

CURVES OF MEDIUM GENUS WITH MANY POINTS

EVERETT W. HOWE

ABSTRACT. The *defect* of a curve over a finite field is the difference between the number of rational points on the curve and the Weil–Serre upper bound for the number of points on the curve. We present algorithms for constructing curves of genus 5, 6, and 7 with small defect. Our aim is to be able to produce, in a reasonable amount of time, curves that can be used to populate the online table of curves with many points found at manypoints.org.

1. INTRODUCTION

For every prime power q and non-negative integer g , we let $N_q(g)$ denote the maximum number of rational points on a smooth, projective, absolutely irreducible curve of genus g over the finite field \mathbf{F}_q . At the turn of the present century, van der Geer and van der Vlugt published tables [5] of the best upper and lower bounds on $N_q(g)$ known at the time, for $g \leq 50$ and for q ranging over small powers of 2 and 3. In 2010, van der Geer, Lauter, Ritzenthaler, and the author (with technical assistance from Gerrit Oomens) created the [manypoints](http://manypoints.org) web site [4], which gives the currently-known best upper and lower bounds on $N_q(g)$ for $g \leq 50$ and for a range of prime powers q : the primes less than 100, the prime powers p^i for $p < 20$ and $i \leq 5$, and the powers of 2 up to 2^7 .

The *Weil–Serre upper bound* [16] for $N_q(g)$ states that

$$N_q(g) \leq q + 1 + g[2\sqrt{q}].$$

When $q \geq (g + \sqrt{g+1})^2$ the Weil–Serre bound is almost always the best upper bound currently known for $N_q(g)$; the exceptions come from “exceptional” prime powers [6, Theorem 4, p. 1682] and from careful case-by-case analyses — see the introduction to [9] for a summary. On the other hand, lower bounds for $N_q(g)$ are generally obtained by producing more-or-less explicit examples of curves with many points. Typically, this is done by searching through specific families of curves — for instance, families of curves obtained via class field theory as covers of lower-genus curves, or families of curves with specific nontrivial automorphism groups. For small finite fields of characteristic 2 and 3, such searches have been carried out for many genera, so even the earliest versions of the van der Geer–van der Vlugt tables gave nontrivial lower bounds for many values of $N_q(g)$.

One of the goals of the [manypoints](http://manypoints.org) web site is to encourage researchers to consider curves over finite fields of larger characteristics. Curves over these fields have received far less attention than curves in characteristic 2 or 3, so at present the table entries for lower bounds for $N_q(g)$ remain unpopulated for most q and g .

Date: 29 March 2017.

2010 Mathematics Subject Classification. Primary 11G20; Secondary 14G05, 14G10, 14G15.

Key words and phrases. Curve, Jacobian, rational point, defect.

Of course, there are trivial lower bounds for $N_q(g)$: for instance, if C is a hyper-elliptic curve of any genus over \mathbf{F}_q , then either C or its quadratic twist will have at least $q + 1$ points. To avoid having to worry about such “poor” lower bounds, van der Geer and van der Vlugt decided not to print a lower bound for $N_q(g)$ in their tables unless it was greater than $1/\sqrt{2}$ times the best upper bound known for $N_q(g)$. This restriction was adopted for the [manypoints](#) table as well, but it turns out that it is not a strong enough filter when q is large with respect to g . The administrators of the [manypoints](#) site are considering replacing it with the requirement that a lower bound not be published unless the difference between the lower bound and $q + 1$ is at least $1/\sqrt{2}$ times the difference between the best proven upper bound and $q + 1$.

Every genus-0 curve over a finite field is isomorphic to \mathbf{P}^1 , so $N_q(0) = q + 1$ for all q . For $g = 1$ and $g = 2$, the value of $N_q(g)$ is also known for all q . For $g = 1$ this is due to a classical result of Deuring [3] (see [19, Theorem 4.1, p. 536]); for $g = 2$, this is due to work of Serre [16, 15, 17] (see also [11]). There is no easy formula known for $N_q(3)$, but for all q in the [manypoints](#) table the value has been computed; see the introduction to [14]. For genus 4, the exact value of $N_q(4)$ is known for 43 of the 59 prime powers q in the [manypoints](#) table, and for the remaining 16 prime powers the lower bound for $N_q(4)$ is within 4 of the best proven upper bound; see [7] and [8].

In this paper we develop methods for finding curves of genus 5, 6, and 7 with reasonably many points. Our goal is to find lower bounds for $N_q(g)$ for these genera that are somewhat close to the best proven upper bounds, in order to “raise the bar” for what counts as an interesting example. We hope that this will inspire others to think of new constructions, new search strategies, and faster algorithms.

The *defect* of a curve C of genus g over \mathbf{F}_q is the difference between $\#C(\mathbf{F}_q)$ and the Weil–Serre upper bound for genus- g curves over \mathbf{F}_q . If $\pi_1, \bar{\pi}_1, \dots, \pi_g, \bar{\pi}_g$ are the Frobenius eigenvalues (with multiplicity) of C , listed in complex-conjugate pairs, then we have

$$\#C(\mathbf{F}_q) = q + 1 - (\pi_1 + \bar{\pi}_1 + \dots + \pi_g + \bar{\pi}_g),$$

so the defect of C is given by

$$(q + 1 + g\lfloor 2\sqrt{q} \rfloor) - \#C(\mathbf{F}_q) = \sum_{i=1}^g (\lfloor 2\sqrt{q} \rfloor + \pi_i + \bar{\pi}_i).$$

If the Jacobian of C decomposes up to isogeny as the product of the Jacobians of some other curves C_i , then the multiset of Frobenius eigenvalues for C is the union of the multisets of Frobenius eigenvalues for the C_i , and it follows that the defect of C is the sum of the defects of the C_i .

