Canad. J. Math. Vol. **55** (2), 2003 pp. 331–352

The Maximum Number of Points on a Curve of Genus 4 over $\mathbb{F}_8$ is 25

David Savitt

with an Appendix by Kristin Lauter

Abstract. We prove that the maximum number of rational points on a smooth, geometrically irreducible genus 4 curve over the field of 8 elements is 25. The body of the paper shows that 27 points is not possible by combining techniques from algebraic geometry with a computer verification. The appendix shows that 26 points is not possible by examining the zeta functions.

1 Introduction

Our aim in this paper is to prove that a smooth geometrically irreducible curve C of genus 4 over the finite field $\mathbb{F}_8$ may have at most 25 $\mathbb{F}_8$-points. Our strategy is as follows: if C has more than 18 $\mathbb{F}_8$-points, then C may not be hyperelliptic, and so the canonical divisor of C yields an embedding of C into $\mathbb{P}^3_{\mathbb{F}_8}$. The image of C under this embedding is a degree 6 curve which is precisely the intersection of an irreducible cubic hypersurface with an irreducible quadric hypersurface, both defined over $\mathbb{F}_8$. (This is Example IV.5.2.2 in [Har]. Hartshorne works over an algebraically closed field, but his argument is equally valid over the smaller field. See, for example, Theorem III.5.1 in [Har] and Theorem A.4.2.1 in [HS] for the necessary tools.)

Consequently, finding the maximum possible number of points on a curve of genus 4 over $\mathbb{F}_8$ is reduced to a finite task: one can write down all cubic hypersurfaces and all quadric hypersurfaces in $\mathbb{P}^3_{\mathbb{F}_8}$, and count the number of points on their intersection. As a practical matter, however, one must make significant reductions before this program becomes computationally feasible. For example, the space of homogeneous cubics in four variables is already $\binom{6}{3} - 1 = 19$-dimensional.

We begin in Section 2 by noting that up to isomorphism there are only three irreducible quadric surfaces in $\mathbb{P}^3_{\mathbb{F}_8}$ which contain many $\mathbb{F}_8$-points. Therefore we may select representatives of the isomorphism classes and assume that our curve C lies on one of these three specific quadrics. Next, we recall (see [Lau1] and [GV]) that it is known that any curve of genus 4 over $\mathbb{F}_8$ has no more than 27 points, and that such curves with 25 points exist. Moreover, using the techniques of [Lau2], K. Lauter demonstrates in an appendix to this paper that such curves with 26 points do not exist. We may therefore suppose that the curve C for which we are searching has exactly 27 points. In Section 3, we employ the following strategy to reduce the problem

Received by the editors February 6, 2002; revised July 12, 2002.
Partially supported by an NSERC postdoctoral fellowship.
AMS subject classification: 11G20, 14H25.

further. If Q is one of our three quadrics, then the subgroup $\mathrm{Fix}(Q)$ of $\mathrm{PGL}_4(\mathbb{F}_8)$ preserving Q is large. If P is a cubic surface and if $\sigma \in \mathrm{Fix}(Q)$, then $P \cap Q$ and $\sigma(P) \cap Q = \sigma(P \cap Q)$ have the same number of points. If the intersection $P \cap Q$ is a geometrically irreducible curve of degree 6, then by Bézout's theorem the intersection may contain at most three points of any line. We study the action of $\mathrm{Fix}(Q)$ on the points of Q to show that if $S \subset Q$ is a subset with 27 points, no four of which are collinear, then we may find $\sigma \in \mathrm{Fix}(Q)$ such that $\sigma(S)$ contains a particular list of points of Q (or one of several lists of points of Q).

The problem is therefore reduced to studying cubics P which contain particular points of Q, cutting down significantly on the dimension of the space of cubics under consideration. Depending on the cubic, we are able to eliminate between 5 and 7 dimensions in this fashion. The space is cut down further by 4 dimensions by noting that we may subtract appropriate multiples of our quadric Q. Thus we have reduced a 19-dimensional search space over $\mathbb{F}_8$ to a search space over $\mathbb{F}_8$ of no greater than 10 dimensions, which is easily tractable for a computer.

Finally, we note that this search will *a priori* turn up many cubics and quadrics whose intersection contains 27 points. This is because we will find many reducible (or at least geometrically reducible) intersections. These "bad" curves are relatively straightforward to identify and discard. In Section 5, we give a precise list of the ways in which bad curves with 27 points can occur.

Acknowledgements The author is grateful to J.-P. Serre for his comments and corrections, and in particular for the suggestion that Section 5 be included. We also thank Jason Starr for several helpful conversations, William Stein for the use of his computer, and the anonymous referee for his or her comments. Computations were performed partly by C programs, and partly using the MAGMA package. This problem came to the author's attention at the 2000 Arizona Winter School on Arithmetic Algebraic Geometry, and the author thanks the organizers of this conference for their hard work and hospitality.

2 Quadric Surfaces in $\mathbb{P}^3_{\mathbb{F}_8}$

Let C be a non-hyperelliptic curve of genus 4 over $\mathbb{F}_8$. As we have noted, we may suppose that C is canonically embedded into $\mathbb{P}^3_{\mathbb{F}_8}$ as the intersection of an irreducible quadric hypersurface Q with an irreducible cubic hypersurface P. It is a classical result that over a finite field $\mathbb{F}$, there are exactly three reduced and geometrically irreducible quadric surfaces in $\mathbb{P}^3_{\mathbb{F}}$ up to $\mathbb{F}$-isomorphism: the split nonsingular quadric (isomorphic to $\mathbb{P}^1_{\mathbb{F}} \times \mathbb{P}^1_{\mathbb{F}}$), the nonsplit nonsingular quadric (the quadratic twist of $\mathbb{P}^1_{\mathbb{F}} \times \mathbb{P}^1_{\mathbb{F}}$), and the singular quadric.

We give an argument, essentially found on p. 206 of [ACGH], explaining for each C into which of the above categories the quadric Q falls. Note that any linear system of degree 3 and dimension at least 1 on C defines a ruling of Q. Indeed, if D is a divisor in such a linear system, then by the geometric version of the Riemann-Roch theorem, the linear span in $\mathbb{P}^3$ of the support of D is a line. By Bézout's theorem, this line is contained in Q.

The $\mathbb{F}_8$-scheme $W^1_3(C)$ defined in [ACGH], whose geometric points correspond

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

to the complete linear series of degree 3 and dimension at least 1 on C, is a zero-dimensional affine scheme, and by the Thom-Porteous formula this scheme has degree 2. Hence there are exactly three possibilities for $W_3^1(C)$: two reduced $\mathbb{F}_8$-points (so Q is the split nonsingular quadric), two conjugate $\mathbb{F}_{64}$-points (nonsplit nonsingular), and one nonreduced $\mathbb{F}_8$-point (singular).

To make our classification of quadrics concrete, we first recall the following result from [Arf]:

Proposition 2.1 *Let* $\mathbb{F}$ *be a field of characteristic* 2. *Then any quadratic form in* n *variables over* $\mathbb{F}$ *is equivalent to one of the form*

$$\sum_{i=1}^{\mu} x_i y_i + \sum_{j=\mu+1}^{\mu+\nu} (a_j x_j^2 + x_j y_j + b_j y_j^2) + \sum_{k=1}^{d} c_k z_k^2$$

with $2\mu + 2\nu + d \leq n$.

This is by no means a classification: two distinct quadratic forms written as above may still be isomorphic. For example, when the field $\mathbb{F}$ is perfect evidently we may take $d = 0$ or 1 and $c_1 = 1$. Similarly we may suppose each $a_j = 1$.

When the field $\mathbb{F} = \mathbb{F}_{2^n}$ with n odd, one can check with little difficulty that the form $x^2 + xy + by^2$ is equivalent either to the form xy or to $x^2 + xy + y^2$, depending on whether or not the form nontrivially represents 0 over $\mathbb{F}$. Combining this with the identity

$$X^2 + XY + Y^2 + Z^2 = XY + (X + Y + Z)^2$$

and the fact that

$$(X^2 + XY + Y^2) + (Z^2 + ZW + W^2)$$

is identically equal to

$$(X + Z + W)(Y + Z + W) + (X + Y + Z)(X + Y + W),$$

we obtain the following version of Proposition 2.1.

Proposition 2.2 *Let* $\mathbb{F}_{2^n}$ *be the finite field with* 2^n *elements with* n *an odd integer. Then any quadratic form over* $\mathbb{F}_{2^n}$ *is equivalent over* $\mathbb{F}_{2^n}$ *to a form with one of the following shapes:*

- $\sum_{i=1}^{\mu} x_i y_i$
- $\sum_{i=1}^{\mu} x_i y_i + (X^2 + XY + Y^2)$
- $\sum_{i=1}^{\mu} x_i y_i + (Z^2)$.

