Restrictions on Weil Polynomials of Jacobians of Hyperelliptic Curves

Edgar Costa, Ravi Donepudi, Ravi Fernando, Valentijn Karemaker, Caleb Springer, and Mckenzie West

Abstract Inspired by experimental data, we investigate which isogeny classes of abelian varieties defined over a finite field of odd characteristic contain the Jacobian of a hyperelliptic curve. We provide a necessary condition by demonstrating that the Weil polynomial of a hyperelliptic Jacobian must have a particular form modulo 2. For fixed $g \geq 1$, the proportion of isogeny classes of g-dimensional abelian varieties defined over $\mathbb{F}_q$ which fail this condition is $1 - Q(2g + 2)/2^g$ as $q \to \infty$ ranges over odd prime powers, where $Q(n)$ denotes the number of partitions of n into odd parts.

E. Costa (✉)
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, USA
e-mail: edgarc@mit.edu

R. Donepudi
Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL, USA
e-mail: donepud2@illinois.edu

R. Fernando
Department of Mathematics, University of California — Berkeley, Berkeley, CA, USA
e-mail: fernando@berkeley.edu

V. Karemaker
Mathematical Institute, Utrecht University, Utrecht, The Netherlands
e-mail: V.Z.Karemaker@uu.nl

C. Springer
Department of Mathematics, The Pennsylvania State University, University Park, PA, USA
e-mail: cks5320@psu.edu

M. West
Department of Mathematics, University of Wisconsin-Eau Claire, Eau Claire, WI, USA
e-mail: westmr@uwec.edu

1   Introduction

The question of which abelian varieties arise as Jacobians of curves has a long and rich history. It has classically been investigated over the complex numbers as the Schottky Problem, using techniques from differential geometry and Hodge theory. In positive characteristic, some of these tools are no longer available, but instead the Frobenius endomorphism becomes a formidable weapon.

In this article, we study g-dimensional abelian varieties which are defined over a finite field $\mathbb{F}_q$ of odd cardinality. The $\mathbb{F}_q$-isogeny class of such an abelian variety A is uniquely determined by the characteristic polynomial of its Frobenius endomorphism. This polynomial is called the *Weil polynomial* of the abelian variety and has the following form:

$$Z_A(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{g-1} t^{g+1} + a_g t^g + a_{g-1} q t^{g-1} + \cdots + a_1 q^{g-1} t + q^g \in \mathbb{Z}[t].$$

Given $Z_A(t)$, one would like to determine if the isogeny class of A contains the Jacobian of a smooth curve over $\mathbb{F}_q$.

In genus one, the problem is straightforward, as every one-dimensional abelian variety is an elliptic curve, which is isomorphic to its Jacobian. For genus two, the problem was solved by Howe, Nart, and Ritzenthaler [HNR09] who give an explicit classification using only elementary restrictions involving the integers a_1, a_2, and q. Their method relies on three key facts:

(1) the Jacobian of a curve is canonically principally polarized;
(2) a principally polarized abelian surface is isomorphic to exactly one of the following: a Jacobian of a genus two curve, a product of two elliptic curves, or the restriction of scalars of an elliptic curve from a quadratic extension of the ground field;
(3) every genus two curve is hyperelliptic.

In particular, they take advantage of the canonical involution associated with any genus two curve.

Solving this problem in higher genus appears to be significantly more complicated. For example, every curve of genus three is isomorphic to either a hyperelliptic curve or to a smooth plane quartic curve. Curves of the latter type generically do not possess any non-trivial automorphisms, so the arguments of Howe, Nart and Ritzenthaler for genus two cannot easily be extended to non-hyperelliptic genus three curves.

In this paper, we focus on a more accessible question, namely, whether a given isogeny class of abelian varieties contains the Jacobian of a hyperelliptic curve. We do this by studying the geometric configurations of the Weierstrass points of hyperelliptic curves, as is done in the $g = 2$ case, e.g., [MN02, Appendix]. In doing so, we obtain parity conditions on the coefficients of the Weil polynomials which prevent certain isogeny classes from containing the Jacobian of a hyperelliptic curve. For instance, in genus three we obtain:

Theorem 2.8 *Let q be an odd prime power. The isogeny classes of three-dimensional abelian varieties corresponding to Weil polynomials of the form*

$$t^6 + a_1t^5 + a_2t^4 + a_3t^3 + qa_2t^2 + q^2a_1t + q^3$$

with $a_2 \equiv 0 \pmod 2$ and $a_3 \equiv 1 \pmod 2$ do not contain the Jacobian of a hyperelliptic curve over $\mathbb{F}_q$.

In fact, we can perform the same analysis for abelian varieties of any dimension; as far as we know, this is the first non-existence result for Jacobians in isogeny classes when $g > 2$ and q is any odd prime power. Indeed, we demonstrate that the Weil polynomial of the Jacobian of a hyperelliptic curve of genus g over a finite field of odd characteristic must be congruent modulo 2 to a polynomial of the form $\prod_{i=1}^{r}(t^{d_i} - 1)/(t - 1)^2 \in \mathbb{F}_2[t]$ where $2g + 2 = d_1 + \cdots + d_r$ is a partition. We call a Weil polynomial *admissible* if it takes this form modulo 2, and *inadmissible* otherwise. Notice that it is easy to test whether a polynomial is admissible by explicitly trying all possible partitions, and an isogeny class is guaranteed to not contain a hyperelliptic Jacobian if its Weil polynomial is inadmissible.

By using asymptotic results on the number of Weil polynomials of a fixed degree whose coefficients lie in prescribed congruence classes modulo an integer, it is possible to determine the asymptotic proportion of isogeny classes with admissible, or inadmissible, Weil polynomials.

Theorem 3.3 *Let $c(q, g)$ be the proportion of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ with admissible Weil polynomial. For all $g \geq 2$ we have*

$$\lim_{q \to \infty} c(q, g) = \frac{Q(2g + 2)}{2^g},$$

as q ranges over odd prime powers, where $Q(2g + 2)$ is the number of partitions of $2g + 2$ into distinct parts.

