Séminaires & Congrès
11, 2005, p. 125–141

POINTLESS CURVES OF GENUS THREE AND FOUR

by

Everett W. Howe, Kristin E. Lauter & Jaap Top

Abstract. — A curve over a field k is *pointless* if it has no k-rational points. We show that there exist pointless genus-3 hyperelliptic curves over a finite field $\mathbb{F}_q$ if and only if $q \leqslant 25$, that there exist pointless smooth plane quartics over $\mathbb{F}_q$ if and only if either $q \leqslant 23$ or $q = 29$ or $q = 32$, and that there exist pointless genus-4 curves over $\mathbb{F}_q$ if and only if $q \leqslant 49$.

Résumé **(Courbes de genre 3 et 4 sans point).** — Une courbe sur un corps k est appelée *une courbe sans point* si elle n'a aucun point k-rationnel. Nous prouvons qu'il existe des courbes hyperelliptiques de genre trois sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 25$, qu'il existe des quartiques planes sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 23$, $q = 29$ ou $q = 32$, et qu'il existe des courbes de genre quatre sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 49$.

1. Introduction

What is the largest number of rational points there can be on a curve of genus g over a finite field $\mathbb{F}_q$? Researchers have been studying variants of this question for several decades. As van der Geer and van der Vlugt write in the introduction to their biannually-updated survey of results related to certain aspects of this subject, the attention paid to this question is

> motivated partly by possible applications in coding theory and cryptography, but just as well by the fact that the question represents an attractive mathematical challenge. [**4**]

The complementary question — What is the *smallest* number of rational points there can be on a curve of genus g over a finite field $\mathbb{F}_q$? — seems to have sparked little

2000 ***Mathematics Subject Classification.*** — Primary 11G20; Secondary 14G05, 14G10, 14G15.
Key words and phrases. — Curve, hyperelliptic curve, plane quartic, rational point, zeta function, Weil bound, Serre bound.

interest among researchers, perhaps because of the apparent *lack* of possible applications in coding theory and cryptography for curves with few points. But despite the paucity of applications, there are still mathematical challenges associated with such curves. In this paper, we address one of them:

Problem. — *Given an integer $g \geqslant 0$, determine the finite fields $\mathbb{F}_q$ over which there exists a curve of genus g having no rational points.*

We will call a curve over a field k *pointless* if it has no k-rational points. Thus the problem we propose is to determine, for a given genus g, the finite fields $\mathbb{F}_q$ over which there is a pointless curve of genus g.

The solutions to this problem for $g \leqslant 2$ are known. There are no pointless curves of genus 0 over any finite field; this follows from Wedderburn's theorem, as is shown by [**18**, § III.1.4, exer. 3]. The Weil bound for curves of genus 1 over a finite field, proven by Hasse [**5**], shows that there are no pointless curves of genus 1 over any finite field. If there is a pointless curve of genus 2 over a finite field $\mathbb{F}_q$ then the Weil bound shows that $q \leqslant 13$, and in 1972 Stark [**19**] showed that in fact $q < 13$. For each $q < 13$ there do exist pointless genus-2 curves over $\mathbb{F}_q$; a complete list of these curves is given in [**14**, Table 4].

In this paper we provide solutions for the cases $g = 3$ and $g = 4$.

Theorem 1.1. — *There exists a pointless genus-3 curve over $\mathbb{F}_q$ if and only if either $q \leqslant 25$ or $q = 29$ or $q = 32$.*

Theorem 1.2. — *There exists a pointless genus-4 curve over $\mathbb{F}_q$ if and only if $q \leqslant 49$.*

In fact, for genus-3 curves we prove a statement slightly stronger than Theorem 1.1:

Theorem 1.3. — *There exists a pointless genus-3 hyperelliptic curve over $\mathbb{F}_q$ if and only if $q \leqslant 25$; there exists a pointless smooth plane quartic curve over $\mathbb{F}_q$ if and only if either $q \leqslant 23$ or $q = 29$ or $q = 32$.*

The idea of the proofs of these theorems is simple. For any given genus g, and in particular for $g = 3$ and $g = 4$, the Weil bound can be used to provide an upper bound for the set of prime powers q such that there exist pointless curves of genus g over $\mathbb{F}_q$. For each q less than or equal to this bound, we either provide a pointless curve of genus g or use the techniques of [**8**] to prove that none exists.

We wrote above that the question of how few points there can be on a genus-g curve over $\mathbb{F}_q$ seems to have attracted little attention, and this is certainly the impression one gets from searching the literature for references to such curves. On the other hand, the question has undoubtedly occurred to researchers before. Indeed, the third author was asked this very question for the special case $g = 3$ by both N.D. Elkies and J.-P. Serre after the appearance of his joint work [**1**] with Auer. Also, while it is true that there seem to be no applications for pointless curves, it *can* be useful to know whether or not they exist. For example, Leep and Yeomans were concerned with the existence of pointless plane quartics in their work [**13**] on explicit versions of special cases of the Ax-Kochen theorem. Finally, we note that Clark and Elkies have recently proven that for every fixed prime p there is a constant A_p such that for every integer $n > 0$ there is a curve over $\mathbb{F}_p$ of genus at most $A_p n p^n$ that has no places of degree n or less.

In Section 2 we give the heuristic that guided us in our search for pointless curves. In Section 3 we give the arguments that show that there are no pointless curves of genus 3 over $\mathbb{F}_{27}$ or $\mathbb{F}_{31}$, no pointless smooth plane quartics over $\mathbb{F}_{25}$, no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{29}$ or $\mathbb{F}_{32}$, and no pointless curves of genus 4 over $\mathbb{F}_{53}$ or $\mathbb{F}_{59}$. Finally, in Sections 4 and 5 we give examples of pointless curves of genus 3 and 4 over every finite field for which such curves exist.