We are interested in particular in the geometrically integral quadric surfaces in $\mathbb{P}^3_{\mathbb{F}_8}$, which correspond to geometrically irreducible quadratic forms in at most four variables over $\mathbb{F}_8$. Their classification is as follows.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

Proposition 2.3 *Up to $\mathbb{F}_8$-isomorphism, there are exactly three geometrically irreducible quadratic forms in four variables X, Y, Z, W over $\mathbb{F}_8$. They are: $XY + ZW$ (the split nondegenerate form), $X^2 + XY + Y^2 + ZW$ (the nonsplit nondegenerate form), and $XY + Z^2$ (the degenerate form).*

Proof According to Proposition 2.2, up to isomorphism there are at most six quadratic forms in four variables over any finite field $\mathbb{F}_{2^n}$ with n odd, namely: XY, $XY + ZW$, $X^2 + XY + Y^2$, $X^2 + XY + Y^2 + ZW$, Z^2, and $Z^2 + XY$. The forms XY and Z^2 are reducible, and $X^2 + XY + Y^2$ is irreducible but geometrically reducible, and so we eliminate them.

The hypersurface defined by $XY + ZW$ is $\mathbb{F}_8$-isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, and possesses two $\mathbb{F}_8$-rulings. The hypersurface defined by $X^2 + XY + Y^2 + ZW$ is $\mathbb{F}_{64}$-isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, and so one sees that it has two Galois-conjugate rulings over $\mathbb{F}_{64}$ but contains no lines over $\mathbb{F}_8$. Finally, the hypersurfaces defined by $XY+ZW$ and X^2+XY+Y^2+ZW are nonsingular, whereas the hypersurface defined by $XY+Z^2$ is singular at $[0:0:0:1]$. These facts together show that these three forms cannot be $\mathbb{F}_8$-isomorphic. ■

Remark We can also see that these forms are not $\mathbb{F}_8$-isomorphic by verifying that a different number of points of $\mathbb{P}^3_{\mathbb{F}_8}$ lie on each of the resulting quadric surfaces. In fact there are 81 points on the surface $XY + ZW = 0$, there are 73 points on the surface $X^2 = YZ$, and there are 65 points on the surface $X^2 + XY + Y^2 = ZW$.

3 Reductions

3.1 Action of $\mathrm{PGL}_4(\mathbb{F}_8)$ on Quadrics

In this subsection, we describe the subgroups of $\mathrm{PGL}_4(\mathbb{F}_8)$ preserving each of our quadrics. If we can correctly list these subgroups in their entirety, we will automatically be able to obtain a proof that the description is correct, by counting the size of the orbits of our quadrics under $\mathrm{PGL}_4(\mathbb{F}_8)$.

We begin with the quadric $XY + ZW = 0$. This quadric is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, as can be seen via the map $\mathbb{P}^1 \times \mathbb{P}^1 \to \{XY = ZW\}$ sending $([x:y],[z,w]) \mapsto [xz:yw:xw:yz]$. The inverse map is defined on coordinate patches, for example sending $[X:Y:Z:W] \mapsto ([X : W],[W:Y])$ on the affine $\{W \neq 0\}$. The group $\mathrm{PGL}_2(\mathbb{F}_8) \times \mathrm{PGL}_2(\mathbb{F}_8) \times C_2$ acts on $\mathbb{P}^1 \times \mathbb{P}^1$, where the cyclic factor C_2 is generated by an automorphism interchanging the two copies of $\mathbb{P}^1$. Evidently each nontrivial one of these automorphisms yields a nontrivial element of $\mathrm{PGL}_4(\mathbb{F}_8)$ preserving $XY + ZW = 0$.

We turn next to the quadric $XY = Z^2$. One may easily check that the map

$$\begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ \sqrt{ac} & \sqrt{bd} & \sqrt{ad+bc} & 0 \\ * & * & * & e \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}$$

preserves $XY = Z^2$, where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an element of $\mathrm{GL}_2(\mathbb{F}_8)$, $e \in \mathbb{F}_8^\times$, and each $* \in \mathbb{F}_8$. These will be all the elements of $\mathrm{Fix}(XY = Z^2)$.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

Next, we verify that $\mathrm{Fix}(X^2 + XY + Y^2 = ZW)$ acts doubly-transitively on $\mathbb{F}_8$-points of the quadric. Indeed, we claim that for any point p on $X^2+XY+Y^2 = ZW$ other than $[0{:}0{:}0{:}1]$, there is an element of $\mathrm{Fix}(X^2 + XY + Y^2 = ZW)$ sending $[0{:}0{:}1{:}0]$ to p while fixing $[0{:}0{:}0{:}1]$. Then for any pair of points p_1, p_2 we may send p_1 to $[0{:}0{:}1{:}0]$, then use the automorphism interchanging W and Z to map p_1 to $[0{:}0{:}0{:}1]$. If p_2 has now been moved to p_3, we finish via a map preserving $[0{:}0{:}0{:}1]$ and sending p_3 to $[0 : 0 : 1 : 0]$, so the pair (p_1, p_2) has been moved to $([0{:}0{:}0{:}1], [0{:}0{:}1{:}0])$, and the group is doubly-transitive.

To see the claim, notice that for an element $x \in \mathbb{F}_8$, the map sending $X \mapsto X + xZ$, $Y \mapsto Y, Z \mapsto Z, W \mapsto W + xY + x^2Z$ preserves $X^2+XY+Y^2 = ZW$, sends $[0{:}0{:}1{:}0]$ to $[x{:}0{:}1{:}x^2]$, and fixes $[0{:}0{:}0{:}1]$. Now the map sending $X \mapsto X$, $Y \mapsto Y + yZ$, $Z \mapsto Z$, $W \mapsto W + yX + y^2Z$ preserves $X^2 + XY + Y^2 = ZW$, sends $[x{:}0{:}1{:}x^2]$ to $[x{:}y{:}1{:}x^2 + xy + y^2]$, and fixes $[0{:}0{:}0{:}1]$. Since $[x{:}y{:}1{:}x^2 + xy + y^2]$ is a general $\mathbb{F}_8$-point on the curve besides $[0{:}0{:}0{:}1]$, this proves the claim.

Now an element of $\mathrm{GL}_4(\mathbb{F}_8)$ preserving $X^2+XY+Y^2 = ZW$ and fixing $[0{:}0{:}0{:}1]$ and $[0{:}0{:}1{:}0]$ will be of the form

$$\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & w \end{pmatrix}$$

where $z, w \in \mathbb{F}_8^\times$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an element of $\mathrm{GL}_2(\mathbb{F}_8)$ preserving the form $X^2+XY+Y^2 = 0$, and a, b, c, d, z determine w. One checks that there are exactly 126 such elements of $\mathrm{GL}_2(\mathbb{F}_8)$. They are the scalar multiples of the following 18 matrices: the identity matrix, the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, the four matrices with three entries equal to 1 and the other equal to 0, and, for each of the three roots η of $\eta^3 + \eta + 1 = 0$, the four 90-degree rotations of the matrix $\left(\begin{smallmatrix} \eta & \eta^2 \\ \eta^{-3} & \eta \end{smallmatrix}\right)$.

Furthermore, $X^2 + XY + Y^2 = 0$ in $\mathbb{P}^3$ has automorphisms given by completing those 126 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to matrices

$$\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$$

where the last two rows are independent of the first two.

We now verify that we have indeed found all of the automorphisms of these quadrics.

- For $XY+ZW$, we have found $2\cdot\left((8^2-1)(8^2-8)/7\right)^2 = 508032$ automorphisms. This has index 68024320 in $\mathrm{PGL}_4(\mathbb{F}_8)$, which is therefore an upper bound on the size of the orbit of $XY + ZW$ in the space of quadric surfaces.
- For $XY = Z^2$, we have found $(8^2 - 1)(8^2 - 8) \cdot 8^3 \cdot 7/7 = 1806336$ automorphisms, giving an upper bound of 19131840 on the orbit.
- For $X^2 + XY + Y^2 = ZW$, we have found $65 \cdot 64 \cdot 126 \cdot 7/7 = 524160$ automorphisms, giving an upper bound of 65931264 on the orbit.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

• For $X^2 + XY + Y^2$, we have found $126 * (8^4 - 8^2) * (8^4 - 8^3)/7 = 260112384$ automorphisms, giving an upper bound of 132860 on the orbit.

• It is easy to see that the form X^2 has orbit of size $(8^4 - 1)/7 = 585$ and XY has orbit of size $(8^4 - 1)(8^4 - 8)/(2 \cdot 7^2) = 170820$.

Finally, we note that $68024320 + 19131840 + 65931264 + 132860 + 585 + 170820 = 153391689 = (8^{10} - 1)/7$, precisely the number of quadric surfaces, and so we confirm that we have indeed found all the automorphisms of these quadrics.

3.2 Reductions for $XY + ZW = 0$

Observe that $\{XY + ZW = 0\} \cong \mathbb{P}^1 \times \mathbb{P}^1$ is a ruled surface, and in particular that the set of $\mathbb{F}_8$-points of $\mathbb{P}^1 \times \mathbb{P}^1$ may be written as the union of the nine lines $\{l\} \times \mathbb{P}^1_{\mathbb{F}_8}$, for $l \in \mathbb{P}^1_{\mathbb{F}_8}$, and as the union of the nine lines $\mathbb{P}^1_{\mathbb{F}_8} \times \{r\}$ for $r \in \mathbb{P}^1_{\mathbb{F}_8}$. Each of these lines on $\mathbb{P}^1 \times \mathbb{P}^1$ maps to a line on $\{XY + ZW = 0\}$.

In the remainder of this subsection, we suppose that a cubic hypersurface $P \subset \mathbb{P}^3_{\mathbb{F}_8}$ intersects the quadric $\{XY + ZW = 0\}$ in a smooth geometrically irreducible curve C with 27 $\mathbb{F}_8$-points.

