ANNALES

DE

L'INSTITUT FOURIER

Everett W. HOWE & Kristin E. LAUTER

Improved upper bounds for the number of points on curves over finite fields

Tome 53, n° 6 (2003), p. 1677-1737.

<http://aif.cedram.org/item?id=AIF_2003__53_6_1677_0>

Ann. Inst. Fourier, Grenoble
53, 6 (2003), 1677–1737

IMPROVED UPPER BOUNDS FOR THE NUMBER OF POINTS ON CURVES OVER FINITE FIELDS

by **E. W. HOWE and K. E. LAUTER**

1. Introduction.

The number N of points on a smooth, absolutely irreducible curve of genus g over a finite field $\mathbb{F}_q$ is bounded by

$$q + 1 - 2g\sqrt{q} \leqslant N \leqslant q + 1 + 2g\sqrt{q},$$

an estimate given by André Weil in the 1940s. In 1983, Serre improved this bound to

$$q + 1 - gm \leqslant N \leqslant q + 1 + gm, \quad \text{where } m = [2\sqrt{q}].$$

Serre also introduced the *explicit formulæ method*, which uses numerical conditions on the number of points on a curve over extensions of the ground field to obtain improved bounds on N, at least when g is large compared to q (specifically, when $g > (q - \sqrt{q})/2$). Oesterlé optimized the explicit formulæ method, and the resulting bounds on N are the best possible bounds that can be obtained formally using only Weil's "Riemann hypothesis" for curves and the fact that for every $d \geqslant 0$ the number of places of degree d on a curve is non-negative. But the method does not take the geometry of the curves into account, and for this reason it is natural to suspect that the Weil-Serre-Oesterlé bounds may not be optimal. Indeed, Serre [22] and others [5], [9], [11], [12], [13], [14], [15], [18], [19], [20], [21], [25], [27], [30] have shown that in certain cases these bounds are not attained. However,

Keywords: Curve – Rational point – zeta function – Weil bound – Serre bound – Oesterlé bound.
Math. classification: 11G20 – 14G05 – 14G10 – 14G15.

in many other cases the bounds provided by the explicit formulæ method remain the best known, and significant effort has been made to determine whether or not they are met — see the tables of van der Geer and van der Vlugt [6], which summarize the work of many authors. The purpose of this paper is to provide some new techniques that show that in many cases the current upper bounds cannot be met. In particular, we list in Tables 1 and 2 the improvements we obtain to the tables in [6]. In Table 3 we list the values of q and g for which our improved upper bound meets the known lower bound. (The tables in [6] are updated frequently; the latest version can be found at

`http://www.science.uva.nl/~geer/`

The version of the tables that we will refer to in this paper is dated 18 January 2002, and is available at the URL mentioned below in the acknowledgments.)

Our improved bounds are due to the fact that some zeta functions that satisfy the numerical conditions of the explicit formulæ method are forbidden by a combination of geometrical and numerical conditions. Our approach is in the spirit of [11], [12], [13], [14], [15], [18], [22] where lists of possible zeta functions were compiled and geometric arguments were applied for the purpose of improving the bounds.

The main theorem that we use to improve the known upper bounds deals with a numerical invariant of pairs of abelian varieties. Suppose A_1 and A_2 are abelian varieties over $\mathbb{F}_q$. Let F and V denote, respectively, the Frobenius and Verschiebung endomorphisms of $A_1 \times A_2$. Given an element α of the subring $\mathbb{Z}[F, V]$ of $\mathrm{End}(A_1 \times A_2)$, we let g_1 and g_2 be the minimal polynomials of α restricted to A_1 and A_2, respectively, and we define $r(\alpha)$ to be the resultant of g_1 and g_2. Define $s(A_1, A_2)$ to be the greatest common divisor of the set $\{r(\alpha) : \alpha \in \mathbb{Z}[F, V]\}$. Note that if A_1 and A_2 have an isogeny factor in common then $r(\alpha) = 0$ for every α, so that $s(A_1, A_2) = \infty$. On the other hand, if A_1 and A_2 share no common isogeny factors then $r(F) \neq 0$ by the Honda-Tate theorem [29], so that $s(A_1, A_2) < \infty$. In other words, $\mathrm{Hom}(A_1, A_2) = \{0\}$ if and only if $s(A_1, A_2) < \infty$. Also note that the value of $s(A_1, A_2)$ depends only on the isogeny classes of A_1 and A_2.

THEOREM 1. — *Let A_1 and A_2 be nonzero abelian varieties over $\mathbb{F}_q$.*

(a) *If $s(A_1, A_2) = 1$ then there is no curve C over $\mathbb{F}_q$ whose Jacobian is isogenous to $A_1 \times A_2$.*

(b) *Suppose $s(A_1, A_2) = 2$. If C is a curve over $\mathbb{F}_q$ whose Jacobian is isogenous to $A_1 \times A_2$, then there is a degree-2 map from C to another curve D over $\mathbb{F}_q$ whose Jacobian is isogenous to either A_1 or A_2.*

q	genus	old upper bound	new upper bound
4	5	18	17
4	10	28	27
4	11	30	29
8	5	32	30
8	7	39	38
8	8	43	42
8	9	47	45
8	10	50	49
8	11	54	53
8	15	68	67
16	4	46	45
16	5	54	53
16	7	70	69
16	8	76	75
16	11	92	91
16	13	103	102
16	14	108	107
32	$4 \leqslant g \leqslant 8$	$q+1+gm-2$	$q+1+gm-3$
32	$9 \leqslant g \leqslant 15$	$q+1+gm-2$	$q+1+gm-4$
64	$11 \leqslant g \leqslant 27$ and $g \neq 12$	$q+1+gm-3$	$q+1+gm-5$
128	4	217	215
128	6	261	258
128	8	305	302
128	9	327	322
128	11	371	366
128	$15 \leqslant g \leqslant 64$ and $g \equiv 1 \bmod 7$	$q+1+gm$	$q+1+gm-4$
128	$16 \leqslant g \leqslant 65$ and $g \equiv 2 \bmod 7$	$q+1+gm$	$q+1+gm-5$
128	$10 \leqslant g \leqslant 59$ and $g \equiv 3 \bmod 7$	$q+1+gm$	$q+1+gm-4$
128	$18 \leqslant g \leqslant 60$ and $g \equiv 4 \bmod 7$	$q+1+gm$	$q+1+gm-6$
128	$5 \leqslant g \leqslant 61$ and $g \equiv 5 \bmod 7$	$q+1+gm$	$q+1+gm-5$
128	$13 \leqslant g \leqslant 62$ and $g \equiv 6 \bmod 7$	$q+1+gm$	$q+1+gm-7$

TABLE 1. Improved upper bounds on the number of points on curves of certain genera over small finite fields $\mathbb{F}_q$ of characteristic 2. The symbol m is an abbreviation for $[2\sqrt{q}]$.

q	genus	old upper bound	new upper bound
3	6	15	14
9	9	51	50
9	10	55	54
9	11	59	58
9	12	63	62
9	13	66	65
9	14	70	69
9	15	74	73
9	16	78	77
9	17	82	81
9	18	85	84
27	4	66	64
27	$5 \leqslant g \leqslant 8$	$q+1+gm-2$	$q+1+gm-3$
27	$9 \leqslant g \leqslant 13$	$q+1+gm-2$	$q+1+gm-5$
27	14	164	163
81	$13 \leqslant g \leqslant 17$ and $g \neq 16$	$q+1+gm-2$	$q+1+gm-4$
81	$18 \leqslant g \leqslant 35$	$q+1+gm-2$	$q+1+gm-5$

TABLE 2. Improved upper bounds on the number of points on curves of certain genera over small finite fields $\mathbb{F}_q$ of characteristic 3. The symbol m is an abbreviation for $[2\sqrt{q}]$.

q	genus g	$N_q(g)$
4	5	17
4	10	27
8	9	45
16	4	45
128	4	215
3	6	14
9	10	54
27	4	64

TABLE 3. New values of $N_q(g)$ obtained in this paper.

One can get upper and lower bounds on $s(A_1, A_2)$ by using the following result. (Recall that the *radical* of a nonzero integer is the product of its prime divisors.)

THEOREM 2. — *Suppose A_1 and A_2 are abelian varieties over $\mathbb{F}_q$ with $s(A_1, A_2) \neq 0$. Then $s(A_1, A_2)$ divides $r(F+V)$ and is divisible by the radical of $r(F+V)$.*

Theorem 2 shows that Theorem 1(a) is equivalent to a result of Serre [12], [22] that states that the Jacobian of a curve is never isogenous to a product $A_1 \times A_2$ of nonzero abelian varieties for which $r(F+V) = \pm 1$.

It is not clear whether there are any similarly strong conclusions to be drawn from other values of $s(A_1, A_2)$. However, if we make some assumptions about A_1 and A_2, we can prove that certain other values of $s(A_1, A_2)$ prohibit the existence of a curve with Jacobian isogenous to $A_1 \times A_2$ — see Propositions 11 and 13 and Corollaries 12 and 14.

Theorem 1, combined with previously known results and some straightforward facts about degree-2 maps of curves, allows us to greatly restrict the possible zeta functions of curves having a large number N of points. For some values of q and g these restrictions are strong enough to allow us to immediately eliminate certain values of N from consideration. For other combinations of q, g, and N, we can quickly eliminate most possible zeta functions and are left with a few special cases to consider. For some of these special cases we can use Theorem 1(b) to restrict the form of the curves in question to such an extent that a computer search for curves with the desired number of points becomes feasible. For one such case, detailed in Section 5, we manage to avoid significant computer calculations by extending a Galois descent argument used in [22].

The *defect* of a genus-g curve C over $\mathbb{F}_q$ is the difference between the Weil-Serre upper bound for genus-g curves over $\mathbb{F}_q$ and the number of rational points on C; in other words, a curve C has defect k if it has exactly $(q+1+g[2\sqrt{q}]) - k$ rational points. Theorem 1 allows us to prove some general results about curves with small defect. For example, we have the following theorem for square q.

THEOREM 3. — *Suppose q is a square.*

(a) *If $q \neq 4$ and $g > 2$ then there are no defect-2 curves of genus g over $\mathbb{F}_q$.*

(b) *If $q \neq 9$ and $g > 3$ then there are no defect-3 curves of genus g over $\mathbb{F}_q$.*

(c) *If $g > (3q + 4m - 9)/m$, where $m = 2\sqrt{q}$, then there are no defect-4 curves of genus g over $\mathbb{F}_q$.*

(d) *If $q = 2^{2e}$ with $e > 2$, and if $g > 2^{e-1} + 2$, then there are no defect-4 curves of genus g over $\mathbb{F}_q$.*

For certain nonsquare q the Weil-Serre bound can be improved via a different method. Suppose q is a prime power. We define the *defect-0 dimension* of q to be the smallest positive integer δ for which there is a δ-dimensional abelian variety over $\mathbb{F}_q$ with characteristic polynomial of Frobenius equal to $(x^2+mx+q)^\delta$. We say that q is *exceptional* if its defect-0 dimension is greater than 1.

THEOREM 4. — *Suppose q is a prime power and let δ be the defect-0 dimension of q. If C is a curve of genus g over $\mathbb{F}_q$, then the defect of C is at least $r/2$, where $r \in [0, \delta)$ is the remainder when g is divided by δ.*

Theorem 4 says something nontrivial about q only if q is exceptional, so we would like to be able to find the exceptional prime powers. In fact, there is an easy way to calculate the defect-0 dimension of a power q of a prime p. Let ν be an additive p-adic valuation on $\mathbb{Q}$ and let $m = [2\sqrt{q}]$.

PROPOSITION 5. — *If q is a square or if $q < 4$ then the defect-0 dimension of q is 1. If $q > 4$ is not a square, then the defect-0 dimension of q is the smallest positive integer δ such that $\delta\nu(m)/\nu(q)$ is an integer.*

We will prove Theorem 4 and Proposition 5 in Section 3. The proofs will foreshadow the arguments that produce the entries in Table 1 for $q = 128$.

It is easy to show that there are infinitely many q of the form 2^{2e+1} whose defect-0 dimension is $2e + 1$; we will provide a proof of this fact in Section 3. For such a q we see that a curve of genus $g \leqslant 2e$ must have defect at least $g/2$. The existence of these q allows us to prove an interesting fact about the function $N_q(g)$ defined by

$$N_q(g) = \max\{\#C(\mathbb{F}_q) : C \text{ is a genus-}g \text{ curve over } \mathbb{F}_q\}.$$

COROLLARY 6. — *There are infinitely many powers q of 2 such that for every g with $0 < g < \log_2 q$ we have $(q + 1 + g[2\sqrt{q}]) - N_q(g) \geqslant g/2$.*

In particular, this implies that there is a sequence of pairs (q, g) where g is small with respect to q and for which the Weil-Serre bound becomes arbitrarily far from the true value of $N_q(g)$. Zieve [30] has already shown that there is a sequence of pairs (q, g) where $g/q \to 1/2$ and for which all

previously-known bounds on $N_q(g)$ become arbitrarily far from the true value of $N_q(g)$.

Savitt [18] recently showed, through extensive computer calculation, that there is no genus-4 curve over $\mathbb{F}_8$ having exactly 27 rational points. We prove this same result in Section 8 with an argument much less dependent on the computer. In [14] it was shown that there are only two possibilities for the zeta function of such a curve. We can show that the first zeta function cannot occur by using Theorem 1(b). For the second zeta function, we introduce a new argument that generalizes the Hermitian form argument used in [15]. We are able to eliminate the second zeta function by showing that if A is an abelian variety whose characteristic polynomial of Frobenius is f^2, where

$$f = x^4 - 9x^3 + 35x^2 - 72x + 64,$$

then every principal polarization on A is decomposable. To prove this, we show that there are no indecomposable unimodular Hermitian forms of rank 2 over the ring of integers of the quartic number field defined by f.

In Section 2 we prove Theorems 1, 2, and 3, and we provide a number of useful corollaries. In Section 3 we prove Theorem 4, Proposition 5, and Corollary 6. In Section 4 we prove the results mentioned in Tables 1 and 2, although we postpone the consideration of some cases to later sections. In Section 5 we use a Galois descent argument to show that there is no genus-5 curve over $\mathbb{F}_8$ with 31 points. In Section 6 we check by exhaustion that there is no genus-4 curve over $\mathbb{F}_{27}$ with 66 points, that there is no genus-4 curve over $\mathbb{F}_{32}$ with 75 points, and that there is no genus-6 curve over $\mathbb{F}_3$ with a certain Weil polynomial; these calculations are feasible only because Theorem 1 allows us to considerably reduce the spaces we must search over. In Section 7 we show that there is no genus-6 curve over $\mathbb{F}_3$ with a certain Weil polynomial and that there is no genus-4 curve over $\mathbb{F}_{27}$ with 65 points; the arguments in this section depend on our ability to easily parameterize degree-3 covers of elliptic curves in characteristic 3. In Section 8 we use the Hermitian form argument mentioned above to prove Savitt's result that there is no genus-4 curve over $\mathbb{F}_8$ with 27 points.

Notation. — Throughout this paper a *curve* over $\mathbb{F}_q$ will mean a smooth, projective, absolutely irreducible curve. We will denote by $N_q(g)$ the largest N such that there is a curve of genus g over $\mathbb{F}_q$ with exactly N rational points. The *Weil polynomial* of an abelian variety over a finite field is the characteristic polynomial of the Frobenius endomorphism of the variety. The *Weil polynomial* of a curve over a finite field is the Weil

polynomial of its Jacobian. Note that if $f \in \mathbb{Z}[x]$ is the Weil polynomial of a genus-g curve C over $\mathbb{F}_q$, then the numerator of the zeta function of C is equal to $x^{2g} f(1/x)$. If f is the Weil polynomial of a curve or an abelian variety, say with $\deg f = 2g$, then there is a degree-g polynomial $h \in \mathbb{Z}[x]$, all of whose roots are real, such that $f(x) = x^g h(x + q/x)$. We will refer to h as the *real Weil polynomial* of the curve or the abelian variety.

Acknowledgments. — We thank Jean-Pierre Serre for his helpful comments. In the course of doing the work described in this paper we used the computer algebra systems Pari/GP and Magma [1]. Several of our Magma programs are available on the web: start at

`http://www.alumni.caltech.edu/~however/biblio.html`

and follow the links related to this paper. We have also placed a copy of the 18 January 2002 version of the van der Geer-van der Vlugt tables on this site.

2. Proofs of Theorems 1, 2 and 3.

In this section we will prove Theorems 1, 2, and 3, as well as some useful corollaries. We begin with a lemma.

LEMMA 7. — *Suppose B is an abelian variety over $\mathbb{F}_q$ isogenous to a product $A_1 \times A_2$, where $s(A_1, A_2) < \infty$. Then there exist abelian varieties A_1' and A_2', isogenous to A_1 and A_2, respectively, and an exact sequence*

$$0 \to \Delta' \to A_1' \times A_2' \to B \to 0$$

such that the projection maps $A_1' \times A_2' \to A_1'$ and $A_1' \times A_2' \to A_2'$ give monomorphisms from Δ' to $A_1'[s]$ and to $A_2'[s]$, where $s = s(A_1, A_2)$.

Suppose in addition that B has a principal polarization μ. Then the pullback of μ to $A_1' \times A_2'$ is a product polarization $\lambda_1 \times \lambda_2$, and the projection maps $A_1' \times A_2' \to A_1'$ and $A_1' \times A_2' \to A_2'$ give isomorphisms of Δ' with $\ker \lambda_1$ and $\ker \lambda_2$. In particular, Δ' is isomorphic to its own Cartier dual.

Proof. — Let φ be an arbitrary isogeny from $A_1 \times A_2$ to B and let Δ be the kernel of φ. Let G_1 and G_2 be the largest closed subgroup-schemes of A_1 and A_2 such that $G_1 \times G_2$ is a closed subgroup-scheme of Δ, let $\Delta' = \Delta/(G_1 \times G_2)$, and let $A_1' = A_1/G_1$ and $A_2' = A_2/G_2$. Then we have an exact sequence

$$0 \to \Delta' \to A_1' \times A_2' \to B \to 0$$

such that the projection maps give monomorphisms of Δ' to A_1' and A_2'. We will show that in fact the projection maps take Δ' to $A_1'[s]$ and $A_2'[s]$.