Conventions. — By a *curve* over a field k we mean a smooth, projective, geometrically irreducible 1-dimensional variety over k. When we define a curve by a set of equations, we mean the normalization of the projective closure of the variety defined by the equations.

Acknowledgments. — The first author spoke about the work [**8**] at AGCT-9, and he thanks the organizers Yves Aubry, Gilles Lachaud, and Michael Tsfasman for inviting him to Luminy and for organizing such a pleasant and interesting conference. The first two authors thank the editors for soliciting this paper, which made them think about other applications of the techniques developed in [**8**].

In the course of doing the work described in this paper we used the computer algebra system Magma [**2**]. Several of our Magma programs are available on the web: start at

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

and follow the links related to this paper. One of our proofs depends on an explicit description of the isomorphism classes of unimodular quaternary Hermitian forms over the quadratic ring of discriminant −11. The web site mentioned above also contains a copy of a text file that gives a list of the six isomorphism classes of such forms; we obtained this file from the web site

`http://www.math.uni-sb.de/~ag-schulze/Hermitian-lattices/`

maintained by Rainer Schulze-Pillot-Ziemen.

2. Heuristics for constructing pointless curves

To determine the correct statements of Theorems 1.1 and 1.2 we began by searching for pointless curves of genus 3 and 4 over various small finite fields. In this section we explain the heuristic we used to find families of curves in which pointless curves might be abundant. We begin with a lemma from the theory of function fields over finite fields.

Lemma 2.1. — *Let L/K be a degree-d extension of function fields over a finite field k, let M be the Galois closure of L/K, let $G = \mathrm{Gal}(M/K)$, and let $H = \mathrm{Gal}(M/L)$. Let S be the set of places $\mathfrak{p}$ of K that are unramified in L/K and for which there is at least one place $\mathfrak{q}$ of L, lying over $\mathfrak{p}$, with the same residue field as $\mathfrak{p}$. Then the set S has a Dirichlet density in the set of all places of K unramified in L/K, and this density is*

$$\delta := \frac{\# \cup_{\tau \in G} H^{\tau}}{\# G}.$$

We have $\delta \geqslant 1/d$, with equality precisely when L is a Galois extension of K. Furthermore, we have $\delta \leqslant 1 - (d-1)/\#G$.

Proof. — An easy exercise in the class field theory of function fields (*cf.* [**6**, proof of Lem. 2]) shows that the set S is precisely the set of places $\mathfrak{p}$ whose Artin symbol $(\mathfrak{p}, L/K)$ lies in the union of the conjugates of H in G. The density statement then follows from the Chebotarev density theorem.

Since H is an index-d subgroup of G, we have

$$\frac{\# \cup_{\tau \in G} H^{\tau}}{\# G} \geqslant \frac{\# H}{\# G} = \frac{1}{d}.$$

If L/K is Galois then H is trivial and the first relation in the displayed equation above is an equality. If L/K is not Galois then H is a non-normal subgroup of G, so the first relation above is an inequality.

To prove the upper bound on δ, we note that two conjugates H^{σ} and H^{τ} of H are identical when σ and τ lie in the same coset of H in G, so when we form the union of the conjugates of H we need only let τ range over a set of coset representatives of the d cosets of H in G. Furthermore, the identity element lies in every conjugate of H, so the union of the conjugates of H contains at most $d \cdot \#H - (d-1)$ elements. The upper bound follows. $\square$

Note that the density mentioned in Lemma 2.1 is a Dirichlet density. If the constant field of K is algebraically closed in the Galois closure of L/K, then the set S also has a natural density (see [**10**]). In particular, the set S has a natural density when L/K is a Galois extension and L and K have the same constant field.

Lemma 2.1 leads us to our main heuristic:

Heuristic. — *Let $C \to D$ be a degree-d cover of curves over $\mathbb{F}_q$, let L/K be the corresponding extension of function fields, and let δ be the density from Lemma 2.1. If the constant field of the Galois closure of L/K is equal to $\mathbb{F}_q$, then C will be pointless with probability $(1-\delta)^{\#D(\mathbb{F}_q)}$. In particular, if $C \to D$ is a Galois cover, then C will be pointless with probability $(1-1/d)^{\#D(\mathbb{F}_q)}$.*

Justification. — Lemma 2.1 makes it reasonable to expect that with probability $1-\delta$, a given rational point of D will have no rational points of C lying over it. Our heuristic follows if we assume that all of the points of D behave independently. □

Consider what this heuristic tells us about hyperelliptic curves. Since a hyperelliptic curve is a double cover of a genus-0 curve, we expect that a hyperelliptic curve over $\mathbb{F}_q$ will be pointless with probability $(1/2)^{q+1}$. However, if the hyperelliptic curve has more automorphisms than just the hyperelliptic involution, it will be more likely to be pointless. For instance, suppose C is a hyperelliptic curve whose automorphism group has order 4. This automorphism group will give us a Galois cover $C \to \mathbb{P}^1$ of degree 4. Then our heuristic suggests that C will be pointless with probability $(3/4)^{q+1}$.

This heuristic suggested two things to us. First, to find pointless curves it is helpful to look for curves with larger-than-usual automorphism groups. We decided to focus on curves whose automorphism groups contain the Klein 4-group, because it is easy to write down curves with this automorphism group and yet the group is large enough to give us a good chance of finding pointless curves. Second, the heuristic suggested that we look at curves C that are double covers of curves D that are double covers of $\mathbb{P}^1$. The Galois group of the resulting degree-4 cover $C \to \mathbb{P}^1$ will typically be the dihedral group of order 8, and the heuristic predicts that C will be pointless with probability $(5/8)^{q+1}$. For a fixed D, if we consider the family of double covers $C \to D$ with C of genus 3 or 4, our heuristic predicts that C will be pointless with probability $(1/2)^{\#D(\mathbb{F}_q)}$. If $\#D(\mathbb{F}_q)$ is small enough, this probability can be reasonably high.