If P intersected any of these lines on $\{XY + ZW = 0\}$ in at least 4 points, then by Bézout's theorem the line would be contained in P, and consequently the line would be contained in the intersection $P \cap \{XY + ZW = 0\}$. Therefore the curve C would be reducible, which we have assumed is not the case. We may therefore conclude that P intersects each of these lines in at most 3 points. However, since there are nine lines in each ruling, P must intersect each of these lines in *exactly* 3 points. Note that this argument yields a combinatorial proof that if the canonical embedding of a smooth curve of genus 4 over $\mathbb{F}_8$ lies on $\{XY + ZW = 0\}$, then it cannot contain 28 points.

Write the $\mathbb{F}_8$-points of $\mathbb{P}^1 \times \mathbb{P}^1$ as (l_i, r_j) with $0 \leq i, j \leq 8$. We have seen that for each i there are exactly three j such that (l_i, r_j) lies on P, and similarly for each j there are exactly three i. Suppose, after renumbering, that (l_0, r_0), (l_0, r_1), and (l_0, r_2) all lie on P. We divide into two cases. First, suppose there exists $i > 0$ such that two of (l_i, r_0), (l_i, r_1), (l_i, r_2) lie on P. After renumbering, we may assume that (l_i, r_0), (l_i, r_1) lie on P, and we may select $i' \neq 0, i$ so that $(l_{i'}, r_2)$ lies on P. Since $\mathrm{PGL}_2(\mathbb{F}_8)$ acts 3-transitively on $\mathbb{P}^1_{\mathbb{F}_8}$, we may select an automorphism σ of $\mathbb{P}^1 \times \mathbb{P}^1$ such that $([0{:}1] : [0{:}1])$, $([0{:}1] : [1{:}0])$, $([0{:}1] : [1, 1])$, $([1{:}0], [0{:}1])$, $([1{:}0], [1{:}0])$, $([1{:}1], [1{:}1])$ all lie on $\sigma(P)$. Therefore, without loss of generality, in this case we may assume that these six points lie on P. We refer to this as the $3, 2, 1$-case.

Second, suppose that no such i exists. Without loss of generality, after renumbering we may assume that (l_1, r_0), (l_2, r_0), (l_3, r_1), (l_4, r_1), (l_5, r_2), (l_6, r_2) all lie on P. Then, by the pigeonhole principle, for some $j > 2$ there are $1 \leq i, i' \leq 6$ so that (l_i, r_j) and $(l_{i'}, r_j)$ lie on P. If $\{i, i'\} = \{1, 2\}, \{3, 4\}$, or $\{5, 6\}$, we may suppose after renumbering that $\{i, i'\} = \{1, 2\}$, and we are reduced to the case of the previous paragraph: namely (l_0, r_0), (l_1, r_0), (l_2, r_0), (l_1, r_j), (l_2, r_j), and some $(l_0, r_{j'})$ lie on P, so after interchanging the two copies of $\mathbb{P}^1$ and applying an element of $\mathrm{PGL}_2(\mathbb{F}_8) \times \mathrm{PGL}_2(\mathbb{F}_8)$, we may again assume that $([0{:}1] : [0{:}1])$, $([0{:}1] : [1{:}0])$, $([0{:}1] : [1, 1])$, $([1{:}0], [0{:}1])$, $([1{:}0], [1{:}0])$, $([1{:}1], [1{:}1])$ all lie on P.

On the other hand, if $\{i, i'\} \neq \{1, 2\}, \{3, 4\}$, or $\{5, 6\}$, we may assume (after renumbering) that $\{i, i'\} = \{1, 3\}$. In this case we have (l_0, r_0), (l_0, r_1), (l_1, r_0),

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

(l_1, r_j), (l_3, r_1), and (l_3, r_j) all lying on P. Applying an element of $\mathrm{PGL}_2(\mathbb{F}_8) \times \mathrm{PGL}_2(\mathbb{F}_8)$ we may assume that $([0:1],[0:1])$, $([0:1],[1:0])$, $([1:0],[0:1])$, $([1:0],[1:1])$, $([1:1],[1:0])$, $([1:1],[1:1])$ all lie on P. We refer to this as the $2,2,2$-case. Moreover, we may suppose that $([1:0],[1:0])$ is not on P, or else we would be able to reduce to the $3,2,1$-case.

Suppose that homogeneous cubic polynomial defining P is written $c_{X^3}X^3 + c_{X^2Y}X^2Y + \cdots + c_{W^3}W^3$. We can now verify the following proposition.

Proposition 3.1 *If there exists a cubic hypersurface $P \subset \mathbb{P}^3_{\mathbb{F}_8}$ whose intersection with $\{XY = ZW\}$ is a smooth geometrically irreducible curve of genus* 4 *with* 27 $\mathbb{F}_8$*-points, then there exists such a hypersurface whose coefficients satisfy one or the other of the two sets of conditions below:*

1. • $c_{X^3} = c_{Y^3} = c_{Z^3} = c_{W^3} = c_{X^2Y} = c_{XY^2} = c_{Z^2W} = c_{ZW^2} = 0$,
   • $c_{Y^2W} = c_{YW^2} = 1$, *and*
   • $c_{X^2Z} + c_{X^2W} + c_{XYZ} + c_{XYW} + c_{XZ^2} + c_{XZW} + c_{XW^2} + c_{Y^2Z} + c_{YZ^2} + c_{YZW} = 0$, *or*
2. • $c_{X^3} = 1$,
   • $c_{Y^3} = c_{Z^3} = c_{W^3} = c_{X^2Y} = c_{XY^2} = c_{Z^2W} = c_{ZW^2} = 0$,
   • $c_{XZ^2} = c_{X^2Z} + 1$, $c_{XW^2} = c_{X^2W} + 1$, *and*
   • $c_{XYZ} + c_{XYW} + c_{XZW} + c_{Y^2Z} + c_{Y^2W} + c_{YZ^2} + c_{YZW} + c_{YW^2} = 1$.

Proof Recall that we map $\mathbb{P}^1 \times \mathbb{P}^1 \to \{XY = ZW\}$ via $([x:y],[z,w]) \mapsto [xz:yw:xw:yz]$. In the $3,2,1$-case, we have shown that we may assume $([0:1]:[0:1]),([0:1]:[1:0]),([0:1]:[1,1]),([1:0],[0:1]),([1:0],[1:0]),([1:1],[1:1])$ all lie on P. In $\mathbb{P}^3$-coordinates, these six points are, respectively, $[0:1:0:0]$, $[0:0:0:1]$, $[0:1:0:1]$, $[0:0:1:0]$, $[1:0:0:0]$, and $[1:1:1:1]$. For these points to lie on P, it follows that $c_{X^3} = c_{Y^3} = c_{Z^3} = c_{W^3} = 0$, that $c_{Y^2W} = c_{YW^2}$, and that all 20 coefficients sum to zero. If $c_{Y^2W} = c_{YW^2} = 0$, one easily verifies that the line $[0:Y:0:W]$ is contained in the curve, and so we may suppose without loss of generality that $c_{Y^2W} = c_{YW^2} = 1$. Further, by subtracting appropriate multiples of the quadric $XY = ZW$, we may suppose that $c_{X^2Y} = c_{XY^2} = c_{Z^2W} = c_{ZW^2} = 0$.

In the $2,2,2$-case we may assume that $([0:1],[0:1])$, $([0:1],[1:0])$, $([1:0],[0:1])$, $([1:0],[1:1])$, $([1:1],[1:0])$, $([1:1],[1:1])$ all lie on P. In $\mathbb{P}^3$-coordinates, these six points are, respectively, $[0:1:0:0]$, $[0:0:0:1]$, $[0:0:1:0]$, $[1:0:1:0]$, $[1:0:0:1]$, and $[1:1:1:1]$. For these points to lie on P, it follows that $c_{Y^3} = c_{W^3} = c_{Z^3} = 0$, that $c_{X^3} + c_{X^2Z} + c_{XZ^2} = 0$, that $c_{X^3} + c_{X^2W} + c_{XW^2} = 0$, and that all the coefficients sum to 0. Moreover, we may assume that $([1:0],[1,0])$, which in $\mathbb{P}^3$-coordinates is $[1:0:0:0]$, does not lie on P. This implies that $c_{X^3} \neq 0$, so we may suppose without loss of generality that $c_{X^3} = 1$. Once again, by subtracting appropriate multiples of the quadric $XY = ZW$, we may suppose that $c_{X^2Y} = c_{XY^2} = c_{Z^2W} = c_{ZW^2} = 0$. ∎

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

3.3 Reductions for $XY = Z^2$

Suppose that a cubic hypersurface $P \subset \mathbb{P}^3_{\mathbb{F}_8}$ intersects the quadric $\{XY = Z^2\}$ in a smooth geometrically irreducible curve C with 27 $\mathbb{F}_8$-points.

The $\mathbb{F}_8$-points of the surface $\{XY = Z^2\}$ are ruled by the pencil of nine lines $[1:z^2:z:W]$, $[0:1:0:W]$ parametrized by the variable W, all passing through the point $[0:0:0:1]$. By an argument essentially the same as the pigeonhole argument in the previous subsection, we see that $[0:0:0:1]$ cannot lie on P, while each of the nine lines intersects C in exactly 3 other $\mathbb{F}_8$-points. Note that once again we obtain an elementary proof that there cannot be 28 points on such a curve C lying on this quadric.