Let α be an arbitrary endomorphism of $A_1' \times A_2'$ that lies in $\mathbb{Z}[F, V]$. (Here we use the fact that $\mathbb{Z}[F, V]$ is contained in the endomorphism ring of every abelian variety isogenous to $A_1 \times A_2$.) For $i = 1, 2$ let g_i be the minimal polynomial of α acting on A_i'. Then $g_1(\alpha)$ and $g_2(\alpha)$ both act as 0 on Δ', because Δ' can be viewed as a subgroup-scheme of both A_1' and A_2'. But then $r(\alpha)$ must act as 0 on Δ' as well. Since this is true for every α, we see that $s(A_1, A_2)$ must kill Δ'; this shows that the projection maps embed Δ' into $A_1'[s]$ and $A_2'[s]$.

Now suppose B has a principal polarization μ. Let λ be the pullback of μ to $A_1' \times A_2'$. Since $\mathrm{Hom}(A_1', A_2')$ and $\mathrm{Hom}(A_2', A_1')$ are both trivial, λ must be a product polarization $\lambda_1 \times \lambda_2$. The degree of λ is equal to the degree of μ (which is 1) times the square of the degree of the isogeny $A_1' \times A_2' \to B$, so we have

$$(\#\Delta')^2 = \#\ker\lambda = (\#\ker\lambda_1)(\#\ker\lambda_2),$$

where we use $\#$ to denote the rank of a finite group-scheme. Since the projection maps give monomorphisms from Δ' to A_1' and A_2', we see that $\#\Delta' \leqslant \#\ker\lambda_i$ for $i = 1$ and $i = 2$. This means that we must have $\#\Delta' = \#\ker\lambda_i$ for each i, and it follows that $\Delta' \cong \ker\lambda_i$ for each i. Since kernels of polarizations are isomorphic to their own duals, we obtain the final statement of the lemma. □

Proof of Theorem 1. — Suppose $s(A_1, A_2) = 1$. Then Lemma 7 shows that every abelian variety isogenous to $A_1 \times A_2$ is a product $A_1' \times A_2'$. Since $s(A_1', A_2') = s(A_1, A_2) < \infty$ we see that $\mathrm{Hom}(A_1', A_2') = \{0\}$, so every polarization on $A_1' \times A_2'$ is a product polarization. In particular, we see that every principal polarization of an abelian variety isogenous to $A_1 \times A_2$ is decomposable, so there can be no Jacobians isogenous to $A_1 \times A_2$. This is the first statement of the theorem.

Now suppose that $s(A_1, A_2) = 2$. Apply Lemma 7 and replace A_1 and A_2 with the resulting A_1' and A_2', so that we have an exact sequence

$$0 \to \Delta \to A_1 \times A_2 \to \mathrm{Jac}\, C \to 0$$

where Δ can be viewed as a subscheme of $A_1[2]$ and $A_2[2]$.

Let μ be the canonical polarization on $\mathrm{Jac}\, C$ and let λ be the polarization on $A_1 \times A_2$ obtained by pulling back μ via φ. Lemma 7 shows that λ is the product of a polarization λ_1 on A_1 and a polarization λ_2 of

A_2. Let $(1,-1)$ denote the involution of $A_1 \times A_2$ that acts as 1 on A_1 and as -1 on A_2. Clearly $(1,-1)$ respects the polarization λ, because 1 respects λ_1 and -1 respects λ_2. Furthermore, $(1,-1)$ acts as the identity on Δ, so it gives rise to an involution β on $\operatorname{Jac} C$ that respects the polarization μ. By Torelli's theorem, there exists an involution α of C such that either $\beta = \alpha^*$ or $\beta = -\alpha^*$.

Let D be the quotient of C by the involution α, so that there is a degree-2 map ψ from C to D with $\psi = \psi \circ \alpha$. Then the morphism $\psi^* : \operatorname{Jac} D \to \operatorname{Jac} C$ gives an isogeny from $\operatorname{Jac} D$ to the connected component of the subvariety of $\operatorname{Jac} C$ on which β acts as the identity. This subvariety is isogenous to A_1 if $\beta = \alpha^*$ and to A_2 if $\beta = -\alpha^*$. □

We will use Theorem 1(b) in conjunction with some obvious facts about degree-2 covers of curves, which we state here for convenience.

LEMMA 8. — *Suppose C and D are curves over $\mathbb{F}_q$ of genus g_C and g_D, respectively, and suppose there is a degree-2 map $C \to D$. For every integer $d > 0$ let a_d denote the number of degree-d places on C and let b_d denote the number of degree-d places on D.*

(a) *For every odd d we have $a_d \leqslant 2b_d$.*

(b) *We have $g_C \geqslant 2g_D - 1$, with equality if and only if $C \to D$ is unramified.*

(c) *Let $d_1 < \cdots < d_n$ be odd positive integers such that a_{d_i} is odd for every i, and let $r = d_1 + \cdots + d_n$. Then $g_C \geqslant 2g_D - 1 + r/2$, and equality holds if and only if $C \to D$ is ramified at exactly n places $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, where each $\mathfrak{p}_i$ has degree d_i and where the ramification at each $\mathfrak{p}_i$ is tame.*

Proof. — Suppose d is odd. Every degree-d place of D has at most 2 degree-d places of C lying over it, and every degree-d place of C lies over a degree-d place of D. Statement (a) follows immediately.

Statement (b) is the special case $n = 0$ of statement (c).

Let ι be the involution of C corresponding to the cover $C \to D$. Suppose d is an odd number such that a_d is odd. Then there is a degree-d place $\mathfrak{p}$ of C that is taken to itself by ι. Since $\mathfrak{p}$ consists of an odd number of geometric points of C, there must be a geometric point P in $\mathfrak{p}$ that is fixed by ι, and since all of the geometric points in $\mathfrak{p}$ are conjugate to each other, *all* of the points in $\mathfrak{p}$ must be fixed by ι. These d points must be ramification

points of the cover $C \to D$. Thus, the hypothesis of statement (c) implies that there are at least r ramification points in the cover $C \to D$. The conclusion of the statement then follows by applying the Riemann-Hurwitz formula to the cover $C \to D$. □

Suppose A is a g-dimensional abelian variety over $\mathbb{F}_q$ and let

$$\{\alpha_1, \ldots, \alpha_g, \overline{\alpha}_1, \ldots, \overline{\alpha}_g\}$$

be the multiset of complex roots of the Weil polynomial of A. For each i let $x_i = -(\alpha_i + \overline{\alpha}_i)$. We will say that A is *of type* $[x_1, \ldots, x_g]$. If A is the Jacobian of a curve C we will also say that C and its zeta function are *of type* $[x_1, \ldots, x_g]$. Note that the zeta function of a curve of type $[x_1, \ldots, x_g]$ is given by

$$\frac{n(t)}{(1-t)(1-qt)},$$

where

$$n(t) = \prod_{i=1}^{g}(1 + x_i t + qt^2).$$

Also, if F is the Frobenius morphism of A and if $V = q/F$ is the Verschiebung, then the characteristic polynomial of $F+V$ is equal to $h^2(t)$, where

$$h(t) = \prod_{i=1}^{g}(t + x_i)$$

is the real Weil polynomial of A.

COROLLARY 9. — *There are no genus-g curves of type $[m, \ldots, m, m-2]$ over $\mathbb{F}_q$ if $g > (q-1+2m)/m$ and $g > 3$, where $m = [2\sqrt{q}]$.*

Proof. — We will prove the contrapositive statement. Suppose C is a curve of genus g over $\mathbb{F}_q$ with zeta function $[m, \ldots, m, m-2]$. Then $\operatorname{Jac} C$ is isogenous to a product $A \times E$ of abelian varieties, where E is an elliptic curve over $\mathbb{F}_q$ of type $[m-2]$ and where A is a $(g-1)$-dimensional abelian variety over $\mathbb{F}_q$ of type $[m, \ldots, m]$. We see that $r(F+V) = 2$, so $s(A, E) = 2$. According to Theorem 1, the curve C is a degree-2 cover of a curve D whose Jacobian is isogenous to either A or E. If $\operatorname{Jac} D \sim A$ then D has genus $g-1$, and Lemma 8(b) shows that $g \leqslant 3$. If $\operatorname{Jac} D \sim E$ then D is an elliptic curve with $q+m-1$ points, and applying Lemma 8(a) with $d = 1$ shows that

$$q + gm - 1 \leqslant 2q + 2m - 2,$$

which gives $g \leqslant (q-1+2m)/m$. □

Recall that the *defect* of a genus-g curve C over $\mathbb{F}_q$ is the difference between the Weil-Serre upper bound and the number of rational points on C.

COROLLARY 10. — *There are no defect-2 curves of genus g over $\mathbb{F}_q$ if $g > (q-1+4m)/m$ and $g > 5$, where $m = [2\sqrt{q}]$.*

Proof. — If C has defect 2, then its zeta function must be of one of the seven types listed in [14]. For $g \geqslant 5$, all but two of these types are eliminated by Theorem 1(a). The two remaining types are $[m, \dots, m, m-2]$ and $[m, \dots, m, m+\sqrt{3}-1, m-\sqrt{3}-1]$. Since we are assuming that $g > (q-1+4m)/m$, Corollary 9 eliminates the former possibility, so C must have the latter type. In this case $\operatorname{Jac} C$ is isogenous to the product of a $(g-2)$-dimensional abelian variety A_1 of type $[m, \dots, m]$ and a 2-dimensional abelian variety A_2 of type $[m+\sqrt{3}-1, m-\sqrt{3}-1]$. Applying Theorem 1(b), we find that C is a double cover of a curve D that is either of type $[m, \dots, m]$ or of type $[m+\sqrt{3}-1, m-\sqrt{3}-1]$. In the first case D would have genus $g-2$, and Lemma 8(b) shows that then $g \leqslant 5$. In the second case, Lemma 8(a) with $d = 1$ gives us

$$q + gm - 1 \leqslant 2(q + 2m - 1),$$

which leads to $g \leqslant (q-1+4m)/m$. □

We have mentioned that we do not know any strong conclusions one can draw in general when $s(A_1, A_2) > 2$. However, with a little more information about A_1 and A_2 we can indeed say something.

PROPOSITION 11. — *Let A_1' and A_2' be abelian varieties over $\mathbb{F}_q$ and let $s = s(A_1', A_2')$. Suppose that for every A_1 isogenous to A_1' and every A_2 isogenous to A_2', the only self-dual finite group-scheme that can be embedded in both $A_1[s]$ and $A_2[s]$ as the kernel of a polarization is the trivial group-scheme. Then there is no curve over $\mathbb{F}_q$ with Jacobian isogenous to $A_1' \times A_2'$.*

Proof. — Suppose there were such a curve. Then Lemma 7 shows that we can find a group-scheme Δ that fits in an exact sequence

$$0 \to \Delta \to A_1 \times A_2 \to \operatorname{Jac} C \to 0$$

and that can be embedded in both $A_1[s]$ and $A_2[s]$. Furthermore, since $\operatorname{Jac} C$ has a principal polarization, for each $i = 1, 2$ we have that Δ is

isomorphic to the kernel of the polarization of A_i obtained by pulling back the principal polarization of $\operatorname{Jac} C$. The hypotheses of the proposition show that Δ must be the trivial group-scheme, so $\operatorname{Jac} C$ is isomorphic to the product of two abelian varieties that share no isogeny factor. As we have seen, this is a contradiction. □

The next corollary describes a situation in which the hypotheses of Proposition 11 are met.

COROLLARY 12. — *Suppose q is a square prime power and n is a squarefree integer coprime to q. Let $m = 2\sqrt{q}$. Then there is no curve over $\mathbb{F}_q$ of type $[m, \ldots, m, m-n]$.*

Proof. — Let A_1 be any abelian variety over $\mathbb{F}_q$ isogenous to the product of $(g-1)$ copies of a supersingular elliptic curve over $\mathbb{F}_q$ with Weil polynomial $x^2 + mx + q = (x + \sqrt{q})^2$, and let A_2 be any ordinary elliptic curve over $\mathbb{F}_q$ with Weil polynomial $x^2+(m-n)x+q$. Clearly $s(A_1, A_2) = n$. Suppose Δ is a nontrivial self-dual finite group scheme that embeds in both $A_1[n]$ and $A_2[n]$ as the kernel of a polarization. Since the only polarizations on A_2 are the multiplication-by-ℓ maps for positive integers ℓ, we must have $\Delta \cong A_2[\ell]$ for some divisor $\ell > 1$ of n. Since Δ embeds in $A_1[\ell]$ as well, and since the Frobenius F on A_1 satisfies $F + \sqrt{q} = 0$, we know that Frobenius must act as the integer $-\sqrt{q}$ on Δ, and hence on $A_2[\ell]$. This means that $F + \sqrt{q} = 0$ on $A_2[\ell]$, which means that $(F + \sqrt{q})/\ell$ is an endomorphism of A_2. But from the characteristic polynomial of F on A_2 we can calculate that the characteristic polynomial of $(F + \sqrt{q})/\ell$ on A_2 is

$$x^2 - (n/\ell)x + (n\sqrt{q}/\ell^2),$$

which is not integral. This contradiction shows that no nontrivial self-dual finite group-scheme can be embedded in both $A_1[n]$ and $A_2[n]$. By Proposition 11, there is no curve over $\mathbb{F}_q$ of type $[m, \ldots, m, m-n]$. □

There is another situation in which we can draw conclusions from values of $s(A_1, A_2)$ greater than 2.

PROPOSITION 13. — *Suppose C is a curve over $\mathbb{F}_q$ whose Jacobian is isogenous to the product $A \times E$ of an abelian variety A with an elliptic curve E, and suppose that $s(A, E) < \infty$. Then there is an elliptic curve E' isogenous to E for which there is map from C to E' of degree dividing $s(A, E)$, and we have $\#C(\mathbb{F}_q) \leqslant s(A, E) \cdot \#E(\mathbb{F}_q)$.*

Proof. — By applying Lemma 7 we find that there are abelian

varieties A' and E', isogenous to A and E, respectively, and an exact sequence

$$0 \to \Delta' \to A' \times E' \to \operatorname{Jac} C \to 0$$

such that the projection maps $A' \times E' \to A'$ and $A' \times E' \to E'$ give monomorphisms from Δ' to $A'[s]$ and $E'[s]$, where $s = s(A, E)$. This implies that the composition $E' \to A' \times E' \to \operatorname{Jac} C$ is a monomorphism. Let λ and μ be the canonical principal polarizations on E' and $\operatorname{Jac} C$, respectively. Then the pullback of μ to E' is $n\lambda$ for some integer $n > 0$, and Lemma 7 says that the kernel of the pullback is isomorphic to Δ'. In particular we see that n must divide s. Thus we have a diagram

$$\begin{array}{ccccc} E' & \xrightarrow{n} & E' & \xrightarrow{\lambda} & \widehat{E'} \\ \downarrow & & \uparrow & & \uparrow \\ \operatorname{Jac} C & \xrightarrow{1} & \operatorname{Jac} C & \xrightarrow{\mu} & \widehat{\operatorname{Jac} C} \end{array}$$

where the vertical arrow on the right is the dual morphism of the vertical monomorphism $E' \to \operatorname{Jac} C$ on the left. From this we see that the composition $C \to \operatorname{Jac} C \to E'$ is a map of degree n. In particular,

$$\#C(\mathbb{F}_q) \leqslant n \cdot \#E'(\mathbb{F}_q) = n \cdot \#E(\mathbb{F}_q) \leqslant s \cdot \#E(\mathbb{F}_q).$$

□

COROLLARY 14. — *Let q be a prime power and let n be a positive integer. Let $m = \lfloor 2\sqrt{q} \rfloor$. If C is a curve over $\mathbb{F}_q$ of type $[m, \ldots, m, m-n]$, then the genus g of C satisfies*

$$g \leqslant \frac{(n-1)q - (n-1)^2 + nm}{m}.$$

Proof. — According to Proposition 13, there is an elliptic curve E' of defect n and a divisor d of n for which there is a degree-d map from C to E', and the number of points on C, which is $q + 1 + gm - n$, is at most n times the number of points on E', which is $q + 1 + m - n$. It follows from this inequality that

$$g \leqslant \frac{(n-1)q - (n-1)^2 + nm}{m}.$$

□

Now we turn to the proof of Theorem 2. Our proof relies on two facts: First, a prime p divides the resultant of two monic polynomials in $\mathbb{Z}[x]$ if and only if the reductions of the polynomials modulo p have a common

root in the algebraic closure of $\mathbb{F}_p$, and second, the ring $\mathbb{Z}[F,V]$ contains no nilpotent elements, so that if $\beta \in \mathbb{Z}[F,V]$ has minimal polynomial $m \in \mathbb{Z}[x]$, then the subring $Z[\beta]$ of $\mathbb{Z}[F,V]$ is isomorphic to $\mathbb{Z}[x]/(m)$.

Proof of Theorem 2. — Clearly $s(A_1,A_2)$ divides $r(F+V)$, because $s(A_1,A_2)$ is defined to be the greatest common divisor of a set of numbers that includes $r(F+V)$. What we must now prove is that if a prime p divides $r(F+V)$ then it also divides $s(A_1,A_2)$. To do this, we must show that for every α in $\mathbb{Z}[F,V]$ the prime p divides $r(\alpha)$.

Consider an α in $\mathbb{Z}[F,V]$, say $\alpha = u(F,V)$ for some polynomial $u \in \mathbb{Z}[x,y]$. Let F_1 and V_1 (resp. F_2 and V_2) be the Frobenius and Verschiebung endomorphisms of A_1 (resp. A_2). The fact that p divides $r(F+V)$ shows that there are homomorphisms $\psi_1 : \mathbb{Z}[F_1+V_1] \to \overline{\mathbb{F}}_p$ and $\psi_2 : \mathbb{Z}[F_2+V_2] \to \overline{\mathbb{F}}_p$ such that $\psi_1(F_1+V_1) = \psi_2(F_2+V_2)$. Let $\tau = \psi_1(F_1+V_1)$ and let σ be an element of $\overline{\mathbb{F}}_p$ such that $\sigma^2 - \tau\sigma + q = 0$. Then the homomorphisms ψ_1 and ψ_2 can be extended to give homomorphisms $\widehat{\psi}_1 : \mathbb{Z}[F_1,V_1] \to \overline{\mathbb{F}}_p$ and $\widehat{\psi}_2 : \mathbb{Z}[F_2,V_2] \to \overline{\mathbb{F}}_p$ such that $\widehat{\psi}_1(F_1) = \sigma = \widehat{\psi}_2(F_2)$ and $\widehat{\psi}_1(V_1) = \tau - \sigma = \widehat{\psi}_2(V_2)$. But then $\widehat{\psi}_1(u(F_1,V_1)) = \widehat{\psi}_2(u(F_2,V_2))$, so the minimal polynomials of $u(F_1,V_1)$ and $u(F_2,V_2)$ have a common root in $\overline{\mathbb{F}}_p$. It follows that $r(\alpha)$ is divisible by p. □

Using Theorem 1 and the corollaries established so far, we can now prove Theorem 3.