The curves that we found by following our heuristic are listed in Sections 4 and 5.

3. Proofs of the theorems

In this section we prove the theorems stated in the introduction. Clearly Theorem 1.1 follows from Theorem 1.3, so we will only prove Theorems 1.2 and 1.3.

Proof of Theorem 1.3. — The Weil bound says that a curve of genus 3 over $\mathbb{F}_q$ has at least $q + 1 - 6\sqrt{q}$ points, and it follows immediately that if there is a pointless genus-3 curve over $\mathbb{F}_q$ then $q < 33$. In Section 4 we give examples of pointless genus-3 hyperelliptic curves over $\mathbb{F}_q$ for $q \leqslant 25$ and examples of pointless smooth plane quartics for $q \leqslant 23$, for $q = 29$, and for $q = 31$. To complete the proof, we need only prove the following statements:

(1) There are no pointless genus-3 curves over $\mathbb{F}_{31}$.
(2) There are no pointless genus-3 curves over $\mathbb{F}_{27}$.
(3) There are no pointless smooth plane quartics over $\mathbb{F}_{25}$.
(4) There are no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{32}$.
(5) There are no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{29}$.

Statement 1. — Theorem 1 of [**12**] shows that every genus-3 curve over $\mathbb{F}_{31}$ has at least 2 rational points, and statement 1 follows.

Statement 2. — To prove statement 2, we begin by running the Magma program `CheckQGN` described in [**8**]. The output of `CheckQGN(27,3,0)` shows that if C is a pointless genus-3 curve over $\mathbb{F}_{27}$ then the real Weil polynomial of C (see [**8**]) must be $(x-10)^2(x-8)$. (To reach this conclusion without relying on the computer, one can adapt the reasoning on 'defect 2' found in [**11**, § 2].) Applying Proposition 13 of [**8**], we find that C must be a double cover of an elliptic curve over $\mathbb{F}_{27}$ with exactly 20 rational points.

Up to Galois conjugacy, there are two elliptic curves over $\mathbb{F}_{27}$ with exactly 20 rational points; one is given by $y^2 = x^3 + 2x^2 + 1$ and the other by $y^2 = x^3 + 2x^2 + a$, where $a^3 - a + 1 = 0$. By using the argument given in the analogous situation in [**8**, § 6.1], we see that every genus-3 double cover of one of these two E's can be obtained by adjoining to the function field of E an element z that satisfies $z^2 = f$, where f is a function on E of degree at most 6 that is regular outside ∞, that has four zeros or poles of odd order, and that has a double zero at a point Q of E that is rational over $\mathbb{F}_{27}$. In fact, it suffices to consider Q's that represent the classes of $E(\mathbb{F}_{27})/2E(\mathbb{F}_{27})$. The first E given above has four such classes and the second has two. We can also demand that the representative points Q not be 2-torsion points.

The divisor of the function f is

$$P_1 + P_2 + P_3 + P_4 + 2Q - 6\infty$$

for some geometric points $P_1, \ldots, P_4$. We are assuming that the double cover C has no rational points, so none of the P_i can be rational over $\mathbb{F}_{27}$. In particular, none of the P_i is equal to the infinite point. Since Q is also not the infinite point (because we chose it not to be a 2-torsion point), we see that the degree of f is exactly 6.

It is easy to have Magma enumerate, for each of the six (E, Q) pairs, all of the degree-6 functions f on E that have double zeros at Q. For each such f we can check to see whether there is a rational point P on E such that $f(P)$ is a nonzero square; if there is such a point, then the double D cover of E given by $z^2 = f$ would have a rational point. For those functions f for which such a P does not exist, we can check to see whether the divisor of f has the right form. If the divisor of f does have the right form, we can compute whether the curve D has a rational point lying over Q or over ∞.

We wrote Magma routines to perform these calculations; they are available on the web at the URL mentioned in the acknowledgments. As it happens, no (E, Q) pair gives rise to a function f that passes the first two tests described in the preceding paragraph, so we never had to perform the third test.

Our conclusion is that there are no pointless genus-3 curves over $\mathbb{F}_{27}$, which completes the proof of statement 2.

Statement 3. — To prove statement 3 we start by running `CheckQGN(25,3,0)`. We find that the real Weil polynomial of a pointless genus-3 curve over $\mathbb{F}_{25}$ is either $f_1 := (x-10)^2(x-6)$ or $f_2 := (x-10)(x^2-16x+62)$ or $f_3 := (x-10)(x-9)(x-7)$ or $f_4 := (x-10)(x-8)^2$. (This list can also be obtained by using Table 4 and Theorem 1(a) of [**8**].)

We begin by considering the real Weil polynomial $f_1 = (x-10)^2(x-6)$. Suppose C is a genus-3 curve over $\mathbb{F}_{25}$ with real Weil polynomial equal to f_1. Arguing as in the proof of [**8**, Cor. 12], we find that there is an exact sequence

$$0 \longrightarrow \Delta \longrightarrow A \times E \longrightarrow \operatorname{Jac} C \longrightarrow 0,$$

where A is an abelian surface with real Weil polynomial $(x-10)^2$, where E is an elliptic curve with real Weil polynomial $x-6$, where Δ is a self-dual finite group scheme that is killed by 4, and where the projections from $A \times E$ to A and to E give monomorphisms $\Delta \hookrightarrow A$ and $\Delta \hookrightarrow E$. Furthermore, there are polarizations λ_A and λ_E on A and E whose kernels are the images of Δ under these monomorphisms, and the polarization on $\operatorname{Jac} C$ induced by the product polarization $\lambda_A \times \lambda_E$ is the canonical polarization on $\operatorname{Jac} C$.

