#A(\mathbb{F}_q) =$  $#A(\mathbb{F}_{q^d})$  implies the same for the isogeny factors of A; we may thus assume that A is simple. Let  $P(T)$  be the Weil polynomial of A. Then the Weil polynomial of A' is  $\prod_{i=1}^{d-1} P(\zeta_d^i T)$ , and hence has roots  $\alpha_1, \ldots, \alpha_{d-1}$  such that

$$
\alpha_1 \zeta_d = \cdots = \alpha_{d-1} \zeta_d^{d-1};
$$

<span id="page-3-1"></span><sup>&</sup>lt;sup>1</sup>On an LMDFB page, the entry "Point counts of the curve" lists  $q^{i}+1-T_{A,q^{i}}$  for  $i=1,\ldots,10$ .

by Lemma [2.1,](#page-2-2) this is impossible if  $q > 2$ . If  $q = 2$ , then by [\(2.2\)](#page-2-1) there must exist roots of unity  $\eta_1, \ldots, \eta_{d-1}$  with

$$
\alpha_i^2 + (\eta_i - 1)\alpha_i - 2\eta_i = 0 \qquad (i = 1, ..., d - 1).
$$

For  $1 \leq i < j \leq d-1$ , applying [\[5,](#page-12-2) Lemma 5.2, Lemma 7.2] to the equation  $\alpha_i =$  $\alpha_j \zeta_d^{j-i}$  shows that  $(\eta_i, \eta_j, \zeta_d^{j-i})$  either appears in one of the parametric solutions in  $[5, (7.2.1)]$  $[5, (7.2.1)]$  or is a sporadic solution fitting a pattern listed in  $[5,$  Table 2.

If only parametric solutions occur, then from [\[5,](#page-12-2) (7.2.1)] we have  $\eta_1 = \cdots = \eta_{d-1}$ , leaving only two distinct values for  $\alpha_1, \ldots, \alpha_{d-1}$ . Hence  $d = 3$ ; from [\[5,](#page-12-2) (7.2.1)] again,  $\eta_1 = \eta_2 = -\zeta_3$  has order 6. This yields the Weil polynomial  $T^2 + T + 2$ .

If we get a sporadic solution for some *i*, *j*, then [\[5,](#page-12-2) Table 2] indicates that  $\zeta_d^{j-i}$ has order dividing 21, 24, or 30; this forces  $d \leq 7$ . For  $d \in \{5, 7\}$ , the  $\eta_i$  must all have order 30 or 7, respectively; however, if  $\alpha$  satisfies [\(2.2\)](#page-2-1) for some root of unity  $\eta$ of this order, then at most two of the quantities  $\{\alpha \zeta_d^i : i = 1, \ldots, d-1\}$  do likewise, and this leaves no options for A'. Hence  $d = 3$ ; from [\[5,](#page-12-2) Table 2] (taking  $\eta_3 = \zeta_3$ ),  $\eta_1 = \eta_2$  has order 4. This yields the Weil polynomial  $T^2 + 2T + 2$ .

<span id="page-4-0"></span>**Lemma 3.2.** Let C be an algebraic curve of genus  $g > 0$  over  $\mathbb{F}_q$  such that  $\#J(C)(\mathbb{F}_q) = \#J(C)(\mathbb{F}_{q^d})$  for some integer  $d > 1$ . Then

$$
(q, d, g) \in \{(2, 2, 1), (2, 2, 2), (2, 2, 3), (2, 3, 1), (3, 2, 1), (4, 2, 1)\}.
$$

*Proof.* It suffices to prove the claim when  $d$  is prime, as the result will then rule out composite values of d. By Lemma [2.1,](#page-2-2)  $q \leq 4$ . By Lemma [3.1](#page-3-4) applied with  $A = J(C)$ , if  $d > 2$  then  $(q, d, g) = (2, 3, 1)$ .

Assume now that  $d = 2$ . Then the Prym variety A' is the quadratic twist of  $J(C)$ , so  $T_{A',q^i} = (-1)^i T_{C,q^i}$ . If  $q \in \{3,4\}$ , then by Lemma [2.5,](#page-3-5)

$$
0 \leq #C(\mathbb{F}_{q^2}) - #C(\mathbb{F}_q) = (q^2 + 1 - T_{A',q}) - (q + 1 + T_{A',q})
$$
  
=  $q^2 - q - T_{A',3} - T_{A',9} = q^2 - q - q(q - 1)g$ 

and so  $q \leq 1$ . If  $q = 2$ , then

$$
0 \leq \#C(\mathbb{F}_4) - \#C(\mathbb{F}_2) = (2^2 + 1 - T_4) - (2 + 1 + T_2) = 2 - T_2 - T_4 \leq 0
$$

with the last inequality strict unless  $A'$  is simple of dimension at most 3.  $\Box$ 

**Lemma 3.3.** Let C be a curve over  $\mathbb{F}_q$  such that  $\#J(C)(\mathbb{F}_q) = \#J(C)(\mathbb{F}_{q^d})$  for some  $d > 1$ . Then C appears in Theorem [1.1.](#page-0-0)

*Proof.* As this property only depends on the isogeny class of  $J(C)$ , it suffices to search over the isogeny classes in LMFDB permitted by Lemma [3.2.](#page-4-0)  $\Box$ 

### 4. Bounds on rational points on curves

We next compile some explicit upper bounds for the number of rational points on a curve over  $\mathbb{F}_q$ . For  $g \leq 10$  $g \leq 10$  $g \leq 10$ , we reproduce in Table 1 some data from [\[24\]](#page-13-25) (see therein for underlying references). For larger  $g$ , we use the "linear programming" method of Oesterlé. (All decimal expansions herein refer to *exact* rational numbers.)

<span id="page-4-1"></span>**Lemma 4.1.** Let C be a curve of genus g over  $\mathbb{F}_q$  with  $q \in \{2,3,4\}$ . Then

$$
\#C(\mathbb{F}_q) \le \begin{cases} 0.6272g + 9.562 & (q = 2) \\ 1.153g + 11.67 & (q = 3) \\ 1.435g + 21.75 & (q = 4). \end{cases}
$$

| $g \qquad   \quad 1 \quad   \quad 2 \quad   \quad 3 \quad   \quad 4 \quad   \quad 5 \quad   \quad 6 \quad   \quad 7 \quad   \quad 8 \quad   \quad 9 \quad   \quad 10$   |  |  |  |  |  |
|---|--|--|--|--|--|
|   |  |  |  |  |  |
|   |  |  |  |  |  |
| $\begin{array}{c ccccc} q=2 & 5 & 6 & 7 & 8 & 9 & 10 & 10 & 11 & 12 & 13 \\ q=2^2 & 9 & 10 & 14 & 15 & 17 & 20 & 21 & 23 & 26 & 27 \\ q=2^3 & 25 & 33 & 38 & 45 & 53 & 65 & 69 & 75 & 81 & 86 \\ \end{array}$ |  |  |  |  |  |
|   |  |  |  |  |  |
|   |  |  |  |  |  |

<span id="page-5-0"></span>TABLE 1. Upper bounds on  $\#C(\mathbb{F}_q)$  for a genus-g curve C from [\[24\]](#page-13-25).

*Proof.* For  $q = 2$ , this is the "third choice" bound of [\[30,](#page-13-12) (7.1.4)]. For  $q = 3, 4$ , we adapt the proof of the "first choice" bound of [\[30,](#page-13-12) (7.1.1)]). For  $x_1, x_2, \ldots \ge 0$ , define  $c = 1 + 2x_1^2 + 2x_2^2 + \cdots$  and consider the function

$$
f(\theta) = \frac{1}{c}(1 + 2x_1 \cos(\theta) + 2x_2 \cos(2\theta) + \cdots)^2 = 1 + 2 \sum_{n \ge 1} c_n \cos(n\theta).
$$

By construction,  $f(\theta) \ge 0$  for all  $\theta \in \mathbb{R}$  and  $c_n \ge 0$  for all n (that is, f is *doubly positive* in the sense of Serre). Define  $\psi(t) = \sum_{n=1}^{\infty} c_n t^n$ ; then by [\[30,](#page-13-12) Theorem 5.3.3].

$$
\#C(\mathbb{F}_q)\psi(q^{-1/2}) \le g + \psi(q^{-1/2}) + \psi(q^{1/2}),
$$

or in other words

$$
\#C(\mathbb{F}_q)\leq \frac{1}{\psi(q^{-1/2})}g+1+\frac{\psi(q^{1/2})}{\psi(q^{-1/2})}.
$$

For  $x_1 = 1, x_2 = 0.7, x_3 = 0.2, x_4 = \cdots = 0$ , this yields the indicated results.  $\Box$ 

The bounds produced by linear programming also include some correction terms counting points over extension fields. We make one such bound explicit for  $q = 2$ .

