TERNARY AND QUATERNARY CURVES OF SMALL FIXED GENUS AND GONALITY WITH MANY RATIONAL POINTS

XANDER FABER AND JON GRANTHAM

ABSTRACT. We extend the computations from our previous paper [5] to determine the maximum number of rational points on a curve over \mathbb{F}_3 and \mathbb{F}_4 with fixed gonality and small genus. We find, for example, that there is no curve of genus 5 and gonality 6 over a finite field. We propose two conjectures based on our data. First, an optimal curve of genus g has gonality at most $\lfloor \frac{g+3}{2} \rfloor$. Second, an optimal curve of gonality γ and large genus over \mathbb{F}_q has $\gamma(q+1)$ rational points.

1. INTRODUCTION

Let C be a smooth proper geometrically connected scheme of dimension 1 over a finite field — a "curve", for brevity. There are two well-known upper bounds for the number of rational points on C. First, there is the bound of André Weil that arises in the study of the zeta function:

 $#C(\mathbb{F}_q) \le q + 1 + 2g\sqrt{q},$

where g is the genus of C. Define the quantity $N_q(g)$ to be the maximum number of rational points on a curve of genus g over \mathbb{F}_q . Many techniques have been developed to bound $N_q(g)$ and to produce examples of curves with large numbers of rational points; see [26], [17], or [23]. Van der Geer and van der Vlugt [25] compiled the first comprehensive table of maximal values for small genus and field size, which eventually evolved into manypoints.org. Table 1 gives the first few values of $N_q(g)$.

| g | $N_2(g)$ | $N_3(g)$ | $N_4(g)$ |
|---|----------|----------|----------|
| 0 | 3 | 4 | 5 |
| 1 | 5 | 7 | 9 |
| 2 | 6 | 8 | 10 |
| 3 | 7 | 10 | 14 |
| 4 | 8 | 12 | 15 |
| 5 | 9 | 13 | 17 |

TABLE 1. Maximum number of rational points on a curves of genus g over \mathbb{F}_q

Second, if $f: C \to \mathbb{P}^1$ is a morphism defined over \mathbb{F}_q , then every rational point of C must map to a rational point of \mathbb{P}^1 . Consequently, we get the bound $\#C(\mathbb{F}_q) \leq (\deg f)(q+1)$. This bound is optimized when we take f to have minimum degree over all such morphisms we call this degree the **gonality** of C and write γ for it. This gives rise to the "gonality-point bound" for C:

$$#C(\mathbb{F}_q) \le \gamma(q+1). \tag{1.1}$$

We define the quantity $N_q(g, \gamma)$ to be the supremum of the number of rational points on a curve C of genus g and gonality γ . (Many pairs (g, γ) exist for which there is no such curve, so we use the supremum.)

Remark 1.1. One might ask why we do not consider the maximum number of rational points on a curve over \mathbb{F}_q of fixed gonality, while letting the genus vary freely. We expect this quantity to be $\gamma(q+1)$ for sufficiently large genus; see Conjecture 1.4.

In our first paper [5], we laid out a plan for computing the maximum number of rational points on a curve C over \mathbb{F}_q with small genus and fixed gonality, and we executed this program for curves over the binary field with genus at most 5. In the present paper, we extend those computations to the fields \mathbb{F}_3 and \mathbb{F}_4 . For many cases where curves of a given genus and gonality exist, this was fairly straightforward: we either dug through the literature to find examples of curves that met certain bounds we had already exhibited, or else we ran general search code that we wrote for our first paper. But in the cases where we prove non-existence results, the increased size of the relevant search spaces requires improved algorithms and code development.

Table 2 summarizes the quantities $N_q(g, \gamma)$ for $q \leq 4$ and $g \leq 5$. The entries in the column for q = 2 were determined in [5], while the entries for q = 3, 4 are justified in the present paper. Recall that $N_q(g, \gamma) = -\infty$ if there is no curve of genus g and gonality γ . The gonality of a curve over a finite field is at most one more than the genus [5, Prop. 2.1], so we omit entries in the table beyond g + 1.

| g | γ | $N_2(g,\gamma)$ | $N_3(g,\gamma)$ | $N_4(g,\gamma)$ |
|---|----------|-----------------|-----------------|-----------------|
| 0 | 1 | 3 | 4 | 5 |
| 1 | 2 | 5 | 7 | 9 |
| 2 | 2 | 6 | 8 | 10 |
| 3 | 2 | 6 | 8 | 10 |
| | 3 | 7 | 10 | 14 |
| | 4 | 0 | 0 | 0 |
| 4 | 2 | 6 | 8 | 10 |
| | 3 | 8 | 12 | 15 |
| | 4 | 5 | 10 | 13 |
| | 5 | 0 | 0 | $-\infty$ |
| 5 | 2 | 6 | 8 | 10 |
| | 3 | 8 | 12 | 15 |
| | 4 | 9 | 13 | 17 |
| | 5 | 3 | 4 | 5 |
| | 6 | $-\infty$ | $-\infty$ | $-\infty$ |

TABLE 2. Supremum of the number of rational points on a binary, ternary, or quaternary curve with fixed genus and gonality.

The final row of Table 2 suggests a pattern, which we are able to complete: **Theorem 1.2.** There is no curve of genus 5 and gonality 6 over a finite field. *Proof.* Suppose there were a curve C of genus 5 and gonality 6 over \mathbb{F}_q . Table 2 shows that $q \geq 5$. Weil's lower bound yields

$$#C(\mathbb{F}_{q^3}) \ge q^3 + 1 - 10q^{3/2} = (q^{3/2} - 5)^2 - 24 \ge 14,$$

so that $C(\mathbb{F}_{q^3}) \neq \emptyset$. The presence of a cubic point implies that C has gonality at most 5 by [5, Cor. 2.5].

Serre introduced a powerful technique for showing that curves over finite fields with certain numerical properties cannot exist [22, II - The Case q = 2]. Lauter transformed this technique into a proper algorithm in the self-contained article [13]; see also [12] and [23, §VII.2]. The idea is to efficiently list all real Weil polynomials (essentially zeta functions) that could belong to a curve with given genus and number of rational points (perhaps over extension fields). Each of these is the real Weil polynomial of an isogeny class of abelian varieties, and one attempts to show by arithmetic/geometric methods that there is no Jacobian variety in this class. For example, upon applying Lauter's algorithm to the case of curves of genus 5 and gonality 6 over \mathbb{F}_4 , one finds a single real Weil polynomial:

$$(T-4)^2(T+1)^3$$
.

None of the methods developed in [8, 9, 14] seem able to rule out the possibility of a Jacobian in the associated isogeny class (which would yield an alternate proof of Theorem 1.2). We will return to this line of thought in the forthcoming paper [6].

An **optimal curve** is a curve of genus g over \mathbb{F}_q with $N_q(g)$ rational points. One expects the geometry of these to be rather special because their arithmetic sets them apart. For example, Rigato showed that for small-genus curves over \mathbb{F}_2 , there are very few isomorphism classes of optimal curves [18]. We propose a conjecture on the gonality of optimal curves:

Conjecture 1.3 (Optimal Gonality). Let C be an optimal curve over \mathbb{F}_q of genus g. Then C has gonality at most $\left|\frac{g+3}{2}\right|$.