The ideas behind our new constructions for producing curves of genus 5, 6, and 7 with small defect are similar to those used in [8] to produce curves of genus 4 with small defect. The basic strategy is to search through families of curves D that are Galois extensions of \mathbf{P}^1 with group G isomorphic to a 2-torsion group; in practice, we will consider $G \cong (\mathbf{Z}/2\mathbf{Z})^2$ and $G \cong (\mathbf{Z}/2\mathbf{Z})^3$. The extension $D \rightarrow \mathbf{P}^1$ will then have $\#G - 1$ subextensions $C_i \rightarrow \mathbf{P}^1$ of degree 2, corresponding to the index-2 subgroups of G . A result of Kani and Rosen [12, Theorem B, p. 308] says that in this situation, the Jacobian of D is isogenous to the product of the Jacobians of

the C_i ; it follows that the genus of D is the sum of the genera of the C_i , and the defect of D is equal to the sum of the defects of the C_i .

Within this basic framework, however, there are many ways of structuring an algorithm, some of which are much more efficient than others. In Section 2 we review the genus-4 construction used in our earlier paper [8], and we describe our new constructions for higher genera in Sections 3, 4, and 5.

At various points in this paper we will find it convenient to consider the *minimal defect* $D_q(g)$ for genus- g curves over \mathbf{F}_q , which we define by

$$D_q(g) = q + 1 + g[2\sqrt{q}] - N_q(g).$$

Giving a lower bound for $N_q(g)$ is equivalent to giving an upper bound for $D_q(g)$.

The computations we describe in this paper were implemented in Magma [1] on a 2010-era laptop computer, with a 2.66 GHz Intel Core i7 “Arrandale” processor and 8 GB of RAM.

2. REVIEW OF THE GENUS-4 CONSTRUCTION

In [8], we presented an algorithm to produce genus-4 curves D of small defect over finite fields \mathbf{F}_q of odd characteristic. The heuristic argument presented in [8] leads us to expect that as q ranges over all sufficient large primes and over almost all prime powers, the algorithm will produce a genus-4 curve with defect at most 4 in time $\tilde{O}(q^{4/3})$. The construction has two main ideas: First, if one is given a genus-2 curve C/\mathbf{F}_q that can be written $y^2 = f_1 f_2$ for two cubic polynomials f_1 and f_2 in $\mathbf{F}_q[x]$, then one can efficiently find a value of $a \in \mathbf{F}_q$, if such a value exists, such that the two genus-1 curves E_1 and E_2 defined by $y^2 = (x - a)f_1$ and $y^2 = (x - a)f_2$ have small defect. If such an a exists, and if we let D be the curve defined by the two equations $w^2 = (x - a)f_1$ and $z^2 = (x - a)f_2$, then the degree-4 cover $D \rightarrow \mathbf{P}^1$ that sends (x, w, z) to x is a Galois extension, with group $(\mathbf{Z}/2\mathbf{Z})^2$, and we have the following diagram, in which each arrow denotes a degree-2 map:

$$(1) \quad \begin{array}{ccccc} & & D & & \\ & \swarrow & \downarrow & \searrow & \\ E_1 & & C & & E_2 \\ & \swarrow & \downarrow & \searrow & \\ & & \mathbf{P}^1 & & \end{array}$$

This is the situation described in Section 1, and we find that the genus of D is 4 and the defect of D is equal to the sum of the defects of E_1 , E_2 , and C . In particular, since E_1 and E_2 have small defect, we see that the defect of D is not much larger than the defect of C .

The second main idea in the construction of [8] is to have a method for efficiently producing genus-2 curves C with small defect. In [8] this is accomplished by taking pairs of elliptic curves with small defect, “gluing” them together along their 2- or 3-torsion subgroups using [10, Proposition 4, p. 325] and [2, Algorithm 5.4, p. 185] to produce genus-2 curves with small defect, and then using Richelot isogenies to produce more and more curves with small defect from these seed curves.

The algorithm to produce genus-4 curves with small defect works by producing many genus-2 curves with small defect (using the second idea) until one is produced

for which one can find a value of a (using the first idea) that leads to a diagram like Diagram (1).

We note for future reference that the discussion leading up to Heuristic 5.6 in [8] suggests that for fixed d and for $q \rightarrow \infty$ we might expect there to be on the order of $d^{3/2}q^{3/4}$ genus-2 curves of defect d . Therefore, we might also expect there to be on the order of $d^{5/2}q^{3/4}$ genus-2 curves of defect d or less. Similarly, we might expect there to be on the order of $d^{3/2}q^{1/4}$ elliptic curves of defect d or less. Since there are about $2q$ elliptic curves over \mathbf{F}_q and about $2q^3$ curves of genus 2, we see that it is reasonable to expect that a random elliptic curve will have defect at most d with probability on the order of $d^{3/2}/q^{3/4}$, while a random genus-2 curve will have defect at most d with probability on the order of $d^{5/2}/q^{9/4}$.

3. CONSTRUCTIONS FOR GENUS-5 CURVES

Before we describe our algorithms for constructing genus-5 curves with small defect, we present a technique for efficiently computing all separable quartics and cubics over a finite field k , up to squares in k^* and the action of $\mathrm{PGL}_2(k)$.

Let $k = \mathbf{F}_q$ be a finite field of odd characteristic, and let S denote the set of separable quartics and cubics in $k[x]$. The group of squares in k^* acts on S by multiplication, and the group $\mathrm{PGL}_2(k)$ acts on S modulo squares as follows: Given $f \in S/k^{*2}$ and $\alpha \in \mathrm{PGL}_2(k)$, we let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a matrix that represents α , and we define

$$\alpha(f \bmod k^{*2}) = (cx + d)^4 f\left(\frac{ax + b}{cx + d}\right) \bmod k^{*2}.$$

Had we chosen a different matrix to represent α , the right-hand side of the preceding equality would be modified by a square, so we do get a well-defined action of $\mathrm{PGL}_2(k)$ on S/k^{*2} . In one of our algorithms it will be useful to be able to quickly calculate orbit representatives for S under this combined action.