We remark that the collection of affine transformations of $\mathbb{F}_8$, *i.e.*, the set of maps $x \mapsto ex + f$ with $f \in \mathbb{F}_8$, $e \in \mathbb{F}_8^\times$, acts transitively on the set of 3-element subsets of $\mathbb{F}_8$. Notice that there are 56 affine transformations of $\mathbb{F}_8$ and 56 3-element subsets of $\mathbb{F}_8$, so it suffices to prove that the stabilizer of the 3-element subset $\{0, 1, \eta\}$ is trivial. (Recall that η is a chosen root of $\eta^3 + \eta + 1 = 0$.) This is easy to check. For example, the affine transformation swapping 0 and 1 is $x \mapsto 1 - x$, which does not fix η; and the affine transformation sending 0 to 1 and 1 to η is $x \mapsto (\eta - 1)x + 1$, which does not send η to 0.

Now, for each line $l_z = \{[1:z^2:z:W]\}$, let $S_z = \{W \mid [1:z^2:z:W] \in C\}$. Observe that each S_z has size 3, and so there is a unique transformation $x \mapsto e_z x + f_z$ mapping S_z to $\{0, 1, \eta\}$. Since there are eight S_z's, by the pigeonhole principle some element $e \in \mathbb{F}_8^\times$ occurs twice in the list of e_z's. Suppose $e = e_{z_1} = e_{z_2}$. Choose any element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbb{F}_8)$ sending the vectors $(1, z_1^2)$, $(1, z_2^2)$ to $(0, 1)$, $(1, 0)$ respectively. Suppose that this matrix maps the line $[1:z_3^2]$ to the line $[1:1]$. (What we say below will work equally well in the case that the transformation maps the line $[0:1]$ to the line $[1:1]$, which we omit for ease of notation.) Select any point of the form $[1:z_3^2:z_3:w_3]$ on C. Then we can solve the system of equations

$$g_X + g_Y z_1^2 + g_Z z_1 = f_{z_1}$$
$$g_X + g_Y z_2^2 + g_Z z_2 = f_{z_2}$$
$$g_X + g_Y z_3^2 + g_Z z_3 = e w_3$$

for the variables g_X, g_Y, g_Z. Let σ be the transformation

$$\begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ \sqrt{ac} & \sqrt{bd} & \sqrt{ad+bc} & 0 \\ g_X & g_Y & g_Z & e \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}.$$

Then σ preserves $XY = Z^2$, and we have constructed σ so that $\sigma(P)$ contains the seven points $[0:1:0:0]$, $[0:1:0:1]$, $[0:1:0:\eta]$, $[1:0:0:0]$, $[1:0:0:1]$, $[1:0:0:\eta]$, $[1:1:1:0]$. Then the following proposition holds.

Proposition 3.2 *If there exists a cubic hypersurface $P \subset \mathbb{P}^3_{\mathbb{F}_8}$ whose intersection with $\{XY = Z^2\}$ is a smooth geometrically irreducible curve of genus 4 with 27 $\mathbb{F}_8$-points, then there exists such a hypersurface whose coefficients satisfy the following conditions:*

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

- $c_{X^3} = c_{X^2Y} = c_{XY^2} = c_{Y^3} = c_{Z^3} = c_{Z^2W} = 0$.
- $c_{W^3} = 1$, $c_{X^2W} = c_{Y^2W} = \eta$, $c_{XW^2} = c_{YW^2} = \eta^3$.
- $c_{X^2Z} + c_{XYZ} + c_{XZ^2} + c_{Y^2Z} + c_{YZ^2} = 0$.

Proof We have seen that the under the hypothesis of the proposition, there exists such a hypersurface P containing the above seven points and not containing the point $[0:0:0:1]$. From the latter, we may assume without loss of generality that $c_{W^3} = 1$. Subtracting appropriate multiples of the quadric $XY = Z^2$, we may assume $c_{X^2Y} = c_{XY^2} = c_{Z^3} = c_{Z^2W} = 0$. Since $[0:1:0:0]$ and $[1:0:0:0]$ are on the cubic P, we get $c_{X^3} = c_{Y^3} = 0$. From the presence of $[0:1:0:1]$ on the cubic P, we get $c_{Y^2W} + c_{YW^2} + 1 = 0$. From the presence of $[0:1:0:\eta]$ on the cubic P, we get $c_{Y^2W}\eta + c_{YW^2}\eta^2 + \eta^3 = 0$. It follows that $c_{Y^2W} = \eta$ and $c_{YW^2} = \eta^3$. Similarly $c_{X^2W} = \eta$, $c_{XW^2} = \eta^2$. The last condition follows from previous deductions and the presence of $[1:1:1:0]$ on the cubic P. ∎

3.4 Reductions for $X^2 + XY + Y^2 = ZW$

Suppose that a cubic hypersurface $P \subset \mathbb{P}^3_{\mathbb{F}_8}$ intersects the quadric $\{X^2 + XY + Y^2 = ZW\}$ in a smooth geometrically irreducible curve C with 27 $\mathbb{F}_8$-points.

Since $\mathrm{Fix}(X^2+XY+Y^2 = ZW)$ acts 2-transitively on the points of $X^2+XY+Y^2 = ZW$, we may assume without loss of generality that $[0:0:1:0]$ and $[0:0:0:1]$ lie on P. Recall that the elements of $\mathrm{PGL}_4(\mathbb{F}_8)$ preserving $X^2+XY+Y^2 = ZW$ and fixing those two points are of the form

$$\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & w \end{pmatrix}$$

where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ preserves the form X^2+XY+Y^2, and so such elements of $\mathrm{PGL}_4(\mathbb{F}_8)$ permute the nine conics $C_y = [1:y:Z:(1+y+y^2)Z^{-1}]$, $y \in \mathbb{F}_8$, and $C_\infty = [0:1:Z:Z^{-1}]$, each conic parametrized by the variable Z, and each conic passing through the two points $[0:0:1:0]$ and $[0:0:0:1]$. Unfortunately our previous pigeonhole arguments do not seem to be of value here, because we now would need seven points of one of these conics to lie on the curve C to induce a contradiction.

One checks, using our explicit list of the 18 elements of $\mathrm{PGL}_2(\mathbb{F}_8)$ preserving $X^2 + XY+Y^2 = 0$, that the action of $\mathrm{Fix}(X^2+XY+Y^2 = ZW)$ on the set of nine conics is as follows: the subsets $\{C_0, C_1, C_\infty\}$, $\{C_\eta, C_{\eta^2}, C_{\eta^{-3}}\}$, and $\{C_{\eta^{-1}}, C_{\eta^{-2}}, C_{\eta^3}\}$ are always permuted as blocks, and the action on the set of three blocks is the cyclic group of order 3. The stabilizer of each of each block induces the full symmetric group of order 6 on the three elements of the block.

By the pigeonhole principle, since there are 25 points of C (besides $[0:0:0:1]$ and $[0:0:1:0]$) on the nine curves, it follows that the conics in at least one of the blocks contain a total of at least 9 points of C. Permuting the blocks, we may assume that this block is $\{C_0, C_1, C_\infty\}$. Permuting the conics within the block, we may also assume that

$$\#(C_\infty \cap P) \geq \#(C_0 \cap P) \geq \#(C_1 \cap P).$$

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

Certainly we now have $\#(C_\infty \cap P) \geq 3$. Applying transformations of the form $X \mapsto X$, $Y \mapsto Y$, $Z \mapsto \alpha Z$, $W \mapsto \alpha^{-1}W$ and transformations of the form $X \mapsto X$, $Y \mapsto Y$, $Z \mapsto \alpha W$, $W \mapsto \alpha^{-1}Z$, as well as by applying the Frobenius automorphism of $\mathbb{F}_8$ to the coefficients of P, we may suppose that $\#(C_\infty \cap P)$ contains the two points $[0{:}1{:}1{:}1]$ and $[0{:}1{:}\eta{:}\eta^{-1}]$, and at least one of the two points $[0{:}1{:}\eta^2{:}\eta^{-2}]$ and $[0{:}1{:}\eta^3{:}\eta^{-3}]$. We obtain the following proposition.

Proposition 3.3 *If there exists a cubic hypersurface $P \subset \mathbb{P}^3_{\mathbb{F}_8}$ whose intersection with $\{X^2 + XY + Y^2 = ZW\}$ is a smooth geometrically irreducible curve of genus 4 with 27 $\mathbb{F}_8$-points, then there exists such a hypersurface satisfying the following conditions:*

- $c_{X^3} = c_{X^2Y} = c_{X^2Z} = c_{X^2W} = c_{Z^3} = c_{W^3} = 0$,
- $c_{Y^2Z} = \eta^{-1}c_{Y^2W} + \eta^3 c_{YZ^2} + \eta c_{YW^2} + c_{Z^2W} + \eta^{-1}c_{ZW^2}$,
- $c_{Y^3} = c_{Y^2Z} + c_{Y^2W} + c_{YZ^2} + c_{YZW} + c_{YW^2} + c_{Z^2W} + c_{ZW^2}$,
- *at least one of* $[0{:}1{:}\eta^2{:}\eta^{-2}]$ *and* $[0{:}1{:}\eta^3{:}\eta^{-3}]$ *lies on P,*
- $\#(C_\infty \cap P) \geq \#(C_0 \cap P) \geq \#(C_1 \cap P)$ *and* $\#(C_\infty \cap P) + \#(C_0 \cap P) + \#(C_1 \cap P) \geq 9$.