Note that $\lfloor \frac{g+3}{2} \rfloor$ is the maximum geometric gonality of a curve $C_{/\mathbb{F}_q}$ of genus g — i.e., among morphisms $C \to \mathbb{P}^1$ defined over the algebraic closure $\overline{\mathbb{F}}_q$, there exists one of degree at most $\lfloor \frac{g+3}{2} \rfloor$.

Our Optimal Gonality Conjecture holds for q = 2, 3, 4 and $g \leq 5$ by Tables 1 and 2. Rigato's work shows that it holds for q = 2 and g = 6 as well; there are exactly two isomorphism classes of optimal curves over \mathbb{F}_2 of genus 6, and both of them have gonality 4. In the appendix to [5], additional examples of optimal curves of genus 7, 8, and 9 over \mathbb{F}_2 are given, and in each case the gonality is strictly smaller than $\lfloor \frac{g+3}{2} \rfloor$.

In [5], we posed a conjecture on the maximum number of rational points on a curve over \mathbb{F}_2 of gonality γ as the genus tends to infinity. Based on our new data, we feel emboldened to extend the statement to all finite fields:

Conjecture 1.4. Fix a prime power q and an integer $\gamma \geq 2$. For g sufficiently large, $N_q(g,\gamma) = \gamma(q+1)$.

In §2, we address the elliptic and hyperelliptic entries in Table 2. We also prove Conjecture 1.4 when $\gamma = 2$; see Theorem 2.3. We quickly handle curves of genus 3 in §3.

In order to describe all curves of genus 4 or 5, we find ourselves in need of a list of all cubic forms (genus 4) or quadratic forms (genus 5) modulo the action of a particular orthogonal

group O(Q). Unfortunately, computing the orthogonal group O(Q) by a naive search as we did in [5] turns out to be computationally untenable for the needs of the present paper. We sketch a more efficient approach in §4. The idea is to view an element $g \in O(Q)$ as a matrix of indeterminates and then observe that equating coefficients in the relation Q(g(x)) = Q(x) gives rise to a very structured system of quadratic equations in these indeterminates.

We treat curves of genus 4 in §5. The majority of our work goes toward proving that there is no curve of genus 4 and gonality 5 over \mathbb{F}_4 . That computation breaks into two parts: the first is a large search implemented in C, while the second uses Sage to identify smooth curves among the output of the first step. Finally, we address curves of genus 5 in §6. Here the bulk of our effort goes toward determining the maximum number of points on a curve with gonality 5, and toward the non-existence of curves with gonality 6. Viewed from a distance, these computations were quite similar to those performed in [5] in order to address curves over \mathbb{F}_2 . However, since the search spaces are so much larger over \mathbb{F}_3 and \mathbb{F}_4 , it was necessary to improve our algorithms and our code. Despite these efforts, our computations still required weeks of compute time on a multi-core machine. We outline these algorithmic changes and present our findings in §6.3.

We close with a discussion about the software used and created for this project. For simple verification of the genus or number of rational points of the smooth model of an algebraic curve, we used Magma [1]. For ease of development and the ability to optimize via analysis of the source code, we used Sage [24]. Our code is Python3 compatible, and hence will run under Sage 9.1 as well. In order to launch many Sage jobs asynchronously, we wrote a flexible Python3 script called sage_launcher.py that may be of use to other researchers. Some of our code for genus-4 computations was written in C and depends on the FLINT library [7]. All of our source code can be found at https://github.com/RationalPoint/gonality.

Throughout this article, the field \mathbb{F}_4 will be represented as $\mathbb{F}_2[t]/(t^2+t+1)$.

2. Elliptic and Hyperelliptic Curves

Let us begin with curves of genus 1. A curve $C_{/\mathbb{F}_q}$ of genus 1 necessarily has a rational point by the Weil bound: $\#C(\mathbb{F}_q) \ge q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0$. In particular, C is an elliptic curve; it is given by a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in \mathbb{F}_q$; and C has gonality 2. We conclude that $N_q(1, 2) = N_q(1)$ for all q. Now we are in a position to quote a result of Serre:

Theorem 2.1 ([23, Thm. 6.3]). Set $m = \lfloor 2\sqrt{q} \rfloor$. Then $N_q(1) = q + 1 + m$ except when $q = p^a$ for a odd, $e \geq 5$, $m \equiv 0 \pmod{p}$, in which case $N_q(1) = q + m$.

Corollary 2.2. $N_3(1,2) = 7$ and $N_4(1,2) = 9$.

Our next task is to look at hyperelliptic curves of genus > 1; see [15, Prop. 7.4.24] for the geometry of hyperelliptic equations. We begin by constructing two families of optimal hyperelliptic curves parameterized by g and q: one for odd q and one for even q.

If q is odd and $g > \frac{q^2-2}{2}$, then we can consider the curve

$$C_{/\mathbb{F}_q}: y^2 = x^{2g+2-q^2}(x^q - x)^q + 1.$$

In order to see that $y^2 = P(x)$ is smooth, one checks that gcd(P, P') = 1. In our case, P' vanishes only at \mathbb{F}_q -rational points, while P does not vanish there. Therefore, C is a

hyperelliptic curve of genus g and has 2(q+1) \mathbb{F}_q -rational points (including the two at infinity). This is optimal: the gonality-point bound (1.1) shows that $N_q(g,2) \leq 2(q+1)$.

If instead q is even and $g \ge q - 1$, we take

$$C_{/\mathbb{F}_q}: y^2 + ((x^q + x)x^{g+1-q} + 1)y = (x^q + x)^2.$$

The criterion for a hyperelliptic equation $y^2 + Q(x)y = P(x)$ in characteristic 2 to define a smooth curve is expressed as $gcd(Q, (Q')^2P + (P')^2) = 1$. One verifies that this holds for our curve by considering the cases g odd and g even separately. Then C has genus g and 2(q+1) rational points (including the two at infinity).

Combining these two constructions, we immediately obtain

Theorem 2.3. Fix a prime power q. Then $N_q(g, 2) = 2(q+1)$ for $g \gg 0$.

Let us turn to the case q = 3 more specifically. The first construction yields a smooth hyperelliptic curve of genus g with 8 rational points when $g \ge 4$. The curve $C_{/\mathbb{F}_3} : y^2 = x^{2g-1}(x^3-x)+1$ is smooth of genus g whenever $g \not\equiv 1 \pmod{6}$, and it has 8 rational points. In particular, this applies when g = 2, 3, and we have proved

Theorem 2.4. $N_3(g, 2) = 8$ for $g \ge 2$.

Finally, we treat the case q = 4. The second construction above gives a smooth hyperelliptic curve with 10 rational points for each genus $g \ge 3$.

For q = 4, the construction above shows that $N_4(g, 2) = 10$ for $g \ge 3$. To deal with genus 2, consider the curve $y^2 + (x^3 + t + 1)y = x^5 + x^2$. It is smooth with 10 rational points (including the two at infinity). Thus,

Theorem 2.5. $N_4(g, 2) = 10$ for $g \ge 2$.

3. Curves of Genus 3

We have already dealt with hyperelliptic curves in the preceding section, so all that remains is gonality 3 and gonality 4 [5, Prop. 2.1]. A non-hyperelliptic curve of genus 3 can be realized as a smooth plane quartic via the canonical embedding. All of our examples will be of this sort.

Theorem 3.1. $N_3(3,3) = 10$.