For comparison, notice that for fixed $g > 6$, it is possible to see by simply counting the number of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ versus the number of hyperelliptic curves of genus g over $\mathbb{F}_q$ that actually 0% of g-dimensional abelian varieties over $\mathbb{F}_q$ contain a hyperelliptic Jacobian as $q \to \infty$ ranges over odd prime powers. However, this counting argument does not provide a way to identify which isogeny classes do or do not contain a hyperelliptic Jacobian. In contrast, for any fixed $g \geq 1$, any isogeny class with an inadmissible Weil polynomial is explicitly known to not contain a hyperelliptic Jacobian. Rephrasing the theorem above for fixed $g > 6$, the proportion of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ which do not contain a hyperelliptic Jacobian but are not found by testing for inadmissible Weil polynomials is $Q(2g + 2)/2^g$ as $q \to \infty$ ranges over odd prime powers. As noted in Remark 3.4, this discrepancy approaches zero as g grows.

On the other hand, over the algebraic closure $\overline{\mathbb{F}}_q$, determining which isogeny classes contain Jacobians remains an open question. In order for our methods to shed light in this context, the behavior of admissibility under finite field extensions must first be understood. We leave this question for future work.

The outline of the paper is as follows. In Sect. 2, we recall some results on the geometry of hyperelliptic curves and their Jacobians and prove Theorem 2.8 and its generalizations to higher genus. In Sect. 3, we study asymptotic consequences of these non-existence results, deriving Theorem 3.3. In Sect. 4, we determine restrictions on point counts of curves, allowing us to reprove Theorem 2.8 by elementary methods. Finally, in Sect. 5, we present experimental data on the optimality of our results.

2 Weil Polynomials Mod 2

Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ (of characteristic $p \neq 2$) with canonical degree two map $\pi \colon C \to \mathbb{P}^1$. Let $W := \{\alpha_1, \alpha_2, \ldots, \alpha_{2g+2}\}$ be the support of ramification divisor of π, i.e., the geometric Weierstrass points of C. The $\mathbb{F}_q$-Frobenius endomorphism Frob acts on W by permuting its elements; we denote the cardinalities of the orbits of this action by d_i. (Alternatively, W consists of some number, r, of $\mathbb{F}_q$-places with respective degrees d_i, where $d_1 + \cdots + d_r = 2g + 2$.)

The multiset $d_C := \{d_i\}$ forms a partition of the integer $2g + 2$; we call this the *degree set* of the curve C, and by convention we order the d_i so that $d_1 \leq d_2 \leq \cdots \leq d_r$.

Explicitly, C can be given in coordinates by $y^2 = f(x)$, where f is a squarefree polynomial of degree either $2g + 1$ or $2g + 2$. Then W consists of the points $(\alpha, 0)$, where α runs over the roots of f, together with the point at infinity if $\deg(f) = 2g + 1$. Then the d_i are precisely the degrees of the irreducible factors of f, along with an extra 1 in the case $\deg(f) = 2g + 1$.

Remark 2.1 If q is small compared to the genus, not all partitions of $2g + 2$ may arise as degree sets of genus g hyperelliptic curves, due to the finite number of irreducible polynomials of any fixed degree in $\mathbb{F}_q[x]$. For example, if $2g+2 > q+1$, then the partition $2g + 2 = 1 + \cdots + 1$ cannot be realized, as there are not enough $\mathbb{F}_q$-points for C to ramify over.

Let J denote the Jacobian variety of C whose elements are degree-zero divisors on C modulo linear equivalence. Then the group $J[2]$ of (geometric) 2-torsion of J is an $\mathbb{F}_2$-vector space that admits the following explicit description.

Lemma 2.2 *The group $J[2]$ of 2-torsion elements of J forms a $2g$-dimensional vector space over $\mathbb{F}_2$. Explicitly, this group can be expressed as the vector space obtained from $\mathbb{F}_2^{2g+2}$ by considering all vectors with an even number of non-zero entries and forming the quotient by $\langle (1, 1, \ldots, 1) \rangle$.*

Proof The first claim follows since $p \neq 2$. For the second, we argue as follows; cf. [Mum07, Corollary 2.11] over $\mathbb{C}$, which extends to any algebraically closed field of characteristic unequal to two. Every element of $J[2]$ can be explicitly represented either by a divisor

$$e_U := \sum_{P \in U} P - |U|(\infty),$$

if the map $\pi : C \to \mathbb{P}^1$ is ramified at infinity, in which case the symbol ∞ slightly abusively denotes $\pi^{-1}(\infty) \in C$, or by a divisor

$$e_U := \sum_{P \in U} P - \frac{|U|}{2}(\infty_1 + \infty_2),$$

if π is split at infinity, in which case $\pi^{-1}(\infty) = \{\infty_1, \infty_2\}$. Either way, the set $U \subseteq W$ is a subset of even cardinality, and two divisors, e_U and $e_{U'}$, represent the same element of $J[2]$ if either $U = U'$ or $U = W \setminus U'$. In the $\mathbb{F}_2$-vector space V whose standard basis is indexed by W, the above set of representatives determine the subspace of vectors with an even number of non-zero entries. Two vectors $v_1, v_2 \in V$ yield the same element of $J[2]$ precisely when their sum is contained in $\langle(1, 1, \ldots, 1)\rangle$. The second claim follows. $\square$

We will also need the following standard fact about vector spaces, whose proof is omitted.

Lemma 2.3 *Consider an exact sequence of vector spaces*

$$0 \to W_1 \to W_2 \to W_3 \to 0$$

and a linear map $T : W_2 \to W_2$ such that $T(W_1) \subseteq W_1$. We will also denote the induced map $T : W_3 \to W_3$. For $i \in \{1, 2, 3\}$, denote the characteristic polynomial of T on W_i by $\chi(T, W_i)$. Then we have

$$\chi(T, W_2) = \chi(T, W_1)\chi(T, W_3).$$

Denote the base-change of C (resp. J) to $\overline{\mathbb{F}}_q$ by C^{alg} (resp. J^{alg}). Exploiting the action of Frob on the geometric Weierstrass points W, we obtain the following result on the characteristic polynomial of Frob modulo 2.