Proof Subtracting appropriate multiples of the quadric, we may assume that $c_{X^3} = c_{X^2Y} = c_{X^2Z} = c_{X^2W} = 0$. Since we may assume that $[0{:}0{:}0{:}1]$ and $[0{:}0{:}1{:}0]$ lie on the cubic P, it follows that we may suppose $c_{Z^3} = c_{W^3} = 0$. The two long sums ensure that $[0{:}1{:}1{:}1]$ and $[0{:}1{:}\eta{:}\eta^{-1}]$ lie on P. That we may suppose the remainder of the conditions follows from our reductions preceding the proposition. ∎

4 Computations

4.1 Publicly Available Data

The programs we use, the data they produce, and documentation, are available on the web at http://www.math.mcgill.ca/∼dsavitt/curves/ and the longest of our computations took under two days to run.

4.2 Listing Cubics

The computations we perform are straightforward. We write a C program to perform arithmetic in $\mathbb{F}_8$, and then for each of our three quadrics, we simply cycle through all possibilities for the coefficients of homogeneous cubics in four variables subject to the conditions we are able to impose from Propositions 3.1, 3.2, and 3.3. For each possible vector of coefficients, we count how many points of the quadric under consideration lie on the cubic. Each time the intersection contains exactly 27 points, the program prints the cubic polynomial in a format which is readable by the MAGMA computation package [BCP]. In order to speed this up significantly, we store in advance the value of each cubic monomial evaluated at each $\mathbb{F}_8$-point of the quadric, so that to determine whether a point of the quadric lies on the cubic is simply a matter of evaluating a predetermined linear form in the coefficients. For the quadric $X^2 + XY + Y^2 = ZW$, we also add routines to check the final two conditions of Proposition 3.3 and discard those cubics in violation of them.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

In order to build redundancy into our computations, we write MAGMA routines which given a cubic will count the number of points of our quadric which lie on that cubic. Using these routines, we can confirm that our C programs are correctly counting the points on our cubics; indeed we can list the points on the cubic and check that the points we wish to force to lie on the cubic are really there. However, the streamlined C programs will be faster than the MAGMA routines, which is why we use the C program and not MAGMA for the computations.

4.3 Discarding Cubics

From the above computations, we obtain a long list of cubics whose $\mathbb{F}_8$-intersection with a particular quadric has size 27. If it is true that there are no smooth geometrically irreducible curves of genus 4 over $\mathbb{F}_8$ with exactly 27 points, we expect that each of these intersections will be (geometrically) reducible. In order to test this, for each of these cubic-quadric pairs we use MAGMA to count the number of $\mathbb{F}_{64}$-points on their intersection. If the original curve were actually smooth and geometrically irreducible, then the number of $\mathbb{F}_{64}$-points will be one of the possibilities admitted by the Weil conjectures. If the original curve is reducible, then we expect the number of $\mathbb{F}_{64}$-points will be too large.

Explicitly, the methods of Section 2 of [Lau2] leave only two possibilities for the list of eigenvalues of Frobenius on a smooth geometrically irreducible curve of genus 4 over $\mathbb{F}_8$ with 27 $\mathbb{F}_8$-points. If the eigenvalues are $\alpha_i, \overline{\alpha_i}$, $i = 1, 2, 3, 4$, the possibilities are: $(-\alpha_i - \overline{\alpha_i})_i = (5, 5, 5, 3)$ and $(-\alpha_i - \overline{\alpha_i})_i = (\frac{9\pm\sqrt{5}}{2}, \frac{9\pm\sqrt{5}}{2})$. Using that $\alpha_i\overline{\alpha_i} = 8$, we compute that $\sum_i(\alpha_i^2 + \overline{\alpha_i}^2) = 20$ or 22, and so the total number of $\mathbb{F}_{64}$-points must be either $1 + 64 - 20 = 45$ or $1 + 64 - 22 = 43$.

In fact, our computations in MAGMA show that every one of the cubics we have listed intersects the associated quadric in at least 119 points. This establishes:

Theorem 4.1 *There is no smooth, geometrically irreducible curve of genus* 4 *over* $\mathbb{F}_8$ *with* 27 *points.*

Combined with what was already known, we obtain:

Corollary 4.2 *The maximal number of points on a curve of genus* 4 *over* $\mathbb{F}_8$ *is* 25.

Remark It would be of interest to know whether the combinatorial arguments we have given which eliminate the possibility of 28 points on an irreducible curve of genus 4 over $\mathbb{F}_8$ lying on $XY = Z^2$ or $XY = ZW$ can be improved to eliminate the possibility of 27 points, or can be extended to curves lying on $X^2 + XY + Y^2 = ZW$.

5 Bad Curves With 27 Points

As explained above, in our computer search we find numerous examples where our cubic and our quadric intersect in exactly 27 $\mathbb{F}_8$-points. However, when we count the number of $\mathbb{F}_{64}$-points on the intersection, we find that the answer is always in the

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

following list: 119, 181, 189, 191, 195, 197, 199, or 205. Moreover, on the degenerate and the nonsplit nondegenerate quadrics, we only find examples with 189 and 191 $\mathbb{F}_{64}$-points. In this section, we explain why these are the only possibilities, and we list (along with examples) precisely the ways in which they can occur. This provides significant reassurance that our computer calculations are correct.

5.1 Preliminary Lemmas

For ease of reference, we note the following facts:

Lemma 5.1 *If K/k is any nontrivial field extension, then a curve of degree d over K which is not definable over k may have at most d^2 k-points under any embedding into $\mathbb{P}^3_K$.*

Proof By Bézout's theorem, two plane curves of degree d intersect in d^2 points. As a consequence, two different curves of degree d in projective space may intersect in at most d^2 points: otherwise, they coincide under every projection to the plane, and so they must coincide. As a result, there is at most one curve of degree d through any $d^2 + 1$ points in projective space. However, if there is only one curve of degree d through a set of k-points, then by linear algebra that curve is defined over k. The lemma follows. ∎

Lemma 5.2 *If the intersection of a cubic and a quadric in $\mathbb{P}^3_{\mathbb{F}_8}$ has a component defined over $\mathbb{F}_8$ and of degree* 3, 4, *or* 5, *then that component has at most* 9, 14, *or* 18 $\mathbb{F}_8$*-points respectively.*

Proof Any component of our intersection which is a plane curve lies on a quadric, and so has degree at most 2. Therefore any cubic component has genus 0, any quartic component has genus at most 1, and any quintic component has genus at most 2. (See Figure 18 on page 354 of [Har].) The Serre-Weil bounds on the number of points on curves of genus 0, 1, and 2 over $\mathbb{F}_8$ are 9, 14, and 19 respectively. The first two of these bounds are met. The maximum number of points on a curve of genus 2 over $\mathbb{F}_q$ was determined for all q by Serre (this is Théorème 4 in [Se2], and may also be found as Proposition 1 in [GV]). When $q = 8$, this bound is 18. ∎

Lemma 5.3 *If the intersection C of a cubic and a quadric in $\mathbb{P}^3_{\mathbb{F}_8}$ has* 27 $\mathbb{F}_8$*-points but is not a smooth, geometrically irreducible curve of genus* 4, *then the intersection is geometrically reducible.*

Proof Assume that C is geometrically irreducible but singular. We will show that it cannot have 27 points. Since the intersection is not planar, the arithmetic genus is at most 4. (Again, see Figure 18 in [Har].) Let C' be the normalization of C. Then by the discussion in Section IV.7 of [Se1], the arithmetic genus of C' is $4 - a$ where a is an integer between 1 and 4, and moreover the number of $\mathbb{F}_8$-points of C' differs from the number of $\mathbb{F}_8$ points by at most a. By the Weil conjectures, C may have at most $9 + 5 \cdot (4 - a) + a = 29 - 4a \leq 25$ points. ∎

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

Similarly, suppose C is a singular curve over $\mathbb{F}_8$ of arithmetic genus 1. Then the normalization C' has arithmetic genus 0, so has exactly 9 $\mathbb{F}_8$-points. The singularity of C must be an ordinary double-point, and the number of $\mathbb{F}_8$-points of C must be either 8 or 10, depending on whether the points of C' lying over the singularity are defined over $\mathbb{F}_8$ or $\mathbb{F}_{64}$ respectively. In either case, the number of points of C over $\mathbb{F}_{64}$ will be 64.

Finally, we note that the components of a geometrically reducible curve are permuted by Galois. In particular, if there is only one component of a curve over $\mathbb{F}_8$ of a given degree, that component must be defined over $\mathbb{F}_8$.

5.2 Analysis of Cases

We saw in the previous section that any "bad" curve with 27 points must be geometrically reducible. We therefore organize our discussion around the possible lists of degrees for the geometric components of our bad curve.