Since Δ is isomorphic to the kernel of λ_E and since Δ is killed by 4, we see that if Δ is not trivial then it is isomorphic to either $E[2]$ or $E[4]$. If Δ were trivial then $\operatorname{Jac} C$ would be equal to $A \times E$ and the canonical polarization on $\operatorname{Jac} C$ would be a product polarization, and this is not possible. Therefore Δ is isomorphic either to $E[2]$ or $E[4]$. Since the Frobenius endomorphism of A is equal to the multiplication-by-5 map on A, the group of geometric 4-torsion points on A is a trivial Galois module. But $E[4]$ is not a trivial Galois module, so we see that Δ must be isomorphic to $E[2]$. Arguing as in the proof of [**8**, Prop. 13], we find that there must be a degree-2 map from C to E.

Thus, to find the genus-3 curves over $\mathbb{F}_{25}$ whose real Weil polynomials are equal to $(x-10)^2(x-6)$, we need only look at the genus-3 curves that are double covers of elliptic curves over $\mathbb{F}_{25}$ with 20 points and with three rational points of order 2. There are two such elliptic curves, and, as in the proof of statement 2, we can use Magma to enumerate their genus-3 double covers with no points. (Our Magma program is available at the URL mentioned in the acknowledgments.) We find that there is exactly one such double cover: if a is an element of $\mathbb{F}_{25}$ with $a^2 - a + 2 = 0$, then the double cover C of the elliptic curve $y^2 = x^3 + 2x$ given by setting $z^2 = a(x^2-2)$ has no points.

The curve C is clearly hyperelliptic, because it is a double cover of the genus-0 curve $z^2 = a(x^2-2)$. By parametrizing this genus-0 curve and manipulating the resulting equation for C, we find that C is isomorphic to the curve $y^2 = a(x^8+1)$, which is the example presented below in Section 4.

Next we show that there are no pointless genus-3 curves over $\mathbb{F}_{25}$ with real Weil polynomial equal to f_2 or f_3 or f_4.

Suppose C is a pointless genus-3 curve over $\mathbb{F}_{25}$ whose real Weil polynomial is f_2 or f_3 or f_4. By applying Proposition 13 of [**8**], we find that C must be a double cover of an elliptic curve over $\mathbb{F}_{25}$ having either 16 or 17 points. There is one elliptic curve over $\mathbb{F}_{25}$ of each of these orders. As we did above and in the proof of statement 2, we can easily have Magma enumerate the genus-3 double covers of these elliptic curves. The only complication is that for the curve with 16 points, we cannot assume that the auxiliary point Q mentioned in the proof of statement 2 is not a 2-torsion point.

The Magma program we used to enumerate these double covers can be found at the web site mentioned in the acknowledgments. Using this program, we found that the curve with 17 points has no pointless genus-3 double covers. On the other hand, we found two functions f on the curve E with 16 points such that the double cover of E defined by $z^2 = f$ is a pointless genus-3 curve. But when we computed an upper bound for the number of points on these curves over $\mathbb{F}_{625}$, we found that both of the curves have at most 540 points over $\mathbb{F}_{625}$. This upper bound is not consistent with any of the three real Weil polynomials we are considering. (In fact, one can show by direct computation that the two curves are isomorphic to the curve $y^2 = a(x^8 + 1)$ that we found earlier, whose real Weil polynomial is f_1.) Thus, there are no pointless genus-3 curves over $\mathbb{F}_{25}$ with real Weil polynomial equal to f_2 or f_3 or f_4.

This proves statement 3.

Statement 4. — Suppose that C is a pointless genus-3 curve over $\mathbb{F}_{32}$. If C were hyperelliptic, then its quadratic twist would be a genus-3 curve over $\mathbb{F}_{32}$ with 66 rational points. But [**11**, Thm. 1] shows that no such curve exists.

We give a second proof of statement 4 as well, which provides us with a little extra information and foreshadows some of our later arguments. This same proof is given in [**3**, § 3.3] and attributed to Serre.

Suppose that C is a pointless genus-3 curve over $\mathbb{F}_{32}$. Then C meets the Weil-Serre lower bound, and (as Serre shows in [**17**]) its Jacobian is therefore isogenous to the cube of an elliptic curve E over $\mathbb{F}_{32}$ whose trace of Frobenius is 11. Note that the endomorphism ring of this elliptic curve is the quadratic order $\mathcal{O}$ of discriminant $11^2 - 4 \cdot 32 = -7$. The polarizations of abelian varieties isogenous to a power of a single elliptic curve whose endomorphism ring is a maximal order can be understood in terms of Hermitian modules (see the appendix to [**12**]). Since the endomorphism ring $\mathcal{O}$ is a maximal order and a PID, there is exactly one abelian variety in the isogeny class of E^3, namely E^3 itself. Furthermore, the theory of Hermitian modules shows that the principal polarizations of E^3 correspond to the isomorphism classes of unimodular Hermitian forms on the $\mathcal{O}$-module $\mathcal{O}^3$. Hoffmann [**7**] shows that there is only one isomorphism class of indecomposable unimodular Hermitian forms on $\mathcal{O}^3$, so there is at most one Jacobian in the isogeny class of E^3, and hence at most one genus-3 curve over $\mathbb{F}_{32}$ with no points. The example we give in Section 4 is a plane quartic, so there are no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{32}$. This proves statement 4.

Statement 5. — We wrote a Magma program to find (by enumeration) all pointless genus-3 hyperelliptic curves over an arbitrary finite field $\mathbb{F}_q$ of odd characteristic with $q > 7$. We applied our program to the field $\mathbb{F}_{29}$, and we found no curves. Our Magma program is available at the URL mentioned in the acknowledgments. $\square$

Note that in the course of proving Theorem 1.3 we showed that the pointless genus-3 curves over $\mathbb{F}_{25}$ and $\mathbb{F}_{32}$ exhibited in Section 4 are the only such curves over their respective fields. Also, our program to enumerate pointless genus-3 hyperelliptic curves shows that there is only one pointless genus-3 hyperelliptic curve over $\mathbb{F}_{23}$.