<span id="page-5-3"></span>**Lemma 4.2.** Let C be a curve of genus g over  $\mathbb{F}_2$ . For  $d = 1, 2, \ldots$ , let  $a_d$  be the number of closed points of degree d on C. Then

<span id="page-5-1"></span>
$$
(4.3) \qquad a_1 + 2a_2(0.3366) + 3a_3(0.1382) + 4a_4(0.0537) \le 0.8042g + 5.619.
$$

*Proof.* With notation as in the proof of Lemma [4.1,](#page-4-1) define  $\psi_d(t) = \sum_{n=1}^{\infty} c_{dn} t^{dn}$ . Then by [\[30,](#page-13-12) Theorem 5.3.3] again,

<span id="page-5-2"></span>
$$
\sum_{d=1}^{\infty} da_d \psi_d(q^{-1/2}) \le g + \psi(q^{-1/2}) + \psi(q^{1/2}),
$$

or in other words

(4.4) 
$$
a_1 + \sum_{d=2}^{\infty} da_d \frac{\psi_d(q^{-1/2})}{\psi(q^{-1/2})} \leq \frac{1}{\psi(q^{-1/2})} g + 1 + \frac{\psi(q^{1/2})}{\psi(q^{-1/2})}
$$

We apply this with  $x_1 = 1, x_2 = 0.85, x_3 = 0.25, x_4 = \cdots = 0$ . This yields [\(4.3\)](#page-5-1) by discarding the terms  $d \geq 5$  in [\(4.4\)](#page-5-2).

.

### 5. Numerical estimates

We next apply the bounds on rational points to bound the genera of function fields occurring in a purely geometric extension with relative class number 1. We will later take a closer account of the degree of the extension; see §[7.](#page-8-0)

For the remainder of the paper, let  $F'/F$  be a purely geometric extension of degree d such that  $g_{F'} > g_F$  and  $h_{F'/F} = 1$ . For brevity, we write  $q, g, g'$  in place

of  $q_F, g_F, g_{F'}$ . Let A be the Prym variety of  $C' \rightarrow C$ ; then A has order 1, so Lemma [2.1](#page-2-2) implies  $q \leq 4$ . By Riemann–Hurwitz,

<span id="page-6-1"></span>(5.1) 
$$
\dim(A) = g' - g = (d-1)(g-1) + \delta
$$
 with  $\delta \ge 0$ ,

with equality if and only if  $C' \to C$  is étale. Since  $T_{C',q^i} = T_{C,q^i} + T_{A,q^i}$ , we have

<span id="page-6-5"></span>
$$
(5.2) \quad 0 \leq #C'(\mathbb{F}_{q^i}) = q^i + 1 - T_{C',q^i} = q^i + 1 - T_{C,q^i} - T_{A,i} = #C(\mathbb{F}_{q^i}) - T_{A,q^i}
$$

for each positive integer  $i$ , and hence

<span id="page-6-2"></span>(5.3) 
$$
T_{A,q^i} \leq #C(\mathbb{F}_{q^i}) \qquad (i = 1, 2, ...).
$$

<span id="page-6-6"></span>**Lemma 5.4.** If  $q > 2$ , then  $q \leq 6$ .

*Proof.* By combining Lemma [2.5,](#page-3-5) Lemma [4.1,](#page-4-1)  $(5.1)$ , and  $(5.3)$ , we obtain

<span id="page-6-3"></span>(5.5) 
$$
q(g-1) \le q(g'-g) \le \#C(\mathbb{F}_q) \le \begin{cases} 1.153g + 11.67 & (q = 3) \\ 1.435g + 21.75 & (q = 4). \end{cases}
$$

Comparing the ends of this equation yields

$$
g \le \begin{cases} (11.67 + 3)/(3 - 1.153) \le 7.95 & (q = 3) \\ (21.75 + 4)/(4 - 1.435) \le 10.04 & (q = 4); \end{cases}
$$

hence  $g \le 7$  if  $g = 3$  and  $g \le 10$  if  $g = 4$ . Replacing the right-hand side of [\(5.5\)](#page-6-3) with the explicit bounds given in Table [1,](#page-5-0) we may eliminate the case  $g = 7$ .  $\Box$ 

For  $q = 2$ , it is not enough to control  $\#C(\mathbb{F}_2)$  because there exists a simple abelian variety of order 1 with trace 0 (namely [2.2.a](http://www.lmfdb.org/Variety/Abelian/Fq/2.2.a_ae) ae). Instead, we use a bound modeled on Lemma [4.2.](#page-5-3) For A an abelian variety over  $\mathbb{F}_2$ , define its excess as

$$
1.3366T_{A,2} + 0.3366T_{A,4} + 0.1137(T_{A,8} - T_{A,2}) + 0.0537(T_{A,16} - T_{A,4}) - 1.5612g.
$$

<span id="page-6-0"></span>**Lemma 5.6.** For A an abelian variety of order 1 and dimension g over  $\mathbb{F}_2$ , the excess of A is nonnegative.

*Proof.* We may assume that A is simple; define  $n$  as in Lemma [2.1.](#page-2-2) We again treat the case  $g \leq 6$  using LMFDB; see Table [2.](#page-7-1) For  $g \geq 7$ , we have  $g = \phi(n)$ ; per Lemma [2.3](#page-3-2) we can write the excess as

$$
0.112g - 0.1012t_1 - 0.1656t_2 + 0.1011t_3 + 0.0537t_4.
$$

For  $g \in \{7, 8\}$ , we have  $n \in \{15, 16, 20, 24, 30\}$ ; we compute the excess using  $(2.4)$ to obtain a lower bound of 0.4807. For  $g \geq 9$ , we apply [\(2.4\)](#page-3-3) to deduce that  $|t_d| \leq d$ and then obtain a lower bound of  $0.112g - 0.9505 \ge 0.112 \cdot 9 - 0.9505 \ge 0.0575$ . □

<span id="page-6-4"></span>**Lemma 5.7.** For  $q = 2$ , we have

$$
g' \le 0.4313 \# C(\mathbb{F}_2) + 1.5152g + 3.6.
$$



<span id="page-7-1"></span>TABLE 2. Simple abelian varieties over  $\mathbb{F}_2$  of order 1 and dimension at most  $6$ , from [LMFDB.](https://www.lmfdb.org/Variety/Abelian/Fq/?q=2&simple=yes&g=1-6&abvar_point_count=%5B1%5D&search_type=List) For the definitions of  $n$  and the excess, see Lemma [2.1](#page-2-2) and Lemma [5.6.](#page-6-0)

Proof. We combine Lemma [4.2,](#page-5-3) [\(5.3\)](#page-6-2), and Lemma [5.6](#page-6-0) to obtain

$$
1.5612(g'-g) \le 1.3366T_{A,q} + 0.3366T_{A,q^2} + 0.1137(T_{A,q^3} - T_{A,q})
$$
  
+ 0.0537(T\_{A,q^4} - T\_{A,q^2})  
= (1.3366 - 0.1137)T\_{A,q} + (0.3366 - 0.0537)T\_{A,q^2}  
+ 0.1137T\_{A,q^3} + 0.0537T\_{A,q^4}  
\le (1.3366 - 0.1137) \# C(\mathbb{F}\_q) + (0.3366 - 0.0537) \# C(\mathbb{F}\_{q^2})  
+ 0.1137 \# C(\mathbb{F}\_{q^3}) + 0.0537 \# C(\mathbb{F}\_{q^4})  
= 1.3366a\_1 + 0.3366(a\_1 + 2a\_2) + 0.1137(3a\_3) + 0.0537(4a\_4)  
= 1.6732a\_1 + 0.3366(2a\_2) + 0.1137(3a\_3) + 0.0537(4a\_4)  
\le 0.6732 \# C(\mathbb{F}\_2) + 0.8042g + 5.619,

which yields the claimed inequality.  $\Box$ 

<span id="page-7-2"></span>**Corollary 5.8.** For  $q = 2$ , we have  $q \leq 40$ . Moreover, if  $d \geq 3$  then  $q \leq 6$ ; if  $d \geq 4$  then  $g \leq 4$ ; if  $d \geq 5$  then  $g \leq 3$ ; and if  $d \geq 6$  then  $g \leq 2$ .

Proof. By [\(5.1\)](#page-6-1) and Lemma [5.7,](#page-6-4)

$$
(d - 1.5152)g \le 0.4313 \# C(\mathbb{F}_2) + (d + 2.6).
$$

Taking  $d = 2$  and using the bound on  $\#C(\mathbb{F}_2)$  from Lemma [4.1](#page-4-1) yields  $g \leq 40$ . For  $d \geq 3$  we obtain  $g \leq 8$ ; we then use Table [1](#page-5-0) to obtain the remaining bounds.  $\Box$ 

### 6. Exhaustion over Weil polynomials

<span id="page-7-0"></span>We next describe an exhaustive search over Weil polynomials which rules out some additional pairs  $(g, g')$ ; compare [\[30,](#page-13-12) Theorem 7.2.1] for an example in the context of bounding rational points on curves. This will yield Theorem [1.2;](#page-1-0) for  $g > 1$ , we will do better with constraints depending on d (see §[7\)](#page-8-0).