At the outset, we remark that the quadric surface $X^2+XY+Y^2+ZW = 0$ contains no $\mathbb{F}_8$-lines. Moreover, every $\mathbb{F}_8$-line on the cone $XY + Z^2 = 0$ passes through the vertex of the cone, and in our computations we have specifically excluded the cubic surfaces which contain the vertex of the cone. Therefore, every case in which the bad curve contains an $\mathbb{F}_8$-line can arise only when the quadric surface under consideration is $XY + ZW = 0$, which is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. We recall that a curve of bidegree (a, b) in $\mathbb{P}^1 \times \mathbb{P}^1$ has arithmetic genus $(a-1)(b-1)$ and intersects a curve of bidegree (c, d) exactly $ad + bc$ times.

Degrees $(5, 1)$ By the note at the end of the preceding subsection, both components are defined over $\mathbb{F}_8$, and so this case can only be found on $XY + ZW = 0$. By the argument in 5.3, if the component of degree 5 is singular, it has at most 15 points; and since the component of degree 1 has only 9 points, this is too few points. Thus the component of degree 5 is nonsingular. By Lemma 5.2, the component of degree 5 has at most 18 points, so to get a total of 27 $\mathbb{F}_8$-points must have exactly 18 points.

A genus 2 curve of degree 5 over $\mathbb{F}_8$ with 18 points has "defect 1" in the terminology of [Lau2], and the negatives of the Frobenius traces are either $5, 4$ or $9/2 \pm \sqrt{5}/2$. By criterion (2.3) of [Lau2], the former cannot occur. In the second case, one checks from the Weil conjectures that the number of $\mathbb{F}_{64}$-points of the curve is exactly 54.

An $\mathbb{F}_8$-line has 9 points, so the linear component and the component of degree 5 do not meet over $\mathbb{F}_8$. Since the components have bidegrees $(3, 2)$ and $(0, 1)$, and therefore intersect exactly 3 times over the algebraic closure, the two components cannot intersect over $\mathbb{F}_{64}$ either. Consequently, in this case we should find exactly $65 + 54 = 119$ $\mathbb{F}_{64}$-points on the bad curve.

Degrees $(4, 2)$ By Lemma 5.2, there could be at most $14 + 9 = 23$ points on these components, so this case does not occur.

Degrees $(3, 3)$ If the two components are defined over $\mathbb{F}_8$, they have at most 9 $\mathbb{F}_8$-points by Lemma 5.2; if they are not defined over $\mathbb{F}_8$, we draw the same conclusion from Lemma 5.1. Either way, there are at most 18 points on these components, and

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

so this case does not occur.

Degrees $(4,1,1)$ The two lines must be defined over $\mathbb{F}_8$, or else there are at most $14+1+1$ points, so we may restrict attention to the quadric $XY+ZW=0$. We note that the list of bidegrees must either be $(3,1)$, $(0,1)$, $(0,1)$, or $(2,2)$, $(0,1)$, $(1,0)$.

In the former case, all three components have arithmetic genus 0, so have 9 $\mathbb{F}_8$-points and must not intersect over $\mathbb{F}_8$. The components of bidegree $(3,1)$ and $(0,1)$ intersect three times over the algebraic closure, so if they do not intersect over $\mathbb{F}_8$ then they cannot intersect over $\mathbb{F}_{64}$. Since two lines of bidegree $(0,1)$ never intersect, there must be a total of $3 \cdot 65 = 195$ points of intersection over $\mathbb{F}_{64}$.

In the latter case, the component of bidegree $(2,2)$ has arithmetic genus 1. The lines of bidegree $(0,1)$ and $(1,0)$ intersect once, and so have exactly 17 $\mathbb{F}_8$-points between them. Thus the curve of genus 1 must have at least 10 $\mathbb{F}_8$-points. We consider each possibility in turn, recalling that a singular curve of arithmetic genus 1 has at most 10 $\mathbb{F}_8$-points. Note that by Honda-Tate theory, a curve of genus 1 over $\mathbb{F}_8$ does not have 11 points. (See Theorem 4.1 of [Wat].)

- *If the curve of genus* 1 *has* 10 *points and is nonsingular*, then it has 80 points over $\mathbb{F}_{64}$. It does not meet either line over $\mathbb{F}_8$, but must meet them each in a pair of conjugate points over $\mathbb{F}_{64}$. These intersection points are different for each line, as the two lines are distinct. Since the lines intersect once, the total number of $\mathbb{F}_{64}$-points must be $65+65+80-5=205$.

- *If the curve of genus* 1 *has* 10 *points and is singular*, then it has 64 points over $\mathbb{F}_{64}$. The rest of our analysis in the previous case remains the same, and so the total number of $\mathbb{F}_{64}$-points must be $65+65+64-5=189$.

- *If the curve of genus* 1 *has* 12 *points*, then it has 72 points over $\mathbb{F}_{64}$. The curve of genus 1 must have two points of intersection with the lines over $\mathbb{F}_8$, and so depending on the intersection geometry may have either 2 or 4 points of intersection with the lines over $\mathbb{F}_{64}$. The total number of $\mathbb{F}_{64}$ points is either $129+72-2=199$ (if the curve of genus 1 intersects each line at a double-point, or else has a double-point with one line at the intersection of the two lines and meets the other line singly there and at one other point) or $129+72-4=197$ (if the curve of genus 1 intersects both lines in two distinct points).

- *If the curve of genus* 1 *has* 13 *points*, then it has 65 points over $\mathbb{F}_{64}$ and must intersect the two lines in three points over $\mathbb{F}_8$. The only way this is possible is to pass through the point of intersection of the two lines, and to meet each line once more over $\mathbb{F}_8$. Then the total number of points over $\mathbb{F}_{64}$ is $129+65-3=191$.

- *If the curve of genus* 1 *has* 14 *points*, then it has 56 points over $\mathbb{F}_{64}$ and has four distinct points of $\mathbb{F}_8$-intersection with the lines. The total number of points over $\mathbb{F}_{64}$ is then $129+56-4=181$.

Degrees $(3,2,1)$ All must be defined over $\mathbb{F}_8$, and so can occur only in the $XY+ZW=0$ case. Each component would have 9 points, but the component of bidegree $(1,1)$ must meet the linear component, so we cannot reach as many as 27 $\mathbb{F}_8$-points.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

Degrees $(2,2,2)$ All must be defined over $\mathbb{F}_8$, or else we have at most $9+4+4<27$ $\mathbb{F}_8$-points. Each component has 9 points, and is the intersection of a plane with our quadric. Hence any two of the components intersect in 2 points over $\mathbb{F}_{64}$, and so have 128 $\mathbb{F}_{64}$-points between them. The third component has either $65-2$ or $65-4$ points not on either of the first two, and so there are either 189 or 191 $\mathbb{F}_{64}$-points in total. Note that this is the only case in which we are not limited to the split nondegenerate quadric.

Degrees $(3,1,1,1)$ If the lines are not all defined over $\mathbb{F}_8$, then there are at most $9+9+1+1<27$ points. The bidegrees must be $(1,2)$, $(1,0)$, $(1,0)$, $(0,1)$ and so there are at most 7 points of intersection between the components. Then there are at least $36-7>27$ $\mathbb{F}_8$-points, which is too many, and so this case cannot occur.

Degrees $(2,2,1,1)$ Again every component must be defined over $\mathbb{F}_8$, and the bidegrees are $(1,1)$, $(1,1)$, $(0,1)$, $(1,0)$. Once again there are too many points.

Degrees $(2,1,1,1,1)$ At least two of the lines must be defined over $\mathbb{F}_8$. So, if not all of the lines are defined over $\mathbb{F}_8$, then precisely two are not. The two lines not defined over $\mathbb{F}_8$ would either both have bidegree $(1,0)$ or both have bidegree $(0,1)$, and so would not meet; therefore they could not contain any $\mathbb{F}_8$-points, as the lines are Galois-conjugate and any $\mathbb{F}_8$-points on them would lie in their intersection. Therefore, since the curve of bidegree $(1,1)$ intersects the two $\mathbb{F}_8$-lines, the configuration could contain at most $27-2=25$ $\mathbb{F}_8$-points. On the other hand, if all the lines are defined over $\mathbb{F}_8$, there are far too many $\mathbb{F}_8$-points. So this case cannot occur.

Degrees $(1,1,1,1,1,1)$ If four of the lines are defined over $\mathbb{F}_8$, then there are too many points; and if there are only two, then there are too few points. However, it is possible that the three lines of (say) bidegree $(1,0)$ could be defined over $\mathbb{F}_8$, while the three lines of bidegree $(0,1)$ could be defined over $\mathbb{F}_{512}$. Then over F_{64} there would be exactly $3\cdot 65=195$ points.