Proof of Theorem 1.2. — It follows from Serre's refinement of the Weil bound [**16**, Thm. 1] that if a curve of genus 4 over $\mathbb{F}_q$ has no rational points, then $q \leqslant 59$. In Section 5 we give examples of pointless genus-3 curves over $\mathbb{F}_q$ for all q with $q \leqslant 49$, so to prove the theorem we must show that there are no pointless genus-4 curves over $\mathbb{F}_{53}$ or $\mathbb{F}_{59}$.

Combining the output of `CheckQGN(53,4,0)` with Theorem 1(b) of [**8**], we find that a pointless genus-4 curve over $\mathbb{F}_{53}$ must be a double cover of an elliptic curve E over $\mathbb{F}_{53}$ with exactly 42 points. (Again, the information obtained by running `CheckQGN` can also be obtained without recourse to the computer by modifying the 'defect 2' arguments in [**11**, § 2].)

There are four elliptic curves E over $\mathbb{F}_{53}$ with exactly 42 points. Following the arguments of [**8**, § 6.1], we find that every genus-4 double cover of such an E can be obtained by adjoining to the function field of E a root of an equation $z^2 = f$, where f is a function on E whose divisor is of the form

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

where Q is a rational point of E that is not killed by 2, and where it suffices to consider Q that cover the residue classes of $E(\mathbb{F}_{53})$ modulo $3E(\mathbb{F}_{53})$. As in the preceding proof, we wrote Magma programs to enumerate the genus-4 double covers of the four possible E's and to check to see whether all of these covers had rational points. Our programs, available at the URL mentioned in the acknowledgments, showed that every genus-4 double cover of these E's has a rational point. Thus there are no pointless genus-4 curves over $\mathbb{F}_{53}$.

Next we show that there are no pointless curves of genus 4 over $\mathbb{F}_{59}$. If C were such a curve, then C would meet the Weil-Serre lower bound, and therefore the Jacobian of C would be isogenous to the fourth power of an elliptic curve E over $\mathbb{F}_{59}$ with 45 points. Note that there is exactly one such E, and its endomorphism ring $\mathcal{O}$ is the quadratic order of discriminant -11. As in the proof of statement 4 of the proof of Theorem 1.3, we see that there is only one abelian variety in the isogeny class of E^4, and principal polarizations of E^4 correspond to the isomorphism classes of unimodular Hermitian forms on the $\mathcal{O}$-module $\mathcal{O}^4$. Schiemann [**15**] states that there are six isomorphism classes of unimodular Hermitian forms on the module $\mathcal{O}^4$. We were unable to find a listing of these isomorphism classes at the URL mentioned in [**15**], but we did find them by following links from the URL

`http://www.math.uni-sb.de/~ag-schulze/Hermitian-lattices/`

We have placed a copy of the page listing these six forms on the web site mentioned in the acknowledgments.

Three of the isomorphism classes of unimodular Hermitian forms on $\mathcal{O}^4$ are decomposable, and so do not come from the Jacobian of a curve. The three indecomposable Hermitian forms can each be written as a matrix with an upper left entry of 2. Arguing as in the proof of [**8**, Prop. 13], we find that our curve C must be a double cover of the curve E.

We are again in familiar territory. As above, it is an easy matter to write a Magma program to enumerate the genus-4 double covers of the given elliptic curve E and to check that they all have a rational point. (Our Magma programs are available at the URL mentioned in the acknowledgments.) Our computation showed that there are no pointless curves of genus 4 over $\mathbb{F}_{59}$. $\square$

4. Examples of pointless curves of genus 3

In this section we give examples of pointless curves of genus 3 over the fields where such curves exist. We only consider curves whose automorphism groups contain the Klein 4-group V. We begin with the hyperelliptic curves.

Suppose C is a genus-3 hyperelliptic curve over $\mathbb{F}_q$ whose automorphism group contains a copy of V, and assume that the hyperelliptic involution is contained in V. Then V modulo the hyperelliptic involution acts on C modulo the hyperelliptic involution, and gives us an involution on $\mathbb{P}^1$. By changing coordinates on $\mathbb{P}^1$, we may assume that the involution on $\mathbb{P}^1$ is of the form $x \mapsto n/x$ for some $n \in \mathbb{F}_q^*$. (When q is odd we need consider only two values of n, one a square and one a nonsquare. When q is even we may take $n = 1$.)

It follows that when q is odd the curve C can be defined either by an equation of the form $y^2 = f(x + n/x)$, where f is a separable quartic polynomial coprime to $x^2 - 4n$, or by an equation of the form $y^2 = xf(x+n/x)$, where f is a separable cubic polynomial coprime to $x^2 - 4n$. However, the latter possibility cannot occur if C is to be pointless. When q is even, if we assume the curve if ordinary then it may be written in the form $y^2 + y = f(x + 1/x)$, where f is a rational function with 2 simple poles, both nonzero.

q	curve
2	$y^2 + y = (x^4 + x^2 + 1)/(x^4 + x^3 + x^2 + x + 1)$
3	$y^2 = -x^8 + x^7 - x^6 - x^5 - x^3 - x^2 + x - 1$
4	$y^2 + y = (ax^4 + ax^3 + a^2x^2 + ax + a)/(x^4 + ax^3 + x^2 + ax + 1)$ where $a^2 + a + 1 = 0$
5	$y^2 = 2x^8 + 3x^4 + 2$
7	$y^2 = 3x^8 + 2x^6 + 3x^4 + 2x^2 + 3$
8	$y^2 + y = (x^4 + a^6x^3 + a^3x^2 + a^6x + 1)/(x^4 + x^3 + x^2 + x + 1)$ where $a^3 + a + 1 = 0$
9	$y^2 = a(x^8 + 1)$ where $a^2 - a - 1 = 0$
11	$y^2 = 2x^8 + 4x^6 - 2x^4 + 4x^2 + 2$
13	$y^2 = 2x^8 + 3x^7 + 3x^6 + 4x^4 + 3x^2 + 3x + 2$
16	$y^2 + y = (a^3x^4 + a^3x^3 + a^{14}x^2 + a^3x + a^3)/(x^4 + a^3x^3 + x^2 + a^3x + 1)$ where $a^4 + a + 1 = 0$
17	$y^2 = 3x^8 - 2x^5 + 4x^4 - 2x^3 + 3$
19	$y^2 = 2x^8 - x^6 - 8x^4 - x^2 + 2$
23	$y^2 = 5x^8 + x^6 + 6x^5 + 7x^4 - 6x^3 + x^2 + 5$
25	$y^2 = a(x^8 + 1)$ where $a^2 - a + 2 = 0$