Proof. Serre [21] showed that $N_3(3) \leq 10$, so we immediately have $N_3(3,3) \leq 10$. Serre also exhibited the smooth plane quartic

$$C_{/\mathbb{F}_3}: y^3 z - y z^3 = x^4 - x^2 z^2,$$

which has 10 rational points. A non-hyperelliptic curve of genus 3 with a rational point has gonality 3 [5, Cor. 2.3], so $N_3(3,3) \ge 10$.

Theorem 3.2. $N_4(3,3) = 14$.

Proof. Ihara's explicit bound shows that $N_4(3) \leq 14$ [11, §2], and Serre exhibited the smooth plane quartic

$$C_{/\mathbb{F}_4} : (x+y+z)^4 + (xy+xz+yz)^2 + xyz(x+y+z) = 0,$$

which has 14 rational points. A non-hyperelliptic curve of genus 3 with a rational point has gonality 3 [5, Cor. 2.3], so we conclude that $N_4(3,3) = 14$.

Theorem 3.3. $N_3(3,4) = 0$ and $N_4(3,4) = 0$.

Proof. A curve of genus g with a rational point has gonality at most g [5, Prop. 2.1]; hence, $N_g(3,4) \leq 0$. Howe, Lauter, and Top [10] produced the following examples of pointless smooth plane quartics:

$$C_{/\mathbb{F}_3} \colon x^4 + xyz^2 + y^4 + y^3z - yz^3 + z^4 = 0$$

$$C_{/\mathbb{F}_4} \colon (x^2 + xz)^2 + t(x^2 + xz)(y^2 + yz) + (y^2 + yz)^2 + t^2z^4 = 0$$

A non-hyperelliptic curve of genus 3 with no rational point has gonality 4 [5, Cor. 2.3], and the theorem follows. $\hfill \Box$

4. Interlude on the computation of orthogonal groups

Fix a finite field \mathbb{F}_q , and let

$$Q(x) = \sum_{1 \le i \le j \le n} c_{i,j} x_i x_j$$

be a quadratic form in n variables, where $x = (x_1, \ldots, x_n)$ and $c_{i,j} \in \mathbb{F}_q$ are not all zero. The **orthogonal group** of Q is defined to be

$$O(Q) = \{g \in GL_n(\mathbb{F}_q) : Q(g(x)) = Q(x)\}.$$

We wish to write down all of the matrices in O(Q) in an efficient manner.

Let $g = (g_{i,j})$ be an $n \times n$ matrix with undetermined coefficients, and let us impose the equality Q(g(x)) = Q(x). Equating coefficients of the quadratic monomials in the x_i 's on both sides gives rise to a system of $\frac{n^2+n}{2}$ quadratic equations in the $g_{i,j}$'s:

(a) Equating the coefficients of the diagonal term x_i^2 gives the relation

$$Q(g_{1i},\ldots,g_{ni})=c_{i,i}.$$

(b) Write $\langle x, y \rangle = Q(x+y) - Q(x) - Q(y)$ for the associated bilinear form. The relation arising from the coefficients of the term $x_i x_j$ is given by

$$\langle g_{\bullet i}, g_{\bullet j} \rangle = c_{i,j}.$$

In particular, it depends only on g_{rs} with $s \in \{i, j\}$.

Any invertible matrix $g = (g_{i,j})$ that satisfies properties (a) and (b) will be an element of the orthogonal group O(Q), and every element of O(Q) is obtained in this way. It follows that the output of Algorithm 1 is correct.

Example 4.1. Let $Q(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4 \in \mathbb{F}_q[x_1, x_2, x_3, x_4]$. If $g = (g_{i,j})$ is a 4×4 matrix of indeterminates, then the equation $Q(g(x_1, x_2, x_3, x_4)) = Q(x_1, x_2, x_3, x_4)$ gives rise

to the following system of 10 quadratic equations:

$$\begin{aligned} x_1^2 &: g_{11}g_{21} + g_{31}g_{41} = 0 \\ x_1x_2 &: g_{12}g_{21} + g_{11}g_{22} + g_{32}g_{41} + g_{31}g_{42} = 1 \\ x_1x_3 &: g_{13}g_{21} + g_{11}g_{23} + g_{33}g_{41} + g_{31}g_{43} = 0 \\ x_1x_4 &: g_{14}g_{21} + g_{11}g_{24} + g_{34}g_{41} + g_{31}g_{44} = 0 \\ x_2^2 &: g_{12}g_{22} + g_{32}g_{42} = 0 \\ x_2x_3 &: g_{13}g_{22} + g_{12}g_{23} + g_{33}g_{42} + g_{32}g_{43} = 0 \\ x_2x_4 &: g_{14}g_{22} + g_{12}g_{24} + g_{34}g_{42} + g_{32}g_{44} = 0 \\ x_3^2 &: g_{13}g_{23} + g_{33}g_{43} = 0 \\ x_3x_4 &: g_{14}g_{23} + g_{13}g_{24} + g_{34}g_{43} + g_{33}g_{44} = 1 \\ x_4^2 &: g_{14}g_{24} + g_{34}g_{44} = 0. \end{aligned}$$

Algorithm 1 — Compute the elements of the orthogonal group for a quadratic form $Q = \sum c_{i,j} x_i x_j$ over \mathbb{F}_q . $1 \le i \le j \le n$ 1: initialize an empty list L2: for $1 \leq i \leq n$ do compute the set S_i of solutions to the equation $Q(x) = c_{i,i}$ 3: 4: end for 5: for $(g_{11}, \ldots, g_{n1}) \in S_1$ do for $(g_{12}, \ldots, g_{n2}) \in S_2$ do 6: if $\langle g_{\bullet 1}, g_{\bullet 2} \rangle \neq c_{1,2}$ then continue 7: 8: for $(g_{13}, \ldots, g_{n3}) \in S_3$ do if $\langle g_{\bullet 1}, g_{\bullet 3} \rangle \neq c_{1,3}$ then continue 9: if $\langle g_{\bullet 2}, g_{\bullet 3} \rangle \neq c_{2,3}$ then continue 10: for $(g_{1n},\ldots,g_{nn}) \in S_n$ do 11: 12:if $\langle g_{\bullet i}, g_{\bullet n} \rangle \neq c_{i,n}$ for some i < n then continue if $g = (g_{i,j})$ is invertible then append g to the list L 13:end for 14: end for 15:end for 16:17: end for 18: return L

Algorithm 1 begins with the precomputation of the sets $S_i \subset \mathbb{F}_q^n$; for example, one can simply loop over the elements of \mathbb{F}_q^n to find solutions. By the Weil conjectures, one expects $\#S_i \approx q^{n-1}$, so the overall search space has size approximately $q^{n(n-1)}$. However, the checks involving the associated bilinear form yield a substantial cutdown of the set of matrices to test for invertibility. Example 4.2. Consider the quadratic form $Q = x_1x_2 + x_3^2 \in \mathbb{F}_2[x_1, x_2, x_3, x_4, x_5]$. Computing O(Q) via a naive loop over all 5×5 matrices with coefficients in \mathbb{F}_2 takes approximately 54 minutes in Sage on a 2.6GHz Intel Core i5 with 16GB RAM. If we instead apply Algorithm 1, we first precompute the sets S_i . Note that $S_1 = S_2 = S_4 = S_5$, and that $\#S_i = 16$ for all *i*. It follows that our search space has size $(2^4)^5$ instead of 2^{25} , and we only test around $2^{14.6}$ matrices for invertibility. Our Sage implementation produced O(Q) in less than a second.