To summarize: on any of the quadrics, our bad curve may decompose into three plane quadric curves over $\mathbb{F}_8$. In this case there are either 189 or 191 $\mathbb{F}_{64}$-points on the bad curve. This is the only possibility on the degenerate and nonsplit nondegenerate quadrics. In the split nondegenerate case, we have the following additional possibilities:

- The bad curve has two components, both defined over $\mathbb{F}_8$, one of bidegree $(3,2)$ and one of bidegree $(0,1)$. In this case there are 119 $\mathbb{F}_{64}$-points.
- The bad curve has three components, all defined over $\mathbb{F}_8$, one of bidegree $(3,1)$ and two lines of bidegree $(0,1)$. In this case there are 195 $\mathbb{F}_{64}$-points.
- The bad curve has three components, all defined over $\mathbb{F}_8$, one of bidegree $(2,2)$ and lines of bidegree $(0,1)$ and $(1,0)$. In this case, there are 189, 205, 199, 197, 191, or 181 $\mathbb{F}_{64}$-points, depending on whether the curve of bidegree $(2,2)$ is singular with 10 $\mathbb{F}_8$-points, or nonsingular with 10, 12, 12, 13, or 14 $\mathbb{F}_8$-points respectively.
- The bad curve has six linear components, three defined over $\mathbb{F}_8$ and three defined over $\mathbb{F}_{512}$. In this case there are 195 $\mathbb{F}_{64}$-points.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

5.3 Examples

Scouring our computer calculations, we have found an example of each of the possibilities for bad curves enumerated in the previous section, and so all of these possibilities do indeed occur. We give a few of these examples here; the interested reader may refer to math.NT/0201226 at http://arXiv.org or to http://www.math.mcgill.ca/~dsavitt/curves/examples.dvi for the full list. (This file is also available in .ps and .pdf format.)

Recall that $\eta \in \mathbb{F}_8$ is a chosen root of $\eta^3 + \eta + 1 = 0$. Let β be a generator of $\mathbb{F}_{64}^\times$ such that $\beta^9 = \eta$. Each intersection described below has exactly 27 points over F_8.

- The intersection of $XY + ZW = 0$ with the cubic $X^2W + \eta XYW + \eta^{-1}XZW + \eta^{-3}XW^2 + \eta Y^2Z + Y^2W + \eta^{-2}YZ^2 + \eta^{-1}YZW + YW^2 = 0$ contains the line $[X:0:Z:0]$ and a component of degree 5, and has 119 points over $\mathbb{F}_{64}$.
- The intersection of $XY + ZW = 0$ with the cubic

$$(\eta Y + Z)(YZ + XZ + \eta XW + \eta^{-1}W^2 + \eta ZW + \eta^{-1}YW)$$

contains the lines $[\eta W:Y:\eta Y:W]$ and $[X:0:0:W]$. The intersection of $XY + ZW = 0$ with $YZ + XZ + \eta XW + \eta^{-1}W^2 + \eta ZW + \eta^{-1}YW = 0$ is an elliptic curve with 12 $\mathbb{F}_8$-points and 72 $\mathbb{F}_{64}$-points. It meets the line $[X:0:0:W]$ at the two points $[1:0:0:0]$ and $[1:0:0:\eta^2]$, and meets the line $[\eta W:Y:\eta Y:W]$ at the two Galois-conjugate points $[\beta^{59}:1:\beta^9:\beta^{50}]$ and $[\beta^{31}:1:\beta^9:\beta^{22}]$. The intersection of the quadric and the cubic has 197 points over $\mathbb{F}_{64}$.

- The intersection of $XY + ZW = 0$ with the cubic $\eta^{-2}X^2Z + \eta^3XYZ + \eta^3XYW + \eta^{-2}XZ^2 + \eta^3XZW + Y^2W + \eta^3YZW + YW^2 = 0$ contains the three non-intersecting lines $[0:Y:Z:0]$, $[X:0:0:W]$, and $[X:Y:X:Y]$ and three lines defined over $\mathbb{F}_{512}$. The intersection has 195 points over $\mathbb{F}_{64}$.

References

[ACGH] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves, Volume I*. New York, Springer-Verlag, 1985.

[Arf] Cahit Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik 2. I.* J. Reine Angew. Math. **183**(1941), 148–167.

[BCP] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language.* Computational Algebra and Number Theory, London, 1993, J. Symbolic Comput. **24**(1997), 3–4, 235–265.

[GV] Gerard van der Geer and Marcel van der Vlugt. *Tables of curves with many points*. Available at: http://www.science.uva.nl/~geer/

[Har] Robin Hartshorne, *Algebraic Geometry*. New York, Springer-Verlag, 1977.

[HS] Marc Hindry and Joseph H. Silverman, *Diophantine Geometry, An Introduction*. New York, Springer-Verlag, 2000.

[Lau1] Kristin Lauter, *Improved upper bounds for the number of rational points on algebraic curves over finite fields*. C. R. Acad. Sci. Paris Sér. I **328**(1999), 1181–1185.

[Lau2] ———, *Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields*. With an appendix in French by J.-P. Serre., J. Algebraic Geom. (1) **10**(2001), 19–36.

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

[Se1] J.-P. Serre, *Algebraic Groups and Class Fields*. New York, Springer-Verlag, 1988.
[Se2] ———, *Nombre de points des courbes algébriques sur* $\mathbb{F}_q$. Sém. de Théorie des Nombres de Bordeaux, 1982/83, **22**, = Oeuvres III, No. 129, 664–668.
[Wat] William C. Waterhouse, *Abelian Varieties over Finite Fields*. Ann. Sci. École Norm. Sup. (4) **2**(1989), 521–560.

Department of Mathematics
McGill University
and
CICMA
e-mail: dsavitt@math.mcgill.ca

Appendix

Kristin Lauter

A.1. Introduction

The purpose of this appendix is to give a list of the possible zeta functions for curves with defect 3. As a special case, we will show that there is no genus 4 curve over $\mathbb{F}_8$ with 26 rational points.

A.2. Definitions

By a *curve* over $\mathbb{F}_q$, we mean a smooth, projective, absolutely irreducible curve. For a curve, C, let $g = g(C)$ denote the genus, and $N(C)$ denote the number of rational points over $\mathbb{F}_q$. A curve C has *defect* k if it fails to meet the Serre-Weil bound by exactly k:

$$N(C) = q + 1 + gm - k,$$

where

$$m = [2\sqrt{q}].$$

The *zeta function* of a curve over $\mathbb{F}_q$ is defined as a power series, but it is known that it is a rational function, and can be written in the form

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

where

$$h(t) = \prod_{i=1}^{g}(1-\alpha_i t)(1-\bar{\alpha}_i t)$$

is a polynomial with coefficients in $\mathbb{Z}$, and α_i and $\bar{\alpha}_i$ are algebraic integers with complex absolute value $\sqrt{q}$. We say that a curve has *zeta function of type* $(x_1, \ldots, x_g)$ if

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

$x_i = -(\alpha_i + \bar{\alpha}_i)$, $i = 1, \ldots, g$. Define the polynomial $P(t)$:

$$P(t) = \prod_{i=1}^{g} \big(t - (m + 1 - x_i)\big),$$

and the set F_k:

$$F_k = \{t^d + a_1 t^{d-1} + \cdots + a_d \in \mathbb{Z}[t] \mid -a_1 = d + k, \text{ all roots positive reals}\}.$$

The $m + 1 - x_i$ are totally positive algebraic integers, so if

$$\sum_{i=1}^{g} x_i = gm - k,$$

then $P(t) \in F_k$, since $\deg P = g$, and $-a_1 = g + k$. We say $P(t)$ is a *polynomial of defect k*.

A.3. Defect 3

Using the method of Smyth as explained in [3] or Section 2 of [2], we restrict the possibilities for the type of the zeta function for defect 3 curves by making a list of the possibilities for the irreducible factors of the polynomials $P(t)$.

The possibilities are divided into four types given in the following four tables.

Type 1 is an irreducible polynomial of defect 3 and the rest of the factors are made up of defect 0 polynomials. For $k = 0$, the defect 0 polynomial is $P(t) = (t - 1)$, so the x_i corresponding to this factor is $x_i = m$.

Type 2 is an irreducible polynomial of defect 2 combined with the defect 1 polynomial $(t - 2)$ and copies of the defect 0 polynomial $(t - 1)$.

Type 3 is an irreducible polynomial of defect 2 combined with the defect 1 polynomial $(t^2 - 3t + 1)$ and copies of the defect 0 polynomial $(t - 1)$.

Type 4 consists of the four possible combinations of the two defect 1 polynomials with the rest of the factors equal to the defect 0 polynomial $(t - 1)$.

For each pair (q, g),there could be a number of reasons why an entry in the above tables does not correspond to the zeta function of a curve.

Using the following three reasons from Section 2 of [2] we can eliminate many of the entries from the tables.

(2.1) The absolute value of each x_i must be less than $2\sqrt{q}$.

(2.2) The number of places of degree d on a curve is nonnegative.

(2.3) The numerator of the zeta function of a curve is not decomposable.

The last column in each table indicates the restriction that comes from reason (2.1): $\{2\sqrt{q}\} \geq 1 - x$, where x is the smallest root of $P(t)$.