Proposition 2.4 *Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$. Let $\{d_i\}_{i=1}^r$ be the partition of $2g + 2$ which records the sizes of the orbits of Frobenius acting on the $2g + 2$ geometric Weierstrass points. For any prime $\ell \neq p$ we have*

$$\det\left(1 - \text{Frob}\, t \mid H^1_{\text{ét}}(C^{\text{alg}}, \mathbb{Q}_\ell)\right) \equiv \left(\prod_{i=1}^r t^{d_i} - 1\right)/(t - 1)^2 \pmod{2}. \qquad (2.5)$$

Proof We have (cf. [Mil86, Corollary 9.6]) that

$$\det\left(1 - \mathrm{Frob}\, t \mid H^1_{\text{ét}}(C^{\mathrm{alg}}, \mathbb{Q}_\ell)\right) = \det\left(1 - \mathrm{Frob}\, t \mid H^1_{\text{ét}}(J^{\mathrm{alg}}, \mathbb{Q}_\ell)\right)$$

$$= \det\left(1 - \mathrm{Frob}\, t \mid V_\ell(J)\right),$$

where $V_\ell(J) = T_\ell(J) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and where $T_\ell(J)$ is the ℓ-adic Tate module of J. By the Weil conjectures the polynomials above all have integer coefficients. By taking $\ell = 2$, we further have

$$\det\left(1 - \mathrm{Frob}\, t \mid V_2(J)\right) \equiv \det\left(1 - \mathrm{Frob}\, t \mid J[2]\right) \pmod{2}.$$

As before, consider the $\mathbb{F}_2$-vector space $W_2 := \mathbb{F}_2^{2g+2}$ whose standard basis is indexed by W and which is acted on by the $\mathbb{F}_q$-Frobenius endomorphism Frob. By assumption, the action of Frob on W_2 can be represented by a block-diagonal matrix with r blocks, whose ith block (of order d_i) is a cyclic permutation of basis vectors. Since the characteristic polynomial of a cyclic permutation of order n is $t^n - 1$, it follows that

$$\chi(\mathrm{Frob}, W_2) = \prod_{i=1}^{r} \left(t^{d_i} - 1\right).$$

Furthermore, let W_1 be the codimension-one subspace of vectors with an even number of non-zero entries. Then W_1 is stable under Frob. Moreover, Frob acts invertibly on W_1 and hence also on the one-dimensional quotient $W_3 := W_2/W_1$, so that $\chi(\mathrm{Frob}, W_3) = t - 1$. Applying Lemma 2.3 to the short exact sequence $0 \to W_1 \to W_2 \to W_2/W_1 \to 0$ yields

$$\chi(\mathrm{Frob}, W_1) = \frac{\prod_{i=1}^{r}(t^{d_i} - 1)}{t - 1}.$$

Now let W_4 be the one-dimensional subspace of $\langle(1, 1, \ldots, 1)\rangle \subseteq W_1$ and define $W_5 := W_1/W_4$. Similarly, W_4 is stable under Frob with $\chi(\mathrm{Frob}, W_4) = t - 1$ since Frob acts invertibly. Applying Lemma 2.3 to the short exact sequence $0 \to W_4 \to W_1 \to W_5 \to 0$, we find

$$\chi(\mathrm{Frob}, W_5) = \frac{\prod_{i=1}^{r}\left(t^{d_i} - 1\right)}{(t - 1)^2}.$$

Since, by Lemma 2.2, Frob acts on W_5 as it does on $J[2]$, the result follows. □

Remark 2.6 It is possible to prove a congruence modulo 2 similar to (2.5) in Proposition 2.4 also when the finite field $\mathbb{F}_q$ is allowed to have characteristic 2. In this case, Frobenius acts on Weierstrass points as it does on the étale part of

Table 2.9 Weil coefficients modulo 2 and corresponding partitions for threefolds

Coefficients (a_1, a_2, a_3) (mod 2)	Partition of 8
$(0, 1, 1)$	$\{3, 5\}$
$(1, 1, 0)$	$\{1, 1, 1, 1, 1, 3\}, \{1, 1, 1, 2, 3\}, \{1, 2, 2, 3\}, \{1, 3, 4\}$
$(1, 0, 0)$	$\{1, 1, 1, 5\}, \{1, 2, 5\}$
$(0, 0, 0)$	$\{1, 1, 3, 3\}, \{1, 1, 6\}, \{2, 3, 3\}, \{2, 6\}$
$(0, 1, 0)$	$\{1, 1, 1, 1, 1, 1, 1, 1\}, \{1, 1, 1, 1, 1, 1, 2\}, \{1, 1, 1, 1, 2, 2\},$
	$\{1, 1, 1, 1, 4\}, \{1, 1, 2, 2, 2\}, \{1, 1, 2, 4\},$
	$\{2, 2, 2, 2\}, \{2, 2, 4\}, \{4, 4\}, \{8\}$
$(1, 1, 1)$	$\{1, 7\}$

$J[2]$. Since we require odd characteristic throughout the rest of the paper, notably in Theorem 3.1, we do not pursue this further.

Definition 2.7 We call any polynomial of the form (2.5) an *admissible Weil polynomial modulo 2*. Note that the notion of admissibility is independent of q.

By applying Proposition 2.4 to all possible partitions of 8 we obtain our main theorem.

Theorem 2.8 *Let q be an odd prime power. The isogeny classes of three-dimensional abelian varieties corresponding to Weil polynomials of the form*

$$t^6 + a_1 t^5 + a_2 t^4 + a_3 t^3 + q a_2 t^2 + q^2 a_1 t + q^3$$

with $a_2 \equiv 0$ (mod 2) and $a_3 \equiv 1$ (mod 2) do not contain the Jacobian of a hyperelliptic curve over $\mathbb{F}_q$.