Here is another practical improvement for computing some orthogonal groups. Suppose that Q is a quadratic form in $\mathbb{F}_q[x_1, \ldots, x_n]$, but there is m < n such that x_{m+1}, \ldots, x_n do not appear in any monomial with nonzero coefficient. Write $\mathbb{F}_q^n = U \oplus V$, where U is spanned by the first m standard basis vectors and V is spanned by the remaining n - m. Then Lemma B.11 of the arXiv edition of [5] implies $g \in O(Q)$ if and only if it has the form

$$g = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix},$$

where $A \in O(Q|_U)$, $B : U \to V$ is an arbitrary linear map, and $C \in GL(V)$. In particular, this means that we can perform the search in Algorithm 1 on a quadratic form in *m* variables and then build up the orthogonal group of Q.

Remark 4.3. How does one verify that Algorithm 1 has been implemented correctly? We provide strong evidence via two methods. First, we have several implementations, including a naive search over all matrices and the method from Appendix B.2 of the arXiv edition of [5]. These can be applied to quadratic forms in very low dimension over small finite fields $(q \leq 4)$ to vet the code. Second, we can verify that the cardinality of our output is correct because L.E. Dickson computed the order of O(Q) well over a century ago. See Chapters VII and VIII of [4].

5. Curves of Genus 4

Hyperelliptic curves of genus 4 were treated in Theorems 2.4 and 2.5. It remains to handle curves of gonality 3, 4, and 5 [5, Prop. 2.1]. We easily produce upper and lower bounds for curves over \mathbb{F}_3 , so we do these first. Afterward, we treat curves over \mathbb{F}_4 .

5.1. Ternary curves.

Theorem 5.1. $N_3(4,3) = 12$.

Proof. Using Oesterlé's method, Serre showed that $N_3(4) = 12$, which immediately implies that $N_3(4,3) \leq 12$. Using global class field theory, Niederreiter and Xing [16] found the following example of an affine plane curve whose smooth model has genus 4 and 12 rational points:

$$(y^{3} - y) = \frac{x^{3} - x}{(x^{2} + 1)^{2}}.$$

The rational function x gives a map to \mathbb{P}^1 of degree 3, and this curve would violate the gonality-point bound if it were hyperelliptic. Thus, $N_3(4,3) \ge 12$.

By Lemma 5.1 of [5], a curve of genus 4 and gonality 4 or 5 can be realized in $\mathbb{P}^3 = \mathbb{F}_3[x, y, z, w]$ as the intersection of a cubic surface and the quadric surface

$$V(Q): xy + z^2 + w^2 = 0,$$

and conversely, any smooth geometrically irreducible intersection of V(Q) with a cubic surface has genus 4 and gonality at least 4.

Theorem 5.2. $N_3(4,4) = 10$.

Proof. The surface $Q = xy + z^2 + w^2 = 0$ has 10 rational points on it, so we must have $N_3(4,4) \leq 10$. The cubic surface with equation

$$x^{2}y - xyz - y^{2}z + xz^{2} + x^{2}w + y^{2}w + xw^{2} - zw^{2} + w^{3} = 0,$$

passes through all 10 of those rational points, and its intersection with V(Q) is smooth and geometrically irreducible. Since this curve has a rational point, it must have gonality exactly 4 by [5, Cor. 2.4]. Therefore, $N_3(4, 4) \ge 10$.

Theorem 5.3. $N_3(4,5) = 0.$

Proof. A curve of genus g with a rational point has gonality at most g by [5, Prop. 2.1]. It follows that $N_3(4,5) \leq 0$. Consider the curve in $\mathbb{P}^3 = \text{Proj } \mathbb{F}_3[x, y, z, w]$ cut out by the following equations:

$$xy + z^{2} + w^{2} = 0$$

$$x^{3} + y^{3} + y^{2}z + x^{2}w + xyw - y^{2}w - yzw + z^{2}w = 0.$$

It is smooth and geometrically irreducible, hence of genus 4 and gonality at least 4. A direct search shows that it has no \mathbb{F}_9 -rational point, so it must have gonality 5 [5, Cor. 2.4].

Remark 5.4. Our practice has been to look in the literature for examples of the curves we need before turning to computer searches. Castryck and Tuitman seem to have given the first example of a curve with gonality 5 over \mathbb{F}_3 [2, p.15]. (The cited arXiv paper contains examples that were excised before publication as [3].) We opted to use our own example in the above proof because it has somewhat shorter defining polynomials.

5.2. Quaternary curves. A non-hyperelliptic curve of genus 4 over \mathbb{F}_4 can be realized in $\mathbb{P}^3 = \mathbb{F}_4[x, y, z, w]$ as the intersection of a cubic surface and one of the following quadric surfaces:

Gonality 3:
$$xy + z^2 = 0$$
;
Gonality 3: $xy + zw = 0$; or
Gonality 4 or 5: $xy + z^2 + tzw + w^2 = 0$.

See Lemma 5.1 of [5].

Theorem 5.5. $N_4(4,3) = 15$.

Proof. Serve showed that $N_4(4) = 15$, so it will suffice to find a curve of gonality 3 with 15 rational points. Consider the curve in \mathbb{P}^3 cut out by the equations

$$xy + z^{2} = 0$$
$$x^{3} + xyz + ty^{2}w + (t+1)yw^{2} + w^{3} = 0$$

It is smooth, hence of genus 4 and gonality 3 by the remarks at the beginning of this section. One verifies by direct search that it has 15 rational points. \Box

Lemma 5.6. $N_4(4,4) \le 13$.

Proof. Let C be a curve of genus 4 and gonality 4 over \mathbb{F}_4 , which we may realize as the intersection of $Q = xy + z^2 + tzw + w^2 = 0$ and a cubic surface in \mathbb{P}^3 . Serre showed that $N_4(4) = 15$, so in order to prove the lemma, we must rule out the possibility that a cubic surface meets V(Q) smoothly and passes through 14 or 15 rational points of V(Q). Note that V(Q) has 17 rational points.

The space of cubic surfaces has (projective) dimension 19. If F is a cubic form, the ideal generated by F and Q is not affected by replacing F with F + LQ for any linear form L. Consequently, by adding a suitable constant multiple of xQ, we may assume that F has no x^2y -term. Similarly, we may kill the xy^2 -, z^3 -, and w^3 -terms by adding suitable multiples of yQ, zQ, and wQ, respectively. In this way, we reduce the dimension of the space of cubic surfaces under consideration down to 15.

Let us now rule out the possibility of a curve of gonality 4 with 15 rational points. Insisting that a cubic surface pass through a particular rational point is a linear condition on the coefficients of the cubic's defining polynomial. For each choice of 15 points on V(Q) — of which there are $\binom{17}{15} = 136$ — we use linear algebra to find a basis for the space of cubic surfaces that vanish at all of the points. From a naive dimension-count, we expect the resulting space to have (projective) dimension 0, so there is a unique such cubic surface. In fact, this turns out to be the case: we executed this procedure in Sage and determined that none of the resulting 136 cubic surfaces meet the quadric surface V(Q) in a smooth curve. The resulting computation took under a minute on a single 2.6Ghz Intel Core i5 CPU.

