Algebra & Number Theory

Volume 19
2025
No. 8

On the maximum gonality of a curve over a finite field

Xander Faber, Jon Grantham and Everett W. Howe

msp

ALGEBRA AND NUMBER THEORY 19:8 (2025)
https://doi.org/10.2140/ant.2025.19.1637

On the maximum gonality of a curve over a finite field

Xander Faber, Jon Grantham and Everett W. Howe

The gonality of a smooth geometrically connected curve over a field k is the smallest degree of a nonconstant k-morphism from the curve to the projective line. In general, the gonality of a curve of genus $g \geq 2$ is at most $2g-2$. Over finite fields, a result of F. K. Schmidt from the 1930s can be used to prove that the gonality is at most $g+1$. Via a mixture of geometry and computation, we improve this bound: for a curve of genus $g \geq 5$ over a finite field, the gonality is at most g. For genus $g = 3$ and $g = 4$, the same result holds with exactly 217 exceptions: there are two curves of genus 4 and gonality 5, and 215 curves of genus 3 and gonality 4. The genus-4 examples were found in other papers, and we reproduce their equations here; in supplementary material, we provide equations for the genus-3 examples.

1. Introduction

Throughout, we use the unqualified term "curve" to mean a smooth complete geometrically connected variety of dimension 1 over a field. Let $C_{/k}$ be a curve of genus g over a field k. The *gonality* of C is the minimum degree of a nonconstant k-morphism $f : C \to \mathbb{P}^1$. For the algebraically inclined reader, the function field $\kappa(C)$ contains infinitely many isomorphic copies of a rational function field $k(x)$, and the gonality of C is the minimum value of $[\kappa(C) : k(f)]$ as f varies over nonconstant functions on C. For the geometrically minded reader, the gonality is the minimum degree of an effective divisor D on C whose associated linear system has positive dimension. Taking D to be a canonical divisor, the Riemann–Roch theorem shows that the gonality of C is at most $2g-2$ for any curve C of genus $g \geq 2$. See [Poonen 2007, Appendix] for general results on gonality.

We are interested in bounding the gonality of curves over a finite field $\mathbb{F}_q$. We will restrict our attention to curves of genus $g \geq 3$ because the gonalities of curves of genus $g = 0, 1, 2$ are known to be 1, 2, 2, respectively. The gonality of a curve of genus $g \geq 3$ over a finite field is at most $g+1$ by a theorem of F. K. Schmidt from the 1930s [Tsfasman et al. 2007, Corollary 3.1.12], and it is at most g if the curve admits a rational point. See [Faber and Grantham 2022, Proposition 2.1] for proofs of both of these statements. For convenience, let us say that a curve of genus g over a finite field is *excessive* if it has gonality $g+1$. If $C_{/\mathbb{F}_q}$ is a curve of genus $g \geq 3$, and if $q > 4g^2$, then Weil's inequality implies C has a rational point. Consequently, for a given genus g, there are only finitely many pairs (g, q) for which an excessive curve could possibly exist. In fact, excessive curves are substantially rarer than this simple argument suggests.

MSC2020: primary 11G20, 14H51; secondary 14Q05.
Keywords: curves over finite fields, gonality.

© 2025 MSP (Mathematical Sciences Publishers). Distributed under the Creative Commons Attribution License 4.0 (CC BY).
Open Access made possible by subscribing institutions via Subscribe to Open.

Theorem 1.1. *Let q be a prime power.*

- *There exists an excessive curve of genus 3 over $\mathbb{F}_q$ if and only if $q \leq 23$ or $q = 29$ or $q = 32$.*
- *There exists an excessive curve of genus 4 over $\mathbb{F}_q$ if and only if $q = 2$ or $q = 3$.*
- *If C is a curve of genus $g \geq 5$ over $\mathbb{F}_q$, then its gonality is at most g.*

As there are only finitely many isomorphism classes of curves over $\mathbb{F}_q$ of genus g, the following consequence is immediate:

Corollary 1.2. *With finitely many exceptions (up to isomorphism), a curve over a finite field of genus $g \geq 2$ admits a complete linear system of positive dimension and degree at most g.* □

We wonder whether this corollary is best possible in the following sense:

Question 1.3. *Let $g \geq 2$ be an integer and q a prime power. Does there exist a curve of genus g and gonality g over $\mathbb{F}_q$?*

As every genus-2 curve is hyperelliptic, the answer is "yes" in that case. A curve with genus 3 and gonality 3 is nothing more than a smooth plane quartic with a rational point [Faber and Grantham 2022, Corollary 2.3], and these are easy to produce over any finite field. For $g = 4, 5$ and $q \leq 4$, the answer is "yes" by the main results of [Faber and Grantham 2022; 2023]. More generally, to answer the question for genus 4 and q odd, one could choose a nonsquare $c \in \mathbb{F}_q^\times$ and a cubic form $F \in \mathbb{F}_q[x, y, z, w]$ such that the curve

$$C_{/\mathbb{F}_q} : xy + z^2 - cw^2 = F(x, y, z, w) = 0$$

is nonsingular [Faber and Grantham 2022, Lemma 5.1]. As the space of such cubics is 19-dimensional, surely this holds for some choice of F. A similar heuristic approach using complete intersections of quadrics in $\mathbb{P}^4$ applies to the case of genus-5 curves [loc. cit., Lemma 6.6]. We are unsure what the answer should be for genus larger than 5.

The first two authors originally started this sequence of papers with the following question:

Question 1.4. *Does the zeta function of a curve over a finite field know the gonality of the curve?*

An equivalent formulation would be to ask if gonality is an isogeny class invariant.

The short answer to these two equivalent questions is "no". For example, consider the pair of curves over $\mathbb{Q}$

$$C_1 : x^4 + 4y^4 + 4z^4 + 20x^2y^2 - 8x^2z^2 + 16y^2z^2 = 0,$$
$$C_2 : 3v^2 = -17u^8 + 56u^7 - 84u^6 + 56u^5 - 70u^4 - 56u^3 - 84u^2 - 56u - 17.$$

The former is a smooth plane quartic, while the latter is a hyperelliptic curve of genus 3. In [Howe 2005], the third author showed that these curves have isomorphic Jacobians (as unpolarized varieties). As both of these models have good reduction for all $p > 3$, we obtain examples of curves with the same zeta function and distinct gonalities over $\mathbb{F}_p$ for all $p > 3$. See also [Howe 1996, Section 3] for an example over $\mathbb{F}_3$, and the isogeny class `3.2.ac_c_ac` from [LMFDB] for an example over $\mathbb{F}_2$.

In a sense, this example shows that classifying curves up to isogeny is orthogonal to classifying them by gonality. Nevertheless, we can leverage some information from the isogeny classification in order to learn about gonality. We now summarize the proof of Theorem 1.1. For genus-3 curves, the result follows almost immediately from work of Howe, Lauter, and Top [Howe et al. 2005] on pointless curves of small genus. For the remaining cases, our strategy is as follows:

(1) Use the Riemann–Roch theorem to show that a curve of genus g and gonality $g+1$ cannot have an effective divisor of degree $g-2$.

(2) Apply the Weil bound to rule out all but finitely many pairs (g, q) for which there could exist an excessive curve of genus g over $\mathbb{F}_q$.

(3) Apply a technique of Serre and Lauter to write down a finite list of isogeny classes of abelian varieties that contains the Jacobian of every excessive curve over $\mathbb{F}_q$. This limits us to the cases $g = 4, 5, 6, 7, 9$ and very few finite fields.

(4) For each $g < 9$, construct one or more search spaces of plane curves that contains a birational model of each excessive curve of genus g. Substantially reduce that search space using efficient C code, and then comb through the survivors using Magma.

(5) Rule out the single isogeny class with $g = 9$ using techniques from the third author's PhD thesis.

The first two steps will be performed in Section 2. We discuss the third step in Section 3. The fourth step requires slightly different techniques depending on the genus. The relevant computations for curves of genus at most 5 were performed in the earlier papers [Howe et al. 2005; Faber and Grantham 2022; 2023]; these will be summarized in Section 4. Curves of genus 6 and 7 will be treated in Sections 5 and 6, respectively. Finally, the argument to rule out genus 9 is presented in Section 7.

Remark 1.5. The work in Section 2 is sufficient to prove the qualitative result in Corollary 1.2. The results in Sections 3 and 4 allow us to limit our remaining efforts to looking through 83 isogeny classes of abelian varieties of dimensions 6, 7, and 9 for Jacobians whose associated curves are excessive. We did locate a few potential needles in this haystack: at least four of the isogeny classes in dimension 7 do contain Jacobians. However, we are able to show directly that none of the associated curves has gonality 8. With the exception of one class in dimension 6 and one class in dimension 9, our results do not rule out the presence of Jacobians in other isogeny classes.

Theorem 1.1 and its corollary show that there are only finitely many isomorphism classes of excessive curves. In principle, one should be able to write them all down. This was already carried out for curves of genus 4 in [Faber and Grantham 2023, Section 5]: there is exactly one such curve over $\mathbb{F}_2$ and one over $\mathbb{F}_3$. Defining equations can be found in [Faber and Grantham 2022, Theorem 5.4; 2023, Theorem 5.3], and are reproduced here in Section 8. To finish the story, we carried out an exhaustive search for excessive curves of genus 3. Every such curve arises as a pointless plane quartic. This search can be done for $q \le 5$ by brute force. For $7 \le q \le 23$, it was necessary to be more clever in order to cut the search space of plane quartics down to something manageable. For $q = 29$, we used isogeny class methods to show that

q	2	3	4	5	7	8	9	11	13	16	17	19	23	29	32
# of curves	4	8	21	31	32	39	27	21	11	8	7	2	2	1	1

Table 1. The number of isomorphism classes of excessive curves of genus 3 over $\mathbb{F}_q$.

any such curve must be a double cover of an elliptic curve, which gives another method of searching. And for $q = 32$, we used existing literature. The number of isomorphism classes of excessive curves of genus 3 over each finite field is given in Table 1. Our methods for finding all such curves are described in greater detail in Section 8.

We close this introduction with a comment on terminology and a remark about the software and computational resources used in this work. We view a curve C as a scheme over a base field k, and by a "point" of C we generally mean a *closed point*—that is, a morphism from Spec K to C, for some finite extension K of k. A closed point of degree d is a closed point where K is a degree-d extension, a rational point is a closed point of degree 1, and a quadratic (or cubic, etc.) point is a closed point of degree 2 (or 3, etc.). On the other hand, when we refer to a K-rational point on C for some extension K of k, we mean a rational point on the base extension of C to K.

We wrote our implementation of Lauter's algorithm in [SageMath]. The large searches for plane curves with special vanishing properties were written in C. Our C code benefited from the use of the finite field library in Flint [Hart et al. 2020] as well as a number of bit-level optimizations suggested by [Warren 2002, Chapter 2]. The genus, point counts, and gonality of the survivors of those searches were computed in Magma [Bosma et al. 1997]. Most computations were performed on a cluster of Intel Xeon E5-2699v3 CPUs running at 2.3 GHz at the Center for Computing Sciences in Bowie, MD; some Magma computations related to enumerating excessive curves of genus 3 were performed on an Apple M1 Max running at 3.2 GHz at the third author's home in San Diego, CA. The programs we used are available at https://github.com/RationalPoint/excessive.

2. Implications of the Weil bound

Our goal in this section is to apply the Weil bound to show that there are only finitely many pairs (g, q) for which a curve $C_{/\mathbb{F}_q}$ of genus g and gonality $g+1$ could exist.