Proof For each of the twenty-two partitions $\{d_i\}$ of $2g + 2 = 8$, we compute the corresponding polynomial $(t - 1)^{-2} \prod_{i=1}^{r} (t^{d_i} - 1)$. By Proposition 2.4, these are all of the admissible Weil polynomials modulo 2 for Jacobians of hyperelliptic curves of genus three. In Table 2.9, we tabulate the coefficients (a_1, a_2, a_3) of the resulting Weil polynomials modulo 2 with the corresponding partitions $\{d_i\}$.   □

Although Theorem 2.8 only considers the case of three-dimensional abelian varieties, Proposition 2.4 applies much more generally. Indeed, for any $g \geq 1$, we can produce a list of admissible Weil polynomials modulo 2 for Jacobians of hyperelliptic curves of genus g, independent of q. The following result counts the number of admissible polynomials in terms of partitions.

Proposition 2.10 *The number of admissible Weil polynomials modulo 2 for Jacobians of hyperelliptic curves of genus g over finite fields of odd characteristic is equal to $Q(2g + 2)$, the number of partitions of $2g + 2$ into distinct parts, or equivalently, the number of partitions of $2g + 2$ into odd parts.*

Proof It is well known that the number of partitions of $2g + 2$ into distinct parts is equal to the number of partitions of $2g + 2$ into odd parts; see [NZM91, Theorem

10.2]. For the remainder of this proof, our perspective will focus on partitions into distinct parts.

Proposition 2.4 shows how to compute admissible Weil polynomials modulo 2 using partitions, although many different partitions can correspond to a single admissible polynomial. For the purposes of this proof, we will call two partitions $\{d_1, \ldots, d_r\}$ and $\{e_1, \ldots, e_s\}$ of an integer n *equivalent* if

$$\prod_{i=1}^{r} \left(t^{d_i} - 1\right) \equiv \prod_{j=1}^{s} \left(t^{e_j} - 1\right) \pmod{2}.$$

Using Eq. (2.5), it suffices to prove that every equivalence class of partitions of $2g + 2$ contains precisely one partition with distinct parts.

Observe that every partition of $2g + 2$ is equivalent to a partition with distinct parts. Indeed, if $\{d_1, \ldots, d_{r+1}\}$ is any partition of $2g + 2$ where $d_r = d_{r+1}$, then we can construct another partition $\{d_1, \ldots, d_{r-1}, d_r'\}$ with $d_r' = 2d_r$. These two partitions are equivalent since $t^{2d_r} - 1 \equiv (t^{d_r} - 1)^2 \mod 2$. Thus by induction on the number of equal parts, we conclude that every admissible Weil polynomial modulo 2 arises as a partition of $2g + 2$ into distinct parts.

Now suppose that $\{d_1, \ldots, d_r\}$ and $\{e_1, \ldots, e_s\}$ are two equivalent partitions of $2g + 2$ into distinct parts. Without loss of generality, we order the parts so that d_1 and e_1 are the smallest parts of their respective partitions. After expanding the polynomials above, we see that the non-constant monomials of smallest degree are t^{d_1} and t^{e_1}, respectively. This implies that $d_1 = e_1$, hence $\{d_2, \ldots, d_r\}$ and $\{e_2, \ldots, e_s\}$ are equivalent partitions of $2g + 2 - d_1$. Thus by induction on r, we conclude that two equivalent partitions of $2g + 2$ into distinct parts are equal. □

Remark 2.11 In contrast with Remark 2.1, every admissible Weil polynomial mod 2 arises as the reduction mod 2 of a Weil polynomial for a hyperelliptic curve over $\mathbb{F}_q$, for each q: Since there is at least one irreducible polynomial of every degree, we can construct a hyperelliptic curve ramified at points of degree d_i, where $\{d_i\}$ is the partition of $2g + 2$ into distinct parts.

In Table 2.12, we tabulate the number of admissible and inadmissible Weil polynomials modulo 2 for Jacobians of hyperelliptic curves of genus $g \leq 7$, i.e., the numbers $Q(2g + 2)$ and $2^g - Q(2g + 2)$.

Table 2.12 The number of admissible and inadmissible Weil polynomials modulo 2 for hyperelliptic curves of small genus

g	1	2	3	4	5	6	7
$Q(2g + 2)$	2	4	6	10	15	22	32
	100.00%	100.00%	75.00%	62.50%	46.88%	34.38%	25.00%
$2^g - Q(2g + 2)$	0	0	2	6	17	42	96
	0.00%	0.00%	25.00%	37.50%	53.12%	65.62%	75.00%

3 Asymptotics

The results in the previous section show that an isogeny class cannot contain a hyperelliptic Jacobian if the coefficients of the corresponding Weil polynomial satisfy a certain parity condition. Therefore, it is natural to ask how many Weil polynomials satisfy any given parity condition, or more generally, how many Weil polynomials are congruent to a given fixed polynomial of the correct form modulo an integer m. The following theorem answers this question asymptotically for abelian varieties of fixed dimension.

Theorem 3.1 *Let $g \geq 2$ and m be fixed integers, and let $f(t) \in \mathbb{Z}[t]$ be a fixed polynomial of the form*

$$f(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{g-1} t^{g+1} + a_g t^g + a_{g-1} q t^{g-1} + \cdots + a_1 q^{g-1} t + q^g.$$

For a prime power q coprime to m, write $e_{f,m}(q, g)$ for the proportion of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ whose Weil polynomial is congruent to $f(x)$ modulo m. Then

$$\lim_{q \to \infty} e_{f,m}(q, g) = \frac{1}{m^g},$$

where the limit is taken over all prime powers q coprime to m.