TABLE 1. Examples of pointless hyperelliptic curves of genus 3 over $\mathbb{F}_q$ with automorphism group containing the Klein 4-group. For $q \neq 23$, the automorphism $x \mapsto 1/x$ of $\mathbb{P}^1$ lifts to give an automorphism of the curve; for $q = 23$, the automorphism $x \mapsto -1/x$ lifts.

We wrote a simple Magma program to search for pointless hyperelliptic curves of this form. We found such curves for every q in

$$\{2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25\}.$$

We give examples in Table 1.

Now we turn to the pointless smooth plane quartics. We searched for pointless quartics of the form

$$ax^4 + by^4 + cz^4 + dx^2y^2 + ex^2z^2 + fy^2z^2 = 0$$

over finite fields of odd characteristic, because the automorphism groups of such quartics clearly contain the Klein group. We found pointless quartics of this form over $\mathbb{F}_q$ for q in

$$\{5, 7, 9, 11, 13, 17, 19, 23, 29\}.$$

q	curve
5	$x^4 + y^4 + z^4 = 0$
7	$x^4 + y^4 + 2z^4 + 3x^2z^2 + 3y^2z^2 = 0$
9	$x^4 - y^4 + a^2z^4 + x^2y^2 = 0$ where $a^2 - a - 1 = 0$
11	$x^4 + y^4 + z^4 + x^2y^2 + x^2z^2 + y^2z^2 = 0$
13	$x^4 + y^4 + 2z^4 = 0$
17	$x^4 + y^4 + 2z^4 + x^2y^2 = 0$
19	$x^4 + y^4 + z^4 + 7x^2y^2 - x^2z^2 - y^2z^2 = 0$
23	$x^4 + y^4 + z^4 + 10x^2y^2 - 3x^2z^2 - 3y^2z^2 = 0$
29	$x^4 + y^4 + z^4 = 0$

TABLE 2. Examples of pointless smooth plane quartics over $\mathbb{F}_q$ (with q odd) with automorphism group containing the Klein 4-group.

We present sample curves in Table 2.

Over $\mathbb{F}_3$ there are many pointless smooth plane quartics; for instance, the curve

$$x^4 + xyz^2 + y^4 + y^3z - yz^3 + z^4 = 0$$

has no points.

We know from the proof of Theorem 1.3 that there is at most one pointless genus-3 curve over $\mathbb{F}_{32}$, and its Jacobian is isomorphic to the cube of an elliptic curve whose endomorphism ring has discriminant -7. This suggests that we should look at twists of the reduction of the Klein quartic, and indeed we find that the curve

$$(x^2 + x)^2 + (x^2 + x)(y^2 + y) + (y^2 + y)^2 + 1 = 0$$

has no points over $\mathbb{F}_{32}$. (This fact is noted in [**3**, § 3.3].) For the other fields of characteristic 2, we find examples by modifying the example for $\mathbb{F}_{32}$. We list the results in Table 3.

We close this section by mentioning a related method of constructing pointless genus-3 curves. Suppose C is a genus-3 curve over a field of characteristic not 2, and suppose that C has a pair of commuting involutions (like the curves we considered in this section). Then either C is an unramified double cover of a genus-2 curve, or C is a genus-3 curve of the type considered in [**9**, § 4], that is, a genus-3 curve obtained by 'gluing' three elliptic curves together along portions of their 2-torsion. This suggests a more direct method of constructing genus-3 curves with no points: We can start with three elliptic curves with few points, and try to glue them together using the construction from [**9**, § 4]. This idea was used by the third author to construct genus-3 curves with many points [**20**].

q	curve
2	$(x^2+xz)^2+(x^2+xz)(y^2+yz)+(y^2+yz)^2+z^4=0$
4	$(x^2+xz)^2+a(x^2+xz)(y^2+yz)+(y^2+yz)^2+a^2z^4=0$ where $a^2+a+1=0$
8	$(x^2+xz)^2+(x^2+xz)(y^2+yz)+(y^2+yz)^2+a^3z^4=0$ where $a^3+a+1=0$
16	$(x^2+xz)^2+a(x^2+xz)(y^2+yz)+(y^2+yz)^2+a^7z^4=0$ where $a^4+a+1=0$
32	$(x^2+xz)^2+(x^2+xz)(y^2+yz)+(y^2+yz)^2+z^4=0$

TABLE 3. Examples of pointless smooth plane quartics over $\mathbb{F}_q$ (with q even) with automorphism group containing the Klein 4-group.

5. Examples of pointless curves of genus 4

We searched for pointless genus-4 curves by looking at hyperelliptic curves whose automorphism group contained the Klein 4-group; however, we found that for $q > 31$ no such curves exist. Since we need to find pointless genus-4 curves over $\mathbb{F}_q$ for every $q \leqslant 49$, we moved on to a different family of curves with commuting involutions.