Lemma 2.1. *Let C be a curve of genus $g \geq 3$ over $\mathbb{F}_q$. Then C admits a morphism to $\mathbb{P}^1$ of degree g if and only if it has an effective divisor of degree $g-2$.*

Proof. If D is any divisor of degree g, the Riemann–Roch theorem asserts that

$$\dim |K - D| = \dim |D| + \deg(K - D) + 1 - g = \dim |D| - 1.$$

Hence, the linear system $|K - D|$ contains an effective divisor of degree $g-2$ if and only if $\dim |D| > 0$. The latter condition holds for some degree-g divisor D if and only if C admits a morphism to $\mathbb{P}^1$ of degree g. □

Suppose now that $C_{/\mathbb{F}_q}$ is a curve of genus g and gonality $g+1$. Then C does not admit a morphism to $\mathbb{P}^1$ of degree g. By the previous lemma, C has no effective divisor of degree $g-2$. In particular, this means $C(\mathbb{F}_{q^{g-2}}) = \varnothing$. Weil's inequality tells us that

$$\#C(\mathbb{F}_{q^r}) \geq q^r + 1 - 2gq^{r/2} \quad (r \geq 1).$$

It follows that C has an $\mathbb{F}_{q^r}$-rational point if $q^r \geq 2gq^{r/2}$, or equivalently, if $q \geq (2g)^{2/r}$. Applying this with $r = g-2$, we conclude that

$$q < (2g)^{2/(g-2)}.$$

Define $f(g)$ to be the function on the right in the preceding inequality. Then f is decreasing for $g \geq 3$, and $f(11) < 2$. It follows that there is no curve of genus g and gonality $g+1$ if $g > 10$. For $7 \leq g \leq 10$, we find that $f(g) < 3$. Finally, $f(3) = 36$, $f(4) = 8$, $f(5) \approx 4.64$, and $f(6) \approx 3.46$. The following proposition summarizes these findings.

Proposition 2.2. *If there exists an excessive curve of genus g over $\mathbb{F}_q$, then one of the following is true*:

- $g = 3$ *and* $q \leq 32$.
- $g = 4$ *and* $q \leq 7$.
- $g = 5$ *and* $q \leq 4$.
- $g = 6$ *and* $q = 2$ *or* 3.
- $7 \leq g \leq 10$ *and* $q = 2$. □

3. Implications of Lauter's algorithm

Following an idea of Robinson [1964] that was used by Serre [2020, VII.2] in the context of curves over finite fields, Lauter [2000] gave an algorithm for writing down all zeta functions of hypothetical curves with a specified large number of points. The magic is that "large" is irrelevant to the method, and rather, one is actually specifying zeta functions of curves with *given* number of rational points. We capitalize on this method by adding constraints on the number of points of higher degree.

Let $C_{/\mathbb{F}_q}$ be a curve of genus $g \geq 2$ over the finite field $\mathbb{F}_q$. Write a_d for the number of closed points of degree d on the curve C. An inclusion-exclusion argument relates a_d to the number of points on C of a particular degree:

$$\#C(\mathbb{F}_{q^r}) = \sum_{d \mid r} d a_d \quad \Longleftrightarrow \quad a_d = \frac{1}{d} \sum_{r \mid d} \mu\left(\frac{d}{r}\right) \#C(\mathbb{F}_{q^r}).$$

Proposition 3.1. *Suppose that C is an excessive curve of genus g over $\mathbb{F}_q$. Write a_d for the number of closed points of degree d on C. Then the conditions in Table 2 must hold.*

Proof. The argument in all cases is similar, so we describe the case $g = 7$ by way of example. If C is excessive, then it has gonality 8. In particular, it does not admit a morphism to $\mathbb{P}^1$ of degree 7, and so

g	vanishing conditions
3	$a_1 = 0$
4	$a_1 = a_2 = 0$
5	$a_1 = a_3 = 0$
6	$a_1 = a_2 = a_4 = 0$
7	$a_1 = a_5 = a_2 a_3 = 0$
8	$a_1 = a_2 = a_3 = a_6 = 0$
9	$a_1 = a_7 = a_2 a_3 = a_2 a_5 = a_3 a_4 = 0$
10	$a_1 = a_2 = a_4 = a_8 = a_3 a_5 = 0$

Table 2. Conditions for Proposition 3.1.

Lemma 2.1 implies that C does not admit an effective divisor of degree 5. If C has a rational point P, then $5P$ is just such an effective divisor. Hence, $a_1 = 0$.

In what remains, if P is a point of $C(\mathbb{F}_{q^d})$, we write $\overline{P}$ for the effective divisor of degree d with simple support on the Galois orbit of P. Now if C has a point P of degree 5, then the divisor $\overline{P}$ is effective of degree 5. Hence, $a_5 = 0$. If C admits a quadratic point P and a cubic point Q, then the divisor $\overline{P} + \overline{Q}$ is effective of degree 5. Hence $a_2 a_3 = 0$. □

The zeta function of a genus-g curve $C_{/\mathbb{F}_q}$ is of the form $P(T)/((1-T)(1-qT))$, where $P \in \mathbb{Z}[T]$ is a polynomial of degree $2g$. The *Weil polynomial* of C is the polynomial $f := T^{2g} P(1/T)$. The Weil polynomial is a monic polynomial in $\mathbb{Z}[T]$ whose roots in the complex numbers all lie on the circle of radius $\sqrt{q}$, and whose real roots (if any) have even multiplicity. The Weil polynomial of C is determined by the numbers $a_1, \ldots, a_g$. The *real Weil polynomial* of C is the unique polynomial $h \in \mathbb{Z}[T]$ such that $f(T) = T^g h(T + q/T)$. It is monic of degree g, all of its complex roots are real numbers in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, and it is also determined by $a_1, \ldots, a_g$. Lauter's algorithm takes constraints on the $a_1, \ldots, a_g$ and returns real Weil polynomials for hypothetical curves satisfying those constraints. Using the vanishing conditions from Proposition 3.1 and a Sage implementation of Lauter's algorithm, we arrived at the following result.

Theorem 3.2. *The following are true*:

- *There is no excessive curve of genus* 4 *over* $\mathbb{F}_5$ *or* $\mathbb{F}_7$.
- *If there is an excessive curve of genus* 6 *over* $\mathbb{F}_2$, *then its real Weil polynomial is among the following*:

$$(T-2)(T+1)(T^2-2T-2)(T^2-8),$$
$$(T^2-8)(T^4-3T^3-2T^2+7T+1),$$
$$(T^2-8)(T^4-3T^3-2T^2+8T-2).$$

- *There is no excessive curve of genus* 6 *over* $\mathbb{F}_3$.

- *If there is an excessive curve of genus* 7 *over* $\mathbb{F}_2$, *then its real Weil polynomial is among the* 79 *options given in the table in Appendix C.*
- *There is no excessive curve of genus* 8 *over* $\mathbb{F}_2$.
- *If there is an excessive curve of genus* 9 *over* $\mathbb{F}_2$, *then its real Weil polynomial is*

$$(T+1)(T^4-2T^3-6T^2+10T+1)^2.$$

- *There is no excessive curve of genus* 10 *over* $\mathbb{F}_2$. □

4. Curves of genus 3, 4, 5

Proposition 2.2 and Theorem 3.2 whittled down the list of fields $\mathbb{F}_q$ for which there could exist an excessive curve of genus 3, 4, or 5, as the following table shows:

g	surviving q
3	$q \le 32$
4	$q \le 4$
5	$q \le 4$

The existing literature is sufficient to finish off our description.

Consider curves of genus 3 first. We claim that such a curve is excessive if and only if it can be realized as a smooth plane quartic with no rational point. For the forward implication, we observe that an excessive curve has gonality 4 and no rational point. In particular, it is not hyperelliptic, so its canonical embedding is a smooth plane quartic. For the reverse, we note that a smooth plane quartic curve is canonically embedded and hence not hyperelliptic. Moreover, if its gonality were 3, then Lemma 2.1 asserts that it would have a rational point. We now appeal to a result of Howe, Lauter, and Top [Howe et al. 2005]:

Theorem 4.1. *There exists a pointless smooth plane quartic over* $\mathbb{F}_q$ *if and only if* $q \le 23$ *or* $q = 29$ *or* $q = 32$. □

The remaining cases of curves of genus 4 and 5 were handled by the authors in [Faber and Grantham 2022; 2023]:

Theorem 4.2. *There exists a curve of genus* 4 *and gonality* 5 *over* $\mathbb{F}_q$ *if and only if* $q \le 3$. □

Theorem 4.3. *There does not exist a curve of genus* 5 *and gonality* 6 *over* $\mathbb{F}_q$ *for any* q. □

5. Curves of genus 6

Our goal for this section is to prove the following result:

Theorem 5.1. *There does not exist a curve of genus* 6 *and gonality* 7 *over* $\mathbb{F}_2$.

Theorem 3.2 showed that if such a curve exists, then its real Weil polynomial must be among the following options:

factored real Weil polynomial	a_1	a_2	a_3	a_4	a_5	a_6
$(T-2)(T+1)(T^2-2T-2)(T^2-8)$	0	0	0	0	12	4
$(T^2-8)(T^4-3T^3-2T^2+7T+1)$	0	0	1	0	8	3
$(T^2-8)(T^4-3T^3-2T^2+8T-2)$	0	0	2	0	4	1

We treat the first case using off-the-shelf technology:

Proposition 5.2. *There is no curve of genus* 6 *over* $\mathbb{F}_2$ *with* $a_1 = a_2 = a_3 = a_4 = 0$.

Proof. Suppose otherwise, and let C be such a curve. Our application of Lauter's algorithm implies that the Jacobian of C has real Weil polynomial

$$f(T) = (T-2)(T+1)(T^2-2T-2)(T^2-8).$$

Write $g_1(T) = (T-2)(T+1)(T^2-8)$ and $g_2(T) = T^2-2T-2$. Then $f = g_1 g_2$, and the Jacobian of C is isogenous to the product of abelian varieties A_1, A_2 with real Weil polynomials g_1, g_2, respectively. By [Howe and Lauter 2012, Proposition 2.8, p. 178], the "gluing exponent" of A_1 and A_2 divides 2, so by [loc. cit., Theorem 2.2, p. 176] there is a double cover $C \to D$ for some curve D whose Jacobian is isogenous to A_1 or A_2, and whose real Weil polynomial is therefore g_1 or g_2. A curve with either of these real Weil polynomials has a rational point, which would imply that C has either a rational or a quadratic point. This contradiction completes the proof. □

For the two remaining real Weil polynomials, we make the following critical observation: if such a curve exists, it must have a cubic point.

Proposition 5.3. *Suppose there exists an excessive curve* $C_{/\mathbb{F}_2}$ *of genus* 6. *Then* C *admits a singular plane model of degree* 7. *Moreover, this model does not pass through a rational point of the plane.*

Proof. The above discussion shows that if there exists an excessive curve of genus 6 over $\mathbb{F}_2$, then it must have a cubic point. Let D be the effective divisor of degree 3 that is simply supported on the Galois orbit of such a point. Write K for a canonical divisor on C. Then $\deg(K-D) = 7$, and we aim to show that the linear system $|K-D|$ determines the plane model we seek.

Riemann–Roch shows that

$$\dim |K-D| = \dim |D| + 2.$$

If $\dim |D| > 0$, then $|D|$ is a g^1_3, which would mean C has gonality at most 3, a contradiction. Thus $\dim |D| = 0$ and $\dim |K-D| = 2$.

We now show that $|K-D|$ is basepoint free. Since $K-D$ is defined over $\mathbb{F}_2$, so is the base locus. Write $E \geq 0$ for the base divisor. By definition, we have $\dim |K-D-E| = 2$. We also know that

$$\deg(K-D-E) = 7 - \deg(E).$$

If $\deg(E) > 0$, then a nonzero function in the Riemann–Roch space $L(K-D-E)$ gives a morphism to $\mathbb{P}^1$ of degree strictly smaller than 7, which contradicts the fact that C is excessive. Thus $\deg(E) = 0$ and $E = 0$.

Let $\varphi : C \to \mathbb{P}^2$ be the morphism induced by the linear system $|K - D|$, and let C' be its image. Note that

$$\deg(K - D) = 7 = \deg(C \to C') \deg(C').$$

Since $|K - D|$ has dimension 2, the curve C' cannot be a line. Hence $\deg(C') = 7$, and C' is birational to C.