We first make a list of candidate Weil polynomials for  $A$ . For  $q > 2$  this consists of the single polynomial  $(T^2 - qT + q)^{g'-g}$ . For  $q = 2$ , we identify isogeny classes of simple abelian varieties A of order 1 such that for  $i = 1, 2, T_{A,2}$  and  $T_{A,4}$  is at

most the value listed in Table [1](#page-5-0) for the pair  $(g, 2<sup>i</sup>)$ , and moreover

$$
T_{A,2} + 0.3366(T_{A,4} - T_{A,2}) + 0.1137(T_{A,8} - T_{A,2}) + 0.0537(T_{A,16} - T_{A,4})
$$
  
  $\leq 0.8042g + 5.619;$ 

these are all necessary conditions by Lemma [4.2](#page-5-3) and [\(5.3\)](#page-6-2).

We next identify candidate Weil polynomials for  $C$  for which the resulting values of  $\#C(\mathbb{F}_q)$  (and  $\#C(\mathbb{F}_{q^2})$  for  $q=2$ ) are consistent with at least one choice of A, and eliminate those that are ruled out by any of the following.

- Bounds on point counts from Table [1.](#page-5-0)
- The *positivity condition*: the number of degree-i places on  $C$  must be nonnegative for all  $i > 1$ .
- Data from LMFDB (genus  $\leq$  3), [\[36\]](#page-13-17) (genus 4), and [\[6\]](#page-13-5) (genus 5) indicating which curves have a particular Weil polynomial.
- The resultant-1 and resultant-2 criteria of Serre [\[30,](#page-13-12) Theorem 2.4.1] as extended by Howe–Lauter [\[10,](#page-13-26) Proposition 2.8]. The resultant-2 criterion forces C to occur as a double cover of another curve, whose Weil polynomial can sometimes be ruled out. (Compare Corollary [9.3.](#page-11-0))

Finally, we exhaust over pairs of candidate Weil polynomials for C and A to confirm that the resulting Weil polynomial for  $C'$  is not ruled out. This yields the following.

<span id="page-8-1"></span>**Lemma 6.1.** For  $q = 2$ , for  $g = 0, \ldots, 6$  we have  $g' \le 4, 6, 8, 10, 12, 14, 16$ , respec-tively. Hence by [\(5.1\)](#page-6-1), if  $d \geq 4$  then  $q \leq 3$ ; and if  $d \geq 5$  then  $q \leq 2$ .

*Proof.* From Lemma [5.7,](#page-6-4) for  $g = 0, ..., 6$  we obtain  $g' \le 4, 7, 9, 11, 13, 15, 17$ , respectively. We rule out the pairs  $(g, g') \in \{(1, 7), (2, 9), (3, 11), (4, 13), (5, 15), (6, 17)\}$  by exhausting over Weil polynomials as described above.  $\Box$ 

We can now prove Theorem [1.2](#page-1-0) as follows. By [\(5.5\)](#page-6-3), Lemma [6.1,](#page-8-1) and Table [1,](#page-5-0) for  $(q, g) = (2, 0), (2, 1), (3, 0), (3, 1), (4, 0), (4, 1)$  we have respectively

$$
g' \le 4, 6, 1, 3, 1, 3.
$$

We may settle all cases by table lookups except  $(q, g, g') = (2, 1, 6)$ , which we settle as follows.

- The isogeny class [6.2.ad](http://www.lmfdb.org/Variety/Abelian/Fq/6.2.ad_c_a_a_m_abg) c a a m abg can be ruled out by the following ar-gument from [\[8\]](#page-13-4). By the resultant-2 criterion (compare Remark [10.3\)](#page-12-3), C' is a double cover of a curve  $C_0$  with real Weil polynomial  $T^2 - 2T - 2$ ; this is inconsistent with  $\#C_0(\mathbb{F}_2) = 1, \#C'(\mathbb{F}_4) = 0.$
- The isogeny class  $6.2$  ad  $c_a$  f am q occurs for a cyclic étale quintic cover of a genus-2 curve listed in Table [5](#page-14-2) (see also Remark [6.2\)](#page-8-2).

<span id="page-8-2"></span>Remark 6.2. Table [3](#page-14-0) includes a column counting Jacobians in the isogeny class of  $J(C')$ . This can be obtained by table lookups except for [6.2.ad](http://www.lmfdb.org/Variety/Abelian/Fq/6.2.ad_c_a_f_am_q) c\_a\_f\_am\_q, for which Table [3](#page-14-0) reports a *unique* Jacobian; this will be proved in [\[14\]](#page-13-18).

# 7. Additional constraints on Weil polynomials

<span id="page-8-0"></span>We assume hereafter that  $g > 1$  and introduce constraints on the Weil polynomials of C and C' based on d. Note that none of these presumes  $h_{F'/F} = 1$ , and so may be applicable in other cases of interest.

We start with the full form of Riemann–Hurwitz:

(7.1) 
$$
2g' - 2 = d(2g - 2) + 2\delta, \qquad 2\delta = \sum_{P} (e_P - 1)
$$

where  $P$  runs over geometric points of  $C'$  and  $e_P$  is the ramification index at  $P$ .

Let t denote the number of geometric ramification points, i.e., the number of  $P$ for which  $e_P > 1$ . Then  $t = 0$  iff  $\delta = 0$ , and  $t \leq 2\delta$  in general. If q is even, then  $e_P$ can never equal 2, so  $t \leq \delta$ ; in particular,

<span id="page-9-4"></span>(7.2) 
$$
\delta = 1 \Longrightarrow t = 1 \Longrightarrow \#C'(\mathbb{F}_q) \ge 1
$$

because the unique ramification point of  $C'$  is  $\mathbb{F}_q$ -rational, and similarly

<span id="page-9-5"></span>(7.3) 
$$
\delta = 2 \Longrightarrow \#C'(\mathbb{F}_{q^2}) \ge 1, \qquad t = 2 \Longrightarrow \#C'(\mathbb{F}_{q^2}) \ge 2.
$$

If  $C' \rightarrow C$  is cyclic of prime degree  $d = p \mid q$ , then the Deuring–Shafarevich formula holds (e.g., see [\[32\]](#page-13-27)): for  $\gamma_C, \gamma_{C'}$  the p-ranks of  $C, C',$ 

$$
\gamma_{C'} - 1 = d(\gamma_C - 1) + t
$$

<span id="page-9-1"></span>If  $\delta = 0$  and  $C' \to C$  is cyclic (e.g., if  $d = 2$ ), then by class field theory,

(7.5) 
$$
\#J(C)(\mathbb{F}_q) \equiv 0 \pmod{d}.
$$

For small  $d$ , we have the following additional constraints (building on [\[9,](#page-13-28) Lemma 8]).

<span id="page-9-2"></span>• When  $d = 2$ , every  $\mathbb{F}_{q^i}$ -rational point of C lifts to either an  $\mathbb{F}_{q^i}$ -rational ramification point or two  $\mathbb{F}_{q^{2i}}$ -rational points of C'. Hence

(7.6) 
$$
\#C'(\mathbb{F}_{q^{2i}}) \geq 2 \#C(\mathbb{F}_{q^{i}}) - t;
$$

<span id="page-9-6"></span><span id="page-9-0"></span>by  $(5.2)$  and  $(5.3)$ , this yields

(7.7) 
$$
2T_{A,q^i} + T_{A,q^{2i}} - t \leq 2\#C(\mathbb{F}_{q^i}) + T_{A,q^{2i}} - t \leq \#C(\mathbb{F}_{q^{2i}}).
$$

<span id="page-9-8"></span>For  $i = 2j - 1$  odd, every degree *i*-place of C' projects to a degree-i place of C. If  $t \leq 2$ , then for  $i > 1$  these points occur in pairs in fibers, and so

(7.8) 
$$
t \leq 2 \Longrightarrow \#C'(\mathbb{F}_{q^{2j-1}}) \equiv \#C'(\mathbb{F}_q) \pmod{2} \qquad (j > 0).
$$

• When  $d = 3$ , every  $\mathbb{F}_{q^i}$ -rational point of C lifts to either at least one  $\mathbb{F}_{q^i}$ -rational points of C'. Hence  $\#C'(\mathbb{F}_{q^{3i}})$  –  $\vec{\#C}'(\mathbb{F}_{q^i}) \geq 3(\#C(\mathbb{F}_{q^i}) - \#C'(\mathbb{F}_{q^i}))$ ; by [\(5.3\)](#page-6-2), this yields

(7.9) 
$$
\#C(\mathbb{F}_{q^i}) + 2T_{A,q^i} + T_{A,q^{3i}} \leq \#C(\mathbb{F}_{q^{3i}}).
$$