Proof of Theorem 3. — Suppose q is a square prime power, say $q = p^{2e}$ for a prime p. Of the types of defect-2 zeta-functions listed in [14], only two are possible when q is a square: namely $[m,\dots,m,m-1,m-1]$ and $[m,\dots,m,m-2]$. The first of these is impossible when $g > 2$ by Theorem 1(a), so the only possible defect-2 zeta function for $g > 2$ is $[m,\dots,m,m-2]$. To prove part (a), first assume that $p \neq 2$. Then it follows from Corollary 12 that this zeta function is not possible. If $p = 2$, then $m-2$ is not the trace of an elliptic curve when $q \neq 4$, so $[m,\dots,m,m-2]$ is not possible in that case either.

The proof of part (b) is essentially the same. From [18] we see that the only possible zeta function for a defect 3 curve when q is a square and $g > 3$ is $[m,\dots,m,m-3]$. (If $g = 3$, then $[m-1,m-1,m-1]$ may be possible; see [15].) If $p \neq 3$ then it again follows from Corollary 12 that this zeta function is not possible. If $p = 3$, then $m-3$ is not the trace of an elliptic curve when $q \neq 9$, so $[m,\dots,m,m-3]$ is not possible in that case either.

Now we prove parts (c) and (d). Using the methods of [22] (see also [14], §2) and the tables from [24], we see that for square q there are exactly eight possible types for a curve of genus g and defect 4 over $\mathbb{F}_q$. For each type, we list in Table 4 the associated real Weil polynomial h evaluated at $x - m$ (where $m = 2\sqrt{q}$) and the associated Weil polynomial f.

type $= [m, \ldots, m, m-4]$ $h(x-m) = x^{g-1} \cdot (x-4)$ $f(x) = (x+\sqrt{q})^{2g-2} \cdot (x^2 + (m-4)x + q)$
type $= [m, \ldots, m, m-2, m-2]$ $h(x-m) = x^{g-2} \cdot (x-2)^2$ $f(x) = (x+\sqrt{q})^{2g-4} \cdot (x^2 + (m-2)x + q)^2$
type $= [m, \ldots, m, m-1, m-1, m-2]$ $h(x-m) = x^{g-3} \cdot (x-1)^2 \cdot (x-2)$ $f(x) = (x+\sqrt{q})^{2g-6} \cdot (x^2 + (m-1)x + q)^2 \cdot (x^2 + (m-2)x + q)$
type $= [m, \ldots, m, m-(2-\sqrt{2}), m-(2+\sqrt{2})]$ $h(x-m) = x^{g-2} \cdot (x^2 - 4x + 2)$ $f(x) = (x+\sqrt{q})^{2g-4} \cdot (x^4 + (2m-4)x^3 + (6q-4m+2)x^2 + (2m-4)qx + q^2)$
type $= [m, \ldots, m, m-1, m-1, m-1, m-1]$ $h(x-m) = x^{g-4} \cdot (x-1)^4$ $f(x) = (x+\sqrt{q})^{2g-8} \cdot (x^2 + (m-1)x + q)^4$
type $= [m, \ldots, m, m-1, m-(3-\sqrt{5})/2, m-(3+\sqrt{5})/2]$ $h(x-m) = x^{g-3} \cdot (x-1) \cdot (x^2 - 3x + 1)$ $f(x) = (x+\sqrt{q})^{2g-6} \cdot (x^2 + (m-1)x + q) \cdot$ $(x^4 + (2m-3)x^3 + (6q-3m+1)x^2 + (2m-3)qx + q^2)$
type $= [m, \ldots, m, m-(2-\sqrt{3}), m-(2+\sqrt{3})]$ $h(x-m) = x^{g-2} \cdot (x^2 - 4x + 1)$ $f(x) = (x+\sqrt{q})^{2g-4} \cdot (x^4 + (2m-4)x^3 + (6q-4m+1)x^2 + (2m-4)qx + q^2)$
type $= [m, \ldots, m, m-1, m-3]$ $h(x-m) = x^{g-2} \cdot (x-1) \cdot (x-3)$ $f(x) = (x+\sqrt{q})^{2g-4} \cdot (x^2 + (m-1)x + q) \cdot (x^2 + (m-3)x + q)$

TABLE 4. The possible types of defect-4 curves over square fields, together with the associated real Weil polynomial h evaluated at $x - m$ and the associated Weil polynomial f.

Suppose that $g > (3q+4m-9)/m$, where $m = 2\sqrt{q}$. Then Corollary 14 shows that the first entry in the table cannot occur. Also, since the inequality we are assuming implies that $g > (q + 4m - 3)/m$ as well, Theorem 1(b) and Lemma 8(a) can be used to show that the second and fourth entries cannot occur. We also see that $g > (q + 2m + 3)/m$, so

Theorem 1(b) and Lemma 8(a) show that the eighth entry cannot occur. Finally, Theorem 1(a) shows that the remaining entries cannot occur when $g > 4$. This proves part (c).

Finally, suppose $q = 2^{2e}$ with $e > 2$, and suppose $g > 2^{e-1} + 2 > 5$. Then the first four entries listed in Table 4 cannot occur because the Honda-Tate theorem [29] shows the final factor of each of the putative Weil polynomials is not in fact a Weil polynomial. (A simple way to check this is to use [4], Lem. 3.1.2.) The next three entries cannot occur when $g > 4$ because of Theorem 1(a), as we have noted already. That leaves us with the final entry. Once again Theorem 1(b) and Lemma 8(a) can be used to eliminate this possibility, because we have $g > 2^{e-1} + 2$. □

3. Exceptional prime powers.

In this section we will prove Theorem 4, Proposition 5, and Corollary 6. Before we begin, let us define the *trace* of a monic degree-n polynomial in $\mathbb{Q}[x]$ to be -1 times the coefficient of x^{n-1}, and the *deficiency* of such a polynomial to be its trace minus its degree.

Proof of Theorem 4. — Let C be a curve of genus g over $\mathbb{F}_q$ and let $h \in \mathbb{Z}[x]$ be its real Weil polynomial. We know that all of the roots of h are real numbers in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, and the number of points on C is equal to $q+1-t$, where t is the trace of h. Write $h = (x+m)^e h_2$, where h_2 has no factors of $(x+m)$. The factor $(x+m)^e$ of h corresponds to the largest isogeny factor of $\operatorname{Jac} C$ on which Frobenius acts as $-m$, and up to isogeny this factor must be a power of the smallest abelian variety over $\mathbb{F}_q$ whose real Weil polynomial is a power of $x+m$. Thus, the exponent e is a multiple of the defect-0 dimension δ of $\mathbb{F}_q$, and we see that the degree g_2 of h_2 is congruent to g modulo δ.

Define $H \in \mathbb{Z}[x]$ by $H(x) = h(x-m-1)$, so that $H = (x-1)^e H_2$ for a polynomial H_2 of degree g_2 that has no factors of $x-1$. All of the roots of H are positive real numbers, and the number of points on C is $q+1-T+gm+g$, where T is the trace of H. The trace T_2 of H_2 is equal to $T-e$, and the degree of h_2 is equal to $g-e$, so we have

$$\#C(\mathbb{F}_q) = q+1+gm-T_2+g_2.$$

In other words, the defect of the curve C is $T_2 - g_2$, which is the deficiency of the polynomial H_2.

Now, all of the roots of H_2 are positive real numbers, and H_2 has no factors of $x-1$, so a result of Siegel [23] says that the trace of H_2 is at least $3/2$ times its degree. It follows that the deficiency of H_2 is at least half its degree. Thus, the defect of C is at least $g_2/2$. We already noted that g_2 is congruent to g modulo δ, so the defect of C is at least $r/2$, where $r \in [0, \delta)$ is the remainder obtained when dividing g by δ. □

Proof of Proposition 5. — If f is a monic irreducible polynomial in $\mathbb{Z}[x]$ whose roots in the complex plane all have magnitude $\sqrt{q}$, then there is an exponent e such that f^e is the Weil polynomial of a simple abelian variety over $\mathbb{F}_q$. The Honda-Tate theorem [29] includes a recipe for calculating this exponent. Proposition 5 is obtained by applying this recipe to either the polynomial x^2+mx+q (if q is not a square) or the polynomial $x+\sqrt{q}$ (if q is a square). We leave the details to the reader. □

The essence of the following argument appears in [22].

Proof of Corollary 6. — Consider the expression for $\sqrt{2}$ in base 2:

$$\sqrt{2} = b_0 + \frac{b_1}{2} + \frac{b_2}{2^2} + \frac{b_3}{2^3} + \cdots$$

where each b_i is either 0 or 1. Suppose $e > 0$ is an integer such that $b_e = 1$ and $b_{e+1} = 0$. Let $q = 2^{2e+1}$. Then the base-2 expression for $2\sqrt{q}$ is

$$2\sqrt{q} = b_0 2^{e+1} + b_1 2^e + \cdots + b_e 2 + b_{e+1} + \frac{b_{e+2}}{2} + \ldots,$$

so the base-2 expression for $m = [2\sqrt{q}]$ is

$$m = b_0 2^{e+1} + b_1 2^e + \cdots + b_e 2 + b_{e+1}.$$

Clearly m is even but not a multiple of 4, so if ν is the usual additive 2-adic valuation of $\mathbb{Q}$ we have $\nu(m) = 1$ and $\nu(q) = 2e+1$. It follows from Proposition 5 that the defect-0 dimension of q is equal to $2e+1$. If we take $g \leqslant 2e$, then Theorem 4 shows that the defect of a genus-g curve over $\mathbb{F}_q$ is at least $g/2$.

Thus, to prove Corollary 6 we need only show that there are infinitely many e with $b_e = 1$ and $b_{e+1} = 0$. But there are only two ways in which there could not be infinitely many such e: either $b_i = 0$ for all sufficiently large i, or $b_i = 1$ for all sufficiently large i. Neither of these can occur, because $\sqrt{2}$ is irrational. □

If p is a prime for which the real number $\sqrt{p}$ is normal in base p — a condition one expects every prime to satisfy — then a similar argument shows that there are infinitely many exceptional powers of p.

4. Improved bounds.

In this section we will explain how we obtained the improvements listed in Tables 1 and 2. Some of the entries in the table are immediate consequence of the corollaries in Section 2, but other entries require a more detailed analysis. We have written a Magma program that carries out some of this analysis for us; let us begin by explaining what the program does.

Given a prime power q and two positive integers g and N, we want to determine, if we can, whether there exists a curve of genus g over $\mathbb{F}_q$ with N rational points. Our program enumerates all of the polynomials that might possibly be the real Weil polynomial h of such a curve, where by "might possibly" we mean that

- all of the roots of h are real numbers in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, and
- the number of places of degree d (for $d = 1, \ldots, g$) predicted by h are non-negative and in accord with the Weil-Serre bounds.

The enumeration is carried out in one of two ways: If the value of N corresponds to a defect of 6 or less, the program uses precomputed tables of totally positive polynomials of deficiency at most 6 (calculated as in [24]) to list all of the appropriate polynomials. Otherwise, the program uses the algorithm from [13] to compute the appropriate h's. For each candidate h, the program then uses the criterion of [29] to determine whether h actually is the real Weil polynomial of an isogeny class of abelian varieties over $\mathbb{F}_q$. For each h that is a real Weil polynomial, the program uses the factorization of h to loop through all of the splittings of the associated isogeny class into a product of lower-dimensional isogeny classes. It then computes the value of $r(F + V)$ for each such splitting. If $r(F + V) = 1$ then we know from Theorem 1(a) that there is no curve with h as its real Weil polynomial. If $r(F + V) = 2$ then the program tries to use Theorem 1(b) and Lemma 8 to show that there is no curve with the given real Weil polynomial. (The program only uses Lemma 8(a) with $d = 1$, and it only uses Lemma 8(c) with all of the d_i less than or equal to g.) If one of the isogeny classes in the splitting is an isogeny class of elliptic curves and if the conclusion of Proposition 13 is not satisfied, then again we know that there is no curve with the given real Weil polynomial. If a polynomial h is not eliminated by these filters, the program flags it as such and prints out three items:

(1) The number of places of degree d (for $d = 1, \ldots, g$) that a curve would have to have in order to have h for its real Weil polynomial,

(2) the factorization of h, and

(3) a matrix giving the resultants of each pair of prime factors of h.

Likewise, if a polynomial h *is* eliminated, the program will print out item (2) above, together with an explanation of why it eliminated the polynomial. The program will also print out item (1) if it had to calculate that information in order to eliminate the polynomial.

For some specific choices of q, g, and N, our program eliminates all possible real Weil polynomials. For other choices there are only a few real Weil polynomials left to consider, and sometimes we can eliminate these by other methods; see Sections 5, 6, 7, and 8 for examples of some of these methods.

Throughout this section, the symbol m will always stand for the integer $[2\sqrt{q}]$, where q is the prime power currently under discussion.

It was proven in [22] (see also [14], Prop. 2) that defect-1 curves are never possible when the genus is bigger than 2. We will frequently use this fact without comment.

4.1. Improvements for $q = 4$.

The case $q = 4$, $g = 5$, $N = 18$. — We ran our Magma program for the case $q = 4$, $g = 5$, $N = 18$. The output is reproduced in the Appendix. The program finds eight polynomials h that might possibly be real Weil polynomials for a genus-5 curve over $\mathbb{F}_4$ with 18 points. The first of the eight possibilities turns out not to be a real Weil polynomial; it fails the local criterion given in [29].

The second, fourth, fifth, seventh, and eighth possibilities are eliminated by Theorem 1(a). For example, for the fifth possibility, the program finds that h factors as $(x+2)^2(x+4)(x^2+5x+5)$. If we let h_1 be the product of the first and second of these factors (as the line

```
Splitting = [ 1, 2 ]
```

in the output indicates we should do) and if we let h_2 be the third factor, then the resultant of the radical of h_1 and the radical of h_2 is 1.

The third and sixth possibilities are eliminated by Theorem 1(b) and Lemma 8. For example, the polynomial h for the third possibility is $(x+1)(x+2)(x+3)^2(x+4)$. We can factor this as h_1h_2 where $h_1 = (x+2)$

and $h_2 = (x+1)(x+3)^2(x+4)$, and then the resultant of the radicals of h_1 and h_2 is 2. Thus Theorem 1(b) shows that any curve with h as its real Weil polynomial would have to be a double cover of a curve D whose real Weil polynomial is either h_1 or h_2. But if D had h_1 as its real Weil polynomial then it would have 7 points, and this would contradict Lemma 8(a) with $d = 1$; while if D had h_2 as its real Weil polynomial then it would have genus 4, and this would contradict Lemma 8(b). This argument is summarized in the lines

```
Splitting = [ 2 ]
Reasons: point counts, Riemann-Hurwitz
```

of the output.

So we see that there is no genus 5 curve over $\mathbb{F}_4$ with 18 points. A curve with 17 points is known, so we obtain the first entry in Table 3.

The cases $q = 4$, $g \in \{10, 11\}$. — The improvements listed in Table 1 for $q = 4$ and $g \in \{10, 11\}$ come from running our program. Note that a curve over $\mathbb{F}_4$ of genus 10 with 27 points is known, so we get the second entry in Table 3.

4.2. Improvements for $q = 8$.

The cases $q = 8$, $g = 5$, $N = 32$ and 31. — Our program shows that no genus-5 curve over $\mathbb{F}_8$ can have exactly 32 points.

The case $N = 31$ is more interesting. Our program shows that if C is a genus-5 curve over $\mathbb{F}_8$ with 31 points, then its real Weil polynomial must be

$$h = (x+5)^3(x^2+7x+8).$$

The resultant of $x+5$ and x^2+7x+8 is 2, so C is a double cover of a curve D whose real Weil polynomial is either $(x+5)^3$ or x^2+7x+8. If D had $(x+5)^3$ for its real Weil polynomial then D would have genus 3, and this would contradict Lemma 8(c) since C has an odd number of rational points. Thus the real Weil polynomial of D must be x^2+7x+8.

We see that the Weil polynomial of C must be

$$f_C = (x^2+5x+8)^3(x^4+7x^3+24x^2+56x+64)$$

and the Weil polynomial of D must be

$$f_D = x^4 + 7x^3 + 24x^2 + 56x + 64.$$

In Section 5 we will use a Galois descent argument to show that this cannot occur.

The cases $q = 8$, $g = 9$, $N = 47$ and 46. — Our program shows that a genus-9 curve over $\mathbb{F}_8$ cannot have exactly 47 points, and that if such a curve has exactly 46 points then its real Weil polynomial is either $(x+3)(x+4)^3(x+5)^3(x^2+7x+9)$ or $(x+3)^4(x+5)^5$. We will consider each of these two possibilities in turn.

Suppose C is a genus-9 curve over $\mathbb{F}_8$ with real Weil polynomial

$$h = (x+3)(x+4)^3(x+5)^3(x^2+7x+9).$$

Since the resultant of $x+5$ and $(x+3)(x+4)(x^2+7x+9)$ is 2, the curve C must be a double cover of a curve D over $\mathbb{F}_8$ whose real Weil polynomial is either $(x+5)^3$ or $(x+3)(x+4)^3(x^2+7x+9)$. The second option would require D to have larger genus than is allowed by Lemma 8(b), so D must have real Weil polynomial $(x+5)^3$. In particular, D must have exactly 24 places of degree 1.

We see from the real Weil polynomial of C that C has no places of degree 2. In particular, no rational places of D can be inert in the double cover $C \to D$. Since C has 46 rational places, it must be the case that 22 of the 24 rational places of D split in the cover $C \to D$ and the other 2 rational places ramify.