A similar computation applied to the $\binom{17}{14} = 680$ choices of 14 rational points on V(Q) took approximately 4.5 minutes to verify that there is no curve of genus 4 and gonality 4 with 14 rational points.

Theorem 5.7. $N_4(4, 4) = 13$.

Proof. The upper bound we want is given by Lemma 5.6. For the lower bound, consider the smooth curve in $\mathbb{P}^3 = \operatorname{Proj} \mathbb{F}_4[x, y, z, w]$ that is cut out by the equations

$$xy + z^{2} + tzw + w^{2} = 0$$
$$y^{2}z + xz^{2} + x^{2}w + y^{2}w + yzw + z^{2}w + xw^{2} + yw^{2} = 0.$$

Direct search shows that it has 13 rational points. Thus, $N_4(4, 4) \ge 13$.

We spend the remainder of this section describing a computational proof of the following non-existence result:

Theorem 5.8. $N_4(4,5) = -\infty$.

Suppose that C is a curve of genus 4 over \mathbb{F}_4 with gonality 5. Then C can be realized in $\mathbb{P}^3 = \operatorname{Proj} \mathbb{F}_4[x, y, z, w]$ as the intersection of the quadric surface

$$Q = xy + z^2 + tzw + w^2 = 0$$

and a cubic surface by [5, Lem.5.1]. Corollary 2.4 of [5] asserts that such a curve satisfies $C(\mathbb{F}_{4^2}) = \emptyset$. Our proof has two main steps:

- Step 1. Loop over cubic surfaces and record those that do not pass through any quadratic point on V(Q).
- Step 2. Intersect each of the survivors from Step 1 with the quadric surface V(Q) and determine which, if any, are smooth and geometrically irreducible.

Naively, there are $(4^{20} - 1)/3 \approx 10^{11.5}$ cubic surfaces to examine, so we wrote a C-program to execute the search. The number of survivors was sufficiently small (65, 280) that we could do the various bits of commutative algebra for Step 2 in Sage. Ultimately, we uncovered no smooth canonical curve C of genus 4 with $C(\mathbb{F}_{4^2}) = \emptyset$, which proves the theorem.

Algorithm 2 gives a more detailed description of Step 1, which we now discuss and justify. Write $\vec{X} = (X_0, \ldots, X_{19})$ for the tuple of cubic monomials in $\mathbb{F}_4[x, y, z, w]$, relative to some fixed ordering. For any coefficient vector $\vec{c} \in \mathbb{F}_4^{20} \setminus \{0\}$, the dot product $\vec{c} \cdot \vec{X}$ is a cubic form, and conversely any cubic form can be represented by such a dot product.

Definition 5.9. Define the set $A \subset \mathbb{F}_4^{20}$ of coefficient vectors \vec{c} such that in the cubic form $\vec{c} \cdot \vec{X}$, the following are true:

- The entry corresponding to x^3 is 1;
- The entry corresponding to y^3 is nonzero;
- The entry corresponding to x^2y is 0;
- The entry corresponding to xy^2 is 0;
- The entry corresponding to z^3 is 0; and
- The entry corresponding to w^3 is 0.

We claim that if C is a curve of gonality 5, then it may be written as the intersection of the quadric surface V(Q) and a cubic surface V(F), where $F = \vec{c} \cdot \vec{X}$ for some $\vec{c} \in A$. Indeed, the point P = (1:0:0:0) lies on the quadric surface V(Q). As $C(\mathbb{F}_{4^2}) = \emptyset$, this point does not lie on C, and hence $F = \vec{c} \cdot \vec{X}$ does not vanish at P. That is, the x^3 -coefficient is nonzero. Since we are only interested in the vanishing locus of F, we may rescale \vec{c} if necessary so that the x^3 -coefficient of F is 1. A similar argument applied to the point (0, 1, 0, 0) shows that we may take the y^3 -coefficient to be nonzero. If the x^2y -coefficient is a, then we replace F with F - axQ to get another cubic with the same x^3 - and y^3 -coefficients, but with x^2y -coefficient equal to 0. The same trick applied to an appropriate multiple of yQ, zQ, and wQ kills the coefficients on xy^2, z^3 , and w^3 . Note that modifying F by a multiple of Q does not change its vanishing locus. This completes the justification of the claim.

There are 17 rational points on V(Q) and 272 quadratic non-rational points. It follows that the set of representatives computed in the first step of Algorithm 2 has cardinality $17 + \frac{272}{2} = 153$. Storing the evaluated monomial vectors allows us to compute dot products rather than cubic polynomial evaluations in the main loop. We have already discussed why it suffices to consider only coefficient vectors in A when looking for cubic surfaces that may contain a curve of gonality 5. The if-statement inside the main loop checks that V(F) passes through no quadratic point of V(Q); it suffices to check this for Galois-orbit representatives since F is defined over \mathbb{F}_4 . This completes the justification of Algorithm 2.

Our C-implementation of Algorithm 2 ran in 1.25 hours on a single 2.6Ghz Intel Core i5 with 16GB RAM, and it found 65, 280 cubic forms.

A few practical observations are in order:

Algorithm 2 — Compute a list of cubic forms $F \in \mathbb{F}_4[x, y, z, w]$ such that the variety $V(F) \cap V(Q)$ has no point over \mathbb{F}_{4^2} , and such that any curve of genus 4 and gonality 5 is isomorphic to one of these intersections

- 1: compute representatives for the $\operatorname{Gal}(\mathbb{F}_{4^2}/\mathbb{F}_4)$ -orbits in the set $V(Q)(\mathbb{F}_{4^2}) \subset \mathbb{P}^3$
- 2: for $P \in V(Q)(\mathbb{F}_{4^2})$ do
- 3: store the vector $\vec{v}_P = (X_0(P), \dots, X_{19}(P))$ of cubic monomials evaluated at P
- 4: end for
- 5: initialize an empty list L
- 6: for each coefficient vector $\vec{c} \in A$ as in Definition 5.9 do
- 7: **if** $\vec{c} \cdot \vec{v}_P \neq 0$ for every $P \in V(Q)(\mathbb{F}_{4^2})$ **then** append $F = \vec{c} \cdot \vec{X}$ to L
- 8: end for

9: return L

- Using dot products instead of polynomial evaluations provide a huge savings in arithmetic operations; we learned this trick from [20].
- The if-block in the main loop can terminate as soon as *some* dot product is zero. If we view a cubic polynomial as a random function with uniform random values in \mathbb{F}_{16} , then one would expect to evaluate around 16 points before seeing a zero. When we ran the code, 15.39 points were tested per cubic.
- For finite field arithmetic, we initially used the FLINT library. However, most of the runtime in the dot product was being spent on memory allocation because finite fields are implemented using polynomials and multi-precision integer arithmetic. To get around this obstacle, we created addition/multiplication tables for \mathbb{F}_4 -arithmetic and then performed these operations via lookup into the tables.
- For rapid debugging, we wrote the code to be flexible enough to work over \mathbb{F}_2 or \mathbb{F}_3 as well. Our implementation over \mathbb{F}_2 found 104 cubics and ran in negligible time. Over \mathbb{F}_3 , it found 2, 248 cubics and required 19 seconds to complete.

Now we turn to Step 2 of the computation that proves Theorem 5.8, which was completed with an implementation of Algorithm 3.