<span id="page-9-7"></span><span id="page-9-3"></span>• When  $d = 4$ , every  $\mathbb{F}_{q^i}$ -rational point of C lifts to at least one  $\mathbb{F}_{q^i}$ -rational point, two  $\mathbb{F}_{q^{2i}}$ -rational ramification points, or four  $\mathbb{F}_{q^{4i}}$ -rational points of C'. Hence  $\#C'(\mathbb{F}_{q^{4i}}) \geq 4(\#C(\mathbb{F}_{q^{i}}) - \#C'(\mathbb{F}_{q^{i}})) - 2t$ ; by [\(5.3\)](#page-6-2), this yields

$$
(7.10) \t 4T_{A,q^i} + T_{A,q^{4i}} - 2\delta \le 4T_{A,q^i} + T_{A,q^{4i}} - 2t \le #C(\mathbb{F}_{q^{4i}}).
$$

<span id="page-9-9"></span>**Remark 7.11.** For  $d = 2$ , the compositum  $F' \cdot \mathbb{F}_{q^2}$  contains another purely geometric quadratic extension  $F''/F$ . We call the corresponding cover  $C'' \to C$  the *relative quadratic twist* of  $C' \rightarrow C$ ; it also obeys the conditions listed in §[6.](#page-7-0)

#### 8. PURELY GEOMETRIC EXTENSIONS:  $q > 2$

<span id="page-10-0"></span>We settle Theorem [1.3\(](#page-1-1)a) as follows. For  $q > 2$ , Lemma [5.4](#page-6-6) implies  $q \leq 6$ . If  $d = 2$ , then by Lemma [2.5](#page-3-5) plus [\(7.7\)](#page-9-0),

<span id="page-10-2"></span>
$$
(8.1) \#C(\mathbb{F}_{q^2}) \ge 2T_{A,q} + T_{A,q^2} - c(g'-2g+1) = q^2(g'-g) - c(g'-2g+1) \ge q^2(g-1).
$$

Combining [\(8.1\)](#page-10-2) with Table [1,](#page-5-0) we deduce that

$$
(q, g, g') \in \{(3, 2, 3), (3, 2, 4), (3, 3, 5), (3, 3, 6), (3, 4, 7), (4, 2, 3), (4, 2, 4), (4, 3, 5)\}.
$$

If  $d > 2$ , then by upgrading [\(5.5\)](#page-6-3) using Table [1,](#page-5-0) we deduce that  $(d, g, g') = (3, 2, 4)$ . We also have the following.

<span id="page-10-1"></span>**Lemma 8.2.** If  $q > 2$ ,  $q = 2$ , and  $d = 3$ , then  $C' \rightarrow C$  is cyclic.

*Proof.* Suppose first that  $C' \rightarrow C$  is a non-Galois cover which becomes Galois after a quadratic constant field extension. By Lemma [2.5,](#page-3-5) the quadratic twist  $\tilde{C}$  of C admits a cyclic cubic étale cover  $\tilde{C}'$  whose Prym has Weil polynomial  $(T^2 + qT + q)^2$ . Since each  $\mathbb{F}_q$ -point of  $\tilde{C}$  lifts to at most three  $\mathbb{F}_q$ -points of  $\tilde{C}'$ , we have  $\#\tilde{C}(\mathbb{F}_q) + 2q = \tilde{C}'(\mathbb{F}_q) \leq 3\#\tilde{C}(\mathbb{F}_q)$  and so  $\tilde{C}(\mathbb{F}_q) \geq q$ . However,  $\#C(\mathbb{F}_q) \geq 2q$ by [\(5.3\)](#page-6-2), yielding the impossibility

$$
2q + 2 = \#C(\mathbb{F}_q) + \# \tilde{C}(\mathbb{F}_q) \ge 3q.
$$

Suppose next that  $C' \to C$  is geometrically non-Galois. In this case, the Galois closure F'' of F'/F is itself the function field of a curve C'' with  $q_{F}$  =  $q_F$ . The abelian variety  $J(C'')$  is isogenous to  $J(C) \times A^2 \times E$  for some elliptic curve E, so

 $\#C''(\mathbb{F}_q) = \#C(\mathbb{F}_q) - 2T_{A,q} - T_{E,q} = \#C(\mathbb{F}_q) - 4q - T_{E,q} \leq \#C(\mathbb{F}_q) - 3q;$ 

this yields  $\#C(\mathbb{F}_q) \geq 3q$ , which is inconsistent with Table [1.](#page-5-0)  $\Box$ 

We now know that in all cases  $C' \to C$  is cyclic, so we may proceed as follows.

- We again exhaust over Weil polynomials for  $C$  and  $A$ , but this time accounting for  $(7.4)$ ,  $(7.5)$ ,  $(7.7)$ ,  $(7.9)$ ,  $(8.1)$ . At this point the cases  $(q, d, g, g') =$  $(3, 2, 3, 6), (4, 2, 2, 4)$  drop out.
- For each candidate Weil polynomial for  $C$ , we consult LMFDB to find all candidates for C. At this point the case  $(q, d, g, g') = (3, 2, 4, 7)$  drops out: the only isogeny class for  $J(C)$  is [4.3.f](http://www.lmfdb.org/Variety/Abelian/Fq/4.3.f_v_ca_eg) v ca eg, which contains no Jacobian.
- We then use MAGMA to compute all cyclic extensions of  $F$  with the desired degree and ramification behavior and check the resulting Weil polynomial for A. At this point the case  $(q, d, g, g') = (4, 2, 3, 5)$  drops out.

This yields Theorem [1.3\(](#page-1-1)a).

### 9. A refined resultant criterion

In preparation for the case  $q = 2$ , we next introduce a refinement of the resultant criteria, modeled on [\[10,](#page-13-26) Proposition 2.8] (applicable over any finite base field).

<span id="page-10-3"></span>**Lemma 9.1.** Let  $f: C' \to C$  be a finite flat morphism of degree d between smooth projective curves over an arbitrary field k. Let  $f^* : J(C) \to J(C')$  denote the pullback map and let  $f_* : J(C') \to J(C)$  denote the pushforward map. Let A be the Prym variety of  $f$ , defined as the reduced closed subscheme of the identity component of  $\ker(f_*)$ . Then there is an exact sequence

<span id="page-10-4"></span>(9.2) 
$$
0 \to \Delta \to J(C) \times_k A \to J(C') \to 0
$$

where the map  $J(C) \to J(C')$  is  $f^*$  and  $\Delta$  is a finite flat group scheme killed by d.

*Proof.* The composition  $J(C) \stackrel{f^*}{\to} J(C') \stackrel{f_*}{\to} J(C)$  equals the isogeny [d]; consequently,  $f_*$  is surjective (as a morphism of group schemes) and  $J(C) \stackrel{f^*}{\to} J(C') \to$  $J(C')/\ker(f_*)$  is surjective. The latter implies that  $J(C) \times_k \ker(f_*) \to J(C')$  is surjective, as then is  $\ker(f_*) \to \operatorname{coker}(f^*)$ ; since the target is connected and reduced,  $A \to \mathrm{coker}(f^*)$  is surjective, as then is  $J(C) \times_k A \to J(C')$ .

Let S be an arbitrary k-scheme and suppose  $x \in (J(C) \times_k A)(S)$  maps to zero to  $J(C')$ . Write  $x = (x_1, x_2)$  with  $x_1 \in J(C)(S)$  and  $x_2 \in A(S)$ . By definition,  $x_1$  and  $-x_2$  have the same image in  $J(C')(S)$ ; that is,  $f^*(x_1) = -x_2$ . Applying  $f_*$ , we deduce that  $f_* f^*(x_1) = 0$ , and so  $[d](x_1) = 0$ ; it follows that  $[d](x) =$  $([d](x_1), [d](x_2)) = (0, [d](x_2))$  maps to zero in  $J(C')$ , and hence  $[d](x_2) = 0$ .

<span id="page-11-0"></span>Corollary 9.3. In Lemma [9.1,](#page-10-3) let  $h_1$  and  $h_2$  be the radicals of the real Weil polynomials associated to  $J(C)$  and A. Let  $\widetilde{\operatorname{res}}(h_1, h_2)$  be the modified reduced resultant of  $h_1$  and  $h_2$  in the sense of [\[10,](#page-13-26) Proposition 2.8]. Then

(9.4) 
$$
\gcd(d, \widetilde{\operatorname{res}}(h_1, h_2)) > 1.
$$

*Proof.* In [\(9.2\)](#page-10-4),  $\Delta$  cannot be trivial: otherwise,  $J(C')$  would be decomposable as a principally polarized abelian variety, violating Torelli [\[26,](#page-13-29) Theorem 12.1]. The exponent of  $\Delta$  divides d by Lemma [9.1](#page-10-3) and res $(h_1, h_2)$  by [\[10,](#page-13-26) Proposition 2.8]. □

<span id="page-11-1"></span>10. PURELY GEOMETRIC EXTENSIONS:  $q = 2$ 

To conclude, we establish parts (b) and (c) of Theorem [1.3.](#page-1-1)

<span id="page-11-2"></span>**Lemma 10.1.** If  $q = 2$  and  $d = 2$ , then  $q \leq 9$ . Moreover, for  $q = 2, \ldots, 9$  we have respectively  $g' \leq 7, 9, 10, 11, 13, 14, 15, 17$ .