We also see from the real Weil polynomial of C that C has 109 places of degree 3. As we argued in the proof of Lemma 8, the fact that C has an odd number of degree-3 places implies that at least one degree-3 place of D ramifies. Thus, at least 5 geometric points of D ramify in the double cover $C \to D$. Since the ramification is necessarily wild, each ramification point contributes at least 2 to the degree of the different of the cover, which means that the degree of the different is at least 10. But the Riemann-Hurwitz formula shows that the degree of the different of the double cover $C \to D$ is equal to 8. This contradiction shows that there is no genus-9 curve over $\mathbb{F}_8$ with $(x+3)(x+4)^3(x+5)^3(x^2+7x+9)$ for its real Weil polynomial.

Suppose C is a genus-9 curve over $\mathbb{F}_8$ with real Weil polynomial $(x+3)^4(x+5)^5$. Since the resultant of $x+3$ and $x+5$ is 2, the curve C must be a double cover of a curve D whose real Weil polynomial is either $(x+3)^4$ or $(x+5)^5$. But the first option is impossible, because in that case

D would have only 21 rational points, which contradicts Lemma 8(a). The second option is impossible as well, because in that case the genus-5 curve D would have 34 rational points, whereas we know that $N_8(5) \leqslant 30$.

Thus there are no genus-9 curves over $\mathbb{F}_8$ with 46 points. A curve with 45 points is known, so we get the third entry in Table 3.

The cases $q = 8$, $g \in \{7, 8, 10, 11, 15\}$. — The improvements we get when $q = 8$ and $g \in \{7, 8, 10, 11, 15\}$ can all be obtained by running our program.

4.3. Improvements for $q = 16$.

The cases $q = 16$, $g \in \{4, 5, 7\}$. — These improvements come directly from Theorem 3(b). Since a genus-4 curve over $\mathbb{F}_{16}$ with 45 points is known, we obtain the fourth entry in Table 3.

The cases $q = 16$, $g \in \{8, 11, 13, 14\}$. — The improvements we list in these cases are all obtained by running our program.

4.4. Improvements for $q = 32$.

The case $q = 32$, $g = 4$, $N = 75$. — Suppose C is a genus-4 curve over $\mathbb{F}_{32}$ with exactly 75 rational points. Then C has defect 2, so it must be of one of the seven types listed in [14]. The type $[m, m, m-1, m-1]$ is forbidden by Theorem 1(a), and the fractional part of $2\sqrt{32}$ is small enough to eliminate five of the others. Thus C must have type $[m, m, m, m-2]$, where $m = [2\sqrt{32}] = 11$. Theorem 1 tells us that C must be a double cover of either a genus-3 curve (which is impossible, by Lemma 8(b)) or of an elliptic curve whose Weil polynomial is $x^2 + (m-2)x + 32 = x^2 + 9x + 32$. In Section 6.2 we will show how the set of all genus-4 double covers of such elliptic curves can be enumerated. We will see that none of the curves has 75 points.

The cases $q = 32$, $5 \leqslant g \leqslant 15$. — For $q = 32$ and $g \geqslant 3$, a Galois descent argument [14] shows that the Weil-Serre upper bound cannot be met, and the previously-known best upper bound for $3 \leqslant g \leqslant 15$ was

$q+1+gm-2$. As we saw above, the only possible defect-2 zeta function is of type $[m,\dots,m,m-2]$. However, Corollary 9 rules out this type of zeta function when $g \geqslant 5$, so defect 2 is impossible when $g \geqslant 5$.

Likewise, the arguments from the appendix of [18] show that for $g \geqslant 9$ the only possible defect-3 zeta function for $q = 32$ is of type $[m,\dots,m,m-3]$. (This also depends on the fact that the fractional part of $2\sqrt{32}$ is relatively small.) But Corollary 14 shows that then $g \leqslant 8$, so defect 3 is impossible when $g \geqslant 9$. Thus our new upper bound is $q+1+gm-3$ for $5 \leqslant g \leqslant 8$, and is $q+1+gm-4$ for $9 \leqslant g \leqslant 15$.

4.5. Improvements for $q = 64$.

The cases $q = 64$, $11 \leqslant g \leqslant 27$, $g \neq 12$. — If $g = 11$, then a curve meeting the Weil-Serre bound is not possible due to the results of Korchmaros-Torres [9]. Defect 2 is also impossible, by Corollary 10.

We know from [5] that there is also no defect-0 curve when $13 \leqslant g \leqslant 27$, and it was shown in [14] that defect 2 is ruled out by the Honda-Tate theorem. But Theorem 3 shows that defects 3 and 4 are not possible either, so we get an upper bound of $q+1+gm-5$.

4.6. Improvements for $q = 128$.

Apart from the case $g = 9$ and $N = 324$ (explained below), all of our improved bounds for $q = 128$ can be obtained by running our program. However, we will take some time here to indicate how the structure apparent in the $q = 128$ results is a consequence of the fact that 128 is exceptional (in the terminology of Section 3). To simplify our discussion, let us introduce some terminology.

Suppose h is a monic irreducible polynomial in $\mathbb{Z}[x]$, all of whose roots in $\mathbb{C}$ are real and have magnitude at most $2\sqrt{q}$. By the Honda-Tate theorem there is an integer $e > 0$ such that a power h^n of h is the real Weil polynomial of an abelian variety over $\mathbb{F}_q$ if and only if n is divisible by e. We will say that h^e is an *elementary* real Weil polynomial. For example, the polynomial $(x+22)^7$ is an elementary real Weil polynomial over $\mathbb{F}_{128}$.

We define the *defect* of a real Weil polynomial h over $\mathbb{F}_q$ to be $m \deg h + \operatorname{trace} h$, where the trace of a polynomial is as defined in Section 3.

Note that if C is a curve over $\mathbb{F}_q$ of defect d then its real Weil polynomial has defect d. Also, the defect of a product of real Weil polynomials is the sum of the defects.

Suppose $h \in \mathbb{Z}[x]$ is the real Weil polynomial of a curve C over $\mathbb{F}_q$. Let $H(x) = h(x - m - 1)$, so that all of the roots of H are positive real numbers. One checks that the defect of h is the deficiency of H, as defined in Section 3. Smyth [24] has written down all irreducible monic polynomials H in $\mathbb{Z}[x]$ with totally positive roots and with deficiency at most 6, and using Smyth's work and the Honda-Tate theorem it is not hard to write down a list of all of the elementary real Weil polynomials h over $\mathbb{F}_q$ with defect at most 6. (A Magma program to reproduce Smyth's work is available at the URL mentioned in the acknowledgments.)

There is only one elementary real Weil polynomial of defect 0, namely $(x+m)^\delta$, where δ is the defect-0 dimension of q. Let us say that a real Weil polynomial over $\mathbb{F}_q$ is *minimal* if it is coprime to $x + m$. Given the list of elementary real Weil polynomials over F_q of defect at most 6, it is a simple matter to make a list of all of the minimal real Weil polynomials over $\mathbb{F}_q$ of defect at most 6.

Now suppose one is interested in genus-g curves C over $\mathbb{F}_q$ with defect $d \leqslant 6$. The real Weil polynomial of C must be of the form $(x+m)^n h$, where h is a minimal real Weil polynomial of defect d. As we just noted, one can easily list these polynomials; the task is made even simpler by the fact that only h of certain degrees can occur, since $n = g - \deg h$ must be a multiple of the defect-0 dimension of q. Furthermore, one can use Theorem 1(a) to exclude certain polynomials $(x + m)^n h$.

For instance, consider the case where $q = 128$ and $g \equiv 2 \bmod 7$, with $g > 2$. There can be no defect-0 curves of genus g because the defect-0 dimension of q is 7. There are no defect-1 real Weil polynomials because we took $g > 2$. The only possible defect-2 polynomials are $y^{g-2}(y-1)^2$ and $y^{g-2}(y^2 - 2y - 1)$, where $y = x + m$, but these are eliminated by Theorem 1(a). The possible defect-3 polynomials are $y^{g-2}(y^2 - 3y + 1)$ and $y^{g-2}(y^2 - 3y - 1)$ and $y^{g-2}(y^2 - 3y - 2)$. The first two are eliminated by Theorem 1(a), and when $g > 9$ the third is eliminated by Theorem 1(b) and Lemma 8. The possible defect-4 polynomials are $y^{g-2}(y^2 - 4y - 1)$ and $y^{g-2}(y^2 - 4y + 1)$ and $y^{g-2}(y-1)(y-3)$. The first two are eliminated by Theorem 1(a), and when $g \geqslant 9$ the third is eliminated by Theorem 1(b) and Lemma 8. For defect 5 there are several possible polynomials that we cannot eliminate using our theorems. Combining all of the above, we see

that when $g > 9$ is congruent to 2 mod 7, we have $N_{128}(g) \leqslant q+1+mg-5$. A similar analysis can be done for the other congruence classes modulo 7.

There is a known curve of genus 4 over $\mathbb{F}_{128}$ with 215 rational points, so we obtain the fifth entry in Table 3.

The case $q = 128$, $g = 9$, $323 \leqslant N \leqslant 327$. — The defect-0 dimension of q is 7, so there is no defect-0 curve of genus 9. Defect 1 is impossible because $g > 2$. The cases $N = 325$ and $N = 323$ are eliminated by our program. The only case remaining is $N = 324$.

Our program shows that a genus-9 curve C over $\mathbb{F}_{128}$ with 324 points would have to have real Weil polynomial $(x+22)^7(x^2+41x+416)$ and would have to be a double cover of a genus-2 curve D with real Weil polynomial $x^2+41x+416$. From their real Weil polynomials, we see that C and D each have 2-rank 1; that is, the $\mathbb{F}_2$-dimension of the geometric 2-torsion of their Jacobians is 1. But then the Deuring-Shafarevich formula (see [28] and the references listed in [2], §3) shows that the double cover $C \to D$ must be unramified, which is clearly impossible.

4.7. Improvements for $q = 3$.

The case $q = 3$, $g = 6$, $N = 15$. — Running our program on this case leaves us with three real Weil polynomials to consider.

The first is $(x+2)^2(x+3)(x^3+4x^2+x-3)$. Factoring this as $(x+3)$ times $(x+2)^2(x^3+4x^2+x-3)$ and applying Proposition 13, we find that a curve with this real Weil polynomial must be a triple cover of an elliptic curve with Weil polynomial x^2+3x+3. We will show in Section 7.3 that no such triple cover can have 15 points.

The second real Weil polynomial we must consider is $(x+2)^2(x^2+3x-1)(x^2+4x+2)$. Factoring this as (x^2+4x+2) times $(x+2)^2(x^2+3x-1)$ and applying Theorem 1(b), we find that a curve with this real Weil polynomial must be a double cover of a genus-2 curve with real Weil polynomial (x^2+4x+2). Searching through the genus-2 curves over $\mathbb{F}_3$, we find that there is exactly one curve with that real Weil polynomial; it is given by the equation $y^2 = x^6+x^5+x^4+x^2-x+1$. In Section 6.3 we will show that there is no genus-6 double cover of this curve with 15 points.

The third real Weil polynomial we are left to consider is $(x+1)^2(x+3)^2(x^2+3x-1)$. Writing this polynomial as the product of $(x+3)^2$ and

$(x+1)^2(x^2+3x-1)$ and applying Theorem 1(b), we find that a curve C with this real Weil polynomial must be a double cover of a genus-2 curve with real Weil polynomial $(x+3)^2$. Such a genus-2 curve would have 10 rational points — but this is impossible, because $N_3(2) = 8$.

Thus there is no genus-6 curve over $\mathbb{F}_3$ with 15 rational points. A curve with 14 points is known, so we obtain the sixth entry in Table 3.

4.8. Improvements for $q = 9$.

The case $q = 9$, $g = 13$, $N = 66$. — Running our program shows that the only possible real Weil polynomial in this case is $(x+2)(x+4)^6(x+5)^6$. Writing this polynomial as the product of $(x+4)^6$ with $(x+2)(x+5)^6$ and applying Theorem 1(b), we see that a genus-13 curve C over $\mathbb{F}_9$ with 66 points must be a double cover of a curve D such that either

(1) the curve D has 34 rational points and has genus 6, and the double cover $C \to D$ is ramified at 4 geometric points, or

(2) the curve D has 42 rational points and has genus 7, and the double cover $C \to D$ is unramified.

We note that the real Weil polynomial of C shows that it has no places of degree 2, so that no rational point of D can be inert in the double cover $C \to D$, and so that every degree-2 place of D must be inert in $C \to D$.

Suppose D has genus 6. Since D has 34 rational points and none of them are inert in $C \to D$, and since C has 66 rational points, we see that exactly 2 rational points of D are ramified. Since there are 4 geometric ramification points, a degree-2 place of D must ramify as well — but we have just seen that every degree-2 place of D must be inert, a contradiction.

Suppose D has genus 7. Since no rational point of D can be inert or ramified in the double cover $C \to D$, each of the 42 rational points of D must split. But then C would have to have 84 rational points, contradicting the fact that it has only 66.

Thus neither of the two possibilities listed above can hold, and there can be no genus-13 curve over $\mathbb{F}_9$ with 66 points.

The cases $q = 9$, $g \in \{9, 10, 11, 12, 14, 15, 16, 17, 18\}$. — The improvements listed in Table 2 for $q = 9$ and $g \in \{9, 10, 11, 12, 14, 15, 16, 17, 18\}$ can all be obtained simply by running our program. Note that there

is a known genus-10 curve over $\mathbb{F}_9$ with 54 points, so we get the seventh entry in Table 3.

4.9. Improvements for $q = 27$.

The cases $q = 27$, $g = 4$, $N = 66$ and $N = 65$. — Suppose C is a genus-4 curve over $\mathbb{F}_{27}$ with exactly 66 rational points. Then C has defect 2, and of the seven types of zeta function from [14] one is eliminated by Theorem 1(a) and five more are forbidden by the size of the fractional part of $2\sqrt{27}$. The only possibility remaining is $[m, m, m, m-2]$, where $m = [2\sqrt{27}] = 10$. Theorem 1(b) tells us that C must be a double cover of either a genus-3 curve (which is impossible, by Lemma 8(b)) or of an elliptic curve whose Weil polynomial is $x^2 + (m-2)x + 27 = x^2 + 8x + 27$. In Section 6.1 we will show how the set of all genus-4 double covers of such elliptic curves can be enumerated. We will see that none of the curves has 66 points.

Suppose C is a genus-4 curve over $\mathbb{F}_{27}$ with exactly 65 rational points. Then C has defect 3, and using the results of the appendix to [18] we find that C must be of type $[m, m, m, m-3]$. Then Proposition 13 shows that C must be a triple cover of an elliptic curve whose Weil polynomial is $x^2 + 7x + 27$. In Section 7.4 we will show how the set of all genus-4 triple covers of such elliptic curves can be enumerated. We will see that none of the curves has 65 points.

A genus-4 curve over $\mathbb{F}_{27}$ with 64 points is known, so we obtain the eighth entry in Table 3.

The cases $q = 27$, $5 \leqslant g \leqslant 13$. — First we note that [14], Thm. 1, shows that the Weil-Serre bound cannot be met when $g \geqslant 3$.

Now we show that defect 2 is impossible for $g \geqslant 5$. For $g > 5$ this follows from Corollary 10. When $g = 5$ Corollary 9 shows that $[m, m, m, m, m-2]$ is not a possible type, and the proof of Corollary 10 shows that the only other possible type is $[m, m, m, m+\sqrt{3}-1, m-\sqrt{3}-1]$. But this last type is also impossible, because the fractional part of $2\sqrt{27}$ is less than $\sqrt{3} - 1$.

Finally we note that the Appendix to [18] shows that the only defect-3 curves over $\mathbb{F}_{27}$ when $g \geqslant 9$ are of type $[m, \ldots, m, m-3]$, and Corollary 14 shows that this type is impossible for $g \geqslant 9$.

The case $q = 27$, $g = 14$, $N = 164$. — Our program eliminates this possibility.

4.10. Improvements for $q = 81$.

The cases $q = 81$, $13 \leqslant g \leqslant 35$, $g \neq 16$. — From [5] and [9], we know that no defect-0 curves are possible for $13 \leqslant g \leqslant 35$, $g \neq 16$. But defect 2 and 3 are not possible either by Theorem 3, so the upper bound for these cases is at most $q + 1 + gm - 4$. When $g \geqslant 18$ we see from Theorem 3(c) that defect 4 is impossible as well, so our new upper bound for $18 \leqslant g \leqslant 35$ is $q + 1 + gm - 5$.

4.11. Cases where few Weil polynomials are possible.

We have tried to use our program to obtain further improvements to the upper bounds listed in the van der Geer-van der Vlugt tables, but it appears that we have already picked most of the low-hanging fruit. For example, for every q listed in the tables, and for every $g \leqslant 10$, we have taken the best current upper bound N for $N_q(g)$ and run our program on the triple (q, g, N). In each such case, our program indicates that there are real Weil polynomials that are not eliminated by the criteria that we built into the program. This is not to say, however, that our methods cannot give further improvements in these cases: For instance, for $q = 27$ and $5 \leqslant g \leqslant 8$, a curve meeting the best current upper bound would have to be a triple cover of a defect-3 elliptic curve, and by using methods as in Section 7 it should be possible to enumerate all such triple covers.

We mention just two more interesting cases. The smallest genus g for which $N_2(g)$ is not known is $g = 12$; it is known that $N_2(12)$ is either 14 or 15. Running our program on the case $q = 2$, $g = 12$, $N = 15$ took almost 18 hours using Magma 2.8 on a 2 GHz Pentium 4, and we found that there are eight possible real Weil polynomials to consider. We were unable to eliminate all of these polynomials, and we were not able to use them to direct a search for a genus-12 curve with 15 points.

On the other hand, running our program on the case $q = 4$, $g = 7$, $N = 22$ produces six candidate real Weil polynomials, and by a number of *ad hoc* arguments we were able to eliminate all but one of them from

consideration. We find that if a genus-7 curve over $\mathbb{F}_4$ has 22 points, then its real Weil polynomial must be $x(x+2)^2(x+3)^3(x+4)$. We have not yet been able to eliminate this possibility.