Suppose q is an odd prime power and suppose f and g are separable cubic polynomials in $\mathbb{F}_q[x]$ with no factor in common. An easy ramification computation shows that then the curve defined by $y^2 = f$ and $z^2 = g$ has genus 4. Clearly the automorphism group of this curve contains a copy of the Klein 4-group. It is easy to check whether a curve of this form is pointless: For every value of x in $\mathbb{F}_q$, at least one of $f(x)$ and $g(x)$ must be a nonsquare, and exactly one of f and g should have a nonsquare as its coefficient of x^3. We found pointless curves of this form over every $\mathbb{F}_q$ with q odd and $q \leqslant 49$. Examples are given in Table 4.

We mention two points of interest about curves of this form. First, if the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q[x]$ spanned by the cubic polynomials f and g contains the constant polynomial 1, then the curve C defined by the two equations $y^2 = f$ and $z^2 = g$ is trigonal: If we have $af + bg = 1$, then $(x, y, z) \mapsto (y, z)$ defines a degree-3 map from C to the genus-0 curve $ay^2 + bz^2 = 1$. Second, if $q \equiv 1 \bmod 3$ and if the coefficients of x and x^2 in f and g are zero, then the curve C has even more automorphisms, given by multiplying x by a cube root of unity. (Likewise, if q is a power of 3 and if f and g are both of the form $a(x^3 - x) + b$, then $x \mapsto x + 1$ gives an automorphism of C.) When it was possible, we chose the examples in Table 4 to have these properties. In Table 5 we provide trigonal models for the curves in Table 4 that have them.

It remains for us to find examples of pointless genus-4 curves over $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$, and $\mathbb{F}_{32}$.

q	curve	
3	$y^2 = x^3 - x - 1$	$z^2 = -x^3 + x - 1$
5	$y^2 = x^3 - x + 2$	$z^2 = 2x^3 - 2x$
7	$y^2 = x^3 - 3$	$z^2 = 3x^3 - 1$
9	$y^2 = x^3 - x + 1$ where $a^2 - a - 1 = 0$	$z^2 = a(x^3 - x - 1)$
11	$y^2 = x^3 - x - 3$	$z^2 = 2x^3 - 2x - 5$
13	$y^2 = x^3 + 1$	$z^2 = 2x^3 - 5$
17	$y^2 = x^3 + x$	$z^2 = 3x^3 - 8x^2 - 3x + 5$
19	$y^2 = x^3 + 2$	$z^2 = 2x^3 + 1$
23	$y^2 = x^3 + x + 6$	$z^2 = 5x^3 + 9x^2 - 3x + 10$
25	$y^2 = x^3 + x + 1$ where $a^2 - a + 2 = 0$	$z^2 = a(x^3 + x^2 + 2)$
27	$y^2 = x^3 - x + a^5$ where $a^3 - a + 1 = 0$	$z^2 = -x^3 + x + a^5$
29	$y^2 = x^3 + x$	$z^2 = 2x^3 + 12x + 14$
31	$y^2 = x^3 - 10$	$z^2 = 3x^3 + 9$
37	$y^2 = x^3 + x + 4$	$z^2 = 2x^3 - 17x^2 + 5x + 15$
41	$y^2 = x^3 + x + 17$	$z^2 = 3x^3 - x^2 - 12x - 16$
43	$y^2 = x^3 - 9$	$z^2 = 2x^3 + 18$
47	$y^2 = x^3 + 5x - 12$	$z^2 = 5x^3 + 2x^2 + 19x - 9$
49	$y^2 = x^3 + 4$ where $a^2 - a + 3 = 0$	$z^2 = a(x^3 + 2)$

TABLE 4. Examples of pointless curves of genus 4 over $\mathbb{F}_q$ (with q odd) with automorphism group containing the Klein 4-group.

Let q be a power of 2. An easy argument shows that a genus-4 hyperelliptic curve over $\mathbb{F}_q$ provided with an action of the Klein group must have a rational Weierstraß point, and so will not be pointless. Thus we decided simply to enumerate the genus-4 hyperelliptic curves (with no rational Weierstraß points) over the remaining $\mathbb{F}_q$ and to check for pointless curves. We found pointless hyperelliptic curves over $\mathbb{F}_q$ for $q \in \{2, 4, 8, 16\}$; the examples we give in Table 6 are all twists over $\mathbb{F}_q$ of curves that can be defined over $\mathbb{F}_2$.

Our computer search also revealed that every genus-4 hyperelliptic curve over $\mathbb{F}_{32}$ has at least one rational point. So to find an example of a pointless genus-4 curve over $\mathbb{F}_{32}$, we decided to look for genus-4 double covers of elliptic curves E. Our heuristic

q	curve	involutions of $\mathbb{P}^1$	
3	$v^3 - v = (u^4+1)/(u^2+1)^2$	$u \mapsto -u$	$u \mapsto 1/u$
5	$v^3 - v = -2(u^2-2)^2/(u^2+2)^2$	$u \mapsto -u$	$u \mapsto 2/u$
7	$v^3 = 2u^6 + 2$	$u \mapsto -u$	$u \mapsto 1/u$
9	$v^3 - v = (u^4+a^2)/(u^2+a^5)^2$ where $a^2 - a - 1 = 0$	$u \mapsto -u$	$u \mapsto a/u$
11	$v^3 - v = (3u^4+4u^2+3)/(u^2+1)^2$	$u \mapsto -u$	$u \mapsto 1/u$
13	$v^3 = 4u^6 + 6$	$u \mapsto -u$	$u \mapsto 2/u$
19	$v^3 = 2u^6 + 2$	$u \mapsto -u$	$u \mapsto 1/u$
27	$v^3 - v = a^{18}(u^4+1)/(u^2+1)^2$ where $a^3 - a + 1 = 0$	$u \mapsto -u$	$u \mapsto 1/u$
31	$v^3 = 5u^6 - 11u^4 - 11u^2 + 5$	$u \mapsto -u$	$u \mapsto 1/u$
43	$v^3 = 7u^6 + 8u^4 + 8u^2 + 7$	$u \mapsto -u$	$u \mapsto 1/u$
49	$v^3 = 2u^6 + a$ where $a^2 - a + 3 = 0$	$u \mapsto -u$	$u \mapsto a^3/u$