Proof. Combining [\(5.1\)](#page-6-1), Lemma [5.6,](#page-6-0)and [\(7.7\)](#page-9-0) yields

 $1.5612(g-1) \le 1.5612(g'-g) - 0.3366\delta$  $\leq T_{A,q} + 0.3366(T_{A,q} + T_{A,q^2} - \delta)$ +  $0.1137(T_{A,q^3}-T_{A,q})+0.0537(T_{A,q^4}-T_{A,q^2})$  $\leq (1 - 0.3366 - 0.1137 + 0.0537)T_{A,q}$ +  $(0.3366 - 0.0537)(T_{A,q} + T_{A,q^2} - t) + 0.1137T_{A,q^3} + 0.0537T_{A,q^4}$  $\leq (1 - 0.3366 - 0.1137 + 0.0537) \# C(\mathbb{F}_q)$ +  $(0.3366 - 0.0537)(\#C(\mathbb{F}_{q^2}) - \#C(\mathbb{F}_{q}))$  $+ 0.1137 \# C(\mathbb{F}_{q^3}) + 0.0537 \# C(\mathbb{F}_{q^4})$  $= a_1 + 0.3366(2a_2) + 0.1137(3a_3) + 0.0537(4a_4) \le 0.8042g + 5.619.$ 

This yields the claimed results. □

<span id="page-11-3"></span>**Lemma 10.2.** Suppose that  $q = 2$  and  $q > 1$ .

(a) If  $d = 2$ , then  $(g, g') \in \{(2, 3), (2, 4), (2, 5), (3, 5), (3, 6), (4, 7), (4, 8), (5, 9), (6, 11), (7, 13)\}.$ (b) If  $d = 3$ , then  $(g, g') \in \{(2, 4), (2, 6), (3, 7), (4, 10)\}.$ (c) If  $d = 4$ , then  $(g, g') \in \{(2, 5), (2, 6), (3, 9)\}.$ (d) If  $d > 4$ , then  $g = 2$  and  $(d, g') \in \{(5, 6), (6, 7), (7, 8)\}.$ 

Proof. We run an exhaustive search over Weil polynomials as in §[6,](#page-7-0) but also accounting for  $(7.2)$ ,  $(7.3)$ ,  $(7.5)$  (for  $d = 2$ ),  $(7.6)$  (taking  $i = 1, 2, 3$ ),  $(7.9)$  (taking  $i = 1, 2$ , [\(7.10\)](#page-9-7) (taking  $i = 1$ ), and [\(9.4\)](#page-11-1). This rules out

 $(d, g, g') \in \{(2, 2, 6), (2, 2, 7), (2, 3, 7), (2, 3, 8), (2, 3, 9), (2, 4, 9), (2, 4, 10), (2, 4, 11),$  $(2, 5, 10), (2, 5, 11), (2, 6, 12), (2, 6, 13), (2, 7, 14), (2, 8, 15), (2, 9, 17),$ 

 $(3, 2, 5), (3, 2, 7), (3, 2, 8), (3, 3, 8), (3, 3, 9), (3, 3, 10), (3, 4, 11), (3, 4, 12),$ 

 $(3, 5, 13), (3, 5, 14), (3, 6, 16), (4, 2, 7), (4, 2, 8), (4, 3, 10), (5, 2, 7), (5, 2, 8), (6, 2, 8)$ .

(The runtime is dominated by the cases  $(d, g, g') = (2, 8, 15), (2, 9, 17)$ .) We may thus deduce (a) from [\(5.1\)](#page-6-1) and Lemma [10.1,](#page-11-2) (b) from Lemma [5.8](#page-7-2) and Lemma [6.1,](#page-8-1) and (c) and (d) from Lemma [6.1.](#page-8-1)  $\Box$ 

We obtain Theorem  $1.3(b)$  by a similar calculation which also accounts for  $(7.8)$ (taking  $j = 2$ ), Remark [7.11,](#page-9-9) and the following Remark [10.3.](#page-12-3)

<span id="page-12-3"></span>**Remark 10.3.** If  $C' \to C$  is étale and geometrically cyclic (i.e., cyclic after base extension from  $\mathbb{F}_2$  to an algebraic closure), we can upgrade Lemma [9.1](#page-10-3) to say that  $\Delta$  has exponent exactly d (because ker( $f^*$ ) is étale and cyclic of order d; compare  $(7.5)$ , and Corollary [9.3](#page-11-0) to say that  $\widetilde{\operatorname{res}}(h_1, h_2)$  must be divisible by d.

If we drop these conditions on  $C' \rightarrow C$ , we can still say something when  $gcd(d, \widetilde{\operatorname{res}}(h_1, h_2)) = 2$ : as in [\[10,](#page-13-26) Theorem 2.2] there must be a degree-2 map from C' to another curve D whose Jacobian is isogenous to  $J(C)$  or A. By  $(5.1)$ , the second option cannot occur if  $g' > 2g + 1$ ; in characteristic 2, [\(7.4\)](#page-9-1) also applies.

In the context of Theorem [1.3\(](#page-1-1)b), the condition that  $gcd(d, \widetilde{\operatorname{res}}(h_1, h_2)) = 2$  rules out some cases with  $(d, g, g') \in \{(4, 2, 6), (4, 3, 9), (6, 2, 7)\}$ : there would have to be a double cover  $C' \to D$  with  $J(D)$  isogenous to  $J(C)$ , but this is forbidden by Lemma [10.2\(](#page-11-3)a). Similarly, if  $(d, g, g') = (4, 2, 5)$ , then  $J(D)$  cannot be isogenous to A: otherwise D would admit an étale double cover while  $\#J(D)(\mathbb{F}_2) = 1$ . Hence  $J(C)$ ,  $J(C')$  must occur in Theorem [1.3\(](#page-1-1)c) with  $(d, g, g') = (2, 2, 5)$ .

<span id="page-12-6"></span>**Remark 10.4.** When  $d = 2$  and  $\delta \leq 1$ , A admits a principal polarization; over  $\mathbb{C}$ this is classical [\[3,](#page-12-4) Theorem 12.3.3], and a characteristic-free argument will appear in  $[1]$ . Our formulation of Theorem [1.3\(](#page-1-1)b) does not account for this constraint; it would rule out a further 16 pairs, which are marked with stars in Table [7.](#page-16-0)

To obtain Theorem [1.3\(](#page-1-1)c), we use table lookups to find candidates for  $C$  with a given Weil polynomial (see §[6\)](#page-7-0), then use Magma to enumerate cyclic extensions. As a consistency check, for each triple  $(d, g, g')$  listed in Lemma [10.2](#page-11-3) with  $g \leq 5$ , we enumerated cyclic extensions for all curves  $C$  of genus  $q$ ; this took about 14 hours and yielded no new results.

# **REFERENCES**

- <span id="page-12-5"></span>[1] J. Achter and S. Casalaina-Martin, Putting the p back in Prym, in preparation.
- <span id="page-12-0"></span>[2] S. Bae and P. Kang, Class numbers of cyclotomic function fields, Acta Arith. 102 (2002), 251–259.
- <span id="page-12-4"></span>[3] C. Birkenhake and H. Lange, Complex Algebraic Varieties, second edition, Grundlehren der math. Wissenschaften 302, Springer-Verlag, Berlin, 2004.
- <span id="page-12-1"></span>[4] J. Booher and J.F. Voloch, Recovering affine curves over finite fields from L-functions, Pacific J. Math.  $314$  (2021), 1-28.
- <span id="page-12-2"></span>[5] T. D'Nelly-Warady and K.S. Kedlaya, Geometric decomposition of abelian varieties of order 1, [arXiv:2109.03986v1](https://arxiv.org/abs/2109.03986) (2021).