5. A Galois descent argument.

In Section 4.2 we showed that a genus-5 curve C over $\mathbb{F}_8$ having exactly 31 points must be a double cover of a genus-2 curve D. In this section we will use a Galois descent argument to show that the curves C and D and the degree-2 map $C \to D$ can all be defined over $\mathbb{F}_2$, and we will show how this leads to a contradiction.

Let $f_2 = x^4 + x^3 + 2x + 4$ and let $g_2 = x^2 - x + 2$. Let π be a root of f_2 in $\overline{\mathbb{Q}}$ and ρ be a root of g_2 in $\overline{\mathbb{Q}}$. Let

$$f_8 = x^4 + 7x^3 + 24x^2 + 56x + 64 \quad \text{and} \quad g_8 = x^2 + 5x + 8.$$

Note that π^3 is a root of f_8 and that ρ^3 is a root of g_8. The arguments from Section 4.2 show that it will suffice for us to prove the following:

PROPOSITION 15. — *There is no genus-5 curve over $\mathbb{F}_8$ with Weil polynomial $f_8 g_8^3$.*

Proof. — We know from Section 4.2 that any such curve must be a double cover of a genus-2 curve D with Weil polynomial f_8. Let us first identify the curve D.

CLAIM. — *There is exactly one principally polarized abelian surface over $\mathbb{F}_8$ with Weil polynomial equal to f_8. It is the polarized Jacobian of the curve $y^2 + xy = x^5 + x$.*

Proof. — Every such principally-polarized variety is a Jacobian, because the varieties in the isogeny class determined by f_8 are absolutely simple (see [8], Thm. 6). By explicitly enumerating the genus-2 curves over $\mathbb{F}_8$ one finds that the curve given above is the only curve whose Jacobian has Weil polynomial f_8. □

Suppose, to get a contradiction, that C is a genus-5 curve over $\mathbb{F}_8$ with Weil polynomial $f_8 g_8^3$. Since the resultant of the real Weil polynomials associated with f_8 and g_8 is 2, Lemma 7 shows that there is an exact sequence

$$0 \to \Delta \to A \times B \to \operatorname{Jac} C \to 0,$$

where A and B are abelian varieties over $\mathbb{F}_8$ with Weil polynomials f_8 and g_8^3, respectively, and where the projections $A \times B \to A$ and $A \times B \to B$ induce monomorphisms $\Delta \hookrightarrow A[2]$ and $\Delta \hookrightarrow B[2]$. Since $\operatorname{Jac} C$ is a Jacobian and hence has a principal polarization, Lemma 7 shows that Δ is self-dual. Furthermore, Δ is nontrivial, because the principal polarization on $\operatorname{Jac} C$ is indecomposable.

Every finite group-scheme G in characteristic p can be written as a product of four sub-group-schemes:

$$G = G_{\mathrm{red,red}} \times G_{\mathrm{red,loc}} \times G_{\mathrm{loc,red}} \times G_{\mathrm{loc,loc}},$$

where $G_{\mathrm{red,red}}$ is a reduced group-scheme whose Cartier dual is reduced, where $G_{\mathrm{red,loc}}$ is a reduced group-scheme whose Cartier dual is local, and so on. (See [17], §I.2.) A group-scheme of p-power rank in characteristic p can have no reduced-reduced part. Furthermore, if G is self-dual — for example, if G is the kernel of a polarization — then $G_{\mathrm{red,loc}}$ and $G_{\mathrm{loc,red}}$ are dual to one another.

Now, B is an ordinary abelian variety, and the kernel of multiplication-by-p on an ordinary abelian variety in characteristic p has no local-local part. Thus $B[2]$ consists of a reduced-local factor of rank 8 and a local-reduced factor of rank 8.

The variety A is not ordinary, so $A[2]$ has a local-local component. However, A has positive 2-rank, so $A[2]$ has a reduced-local component as well. The only possibility is that $A[2]$ has a reduced-local component of rank 2, a local-reduced component of rank 2, and a local-local component of rank 4.

There are supposed to be monic maps from Δ to $A[2]$ and to $B[2]$. Since Δ can be viewed as a subscheme of $B[2]$ it can have no local-local part. Thus, the monomorphism $\Delta \to A[2]$ must take Δ onto the product of the reduced-local and the local-reduced part of A[2]. Since Δ is self-dual, it follows that Δ has rank 4 and is the product of a rank-2 reduced-local group and a rank-2 local-reduced group.

As in the proof of Lemma 7, let μ_A and μ_B be the degree-4 polarizations on A and B that we get by pulling back the canonical polarization of $\operatorname{Jac} C$ via the map $A \times B \to \operatorname{Jac} C$. We know that Δ is isomorphic to $\ker \mu_A$ and to $\ker \mu_B$. The local-reduced subgroup of $\ker \mu_A$ is maximal isotropic, so the polarization μ_A on A gives rise to a principal polarization on the quotient of A by this subgroup. It follows from the claim we made above that this quotient variety is the Jacobian of the curve D.

We can make a diagram

$$\begin{array}{ccc} A & \xrightarrow{\mu_A} & \widehat{A} \\ \downarrow & & \uparrow \\ \operatorname{Jac} D & \longrightarrow & \widehat{\operatorname{Jac} D} \end{array}$$

where the left arrow is the degree-2 isogeny $A \to \operatorname{Jac} D$, the right arrow is the dual of this isogeny, and the bottom arrow is the canonical polarization on $\operatorname{Jac} D$.

Now, $\operatorname{Jac} D$ has exactly one reduced-local subgroup of order 2, and it is defined over $\mathbb{F}_2$. It is in fact the kernel of multiplication by $1+\pi$, so $\operatorname{Jac} D$ divided by this subgroup is geometrically isomorphic to $\operatorname{Jac} D$. Now, the composition of the bottom and right arrows gives an isogeny $\operatorname{Jac} D \to \widehat{A}$ whose kernel is reduced-local and of order 2. So geometrically, $\widehat{A}$ is isomorphic to $\operatorname{Jac} D$, which means that $\widehat{A}$ is a twist of $\operatorname{Jac} D$. But $\widehat{A}$ is isogenous to $\operatorname{Jac} D$ over $\mathbb{F}_8$, and the quadratic twist of $\operatorname{Jac} D$ is not isogenous to $\operatorname{Jac} D$ (as we can see by checking Weil polynomials), so $\widehat{A}$ must be isomorphic to $\operatorname{Jac} D$ over $\mathbb{F}_8$. It follows that A is isomorphic to $\operatorname{Jac} D$ as well. Thus A, and the polarization μ_A, can be defined over $\mathbb{F}_2$.

On the other hand, B and the polarization μ_B can be defined over $\mathbb{F}_2$ simply because $\mathbb{Z}[\rho, \bar{\rho}] = \mathbb{Z}[\rho^3, \bar{\rho}^3]$. (This is essentially the Galois descent argument that Serre gives in [22] and in the appendix to [14].) This means that the whole diagram

$$\begin{array}{ccc} A \times B & \longrightarrow & \widehat{A} \times \widehat{B} \\ \downarrow & & \uparrow \\ \operatorname{Jac} C & \longrightarrow & \widehat{\operatorname{Jac} C} \end{array}$$

can be descended down to $\mathbb{F}_2$.

Now we want to know whether we can have a curve C over $\mathbb{F}_2$ with Weil polynomial equal to $f_2 g_2^3$. Again we find that C must be a double cover of a genus-2 curve D with Weil polynomial f_2. But then we find that C has 13 points over $\mathbb{F}_4$ and D has 4 points over $\mathbb{F}_4$, and this is impossible. □

6. Exhaustive searches over small spaces.

In this section we will give three examples that show how Theorem 1 can give us enough information about a curve with a certain number of

points for us to have a computer look at every such curve and bound its number of rational points.

6.1. The case $q = 27$, $g = 4$, $N = 66$.

We showed in Section 4.9 that a genus-4 curve over $\mathbb{F}_{27}$ with exactly 66 rational points must be a double cover of an elliptic curve with Weil polynomial $x^2 + 8x + 27$. There are exactly 4 elliptic curves over $\mathbb{F}_{27}$ with this Weil polynomial; one of them is defined over $\mathbb{F}_3$, and the other three are Galois conjugates of one another. Given such an elliptic curve E, we will show how the genus-4 double covers C of E can be enumerated by computer.

The function field of C must be obtained from that of E by adjoining a root of $z^2 = f$, where f is a function on E. By the Riemann-Hurwitz formula, in order for C to have genus 4 the divisor of f must be of the form

$$P_1 + \cdots + P_6 + 2D,$$

where the P_i are distinct geometric points on E and where D is a divisor of degree -3. There is a function g on E such that

$$D + \operatorname{div} g = Q - 4\infty,$$

where ∞ is the infinite point on E and where Q is a rational point on E. Replacing f with fg^2 does not change the double cover of E. Thus, we may assume that C is given by adjoining a root of $z^2 = f$, where f is a function on E whose divisor is of the form

$$P_1 + \cdots + P_6 + 2Q - 8\infty.$$

We can also change the map $C \to E$ by following it with a translation map on E. Translating E by a rational point R has the effect of replacing f with a function whose divisor is

$$(P_1 + R) + \cdots + (P_6 + R) + 2(Q + R) - 8R$$

(where the sums in parentheses take place in the algebraic group E). By modifying this new f by the square of a function we can get the divisor of f to be

$$(P_1 + R) + \cdots + (P_6 + R) + 2(Q - 3R) - 8\infty.$$

If we choose representatives of the classes of $E(\mathbb{F}_{27})$ modulo $3E(\mathbb{F}_{27})$, then we may assume that Q is one of these representatives. It turns out that for

each of the possible curves E the group $E(\mathbb{F}_{27})/3E(\mathbb{F}_{27})$ has order 3, so for each E we need consider only 3 possible Q's. We can choose our Q's so that they do not lie in $E[2]$.

Let us write E in standard Weierstrass form $y^2 = x^3 + ax^2 + bx + c$ and try to write down all of the functions f as above in a standard form. There are two cases to consider, depending on whether or not any of the P_i is ∞.

Suppose that one of the P_i is ∞. Then f has degree 7 and its only pole is at ∞, and f has a double zero at Q. Since Q is not a 2-torsion point by assumption, we may write $Q = (x_0, y_0)$ with $y_0 \neq 0$. Note that then $x - x_0$ is a uniformizing parameter at Q. Let f_0 be a linear polynomial that defines the tangent line to E at Q. Then up to squares f can be written as

$$f = \pm(f_1 + c_0 f_0),$$

where f_1 is a function of the form

$$(x - x_0)^2 \cdot (\text{polynomial in } x \text{ of degree} \leqslant 1) + (x - x_0)(y - y_0) \cdot (\text{monic linear in } x).$$

Likewise, if no P_i is ∞, then we may write $f = \pm(f_1 + c_0 f_0)$ where f_1 is a function of the form

$$(x - x_0)^2 \cdot (\text{monic quadratic in } x) + (x - x_0)(y - y_0) \cdot (\text{polynomial in } x \text{ of degree} \leqslant 1).$$

It is not hard at all to have a computer algebra system write down all of these possible f's for a given E.

Now our problem is to count the points on the extension of E defined by $z^2 = f$. It is easy to get an overestimate: If P is a rational point on E for which $f(P)$ is a nonzero square, then there are two rational points of C lying above P. If $f(P)$ is not a square, then there are no rational points of C above P. If P is a simple or a triple zero of f, then there is one rational point of C above P. And if P is a double zero of f, then there are at most 2 rational points of C lying above P.

What we actually did in practice for each candidate f was to:

(1) Eliminate f from consideration if we could find more than three points P on E with $f(P)$ nonsquare.

(2) Calculate the overestimate for $\#C(\mathbb{F}_{27})$ described above.

(3) Discard f if the overestimate was less than 66.

(4) Check to see that the divisor of f was of the proper form, and discard f if it was not.

No candidate f's made it through these filters, so we never had to worry about resolving the singularities of our model for C to get an exact point count.

It took a little more than twelve hours using Magma 2.9 on a 400 MHz PowerPC G4 processor to search through all of the (E, f) pairs that we had to consider. (Our Magma program is available at the URL mentioned in the acknowledgments.) Note that we need only consider two E's; if one of the E's that is defined only over $\mathbb{F}_{27}$ has a double cover with 66 points, then so do all of its conjugates.

6.2. The case $q = 32$, $g = 4$, $N = 75$.

We showed in Section 4.4 that a genus-4 curve over $\mathbb{F}_{32}$ with exactly 75 rational points must be a double cover of an elliptic curve with Weil polynomial $x^2 + 9x + 32$. There are exactly 5 elliptic curves over $\mathbb{F}_{32}$ with this Weil polynomial, and they are all conjugate to one another over $\mathbb{F}_2$. (If $a \in \mathbb{F}_{32}$ satisfies $a^5 + a^2 + 1 = 0$ then the elliptic curve E defined by $y^2 + xy = x^3 + x^2 + a^7$ has the correct Weil polynomial.) As in the preceding section, we can easily program a computer to enumerate the genus-4 double covers of such an elliptic curve and check to see whether any of these double covers has 75 points. The only complication is that a double cover in characteristic 2 is given by an Artin-Schreier extension of function fields instead of a Kummer extension.

Suppose C is a double cover of the curve E given above. Then the function field of C is obtained from that of E by adjoining a root of $z^2 + z = f$, where f is a function on E. The points of E that ramify in the cover $C \to E$ are contained in the set of poles of f; to determine whether a pole P of f is a ramification point, and to determine the contribution of P to the different of the extension $C \to E$, we look at the expansion of f in the local ring of E at P. According to [26], Prop. III.7.10, if there is a function g_P such that $f + g_P^2 + g_P$ has no pole at P, then P is unramified. If there is no such function, then we can at least find a function g_P so that $f + g_P^2 + g_P$ has a pole of odd order at P. If the pole has order m, then the differential exponent of P in the extension $C \to E$ is $m + 1$.

Suppose for each pole P of f we find a function g_P as above. Then by Riemann-Roch we can find a function g on E that has poles only at ∞

and at the poles P of f and such that $g - g_P$ has no pole at P for every $P \neq \infty$. Replacing f by $f + g^2 + g$ does not change the extension $C \to E$, but it allows us to assume that f has only odd-order poles, except perhaps at infinity. By modifying f in this same way by functions with poles only at ∞, we may also assume that if f has an even order pole at infinity, then the order of the pole is at most 2.

Now suppose that C has genus 4 and has 75 rational points. Then the Riemann-Hurwitz formula shows that there are three possible configurations for the different of $C \to E$: There are either

(1) three points with differential exponent 2,

(2) one point with differential exponent 2 and one with differential exponent 4, or

(3) one point with differential exponent 6.

The second possibility cannot occur, because each of the ramification points would have to be rational over $\mathbb{F}_{32}$, and this would force C to have an even number of rational points.

Suppose we are in case (3). Then the one ramification point P is rational, and by following the map $C \to E$ with a translation by $-P$, we may assume that the point P is the infinite point ∞ on E. Modifying the corresponding f as above, we find that we may assume that f is a function of degree 5 whose only pole is at ∞. Thus we may assume that f has the shape

$$f = (ax + b)y + (cx + d)$$

where $a \neq 0$. Furthermore, by modifying f by constants of the form $e^2 + e$, we may assume that d is either 0 or 1.

Suppose we are in case (1), with ramification at P_1, P_2, and P_3. Since C has an odd number of rational points, at least one of the P_i is rational. If we label this point P_3 and then translate by $-P_3$, we find that we may assume that $P_3 = \infty$. We may also assume that neither P_1 nor P_2 is the unique 2-torsion point on E (that is, the unique point with $x = 0$), because if (say) P_1 is the 2-torsion point on E, we can translate by $-P_2$ so that the ramification locus becomes $\{P_1 - P_2, \infty, -P_2\}$. Thus we may write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $x_1 \neq 0$ and $x_2 \neq 0$. Then we may write f in the form

$$f = ax + b\,\frac{y + y_1 + x_1}{x + x_1} + c\,\frac{y + y_2 + x_2}{x + x_2} + d$$

where b and c are nonzero, where d is either 0 or 1, and where a is nonzero if and only if f has a pole of order 2 at ∞. Note that if P_1 and P_2 are not defined over $\mathbb{F}_{32}$ then they are quadratic conjugates of one another, and so b and c must be quadratic conjugates of one another in order for f to be defined over $\mathbb{F}_{32}$.

It is a simple matter to count points on the curve C defined by $z^2 + z = f$, where f is as above, because we are assuming that every pole of f ramifies. So if P is a rational point on E that is a pole of f, then there is one point on C lying above P. If P is a rational point that is not a pole of f, then there are either two or zero rational points on C over P, depending on whether the trace of $f(P)$ to $\mathbb{F}_2$ is 0 or 1.

We used Magma to enumerate all of the possible f's for one of the elliptic curves E given above. (Our Magma program is available at the URL mentioned in the acknowledgments.) For each f we counted points on the curve $z^2 + z = f$. No f gave us 75 points. Thus we verified that there is no genus-4 curve over $\mathbb{F}_{32}$ having exactly 75 rational points.

6.3. The case $q = 3$, $g = 6$, $N = 15$.

In Section 4.7 we showed that there were two possible real Weil polynomials for a genus-6 curve over $\mathbb{F}_3$ having 15 points. One of the two polynomials was $(x + 2)^2(x^2 + 3x - 1)(x^2 + 4x + 2)$, and we showed that any curve C with this real Weil polynomial must be a double cover of the genus-2 curve D defined by $y^2 = x^6 + x^5 + x^4 + x^2 - x + 1$. We note that C has 15 places of degree 1 and 53 places of degree 5, and the proof of Lemma 8 shows that therefore a degree-1 place and a degree-5 place of D must ramify in the double cover $C \to D$. (Since the degree of the different of the cover is 6 by Riemann-Hurwitz, no other places of D can be ramified.) In this section we will show how one can make a short list of double covers of D that contains all of the genus-6 covers ramified only at a degree-1 place and a degree-5 and having 15 rational points. We will find that there are no such double covers.

Note that the automorphism group of D is cyclic of order 8, generated by the map $(x, y) \mapsto \big((1+x)/(1-x), y/(1-x^3)\big)$. This group acts transitively on the rational points of D, so we may assume that the rational ramification point of the double cover $C \to D$ is our favorite rational point on D. We will choose this point to be the rational point on D that is a pole of the

function x and a zero of the function $y - x^3$, which point we will denote by ∞^+.