It remains to show that C' does not pass through a rational point of the plane. Suppose otherwise, and let $P \in \mathbb{P}^2(\mathbb{F}_2)$ be such a point. Then we can project through P to get a morphism $C' \to \mathbb{P}^1$ of degree at most 6. But then the composition $C \to C' \to \mathbb{P}^1$ has degree strictly smaller than 7. This contradiction completes the proof. □

The proposition allows us to construct a search space for excessive curves of genus 6. The space of homogeneous septic polynomials has dimension $\binom{7+2}{2} = 36$. We may insist that our polynomials do not vanish at a rational point of the plane. Ordinarily, this is an open condition on the space. But "not vanishing" is a closed condition on an $\mathbb{F}_2$-vector space, so we are able to leverage this information to cut the space down by seven additional dimensions. We now describe how to do this in practice.

Suppose F is a homogeneous septic polynomial over $\mathbb{F}_2$ in x, y, z, and let C' be the plane curve it cuts out. We find that

$$F \text{ includes the monomials } x^7, y^7, \text{ and } z^7.$$

Indeed, if x^7 is not present, then the point $[1:0:0]$ lies on the curve C'. A similar argument applies to $[0:1:0]$ and $[0:0:1]$. Now we can write

$$F = x^7 + y^7 + z^7 + xyF_1(x, y) + xzF_2(x, z) + yzF_3(y, z) + xyzG(x, y, z),$$

where

- F_1, F_2, F_3 are bivariate homogeneous polynomials of degree 5, and
- G is homogeneous in three variables of degree 4.

In order that $F(1, 1, 0) \neq 0$, we see that F_1 must have an odd number of nonzero coefficients. Half of all bivariate polynomials have this property, so there are 2^5 choices for F_1. A similar count applies to F_2 and F_3 since F cannot vanish at $[1:0:1]$ or $[0:1:1]$. Assuming we have chosen such polynomials for the F_i, we find that in order that $F(1, 1, 1) \neq 0$, G must have an odd number of nonzero coefficients. The space of polynomials of degree 4 has dimension $\binom{4+2}{2} = 15$, so there are 2^{14} choices for G. It follows that there are 2^{29} choices for F that do not vanish at a rational point of $\mathbb{P}^2_{\mathbb{F}_2}$.

We may now perform a search over all polynomials F satisfying the above constraints. We reject any polynomial F that satisfies one of the following additional properties:

- F vanishes at a point $P \in \mathbb{P}^2(\mathbb{F}_{16})$ and some partial derivative of F does not vanish at P.
- F does not vanish at either of $[0:1:t]$ or $[1:t:t^2]$, where $t^3 + t + 1 = 0$.

The first property asserts that there is a smooth quadratic or quartic point P on $C' = \{F = 0\}$. If that were to occur, then the normalization C would have a quadratic or quartic point, in violation of Proposition 3.1. We know that a hypothetical excessive curve of genus 6 over $\mathbb{F}_2$ must have a cubic point. Pushing that point down to the plane model C' would give a cubic point or a rational point. We have already ruled out the possibility of the latter. The group $\mathrm{PGL}_3(\mathbb{F}_2)$ acts on $\mathbb{P}^2$. There are two orbits of cubic points: one contains $[0:1:t]$ and the other contains $[1:t:t^2]$. So we may insist that our curve contains at least one of these points, which justifies the second property above.

We wrote C code to execute our search for homogeneous polynomials of degree 7 satisfying the above constraints. The search required about 2 minutes on a single CPU, and it found 110,770 polynomials. We passed these polynomials through a Magma script that looked for irreducible plane curves of genus 6 with no point of degree 1, 2, or 4. This took around 3 minutes. No curve survived.

The results of this search, combined with Proposition 5.2, provide a proof of Theorem 5.1.

6. Curves of genus 7

We apply the same strategy as in the previous section, but there is one annoying wrinkle to be ironed out. If C is an excessive curve of genus 7 with an effective divisor of degree 4, then C can be realized as a singular plane curve of degree 8. We treat this case in Section 6.1. Looking at the table in Appendix C, we find that all but three of the real Weil polynomials have $a_2 > 0$ or $a_4 > 0$. The exceptions — entries 3, 4, and 6 — cannot support an effective divisor of degree 4. However, each of the exceptions has $a_3 > 0$. An excessive curve of genus 7 with an effective divisor of degree 3 can be realized as a singular plane curve of degree 9. That case will be handled in Section 6.2.

Combining Theorems 6.3 and 6.6 below, we will obtain the desired result:

Theorem 6.1. *There is no curve of genus 7 and gonality 8 over $\mathbb{F}_2$.*

6.1. *An effective divisor of degree 4.*

We begin with some geometry.

Proposition 6.2. *Suppose there exists an excessive curve $C_{/\mathbb{F}_2}$ of genus 7 with an effective divisor of degree 4. Then C admits a singular plane model of degree 8. Moreover, this model does not pass through a rational point of the plane.*

Proof. Let K be a canonical divisor on C and D an effective divisor of degree 4. An argument virtually identical to the one used to prove Proposition 5.3 applies to show that the linear system $|K-D|$ is basepoint free of degree 8 and dimension 2. If we write C' for the image of C under the morphism $C \to \mathbb{P}^2$ determined by $|K-D|$, then we find that

$$\deg(K-D) = 8 = \deg(C \to C')\deg(C').$$

We must argue that $\deg(C') = 8$.

Since $\dim|K-D| = 2$, we find that $\deg(C') > 1$. Write $f : C \to \widetilde{C}'$ for the induced morphism from C to the normalization $\widetilde{C}'$ of C'. If the degree of C' were 2, then $C' = \widetilde{C}'$ would be a smooth rational curve and the morphism f would have degree 4. But the gonality of C is 8, so this cannot occur. If instead the degree of C' were 4, then $\deg(f) = 2$. Writing g' for the genus of $\widetilde{C}'$, we see that $g' \le (4-1)(4-2)/2 = 3$. If $g' \le 2$, then the gonality of $\widetilde{C}'$ is at most 2 [Faber and Grantham 2022, Proposition 2.1]. It would

curve equation	real Weil polynomial	a_1	a_2	a_3
$0 = x^4 + xy^3 + y^4 + xyz^2 + xz^3 + yz^3 + z^4$	$(T-2)(T^2-T-5)$	0	1	1
$0 = x^4 + xy^3 + y^4 + x^2z^2 + xyz^2 + yz^3 + z^4$	$(T-2)(T^2-T-4)$	0	2	2
$0 = x^4 + xy^3 + y^4 + x^3z + xyz^2 + yz^3 + z^4$	$T^3-3T^2-4T+13$	0	0	1
$0 = x^4 + x^2y^2 + y^4 + x^2yz + xy^2z + x^2z^2 + xyz^2 + y^2z^2 + z^4$	$(T-1)^3$	0	7	8

Table 3. The four isomorphism classes of pointless smooth plane quartic curves over $\mathbb{F}_2$, along with their real Weil polynomial and numbers of closed points.

then follow that C has gonality at most $2\deg(f) = 4$, a contradiction. Therefore, $g' = 3$ and $C' = \widetilde{C}'$ is a smooth plane quartic. If C' has a rational point, then it has gonality 3 [Faber and Grantham 2022, Corollary 2.3]. Again we arrive at a contradiction because the gonality of C would be at most $2 \cdot 3 = 6$. Thus $C'(\mathbb{F}_2) = \varnothing$.

To summarize, we are now assuming that C' is a smooth plane quartic with no rational point, and $f : C \to C'$ has degree 2. A direct computer search shows that there are four isomorphism classes of smooth pointless plane quartics over $\mathbb{F}_2$. Table 3 gives representative equations for these four classes, their number of points over $\mathbb{F}_2$, $\mathbb{F}_4$, and $\mathbb{F}_8$, and their real Weil polynomials. By a result of Tate [1966, Theorem 1(b)], the real Weil polynomial for $\widetilde{C}'$ divides that of C. Looking through all of the entries in Appendix C, we find that none of those polynomials is divisible by any of the polynomials in Table 3. We conclude that C' cannot have degree 4.

Thus, we have shown that C' has degree 8, and the morphism $C \to C'$ is birational. To complete the proof, we note that C' cannot pass through a rational point; otherwise, we could project through that point to get a morphism $C \to C' \to \mathbb{P}^1$ of degree strictly smaller than 8. □

We now spell out the differences between the genus-6 search and the related genus-7 search. Octic homogeneous polynomials that do not vanish at any of the rational points of the plane have the form

$$F = x^8 + y^8 + z^8 + xyF_1(x, y) + xzF_2(x, z) + yzF_3(y, z) + xyzG(x, y, z),$$

where

- F_1, F_2, F_3 are bivariate homogeneous polynomials of degree 6,
- G is homogeneous in three variables of degree 5, and
- the F_i and G each has an odd number of nonzero coefficients.

There are 2^{38} polynomials satisfying these constraints. We loop over all such polynomials and *reject* any that satisfies one of the following additional properties:

- F vanishes at a point $P \in \mathbb{P}^2(\mathbb{F}_{2^5})$ and some partial derivative of F does not vanish at P.
- F does not vanish at any of the points $[0:1:s]$, $[1:s:s^2]$, or $[0:1:s^2+s]$, where $s^4+s+1=0$.

The first property asserts that the plane model C' has a smooth quintic point, which would mean C has a smooth quintic point, a contradiction. By hypothesis, we know C has an effective divisor of degree 4, and hence a quadratic or quartic point. It follows that C' must pass through such a point. (Note that the image of a quartic point may be a quadratic point on C'.) There are two $\mathrm{PGL}_3(\mathbb{F}_2)$-orbits of quartic points and one orbit of quadratic points; representatives are $[0:1:s]$, $[1:s:s^2]$, and $[0:1:s^2+s]$, where $s^4+s+1=0$.

We divided the space of 2^{38} such polynomials into 64 tiles and distributed the search to 64 CPUs. The entire search required about 70 minutes of wall time. Each tile generated around 2.2 million polynomials for further investigation. We ran 64 instances of our Magma script, one for each tile; these required between 3 and 4 hours to complete. Out of the entire pool of approximately 140 million polynomials, only 606 describe irreducible genus-7 curves that have no quintic point and that do not simultaneously have a quadratic and a cubic point. More precisely, we found

- 248 curves with a_d-sequence (0, 2, 0, 3, 0, 3, 12), and
- 358 curves with a_d-sequence (0, 2, 0, 6, 0, 4, 16).

Each of these curves has gonality 4. We determined this by searching for divisors D of degree 2 or 4 with $\dim|D| > 0$; such a divisor must be a linear combination of Galois orbits of quadratic or quartic points. We used Magma to verify the existence of these divisors and to compute the dimension of the relevant Riemann–Roch spaces. We summarize our findings thus far:

Theorem 6.3. *If there is an excessive curve of genus* 7 *over* $\mathbb{F}_2$, *then its real Weil polynomial is one of the following options from the table in Appendix C*:

no.	*factored real Weil polynomial*	a_1	a_2	a_3	a_4	a_5	a_6	a_7
3	$T(T^6-3T^5-12T^4+39T^3+27T^2-126T+57)$	0	0	3	0	0	13	9
4	$T^7-3T^6-12T^5+40T^4+24T^3-132T^2+75T+1$	0	0	4	0	0	9	10
6	$(T^3-T^2-7T+6)(T^4-2T^3-7T^2+14T-2)$	0	0	5	0	0	9	12

6.2. ***An effective divisor of degree 3.*** Again, we begin with some geometry.