Proof This is essentially a theorem of Holden [Hol04, Theorem 5], although we present a slightly more general statement here. Specifically, Holden's theorem only considers the case when $m = \ell$ is a prime, and the limit is taken over $q = p^r$ for a single fixed prime p. However, the more general version of the theorem presented above is obtained immediately from Holden's methods, as follows. Denote by $I(q, g)$ the number of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ and write $I_{f,m}(q, g)$ for the number of such isogeny classes whose Weil polynomial is congruent to $f(x)$ modulo m. With this notation we may write $e_{f,m}(q, g) = \frac{I_{f,m}(q,g)}{I(q,g)}$. Using lattices, DiPippo and Howe obtained upper and lower bounds for $I(q, g)$; see [DH98, Theorem 1.2] and [DH00]. Holden employed analogous techniques to obtain similar bounds for $I_{f,m}(q, g)$; see [Hol04, Proposition 2.2]. Using these bounds, as in the proof of [Hol04, Theorem 5], we find

$$\frac{v_g r(q) q^{g(g+1)/4} m^{-g} - 2c(g, m) q^{g(g+1)/4 - 1/2} m^{1-g}}{v_g r(q) q^{g(g+1)/4} + (v_g + 3c(g, 1)) q^{g(g+1)/4 - 1/2}}$$

$$\leq \frac{I_{f,m}(q, g)}{I(q, g)}$$

$$\leq \frac{v_g r(q) q^{g(g+1)/4} m^{-g} + (v_g + 3c(g, 1)) q^{g(g+1)/4 - 1/2} m^{1-g}}{v_g r(q) q^{g(g+1)/4} - 2c(g, m) q^{g(g+1)/4 - 1/2}},$$

where v_g is a constant depending g, and $c(g, m)$ is a constant depending on both g and m, and $r(q) = \varphi(q)/q$, where φ denotes Euler totient function. Letting $q \to \infty$, the theorem follows. $\qquad\square$

Recall that, in light of Theorem 2.8 and Proposition 2.10, we say that the Weil polynomial of an isogeny class of g-dimensional abelian varieties is admissible if it is congruent modulo 2 to a polynomial of the form $\prod_{i=1}^{r}(t^{d_i}-1)/(t^2-1) \in \mathbb{F}_2[t]$ for some partition $2g+2 = d_1+\cdots+d_r$, and is inadmissible otherwise. By combining Theorems 2.8 and 3.1, we obtain the following corollary.

Corollary 3.2 *Denote by $c(q)$ the proportion of isogeny classes of abelian three-folds over $\mathbb{F}_q$ with admissible Weil polynomials. Then*

$$\lim_{q\to\infty} c(q) = 75\%,$$

where the limit is taken over all odd prime powers q.

More generally, by combining Theorem 2.8 and Proposition 2.10, we can determine the proportion of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ with admissible Weil polynomials in terms of the number of partitions of $2g+2$ into distinct parts.

Theorem 3.3 *Let $c(q, g)$ be the proportion of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ with admissible Weil polynomial. For all $g \geq 2$ we have*

$$\lim_{q\to\infty} c(q, g) = \frac{Q(2g+2)}{2^g},$$

as q ranges over odd prime powers, where $Q(2g+2)$ is the number of partitions of $2g+2$ into distinct parts.

Proof By Proposition 2.10, we know there is a set of polynomials $S = \{f_1, \ldots, f_{Q(2g+2)}\}$ such that the Weil polynomial of the Jacobian of a hyperelliptic curve of genus g over any finite field of odd characteristic is equivalent modulo 2 to some polynomial in S. Thus, the result follows immediately from Theorem 3.1. $\quad\square$

Remark 3.4 For fixed $g \geq 2$, the number of isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ and the number of hyperelliptic curves of genus g over $\mathbb{F}_q$ are asymptotically bounded by $q^{g(g+1)/4}$ and q^{2g-1}, respectively, as $q \to \infty$ ranges over odd prime powers; see [DH98, Theorem 1.1], and [Nar09, Table 1, Corollary 3.4]. For $g > 6$, this means that asymptotically 0% of the isogeny classes of g-dimensional abelian varieties over $\mathbb{F}_q$ contain a hyperelliptic Jacobian as $q \to \infty$ ranges over odd prime powers. Comparing this reality to Theorem 3.3, we see that the proportion of isogeny classes of g-dimensional abelian varieties that have an admissible Weil polynomial but still do not contain a hyperelliptic Jacobian is $\frac{Q(2g+2)}{2^g}$ as $q \to \infty$. Notice that this discrepancy gets smaller as g grows. Indeed, $Q(N) \sim \frac{3^{3/4}}{12N^{3/4}} \exp(\pi\sqrt{N/3})$ as $N \to \infty$ [FS09, Figure 1.9], so it follows that $\frac{Q(2g+2)}{2^g} \to 0$ as $g \to \infty$.

4 Point Counts

In Sect. 2 we determined restrictions modulo 2 for Weil polynomials of hyperelliptic Jacobians. These Weil polynomials govern the point counts of the corresponding hyperelliptic curve $C/\mathbb{F}_q$ over all extensions of $\mathbb{F}_q$. In this section, we determine 2-adic restrictions on the point counts of hyperelliptic curves over extensions of $\mathbb{F}_q$ by more elementary means. Rather than studying the action of Frobenius on $J[2]$, we study its action on the Weierstrass points of the curve directly. In particular, this provides an alternative proof of Theorem 2.8.

4.1 Restrictions on Parity of Point Counts

As before, let q be an odd prime power, $C/\mathbb{F}_q$ be a hyperelliptic curve of genus $g > 1$. Recall that we denote the support of the ramification divisor by W and we denote by $\{d_i\}$ a partition of $2g + 2$, corresponding to the decomposition of W into Frobenius orbits. We begin with the following observations on the point counts of C over extensions of $\mathbb{F}_q$.