Let K be the function field of D and let L be the function field of C. Then there is a function f on D such that $L = K(z)$ for an element z with $z^2 = f$. Let P be the degree-5 place at which $C \to D$ ramifies. Then the divisor of f is $P - 5\infty^+ + 2E$ for some degree-0 divisor E on D. By Riemann-Roch, there is a function g on D whose divisor is $F - 2\infty^+ - E$ for some effective degree-2 divisor F. Replacing z with zg and f with fg^2, we find that we may assume that the divisor of f is $P + 2F - 9\infty^+$ for some effective divisor F of degree 2.

The divisor F must have one of four possible shapes, each considered below. For each possibility, we had Magma check that that there is no function f on E whose divisor is of the right form and that gives an extension with 15 points. (Our Magma routines for doing this are available at the URL mentioned in the acknowledgments.)

Case 1: *F consists of one place of degree* 2. — Since D has 8 rational points and C has 15, we see that the rational points of D that do not ramify in the double cover $C \to D$ must split. Since f is nonzero at the rational points of D other than ∞^+ and since these points all split, f must evaluate to 1 at these points. It is a simple matter to enumerate all of the elements of the Riemann-Roch space $\mathcal{L}(9\infty^+)$ that evaluate to 1 at the other rational points of D, and to check that none of them has a divisor of the form $P + 2F - 9\infty^+$ for a degree-5 place P.

Case 2: *F consists of two possibly equal places of degree* 1, *neither equal to* ∞^+. — To handle this case, we consider all possible pairs of points F_1 and F_2 on D. For each pair, we have Magma enumerate the elements of $\mathcal{L}(9\infty^+)$ that vanish at F_1 and F_2 and that evaluate to 1 at the other rational points on D. For each such function, we check that its divisor is not of the form $P + 2F_1 + 2F_2 - 9\infty^+$ for a degree-5 place P.

Case 3: *F consists of ∞^+ and some other degree-*1 *place.* — Now we loop over all rational points $F_1 \neq \infty^+$ of D, and consider the elements of $\mathcal{L}(7\infty^+)$ that vanish at F_1 and that evaluate to 1 at the other rational points of D. For each such function, we check that its divisor is not of the form $P + 2F_1 - 7\infty^+$ for a degree-5 place P.

Case 4: *F consists of two copies of* ∞^+. — For this case we must consider the elements of $\mathcal{L}(5\infty^+)$ that evaluate to 1 at the other rational

points of D. It turns out that the only such function is the constant function 1.

Thus we find that there are no curves over $\mathbb{F}_3$ having real Weil polynomial $(x+2)^2(x^2+3x-1)(x^2+4x+2)$.

7. Triple covers of elliptic curves in characteristic 3.

7.1. A convenient standard form.

Suppose k is a finite field of characteristic 3, suppose E is an elliptic curve over k, and suppose C is a curve over k for which there is a degree-3 map $C \to E$. We will show that C can be given in a convenient standard form. We will limit ourselves to covers $C \to E$ for which a certain assumption (stated below) holds.

Let L and K be the function fields for C and E, respectively, and view L as a degree-3 extension of K via the degree-3 map $C \to E$. Choose a generator for L over K whose trace to K is 0. Then there are functions f and g in K such that $z^3 - fz - g = 0$. Suppose we write the divisor of f in the form

$$\operatorname{div} f = P_1 + \cdots + P_n + 2D,$$

where the P_i are distinct geometric points of E (and where n is necessarily even). Note that since f is (up to squares) the discriminant of the extension L/K, the number n is the number of points of E at which the discriminant of L/K has odd valuation.

ASSUMPTION. — *We will assume that n is coprime to $\#E(k)$.*

Under this assumption, there is a rational point Q on E such that $nQ = P_1 + \cdots + P_n$ in the group of points of E. By composing the given map $C \to E$ with a translation, we may assume that Q is the infinite point ∞ on E. By replacing the divisor D above with $D + (n/2)\infty$, we may write

$$\operatorname{div} f = P_1 + \cdots + P_n - n\infty + 2D$$

where the P_i are distinct geometric points on E whose sum is 0 in E. It follows that D is a degree-0 divisor, and the sum (in E) of the points in D is a k-rational 2-torsion point on E. But since $\#E(k)$ is coprime to the even number n, the only k-rational 2-torsion point on E is ∞. Therefore D is a principal divisor, because it has degree 0 and the sum (in E) of its points is

zero. Write $D = \operatorname{div} h$ for some function h. Replacing z, f, and g with z/h, f/h^2, and g/h^3, respectively, we find that we still have $z^3 - fz - g = 0$, but now the divisor of f is

$$\operatorname{div} f = P_1 + \cdots + P_n - n\infty.$$

If one of the P_i (say P_n) is equal to ∞, replace n by $n-1$ and delete the point P_n from the expression for $\operatorname{div} f$. The integer n may no longer be even, but now we have that the P_i are all distinct and that none of them is ∞. We do at least know that n is not 1, because there is no function on E with divisor $P - \infty$.

Now suppose P is a finite place of E at which g has a pole. Suppose $\operatorname{ord}_P g$ is a multiple of 3, say $\operatorname{ord}_P g = -3m$ for some positive m. Then there is a function h on E that has poles only at P and at ∞ such that $\operatorname{ord}_P(g - h^3 + fh) > -3m$. Replacing z with $z - h$ and g with $g - h^3 + fh$, we find that we have reduced the order of the pole of g at P. Repeating this process, we find that we may assume that for every finite pole P of g, the order of g at P is not a multiple of 3.

Suppose g has a pole at ∞, and suppose $\operatorname{ord}_\infty g$ is less than $-3n/2$. If $\operatorname{ord}_\infty g$ is a multiple of 3 and is less than -3, then we can find a function h, with poles only at ∞, such that $\operatorname{ord}_\infty(g - h^3 + fh) > \operatorname{ord}_\infty g$. Again we may replace z with $z - h$ and g with $g - h^3 + fh$ to reduce the order of the pole of g at ∞. Repeating this procedure, we may assume that if $\operatorname{ord}_\infty g$ is less than $-3n/2$ and less than -3, then $\operatorname{ord}_\infty g$ is not a multiple of 3.

7.2. Contributions to the different.

Suppose L/K field extension of the type considered above, given in the standard form $z^3 - fz - g = 0$ described in the preceding section. Given a point P on E, we would like to calculate the contribution at P to the different of the extension L/K. The basic fact we will use is that if L/K is a degree-3 Artin-Schreier extension of local fields given by an equation $z^3 - z = h$, where the valuation of h is n, then the degree of the different is zero if $n \geqslant 0$ and is $2 - 2n$ if $n < 0$ and $n \not\equiv 0 \bmod 3$. (This follows from [26], Prop. III.7.10, for example.) Since the contribution to the different is stable under base extension, we may assume that the base field k is the algebraic closure of $\mathbb{F}_3$.

Suppose we are given P on E with $\operatorname{ord}_P f$ even. Note that by the way we normalized f and g, either $2 \operatorname{ord}_P g \geqslant 3 \operatorname{ord}_P f$ or $\operatorname{ord}_P g \not\equiv 0 \bmod 3$,

except in the case when $P = \infty$ and $\operatorname{ord}_P g = -3$ and $\operatorname{ord}_P f = 0$. Let us suppose we are *not* in this exceptional case. Note that if f is nonconstant we will not be in the exceptional case.

In the completion of K at P the function f is a square, say $f = s^2$ for some $s \in K_P$. Locally at P the extension L_P/K_P is given by the equation $w^3 - w = g/s^3$, and the valuation of g/s^3 is $\operatorname{ord}_P g - (3/2)\operatorname{ord}_P f$. Since we are not in the exceptional case, this valuation is either positive or is not a multiple of 3. Thus the contribution to the different at P is

$$\begin{cases} 0 & \text{if } 3\operatorname{ord}_P f - 2\operatorname{ord}_P g \leqslant 0; \\ 2 + 3\operatorname{ord}_P f - 2\operatorname{ord}_P g & \text{if } 3\operatorname{ord}_P f - 2\operatorname{ord}_P g > 0. \end{cases}$$

In particular, note that when $\operatorname{ord}_P f$ is even the contribution at P to the different is even, and is at least 4 if it is nonzero.

Suppose we are given P on E with $\operatorname{ord}_P f$ odd. Again we see that by the way we normalized f and g, either $2\operatorname{ord}_P g \geqslant 3\operatorname{ord}_P f$ or $\operatorname{ord}_P g \not\equiv 0 \bmod 3$, except in the case when $P = \infty$ and $\operatorname{ord}_P g = -3$ and $\operatorname{ord}_P f = -1$. But as we noted before, $\operatorname{ord}_\infty f$ cannot be equal to -1, so there is no exceptional case when $\operatorname{ord}_P f$ is odd.

Our completed extension L_P/K_P fits into a diagram

$$\begin{array}{ccc} L_P & \longrightarrow & L'_P \\ \uparrow & & \uparrow \\ K_P & \longrightarrow & K'_P \end{array}$$

where K'_P and L'_P are obtained from K_P and L_P by adjoining a square root s of f. The extension L'_P/K'_P is given by the equation $w^3 - w = g/s^3$. Let P' be the prime of K'_P. If the P'-adic valuation of g/s^3 is nonnegative (that is, if $2\operatorname{ord}_P g - 3\operatorname{ord}_P f \geqslant 0$) then there is no ramification in L'_P/K'_P, and so the ramification in L_P/K_P is tame. In this case the contribution at P to the different of L/K is 1. On the other hand, if $2\operatorname{ord}_P g - 3\operatorname{ord}_P f < 0$ then the P'-adic valuation of g/s^3 is negative and not a multiple of 3, so the Galois extension L'_P/K'_P is totally ramified. In particular, L'_P is a field. Let $\mathfrak{p}$ be the prime of L'_P lying over P. Then $P' = \mathfrak{p}^3$, the prime of L_P is $\mathfrak{p}^2$, and $P = \mathfrak{p}^6$.

Let us calculate the different of L'_P/K_P in two different ways. First of all, we note that the different of L'_P/K'_P is

$$\delta_{L'_P/K'_P} = \mathfrak{p}^{2+2m}$$

where $m = 3\operatorname{ord}_P f - 2\operatorname{ord}_P g$. Next, we note that the extension K'_P/K_P is tamely ramified, so its different is $\delta_{K'_P/K_P} = P' = \mathfrak{p}^3$. Likewise, the

different of L'_P/L_P is $\delta_{L'_P/L_P} = \mathfrak{p}$. Thus, if the different of L_P/K_P is $\delta_{L_P/K_P} = (\mathfrak{p}^2)^n$, we have

$$\delta_{L_P/K_P}\delta_{L'_P/L_P} = \delta_{K'_P/K_P}\delta_{L'_P/K'_P},$$

so that $\mathfrak{p}^{2n+1} = \mathfrak{p}^{3+2+2m}$. It follows that the contribution n of the different of L/K at P is $n = 2 + 3\operatorname{ord}_P f - 2\operatorname{ord}_P g$.

Thus, when $\operatorname{ord}_P f$ is odd the contribution to the different at P is

$$\begin{cases} 1 & \text{if } 3\operatorname{ord}_P f - 2\operatorname{ord}_P g \leqslant 0; \\ 2 + 3\operatorname{ord}_P f - 2\operatorname{ord}_P g & \text{if } 3\operatorname{ord}_P f - 2\operatorname{ord}_P g > 0. \end{cases}$$

In particular, when $\operatorname{ord}_P f$ is odd the contribution at P to the different is odd.

7.3. The case $q = 3$, $g = 6$, $N = 15$.

In Section 4.7 we showed that there were two possible real Weil polynomials for a genus-6 curve over $\mathbb{F}_3$ having 15 points. One of the polynomials was $h = (x+2)^2(x+3)(x^3+4x^2+x-3)$, and we showed that a curve with this real Weil polynomial must be a triple cover of an elliptic curve with Weil polynomial x^2+3x+3. There is one elliptic curve over $\mathbb{F}_3$ with this Weil polynomial, namely the curve E defined by $y^2 = x^3-x+1$. In this section we will use the theory developed in the preceding two sections to show that there is no curve over $\mathbb{F}_3$ with real Weil polynomial h.

We will argue by contradiction. Suppose that a curve C has the given Weil polynomial. We compute that C has 15 places of degree 1, no places of degree 2, and no places of degree 3. Therefore, in the triple cover $C \to E$ every rational point on E either splits completely or is ramified. Note that a rational point of E that is tamely ramified splits into two rational points of C, while a rational point that is wildly ramified gives just one rational point of C. Thus, if we let

a = the number of rational points of E unramified in $C \to E$

b = the number of rational points of E tamely ramified in $C \to E$

c = the number of rational points of E wildly ramified in $C \to E$

then we have $a + b + c = \#E(\mathbb{F}_3) = 7$ and $3a + 2b + c = \#C(\mathbb{F}_3) = 15$.

The Riemann-Hurwitz formula shows that the degree of the different of $C \to E$ is 10. Each tamely ramified point contributes 1 to this degree, and each wildly ramified point contributes at least 3. Thus we also know

that the number of tamely ramified points plus three times the number of wildly ramified points is at most 10.

In particular, we note that the number of points of E at which the discriminant of $C \to E$ has odd valuation is an even number that is at most 10, and hence is coprime to 7, the number of rational points on E. Thus, the cover $C \to E$ satisfies the assumption of Section 7.1. We may therefore put the cover $C \to E$ in the standard form given in that section, and we may use the results of Section 7.2.

Keeping in mind the above restrictions on the number of unramified, tamely ramified, and wildly ramified rational points of E, we find that there are four situations to consider:

- $a = 1$, $b = 6$, $c = 0$;
- $a = 2$, $b = 4$, $c = 1$;
- $a = 3$, $b = 2$, $c = 2$;
- $a = 4$, $b = 0$, $c = 3$.

We will consider each of these cases in turn, but there are two facts that we will use repeatedly. The first is that if P is a place of E that is wildly ramified, then P must be rational. To see that this is true, note that if P were not rational it would have to have degree at least 4, because C has no places of degree 2 or 3. Thus, P would contribute at least 12 to the degree of the different, contradicting the fact that this degree is 10.

The second fact that we will often use is that if P is a rational point of E that splits completely and that is a pole of neither f nor g, then we must have $f(P) = 1$ and $g(P) = 0$. This follows from the fact that the splitting of P corresponds to the splitting of the polynomial $z^3 - f(P)z - g(P)$ over $\mathbb{F}_3$, and the only completely split monic degree-3 polynomial over $\mathbb{F}_3$ with no quadratic term is $z^3 - z$.

First case: $a = 1$, $b = 6$, $c = 0$. — In this case there is no wild ramification at all, so there must be 10 tamely ramified geometric points on E. Thus there must be exactly 10 points P of E for which $\operatorname{ord}_P f$ is odd. There are two possibilities: either

$$\operatorname{div} f = P_1 + \cdots + P_{10} - 10\infty$$

or

$$\operatorname{div} f = P_1 + \cdots + P_9 - 9\infty.$$

According to the results of Section 7.2, in order for all of the ramification to be tame, the function g must have a double zero (at least) at each of the

P_i, and its only pole can be at ∞. Further, the order of g at infinity must be at least -15 in the first case, and -13 in the second case. Thus either

$$\operatorname{div} g \geqslant 2P_1 + \cdots + 2P_{10} - 15\infty$$

or

$$\operatorname{div} g \geqslant 2P_1 + \cdots + 2P_9 - 13\infty.$$

Neither of these possibilities is consistent with the fact that the degree of the divisor of g is zero.

Second case: $a = 2$, $b = 4$, $c = 1$. — In this case there can be at most 7 tamely ramified geometric points on E, because the single wildly ramified point contributes at least 3 to the different. But if there were a nonrational tamely ramified place on E, it would have to have degree at least 4 (because C has no places of degree 2 or 3); thus this tamely ramified place, plus the 4 rational ones, would give at least 8 tamely ramified geometric points. This shows that the 4 rational tamely ramified points are the only tamely ramified places on E, and it follows that the single wildly ramified point must contribute 6 to the degree of the different.

There are two possibilities for the divisor of f: either

$$\operatorname{div} f = P_1 + P_2 + P_3 + P_4 - 4\infty$$

or

$$\operatorname{div} f = P_1 + P_2 + P_3 - 3\infty.$$

Suppose we are in the second case. Let Q be the rational point at which there is wild ramification. Then $Q \neq \infty$, and we see from Section 7.2 that g must have a pole of order 2 at Q. Furthermore, to prevent any further wild ramification, the order of g at ∞ must be at least -4 and the order of g at each P_i must be at least 2. It follows that

$$\operatorname{div} g \geqslant 2P_1 + 2P_2 + 2P_3 - 2Q - 4\infty,$$

and since the degree of $\operatorname{div} g$ is zero, we must have equality in the relation above. But as we noted above, g must have a zero at every rational point of E that is not in the support of $\operatorname{div} f$ and at which g has no pole, so we cannot have equality, and we have reached a contradiction.

Now suppose we have $\operatorname{div} f = P_1 + P_2 + P_3 + P_4 - 4\infty$. Let Q be the rational point at which there is wild ramification. If $Q \neq \infty$ then we see from Section 7.2 that g must have a pole of order 2 at Q, and furthermore the order of g at ∞ must be at least -6. If $Q = \infty$ then g must have a

pole of order 8 at ∞. Furthermore, g must have double zeros (at least) at the points P_i. Thus

$$\operatorname{div} g \geqslant \begin{cases} 2P_1 + 2P_2 + 2P_3 + 2P_4 - 2Q - 6\infty & \text{if } Q \neq \infty; \\ 2P_1 + 2P_2 + 2P_3 + 2P_4 - 8\infty & \text{if } Q = \infty. \end{cases}$$

Since the degree of $\operatorname{div} g$ is zero, in either case we must have equality. But again we see that equality is impossible because g must also have zeros at every rational point not in the support of f and not in the polar divisor of g.

Third case: $a = 3$, $b = 2$, $c = 2$. — As in the preceding case, the only tamely ramified places are the two tamely ramified rational points. Thus the two wildly ramified points contribute a total of 8 to the degree of the different. Either they each contribute 4, in which case the valuation of f is even at the two points, or one contributes 3 and one contributes 5, in which case the valuation of f is odd at the two points. We consider these two cases in turn.