Proposition 6.4. *Suppose there exists an excessive curve* $C_{/\mathbb{F}_2}$ *of genus* 7 *with an effective divisor of degree* 3. *Then* C *admits a singular plane model of degree* 9. *Moreover, this model does not pass through a rational point of the plane.*

Proof. Let D be an effective divisor of degree 3 and let K be a canonical divisor. Then $\dim|K-D| \geq \dim|K|-3=3$. If this dimension were larger than 3, we would have

$$\dim|K-2D| \geq \dim|K-D| - \deg(D) \geq 1,$$

which means C admits a nonconstant morphism to $\mathbb{P}^1$ of degree $\deg(K-2D)=6$, a contradiction. We conclude that $|K-D|$ has degree 9 and dimension 3.

Now we argue that $|K-D|$ is basepoint free. Let $E \geq 0$ be its base divisor. Then $\dim|K-D-E|=3$ and $\deg(K-D-E)=9-\deg(E)$. If $\deg(E)\geq 2$, then $L(K-D-E)$ contains a nonconstant rational function of degree at most 7, a contradiction. If $\deg(E) = 1$, then E is supported at a rational point, which an excessive curve cannot have. Thus, $E = 0$.

The linear system $|K - D|$ determines a morphism $C \to \mathbb{P}^3$. Composing this with projection through a rational point of $\mathbb{P}^3$ (which does not lie on C), we obtain a morphism to $\mathbb{P}^2$. Write C' for the image in the plane. Then

$$\deg(K - D) = 9 = \deg(C \to C')\deg(C').$$

The curve C' does not lie in a line, so its degree is bigger than 1. If $\deg(C') = 3$, then C' has genus 0 or 1, and so gonality at most 2. But then $\deg(C \to C') = 3$, and composing $C \to C'$ with a morphism to $\mathbb{P}^1$ of minimum degree would show that C has gonality at most 6, a contradiction. So C' has degree 9, as desired.

Finally, suppose that C' passes through a rational point P of the plane. Since C has no rational point, and since $C \to C'$ is the normalization morphism, we see that P cannot be smooth. Suppose that P has multiplicity $r \geq 2$ on C'. Then linear projection through P gives rise to a morphism $C \to \mathbb{P}^1$ of degree $9 - r \leq 7$, which contradicts the fact that C has gonality 8. We conclude that C' cannot pass through a rational point. □

Following the proposition, our first attempt might be to search through plane curves defined by homogeneous polynomials of degree 9. The space of such polynomials has $\mathbb{F}_2$-dimension $\binom{9+2}{2} = 55$. As in the case of degree-6 curves, we can avoid looking at polynomials that vanish at a rational point of the plane, which cuts the space down to 2^{48} polynomials. This is much too large to be efficiently searched, so we need an additional improvement. We will leverage the fact that curves in the three remaining isogeny classes have at least three cubic points.

Proposition 6.5. *Suppose there exists an excessive curve $C_{/\mathbb{F}_2}$ of genus* 7 *with at least three distinct closed points of degree* 3. *Write $\mathbb{F}_8 = \mathbb{F}_2(t)$, where $t^3 + t + 1 = 0$. Then C is birational to a plane curve of degree* 9 *that passes through no rational point of the plane, and that satisfies at least one of the following*:

- *C has a triple point at* $[0:1:t]$.
- *C has a double point at* $[0:1:t]$ *and passes through* $[0:1:t+1]$.
- *C passes through* $[0:1:t]$ *and* $[1:0:t]$.

Proof. By hypothesis, C has three effective divisors D_1, D_2, D_3 of degree 3 with pairwise disjoint support. Let K be an effective canonical divisor. The proof of Proposition 6.4 shows that $\dim|K - D_1| = 3$. For $j = 1, 2, 3$, we also see that

$$\dim|K - D_1 - D_j| = 0,$$

since otherwise this linear system would give a morphism to $\mathbb{P}^1$ of degree 6. It follows that there are unique effective divisors E_1, E_2, E_3 of degree 6 such that

$$K - D_1 \sim D_1 + E_1 \sim D_2 + E_2 \sim D_3 + E_3.$$

Let $f_1, f_2, f_3 \in L(K - D_1)$ be rational functions corresponding to these three linear relations; the f_i are unique up to a constant.

Suppose first that the f_i generate a subspace of $L(K - D_1)$ of dimension 1. Then there is a single function f on C with

$$\operatorname{div}(f) = 2D_1 + E_1 - K = D_1 + D_2 + E_2 - K = D_1 + D_3 + E_3 - K.$$

Since the D_i have disjoint support, we see that $\operatorname{div}(f) = 2D_1 + D_2 + D_3 - K$. Using f as one of the coordinate functions for our map $C \to \mathbb{P}^2$, we see that there is a line $\ell \subset \mathbb{P}^2$ that passes through the images of D_1, D_2, and D_3. Let C' be the image of C in $\mathbb{P}^2$, and let P_1, P_2, P_3 be the images of the cubic points in C' corresponding to D_1, D_2, D_3, respectively. None of the P_i is rational since C' cannot pass through a rational point of the plane. Moreover, the P_i cannot all be distinct, for otherwise the line ℓ would contain three distinct cubic closed points. (An $\mathbb{F}_2$-rational line contains three rational points and two cubic closed points.) Thus, either C' has a triple point at P_1, or C' has a double point at P_1 and a second cubic point on the line ℓ. Since $\mathrm{PGL}_3(\mathbb{F}_2)$ acts transitively on the set of 14 cubic closed points of the plane that lie on some $\mathbb{F}_2$-rational line, we may assume without loss that we are in one of the first two cases of the proposition.

Now suppose that the f_i generate a subspace of $L(K - D_1)$ of dimension at least 2. We use two linearly independent f_i as coordinate functions for our map $C \to \mathbb{P}^2$. Keeping the notation of the previous paragraph, it follows there are distinct lines ℓ_1 and ℓ_2 containing cubic points P_1 and P_2 of C'. After applying a linear transformation of the plane, we may assume that our lines are $\ell_1 = \{x = 0\}$ and $\ell_2 = \{y = 0\}$. The subgroup of $\mathrm{PGL}_3(\mathbb{F}_2)$ that fixes these two lines is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ * & * & 1 \end{pmatrix} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

One can verify directly that this group acts faithfully on the set of four cubic closed points on $\ell_1 \cup \ell_2$. It follows that there is some transformation mapping P_1 to the Galois orbit of $[0:1:t]$ and P_2 to the Galois orbit of $[1:0:t]$. □

The preceding proposition allows us to restrict our attention to homogeneous polynomials of degree 9 over $\mathbb{F}_2$ with certain extra vanishing conditions. In each of the three cases, we obtain a number of linear constraints on the coefficients of our polynomials: 18, 12, and 6, respectively. Starting with a space of dimension 55, this means we have three search spaces to consider, consisting of 2^{37}, 2^{43}, and 2^{49} polynomials, respectively. Using linear algebra, we can produce three explicit bases for the spaces of polynomials with these vanishing conditions. Unlike the basis of monomials used in Section 6.1, a naive choice of new basis may not be well conditioned for efficiently searching for polynomials that do not vanish at a rational point. For completeness, we write down explicit bases of polynomials that *are* well conditioned in Appendix A and argue that they have the properties we want. In the first two cases, avoiding polynomials that vanish at a rational point cuts five dimensions off the search space; in the third

case	CPUs	C search time	survivors	Magma search time	survivors
1	1	37m	162,552	43m	24
2	64	54m	5,314,648	28m	0
3	64	11h 45m	75,877,946	1h 44m	40

Table 4. Search resources and wall time for the three cases of Proposition 6.5.

case it cuts seven dimensions off the search space. In summary, this means we will have three searches consisting of 2^{32}, 2^{38}, and 2^{42} polynomials, respectively.

Table 4 describes the search resources, wall time, and number of survivors for the three searches we performed, one for each case of Proposition 6.5. As expected, the C search times for Cases 2 and 3 are approximately 64 times and 1024 times that of Case 1, respectively. For Case 1, the 24 curves that survived the Magma search were equally split between the first and third isogeny classes of Theorem 6.3. For Case 3, twelve of the curves that survived fell into the first isogeny class of Theorem 6.3, while the remainder fell into the third isogeny class of the theorem. Using Magma, we verified that all 64 of the survivors have gonality 6 by producing an effective divisor D of degree 6 with $\dim |D| > 0$. In summary:

Theorem 6.6. *There is no curve of genus* 7 *and gonality* 8 *over* $\mathbb{F}_2$ *that admits at least three closed points of degree* 3. □

7. Genus 9

Theorem 3.2 shows that if there is an excessive curve C of genus 9 over $\mathbb{F}_2$, then its real Weil polynomial and counts of closed points of various degrees are as below:

factored real Weil polynomial	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
$(T+1)(T^4-2T^3-6T^2+10T+1)^2$	0	4	0	0	0	8	0	18	64

In particular, note that C has a closed point of degree 6. If we took the tack of Section 5, we could show that a hypothetical excessive curve of genus 9 over $\mathbb{F}_2$ admits a singular plane model of degree 10 with no rational point. There are 2^{59} such curves that we would need to search. Even after imposing vanishing conditions at the four quadratic points, we would not be able to shrink the search space below about 2^{50} polynomials. This is far too large for us to handle, so instead we will use a different method: By analyzing the principally polarized varieties with the given real Weil polynomial, we can show that there is no genus-9 curve over $\mathbb{F}_2$ (of any gonality) with the given real Weil polynomial. Our argument uses results and techniques from [Howe 1995; Howe and Lauter 2003; 2012]; an expository overview of many of these results can be found in [Howe 2023].

Theorem 7.1. *Let* $h_1 = T+1$ *and let* $h_2 = T^4-2T^3-6T^2+10T+1$. *Then there is no curve over* $\mathbb{F}_2$ *whose real Weil polynomial is equal to* $h_1h_2^2$.

Proof. Let $E_{/\mathbb{F}_2}$ be the unique elliptic curve with real Weil polynomial h_1. Suppose there were a curve $C_{/\mathbb{F}_2}$ with real Weil polynomial $h_1h_2^2$. Since the resultant of the two polynomials h_1 and h_2 is -12, we see from

[Howe and Lauter 2003, Lemma 7] (or its generalization [Howe and Lauter 2012, Lemma 2.3]; see also [Howe 2023, Propositions 3.7 and 3.10]) that there is an abelian variety $A_{/\mathbb{F}_2}$ with real Weil polynomial h_2^2 and a finite 12-torsion group scheme Δ such that the Jacobian of C fits into an exact sequence

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

and where the induced maps $\Delta \to E$ and $\Delta \to A$ are both embeddings. Furthermore, the pullback to $E \times A$ of the canonical principal polarization of $\operatorname{Jac} C$ is the product $\lambda \times \mu$ of a polarization λ of E and a polarization μ of A, and the images of Δ in E and in A are the kernels of λ and μ.

If we let λ_0 be the canonical principal polarization of E, then every polarization of E is of the form $d\lambda_0$ for a positive integer d. Since the group scheme Δ is killed by 12, it follows that Δ is isomorphic to $E[d]$ for a divisor d of 12.

From [Howe and Lauter 2012, Lemma 4.3] (see also [Howe 2023, Proposition 4.13]) we see that there must be a nonconstant degree-d map from C to E. It follows that the number of closed points of degree at most d on C must be at least the number of rational points of E, because each rational point of E has at least one closed point of C lying over it, and the degree of each such closed point is at most d. Since E has five rational points, while C has no closed points of degree 1, 3, or 4 and only four of degree 2, we see that $d > 4$. That leaves open only two possibilities: $d = 6$ or $d = 12$.

We claim that neither of these possibilities can occur, because there is no polarization of A whose kernel is isomorphic to either $E[6]$ or $E[12]$. To prove this, we use the results of [Howe 1995], which give us information on the group schemes that occur as kernels of polarizations of abelian varieties in a given ordinary isogeny class. Given a finite multiset of finite simple group schemes, the results tell us whether there is a polarization of a variety in the given isogeny class such that the composition series of the kernel of the polarization is equal to the given multiset.