Let C be a curve of genus 4 and gonality 5 over \mathbb{F}_4 . We know $C = V(F) \cap V(Q)$ for some cubic form F that was output by Step 1. We may assume without loss that F is the first such form that was output, so that F is immediately added to the set M. If $C' = V(F') \cap V(Q)$ is another such curve isomorphic to C, then there is an element $g \in \mathrm{GL}_4(\mathbb{F}_4)$ that maps C to C'. Since the quadric surface containing C' is unique [5, Lem. 5.1], g must lie in O(Q). Thus, we have an equality of homogeneous ideals: $(F \circ g, Q) = (F', Q)$. Consequently, there is a linear form H and $a \in \mathbb{F}_4$ such that $F' = a(F \circ g) + HQ$. The while-loop in Algorithm 3 identifies this relationship and removes F' from S. It follows that F, and not F', appears in the list M.

To complete the justification of Algorithm 3, we must argue that each of its outputs yields a smooth geometrically connected scheme of dimension 1. By construction, $C := V(F) \cap V(Q)$ is smooth for $F \in M$. And C is 1-dimensional, for otherwise F = QH for some linear form H, which contradicts the fact that F has nonzero x^3 -coefficient. To see that C is geometrically connected, we pass to the algebraic closure $\overline{\mathbb{F}}_4$, where C is a (3,3)-divisor on

Algorithm 3 — Compute a list of cubic forms $F \in \mathbb{F}_4[x, y, z, w]$ such that any curve of genus 4 and gonality 5 is isomorphic to $V(F) \cap V(Q)$ for exactly one choice of F on the list

- 1: compute the orthogonal group O(Q)
- 2: initialize an empty list M
- 3: $S \leftarrow$ the list of cubic forms output by Algorithm 2.
- 4: while S is nonempty do
- 5: pop the first element F from S
- 6: for each $g \in O(Q)$ do
- 7: compute F(g(x, y, z, w)), scale the coefficient on x^3 to be 1, and subtract an appropriate multiple of Q to kill the x^2y xy^2 -, z^3 -, and w^3 -coefficients
- 8: remove the resulting element from S
- 9: end for
- 10: **if** $V(F) \cap V(Q)$ is smooth **then** append F to M
- 11: end while
- 12: return M

the surface $V(Q) \cong \mathbb{P}^1 \times \mathbb{P}^1$. If $C = C' \cup C''$, then C would have a singularity at each point of intersection of C' and C''.

Our Sage code performs Algorithm 3 in under 2 minutes. It identified 18 ideals corresponding to 1-dimensional varieties C with $C(\mathbb{F}_{4^2}) = \emptyset$, but each of these varieties is singular. Therefore, there is no curve of genus 4 and gonality 5 over \mathbb{F}_4 .

We close with a few implementation remarks:

- Sage defaults to a try/except construction to determine if a Gröbner basis or primary decomposition has already been computed for a given ideal. The try/except construction is painfully slow if the "except" clause is executed often, so we wrote special routines that avoid these issues.
- As with Step 1, we tested our code over \mathbb{F}_2 and \mathbb{F}_3 for rapid debugging and verification of output. Over \mathbb{F}_2 , we found a unique curve of genus 4 and gonality 5 up to isomorphism. This agrees with the recent calculations of Xarles [27]. Over \mathbb{F}_3 , we found a unique isomorphism class of genus-4 curves with gonality 5.

6. Curves of Genus 5

We have already shown that $N_3(5,2) = 8$ and $N_4(5,2) = 10$ in §2. We rapidly dispose of curves of gonality 3 and 4 with examples in the next couple of subsections, and we turn to a description of our computation on curves of gonality at least 5 in §6.3.

6.1. Gonality 3. For the fields at hand, the gonality-point inequality will be a sufficient upper bound for the number of points on a trigonal curve:

$$#C(\mathbb{F}_q) \le 3(q+1).$$

Theorem 6.1. $N_3(5,3) = 12$.

Proof. The gonality-point inequality gives a sharp upper bound. The plane curve with defining polynomial

$$x^{3}y^{2} - xy^{4} + x^{4}z - x^{2}y^{2}z + y^{4}z - x^{2}yz^{2} + y^{3}z^{2} - x^{2}z^{3}$$

is singular only at (0:0:1), where it has a cusp. By [5, Lem. 6.1], we find that its normalization C has genus 5 and is trigonal. The above plane curve passes through 12 rational points of the plane. Blowing up (0:0:1) yields a single rational point on C, so we conclude that $N_3(5,3) \ge 12$.

Theorem 6.2. $N_4(5,3) = 15$.

Proof. The gonality-point bound shows that $N_4(5,3) \leq 15$. The plane curve with defining polynomial

$$\begin{array}{l} (t+1)x^3y^2 + x^2y^3 + txy^4 + tx^4z + tx^3yz + tx^2y^2z \\ + xy^3z + ty^4z + (t+1)x^3z^2 + (t+1)x^2yz^2 + y^3z^2 + x^2z^3 \end{array}$$

passes through 15 rational points, has a cusp at (0 : 0 : 1), and no other singularity. Just as in the proof of Theorem 6.1, its normalization is a trigonal curve of genus 5 and $N_4(5,3) \ge 15$.

6.2. Gonality 4. The upper bound $N_q(5,4) \leq N_q(5)$ enables us to determine $N_q(5,4)$ for q = 3, 4.

Theorem 6.3. $N_3(5,4) = 13$.

Proof. Ritzenthaler [19] located the following curve $C \subset \mathbb{P}^4 = \operatorname{Proj} \mathbb{F}_3[v, w, x, y, z]$ of genus 5 with 13 rational points, presented as the complete intersection of three quadric hypersurfaces:

$$vw + xy = 0$$
$$-vx + xz - y^2 + z^2 = 0$$
$$v^2 + vx + w^2 - z^2 = 0.$$

(To get this form from Ritzenthaler's paper, set $x_1 = v, x_2 = x, x_3 = z, x_4 = -y, x_5 = w$.) Lemma 6.6 of [5] shows that C has gonality 4. Thus, $N_3(5,4) \ge 13$. Conversely, Lauter showed that $N_3(5) \le 13$ [12].

Theorem 6.4. $N_4(5,4) = 17$.

Proof. Howe and Lauter showed that $N_4(5) = 17$ [8], so it suffices to exhibit a curve of genus 5 and gonality 4 with 17 rational points. Fischer gave the following example on manypoints.org in 2014. Let C be the (smooth proper) curve birational to the affine scheme in $\mathbb{A}^3 = \mathbb{F}_4[x, y, z]$ cut out by the equations

$$y^{2} + y + x^{3} = 0$$

 $z^{2} + z + yx^{2} + xy^{2} = 0.$

Magma verifies that it has genus 5 and 17 rational points. If we write E for the elliptic curve with affine equation $y^2 + y = x^3$, then we see immediately that C is a double-cover of E. Consequently, C has gonality at most 4. If C has gonality $\gamma \leq 3$, then the gonality-point bound shows that $\#C(\mathbb{F}_4) \leq 5\gamma \leq 15$. Thus C has gonality exactly 4, and $N_4(5,4) = 17$. \Box 6.3. Gonality 5 and 6. The primary difficulty in immediately applying the code that we used to treat curves over \mathbb{F}_2 in [5] is that the relevant search space of quadric surfaces has increased dramatically in size: from $2^{15} \approx 10^{4.5}$ to $3^{15} \approx 10^{7.2}$ or $4^{15} \approx 10^{9.0}$. Beyond some coding tricks to speed things up and to deal with memory management, this required three major changes to our approach:

- We moved away from thinking of a curve C as cut out by a triple (Q_1, Q_2, Q_3) of quadratic forms and toward thinking of C as defined by the homogeneous ideal generated by this triple. In practice, this cut down the number of choices of Q_2 to be considered for each of the standard choices of Q_1 . Additional details are given below.
- We did not attempt to find *all* curves of gonality at least 5. Instead, we targeted curves with a particular number of points and either stopped searching as soon as an example was located or finished the search to certify that no curve with that many points exists. The available bounds $N_3(5) = 13$ and $N_4(5) = 17$ limited the total number of searches that were necessary.
- We distributed much of the computation across 48 CPUs Xeon(R) E5-2699 v3 2.30GHz with 500GB shared memory each running its own Sage process in order to complete the searches in a reasonable amount of time. Despite this, some of the searches over F₄ still required multiple days of compute time.