Lemma 4.1 *For each $n \geq 1$, we have $\#W(\mathbb{F}_{q^n}) = \sum_{i:d_i|n} d_i$.*

Proof A point of degree d contributes d $\mathbb{F}_{q^n}$-points if $d|n$, and none otherwise. $\square$

Lemma 4.2 *For each $n \geq 1$, we have $\#C(\mathbb{F}_{q^n}) \equiv \#W(\mathbb{F}_{q^n}) \pmod 2$.*

Proof The $\mathbb{F}_{q^n}$-points of W are precisely the $\mathbb{F}_{q^n}$-points of C that are fixed by the hyperelliptic involution. Since all other points appear in pairs, it follows that $\#C(\mathbb{F}_{q^n}) \equiv \#W(\mathbb{F}_{q^n}) \pmod 2$. $\square$

Corollary 4.3 *For each $n \geq 1$, we have $\#C(\mathbb{F}_{q^n}) \equiv \#C(\mathbb{F}_{q^{2n}}) \pmod 2$.*

Proof The numbers n and $2n$ share the same set of odd divisors, therefore by Lemmas 4.1 and 4.2

$$\#C(\mathbb{F}_{q^n}) \equiv \#W(\mathbb{F}_{q^n}) = \sum_{i:d_i|n} d_i \equiv \sum_{i:d_i|2n} d_i = \#W(\mathbb{F}_{q^{2n}}) \equiv \#C(\mathbb{F}_{q^{2n}}) \pmod 2.$$

$\square$

Corollary 4.4 *For each n, we have*

$$n \cdot \#\{i : d_i = n\} \equiv \sum_{d|n} \mu(n/d) \#C(\mathbb{F}_{q^d}) \pmod 2,$$

where μ is the Möbius function.

Proof Using Lemma 4.1 we can restate Lemma 4.2 as

$$\#C(\mathbb{F}_{q^n}) \equiv \sum_{d|n} d \cdot \#\{i : d_i = d\} \pmod 2.$$

The result follows by applying Möbius inversion.   □

Remark 4.5 For C as above, consider the binary sequence

$$a_C(n) := \#C(\mathbb{F}_{q^n}) \pmod 2.$$

Lemma 4.2 and Corollary 4.4 imply that a_C determines, and is determined by, the numbers $n \cdot \#\{i : d_i = n\} \pmod 2$ for all n. These numbers are encoded in the degree set d_C; they tell us the parity of $\#(i : d_i = n)$ when n is odd, and give no information when n is even.

More precisely, Lemma 4.2 and Corollary 4.4 give us a dictionary between the sequence a_C of parities of point counts and the set

$$\{d : d \text{ is odd and appears an odd number of times in } d_C\}.$$

This is consistent with Proposition 2.10.

This is already enough to prove that some sequences of point count parities are inconsistent with the identity $\sum d_i = 2g + 2$. For example:

Lemma 4.6 *If the genus of C is 3, then we cannot have $\#C(\mathbb{F}_q) \equiv 0$, $\#C(\mathbb{F}_{q^3}) \equiv 1$, and $\#C(\mathbb{F}_{q^5}) \equiv 0 \pmod 2$.*

Proof If such a curve C existed, Corollary 4.4 implies that $\#\{d_i = 1\}$ is even, $\#\{d_i = 3\}$ is odd, and $\#\{d_i = 5\}$ is even. Thus $\#\{d_i = 3\} = 1$ and $\#\{d_i = 5\} = 0$, which contradicts $\#\{d_i = 1\}$ being even.   □

4.2 Restrictions on Point Counts Modulo Powers of 2

We have just seen some restrictions on the point counts modulo 2 of hyperelliptic curves. In this section we will obtain further restrictions modulo higher powers of 2.

Fix an integer $m \geq 1$. Let G be the group $\{\pm1\} \times \mathrm{Gal}(\mathbb{F}_{q^{2m}}/\mathbb{F}_q)$ of order 2^{m+1}. This acts on the $\mathbb{F}_{q^{2m}}$-points of C, where the first factor acts by the hyperelliptic involution and the second by field automorphisms. We will study $\#C(\mathbb{F}_{q^{2m}}) \pmod{2^{m+1}}$ by examining the orbits of the action of G.

Proposition 4.7 *If C is a genus g hyperelliptic curve over $\mathbb{F}_q$, then*

$$\#C(\mathbb{F}_{q^n}) \equiv 2(q^n + 1) - \#W(\mathbb{F}_{q^n}) \pmod{2^{a+1}},$$

where $n = 2^a \cdot m \geq 1$ with m odd.

Proof We will count the $\mathbb{F}_{q^n}$-points of C by considering the fibers of the hyperelliptic map $\pi : C(\mathbb{F}_{q^n}) \to \mathbb{P}^1(\mathbb{F}_{q^n})$. If $x \in \mathbb{P}^1(\mathbb{F}_{q^n})$, then $\pi^{-1}(x)$ can be computed by extracting the square roots of $f(x)$, where f is a polynomial of degree $2g + 1$ or $2g + 2$. Accordingly, $\pi^{-1}(x)$ contains either zero, one, or two $\mathbb{F}_{q^n}$-points, and a preimage of size one occurs if and only if $x \in W$. Further, if n is even and x is defined over $\mathbb{F}_{q^{n/2}}$ (equivalently, if its degree is not divisible by 2^a), then the preimage must have size two, since quadratic equations $y^2 = f(x)$ over $\mathbb{F}_{q^{n/2}}$ can be solved over $\mathbb{F}_{q^n}$. Thus, the preimage may have size zero only if the degree of x is divisible by 2^a. In this case, the Galois orbit of x has size divisible by 2^a, so if there are $\mathbb{F}_{q^n}$-points above x, they occur in an orbit whose size is divisible by 2^{a+1}. Hence, to count modulo 2^{a+1}, we may assume that all unramified $\mathbb{F}_{q^n}$-points of $\mathbb{P}^1$ have exactly two preimages defined over $\mathbb{F}_{q^n}$, and subtract the number of $\mathbb{F}_{q^n}$-points of W to obtain the result. □

As with Proposition 2.4, this implies that certain sequences of point counts of hyperelliptic curves (equivalently, certain Weil polynomials of their Jacobians) cannot be realized.