Let π denote the Frobenius endomorphism of A and let $\bar{\pi}$ denote its dual isogeny (the *Verschiebung*). Honda–Tate theory [Tate 1971] shows that the minimal polynomial of the endomorphism $\pi + \bar{\pi}$ is h_2, and since $\bar{\pi} = 2/\pi$, we find that the minimal polynomial of π is $f := T^4 h_2(T + 2/T)$. Let R denote the subring $\mathbb{Z}[\pi, \bar{\pi}]$ of $\operatorname{End} A$. Then $K := R \otimes \mathbb{Q}$ is the number field defined by f, and we can view R as an order in this field. The field K is a CM field, and its maximal real subfield K^+ is $\mathbb{Q}(\pi + \bar{\pi})$. We let R^+ denote the subring $\mathbb{Z}[\pi + \bar{\pi}]$ of R.

Let G be a finite group scheme that is a subgroup scheme of an abelian variety isogenous to A, so that the Frobenius and Verschiebung endomorphisms F and V of G satisfy $f(F) = f(V) = 0$. We associate to G a finite R-module $\operatorname{Mod}_R G$ as follows. First, we write G as a product $G_{rr} \times G_{r\ell} \times G_{\ell r}$, where G_{rr} is a reduced group scheme with reduced dual, $G_{r\ell}$ is a reduced group scheme with local dual, and $G_{\ell r}$ is a local group scheme with reduced dual. (Every finite group scheme over a finite field can be written as a product of three such group schemes together with another factor that is local with local dual [Manin 1963, p. 17; Waterhouse 1979, Corollary, p. 52], but for group schemes that can be embedded in an ordinary abelian variety, the local-local factor is trivial; this follows from the fact that, geometrically, the local part of the p-torsion of an ordinary abelian variety is isomorphic to a power of the local-reduced group scheme $\boldsymbol{\mu}_p$ [Deligne 1969, Section 2].) Let k be an algebraic closure of $\mathbb{F}_2$. Let M_{rr} and $M_{r\ell}$ be the finite R-modules whose underlying abelian groups are $G_{rr}(k)$ and $G_{r\ell}(k)$, respectively, and whose R-module structure is such that π acts as F and $\bar{\pi}$ acts as V. Let $\widehat{G}_{\ell r}$ be the Cartier dual of $G_{\ell r}$, and let $M_{\ell r}$ be the finite R-module whose underlying abelian group is $\widehat{G}_{\ell r}(k)$ and where π acts as V and $\bar{\pi}$ acts as F. Finally, we take $\operatorname{Mod}_R G = M_{rr} \oplus M_{r\ell} \oplus M_{\ell r}$.

The *Grothendieck group* $\mathscr{G}(S)$ of an order S in a number field is the group obtained from the free abelian group on finite S-modules by dividing out by the subgroup generated by the expressions $[M'] - [M] - [M'']$ for every exact sequence $0 \to M \to M' \to M'' \to 0$ of finite S-modules. The group $\mathscr{G}(S)$ is free, with a basis given by the classes of the simple S-modules.

The main result of [Howe 1995] tells us exactly which elements of the Grothendieck group of R contain the classes $[\operatorname{Mod}_R G]$ of the R-modules corresponding to kernels G of polarizations of varieties isogenous to A. (Such classes are called *attainable*.) To state the result, we need to define a certain quotient of the group $\mathscr{G}(R^+)$.

Every finite R-module is also a finite R^+-module, and an exact sequence of R-modules is also an exact sequence of R^+-modules. Thus there is a homomorphism $N_{R/R^+} : \mathscr{G}(R) \to \mathscr{G}(R^+)$. Also, for every nonzero element α of R^+ we have a finite R^+-module $R^+/\alpha R^+$. We let $\mathscr{B}(R)$ denote the quotient of $\mathscr{G}(R^+)$ by the subgroup generated by the image of N_{R/R^+} and by the classes of the modules $R^+/\alpha R^+$, where we let α range over the *totally positive* elements of R^+ — that is, the elements that are positive under every embedding of R^+ into the real numbers. Since $R = R^+[\pi]$ is free of rank 2 as an R^+-module, if we take any finite R^+-module M we find that $N_{R/R^+}([M \otimes_{R^+} R]) = 2[M]$, so the group $\mathscr{B}(R)$ is 2-torsion.

We define an element $I \in \mathscr{B}(R)$ associated to the isogeny class of A as in [Howe 1995, Definition 5.4]. Since $\mathscr{B}(R)$ is 2-torsion and since A is isogenous to the square of a simple abelian variety, the formula in [loc. cit., Definition 5.4] shows that $I = 0$.

Theorem 5.6 of [loc. cit.] says that a class of $\mathscr{G}(R)$ is attainable if and only if it is of the form $[M \otimes_{R^+} R]$ for an R^+-module M such that the image of the class $[M] \in \mathscr{G}(R^+)$ under the quotient map $\mathscr{G}(R^+) \to \mathscr{B}(R)$ is equal to I. (Note that if a class in $\mathscr{G}(R)$ is of the form $[M \otimes_{R^+} R]$ for an R^+-module M, then the class $[M] \in \mathscr{G}(R^+)$ is unique. Indeed, the map $T : \mathscr{G}(R^+) \to \mathscr{G}(R)$ given by $[M] \mapsto [M \otimes_{R^+} R]$ is a homomorphism because R is flat over R^+, and this homomorphism is injective because its composition with the norm from $\mathscr{G}(R)$ to $\mathscr{G}(R^+)$ is the multiplication-by-2 map on $\mathscr{G}(R^+)$.) To complete our proof of Theorem 7.1, then, it will be enough for us to show that both $\operatorname{Mod}_R E[6]$ and $\operatorname{Mod}_R E[12]$ are of the form $M \otimes_{R^+} R$ for an R^+-module M whose image in $\mathscr{B}(R)$ is *not* equal to I; that is, the image of M in $\mathscr{B}(R)$ should be nonzero.

Let $\mathfrak{q}_3$ be the prime ideal $(3, \pi + \bar{\pi} + 1)$ of R, let $\mathfrak{q}_2$ be the prime ideal $(2, \pi - 1) = (2, \bar{\pi})$ of R, and let $\bar{\mathfrak{q}}_2$ be the complex conjugate $(2, \bar{\pi} - 1) = (2, \pi)$ of $\mathfrak{q}_2$. We check that $E[6]$ and $E[12]$ can both be embedded in A, and that

$$[\operatorname{Mod}_R E[6]] = [\operatorname{Mod}_R E[3]] + \ [\operatorname{Mod}_R E[2]] = [R/\mathfrak{q}_3] + \ [R/\mathfrak{q}_2] + \ [R/\bar{\mathfrak{q}}_2],$$
$$[\operatorname{Mod}_R E[12]] = [\operatorname{Mod}_R E[3]] + 2[\operatorname{Mod}_R E[2]] = [R/\mathfrak{q}_3] + 2[R/\mathfrak{q}_2] + 2[R/\bar{\mathfrak{q}}_2].$$

Let $\mathfrak{p}_3$ be the prime ideal $(3, \pi+\bar{\pi}+1)$ of R^+ and let $\mathfrak{p}_2$ be the prime ideal $(2, \pi+\bar{\pi}+1)$ of R^+. We check that

$$(R^+/\mathfrak{p}_2)\otimes_{R^+} R \cong R/\mathfrak{q}_2 \oplus R/\bar{\mathfrak{q}}_2 \quad \text{and} \quad (R^+/\mathfrak{p}_3)\otimes_{R^+} R \cong R/\mathfrak{q}_3,$$

so [Howe 1995, Theorem 5.6] says that $[\mathrm{Mod}_R\, E[6]]$ will be attainable if and only if the image of $[R^+/\mathfrak{p}_3]+[R^+/\mathfrak{p}_2] \in \mathscr{G}(R^+)$ in $\mathscr{B}(R)$ is equal to zero, and that $[\mathrm{Mod}_R\, E[12]]$ will be attainable if and only if the image of $[R^+/\mathfrak{p}_3]+2[R^+/\mathfrak{p}_2]$ in $\mathscr{B}(R)$ is equal to zero.

As a first step, we note that $N_{R/R^+}([R/\mathfrak{q}_2]) \cong [R^+/\mathfrak{p}_2]$, so $[R^+/\mathfrak{p}_2]$ is in the kernel of the map $\mathscr{G}(R^+) \to \mathscr{B}(R)$. Thus, to complete the proof of the theorem, all we must show is that the image of $[R^+/\mathfrak{p}_3]$ in $\mathscr{B}(R)$ in nonzero. Our next step, then, is to compute the group $\mathscr{B}(R)$.

Let $\mathscr{O}$ be the maximal order of $K=\mathbb{Q}(\pi)$ and $\mathscr{O}^+$ be the maximal order of K^+. Computing the discriminants of $\mathscr{O}$ and $\mathscr{O}^+$, we find that no finite prime of $\mathscr{O}^+$ ramifies in $\mathscr{O}$, so [loc. cit., Proposition 10.2] tells us $\mathscr{B}(\mathscr{O}) \cong \mathrm{Gal}(K/K^+)$, and under this isomorphism the map $\mathscr{G}(\mathscr{O}^+) \to \mathscr{B}(\mathscr{O})$ is essentially the Artin map: if $\mathfrak{P}$ is a prime of $\mathscr{O}^+$, then the class of $\mathscr{O}^+/\mathfrak{P}$ in $\mathscr{G}(\mathscr{O}^+)$ is sent to 0 in $\mathscr{B}(\mathscr{O})$ if and only if $\mathfrak{P}$ splits in K/K^+.

The inclusion map $i: R \to \mathscr{O}$ gives us a pullback map $i^*: \mathscr{B}(\mathscr{O}) \to \mathscr{B}(R)$, and [loc. cit., Proposition 10.5] gives us two finite 2-torsion groups D_{s} and C_{s}, maps from these groups to $\mathscr{B}(\mathscr{O})$ and $\mathscr{B}(R)$, respectively, and a map $D_s \to C_s$ such that the diagram

$$\begin{array}{ccc} D_{\mathrm{s}} & \longrightarrow & \mathscr{B}(\mathscr{O}) \\ \big\downarrow & & \big\downarrow i^* \\ C_{\mathrm{s}} & \longrightarrow & \mathscr{B}(R) \end{array}$$

is a pushout diagram.

We see from [Howe 1995, pp. 2386–2387] that the group C_{s} is an $\mathbb{F}_2$-vector space with a basis consisting of symbols $x_{\mathfrak{p}}$ for the singular primes $\mathfrak{p}$ of R^+ that are inert in R/R^+. We compute that the discriminant of R^+ is 16 times the discriminant of $\mathscr{O}^+$, so the only singular prime of R^+ is the unique prime of R^+ that lies over 2, namely $\mathfrak{p}_2$. Since $\mathfrak{p}_2$ splits in R/R^+, the group C_{s} is trivial.

To compute D_{s} we again use the definition found in [loc. cit., pp. 2386–2387] together with [loc. cit., Remark 10.6]. We find that D_{s} is an $\mathbb{F}_2$-vector space with a basis consisting of symbols $y_{\mathfrak{P}}$ for the primes $\mathfrak{P}$ of $\mathscr{O}^+$ that are inert in $\mathscr{O}/\mathscr{O}^+$ and such that $\mathfrak{P} \cap R^+$ lies under a singular prime of R. Using [loc. cit., Proposition 9.4] we compute that the discriminant of R is $2^{16}\cdot 3^6 \cdot 11^2$, and since the discriminant of $\mathscr{O}$ is $2^8 \cdot 3^6 \cdot 11^2$, the singular primes of R all lie above $\mathfrak{p}_2$. There is only one prime of $\mathscr{O}^+$ that lies over 2, and it splits in $\mathscr{O}/\mathscr{O}^+$. Therefore D_{s} is also trivial.

Since the diagram above is a pushout diagram, we find that the map $i^*: \mathscr{B}(\mathscr{O}) \to \mathscr{B}(R)$ is an isomorphism.