TABLE 5. Trigonal forms for some of the curves in Table 4. The third and fourth columns give two involutions of $\mathbb{P}^1$ that lift to give commuting involutions of the curve.

q	curve
2	$y^2 + y = t + (x^4+x^3+x^2+x)/(x^5+x^2+1)$
4	$y^2 + y = t + (x^3+1)/(x^5+x^2+1)$
8	$y^2 + y = t + (x^4+x^3+x^2+x)/(x^5+x^2+1)$
16	$y^2 + y = t + (x^3+1)/(x^5+x^2+1)$

TABLE 6. Examples of pointless genus-4 hyperelliptic curves over $\mathbb{F}_q$ (with q even). On each line, the symbol t refers to an arbitrary element of $\mathbb{F}_q$ whose trace to $\mathbb{F}_2$ is equal to 1.

suggested that we might have good luck finding pointless curves if E had few points, but for the sake of completeness we examined every E over $\mathbb{F}_{32}$.

We found that up to isomorphism and Galois conjugacy there are exactly two pointless genus-4 curves over $\mathbb{F}_{32}$ that are double covers of elliptic curves. The first can be defined by the equations

$$y^2 + y = x + 1/x + 1$$
$$z^2 + z = \frac{a^7x^4 + a^{30}x^3y + a^{13}x^2 + x + a^{23}xy + a^6}{x^3 + a^{15}x^2 + x + a^{28}}$$

and the second by

$$y^2 + y = x + a^7/x$$
$$z^2 + z = \frac{a^4x^4 + a^7x^3y + a^3x^3 + a^{23}x^2y + a^{28}x^2 + a^{28}xy + a^{16}}{x^3 + a^{25}x^2 + a^{22}x + a^{25}},$$

where $a^5 + a^2 + 1 = 0$.

References

[1] R. Auer & J. Top – Some genus 3 curves with many points, in *Algorithmic Number Theory (Sydney, 2002)* (C. Fieker & D.R. Kohel, eds.), Lecture Notes in Comp. Sci., vol. 2369, Springer-Verlag, Berlin, 2002, p. 163–171.

[2] W. Bosma, J. Cannon & C. Playoust – The Magma algebra system. I. The user language, *J. Symb. Comput.* **24** (1997), p. 235–265.

[3] N.D. Elkies – The Klein quartic in number theory, in *The eightfold way* (S. Levy, ed.), Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, p. 51–101.

[4] G. van der Geer & M. van der Vlugt – Tables of curves with many points, *Math. Comp.* **69** (2000), p. 797–810, updates available at `http://www.science.uva.nl/~geer`.

[5] H. Hasse – Zur Theorie der abstrakten elliptischen Funktionkörper. I, II, III, *J. reine angew. Math.* **175** (1936), p. 55–62, 69–88, 193–208.

[6] G.-J. van der Heiden – Local-global problem for Drinfeld modules, *J. Number Theory* **104** (2004), p. 193–209.

[7] D.W. Hoffmann – On positive definite Hermitian forms, *Manuscripta Math.* **71** (1991), p. 399–429.

[8] E.W. Howe & K.E. Lauter – Improved upper bounds for the number of points on curves over finite fields, *Ann. Inst. Fourier (Grenoble)* **53** (2003), p. 1677–1737, arXiv: `math.NT/0207101`.

[9] E.W. Howe, F. Leprévost & B. Poonen – Large torsion subgroups of split Jacobians of curves of genus two or three, *Forum Math.* **12** (2000), p. 315–364.

[10] V. Kumar Murty & J. Scherk – Effective versions of the Chebotarev density theorem for function fields, *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), p. 523–528.

[11] K.E. Lauter – Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, *J. Algebraic Geom.* **10** (2001), p. 19–36, with an appendix by J.-P. Serre, arXiv: `math.AG/0104247`.

[12] ———, The maximum or minimum number of rational points on genus three curves over finite fields, *Compositio Math.* **134** (2002), p. 87–111, with an appendix by J.-P. Serre, arXiv: `math.AG/0104086`.

[13] D.B. Leep & C.C. Yeomans – Quintic forms over p-adic fields, *J. Number Theory* **57** (1996), p. 231–241.

[14] D. Maisner & E. Nart – Abelian surfaces over finite fields as Jacobians, *Experiment. Math.* **11** (2002), p. 321–337, with an appendix by E.W. Howe.

[15] A. Schiemann – Classification of Hermitian forms with the neighbour method, *J. Symb. Comput.* **26** (1998), p. 487–508.

[16] J.-P. Serre – Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris Sér. I Math.* **296** (1983), p. 397–402.

[17] ______, Rational points on curves over finite fields, unpublished notes by F.Q. Gouvêa of lectures at Harvard University, 1985.

[18] ______, *Cohomologie Galoisienne*, Lect. Notes in Math., vol. 5, Springer-Verlag, Berlin, 1994, cinquième édition, révisée et complétée.

[19] H.M. Stark – On the Riemann hypothesis in hyperelliptic function fields, in *Analytic number theory* (H.G. Diamond, ed.), Proc. Sympos. Pure Math., vol. 24, American Mathematical Society, Providence, R.I., 1973, p. 285–302.

[20] J. Top – Curves of genus 3 over small finite fields, *Indag. Math. (N. S.)* **14** (2003), p. 275–283.

E.W. Howe, Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967, USA • *E-mail :* `however@alumni.caltech.edu`
Url : `http://www.alumni.caltech.edu/~however/`

K.E. Lauter, Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
E-mail : `klauter@microsoft.com`

J. Top, Department of Mathematics, University of Groningen, P.O. Box 800, 9700 AV Groningen, The Netherlands • *E-mail :* `top@math.rug.nl`