We now briefly sketch the strategy used to search for curves of genus 5 and gonality at least 5; the reader should consult [5, §6.4] for additional details. A non-hyperelliptic, nontrigonal curve of genus 5 can be written as the intersection of three quadric surfaces in $\mathbb{P}^4 = \operatorname{Proj} \mathbb{F}_q[v, w, x, y, z]$, given by quadratic forms Q_1, Q_2, Q_3 . By [5, Lem. 6.6], we may take Q_1 to be of one of the following forms:

III. vw + N(x, y), where N is a norm form for $\mathbb{F}_{q^2}/\mathbb{F}_q$, or IV. $vw + xy + z^2$.

We may use the action of the orthogonal group $O(Q_1)$ to restrict Q_2 to a small set of forms. More precisely, we construct a set $A(Q_1)$ of quadratic forms Q_2 such that

- (1) Each ideal $\langle Q_1, Q_2 \rangle$ cuts out a surface in \mathbb{P}^4 ;
- (2) Every quadratic form in the ideal $\langle Q_1, Q_2 \rangle$ is of the same type as Q_1 or of type IV; and
- (3) For any quadratic form Q such that the ideal $\langle Q_1, Q \rangle$ satisfies (1) and (2), there is a unique $Q_2 \in A(Q_1)$ and an element $g \in O(Q_1)$ such that $\langle Q_1, Q \circ g \rangle = \langle Q_Q, Q_2 \rangle$.

Finally, we let $B(Q_1)$ be the set of quadratic forms of the same type as Q_1 or of type IV.

Before beginning any of the searches for genus 5 curves, we precompute $O(Q_1)$, $B(Q_1)$, and $A(Q_1)$, in that order. Computing $O(Q_1)$ as in Section 4 is straightforward and fast. The computation of $B(Q_1)$ is also straightforward: for each quadratic form Q we can determine its type by computing the dimension of the singular locus of the quadric surface V(Q) and the number of rational points on this surface. As there are a huge number of forms to look at, and as this operation is easily parallelized, we distributed it across 24 CPUs — Xeon(R) E5-2699 v3 2.30GHz with 500GB shared memory — each running its own Sage process. Finally, computing $A(Q_1)$ requires one to keep track of which ideals have already appeared in some $O(Q_1)$ -orbit; this was performed on a single CPU. Knowledge of the precomputed set $B(Q_1)$ was used to determine the type of candidate elements of $A(Q_1)$. See Table 3 for the sizes of these sets and the wall time required to compute them. Note that when computing $B(vw + xy + z^2)$, we can recycle most of the computation from B(vw + N(x, y)), so the latter requires substantially less wall time to compute.

With these precomputations in hand, we now give a coarse description of our algorithm for searching for curves of genus 5 and gonality 5 or 6; see Algorithm 4. Rather than searching for all such curves, we instead attempt to find just one such curve if it exists. In order to keep each individual process from running too long, we target curves with a particular number of rational points. For curves of gonality 5, the total number of searches is limited by $N_q(5,5) \leq N_q(5)$. For curves of gonality 6, we look for pointless curves with no rational point over \mathbb{F}_{q^3} [5, Cor. 2.5].

Algorithm 4 — Find a genus 5 curve over \mathbb{F}_q with (a) gonality 5 and *n* rational points, or (b) gonality 6.

1: for $Q_1 \in \{vw + N(x, y), vw + xy + z^2\}$ do 2: for $(Q_2, Q_3) \in A(Q_1) \times B(Q_1)$ do 3: if case (a) and $\#V(Q_1, Q_2, Q_3)(\mathbb{F}_q) \neq n$ then continue 4: if case (b) and $\#V(Q_1, Q_2, Q_3)(\mathbb{F}_{q^3}) > 0$ then continue 5: if every nonzero member of the linear span of $\{Q_1, Q_2, Q_3\}$ has the same type as Q_1 or type IV, and the variety $V(Q_1, Q_2, Q_3)$ is irreducible and smooth of dimension 1 then return (Q_1, Q_2, Q_3) 6: end for 7: end for

Tables 5 and 6 indicate whether we found a curve lying on $V(Q_1)$ with a particular number of points or with gonality 6, as well as the total wall time involved for all searches. As a sanity check on our code, and also to see how this new strategy compares to the one in [5], we consider the case of curves over \mathbb{F}_2 ; these details are given in Table 4.

Looking at the tables, we immediately conclude the following:

Theorem 6.5.

$$N_3(5,5) = 4;$$
 $N_3(5,6) = -\infty;$ $N_4(5,5) = 5;$ and $N_4(5,6) = -\infty.$

Example 6.6. Our search uncovered the following example of a curve of genus 5 and gonality 5 over \mathbb{F}_3 with 4 rational points:

$$Q_1 = vw + xy + z^2$$
$$Q_2 = x^2 + wy + vz - xz$$
$$Q_3 = vw - wx + vy + xy + vz + xz + yz$$

Example 6.7. We located the following example of a curve of genus 5 and gonality 5 over \mathbb{F}_4 with 5 rational points:

$$Q_1 = vw + xy + z^2$$
$$Q_2 = vz + wy + x^2 + tz^2$$
$$Q_3 = v^2 + vw + wz + txy + xz + y^2 + z^2$$

| q | Q_1 | $\#O(Q_1)$ | wall time | $\#B(Q_1)$ | wall time | $#A(Q_1)$ | wall time |
|---|------------------------|--------------|---------------|-----------------|-----------|-----------|----------------|
| 2 | $vw + x^2 + xy + y^2$ | 1920 | 0s | 19,096 | 10s | 11 | 11s |
| | $vw + xy + z^2$ | 720 | 0s | 13,888 | 0s | 5 | 4s |
| 3 | $vw + x^2 + y^2$ | $116,640^*$ | 3s | $5,\!606,\!172$ | 13m 11s | 33 | $51\mathrm{m}$ |
| | $vw + xy + z^2$ | $51,840^{*}$ | 19s | $4,\!586,\!868$ | 16s | 16 | 24m |
| 4 | $vw + x^2 + txy + y^2$ | 2,088,960 | 2m 13s | 305,230,464 | 17h 1m | 83 | 43h 47m |
| | $vw + xy + z^2$ | 979,200 | $3\mathrm{m}$ | 263,983,104 | 12m | 37 | 20h 19m |