To compute the image of $R^+/\mathfrak{p}_3$ in $\mathscr{B}(R)$, we use another pushout diagram that relates $\mathscr{B}(\mathscr{O})$ and $\mathscr{B}(R)$, namely the one found in [loc. cit., Proposition 10.4], which is

$$\begin{array}{ccc} \mathscr{G}(\mathscr{O}^+)/N_{\mathscr{O}/\mathscr{O}^+}(\mathscr{G}(\mathscr{O})) & \longrightarrow & \mathscr{B}(\mathscr{O}) \\ \big\downarrow N & & \big\downarrow i^* \\ \mathscr{G}(R^+)/N_{R/R^+}(\mathscr{G}(R)) & \longrightarrow & \mathscr{B}(R). \end{array}$$

Here the map N on the left side of the diagram is induced from the map $\mathscr{G}(\mathscr{O}^+) \to \mathscr{G}(R^+)$ that takes the class of a finite $\mathscr{O}^+$-module M to the class of M viewed as an R^+-module.

Let $\mathfrak{P}_3$ be the prime $(3, \pi + \bar{\pi} + 1)$ of $\mathscr{O}^+$; this is the unique prime of $\mathscr{O}^+$ over 3. Since R^+ is nonsingular at 3, the restriction of $\mathfrak{P}_3$ to R^+ is $\mathfrak{p}_3$, and the map N in the diagram takes the class of $\mathscr{O}^+/\mathfrak{P}_3$ in the upper-left group to the class of $R^+/\mathfrak{p}_3$ in the lower-left group. Since i^* is an isomorphism, the image of $R^+/\mathfrak{p}_3$ in $\mathscr{B}(R)$ is nonzero if and only if the image of $\mathscr{O}^+/\mathfrak{P}_3$ in $\mathscr{B}(\mathscr{O})$ is nonzero. We check that $\mathfrak{P}_3$ is inert in K/K^+, so the image of $\mathscr{O}^+/\mathfrak{P}_3$ in $\mathscr{B}(\mathscr{O})$ is nonzero. Therefore the image of $R^+/\mathfrak{p}_3$ in $\mathscr{B}(R)$ is nonzero, and the theorem is proved. □

8. Enumerating all excessive curves

As we noted in Section 4, an excessive curve over $\mathbb{F}_q$ of genus 3 is precisely a nonhyperelliptic curve of genus 3 with no rational points (a "pointless curve"), and a result of Howe, Lauter, and Top [Howe et al. 2005, Theorem 1.1] says that such curves exist over $\mathbb{F}_q$ if and only if $q \le 23$ or $q = 29$ or $q = 32$. In this section we sketch the method we used to enumerate all such curves over these fields. In total, there are 215 excessive genus-3 curves over these fields; the counts over each finite field were given in Table 1 in the Introduction.[1] Together with the excessive curve of genus 4 over $\mathbb{F}_2$ defined by the two equations $xy + z^2 + zw + w^2 = 0$ and $x^3 + y^3 + z^3 + y^2w + xzw = 0$ in $\mathbb{P}^4$ [Faber and Grantham 2022, Theorem 5.4] and the excessive curve of genus 4 over $\mathbb{F}_3$ defined by the two equations $xy + z^2 + w^2 = 0$ and $x^3 + y^3 + yz^2 + xw^2 - yw^2 - zw^2 = 0$ in $\mathbb{P}^4$ [Faber and Grantham 2023, Theorem 5.3], this gives a total of exactly 217 excessive curves over finite fields.

A human- and computer-readable Magma file, `AllGenus3.magma`, containing a list of all 215 of the excessive genus-3 curves over finite fields, is available with the other programs associated with this paper.

For $q \le 5$, we used a simple brute force search to find representatives of the $\mathrm{PGL}_2(\mathbb{F}_q)$ orbits of pointless plane quartics. We find unique representatives of each orbit by explicitly calculating the orbits. We confirmed our computations for $q = 2$ and $q = 3$ by checking the [LMFDB] database, which includes data collected from every curve of genus 3 over $\mathbb{F}_2$ and $\mathbb{F}_3$.

For $7 \le q \le 23$, we used a more efficient brute force search that depends on the curves having enough quadratic points. Note that the Weil bound shows that if $q \ge 7$, then a genus-3 curve over $\mathbb{F}_q$ has at least $q^2 + 1 - 6q \ge 8$ points over $\mathbb{F}_{q^2}$. If the curve is also pointless over $\mathbb{F}_q$, then it must have at least 4 quadratic points, and this will be enough for our method to work. Let us explain the idea.

Let s_1 and s_2 be distinct elements of $\mathbb{F}_{q^2}$ that are conjugate over $\mathbb{F}_q$. We let P_1 be the quadratic point of $\mathbb{P}^2$ whose geometric points are $[s_1 : 0 : 1]$ and $[s_2 : 0 : 1]$, and we let P_2 be the quadratic point of $\mathbb{P}^2$ whose geometric points are $[0 : s_1 : 1]$ and $[0 : s_2 : 1]$. If $f \in \mathbb{F}_q[x, y, z]$ is a homogeneous quartic, we say that f is *pinned* (with respect to P_1 and P_2) if it vanishes at P_1 and P_2.

Suppose $C_{/\mathbb{F}_q}$ is an excessive curve of genus 3 that has at least three quadratic points. We identify C with one of its plane quartic models, so that C is given by a homogeneous quartic $f \in \mathbb{F}_q[x, y, z]$.

[1] Note that the curve $(x^2 + xz)^2 + (y^2 + yz)(x^2 + xz) + (y^2 + yz)^2 + z^4 = 0$ is excessive as a curve over $\mathbb{F}_2$ *and* as a curve over $\mathbb{F}_{32}$, but we count it twice in our enumeration because we consider curves to be schemes over a base field.

q	7	8	9	11	13	16	17	19	23
CPUs	1	1	1	1	1	1	16	64	64
wall time (m)	0	0	1	7	42	281	90	113	778

Table 5. Search resources and wall time for finding excessive plane quartic curves.

Each quadratic point of C determines a rational line in the plane, and at most two quadratic points of C can lie on a given line because C is defined by a quartic. Since we are assuming that C has at least three quadratic points, we can choose two such points that determine distinct rational lines. Then there are exactly four automorphisms of $\mathbb{P}^2$ that take the two chosen quadratic points to the quadratic points P_1 and P_2, respectively. By applying such an automorphism, we can assume that C passes through P_1 and P_2; that is, we may assume that f is a pinned quartic.

The space of plane quartics (up to scalars) is 14-dimensional. By limiting ourselves to pinned quartics, we cut our search space down to 10 dimensions. We can further increase our efficiency in looping through this search space by using the fact that we only want to consider pointless quartics f. For example, since $f(1, 0, 0)$ and $f(0, 1, 0)$ and $f(0, 0, 1)$ are all supposed to be nonzero, we see that the coefficients of x^4, y^4, and z^4 in f are all nonzero. Going further, we can choose the collection of coefficients of x^4, x^3y, x^2y^2, xy^3, and y^4 all at once, and use the requirement that $f(a, b, 0) \neq 0$ for all $a, b \in \mathbb{F}_q$ to limit the possible values of these coefficients. We implemented our search using these ideas as often as possible.

Suppose $f \in \mathbb{F}_q[x, y, z]$ is a homogeneous quartic that defines an excessive curve C. It is a straightforward matter to produce a list of all pinned quartics g that define a curve isomorphic to C: simply loop through all of the pairs (Q_1, Q_2) of noncollinear quadratic points on C, and for each such pair write down the four pinned quartics obtained by moving Q_1 to P_1 and Q_2 to P_2. There are at most $(q^2 + 6q + 1)/2$ quadratic points on C, and so there are roughly q^4 pinned quartics defining C. For the prime powers q that we are considering, we can easily list all of these quartics. If we order them — say, by number of nonzero terms, and lexicographically within that grouping — we can then identify the first one. This “first pinned quartic” is a well-defined normal form for C that allows us to quickly test whether two pointless quartics are isomorphic to one another.

The basic idea of our enumeration strategy is to run through all pointless pinned quartics f using the method described above. If such an f defines a curve of genus 3 (that is, if f is geometrically irreducible and defines a nonsingular curve), then we compute its “first pinned quartic” normal form and add this to our list of excessive curves, if it is not already on the list.

We wrote Magma code to implement this algorithm, and ran it for all $q \leq 16$. Running in Magma 2.26-10 on a 3.2 GHz Apple M1 Max, the case $q = 16$ took just under 90 core-hours. To double-check our work and to reach the larger values of q, we rewrote the code in C as well, and ran it on a cluster of Intel Xeon E5-2699v3 CPUs. This allowed us to reach all $q \leq 23$. See Table 5 for resources and timing for this computation.

We estimate that it would take about 10,000 CPU-hours to do this calculation for $q = 29$, and about 30,000 CPU-hours for $q = 32$. Fortunately, there are other methods available for these cases.

For $q = 29$, we use Lauter's algorithm to show that if there is a genus-3 curve $C_{/\mathbb{F}_{29}}$ with no points, then its real Weil polynomial is $(T - 10)^3$. Suppose there is such a C, and let J be its Jacobian. There are two elliptic curves over $\mathbb{F}_{29}$ that have real Weil polynomial $T - 10$: the curve $E_1 : y^2 = x^3 + x$, whose endomorphism ring is isomorphic to $\mathbb{Z}[i]$, where $i^2 = -1$, and the curve $E_2 : y^2 = x^3 + 12x^2 + 4x$, whose endomorphism ring isomorphic to $\mathbb{Z}[2i]$. From [Kani 2011, Theorem 2] we see that J is isomorphic (as an abelian threefold without polarization) to one of the products

$$E_1 \times E_1 \times E_1, \quad E_1 \times E_1 \times E_2, \quad E_1 \times E_2 \times E_2, \quad \text{and} \quad E_2 \times E_2 \times E_2.$$

Let $A := E_1 \times E_1 \times E_1$. Then there is an isogeny $\varphi : A \to J$ of degree 1, 2, 4, or 8, depending on which of the four products J is isomorphic to. The principal polarization on J pulls back to a polarization λ on A of degree 1, 4, 16, or 64. This polarization can be represented by a Hermitian matrix $M \in M_3(\mathbb{Z}[i])$ of determinant 1, 2, 4, or 8. Then [Howe and Lauter 2012, Table 2, p. 190] shows that there is an embedding $\psi : E_1 \to A$ such that $\psi^*\lambda$ is either the principal polarization on E_1 or twice the principal polarization on E_1. We see from [loc. cit., Lemma 4.3] that then there must be a map $C \to E_1$ of degree 1 or 2. A degree-1 map would be impossible, so C must be a double cover of E_1. It is a straightforward matter to enumerate all of the genus-3 double covers of E_1; see [Howe and Lauter 2003, Section 6.1] for a detailed description of the similar calculation of all genus-4 double covers of an elliptic curve over a finite field. We find that up to isomorphism, there is exactly one pointless plane quartic over $\mathbb{F}_{29}$, already listed in [Howe et al. 2005, Table 2]: the curve $x^4 + y^4 + z^4 = 0$.

For $q = 32$, we note that it was already proven in [Elkies 1999, Section 3.3] that there is exactly one pointless plane quartic over $\mathbb{F}_{32}$ (and that this curve is the reduction modulo 2 of a twist of the Klein quartic).

Appendix A: Polynomial bases for Proposition 6.5

For completeness, we give the bases of polynomials used to search for singular plane curves of genus 7 as described by Proposition 6.5. To unify the presentation, we formalize the properties these bases must have in order to efficiently construct curves that do not pass through a rational point of the plane.