Given a separable quartic or cubic $f \in k[x]$, let C be the curve $y^2 = f$ and let E be the Jacobian of C . Since C has genus 1, E is an elliptic curve, and since genus-1 curves over k have rational points, there is an isomorphism $\varphi: C \rightarrow E$. Under this isomorphism, the involution ι of C given by $(x, y) \mapsto (x, -y)$ becomes an involution on E , which must be of the form $P \mapsto P_0 - P$ for some point P_0 in $E(k)$. If $\varphi': C \rightarrow E$ is another isomorphism, then there is an automorphism ε of E and a point $Q_0 \in E(k)$ such that

$$\varphi'(P) = \varepsilon\varphi(P) + Q_0,$$

so that φ' takes the involution ι on C to the involution $P \mapsto P'_0 - P$ on E , where $P'_0 = \varepsilon(P_0) + 2Q_0$. Thus, given $f \in S$, we obtain a pair $(E, [P_0])$, where E is an elliptic curve over k and $[P_0]$ is an element of $E(k)/2E(k)$ up to the action of $\mathrm{Aut} E$.

Lemma. *The map from S to pairs $(E, [P_0])$ defined above induces a bijection between the orbits of S/k^{*2} under the action of $\mathrm{PGL}_2(k)$ and the set of all pairs $(E, [P_0])$.*

Proof. The pair $(E, [P_0])$ that we obtain from f clearly depends only on the isomorphism class of the pair (C, ι) , and that isomorphism class is fixed by the actions of k^{*2} and $\mathrm{PGL}_2(k)$. Thus, we do indeed get a map from orbits to pairs.

Suppose f_1 and f_2 are two elements of S that give rise to the same pair $(E, [P_0])$. Let C_1 and C_2 be the curves $y^2 = f_1$ and $y^2 = f_2$, respectively, with involutions ι_1 and ι_2 . Then there are isomorphisms $\varphi_1: C_1 \rightarrow E$ and $\varphi_2: C_2 \rightarrow E$ that take ι_1

and ι_2 to the involution $P \mapsto P_0 - P$ of E , so the isomorphism $\psi = \varphi_2^{-1}\varphi_1$ from C_1 to C_2 takes ι_1 to ι_2 . It follows that ψ is of the form

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^2} \right)$$

for some $a, b, c, d, e \in k$. We see that $f_1 \bmod k^{*2} = \alpha(f_2 \bmod k^{*2})$, where α is the class of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\text{PGL}_2(k)$. Thus, the map from orbits to pairs is injective.

To finish the proof, we need to show that the map from orbits to pairs is surjective. Suppose E is an elliptic curve over k and P_0 is a point in $E(k)$. We will produce a cubic or quartic f that gives rise to the pair $(E, [P_0])$.

Let $y^2 = g$ be a Weierstrass model for E , where $g \in k[x]$ is a monic cubic. If P_0 is the infinite point on E then we can just take $f = g$, so assume that P_0 is an affine point (x_0, y_0) . By replacing $g(x)$ with $g(x + x_0)$, we may assume that $x_0 = 0$, so that g is of the form $x^3 + ax^2 + bx + c^2$ and $P_0 = (0, c)$.

Let $f = x^4 - 2ax^2 - 8cx + a^2 - 4b$. We compute that the discriminant of f is 2^{12} times the discriminant of g , so f is a separable quartic. If we let C be the curve $y^2 = f$, then there is an isomorphism $\psi: C \rightarrow E$ given by

$$(x, y) \mapsto \left(\frac{y + x^2 - a}{2}, \frac{x(y + x^2 - a)}{2} - c \right),$$

and we compute that the two infinite points on C are sent to the points P_0 and ∞ on E . It follows that the involution ι , which swaps the two infinite points on C , gets sent to the involution $P \mapsto P_0 - P$, which swaps P_0 and ∞ . Thus every pair $(E, [P_0])$ comes from an element of S . \square

Note that the proof of this lemma gives us an algorithm for producing representatives for all of the orbits of S/k^{*2} under the action of $\text{PGL}_2(k)$, in time $\tilde{O}(q)$: For each j -invariant in k , we list all the isomorphism classes of elliptic curves E with that j -invariant, compute the group $E(k)/2E(k)$ up to the action of $\text{Aut } E$, and for a representative point P_0 for each element we compute the quartic f that appears at the end of the proof of the lemma.

We turn now to our constructions of small-defect curves of genus 5 over a finite field $k = \mathbf{F}_q$ of odd characteristic. Our strategy for producing such curves will be to construct diagrams like Diagram (1), except that the genera of the intermediate curves will be 2, 1, and 2, instead of 1, 2, and 1. In other words, our aim will be to construct a diagram

$$(2) \quad \begin{array}{ccccc} & & D & & \\ & \swarrow & \downarrow & \searrow & \\ C_1 & & E & & C_2 \\ & \searrow & \downarrow & \swarrow & \\ & & \mathbf{P}^1 & & \end{array}$$

in which C_1 and C_2 are genus-2 curves with small defect, E is a genus-1 curve with small defect, and the arrows are maps of degree 2. This means that we would like to find genus-2 curves $w^2 = fg_1$ and $z^2 = fg_2$, where f is a quartic or a cubic polynomial and g_1 and g_2 are coprime quadratics, such that both of the genus-2

curves have small defect, and such that the genus-1 curve $y^2 = g_1g_2$ also has small defect. (If f is a quartic, we can also allow one of g_1 and g_2 to be linear.)