First suppose that the wildly ramified points Q_1 and Q_2 each contribute 4 to the degree of the different. Then the divisor of f is of the form

$$\operatorname{div} f = P_1 + P_2 - 2\infty,$$

where no P_i is equal to any Q_j. We know from Section 7.2 that g must have a double zero (at least) at each P_i. If neither Q_i is ∞, then g must have a simple pole at each Q_i, and the order of g at ∞ must be at least -3. Thus

$$\operatorname{div} g \geqslant 2P_1 + 2P_2 - Q_1 - Q_2 - 3\infty.$$

But g must have a zero at each of the 2 rational points in

$$E(\mathbb{F}_3) \setminus \{P_1, P_2, Q_1, Q_2, \infty\},$$

and this is enough to contradict the fact that the degree of $\operatorname{div} g$ is zero.

If on the other hand one of the Q_i (say Q_2) is ∞, then g must still have a simple pole at Q_1, but now the order of g at ∞ must be -4. Then we find that

$$\operatorname{div} g \geqslant 2P_1 + 2P_2 - Q_1 - 4\infty.$$

But we also know that g has a zero at each of the three points in

$$E(\mathbb{F}_3) \setminus \{P_1, P_2, Q_1, \infty\},$$

and again we get a contradiction.

Now suppose that Q_1 contributes 3 to the degree of the different and Q_2 contributes 5. Again we let the tamely ramified points be P_1 and P_2, but now any one of the P_i and Q_i might be ∞. Analysis as above shows that

$$\operatorname{div} g \geqslant \begin{cases} 2P_2 + Q_1 - 4\infty & \text{if } P_1 = \infty; \\ 2P_1 + Q_1 - 4\infty & \text{if } P_2 = \infty; \\ 2P_1 + 2P_2 - 5\infty & \text{if } Q_1 = \infty; \\ 2P_1 + 2P_2 + Q_1 - 6\infty & \text{if } Q_2 = \infty; \\ 2P_1 + 2P_2 + Q_1 - 6\infty & \text{otherwise.} \end{cases}$$

In every case, the fact that g must also have zeros at every point in $E(\mathbb{F}_3) \setminus \{P_1, P_2, Q_1, Q_2, \infty\}$ provides a contradiction.

Fourth case: $a = 4$, $b = 0$, $c = 3$. — In this case we have three rational wildly ramified points and no other ramification points at all. Let the ramification points be Q_1, Q_2, and Q_3. We can order the points so that the Q_1 and Q_2 each contribute 3 to the degree of the different, and Q_3 contributes 4. Then f must have odd order at Q_1 and Q_2 and at no other points. The only possibility is that $\operatorname{div} f = Q_1 + Q_2 - 2\infty$. From Section 7.2 we see that g must have simple zeros at Q_1 and Q_2.

Suppose $Q_3 = \infty$. Then g must have a pole of order 4 at ∞ and no other poles. But as we noted earlier, g must also have zeros at every rational point that is not in the support of f and not in the polar divisor of g. This means that g must have zeros at all six rational points of E other than ∞, and this is not compatible with the divisor of g having degree 0.

Suppose $Q_3 \neq \infty$. Then g must have a simple pole at Q_3, and the order of g at ∞ must be at least -3. But then the degree of the polar divisor of g is at least -4, while the degree of the divisor of zeros of g is at least 5. Again, this is impossible.

7.4. The case $q = 27$, $g = 4$, $N = 65$.

In Section 4.9 we showed that a genus-4 curve over $\mathbb{F}_{27}$ having exactly 65 points must be a triple cover of an elliptic curve with Weil polynomial $x^2 + 7x + 27$. There are three such elliptic curves and they are all conjugate to one another over $\mathbb{F}_3$. If one of these elliptic curves has a triple cover of the right kind then they all do, so to search for triple covers of the desired form we may as well choose our favorite E with Weil polynomial

$x^2+7x+27$ and look for triple covers of it. We will take E to be the elliptic curve $y^2 = x^3 - x^2 + \alpha^8$, where $\alpha \in \mathbb{F}_{27}$ satisfies $\alpha^3 - \alpha + 1 = 0$.

Suppose C is genus-4 curve over $\mathbb{F}_{27}$ with 65 points for which there is a triple cover $C \to E$. The Riemann-Hurwitz formula shows that the degree of the different of the cover is 6, so the number of points of E at which the discriminant of $C \to E$ has odd valuation is an even number that is at most 6. In particular, this number is coprime to $\#E(\mathbb{F}_{27}) = 35$, so the cover $C \to E$ meets the assumption of Section 7.1. Thus we may put the cover $C \to E$ into the standard form given in Section 7.1, namely $z^3 - fz - g = 0$, where f and g are functions on E satisfying certain conditions.

Our argument will depend on the various possible configurations of wild and tame ramification in the cover $C \to E$. A tame ramification point contributes 1 to the degree of the different, and a wild ramification point contributes at least 3, so we will organize our argument according to the partitions of 6 that do not include 2.

We will require some computer calculations. The Magma program we use is available at the URL mentioned in the acknowledgments.

The partition $6 = 6$. — In this case there is a unique ramification point, and it contributes 6 to the degree of the different. This can happen in our standard form only if $\operatorname{div} f = 0$, so f is a constant and the only pole of g is at ∞. As we saw in Section 7.1, we can modify f by squares, so we may take f to be either 1 or -1.

Suppose $f = 1$. Then C is given by $z^3 - z = g$. If P is a point on E other than ∞, then P splits in $C \to E$ in the same way that the polynomial $z^3 - z - g(P)$ splits over $\mathbb{F}_{27}$. In particular, P will either have no rational points of C lying above it, or it will have 3. Thus, the number of rational points on C lying over finite points of E is a multiple of 3. Since there is one point on C lying over the infinite point of E, we see that $\#C(\mathbb{F}_{27}) \equiv 1 \bmod 3$. But C is supposed to have 65 points, so this is a contradiction.

Suppose $f = -1$. Then C is given by $z^3 + z = g$, and the splitting of a finite point P of E is determined by the splitting of the polynomial $z^3 + z - g(P)$. One checks that such a polynomial will have either 0 or 1 root in $\mathbb{F}_{27}$, so every rational point of E has at most one rational point of C lying over it. In particular we see that $\#C(\mathbb{F}_{27}) \leqslant \#E(\mathbb{F}_{27}) = 35$, and again this contradicts our assumption that C has 65 points.

The partition $6 = 5 + 1$. — In this case we must have $\operatorname{div} f = P_1 + P_2 - 2\infty$, where we may assume that P_1 is the tamely ramified point and P_2 is the wildly ramified point. (Note that in the group law on E we have $P_1 = -P_2$.) Both P_1 and P_2 must be rational, and according to our analysis in Section 7.2 we must have $\operatorname{ord}_{P_1} g \geqslant 2$ and $\operatorname{ord}_{P_2} g = 0$ and $\operatorname{ord}_\infty g \geqslant -3$.

We see that f must be of the form $a(x - x_1)$ for some nonzero a, where x_1 is the x-coordinate of a rational point on E. Modifying f by squares of constants we find that we may assume that $a = \pm 1$. Now consider g. Its degree is at most 3 and it has a double zero at P_1, so the only possibility is that g is an equation for the tangent line to E at P_1.

We can enumerate the possible f's and g's as follows. We let $P_1 = [x_1, y_1]$ run through the set of rational points on E other than ∞. We let a run through the set $\{-1, 1\}$. We take $f = a(x - x_1)$. We compute an equation ℓ for the tangent line to E at P_1. We let c run through $\mathbb{F}_{27}^*$ and we set $g = c\ell$. Then we check to see whether the cover of E defined by $z^3 - fz - g = 0$ has 65 rational points.

We have written a Magma program that goes through this procedure. It finds no triple cover with 65 points.

The partition $6 = 4 + 1 + 1$. — In this case we must have $\operatorname{div} f = P_1 + P_2 - 2\infty$, where either P_1 and P_2 are both rational points, or they are conjugate points defined over $\mathbb{F}_{3^6}$. Note that this means that f must be of the form $f = a(x - b)$ for $a, b \in \mathbb{F}_{27}$ with a nonzero. Since we can modify f by squares of constants, we may assume that $a = \pm 1$.

Now there are two cases to consider, depending on whether or not the wildly ramified rational point Q is equal to ∞. First suppose that $Q \neq \infty$. Then the usual analysis shows that $\operatorname{div} g \geqslant 2P_1 + 2P_2 - Q - 3\infty$, and since the divisor of g has degree 0 we must have equality. It follows that the divisor of f^2/g is $Q - \infty$, but this is impossible. Therefore Q must be ∞, and by the usual methods we see that

$$\operatorname{div} g \geqslant 2P_1 + 2P_2 - 4\infty.$$

In particular, we note that g/f^2 is a constant.

Now we can enumerate all of the possible f's and g's. We consider all triples (a, b, c) with $a = \pm 1$, $b \in \mathbb{F}_{27}$, and $c \in \mathbb{F}_{27}^*$, and we let $f = a(x - b)$ and $g = cf^2$. Then we can check to see whether any of the covers of E defined by $z^3 - fz - g = 0$ have 65 points. We carried out this procedure using Magma, and found no triple cover with 65 points.

The partition $6 = 3+3$. — Again we must have $\operatorname{div} f = P_1+P_2-2\infty$, where P_1 and P_2 are not necessarily rational. The function g must have simple zeros at P_1 and P_2, and g can have at most a triple pole at ∞. Thus we either have $\operatorname{div} g = P_1 + P_2 - 2\infty$ or $\operatorname{div} g = P_1 + P_2 + Q - 3\infty$ for some point $Q \neq \infty$. But the latter case cannot occur, because otherwise g/f would have divisor $Q - \infty$. Thus we see that g is a nonzero constant times f.

We enumerate all of the possible f's and g's as follows: We consider all triples (a, b, c) with $a = \pm 1$, $b \in \mathbb{F}_{27}$, and $c \in \mathbb{F}_{27}^*$, and we let $f = a(x - b)$ and $g = cf$. Then we can check to see whether any of the covers of E defined by $z^3 - fz - g = 0$ have 65 points. Our computations show that no such curve has 65 points.

The partition $6 = 3 + 1 + 1 + 1$. — There are two possibilities for the divisor of f: either $\operatorname{div} f = P_1 + P_2 + P_3 + P_4 - 4\infty$ or $\operatorname{div} f = P_1 + P_2 + P_3 - 3\infty$. We consider each shape in turn.

First suppose that $\operatorname{div} f = P_1 + P_2 + P_3 + P_4 - 4\infty$, and suppose that the wildly ramified point is P_4. Then g must have double zeros at P_1, P_2, and P_3, and a simple zero at P_4. Furthermore, g can have a pole of order at most 6 at ∞. But then

$$\operatorname{div} g \geqslant 2P_1 + 2P_2 + 2P_3 + P_4 - 6\infty,$$

which is impossible.

Next suppose that $\operatorname{div} f = P_1 + P_2 + P_3 - 3\infty$. We may assume that the wildly ramified point is at either P_3 or at ∞. Arguing as in previous cases, we find that

$$\operatorname{div} g \geqslant \begin{cases} 2P_1 + 2P_2 + P_3 - 4\infty & \text{if the wild ramification is at } P_3; \\ 2P_1 + 2P_2 + 2P_3 - 5\infty & \text{if the wild ramification is at } \infty. \end{cases}$$

Both possibilities are impossible, since $\operatorname{div} g$ has degree 0.

The partition $6 = 1 + 1 + 1 + 1 + 1 + 1$. — This time the divisor of f is either $\operatorname{div} f = P_1 + \cdots + P_6 - 6\infty$ or $\operatorname{div} f = P_1 + \cdots + P_5 - 5\infty$. In the first case we find that

$$\operatorname{div} g \geqslant 2P_1 + \cdots + 2P_6 - 9\infty,$$

which is impossible. In the second case we find that

$$\operatorname{div} g \geqslant 2P_1 + \cdots + 2P_5 - 7\infty,$$

which is also impossible.

8. An argument on Hermitian forms.

In this section we prove a theorem of Savitt [18]:

THEOREM 16. — *There is no genus-4 curve over $\mathbb{F}_8$ with exactly 27 rational points.*

Proof. — Suppose such a curve C existed. It has defect 2 and so we know that C must be of type $[m, m, m, m-2]$ or of type

$$[m+(-1+\sqrt{5})/2, m+(-1-\sqrt{5})/2, m+(-1+\sqrt{5})/2, m+(-1-\sqrt{5})/2],$$

where $m = 5$. Corollary 9 eliminates the first possibility, so C must be of the latter type. It follows that the Weil polynomial of C must be f^2, where $f = x^4 - 9x^3 + 35x^2 - 72x + 64$. Our proof of Savitt's theorem is completed by the following proposition, which shows that every principal polarization of an abelian variety with Weil polynomial f^2 is decomposable. □

PROPOSITION 17. — *There is exactly one abelian variety A over $\mathbb{F}_8$ with Weil polynomial f. Up to isomorphism, the variety A has exactly one principal polarization λ. Furthermore, up to isomorphism there is exactly one principally polarized abelian variety over $\mathbb{F}_8$ with Weil polynomial f^2, and it is isomorphic to $(A \times A, \lambda \times \lambda)$.*

Let K be the quartic number field defined by the polynomial f and let $\mathcal{O}_K$ denote the ring of integers of K. Our proof of Proposition 17 will depend on a result about Hermitian forms over $\mathcal{O}_K$. We will state this result now and use it in the proof of Proposition 17, but we will postpone its proof until later in this section.

We will see that K is the totally imaginary biquadratic extension $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$ of the totally real field $K^+ = \mathbb{Q}(\sqrt{5})$; we refer to the nontrivial automorphism of K over K^+ as *complex conjugation*, and we denote the complex conjugate of $x \in K$ by $\overline{x}$. Let $M_2(\mathcal{O}_K)$ denote the ring of 2-by-2 matrices over $\mathcal{O}_K$. If C is an element of $M_2(\mathcal{O}_K)$ we let C^* denote its conjugate-transpose.

PROPOSITION 18. — *Suppose A is an invertible Hermitian matrix in $M_2(\mathcal{O}_K)$ that is totally positive (meaning that all of the roots of its*

minimal polynomial are totally positive algebraic numbers). Then there is an invertible $C \in M_2(\mathcal{O}_K)$ such that $A = C^*C$.

Let us assume this result for the time being, and proceed with the proof of Proposition 17.

Proof of Proposition 17. — We begin by setting some notation related to the number field K.

Let π be a root of f in K, let $\overline{\pi} = 8/\pi$, and let $R = \mathbb{Z}[\pi, \overline{\pi}]$. Let $\varphi = \pi + \overline{\pi} - 4$ and let $\zeta = 17 - 6\pi + \pi^2 - 3\overline{\pi}$. It is easy to check that then $\varphi^2 - \varphi - 1 = 0$ and $\zeta^2 + \zeta + 1 = 0$, and from these relations we see that K is isomorphic to $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$ and that R is the full ring of integers of K.

It is not hard to show that the Dedekind domain R is a PID [10]; in fact, Lemma 20 below shows that R is norm-Euclidean.

Note that the middle coefficient of f is coprime to 8, so there is an isogeny class of ordinary abelian varieties over $\mathbb{F}_8$ with Weil polynomial f. In fact, according to a result of Deligne [3], the abelian varieties in this isogeny class correspond to the isomorphism classes of R-modules that can be embedded in K as lattices. Since R is the full ring of integers of K and since R has class number 1, there is exactly one such isomorphism class of R-modules, and therefore there is exactly one abelian variety A over $\mathbb{F}_8$ with Weil polynomial f. This proves the first statement of the proposition.

Theorem 1.3 of [7] shows that the abelian variety A has a principal polarization λ. Now suppose μ is another principal polarization of A. Then we know from [16], Application III, pp. 208–210 (see especially the final paragraph) that there is a totally positive unit u of the maximal real subfield K^+ of K such that $\mu = \lambda u$. But every totally positive unit of $K^+ = \mathbb{Q}(\sqrt{5})$ is an even power of the fundamental unit φ, so there is a unit v of K^+ with $u = v^2 = v\overline{v}$. Then the automorphism v of A gives an isomorphism of the polarized varieties (A, λ) and (A, μ). This proves the second statement of the proposition.

Applying Deligne's theorem again, we find that the abelian varieties over $\mathbb{F}_8$ with Weil polynomial f^2 correspond to the isomorphism classes of R-modules that can be embedded as lattices in the K-vector space $K \times K$. Since R is a Dedekind domain, such modules are determined up to isomorphism by their Steinitz classes in the class group of R. But the class group of R is trivial, so there is only one such R-module. Thus, the only abelian variety with Weil polynomial f^2 is $A \times A$.

Now suppose that μ is a principal polarization on $A \times A$. Let α be the automorphism $\mu^{-1} \circ (\lambda \times \lambda)$ of $A \times A$. Using the results of [16], Application III, pp. 208–210, again, we see that α is fixed by the Rosati involution associated to $\lambda \times \lambda$ and that α is totally positive, meaning that all of the roots (in the algebraic closure of K) of the minimal polynomial of α are totally positive algebraic numbers. If we identify $\mathrm{End}(A \times A)$ with the ring $M_2(R)$ of 2-by-2 matrices over R in the obvious way, then the Rosati involution is the conjugate-transpose involution, so we see that α is identified with a totally positive Hermitian matrix A of determinant 1. Thus, to show that μ is isomorphic to $\lambda \times \lambda$, we must show that every such Hermitian matrix can be written C^*C, where $C \in M_2(R)$ is nonsingular and where C^* is the conjugate transpose of C. But this is exactly the statement of Proposition 18. □

Before we prove Proposition 18 we must set some notation and give a Euclidean algorithm for the ring R.

Let L be the subfield $\mathbb{Q}(\zeta)$ of K and let $\mathcal{O}_L$ be the ring of integers $\mathbb{Z}[\zeta]$ of L. Let ϕ be the real number $(1 + \sqrt{5})/2$ and let ψ_1 and ψ_2 be two distinct embeddings of K into $\mathbb{C}$ that are not complex conjugates of one another. If z is a complex number, we let $|z|$ be its magnitude and we let $||z||$ be its norm, so that $||z|| = |z|^2 = z\bar{z}$.