Corollary 4.8 *Assume that the genus of C is 3. If $\#C(\mathbb{F}_q) \equiv 1 \pmod 2$ and $\#C(\mathbb{F}_{q^3}) \equiv 0 \pmod 2$, then we have $\#C(\mathbb{F}_{q^{2m}}) \equiv -1 \pmod{2^{m+1}}$ for all $m \geq 1$.*

Proof Since $\#C(\mathbb{F}_q)$ is odd, we have that $\#\{d_i = 1\}$ is odd by Lemma 4.2. Analogously, since $\#\{d_i = 1\}$ is odd and $\#C(\mathbb{F}_{q^3})$ is even, it follows that $\#\{d_i = 3\}$ is odd and hence must equal one. Altogether, we have $d_j = 3$ for a unique j and $d_{j'} \in \{1, 2, 4\}$ for $j' \neq j$. Hence $\# \left(\bigcup_{k \geq 1} W(\mathbb{F}_{q^{2k}}) \right) = 5$, and so $\#W(\mathbb{F}_{q^{2m}}) \equiv 5 \pmod{2^{m+1}}$. The result follows by applying Proposition 4.7 to $n = 2^m$, since we have $q^{2^m} \equiv 1 \pmod{2^{m+1}}$ for q odd. □

4.3 Reproving Theorem 2.8

The results in the previous subsections can be used to reprove Theorem 2.8 as follows:

Alternative Proof of Theorem 2.8 Suppose that the statement is false, so that there is some hyperelliptic curve C of genus three whose Jacobian has the prescribed Weil polynomial. By using Newton's formulae and [Mil86, Theorem 11.1], we can write the point counts $\#C(\mathbb{F}_{q^k})$ in terms of the coefficients of the Weil polynomial for all $k \geq 1$, as follows:

$$\#C(\mathbb{F}_q) = q + 1 + a_1;$$
$$\#C(\mathbb{F}_{q^2}) = q^2 + 1 - a_1^2 + 2a_2;$$
$$\#C(\mathbb{F}_{q^3}) = q^3 + 1 + a_1^3 - 3a_1a_2 + 3a_3;$$

$$\#C(\mathbb{F}_{q^4}) = q^4 + 1 - a_1^4 + 4a_1^2 a_2 - 4a_1 a_3 - 2a_2^2 + 4qa_2;$$

$$\#C(\mathbb{F}_{q^5}) = q^5 + 1 + a_1^5 - 5a_1^3 a_2 + 5a_1 a_2^2 - 5qa_1 a_2 - 5a_2 a_3 + 5q^2 a_1.$$

We will complete our proof by showing that the restrictions $a_2 \equiv 0 \pmod 2$ and $a_3 \equiv 1 \pmod 2$ on the coefficients force the point counts to fall into the impossible cases listed in the lemmas above. First consider the case when $a_1 \equiv 0 \pmod 2$. Expanding the equations above leads to

$$\#C(\mathbb{F}_q) \equiv 0 \pmod 2, \quad \#C(\mathbb{F}_{q^2}) \equiv 2 \pmod 4,$$

$$\#C(\mathbb{F}_{q^3}) \equiv 1 \pmod 2, \quad \#C(\mathbb{F}_{q^4}) \equiv 2 \pmod 8,$$

$$\#C(\mathbb{F}_{q^5}) \equiv 0 \pmod 2.$$

In particular, Lemma 4.6 applies, and we reach a contradiction.

Now assume that $a_1 \equiv 1 \pmod 2$. The analogous computation gives

$$\#C(\mathbb{F}_q) \equiv 1 \pmod 2, \quad \#C(\mathbb{F}_{q^2}) \equiv 1 \pmod 4,$$

$$\#C(\mathbb{F}_{q^3}) \equiv 0 \pmod 2, \quad \#C(\mathbb{F}_{q^4}) \equiv 5 \pmod 8,$$

$$\#C(\mathbb{F}_{q^5}) \equiv 0 \pmod 2.$$

Corollary 4.8 applies, and we again reach a contradiction.   □

Remark 4.9 The argument above can be automated, and by iterating over partitions of $2g + 2$, and applying Proposition 4.7, one can rule out Weil polynomials modulo 2, similarly to Proposition 2.10. We have verified that the sets of unrealizable Weil polynomials obtained by these two different procedures agree up to genus $g \leq 10$ by using the Newton identities. Indeed, we expect both sets to match for any g, although we are unable to prove it in general.

5 Experimental Data

The main results of this paper were inspired by experimental data, which we include here to illustrate the phenomena. By performing an exhaustive search, the number of Jacobians of hyperelliptic curves in each isogeny class over $\mathbb{F}_q$ (up to isomorphism of principally polarized abelian varieties) has been computed for threefolds and prime powers $q \leq 13$ that are either prime or odd. Similarly, by iterating over the isomorphism classes of smooth plane quartic curves, the number of isogeny classes of abelian threefolds which contain the Jacobian of a smooth plane quartic curve has been computed for $q = 2, 3$, and 5. Both searches were done by Andrew Sutherland using the techniques developed in [KS08, KS16], and the data have been incorporated in the *L-functions and Modular Forms Database* [LMF19]; see www.LMFDB.org/Variety/Abelian/Fq/.

Table 5.1 Types of Jacobians per isogeny classes of abelian threefolds

q	Contains Jacobian				Total
	Yes	No	Hyperelliptic	Quartic curve	
2	108	107	59	73	215
	50.23%	49.77%	27.44%	33.95%	
3	479	198	297	389	677
	70.75%	29.25%	43.87%	57.46%	
5	2611	342	1723	2471	2953
	88.42%	11.58%	58.35%	83.68%	

By combining these data sets, one can also deduce which isogeny classes of abelian threefolds do not contain a Jacobian for $q = 2, 3$, and 5, see Table 5.1. These data sets, and more precisely the multisets of virtual point counts modulo 2 and 4 that can be extracted from this data, provide motivation for Theorem 2.8.

In Fig. 5.2, we compare the proportion of isogeny classes of abelian threefolds over $\mathbb{F}_q$ which do not contain a hyperelliptic Jacobian for $q \leq 13$ with the proportion of such isogeny classes which are ruled out via Theorem 2.8, giving us some insight into the efficiency of Theorem 2.8 as q grows. Examples of isogeny classes which do not contain a (hyperelliptic) Jacobian but are not ruled out by Theorem 2.8 are given by the following Weil polynomials, cf. isogeny classes 3.3.a_ab_ac and 3.5.ac_j_aw on the LMFDB [LMF19]:

$$Z_1(t) = t^6 - t^4 - 2t^3 - 3t^2 + 27,$$

$$Z_2(t) = t^6 - 2t^5 + 9t^4 - 22t^3 + 45t^2 - 50t + 125.$$

In fact, neither isogeny class contains the Jacobian of any curve. These isogeny classes correspond to the row of Table 2.9 with the most partitions.