Our first strategy runs as follows. We begin by enumerating separable quartics and cubics $f \in k[x]$ up to the action of k^{*2} and $\text{PGL}_2(k)$, as outlined above. For each such f we enumerate all quadratic and linear polynomials g , up to squares in k^* , such that fg is separable of degree 5 or 6 and such that $y^2 = fg$ has small defect. We then consider all pairs (g_1, g_2) of such g such that g_1g_2 is separable of degree 3 or 4, and we check whether $y^2 = g_1g_2$ has small defect. The meaning of “having small defect” will change dynamically as we run the algorithm, depending on the smallest defect we have found so far for a triple (f, g_1, g_2) .

This first strategy works well for small q , and it is guaranteed to find the genus-5 curve of smallest defect that fits into a diagram like Diagram (2). However, there are on the order of q quartics and cubics f to consider, and for each f we have to enumerate on the order of q^2 quadratics and linears g , and for each (f, g) pair we have to compute the number of points on a genus-2 curve. Assuming we count points naïvely, this means that even just this portion of our first strategy will already take time roughly on the order of q^4 .

For larger fields, therefore, we use an alternate strategy. To produce our pairs of genus-2 curves, we will enumerate many genus-2 curves with small defect, keeping track of the ones that can be written $y^2 = h$ with h the product of a quartic and a quadratic in $k[x]$. Suppose we have two such curves, $w^2 = f_1g_1$ and $z^2 = f_2g_2$. We would like to be able to tell whether a change of coordinates (via a linear fractional transformation in x) could transform f_2 into a constant times f_1 . There are two necessary conditions for this to happen: First, the degrees of the irreducible factors of f_1 must match those of f_2 , and second, the j -invariants of the genus-1 curves $y^2 = f_1$ and $y^2 = f_2$ must be equal. These two conditions are not quite sufficient — there’s only one chance in three that two different products of irreducible quadratics with the same j -invariant can be transformed to constant multiples of one another via a linear fractional transformation, and there are additional complications for curves with j -invariant 0 or 1728 — but for our purposes these necessary conditions will be good enough as a first test.

So our second strategy will be to enumerate genus-2 curves with small defect that can be written $y^2 = fg$ with f a quartic and g a quadratic, and keep a list of the curves together with the j -invariants and factorization degrees of the associated quartics f . Whenever a j -invariant and set of factorization degrees occurs twice, and the associated quartics can be transformed into one another, we will have found two genus-2 curves $y^2 = f_1g_1$ and $y^2 = f_2g_2$ that can be put into Diagram (2) (provided that the linear fractional transformation that takes f_2 to f_1 does not take g_2 to a quadratic with a factor in common with g_1). Then we need to compute the number of points on the genus-1 curve in the middle of the diagram to see whether it has small defect.¹

To produce genus-2 curves with small defect, we use the technique mentioned in the previous section: We “glue together” pairs of elliptic curves with small defect,

¹ Warning: On versions of Magma at least up to V2.22-3, using `#HyperellipticCurve(f)` to count the number of points on $y^2 = f$ will produce incorrect results when f is a quartic with nonsquare leading coefficient over a finite field with more than 10^6 elements. This affects us when $q = 17^5$ or $q = 19^5$.

| q | range | q | range | q | range | q | range |
|----------------|--------------|-----------------|--------------|-----------------|--------------|-----|-------------|
| 3 | 6–6 | 11 | 4–5 | 19 | 3– 6 | 67 | 0– 8 |
| 3 ² | 5–8 | 11 ² | 0–0 | 19 ² | 0–0 | 71 | 0–0 |
| 3 ³ | 3–6 | 11 ³ | 0– 0 | 19 ³ | 0– 5 | 73 | 3– 9 |
| 3 ⁴ | 0– 4 | 11 ⁴ | 0–0 | 19 ⁴ | 0– 4 | 79 | 0– 5 |
| 3 ⁵ | 2– 13 | 11 ⁵ | 0–0 | 19 ⁵ | 0– 15 | 83 | 2– 8 |
| 5 | 6–6 | 13 | 5–9 | 23 | 3– 5 | 89 | 0– 4 |
| 5 ² | 4– 8 | 13 ² | 0– 4 | 29 | 2– 4 | 97 | 0– 5 |
| 5 ³ | 3– 12 | 13 ³ | 0– 9 | 31 | 5–5 | | |
| 5 ⁴ | 0– 8 | 13 ⁴ | 0– 8 | 37 | 4– 8 | | |
| 5 ⁵ | 0– 17 | 13 ⁵ | 0– 8 | 41 | 0–5 | | |
| 7 | 5–7 | 17 | 5– 8 | 43 | 3– 9 | | |
| 7 ² | 0–0 | 17 ² | 0– 4 | 47 | 0– 5 | | |
| 7 ³ | 3– 9 | 17 ³ | 2– 10 | 53 | 0– 4 | | |
| 7 ⁴ | 0– 8 | 17 ⁴ | 0– 4 | 59 | 2– 7 | | |
| 7 ⁵ | 0– 15 | 17 ⁵ | 0– 5 | 61 | 0–5 | | |

TABLE 1. The best upper and lower bounds known for the minimal defect $D_q(5)$ for the odd values of q represented in the [manypoints](#) table, as of 29 March 2017. The upper bounds in boldface come from computations described in this paper.

and then use Richelot isogenies to find more and more genus-2 curves with Jacobians isogenous to the product of the given elliptic curves.

As we continue to compute, we will find more and more examples. If at a certain point we have found a genus-5 curve with defect d , then we know that we can stop looking for better examples once we have examined all of the genus-2 curves with defect at most d that we can construct using the technique described above. If we continue to run the algorithm until this has happened, we say that we have *run the algorithm to completion*. Running to completion simply means that we have reached a point when we know that continuing to run the algorithm will not produce any examples better than what we have already found.