Formalism A.1. Let $S_1, \dots, S_5$ be five sets of homogeneous polynomials of degree 9 in $\mathbb{F}_2[x, y, z]$ that satisfy the following hypotheses:

- At each of the three points $[1:0:0]$, $[0:1:0]$, and $[0:0:1]$, exactly one element of S_1 is nonzero. Each element of S_i with $i > 1$ vanishes at these three points.
- At the point $P = [1:1:0]$, each polynomial in S_2 is nonzero. Each polynomial in S_3, S_4, and S_5 vanishes at P. An even number of elements of S_1 are nonzero at P.
- At the point $P = [1:0:1]$, each polynomial in S_3 is nonzero. Each polynomial in S_2, S_4, and S_5 vanishes at P. An even number of elements of S_1 are nonzero at P.
- At the point $P = [0:1:1]$, each polynomial in S_4 is nonzero. Each polynomial in S_2, S_3, and S_5 vanishes at P. If S_4 is nonempty (resp. empty), an even (resp. odd) number of elements of S_1 are nonzero at P.

• At the point $P = [1:1:1]$, each polynomial in S_i is nonzero for $i = 2, 3, 4, 5$. If S_4 is nonempty (resp. empty), an odd (resp. even) number of elements of S_1 are nonzero at P.

Let F_1 be the sum of all polynomials in S_1. For $i = 2, 3, 4, 5$, let F_i be the sum of an odd number of polynomials in S_i. If $S_4 = \varnothing$, we take $F_4 = 0$. Then $F = \sum F_i$ does not vanish at any rational point of the plane.

Remark A.2. This formalism applies to our constructions in Sections 5 and 6.1. For $g = 6$ and $g = 7$, we used

$$\begin{aligned}
S_1 &= \{x^{g+1}, y^{g+1}, z^{g+1}\},\\
S_2 &= \{x^i y^{g+1-i} : 1 \le i \le g\},\\
S_3 &= \{x^i z^{g+1-i} : 1 \le i \le g\},\\
S_4 &= \{y^i z^{g+1-i} : 1 \le i \le g\},\\
S_5 &= \{x^i y^j z^{g+1-i-j} : 1 \le i \le g-1,\ 1 \le j \le g-i\}.
\end{aligned}$$

A1. ***Triple cubic point on a line.*** In the language of Formalism A.1, we take the following to be our basis for the space of degree-9 homogeneous polynomials that vanish to order 3 at the cubic point $[0:1:t]$:

$$\begin{aligned}
S_1 &= \{x^9, (y^3+y^2z+z^3)^3\},\\
S_2 &= \{x^i y^{9-i} : 3 \le i \le 8\} \cup \{x^2y^4(y^3+y^2z+z^3), xy^2(y^3+y^2z+z^3)^2\},\\
S_3 &= \{x^i z^{9-i} : 3 \le i \le 8\} \cup \{x^2z(y^3+y^2z+z^3)^2, xz^2(y^3+y^2z+z^3)^2\},\\
S_4 &= \varnothing,\\
S_5 &= \{x^i y^j z^{9-i-j} : 3 \le i \le 7,\ 1 \le j \le 5,\ i+j < 9\}\\
&\quad \cup \{xyz(y^3+y^2z+z^3)^2, x^2yz(y^5+yz^4+z^5), x^2y^2z^2(y^3+y^2z+z^3), x^2y^3z(y^3+y^2z+z^3)\}.
\end{aligned}$$

One verifies directly that all of these polynomials vanish to order 3 at $[0:1:t]$. Each polynomial in $S := S_1 \cup \cdots \cup S_5$, except for the element $x^2y^2z^2(y^3+y^2z+z^3)$ of S_5, has the property that it contains a monomial that is not present in any other polynomial in S. Consequently, the full set of 37 polynomials in S must be linearly independent over $\mathbb{F}_2$.

Appendix B. Double and single cubic points on a line

In the language of Formalism A.1, we take the following to be our basis for the space of degree-9 homogeneous polynomials that vanish at the cubic points $[0:1:t]$ and $[0:1:t+1]$, with order at least 2 at the former:

$$\begin{aligned}
S_1 &= \{x^9, (y^3+yz^2+z^3)(y^3+y^2z+z^3)^2\},\\
S_2 &= \{x^i y^{9-i} : 2 \le i \le 8\} \cup \{xy^5(y^3+y^2z+z^3)\},\\
S_3 &= \{x^i z^{9-i} : 2 \le i \le 8\} \cup \{xz^2(y^3+y^2z+z^3)^2\},\\
S_4 &= \varnothing,\\
S_5 &= \{x^i y^j z^{9-i-j} : 2 \le i \le 7,\ 1 \le j \le 6,\ i+j < 9\}\\
&\quad \cup \{xyz(y^3+y^2z+z^3)^2, xy^2z(y^5+yz^4+z^5), xy^3z^2(y^3+y^2z+z^3), xy^4z(y^3+y^2z+z^3)\}.
\end{aligned}$$

One verifies directly that all of these polynomials vanish at $[0:1:t]$ and at $[0:1:t+1]$ to the correct orders. Each polynomial in $S := S_1 \cup \cdots \cup S_5$, except for $xy^4z(y^3+y^2z+z^3)$ and $xy^3z^2(y^3+y^2z+z^3)$, has the property that it contains a monomial that is not present in any other polynomial in S. Therefore, every nontrivial linear relation among the polynomials in S must involve only the two exceptional polynomials, and since those two polynomials are distinct, the full set of 43 polynomials in S must be linearly independent over $\mathbb{F}_2$.

B1. ***Cubic point on two distinct lines.*** In the language of Formalism A.1, we take the following to be our basis for the space of degree-9 homogeneous polynomials that vanish at the cubic points $[0:1:t]$ and $[1:0:t]$:

$S_1 = \{x^2(x^7+z^7),\ y^2(y^7+z^7),\ z^2(x^7+y^7+z^7)\}$,

$S_2 = \{x^i y^{9-i} : 1 \le i \le 8\}$,

$S_3 = \{x^2z(x^3+x^2z+z^3)^2,\ x^2z^2(x^5+xz^4+z^5),\ xz^3(x^5+xz^4+z^5), x^3z^3(x^3+x^2z+z^3),\ xz^5(x^3+x^2z+z^3)\}$,

$S_4 = \{y^2z(y^3+y^2z+z^3)^2,\ y^2z^2(y^5+yz^4+z^5),\ yz^3(y^5+yz^4+z^5), y^3z^3(y^3+y^2z+z^3),\ yz^5(y^3+y^2z+z^3)\}$,

$S_5 = \{x^i y^j z^{9-i-j} : 1 \le i \le 7,\ 1 \le j \le 7,\ i+j < 9\}$.

One verifies directly that all of these polynomials vanish at $[0:1:t]$ and $[1:0:t]$. Every polynomial in $S := S_1 \cup \cdots \cup S_5$, except for those in

$$T := \{xz^3(x^5+xz^4+z^5),\ x^2z^2(x^5+xz^4+z^5),\ yz^3(y^5+yz^4+z^5),\ y^2z^2(y^5+yz^4+z^5)\},$$

has the property that it contains a monomial that is not present in any other polynomial in S. Therefore, if there is a nontrivial linear relation among the polynomials in S, it must involve only the polynomials in T. But now we note that every polynomial in T includes a monomial that appears in no other element of T, so the elements of T — and hence the elements of S — are linearly independent over $\mathbb{F}_2$.

Appendix C: Isogeny classes for genus 7

Here we collect the real Weil polynomials for potentially excessive curves of genus 7 over $\mathbb{F}_2$ that survived Lauter's algorithm and the corresponding numbers of places; see Theorem 3.2.

no.	factored real Weil polynomial	a_1	a_2	a_3	a_4	a_5	a_6	a_7
1	$T^7-3T^6-12T^5+36T^4+44T^3-132T^2-44T+141$	0	0	0	8	0	4	9
2	$T^7-3T^6-12T^5+38T^4+34T^3-132T^2+13T+78$	0	0	2	4	0	6	1
3	$T(T^6-3T^5-12T^4+39T^3+27T^2-126T+57)$	0	0	3	0	0	13	9
4	$T^7-3T^6-12T^5+40T^4+24T^3-132T^2+75T+1$	0	0	4	0	0	9	10
5	$(T^3-4T^2+3T+1)(T^4+T^3-11T^2-8T+25)$	0	0	4	1	0	5	6
6	$(T^3-T^2-7T+6)(T^4-2T^3-7T^2+14T-2)$	0	0	5	0	0	9	12
7	$T^7-3T^6-11T^5+33T^4+33T^3-99T^2-14T+52$	0	1	0	4	0	9	10
8	$(T+2)(T^6-5T^5-T^4+35T^3-36T^2-30T+38)$	0	1	0	5	0	4	10
9	$T^7-3T^6-11T^5+33T^4+35T^3-105T^2-25T+86$	0	1	0	6	0	4	11

no.	factored real Weil polynomial	a_1	a_2	a_3	a_4	a_5	a_6	a_7
10	$T^7-3T^6-11T^5+33T^4+35T^3-105T^2-24T+83$	0	1	0	6	0	5	11
11	$(T^3-2T^2-5T+8)(T^4-T^3-8T^2+4T+12)$	0	1	0	7	0	4	12
12	$T^7-3T^6-10T^5+30T^4+24T^3-72T^2+11$	0	2	0	1	0	10	11
13	$(T^2-T-5)(T^5-2T^4-7T^3+13T^2+3T-7)$	0	2	0	2	0	4	11
14	$T^7-3T^6-10T^5+30T^4+25T^3-75T^2-3T+21$	0	2	0	2	0	9	12
15	$T^7-3T^6-10T^5+30T^4+25T^3-75T^2+2T+7$	0	2	0	2	0	14	13
16	$(T-1)(T^2-T-5)(T^4-T^3-8T^2+5T+9)$	0	2	0	3	0	3	12
17	$T^7-3T^6-10T^5+30T^4+26T^3-78T^2-6T+31$	0	2	0	3	0	8	13
18	$T^7-3T^6-10T^5+30T^4+26T^3-78T^2-5T+28$	0	2	0	3	0	9	13
19	$(T^2-T-5)(T^5-2T^4-7T^3+13T^2+5T-11)$	0	2	0	4	0	2	13
20	$T^7-3T^6-10T^5+30T^4+27T^3-81T^2-13T+52$	0	2	0	4	0	3	13
21	$T^7-3T^6-10T^5+30T^4+27T^3-81T^2-9T+41$	0	2	0	4	0	7	14
22	$(T^2-2T-2)(T^5-T^4-10T^3+8T^2+23T-19)$	0	2	0	4	0	8	14
23	$T^7-3T^6-10T^5+30T^4+28T^3-84T^2-15T+59$	0	2	0	5	0	3	14
24	$T^7-3T^6-10T^5+30T^4+28T^3-84T^2-12T+51$	0	2	0	5	0	6	15
25	$(T+1)(T^3-2T^2-5T+8)^2$	0	2	0	6	0	4	16
26	$T^7-3T^6-9T^5+27T^4+18T^3-54T^2+T+11$	0	3	0	0	0	7	14
27	$T(T^2-T-5)(T^4-2T^3-6T^2+11T-1)$	0	3	0	0	0	11	15
28	$T^7-3T^6-9T^5+27T^4+19T^3-57T^2-2T+21$	0	3	0	1	0	5	15
29	$T^7-3T^6-9T^5+27T^4+19T^3-57T^2-T+18$	0	3	0	1	0	6	15
30	$(T^2-T-5)(T^5-2T^4-6T^3+11T^2-2)$	0	3	0	1	0	9	16
31	$T^7-3T^6-9T^5+27T^4+19T^3-57T^2+3T+7$	0	3	0	1	0	10	16
32	$T^7-3T^6-9T^5+27T^4+19T^3-57T^2+4T+4$	0	3	0	1	0	11	16
33	$(T^3-T^2-5T+1)(T^4-2T^3-6T^2+10T+1)$	0	3	0	1	0	12	16
34	$(T-1)(T^2-2T-2)(T^4-9T^2-2T+14)$	0	3	0	2	0	4	16
35	$T^7-3T^6-9T^5+27T^4+20T^3-60T^2-3T+25$	0	3	0	2	0	5	16
36	$(T^2-T-5)(T^5-2T^4-6T^3+11T^2+T-4)$	0	3	0	2	0	7	17
37	$T^7-3T^6-9T^5+27T^4+20T^3-60T^2+17$	0	3	0	2	0	8	17
38	$T^7-3T^6-9T^5+27T^4+20T^3-60T^2+T+14$	0	3	0	2	0	9	17
39	$T^7-3T^6-9T^5+27T^4+20T^3-60T^2+2T+11$	0	3	0	2	0	10	17
40	$T^7-3T^6-9T^5+27T^4+20T^3-60T^2+3T+8$	0	3	0	2	0	11	17
41	$(T^3-T^2-6T+3)(T^4-2T^3-5T^2+7T+3)$	0	3	0	2	0	11	18
42	$T^7-3T^6-9T^5+27T^4+20T^3-60T^2+4T+6$	0	3	0	2	0	12	18
43	$T^7-3T^6-9T^5+27T^4+21T^3-63T^2-5T+32$	0	3	0	3	0	4	17
44	$(T-1)(T^2-2T-2)(T^2-T-5)(T^2+T-3)$	0	3	0	3	0	5	18
45	$T^7-3T^6-9T^5+27T^4+21T^3-63T^2-3T+27$	0	3	0	3	0	6	18
46	$T^7-3T^6-9T^5+27T^4+21T^3-63T^2-2T+24$	0	3	0	3	0	7	18
47	$T^7-3T^6-9T^5+27T^4+21T^3-63T^2-T+21$	0	3	0	3	0	8	18
48	$(T^3-6T-3)(T^4-3T^3-3T^2+12T-6)$	0	3	0	3	0	9	18
49	$T^7-3T^6-9T^5+27T^4+21T^3-63T^2+19$	0	3	0	3	0	9	19
50	$T^7-3T^6-9T^5+27T^4+22T^3-66T^2-5T+34$	0	3	0	4	0	5	19
51	$T^7-3T^6-9T^5+27T^4+22T^3-66T^2-4T+31$	0	3	0	4	0	6	19
52	$(T-1)(T+2)(T^2-2T-2)(T^3-2T^2-5T+8)$	0	3	0	4	0	6	20