#### 14 KIRAN S. KEDLAYA

- <span id="page-13-5"></span>[6] D. Dragutinović, Supersingular curves of genera four and five in characteristic two, masters thesis, Utrecht University, 2021; [https://github.com/DusanDragutinovic/MT\\_Curves](https://github.com/DusanDragutinovic/MT_Curves).
- <span id="page-13-14"></span>[7] T. Dupuy, K.S. Kedlaya, D. Roe, and C. Vincent, Isogeny classes of abelian varieties over finite fields in the LMFDB, in Arithmetic Geometry, Number Theory, and Computation, Simons Symposia, Springer, 2022, 375–448.
- <span id="page-13-4"></span>[8] X. Faber, J. Grantham, and E.W. Howe, On the maximum gonality of a curve over a finite field, in preparation.
- <span id="page-13-28"></span>[9] E.W. Howe and K.E. Lauter, Improved upper bounds for the number of points on curves over finite fields, Ann. Inst. Fourier (Grenoble) 53 (2000), 1677–1737.
- <span id="page-13-26"></span>[10] E.W. Howe and K.E. Lauter, New methods for bounding the number of points on curves over finite fields, in Geometry and arithmetic, Eur. Math. Soc., Zürich, 2012, 173–212.
- <span id="page-13-0"></span>[11] H. Jung and J. Ahn, Divisor class number one problem for abelian extensions over rational function fields, J. Algebra 310 (2007), 1–14.
- <span id="page-13-13"></span>[12] K.S. Kedlaya, Search techniques for root-unitary polynomials, in Computational Arithmetic Geometry, Contemporary Math. 463, Amer. Math. Soc., 2008, 71–82.
- <span id="page-13-22"></span>[13] K.S. Kedlaya, Abelian varieties over F<sup>2</sup> of prescribed order, [arXiv:2107.12453v2](https://arxiv.org/abs/2107.12453) (2021).
- <span id="page-13-18"></span>[14] K.S. Kedlaya, The relative class number one problem for function fields, II, preprint available at <https://kskedlaya.org/papers>.
- <span id="page-13-19"></span>[15] K.S. Kedlaya, The relative class number one problem for function fields, III, preprint available at <https://kskedlaya.org/papers>.
- <span id="page-13-15"></span>[16] K. Lauter, Zeta functions of curves over finite fields with many rational points, Coding Theory, Cryptography and Related Areas (Guanajuato, 1998), Springer, Berlin, 2000, 167–174.
- <span id="page-13-24"></span>[17] K.S. Kedlaya, GitHub repository <https://github.com/kedlaya/same-class-number>.
- <span id="page-13-1"></span>[18] M. Kida and N. Murabayashi, Cyclotomic function fields with divisor class number one, Tokyo J. Math. 14 (1991), 45–56.
- <span id="page-13-2"></span>[19] J.R.C. Leitzel and M.L. Madan, Algebraic function fields with equal class number, Acta Arith. 30 (1976), 169–177.
- <span id="page-13-6"></span>[20] J.R.C. Leitzel, M.L. Madan, and C.S. Queen, Algebraic function fields with small class number, J. Number Theory 7 (1975), 11–27.
- <span id="page-13-16"></span>[21] The LMFDB Collaboration, L-Functions and Modular Forms Database, <https://lmfdb.org>.
- <span id="page-13-3"></span>[22] R. Macrae, On unique factorization in certain rings of algebraic functions, J. Algebra 17 (1971), 243–261.
- <span id="page-13-10"></span>[23] M.L. Madan and S. Pal, Abelian varieties and a conjecture of R. M. Robinson, J. reine angew. Math. 291 (1977), 78–91.
- <span id="page-13-25"></span>[24] manYPoints — Table of Curves with Many Points, <https://manypoints.org> (accessed Nov 2021).
- <span id="page-13-8"></span>[25] P. Mercuri and C. Stirpe, Classification of algebraic function fields with class number one, J. Number Theory 154 (2015), 365–374.
- <span id="page-13-29"></span>[26] J.S. Milne, Jacobian varieties, in Arithmetic Geometry, Springer-Verlag, New York, 1986.
- <span id="page-13-20"></span>[27] S. Mukai, Curves and Grassmannians, in Algebraic Geometry and Related Topics, International Press, Cambridge, MA, 1993, 19–40.
- <span id="page-13-21"></span>[28] S. Mukai, Curves and symmetric spaces, I, Amer. J. Math. 117 (1995), 1627–1644.
- <span id="page-13-12"></span><span id="page-13-11"></span>[29] R.M. Robinson, Conjugate algebraic units in a special interval, Math. Z. 154 (1977), 31–40. [30] J.-P. Serre, Rational Points on Curves over Finite Fields, Doc. Math. 18, Soc. Math. France,
- 2020.
- <span id="page-13-27"></span><span id="page-13-9"></span>[31] Q. Shen and S. Shi, Function fields of class number one, J. Num. Theory 154 (2015), 375–389. [32] D. Shiomi, On the Deuring–Shafarevich formula, Tokyo Math. J. 34 (2011), 313–318.
- <span id="page-13-23"></span>[33] A. Smith, Algebraic integers with conjugates in a prescribed distribution, [arXiv:2111.12660v1](https://arxiv.org/abs/2111.12660) (2021).
- [34] A.V. Sutherland and F. Voloch, Maps between curves and arithmetic obstructions, in Arithmetic Geometry: Computations and Applications, Contemp. Math. 722, Amer. Math. Soc., 2019, 167–175.
- <span id="page-13-7"></span>[35] C. Stirpe, A counterexample to "Algebraic function fields with small class number", J. Number Theory 143 (2014), 402–404.
- <span id="page-13-17"></span>[36] X. Xarles, A census of all genus 4 curves over the field with 2 elements, [arXiv:2007.07822v1](https://arxiv.org/abs/2007.07822) (2020).

| $q_F$          | $g_F$          | $g_{F}$        | J(C)              | J(C')                          | $\#C'$         | $q_F$          | $g_F$    | $g_{F}$        | J(C)      | J(C')                   | $\#C'$         |
|----------------|----------------|----------------|-------------------|--------------------------------|----------------|----------------|----------|----------------|-----------|-------------------------|----------------|
| $\mathbf{2}$   | $\Omega$       |                | 0                 | $1.2$ .ac                      |                | $\overline{2}$ |          | $\overline{4}$ | 1.2.c     | $4.2$ ad $f$ ag $i$     |                |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{0}$    | $2.2$ .ad $-f$                 |                | $\mathbf{2}$   | Ш.       | 4              | 1.2.c     | $4.2$ .ac $-c$ .ae $-i$ | $\overline{2}$ |
| $\overline{2}$ | $\Omega$       | $\overline{2}$ | 0                 | $2.2 \text{.}$ ac $\text{-}$ c |                | $\overline{2}$ |          | 5              | 1.2.b     | $5.2$ .ad_c_d_ag_h      | 3              |
| $\overline{2}$ | $\Omega$       | 3              | $\overline{0}$    | $3.2$ .ad <sub>-C-</sub> b     |                | $\mathbf{2}$   |          | 5              | 1.2.b     | $5.2$ .ad.c.e.ai.i      | 3              |
| $\overline{2}$ | $\Omega$       | 3              | $\mathbf{0}$      | $3.2$ .ad $-d$ .ac             | Ŧ.             | $\mathbf{2}$   |          | 5              | 1.2.b     | 5.2.ad_e_ag_k_ao        | 3              |
| $\overline{2}$ | $\Omega$       | 4              | $\Omega$          | $4.2$ .ad.c.a.b                |                | $\overline{2}$ |          | 6              | 1.2.c     | $6.2$ .ad.c.a.f.am.q    | $1^*$          |
| $\overline{2}$ |                | $\overline{2}$ | 1.2.a             | $2.2 \text{.ac.e}$             |                | 3              | $\Omega$ |                | $\Omega$  | $1.3$ .ab               |                |
| $\mathbf{2}$   |                | $\mathbf{2}$   | 1.2 <sub>b</sub>  | $2.2$ .ab <sub>-c</sub>        |                | 3              |          | $\overline{2}$ | $1.3$ .ab | $2.3.$ ae $-i$          |                |
| $\mathbf{2}$   |                | $\overline{2}$ | 1.2.c             | 2.2.a.a.                       |                | 3              |          | $\overline{2}$ | 1.3.a     | $2.3$ ad $g$            |                |
| $\overline{2}$ |                | 3              | $1.2 \text{.}$ ac | $3.2$ .ad $-d$ .ac             |                | 3              |          | $\overline{2}$ | 1.3.b     | $2.3.$ ac $-d$          |                |
| $\mathbf{2}$   |                | 3              | $1.2$ .ab         | $3.2$ .ad_g_ak                 |                |                |          |                |           |                         |                |
| $\mathbf{2}$   |                | 3              | $1.2$ .ab         | $3.2$ .ac $_c$ _c $_a$ ad      |                | 3              |          | $\overline{2}$ | 1.3.c     | $2.3$ .ab $-a$          |                |
|                |                |                |                   |                                |                | 3              |          | 3              | 1.3.c     | $3.3.ae-g-ag$           |                |
| $\mathbf{2}$   |                | 3              | 1.2.b             | $3.2$ .ad. $g$ .ai             |                | 3              |          | 3              | 1.3.d     | $3.3.$ ad $-a$ .        | $\overline{2}$ |
| $\mathbf{2}$   |                | 3              | 1.2.b             | $3.2$ .ac $-e$ $ah$            |                |                |          |                |           |                         |                |
| $\overline{2}$ |                | $\overline{4}$ | 1.2.a             | $4.2$ .ad $-e$ $af$ $i$        |                | $\overline{4}$ | $\Omega$ |                | $\Omega$  | $1.4.$ ae               |                |
| $\overline{2}$ |                | 4              | 1.2.a             | $4.2$ .ad $-f$ _ai $-m$        | $\overline{2}$ | $\overline{4}$ |          | $\overline{2}$ | 1.4.a     | $2.4.ae_i$              |                |