We ran the first algorithm for all of the odd prime powers q listed in the [manypoints](#) table with $q \leq 19^2$. On the modest laptop described in Section 1, the computation took 50 minutes for $q = 17^2$ and 108 minutes for $q = 19^2$. For the larger q in the [manypoints](#) table, we were able to run the second algorithm to completion; the computation for $q = 19^5$ took nearly 30 hours. In Table 1 we present the current lower and upper bounds on the minimal defect $D_q(5)$ for the odd values of q listed in the online table, with the upper bound in boldface if it was obtained from our computations. Equations for the curves we found can be obtained from the [manypoints](#) site by clicking on the appropriate table entry.

One could also try to construct curves of genus 5 by considering diagrams like Diagram (1) in which the genera of the intermediate curves are 1, 3, and 1; Soomro [18] takes this approach.

4. CONSTRUCTIONS FOR GENUS-6 CURVES

We work over a finite field $k = \mathbf{F}_q$ of odd characteristic. The genus-6 curves that we will construct will fit into a diagram

$$(3) \quad \begin{array}{ccccc} & & D & & \\ & \swarrow & \downarrow & \searrow & \\ C_1 & & C_2 & & C_3 \\ & \searrow & \downarrow & \swarrow & \\ & & \mathbf{P}^1, & & \end{array}$$

where the curves C_1 , C_2 , and C_3 have genus 2 and where the arrows represent degree-2 maps. Then the defect of D will be the sum of the defects of the C_i . To produce such a diagram, we need to find three cubic polynomials f_1 , f_2 , and f_3 such that each curve C_i is given by $y^2 = \prod_{j \neq i} f_j$. (Actually, one of the f_i could be a quadratic; this will be the case when two of the C_i have a Weierstrass point at infinity.) And, of course, we want the C_i to have small defect.

Before we describe how to construct good triples (f_1, f_2, f_3) , we note that we can define an action of $\mathrm{PGL}_2(k)$ on the set of separable cubics and quadratics in $k[x]$, up to multiplicative constants in k^* , analogous to the action we defined in Section 3 for quartics and cubics up to squares in k^* . Given a cubic or quadratic $f \in k[x]/k^*$ and $\alpha \in \mathrm{PGL}_2(k)$, we let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a matrix that represents α , and we define

$$\alpha(f \bmod k^*) = (cx + d)^3 f\left(\frac{ax + b}{cx + d}\right) \bmod k^*.$$

Since everything is defined only up to k^* , this does not depend on the choice of representative for α . Now we set $g_1 = x(x-1)$, and we fix irreducible quadratic and cubic polynomials g_2 and g_3 . It is easy to see from the 3-transitive action of $\mathrm{PGL}_2(\bar{k})$ on $\mathbf{P}^1(\bar{k})$ that every separable cubic or quadratic polynomial $h \in k[x]$ can be transformed by an element of $\mathrm{PGL}_2(k)$ into a constant times one of the polynomials g_1 , g_2 , or g_3 , depending on the degrees of the irreducible factors of h .

We construct triples (f_1, f_2, f_3) as follows. We start enumerating genus-2 curves C with small defect, and we keep track of the ones that can be written $y^2 = h_1 h_2$, where h_1 and h_2 are cubics. For every such representation of C , we apply a linear fractional transformation that takes h_1 to a constant times one of our three fixed polynomials g_1 , g_2 , g_3 . That means we can write C as $y^2 = g_i f$ for some cubic (or, in some circumstances, quadratic) polynomial f . Whenever we add a new pair (g_i, f) to our growing list, we look at all other pairs (g_i, \hat{f}) already on our list, and we check to see whether $y^2 = f\hat{f}$ is a curve with small defect. If so, by setting $f_1 = f$ and $f_2 = \hat{f}$ and $f_3 = g_i$ we have a triple (f_1, f_2, f_3) that gives us a genus-6 curve with small defect.

We continue enumerating genus-2 curves C with small defect until we reach the defect of the current record-holding triple (f_1, f_2, f_3) . At this point we are guaranteed that we will find no curves of smaller defect by using this construction, and again we say that we have run the algorithm to completion.

One way of producing genus-2 curves of small defect is simply to make a list of all curves of the form $y^2 = g_i f$ for $i = 1, 2, 3$ and for f ranging over the separable cubic

and quadratic polynomials in $k[x]$, up to squares in k^* . Then one can compute the defects of the curves in the list, and sort the list accordingly.

If the field k is too large for this to be feasible, and if k has a proper subfield, one can instead consider only the cubics and quadratics f with coefficients in the subfield. This is much faster, but of course results in missing many possible curves that might have small defect.

A third possibility is to use the procedure already described in earlier sections: gluing together pairs of elliptic curves of small defect, and using Richelot isogenies to obtain even more genus-2 curves.

And finally, we have a fourth algorithm with a slightly different flavor, which depends on the observation that a random element of $\mathrm{PGL}_2(\mathbf{F}_q)$ has order 3 with probability approximately $1/q$. (More precisely, by computing the centralizer of the image of $\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ in $\mathrm{PGL}_2(\mathbf{F}_q)$, one shows that the fraction of elements of $\mathrm{PGL}_2(\mathbf{F}_q)$ of order 3 is equal to either $1/q$ or $1/(q-1)$ or $1/(q+1)$, depending on whether q is congruent to 0, 1, or 2 modulo 3.)