Proposition A.1 *The following entries from the tables do not correspond to the zeta function of a curve for reason (2.3).*

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

#	deg	coefficients	$(x_1, \dots, x_g)$	$g \geq ?$	$\{2\sqrt{q}\} \geq ?$
1.	4	1 −7 14 −8 1		$g \geq 4$	0.827…
2.	4	1 −7 13 −7 1		$g \geq 4$	0.772…
3.	3	1 −6 5 −1		$g \geq 3$	0.692…
4.	3	1 −6 7 −1		$g \geq 3$	0.834…
5.	3	1 −6 8 −1		$g \geq 3$	0.860…
6.	3	1 −6 8 −2		$g \geq 3$	0.675…
7.	3	1 −6 9 −1		$g \geq 3$	0.879…
8.	3	1 −6 9 −3		$g \geq 3$	0.532…
9.	2	1 −5 5	$(m, \dots, m - \frac{3\pm\sqrt{5}}{2})$	$g \geq 2$	
10.	2	1 −5 3	$(m, \dots, m - \frac{3\pm\sqrt{13}}{2})$	$g \geq 2$	0.302…
11.	2	1 −5 2	$(m, \dots, m - \frac{3\pm\sqrt{17}}{2})$	$g \geq 2$	0.561…
12.	2	1 −5 1	$(m, \dots, m - \frac{3\pm\sqrt{21}}{2})$	$g \geq 2$	0.791…
13.	1	1 −4	$(m, \dots, m - 3)$	$g \geq 1$	0

Table 1: Possibilities for $P(t)$ and $(x_1, \dots, x_g)$ for defect 3: Type 1

#	deg	coefficients	$(x_1, \dots, x_g)$	$g \geq ?$	$\{2\sqrt{q}\} \geq ?$
14.	3	1 −5 6 -1		$g \geq 4$	0.8019…
15.	2	1 −4 2	$\big(m - (1 \pm \sqrt{2}), m - 1, m, \dots\big)$	$g \geq 3$	0.414…
16.	2	1 −4 1	$\big(m - (1 \pm \sqrt{3}), m - 1, m, \dots\big)$	$g \geq 3$	0.732…
17.	1	1 −3	$(m - 2, m - 1, m, \dots)$	$g \geq 2$	0

Table 2: Possibilities for $P(t)$ and $(x_1, \dots, x_g)$ for defect 3: Type 2

- #17 *for genus* $g \geq 2$,
- #9, 10, 21 *for genus* $g \geq 3$,
- #3, 4, 6, 8, 14, 15, 19, 20, 22, 23 *for genus* $g \geq 4$,
- #1, 2, 18, 24 *for genus* $g \geq 5$,
- #25 *for genus* $g \geq 7$.

Proof For each entry, it suffices to factor the corresponding polynomial

$$F(T) = \prod_{i=1}^{g} \big(T - (\alpha_i + \bar{\alpha}_i)\big) = \prod_{i=1}^{g} (T + x_i)$$

into two factors, $f(T)$ and $g(T)$ such that the resultant of f and g is ± 1 (see Lemma 4.1, [1]). For example, for entry #8, the resultant of

$$T^3 + (3m - 3)T^2 + (3m^2 - 6m)T + m^3 - 3m^2 + 1 \quad \text{and} \quad (T + m)$$

is -1, so entry #8 is not possible for $g \geq 4$. For entry #19,

$$\text{resultant}\big(T^2 + (2m - 2)T + m^2 - 2m - 1, T^2 + (2m - 1)T + m^2 - m - 1\big) = -1,$$

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

#	deg	coefficients	$(x_1, \dots, x_g)$	$g \geq ?$	$\{2\sqrt{q}\} \geq ?$
18.	3	$1\ -5\ 6\ -1$		$g \geq 5$	0.8019…
19.	2	$1\ -4\ 2$	$(m-(1\pm\sqrt{2}), m-\frac{1\pm\sqrt{5}}{2}, m, \dots)$	$g \geq 4$	0.618…
20.	2	$1\ -4\ 1$	$(m-(1\pm\sqrt{3}), m-\frac{1\pm\sqrt{5}}{2}, m, \dots)$	$g \geq 4$	0.732…
21.	1	$1\ -3$	$(m-2, m-\frac{1\pm\sqrt{5}}{2}, m, \dots)$	$g \geq 3$	0.618…

Table 3: Possibilities for $P(t)$ and $(x_1, \dots, x_g)$ for defect 3: Type 3

#	$(x_1, \dots, x_g)$	$g \geq ?$	$\{2\sqrt{q}\} \geq ?$
22.	$(m-1, m-1, m-1, m, \dots)$	$g \geq 3$	0
23.	$(m-\frac{1\pm\sqrt{5}}{2}, m-1, m-1, m\dots)$	$g \geq 4$	0.618…
24.	$(m-\frac{1\pm\sqrt{5}}{2}, m-\frac{1\pm\sqrt{5}}{2}, m-1, m, \dots)$	$g \geq 5$	0.618…
25.	$(m-\frac{1\pm\sqrt{5}}{2}, m-\frac{1\pm\sqrt{5}}{2}, m-\frac{1\pm\sqrt{5}}{2}, m, \dots)$	$g \geq 6$	0.618…

Table 4: Possibilities $(x_1, \dots, x_g)$ for defect 3: Type 4

so this entry is not possible for $g = 4$, and

$$\text{resultant}\Big(\big(T^2+(2m-2)T+m^2-2m-1\big)(T+m), T^2+(2m-1)T+m^2-m-1\Big) = 1,$$

so it is not possible for $g > 4$ either. The decomposition of other entries is similar. ∎

Proposition A.2 *Entry #11 does not correspond to the zeta function of a curve for*

$$g > \frac{q^2 - q + 8m^2 - 10m - 16}{5m^2 - 7m - 2q}$$

for reason (2.2).

Proof The proof is similar to the proof of Proposition 1 in [2]. The coefficients of the polynomial

$$\left(T + m - \frac{3+\sqrt{17}}{2}\right)\left(T + m - \frac{3-\sqrt{17}}{2}\right)(T+m)^{g-2}$$

can be computed in two ways: as binomial coefficients or via Newton's relations between the elementary symmetric functions, $\{b_n\}$, and the power functions,

$$s_n = \sum_{i=1}^{g} (\alpha_i + \bar{\alpha}_i)^n.$$

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

Using the identity

$$b_2 = \frac{1}{2}(s_1^2 - s_2),$$

and equating the coefficients of the $g-2$ term computed in the two ways yields:

$$\frac{(g-2)(g-3)}{2}m^2 + (g-2)m + (m^2 - 3m - 2)$$
$$= \frac{1}{2}\Big((gm-3)^2 - \big(q^2 + 1 - (q+1+gm-3+2a_2) + 2gq\big)\Big),$$

where a_2 is the number of places of degree 2 on the curve. By reason (2.2), we must have $a_2 \geq 0$, so rearranging yields the desired inequality. ∎

Proposition A.3 *Entry #13 does not correspond to the zeta function of a curve for*

$$g > \frac{q^2 - q + 6m - 6}{m^2 + m - 2q}$$

for reason (2.2). In general, $(m, m, \ldots, m-k)$ *does not correspond to the zeta function of a defect k curve for*

$$g > \frac{q^2 - q + 2km + k - k^2}{m^2 + m - 2q}.$$

Proof The proof is similar to the proof of Proposition A.2 above. ∎

Remark Similar bounds on the genus can be obtained for entries #5, 7, 12, 16.

Proposition A.4 *If q is an even power of a prime, then the only defect* 3 *curves with genus* $g > 3$ *have zeta function of type* $(m, \ldots, m, m-3)$. *For* $g = 3$, $(m-1, m-1, m-1)$ *is possible in some cases. For*

$$g > \frac{q^2 - q + 6m - 6}{m^2 + m - 2q},$$

defect 3 *is not possible.*

Proof This follows from reason (2.1) and the fact that entries #17 and #22 are impossible by reason (2.3) for $g \geq 2$ and $g \geq 4$ respectively. The last statement then follows from Proposition A.3. ∎

Theorem A.5 *There does not exist a genus* 4 *curve over* $\mathbb{F}_8$ *with* 26 $\mathbb{F}_8$*-points.*

Proof When $q = 8$,

$$\{2\sqrt{q}\} \approx 0.6568,$$

so using the above tables, we see that the only zeta function types possible after applying Proposition A.1 are: #11 and #13. By Proposition A.2, #11 is not possible since

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press

$g = 4 > \frac{95}{37}$. For #13, the bound on g from Proposition A.3 is $\frac{40}{7} > 4$, but #13 is not possible for a different reason in this case. Here $q = 2^3$ and $m = 5$, so $m - 3 = 2$. By Honda-Tate theory, when $q = p^e$ is an odd power of a prime, the only possible values for the trace of an elliptic curve which are divisible by the characteristic are: (see [5], p. 536)

$$0, \quad \text{for all } p, \text{ or } p^{\frac{e+1}{2}}, \quad \text{for } p = 2 \text{ or } p = 3.$$

Since an elliptic curve with trace 2 does not exist over $\mathbb{F}_8$, an abelian variety over $\mathbb{F}_8$ of type $(5, 5, 5, 2)$ does not exist either. ■

Theorem A.5 was presented at the Journées Arithmétiques in Rome in July, 1999, and at the Arizona Winter School in March, 2000.

References

[1] K. Lauter, *Non-existence of a curve over F_3 of genus* 5 *with* 14 *rational points*. Proc. Amer. Math. Soc. **128**(2000), 369–374.
[2] 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. (1) **10**(2001), 19–36.
[3] J.-P. Serre, *Rational Points on Curves over Finite Fields*. Notes by F. Gouvea of lectures at Harvard University, 1985.
[4] C. Smyth, *Totally Positive Algebraic Integers of Small Trace*. Ann. Inst. Fourier (Grenoble) (3) **33**(1984), 1–28.
[5] W. C. Waterhouse, *Abelian Varieties over Finite Fields*. Ann. Sci. École Norm. Sup. (4) **2**(1969), 521–560.

Microsoft Research
e-mail: klauter@microsoft.com

https://doi.org/10.4153/CJM-2003-015-7 Published online by Cambridge University Press