Appendix A. Extensions of relative class number 1

<span id="page-14-0"></span>TABLE 3. Purely geometric extensions with  $g_F \leq 1$ ,  $g_{F'} > g_F$ . The column  $\#C'$  counts Jacobians in the isogeny class. The star indicates a conjectural value; see Remark [6.2.](#page-8-2)

| $q_F$          | $^{d}$         | $g_F$          | $g_{F}$        | J(C)                  | F  |
|----------------|----------------|----------------|----------------|-----------------------|--|
| 3              | $\overline{2}$ | $\mathbf{2}$   | 3              | $2.3.ab$ <sub>c</sub> | $y^2 + x^5 + 2x^2 + x$                                     |
| 3              | $\mathbf{2}$   | $\mathbf{2}$   | 3              | 2.3.ab.e              | $y^2 + x^6 + x^4 + 2x^3 + x^2 + 2x$                        |
| 3              | $\mathbf{2}$   | $\mathbf{2}$   | 3              | 2.3.b.c               | $y^2 + 2x^5 + x^2 + 2x$                                    |
| 3              | $\overline{2}$ | $\overline{2}$ | 3              | 2.3.b.e               | $y^2 + 2x^6 + 2x^4 + x^3 + 2x^2 + x$                       |
| 3              | $\overline{2}$ | $\mathbf{2}$   | $\overline{4}$ | 2.3.c <sub>h</sub>    | $y^2 + 2x^6 + x^4 + 2x^3 + x^2 + 2$                        |
| 3              | $\overline{2}$ | 3              | 5              | 3.3.c.g.i             | $y^2 + 2x^8 + x^7 + x^5 + x^3 + 2x^2 + 2x$                 |
| 3              | $\mathbf{2}$   | 3              | 5              | 3.3.c.g.m             | $y^2 + x^7 + 2x^5 + x^4 + x^3 + x^2 + 2$                   |
| 3              | 3              | $\mathbf{2}$   | $\overline{4}$ | 2.3.c.d               | $y^2 + 2x^6 + 2x^4 + x^3 + x + 2$                          |
| $\,3$          | 3              | $\overline{2}$ | $\overline{4}$ | 2.3.c.g.              | $y^2 + 2x^6 + 2x^5 + x^4 + x^3 + x^2 + 2x + 2$             |
| $\overline{4}$ | $\mathbf{2}$   | $\mathbf{2}$   | 3              | 2.4.ab.e              | $y^2 + xy + x^5 + x$                                       |
| $\overline{4}$ | $\mathbf{2}$   | $\overline{2}$ | 3              | 2.4.b.e               | $y^2 + xy + x^5 + ax^2 + x$                                |
| $\overline{4}$ | 3              | $\mathbf{2}$   | $\overline{4}$ | 2.4.d <sub>h</sub>    | $y^{2} + (x^{3} + x + 1)y + ax^{5} + ax^{4} + ax^{3} + ax$ |

<span id="page-14-1"></span>TABLE 4. Purely geometric extensions with  $q_F > 2$  and  $g_F > 1$ .

| $_{d}$         | $g_F$          | $g_{F}$        | J(C)                     | F  |
|----------------|----------------|----------------|--------------------------|--|
| 3              | $\overline{2}$ | 4              | $2.2 \text{.ac.e.}$      | $y^2 + y + x^5 + x^4 + 1$                                      |
| 3              | $\overline{2}$ | $\overline{4}$ | 2.2.b.b                  | $y^{2} + (x^{3} + x + 1)y + x^{6} + x^{3} + x^{2} + x$         |
| 3              | $\overline{2}$ | 6              | 2.2.a.c                  | $y^2 + y + x^5 + x^4 + x^3$                                    |
| 3              | $\mathbf{2}$   | 6              | 2.2.b.c                  | $y^2 + xy + x^5 + x^3 + x^2 + x$                               |
| 3              | $\overline{2}$ | 6              | 2.2.b.d                  | $y^{2} + (x^{3} + x + 1)y + x^{6} + x^{5} + x^{4} + x^{2}$     |
| 3              | 3              | $\overline{7}$ | $3.2.a-b-a$              | $y^4 + (x^3 + 1)y + x^4$                                       |
| 3              | 3              | $\overline{7}$ | $3.2.a_b_d$              | $y^3 + x^2y^2 + x^3y + x^4 + x^3 + x$                          |
| 3              | 3              | $\overline{7}$ | 3.2.b.b.b                | $y^3 + xy^2 + (x^3 + 1)y + x^4$                                |
| 3              | 3              | $\overline{7}$ | 3.2.b.b.e                | $y^3 + (x^2 + x)y^2 + y + x^3$                                 |
| 3              | 3              | $\overline{7}$ | $3.2.b$ <sub>-C-</sub> b | $xy^3 + xy^2 + y + x^3$  |
| 3              | 3              | $\overline{7}$ | 3.2.b.c.e                | $y^4 + xy^2 + y + x^4$   |
| 3              | 3              | $\overline{7}$ | 3.2.b.e.e                | $y^3 + x^2y^2 + xy + x^4 + x$                                  |
| 3              | $\overline{4}$ | 10             | $4.2.d.f_k_s$            | $x^{2}y^{3} + (x^{4} + x^{2} + 1)y + x^{4} + x^{2} + x + 1$    |
| 3              | $\overline{4}$ | 10             | 4.2.e. j. q. z           | $xy^{3} + (x^{2} + x + 1)y^{2} + (x^{4} + x)y + x^{5} + x^{4}$ |
| $\overline{4}$ | $\overline{2}$ | 5              | $2.2ab$ <sub>-C</sub>    | $y^2 + xy + x^5 + x^3 + x$                                     |
| 5              | $\overline{2}$ | 6              | 2.2.a.a.                 | $y^2 + y + x^5$  |
| $\bf 5$        | $\overline{2}$ | 6              | 2.2.b.c                  | $y^2 + xy + x^5 + x^3 + x^2 + x$                               |
| $\bf 5$        | $\overline{2}$ | 6              | 2.2.c.e                  | $y^2 + y + x^5 + x^4$  |
| $\overline{7}$ | $\overline{2}$ | 8              | 2.2.c.d                  | $y^{2} + (x^{2} + x + 1)y + x^{5} + x^{4} + x^{2} + x$         |

<span id="page-14-2"></span>TABLE 5. Cyclic purely geometric extensions with  $q_F = 2$ ,  $g_F > 1$ ,  $d > 2$ . Conjecture [1.5](#page-2-0) asserts that no noncyclic extensions occur.