We enumerate genus-2 curves with small defect by gluing together elliptic curves and using Richelot isogenies. Suppose C is such a curve, say given by an equation $y^2 = g$, where g is a sextic polynomial, and suppose we can write g as $f_1 f_2$, where f_1 and f_2 are cubics. We compute all of the linear fractional transformations μ that take the roots of f_2 to the roots of f_1 . Suppose further that one such μ has order 3 in $\mathrm{PGL}_2(k)$; if we assume that μ behaves like a random element of $\mathrm{PGL}_2(k)$, this will happen with probability about $1/q$. In this case, we write $\mu = (ax+b)/(cx+d)$; the condition that μ has order 3 means that $a^2 + ad + d^2 + bc = 0$. Let e be the constant such that $f_2(x) = e f_1(\mu)(cx+d)^3$, and set $f_3(x) = e f_2(\mu)(cx+d)^3$. Note that then

$$e f_3(\mu)(cx+d)^3 = -e^3(a+d)^9 f_1(x).$$

We see that change of variables $(x, y) \mapsto (\mu, e^{-1}y/(cx+d)^3)$ gives an isomorphism from the curve $y^2 = f_2 f_3$ to the curve $y^2 = f_1 f_2$, and if $-e(a+d)^3$ is a square, say $-e(a+d)^3 = s^2$, then $(x, y) \mapsto (\mu, e^{-1}s^3 y/(cx+d)^3)$ gives an isomorphism from $y^2 = f_3 f_1$ to $y^2 = f_2 f_3$. Thus, if $-e(a+d)^3$ is a square, the triple (f_1, f_2, f_3) gives us a diagram like Diagram (3) in which the three curves C_1 , C_2 , and C_3 are all isomorphic to the small-defect curve C that we started with. Then the genus-6 curve D has defect equal to three times the defect of C .

Asymptotically, we expect this last algorithm to be much faster than the other three, because we are waiting on an event with probability roughly $1/q$, rather than the much rarer event that a random genus-2 curve has small defect. As we noted in Section 2, the heuristics from [8] lead us to expect that the probability that a random genus-2 curve over \mathbf{F}_q has defect at most d grows like $d^{5/2}q^{-9/4}$.

We implemented all four algorithms. We applied the first to all odd $q < 100$ listed in the `manypoints` table. (For $q = 97$ this took 8 minutes on the laptop computer described in Section 1.) We applied the second to all odd $q > 100$ from the `manypoints` table, using the largest subfield of cardinality less than 100. (This took 2 minutes for $q = 7^4$.) We applied the third method to the q with $100 < q < 19^3$ and the fourth method to the q with $q \geq 19^3$. (The third method took 370 minutes for $q = 17^3$ and the fourth method took 15 minutes for $q = 19^5$. However, for $q = 17^5$ the fourth method took nearly 28 hours, because the smallest defect found — 108 — is quite large.) In Table 2 we present the current lower and upper bounds on the minimal defect $D_q(6)$ for the odd values of q listed in the online

| q | range | q | range | q | range | q | range |
|----------------|--------------|-----------------|---------------|-----------------|--------------|-----|-------------|
| 3 | 8–8 | 11 | 3–8 | 19 | 3– 8 | 67 | 0–12 |
| 3 ² | 8–11 | 11 ² | 0–0 | 19 ² | 0–0 | 71 | 0– 8 |
| 3 ³ | 4–12 | 11 ³ | 0– 0 | 19 ³ | 0– 14 | 73 | 2–6 |
| 3 ⁴ | 0–0 | 11 ⁴ | 0– 6 | 19 ⁴ | 0– 6 | 79 | 0–6 |
| 3 ⁵ | 2– 14 | 11 ⁵ | 0– 0 | 19 ⁵ | 0– 18 | 83 | 2–12 |
| 5 | 6–8 | 13 | 6–6 | 23 | 3– 8 | 89 | 0– 4 |
| 5 ² | 4–6 | 13 ² | 0–0 | 29 | 2– 8 | 97 | 0– 8 |
| 5 ³ | 3– 14 | 13 ³ | 0– 14 | 31 | 6– 10 | | |
| 5 ⁴ | 0–0 | 13 ⁴ | 0–0 | 37 | 6–12 | | |
| 5 ⁵ | 0– 20 | 13 ⁵ | 0– 24 | 41 | 2– 10 | | |
| 7 | 6– 10 | 17 | 6– 10 | 43 | 6– 14 | | |
| 7 ² | 0– 8 | 17 ² | 0–0 | 47 | 3–6 | | |
| 7 ³ | 3– 16 | 17 ³ | 2– 12 | 53 | 3–6 | | |
| 7 ⁴ | 0–0 | 17 ⁴ | 0–0 | 59 | 3– 10 | | |
| 7 ⁵ | 2– 42 | 17 ⁵ | 0– 108 | 61 | 0– 8 | | |

TABLE 2. The best upper and lower bounds known for the minimal defect $D_q(6)$ for the odd values of q represented in the [manypoints](#) table, as of 29 March 2017. The upper bounds in boldface come from computations described in this paper.

table, with the upper bound in boldface if it was obtained from our computations. Equations for the curves we found can be obtained from the [manypoints](#) site by clicking on the appropriate table entry.

5. CONSTRUCTIONS FOR GENUS-7 CURVES

We work over a finite field $k = \mathbf{F}_q$ of odd characteristic. In our previous constructions, we produced degree-4 Galois extensions of \mathbf{P}^1 with group $(\mathbf{Z}/2\mathbf{Z})^2$ by adjoining to $k(x)$ the square roots of two polynomials. For our genus-7 construction, we will instead produce degree-8 Galois extensions with group $(\mathbf{Z}/2\mathbf{Z})^3$ by adjoining the square roots of three polynomials f_1, f_2, f_3 . According to the previously-cited result of Kani and Rosen [12, Theorem B, p. 308], the resulting curve D will have Jacobian isogenous to the product of the Jacobians of the seven curves

$$y^2 = f_1, y^2 = f_2, y^2 = f_3, y^2 = f_2f_3, y^2 = f_1f_3, y^2 = f_1f_2, \text{ and } y^2 = f_1f_2f_3,$$

and the defect of D will be the sum of the defects of these seven curves. In order to produce a curve of genus 7, we will therefore want to have a method of choosing the polynomials f_1, f_2 , and f_3 so that the sum of the genera of the seven associated curves is 7.