LEMMA 19. — *For every x in K there is a y in R such that*

$$\mathrm{Norm}_{K/\mathbb{Q}}(x - y) \leqslant 5/9$$

and such that

$$||\psi_i(x - y)|| \leqslant \phi^4/3 \quad \text{for } i = 1, 2.$$

Proof. — Let D be the set of elements of L whose norm to $\mathbb{Q}$ is at most $1/3$. Then for every x in L there is a y in $\mathcal{O}_L$ such that $x - y$ lies in D. (It is easiest to see this by embedding L in the complex numbers, so that D becomes the intersection of L with the disk at the origin of radius $1/\sqrt{3}$. The latter disk clearly contains a fundamental region for the lattice $\mathcal{O}_L$.)

Write $x = x_1 + x_2\varphi$ for $x_1, x_2 \in L$. Choose y_1 and y_2 in O_L such that $x_1 - y_1$ and $x_2 - y_2$ lie in D. Let $y = y_1 + y_2\varphi$ and let $z_1 = x_1 - y_1$ and

$z_2 = x_2 - y_2$. Then

$$\begin{aligned}\mathrm{Norm}_{K/\mathbb{Q}}(x-y) &= \mathrm{Norm}_{L/\mathbb{Q}}(\mathrm{Norm}_{K/L}(z_1 + z_2\varphi)) \\ &= \mathrm{Norm}_{L/\mathbb{Q}}(z_1^2 + z_1 z_2 - z_2^2) \\ &= ||\psi_1(z_1^2 + z_1 z_2 - z_2^2)|| \\ &= ||d_1^2 + d_1 d_2 - d_2^2||\end{aligned}$$

where $d_1 = \psi_1(z_1)$ and $d_2 = \psi_1(z_2)$ are complex numbers that lie in the disk around the origin of radius $1/\sqrt{3}$. But an easy maximization argument shows that the maximum value of $||d_1^2 + d_1 d_2 - d_2^2||$ for d_1, d_2 in this disk is $5/9$.

Also, $\psi_i(x-y)$ is equal to either $d_1 + d_2(1+\sqrt{5})/2$ or $d_1 + d_2(1-\sqrt{5})/2$, depending on the image of φ under ψ_i. Since $|d_1|$ and $|d_2|$ are both at most $1/\sqrt{3}$, we see that

$$|\psi_i(x-y)| \leqslant \frac{1}{\sqrt{3}} \frac{3+\sqrt{5}}{2} = \frac{\phi^2}{\sqrt{3}}$$

so that $||\psi_i(x-y)|| \leqslant \phi^4/3$. □

We note that the $5/9$ in Lemma 19 could be reduced to $4/9$ if we used a hexagonal fundamental domain for the lattice $\mathcal{O}_L$ in place of the disk D, but doing so takes some effort and does not help much in the end.

LEMMA 20. — *Suppose n and d are elements of $\mathcal{O}_K$, with d nonzero. Then there are elements q and r of O_K such that $n = qd + r$ and such that*

$$\mathrm{Norm}_{K/Q}(r) \leqslant (5/9)\,\mathrm{Norm}_{K/Q}(d)$$

and

$$||\psi_i(r)|| \leqslant \frac{\phi^4}{3}||\psi_i(d)||$$

for $i = 1, 2$.

Proof. — Apply Lemma 19 to $x = n/d$, and let q be the resulting y. Then let $r = n - qd$. The lemma follows from the inequalities of Lemma 19. □

We are now ready to prove Proposition 18.

Proof of Proposition 18. — Write

$$A = \begin{bmatrix} \alpha & \overline{\beta} \\ \beta & \gamma \end{bmatrix}$$

for α, γ in the ring of integers of the maximal real subfield $K^+ = \mathbb{Q}(\varphi)$ of K and for β in R. Our strategy will be to modify A by invertible matrices C (that is, to replace A with C^*AC) in order to make the norm of the upper left hand element of A as small as possible.

The determinant of A is a totally positive unit in K^+, and so is an even power of the fundamental unit φ. By modifying A by a matrix C of the form

$$\begin{bmatrix} \varphi^i & 0 \\ 0 & 1 \end{bmatrix}$$

we may assume that A has determinant 1. Then by modifying A by a power of the matrix

$$\begin{bmatrix} \varphi & 0 \\ 0 & \varphi^{-1} \end{bmatrix}$$

we can ensure that the element α of $\mathcal{O}_{K^+}$ has the property that

$$\frac{1}{\phi^2} \leqslant \frac{\psi_1(\alpha)}{\psi_2(\alpha)} \leqslant \phi^2.$$

Another way of expressing this is to say that

$$\frac{1}{\phi^2} \leqslant \frac{\psi_i(\alpha)^2}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)} \leqslant \phi^2 \quad \text{for } i = 1, 2. \tag{1}$$

Apply Lemma 20 with $n = \beta$ and $d = \alpha$ to get a q and an r with $||\psi_i(r)|| \leqslant (\phi^4/3)||\psi_i(\alpha)||$ and with $\mathrm{Norm}_{K/\mathbb{Q}}(r) \leqslant (5/9)\,\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$. If we set

$$C = \begin{bmatrix} 1 & -\overline{q} \\ 0 & 1 \end{bmatrix}$$

then

$$C^*AC = \begin{bmatrix} \alpha & \overline{r} \\ r & \gamma' \end{bmatrix}$$

for some γ' in $\mathcal{O}_K^+$. Replace β with r and γ with γ', so that now we have

$$||\psi_i(\beta)|| \leqslant \frac{\phi^4}{3}||\psi_i(\alpha)|| \quad \text{for } i = 1, 2 \tag{2}$$

and

$$\mathrm{Norm}_{K/\mathbb{Q}}(\beta) \leqslant (5/9)\,\mathrm{Norm}_{K/\mathbb{Q}}(\alpha). \tag{3}$$

Let $B = \beta\overline{\beta}$, so that B is an element of $\mathcal{O}_K^+$. Note that we have $\alpha\gamma - B = 1$, so

$$\psi_i(\alpha)\psi_i(\gamma) = 1 + \psi_i(B) \quad \text{for } i = 1, 2$$

and

$$\psi_i(\gamma)/\psi_i(\alpha) = 1/\psi_i(\alpha)^2 + \psi_i(B)/\psi_i(\alpha)^2 \quad \text{for } i = 1, 2. \tag{4}$$

Now let

$$\begin{aligned} b_1 &= \psi_1(B)/\psi_1(\alpha^2) \\ b_2 &= \psi_2(B)/\psi_2(\alpha^2) \\ c_1 &= 1/\psi_1(\alpha^2) \\ c_2 &= 1/\psi_2(\alpha^2) \end{aligned}$$

so that equation (4) becomes

$$\psi_1(\gamma)/\psi_1(\alpha) = b_1 + c_1 \qquad \text{and} \qquad \psi_2(\gamma)/\psi_2(\alpha) = b_2 + c_2.$$

Multiplying these last two equalities gives

$$\mathrm{Norm}_{K^+/\mathbb{Q}}(\gamma/\alpha) = b_1 b_2 + b_1 c_2 + b_2 c_1 + c_1 c_2. \tag{5}$$

Note that

$$b_1 b_2 = \frac{\mathrm{Norm}_{K^+/\mathbb{Q}}(B)}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)^2} = \frac{\mathrm{Norm}_{K/\mathbb{Q}}(\beta)}{\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)} \leqslant \frac{5}{9} \tag{6}$$

(where the final inequality comes from (3)) and

$$c_1 c_2 = \frac{1}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha^2)}. \tag{7}$$

Furthermore, from inequality (1) we see that

$$c_1 \leqslant \frac{\phi^2}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)} \qquad \text{and} \qquad c_2 \leqslant \frac{\phi^2}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)}, \tag{8}$$

and from inequality (2) we see that

$$b_1 = \frac{||\psi_1(\beta)||}{||\psi_1(\alpha)||} \leqslant \frac{\phi^4}{3} \qquad \text{and} \qquad b_2 = \frac{||\psi_2(\beta)||}{||\psi_2(\alpha)||} \leqslant \frac{\phi^4}{3}. \tag{9}$$

If we view b_1, b_2, c_1, and c_2 as non-negative real variables subject only to the conditions expressed in equations (6), (7), (8), and (9), and if we maximize $b_1 c_1 + b_2 c_2$ subject to these conditions, we find that the maximum value occurs when $b_1 = \phi^4/3$ and $c_1 = \phi^2/\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)$. Thus we have

$$\begin{aligned} b_1 c_1 + b_2 c_2 &\leqslant \frac{\phi^4}{3}\,\frac{\phi^2}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)} + \frac{(5/9)}{(\phi^4/3)}\,\frac{(1/\phi^2)}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)} \\ &\leqslant \frac{6.08}{\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)}. \end{aligned} \tag{10}$$

Let $\epsilon = 1/\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha)$. Then by combining the relations (5), (6), (7) and (10) we find that

$$\mathrm{Norm}_{K^+/\mathbb{Q}}(\gamma/\alpha) \leqslant \epsilon^2 + 6.08\epsilon + 5/9.$$

If $\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha) \geqslant 15$ then $\epsilon < 0.07$ and $\mathrm{Norm}_{K^+/\mathbb{Q}}(\gamma/\alpha) < 1$. Then we can modify A by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

to exchange α and γ, and this decreases the norm of the upper left hand element of A.

We repeat this procedure until we reach the point where $\mathrm{Norm}_{K^+/\mathbb{Q}}(\alpha) \leqslant 14$. Up to Galois conjugacy there are 5 possible values for α: namely, 1, 2, $2+\varphi$, 3, and $3+\varphi$. Inserting the appropriate values of c_1 and c_2 into equation (5) and maximizing over b_1 and b_2, we find that we once again get $\mathrm{Norm}_{K^+/\mathbb{Q}}(\gamma/\alpha) < 1$ except when $\alpha = 1$ or $\alpha = 2$ or $\alpha = 2+\varphi$.

Note that $1 + \beta\overline{\beta}$ is divisible by α. If $\alpha = 2 + \phi$ then there are 6 possible residue classes modulo α that β could lie in. By modifying A by a power of

$$\begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$$

we can arrange that $\beta = 2$. Then A must be the matrix

$$\begin{bmatrix} 2+\varphi & 2 \\ 2 & 2+\overline{\varphi} \end{bmatrix}.$$

Modifying A by

$$\begin{bmatrix} 1-\varphi & 1 \\ \varphi & -1 \end{bmatrix}$$

gives us the identity.

For $\alpha = 2$ there are three possible residue classes for β. By modifying A by a power of

$$\begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$$

we can arrange for β to be 1. Then $\gamma = 1$, so again we can reduce the norm of the upper left hand corner of A by interchanging α and γ.

We finally get to the case $\alpha = 1$. If $\alpha = 1$ then we can reduce β to be 0. Then we find $\gamma = 1$, so that we have reduced A to the identity matrix. □

Appendix.

In this appendix we reproduce the output produced by our Magma program for the case $q = 4$, $g = 5$, $N = 18$.

```
Magma V2.9-10 Fri Sep 27 2002 17:22:30 [Seed = 729997397]
Type ? for help. Type <Ctrl>-D to quit.
> load "CheckQGN.magma";
Loading "CheckQGN.magma"
Loading "DeficientPolynomialList.magma"
> CheckQGN(4,5,18);
[ 18, 0, 4, 81, 164 ]
[
<x + 3, 3>,
<x^2 + 4 * x + 2, 1>
]
ELIMINATED: Not Weil polynomial.
[ 18, 0, 5, 74, 187 ]
[
<x + 3, 2>,
<x^3 + 7 * x^2 + 14 * x + 7, 1>
]
ELIMINATED: resultant=1 method.
Splitting = [ 1 ]
[ 18, 0, 6, 67, 210 ]
[
<x + 1, 1>,
<x + 2, 1>,
```

<$x+3,2$>,

<$x+4,1$>

]

ELIMINATED: resultant=2 method.

Splitting = [2]

Reasons: point counts, Riemann-Hurwitz

[18, 0, 6, 68, 200]

[

<$x+3,1$>,

<$x^2+5*x+5,2$>

]

ELIMINATED: resultant=1 method.

Splitting = [1]

[18, 0, 7, 60, 232]

[

<$x+2,2$>,

<$x+4,1$>,

<$x^2+5*x+5,1$>

]

ELIMINATED: resultant=1 method.

Splitting = [1, 2]

[18, 1, 0, 86, 168]

[

<$x+1,1$>,

<$x+3,4$>

]

ELIMINATED: resultant=2 method.

Splitting = [1]

Reasons: point counts, Riemann-Hurwitz

```
[ 18, 1, 1, 79, 190 ]
[
<x + 2, 1>,
<x + 3, 2>,
<x^2 + 5 * x + 5, 1>
]
ELIMINATED: resultant=1 method.
Splitting = [ 1 ]
[ 18, 1, 2, 71, 222 ]
[
<x + 2, 3>,
<x + 3, 1>,
<x + 4, 1>
]
ELIMINATED: resultant=1 method.
Splitting = [ 2 ]
> quit;
Total time: 4.940 seconds, Total memory usage: 9.22MB
```

BIBLIOGRAPHY

[1] W. BOSMA, J. CANNON and C. PLAYOUST, The Magma algebra system, I: The user language, J. Symbolic Comput., 24 (1997), 235–265.

[2] I. I. BOUW, The p-rank of curves and covers of curves, pp. 267–277 in: Courbes semi-stables et groupe fondamental en géométrie algébrique, (Jean-Benoît Bost, François Loeser, and Michel Raynaud, eds.), Progr. Math., 187, Birkhäuser, Basel 2000.

[3] P. DELIGNE, Variétés abéliennes ordinaires sur un corps fini, Invent. Math., 8 (1969), 238–243.

[4] S. A. DIPIPPO and E. W. HOWE, Real polynomials with all roots on the unit circle and abelian varieties over finite fields, J. Number Theory, 73 (1998), 426–450. Corrigendum, J. Number Theory, 83 (2000), 182, arXiv:math.NT/9803097.

[5] R. FUHRMANN and F. TORRES, The genus of curves over finite fields with many rational points, Manuscripta Math., 89 (1996), 103–106.

[6] G. VAN DER GEER and M. VAN DER VLUGT, Tables of curves with many points, Math. Comp., 69 (2000), 797–810.

[7] E. W. HOWE, Principally polarized ordinary abelian varieties over finite fields, Trans. Amer. Math. Soc., 347 (1995), 2361–2401.

[8] E. W. HOWE and H. J. ZHU, On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field, J. Number Theory, 92 (2002), 139–163, arXiv:math.AG/0002205.

[9] G. KORCHMÁROS and F. TORRES, On the genus of a maximal curve, Math. Ann., 323 (2002), 589–608, arXiv:math.AG/0008202.

[10] R. B. LAKEIN, Euclid's algorithm in complex quartic fields, Acta Arith., 20 (1972), 393–400.

[11] K. LAUTER, Improved upper bounds for the number of rational points on algebraic curves over finite fields, C. R. Acad. Sci. Paris, Sér. I Math., 328 (1999), 1181–1185.

[12] K. LAUTER, Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points, Proc. Amer. Math. Soc., 128 (2000), 369–374.

[13] K. LAUTER, Zeta functions of curves over finite fields with many rational points, pp. 167–174 in: Coding Theory, Cryptography, and Related Areas, (Johannes Buchmann, Tom Høholdt, Henning Stichtenoth, Horacio Tapia-Recillas, eds.), Springer-Verlag, Berlin, 2000.

[14] K. LAUTER with an Appendix by J-P. SERRE, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, J. Algebraic Geom., 10 (2001), 19–36, arXiv:math.AG/0104247.

[15] K. LAUTER with an Appendix by J-P. SERRE, The maximum or minimum number of rational points on genus three curves over finite fields, Compositio Math., 134 (2002), 87–111, arXiv:math.AG/0104086.

[16] D. MUMFORD, Abelian Varieties, Tata Institute of Fundamental Research Studies in Mathematics, 5, Oxford University Press, Oxford, 1985.

[17] F. OORT, Commutative group schemes, Lecture Notes in Math., 15, Springer-Verlag, Berlin, 1966.

[18] D. SAVITT with an Appendix by K. LAUTER, The maximum number of rational points on a curve of genus 4 over $\mathbb{F}_8$ is 25, Canad. J. Math., 55 (2003), 331–352, arXiv:math.NT/0201226.

[19] J.-P. SERRE, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris, Sér. I Math., 296 (1983), 397–402; = Œuvres [128].

[20] J.-P. SERRE, Nombres de points des courbes algébriques sur $\mathbb{F}_q$, Sém. Théor. Nombres Bordeaux 1982/83, Exp. n° 22; = Œuvres [129].

[21] J.-P. SERRE, Résumé des cours de 1983–1984, Ann. Collège France (1984), 79–83; = Œuvres [132].

[22] J.-P. SERRE, Rational points on curves over finite fields, unpublished notes by Fernando Q. Gouvéa of lectures at Harvard University, 1985.

[23] C. L. SIEGEL, The trace of totally positive and real algebraic integers, Ann. of Math. (2), 46 (1945), 302–312.

[24] C. SMYTH, Totally positive algebraic integers of small trace, Ann. Inst. Fourier (Grenoble), 33-3 (1984), 1–28.

[25] H. M. STARK, On the Riemann hypothesis in hyperelliptic function fields, pp. 285–302 in: Analytic number theory (Harold G. Diamond, ed.), Proc. Sympos. Pure Math., 24, American Mathematical Society, Providence, R.I., 1973.

[26] H. STICHTENOTH, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

[27] K.-O. STÖHR and J. F. VOLOCH, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3), 52 (1986), 1–19.

[28] D. SUBRAO, The p-rank of Artin-Schreier curves, Manuscripta Math., 16 (1975), 169–193.

[29] J. TATE, Classes d'isogénie des variétés abéliennes sur un corps fini, Exp. n° 352, pp. 95–110 in: Séminaire Bourbaki 1968/69, Lecture Notes in Math., 179, Springer-Verlag, Berlin, 1971.

[30] M. E. ZIEVE, Improving the Oesterlé bound, preprint.

Manuscrit reçu le 9 septembre 2002,
accepté le 24 mars 2003.

Everett W. HOWE,
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1967 (USA).
however@alumni.caltech.edu
http://www.alumni.caltech.edu/~however/
&
Kristin E. LAUTER,
Microsoft Research
One Microsoft Way
Redmond, WA 98052 (USA).
klauter@microsoft.com