TABLE 3. Size and wall time for computation of the sets $O(Q_1)$, $B(Q_1)$, and $A(Q_1)$. We include the data for the case q = 2 for comparison, both with the cases q = 3, 4 as well as with the sizes in [5, §6.4]. The asterisk on the orthogonal group sizes for the case q = 3 indicate that we computed and counted $PO(Q_1) = O(Q_1)/\{\pm 1\}$.

| $Q_1 \setminus \#C(\mathbb{F}_2)$ | 0 | 1 | 2 | 3 | ≥ 4 | gonality 6 | Wall Time |
|-----------------------------------|--------------|--------------|--------------|--------------|----------|------------|-----------|
| $vw + x^2 + y^2$ | \checkmark | \checkmark | \checkmark | X | X | X | 40s |
| $vw + xy + z^2$ | X | X | X | \checkmark | X | × | 24s |

TABLE 4. Data for curves of genus 5 and gonality at least 5 over \mathbb{F}_2 . We indicate whether a curve of gonality 5 on $V(Q_1)$ with a specified number of rational points exists, whether a curve of gonality 6 on $V(Q_1)$ exists, and the total wall time required on 48 CPUs for all of the searches. Note that $\#C(\mathbb{F}_2) \leq N_2(5) = 9$.

| $Q_1 \setminus \#C(\mathbb{F}_3)$ | 0 | 1 | 2 | 3 | 4 | ≥ 5 | gonality 6 | Wall Time |
|-----------------------------------|--------------|--------------|--------------|--------------|--------------|----------|------------|-----------|
| $vw + x^2 + y^2$ | \checkmark | \checkmark | \checkmark | \checkmark | X | X | X | 59m |
| $vw + xy + z^2$ | X | X | X | X | \checkmark | X | × | 21m |

TABLE 5. Data for curves of genus 5 and gonality at least 5 over \mathbb{F}_3 . We indicate whether a curve of gonality 5 on $V(Q_1)$ with a specified number of rational points exists, whether a curve of gonality 6 on $V(Q_1)$ exists, and the total wall time required on 48 CPUs for all of the searches. Note that $\#C(\mathbb{F}_3) \leq N_3(5) = 13$.

| $Q_1 \setminus \#C(\mathbb{F}_4)$ | 0 | 1 | 2 | 3 | 4 | 5 | ≥ 6 | gonality 6 | Wall Time |
|-----------------------------------|--------------|--------------|--------------|--------------|--------------|--------------|----------|------------|-----------|
| $vw + x^2 + txy + y^2$ | \checkmark | \checkmark | \checkmark | \checkmark | \checkmark | X | X | X | 305h~52m |
| $vw + xy + z^2$ | X | X | X | X | X | \checkmark | X | × | 43h 26m |

TABLE 6. Data for curves of genus 5 and gonality at least 5 over \mathbb{F}_4 . We indicate whether a curve of gonality 5 on $V(Q_1)$ with a specified number of rational points exists, whether a curve of gonality 6 on $V(Q_1)$ exists, and the total wall time required on 48 CPUs for all of the searches. Note that $\#C(\mathbb{F}_4) \leq N_4(5) = 17$.

References

- Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system. I. The user language. Journal of Symbolic Computation, 24(3-4):235-265, 1997.
- [2] Wouter Castryck and Jan Tuitman. Point counting on curves using a gonality preserving lift. Preprint, arXiv:1605.02162v2 [math.NT], 2016.
- [3] Wouter Castryck and Jan Tuitman. Point counting on curves using a gonality preserving lift. Q. J. Math., 69(1):33-74, 2018.
- [4] Leonard Eugene Dickson. Linear groups: With an exposition of the Galois field theory. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.
- [5] Xander Faber and Jon Grantham. Binary curves of small fixed genus and gonality with many rational points. Preprint, arXiv:2102.00900 [math.NT], to appear in J. Algebra, 2021.
- [6] Xander Faber and Jon Grantham. Extremely pointless curves. In preparation, 2021.
- [7] W. Hart, F. Johansson, and S. Pancratz. FLINT: Fast Library for Number Theory, 2020. Version 2.6.0, http://flintlib.org.
- [8] 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(6):1677–1737, 2003.
- [9] Everett W. Howe and Kristin E. Lauter. New methods for bounding the number of points on curves over finite fields. In *Geometry and arithmetic*, EMS Ser. Congr. Rep., pages 173–212. Eur. Math. Soc., Zürich, 2012.
- [10] Everett W. Howe, Kristin E. Lauter, and Jaap Top. Pointless curves of genus three and four. In Arithmetic, geometry and coding theory (AGCT 2003), volume 11 of Sémin. Congr., pages 125–141. Soc. Math. France, Paris, 2005.
- [11] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28(3):721–724 (1982), 1981.
- [12] Kristin Lauter. Non-existence of a curve over \mathbf{F}_3 of genus 5 with 14 rational points. *Proc. Amer. Math. Soc.*, 128(2):369–374, 2000.
- [13] Kristin Lauter. Zeta functions of curves over finite fields with many rational points. In Coding theory, cryptography and related areas (Guanajuato, 1998), pages 167–174. Springer, Berlin, 2000.
- [14] Kristin Lauter. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. J. Algebraic Geom., 10(1):19–36, 2001. With an appendix in French by J.-P. Serre.
- [15] Qing Liu. Algebraic geometry and arithmetic curves, volume 6 of Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.
- [16] Harald Niederreiter and Chaoping Xing. Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places. Acta Arith., 79(1):59–76, 1997.
- [17] Harald Niederreiter and Chaoping Xing. Rational points on curves over finite fields: theory and applications, volume 285 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2001.
- [18] Alessandra Rigato. Uniqueness of low genus optimal curves over F₂. In Arithmetic, geometry, cryptography and coding theory 2009, volume 521 of Contemp. Math., pages 87–105. Amer. Math. Soc., Providence, RI, 2010.
- [19] Christophe Ritzenthaler. Existence d'une courbe de genre 5 sur \mathbb{F}_3 avec 13 points rationels. Preprint, arXiv:math/0302147 [math.NT], 2003.
- [20] David Savitt. The maximum number of points on a curve of genus 4 over \mathbb{F}_8 is 25. Canad. J. Math., 55(2):331–352, 2003. With an appendix by Kristin Lauter.
- [21] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. C. R. Acad. Sci. Paris Sér. I Math., 296(9):397–402, 1983.
- [22] Jean-Pierre Serre. Rational points on curves over finite fields. Course notes by F. Q. Gouvêa, 1985.

- [23] Jean-Pierre Serre. Rational points on curves over finite fields, volume 18 of Documents Mathématiques. Société Mathématique de France, 2020. With contributions by Everett Howe, Joseph Oesterlé, and Christophe Ritzenthaler.
- [24] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 8.7), 2019. http://www.sagemath.org.
- [25] Gerard van der Geer and Marcel van der Vlugt. Tables of curves with many points. Math. Comp., 69(230):797–810, 2000.
- [26] John Voight. Curves over finite fields with many points: an introduction. In Computational aspects of algebraic curves, volume 13 of Lecture Notes Ser. Comput., pages 124–144. World Sci. Publ., Hackensack, NJ, 2005.
- [27] Xavier Xarles. A census of all genus 4 curves over the field with 2 elements. Preprint, arXiv:2007.07822v1 [math.AG], 2020.

INSTITUTE FOR DEFENSE ANALYSES, CENTER FOR COMPUTING SCIENCES, 17100 SCIENCE DRIVE, BOWIE, MD