We used two methods to find such polynomials. The first method involves taking

$$f_1 = s_1(x-1)g_1, \quad f_2 = s_2(x-1)g_2, \quad \text{and} \quad f_3 = sx,$$

where g_1 and g_2 are monic quadratic polynomials that are coprime to one another and to $x-1$, and where s, s_1 , and s_2 are nonzero constants that only matter up to

squares. Up to squares in $k[x]$, the other polynomials we then have to consider are

$$\begin{aligned} f_2 f_3 &= s s_2 x(x-1) g_2 \\ f_1 f_3 &= s s_1 x(x-1) g_1 \\ f_1 f_2 / (x-1)^2 &= s_1 s_2 g_1 g_2 \\ f_1 f_2 f_3 / (x-1)^2 &= s s_1 s_2 x g_1 g_2. \end{aligned}$$

These seven polynomials give us hyperelliptic curves of genus 1, 1, 0, 1, 1, 1, and 2, respectively, so the curve C will have genus 7.

To produce f_1 , f_2 , and f_3 of this form such that all of the seven associated curves have small defect, we begin by enumerating the monic quadratic polynomials h such that the genus-1 curves $y^2 = (x-1)h$ and $y^2 = x(x-1)h$ both have twists with small defect. Then we let g_1 and g_2 range over the set of such h , and we check to see whether we can choose constants s , s_1 , and s_2 such that the curves defined by f_1 , f_2 , $f_1 f_3$, and $f_2 f_3$ simultaneously have small defect. If we succeed in doing so, we then check whether the genus-1 curve defined by $f_1 f_2$ has small defect, and if it does, we check whether the genus-2 curve defined by $f_1 f_2 f_3$ has small defect.

We were able to run this algorithm to completion for the q in the `manypoints` table up to 17^3 . On the laptop described in Section 1, the computation for $q = 17^3$ took just over 29 hours.

The second method involves taking

$$\begin{aligned} f_1 &= s_1 x(x-1)(x-b) \\ f_2 &= s_2 (x-a)(x-b)(x-c) \\ f_3 &= s_3 x(x-a)(x-d), \end{aligned}$$

where a , b , c , and d are elements of k that are distinct from one another and from 0 and 1, and where s_1 , s_2 , and s_3 are nonzero constants that only matter up to squares. Up to squares in $k[x]$, the other polynomials we then have to consider are

$$\begin{aligned} f_2 f_3 / (x-a)^2 &= s_2 s_3 x(x-b)(x-c)(x-d) \\ f_1 f_3 / x^2 &= s_1 s_3 (x-1)(x-a)(x-c)(x-d) \\ f_1 f_2 / (x-b)^2 &= s_1 s_2 x(x-1)(x-a)(x-c) \\ f_1 f_2 f_3 / (x(x-a)(x-b))^2 &= s_1 s_2 s_3 (x-1)(x-c)(x-d). \end{aligned}$$

Each of these seven polynomials gives us a curve of genus 1, so the curve D will have genus 7.

(This construction of a $(\mathbf{Z}/2\mathbf{Z})^3$ -extension of \mathbf{P}^1 of genus 7 such that all the quadratic subextensions have genus 1 can be viewed as a generalization of a method of constructing the Fricke–Macbeath curve [13]; the description of the Fricke–Macbeath curve discussed on pp. 533–534 of [13] makes this clear. In fact, if we take

$$a = -\zeta - \zeta^6, \quad b = \zeta^2 + \zeta^5, \quad c = \zeta^3 + \zeta^4 + 1, \quad \text{and} \quad d = -\zeta - \zeta^6 - 1,$$

where ζ is a primitive 7-th root of unity, we find that our curve is geometrically isomorphic to the Fricke–Macbeath curve, because the linear fractional transformation $x \mapsto (x + \zeta)/(x + \zeta^{-1})$ sends the set of ramification points $\{0, 1, \infty, a, b, c, d\}$ to the set $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\}$. Indeed, our construction was inspired by seeing several records on the `manypoints` site produced by Jaap Top and Carlo Verschoor by studying twists of the Fricke–Macbeath curve.)

| q | range | q | range | q | range | q | range |
|----------------|--------------|-----------------|---------------|-----------------|---------------|-----|--------------|
| 3 | 9–9 | 11 | 4– 10 | 19 | 0– 12 | 67 | 4– 16 |
| 3 ² | 9–12 | 11 ² | 0–0 | 19 ² | 0–0 | 71 | 0– 8 |
| 3 ³ | 3–14 | 11 ³ | 0– 24 | 19 ³ | 0– 23 | 73 | 6– 21 |
| 3 ⁴ | 0– 12 | 11 ⁴ | 0– 28 | 19 ⁴ | 0– 28 | 79 | 0– 7 |
| 3 ⁵ | 2– 21 | 11 ⁵ | 0– 82 | 19 ⁵ | 0– 105 | 83 | 3– 18 |
| 5 | 8–10 | 13 | 6– 11 | 23 | 3– 11 | 89 | 0– 8 |
| 5 ² | 4– 12 | 13 ² | 0– 12 | 29 | 3– 12 | 97 | 0– 15 |
| 5 ³ | 3– 20 | 13 ³ | 0– 37 | 31 | 6– 17 | | |
| 5 ⁴ | 0– 20 | 13 ⁴ | 0– 28 | 37 | 6– 14 | | |
| 5 ⁵ | 0– 39 | 13 ⁵ | 0– 60 | 41 | 2– 10 | | |
| 7 | 7–7 | 17 | 4– 14 | 43 | 7– 11 | | |
| 7 ² | 0–0 | 17 ² | 0–0 | 47 | 3– 15 | | |
| 7 ³ | 3– 27 | 17 ³ | 2– 26 | 53 | 4– 12 | | |
| 7 ⁴ | 0– 16 | 17 ⁴ | 0– 12 | 59 | 5– 17 | | |
| 7 ⁵ | 4– 45 | 17 ⁵ | 0– 123 | 61 | 3– 11 | | |