no.	factored real Weil polynomial	a_1	a_2	a_3	a_4	a_5	a_6	a_7
53	$(T-1)(T^6-2T^5-10T^4+14T^3+28T^2-14T-11)$	0	4	0	0	0	7	20
54	$(T^3-T^2-6T+4)(T^4-2T^3-4T^2+4T+2)$	0	4	0	0	0	8	20
55	$T^7-3T^6-8T^5+24T^4+14T^3-42T^2+4T+9$	0	4	0	0	0	8	21
56	$T^7-3T^6-8T^5+24T^4+14T^3-42T^2+5T+6$	0	4	0	0	0	9	21
57	$T^7-3T^6-8T^5+24T^4+14T^3-42T^2+6T+3$	0	4	0	0	0	10	21
58	$T(T^6-3T^5-8T^4+24T^3+14T^2-42T+7)$	0	4	0	0	0	11	21
59	$(T-1)(T^6-2T^5-10T^4+14T^3+29T^2-16T-13)$	0	4	0	1	0	7	22
60	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+4T+10$	0	4	0	1	0	8	22
61	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+4T+11$	0	4	0	1	0	8	23
62	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+5T+7$	0	4	0	1	0	9	22
63	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+5T+8$	0	4	0	1	0	9	23
64	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+6T+4$	0	4	0	1	0	10	22
65	$(T^2-T-5)(T^5-2T^4-5T^3+9T^2-T-1)$	0	4	0	1	0	10	23
66	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+7T+1$	0	4	0	1	0	11	22
67	$T^7-3T^6-8T^5+24T^4+15T^3-45T^2+7T+2$	0	4	0	1	0	11	23
68	$T(T^3-2T^2-5T+8)(T^3-T^2-5T+1)$	0	4	0	1	0	12	24
69	$T^7-3T^6-8T^5+24T^4+16T^3-48T^2+3T+14$	0	4	0	2	0	7	23
70	$(T-1)^2(T^2-T-5)(T^3-6T-3)$	0	4	0	2	0	7	24
71	$T^7-3T^6-8T^5+24T^4+16T^3-48T^2+4T+11$	0	4	0	2	0	8	23
72	$(T^3-2T^2-4T+6)(T^4-T^3-6T^2+2T+2)$	0	4	0	2	0	8	24
73	$T^7-3T^6-8T^5+24T^4+16T^3-48T^2+4T+13$	0	4	0	2	0	8	25
74	$(T+2)(T^6-5T^5+2T^4+20T^3-24T^2+5)$	0	4	0	2	0	9	25
75	$(T-1)(T^6-2T^5-9T^4+12T^3+23T^2-10T-1)$	0	5	0	0	0	10	28
76	$T^7-3T^6-7T^5+21T^4+11T^3-33T^2+9T+2$	0	5	0	0	0	10	29
77	$(T-1)T(T+2)(T^2-3T+1)(T^2-T-5)$	0	5	0	0	0	11	30
78	$T^7-3T^6-7T^5+21T^4+11T^3-33T^2+10T+1$	0	5	0	0	0	11	31
79	$(T-1)(T^3-T^2-5T+1)^2$	0	5	0	0	0	12	32

References

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Deligne 1969] P. Deligne, "Variétés abéliennes ordinaires sur un corps fini", *Invent. Math.* **8** (1969), 238–243. MR Zbl

[Elkies 1999] N. D. Elkies, "The Klein quartic in number theory", pp. 51–101 in *The eightfold way*, edited by S. Levy, Math. Sci. Res. Inst. Publ. **35**, Cambridge Univ. Press, 1999. MR Zbl

[Faber and Grantham 2022] X. Faber and J. Grantham, "Binary curves of small fixed genus and gonality with many rational points", *J. Algebra* **597** (2022), 24–46. MR Zbl

[Faber and Grantham 2023] X. Faber and J. Grantham, "Ternary and quaternary curves of small fixed genus and gonality with many rational points", *Exp. Math.* **32**:2 (2023), 337–349. MR Zbl

[Hart et al. 2020] W. Hart, F. Johansson, and S. Pancratz, "FLINT: fast library for number theory", C library, 2020, available at http://flintlib.org. Version 2.6.0.

[Howe 1995] E. W. Howe, "Principally polarized ordinary abelian varieties over finite fields", *Trans. Amer. Math. Soc.* **347**:7 (1995), 2361–2401. MR Zbl

[Howe 1996] E. W. Howe, "Constructing distinct curves with isomorphic Jacobians", *J. Number Theory* **56**:2 (1996), 381–390. MR Zbl

[Howe 2005] E. W. Howe, "Infinite families of pairs of curves over $\mathbb{Q}$ with isomorphic Jacobians", *J. London Math. Soc.* (2) **72**:2 (2005), 327–350. MR Zbl

[Howe 2023] E. W. Howe, "Deducing information about curves over finite fields from their Weil polynomials", pp. 1–36 in *Curves over finite fields—past, present and future*, edited by A. Bassa et al., Panor. Synthèses **60**, Soc. Math. France, Paris, 2023. MR Zbl

[Howe and Lauter 2003] E. W. Howe and K. E. Lauter, "Improved upper bounds for the number of points on curves over finite fields", *Ann. Inst. Fourier* (*Grenoble*) **53**:6 (2003), 1677–1737. Correction in **57**:3 (2007), 1019–1021. MR Zbl

[Howe and Lauter 2012] E. W. Howe and K. E. Lauter, "New methods for bounding the number of points on curves over finite fields", pp. 173–212 in *Geometry and arithmetic*, edited by C. Faber et al., Eur. Math. Soc., Zürich, 2012. MR Zbl

[Howe et al. 2005] E. W. Howe, K. E. Lauter, and J. Top, "Pointless curves of genus three and four", pp. 125–141 in *Arithmetic, geometry and coding theory* (*AGCT* 2003), edited by Y. Aubry and G. Lachaud, Sémin. Congr. **11**, Soc. Math. France, Paris, 2005. MR Zbl

[Kani 2011] E. Kani, "Products of CM elliptic curves", *Collect. Math.* **62**:3 (2011), 297–339. MR Zbl

[Lauter 2000] K. Lauter, "Zeta functions of curves over finite fields with many rational points", pp. 167–174 in *Coding theory, cryptography and related areas* (Guanajuato, 1998), edited by J. Buchmann et al., Springer, 2000. MR Zbl

[LMFDB] The LMFDB Collaboration, "The L-functions and modular forms database", electronic reference, available at http://www.lmfdb.org.

[Manin 1963] Y. I. Manin, "Theory of commutative formal groups over fields of finite characteristic", *Uspehi Mat. Nauk* **18**:6 (1963), 3–90. In Russian; translated in *Russ. Math. Surv.* **18** (1963), 1–83. MR Zbl

[Poonen 2007] B. Poonen, "Gonality of modular curves in characteristic p", *Math. Res. Lett.* **14**:4 (2007), 691–701. MR Zbl

[Robinson 1964] R. M. Robinson, "Algebraic equations with span less than 4", *Math. Comp.* **18** (1964), 547–559. MR Zbl

[SageMath] W. A. Stein et al., "Sage mathematics software", Version 9.1, available at http://www.sagemath.org.

[Serre 2020] J.-P. Serre, *Rational points on curves over finite fields*, edited by A. Bassa et al., Documents Mathématiques (Paris) **18**, Société Mathématique de France, Paris, 2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler. MR Zbl

[Tate 1966] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144. MR Zbl

[Tate 1971] J. Tate, "Classes d'isogénie des variétés abéliennes sur un corps fini", exposé 352, pp. 95–110 in *Séminaire Bourbaki*, 1968/1969, Lecture Notes in Math. **175**, Springer, 1971. MR Zbl

[Tsfasman et al. 2007] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic geometric codes: basic notions*, Math. Surv. Monogr. **139**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl

[Warren 2002] H. S. Warren, *Hacker's delight*, Addison-Wesley, Boston, MA, 2002.

[Waterhouse 1979] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics **66**, Springer, 1979. MR Zbl

Communicated by Melanie Matchett Wood
Received 2024-03-04 Revised 2024-07-30 Accepted 2024-09-13

xander@super.org Center for Computing Sciences, Institute for Defense Analyses, Bowie, MD, United States

grantham@super.org Center for Computing Sciences, Institute for Defense Analyses, Bowie, MD, United States

however@alumni.caltech.edu San Diego, CA, United States

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada
Bhargav Bhatt	University of Michigan, USA
Frank Calegari	University of Chicago, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France
Brian D. Conrad	Stanford University, USA
Samit Dasgupta	Duke University, USA
Hélène Esnault	Freie Universität Berlin, Germany
Gavril Farkas	Humboldt Universität zu Berlin, Germany
Sergey Fomin	University of Michigan, USA
Edward Frenkel	University of California, Berkeley, USA
Wee Teck Gan	National University of Singapore
Andrew Granville	Université de Montréal, Canada
Ben J. Green	University of Oxford, UK
Christopher Hacon	University of Utah, USA
Roger Heath-Brown	Oxford University, UK
János Kollár	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne
Martin Olsson	University of California, Berkeley, USA
Irena Peeva	Cornell University, USA
Jonathan Pila	University of Oxford, UK
Anand Pillay	University of Notre Dame, USA
Bjorn Poonen	Massachusetts Institute of Technology, USA
Victor Reiner	University of Minnesota, USA
Peter Sarnak	Princeton University, USA
Michael Singer	North Carolina State University, USA
Vasudevan Srinivas	SUNY Buffalo, USA
Shunsuke Takagi	University of Tokyo, Japan
Pham Huu Tiep	Rutgers University, USA
Ravi Vakil	Stanford University, USA
Akshay Venkatesh	Institute for Advanced Study, USA
Melanie Matchett Wood	Harvard University, USA
Shou-Wu Zhang	Princeton University, USA

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2025 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 19 No. 8 2025