16 KIRAN S. KEDLAYA

| $g_F$          | $g_{F'}$            | J(C)                          | $\boldsymbol{F}$  |
|----------------|---------------------|-------------------------------|---|
| $\overline{2}$ | 3                   | $2.2ab$ <sub>-c</sub>         | $y^2 + xy + x^5 + x^3 + x$  |
| $\overline{2}$ | 3                   | 2.2.b.c                       | $y^2 + xy + x^5 + x^3 + x^2 + x$  |
| $\overline{2}$ | $\overline{4}$      | $2.2.a_a$                     | $y^2 + y + x^5$   |
| $\overline{2}$ | $\overline{4}$      | 2.2.a.c                       | $y^2 + y + x^5 + x^4 + x^3$   |
| $\overline{2}$ | $\overline{4}$      | 2.2.b.b                       | $y^2 + (x^3 + x + 1)y + x^6 + x^3 + x^2 + x$  |
| $\overline{2}$ | 5                   | 2.2.b.d                       | $y^2 + (x^3 + x + 1)y + x^6 + x^5 + x^4 + x^2$  |
| $\overline{2}$ | 5                   | 2.2.c.e                       | $y^2 + y + x^5 + x^4$   |
| 3              | $\overline{5}$      | $3.2$ .ad_ $g$ _ai            | $y^2 + (x^4 + x^2 + 1)y + x^8 + x + 1$  |
| 3              | $\rm 5$             | 3.2.a b.a.c                   | $xy^3 + (x^2 + x)y^2 + y + x^4$   |
| 3              | 5                   | $3.2$ .ab $-a$ <sub>-</sub> c |   |
| 3              | 5                   | $3.2$ .ab $-c$ .ac            | $\begin{array}{l} -y^3 + x^2y^2 + (x^2 + 1)y + x^4 \\ y^2 + xy + x^7 + x^5 + x \end{array}$                     |
| 3              | 5                   | 3.2.a.a.f                     | $xy^3 + y + x^3$  |
| 3              | 5                   | 3.2.a.c.ab                    | $y^2 + (x^4 + x^2 + x + 1)y + x^6 + x^5 + x^2 + 1$  |
| 3              | 5                   | 3.2.a.c.b                     | $y^2 + (x^4 + x^2 + x + 1)y + x^8 + x^6 + x^5 + x^4$  |
| 3              | 5                   | $3.2.b$ <sub>-C-C</sub>       | $y^2 + xy + x^7 + x^5 + x^2 + x$  |
| 3              | 5                   | 3.2.b.c.e                     | $y^2 + (x^4 + x^2)y + x^2 + x$  |
| 3              | 6                   | 3.2.b.d.c                     | $y^3 + x^2y^2 + x^2y + x^4 + x^3 + x^2 + x$   |
| 3              | 6                   | 3.2.b.d.e                     | $xy^{3} + (x+1)y^{2} + x^{4} + x^{3} + x$   |
| 3              | 6                   | 3.2.b.e.d                     | $y^3 + x^2y^2 + (x^3 + x^2)y + x^4 + x$   |
| 3              | 6                   | 3.2.c.d.d                     | $(x+1)y^{3}+y+x^{3}$  |
| $\overline{4}$ | $\overline{7}$      | $4.2.a_c-ab_c$                | $x^3y^3 + (x^3 + x^2)y + x^6 + x^3 + 1$   |
| $\overline{4}$ | $\scriptstyle\rm 7$ | $4.2.a.c(ab-g)$               | $(x^{2} + 1)y^{4} + (x^{3} + x^{2} + x + 1)y^{3} + (x^{5} + x^{4})y + x^{6} + x^{3} + x^{2}$                    |
| $\overline{4}$ | $\overline{7}$      | 4.2.a.c.b.c                   | $x^{2}y^{4} + (x^{3} + 1)y^{2} + (x^{3} + x^{2} + x + 1)y + x^{6} + x^{5} + x^{3} + x^{2}$                      |
| 4              | $\overline{7}$      | $4.2.a_c.d_c$                 | $(x^{2} + x + 1)y^{4} + (x^{3} + x^{2})y^{3} + (x^{4} + x^{3} + 1)y^{2} + (x^{4} + x^{3} + x^{2})y +$           |
|                |                     |                               | $x^5 + x^4 + x^3 + x$   |
| $\overline{4}$ | $\overline{7}$      | 4.2.a.d.b.f                   | $x^3y^3 + (x^3 + x^2)y + x^6 + x^5 + 1$   |
| $\overline{4}$ | $\overline{7}$      | 4.2.a.d.b.h                   | $(x^{2} + x + 1)y^{4} + x^{3}y^{3} + (x^{4} + x^{2} + 1)y^{2} + x^{5} + x^{3} + x$                              |
| $\overline{4}$ | 7                   | $4.2.b_b_c_f$                 | $(x+1)y^{3} + (x^{2}+x)y^{2} + (x^{3}+x)y + x^{5}$  |
| $\overline{4}$ | 7                   | $4.2.b_c.a_a$                 | $y^2 + x^2y + x^9 + x^7 + x + 1$  |
| $\overline{4}$ | $\scriptstyle{7}$   | 4.2.c.e.h.k                   | $y^2 + (x^3 + x + 1)y + x^9 + x^7$  |
| $\overline{4}$ | 8                   | 4.2.d.i.o.x                   | $\frac{y}{(x+1)y^3 + (x^3 + x^2 + 1)y^2 + xy + x^4}$  |
| 5              | 9                   | $5.2$ .ab $-d$ .b $-$ b $-$ j | $(x^4+x^3+x^2)y^4+(x^5+x^3+x)y^3+(x^3+1)y^2+(x^7+x+1)y+x^7+x^4+x+1$   |
| 5              | 9                   | 5.2.b.c.e.i.i                 | $y^2 + x^3y + x^{11} + x^9 + x^5 + x^3 + x^2 + x^3$   |
| 5              | 9                   | $5.2.b_c.e_i$                 | $y^4 + (x^4 + x^2)y^2 + (x^4 + x^2 + 1)y + x^8 + x^6 + x^4 + x$   |
| 5              | 9                   | 5.2.b.f.f.p.l                 | $(x^{4} + x^{3} + x^{2})y^{4} + (x^{5} + x^{3} + x^{2})y^{3} + (x^{6} + x^{3} + x^{2} + x + 1)y^{2} + (x^{7} +$ |
|                |                     |                               | $x^5 + x^4 + x^3 + 1$<br>y + $x^5 + x^4 + x^3 + x^2 + x + 1$  |
| 5              | 9                   | 5.2.b.f.f.p.p                 | $y^4 + x^2y^3 + (x^4 + x^3 + x)y^2 + (x^5 + 1)y + x^3 + x^2 + x + 1$  |
| 5              | 9                   | 5.2.c.e.f.k.o                 | $y^2 + (x^3 + x + 1)y + x^{12} + x^{11} + x^{10} + x^7 + x^5 + x^3$   |
| 5              | 9                   | 5.2.c.f.i.n.r                 | $y^4 + (x^2+x)y^3 + (x^4+x^3+x^2+1)y^2 + (x^6+x^5+x^4+1)y+x^7+x^6+x+1$  |
| 5              | 9                   | 5.2.c.f.i.p.t                 | $(x^{4} + x^{2} + x)y^{4} + (x^{4} + x^{3} + x + 1)y^{3} + (x^{6} + x^{2})y^{2} + (x^{6} + x^{3} + x^{2} +$     |
|                |                     |                               | $(x)y + x^6 + x^5 + 1$  |
| 5              | 9                   | 5.2.c.f.i.p.v                 | $(x^{2} + x + 1)y^{6} + xy^{5} + (x^{4} + x)y^{4} + (x^{5} + x^{4} + x^{3} + x^{2} + x + 1)y^{3} +$             |
|                |                     |                               | $(x^{5}+x^{3}+1)y^{2}+(x^{6}+x^{4}+x^{2})y+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x$                         |
| 5              | 9                   | 5.2.c.g.j.q.u                 | $y^4 + y^3 + (x^4 + x^3 + x^2)y^2 + (x^3 + x^2 + 1)y + x^6 + 1$   |
| 5              | 9                   | 5.2.d.h.n.z.b!                | $y^{2} + (x^{6} + x^{5} + x^{4} + x^{3} + x^{2} + x + 1)y + x^{10} + x^{6} + x^{4} + x^{3}$                     |
| 5              | 9                   | 5.2.d_i_q_bc_bs               | $y^4 + (x^4 + x^2)y^2 + (x^4 + x^2 + 1)y + x^6 + x^5$   |
| 6              | 11                  | $6.2.c.h.k.z.bd_cg$           | $x^2y^5 + (x^3 + x)y^4 + x^4y^3 + (x^5 + x^4 + x^3 + x^2 + x + 1)y^2 + (x^6 + x^3 +$                            |
|                |                     |                               | $(x^2)y + x^7 + x^3 + x + 1$  |
| 6              | 11                  | $6.2.d.j.t.bn_cl.du$          | $(x^{2} + x + 1)y^{4} + (x^{3} + x + 1)y^{3} + (x^{4} + x^{2} + 1)y^{2} + (x^{5} + x^{4} + 1)y +$               |
|                |                     |                               | $x^5 + x^4 + x^3 + x$   |
| $\overline{7}$ | 13                  | (6, 18, 12, 18, 6, 60, 174)   | $y^4 + (x^6 + x^4 + x^3 + x^2 + 1)y^2 + (x^6 + x^4 + x^3 + x^2)y + x^{10} + x^9 + x^7 + x^6$                    |

<span id="page-15-0"></span>TABLE 6. Purely geometric extensions with  $q_F = 2$ ,  $g_F > 1$ ,  $d = 2$ . Completeness of the list is confirmed above the below line and conjectural below it (Conjecture [1.5\)](#page-2-0). For  $g_F = 7$ ,  $J(C)$  does not appear in LMFDB, so we list  $J(C)(\mathbb{F}_{2^i})$  for  $i = 1, \ldots, 7$ .



THE RELATIVE CLASS NUMBER ONE PROBLEM FOR FUNCTION FIELDS,  $\rm I1$ 

<span id="page-16-0"></span>TABLE 7. Candidates for A and  $J(C)$  in Theorem [1.3\(](#page-1-1)b) for  $d =$ 2,  $d = 3$ , and  $d > 3$  respectively;  $\star$  means A is not principally polarizable (Remark [10.4\)](#page-12-6). For  $g = 7$ ,  $J(C)$  does not appear in LMFDB, so we list  $J(C)(\mathbb{F}_{2^i})$  for  $i = 1, \ldots, 7$ .