In Table 5.3, we present the number of isogeny classes which are ruled out by Theorem 2.8, for $17 \leq q \leq 31$. The data show that the proportion of isogeny classes ruled out by Theorem 2.8 quickly approaches 25%, as expected; see Corollary 3.2. Furthermore, naive extrapolation seems to indicate that the proportion of isogeny classes of abelian threefolds over $\mathbb{F}_q$ which do not contain a hyperelliptic Jacobian approaches 25% from above as $q \to \infty$ ranges over odd prime powers, while the proportion of the isogeny classes that are ruled out via Theorem 2.8 approaches 25% from below. Similarly, in Tables 5.4 and 5.5 we display the number of isogeny classes which cannot contain a hyperelliptic Jacobian by Proposition 2.4, and as before, we observe proportions which are already very close to the ones attained in the q-limit; see Corollary 3.2.

To generate Tables 5.3, 5.4 and 5.5, we enumerated all isogeny classes through their Weil polynomials: First, we enumerated Weil polynomials of degree $2g$, and then we filtered by the Honda–Tate condition on its factors, see [Wat69, Chapter 2], to only keep the ones that correspond to an isogeny class of abelian varieties
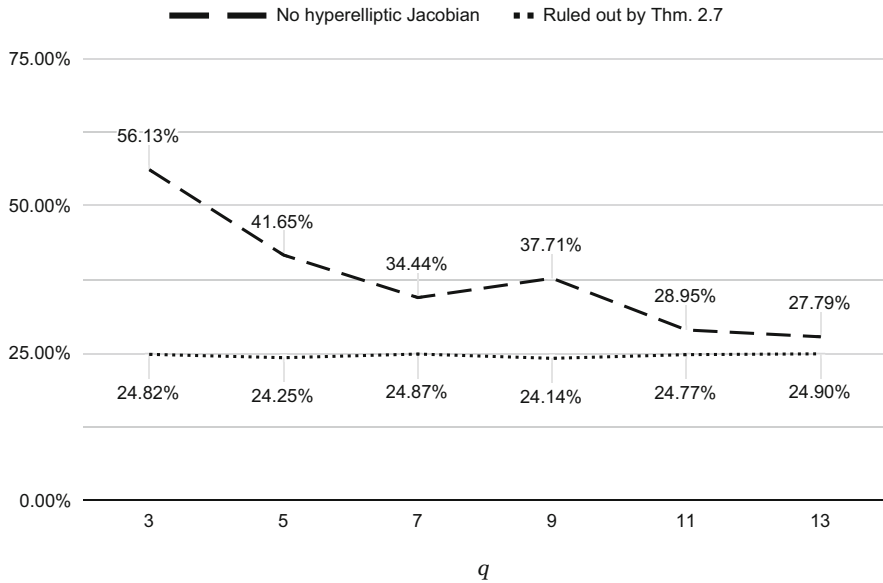
Fig. 5.2 Effectiveness of Theorem 2.8

Table 5.3 Isogeny classes ruled out by Proposition 2.4 for genus 3 and small q

q	17	19	23	25	27	29	31
Number of isogeny classes	112,283	156,589	277,517	332,166	333,695	555,843	678,957
Inadmissible by Theorem 2.8	27,974	39,034	69,268	82,564	83,350	138,730	169,574
	24.91%	24.93%	24.96%	24.86%	24.98%	24.96%	24.98%

Table 5.4 Isogeny classes ruled out by Proposition 2.4 for genus 4 and small q

q	3	5	7	9	11	13	$q \to \infty$
Number of isogeny classes	10,963	132,839	705,593	2,232,114	6,718,947	15,477,119	
Inadmissible by Proposition 2.4	3856	48,910	262,564	829,189	2,513,570	5,794,772	
	35.17%	36.82%	37.21%	37.15%	37.41%	37.44%	37.50%

Table 5.5 Isogeny classes ruled out by Proposition 2.4 in genus 5 and small q

q	3	5	$q \to \infty$
Number of isogeny classes	267,465	11,902,325	
Inadmissible by Proposition 2.4	137,866	6,286,570	
	51.55%	52.82%	53.12%

of dimension g. We enumerated Weil polynomials using *root-unitary*,[1] which implements the techniques introduced in [Ked08].

References

[DH98] Stephen A. DiPippo and Everett W. Howe. Real polynomials with all roots on the unit circle and abelian varieties over finite fields. *J. Number Theory*, 73(2):426–450, 1998.

[DH00] Stephen A. DiPippo and Everett W. Howe. Corrigendum: "Real polynomials with all roots on the unit circle and abelian varieties over finite fields" [J. Number Theory **73** (1998), no. 2, 426–450; MR1657992 (2000c:11101)]. *J. Number Theory*, 83(1):182, 2000.

[FS09] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.

[HNR09] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier (Grenoble)*, 59(1):239–289, 2009.

[Hol04] Joshua Holden. Abelian varieties over finite fields with a specified characteristic polynomial modulo l. *J. Théor. Nombres Bordeaux*, 16(1):173–178, 2004.

[Ked08] Kiran S. Kedlaya. Search techniques for root-unitary polynomials. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 71–81. Amer. Math. Soc., Providence, RI, 2008.

[KS08] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 312–326. Springer, Berlin, 2008.

[KS16] Kiran S. Kedlaya and Andrew V. Sutherland. A census of zeta functions of quartic K3 surfaces over $\mathbb{F}_2$. *LMS J. Comput. Math.*, 19(suppl. A):1–11, 2016.

[LMF19] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2019. [Online; accessed 30 October 2019].

---

[1] https://github.com/kedlaya/root-unitary.

[Mil86] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[MN02] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[Mum07] David Mumford. *Tata lectures on theta. II*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[Nar09] Enric Nart. Counting hyperelliptic curves. *Adv. Math.*, 221(3):774–787, 2009.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.