TABLE 3. The best upper and lower bounds known for the minimal defect $D_q(7)$ for the odd values of q represented in the [manypoints](#) table, as of 29 March 2017. The upper bounds in boldface come from computations described in this paper.

Our strategy is to compute all the values of $\lambda \in k$ such that the curve $y^2 = x(x-1)(x-\lambda)$, or its quadratic twist, has small defect. Then we choose four such values $\lambda_1, \lambda_2, \lambda_3$, and λ_4 , and compute the values of a, b, c , and d such that the curves defined by $y^2 = f_1$, $y^2 = f_3$, $y^2 = f_1 f_3$, and $y^2 = f_1 f_2 f_3$ have those λ -invariants (for a given ordering of their 2-torsion points). Then we check to see whether we can choose the constants s_1, s_2 , and s_3 so that the curves have small defect. If we succeed, we then check to see whether the remaining three curves have small defect. We can do this quickly by first checking to see whether their λ -invariants are among those we computed at the beginning.

Of course, what we mean by “small defect” will change dynamically as we run our algorithm, depending on the curves we find.

We ran this algorithm to completion on all odd $q < 17^5$ from the [manypoints](#) list. (For $q = 13^5$ this took nearly 50 hours.) For $q = 17^5$ and $q = 19^5$, we ran the algorithm for more than a week on a newer and faster desktop machine, but stopped with partial results and did not run to completion. Combining the examples we found using both algorithms, we obtain the results presented in Table 3. The table gives the current lower and upper bounds on the minimal defect $D_q(7)$ for the odd values of q listed in the online table, with the upper bound in boldface if it was obtained from our computations. Equations for the curves we found can be obtained from the [manypoints](#) site by clicking on the appropriate table entry.

6. CONCLUSION

Even as we were writing this paper and implementing the algorithms described here, other researchers were adding new lower bounds for values of $N_q(g)$ in the

manypoints table, including many for $g = 5$. Some of these bounds were better than the results obtained by our methods, some were not. We hope that the inclusion of our new lower bounds in the online table will encourage further development of algorithms to produce curves with many points.

REFERENCES

- [1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). Software available at <http://magma.maths.usyd.edu.au/>.
- [2] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and Jacobians with a given number of points*, LMS J. Comput. Math. **18** (2015), no. 1, 170–197.
- [3] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
- [4] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler, *manypoints.org — Table of curves with many points*, 2009, retrieved 29 March 2017.
- [5] Gerard van der Geer and Marcel van der Vlugt, *Tables of curves with many points*, Math. Comp. **69** (2000), no. 230, 797–810.
- [6] E. W. Howe and K. E. Lauter, *Improved upper bounds for the number of points on curves over finite fields*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 6, 1677–1737, Corrigendum: **57** (2007) 1019–1021.
- [7] Everett W. Howe, *New bounds on the maximum number of points on genus-4 curves over small finite fields*, Arithmetic, Geometry, Cryptography and Coding Theory (Y. Aubry, C. Ritzenthaler, and A. Zykin, eds.), Contemp. Math., vol. 574, American Mathematical Society, Providence, RI, 2012, pp. 69–86.
- [8] ———, *Quickly constructing curves of genus 4 with many points*, Frobenius Distributions: Sato–Tate and Lang–Trotter conjectures (D. Kohel and I. Shparlinski, eds.), Contemp. Math., vol. 663, American Mathematical Society, Providence, RI, 2016, pp. 149–173.
- [9] Everett W. Howe and Kristin E. Lauter, *New methods for bounding the number of points on curves over finite fields*, Geometry and arithmetic (C. Faber, G. Farkas, and R. de Jong, eds.), EMS Ser. Congr. Rep., European Mathematical Society, Zürich, 2012, pp. 173–212.
- [10] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364.
- [11] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 1, 239–289.
- [12] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327.
- [13] A. M. Macbeath, *On a curve of genus 7*, Proc. London Math. Soc. (3) **15** (1965), 527–542.
- [14] Jean-François Mestre, *Courbes de genre 3 avec S_3 comme groupe d’automorphismes*, 2010. [arXiv:1002.4751 \[math.AG\]](https://arxiv.org/abs/1002.4751)
- [15] Jean-Pierre Serre, *Nombres de points des courbes algébriques sur \mathbf{F}_q* , Seminaire de Théorie des Nombres de Bordeaux, 1982–1983, Univ. Bordeaux I, Talence, 1983, Exp. No. 22.
- [16] ———, *Sur le nombre des points rationnels d’une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 9, 397–402.
- [17] ———, *Résumé des cours de 1983–1984*, Ann. Collège France (1984), 79–83, = *Œuvres* **132**.
- [18] Muhammad Afzal Soomro, *Algebraic curves over finite fields*, Ph.D. thesis, University of Groningen, 2013.
- [19] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

CENTER FOR COMMUNICATIONS RESEARCH, 4320 WESTERRA COURT, SAN DIEGO, CA 92121, USA

E-mail address: however@alumni.caltech.edu

URL: <http://www.alumni.caltech.edu/~however/>