FROBENIUS ACTION ON JACOBIANS OF CURVES OVER FINITE FIELDS

by

Wanlin Li

A dissertation submitted in partial fulfillment of

the requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN–MADISON

2019

Date of final oral examination: 5/31/2019

The disertation is approved by the following members of the Final Oral Committee:

Jordan Ellenberg, Professor, Mathematics

Nigel Boston, Professor, Mathematics and ECE

Daniel Erman, Associate Professor, Mathematics

Melanie Matchett Wood, Professor, Mathematics

Tonghai Yang, Professor, Mathematics

ABSTRACT

This thesis focuses on studying the eigenvalues of the Frobenius action on the ℓ-adic Tate modules of Jacobians of curves over finite fields. Some of the results have applications to answering questions in analytic number theory over function fields.

The study of zeros of L-functions associated to Dirichlet characters has been a topic of interest in analytic number theory. Questions and conjectures arising there could also be studied in the function field setting. With the field of rational numbers replaced by the field of rational functions over a finite field, those questions are closely related to the study of the Frobenius action on the ℓ-adic Tate modules of Jacobians of curves over finite fields.

Chowla conjectured that the L-function of any quadratic Dirichlet character does not vanish at the central point $s = 1/2$. Soundararajan showed that Chowla's conjecture holds for a positive proportion of quadratic characters ordered by conductor.

Over the function field $\mathbb{F}_q(t)$, the analogous statement can be phrased but the situation can be very different. Quadratic characters correspond to hyperelliptic curves over $\mathbb{F}_q$ and their L-functions are closely related to the Hasse-Weil zeta functions of the curves. To construct quadratic characters whose L-functions vanish at the central point $s = 1/2$ is equivalent to constructing hyperelliptic curves whose Jacobians admit $\sqrt{q}$ as an eigenvalue of the Frobenius action on its ℓ-adic Tate module.

Over any given finite field $\mathbb{F}_q$, I use the Honda-Tate theory and other previous results to show the existence of such hyperelliptic curves which then give quadratic characters over the function field $\mathbb{F}_q(t)$ whose L-functions vanish at the central point $s = 1/2$. This is in contrast with the situation over the rational numbers. Moreover, using a counting result of Poonen on the number of squarefree values of squarefree polynomials over the function field, I give

a lower bound on the number of such characters which grows to infinity when the conductor is allowed to be arbitrarily large.

Although the analogous statement of Chowla's conjecture does not hold over the function field, it is still believed that 100% of the quadratic characters satisfy the condition that their L-functions do not vanish at the central point $s = 1/2$. So in order to approach this conjecture, joint with J. Ellenberg and M. Shusterman, we use the idea of reduction to give an upper bound on the number of quadratic characters whose L-functions vanish at a given point of the critical line. This upper bound gets better when the size of the constant field is large and the density of such characters goes to 0 when the size of the constant field grows to infinity.

Geometrically, we realize the number of hyperelliptic curves whose Jacobians admit some fixed $\alpha \in \mathbb{F}_l^*$ as an eigenvalue of the Frobenius action on its ℓ-torsion subgroup can be counted by the number of rational points of a twisted Hurwitz scheme over finite fields. Using an earlier result of Ellenberg–Venkatesh–Westerland on the homological stability for Hurwitz spaces, we give an upper bound on the number of rational points of the twisted Hurwitz scheme to get the result.

The previous work are all related to studying Weil integers realized as Frobenius eigenvalues for curves over finite fields. From Honda-Tate theory, it is known that every Weil integer appears as a Frobenius eigenvalue for some abelian variety over finite fields. To show the same holds for Jacobian varieties, it suffices to show that every abelian variety over the finite field is covered by a Jacobian variety. This result can be deduced from Poonen's work on the Bertini theorem over finite fields. But there was not an effective bound on the dimension of the Jacobian variety with respect to the degree and dimension of the abelian variety and this is the topic of the last part of my thesis.

Given an abelian variety in a projective space over a finite field, joint with J. Bruce, we show the existence of a smooth curve whose Jacobian admits a dominant map to the given abelian variety with an explicit upper bound on its genus. Applying this to simple abelian varieties combined with the theory of Honda-Tate, one can deduce the existence of smooth

curves whose Jacobians admit some fixed Weil integer as an eigenvalue with an upper bound on its genus.

Chapter 1

Introduction

In [Cho65], Chowla conjectured that L-functions of quadratic Dirichlet characters never vanish at the central point $s = 1/2$. In [Sou00], Soundararajan showed that Chowla's conjecture holds for a positive proportion of quadratic characters ordered by conductor. The analogous question was studied over the rational function field whose constant field is finite by [BF] and they showed that a positive proportion of quadratic characters over the function field satisfy the condition where the corresponding L-functions do not vanish at $s = 1/2$.

In the first part of this thesis, we use the geometric interpretation to construct quadratic characters whose L-functions do vanish at the central point $s = 1/2$. Then we use a counting argument to give a lower bound on the number of such characters which increases with respect to the conductor. Thus, we prove there are infinitely many quadratic characters over the rational functions over finite fields which don't satisfy the analogous statement of Chowla's conjecture. The theorem is stated below.

Theorem 1.1 ([Li18]). *Let $q = p^e$ where p is an odd prime and define sets:*

$$P(N) = \{D \in \mathbb{F}_q[t] : D \text{ monic, squarefree, } |D| < N\}$$
$$g(N) = \{D \in P(N) : L(1/2, \chi_D) = 0\},$$

where χ_D denotes the quadratic character with conductor D. For any $\epsilon > 0$, there exist nonzero constants B_ϵ and N_ϵ, such that

1. *when e is even, $|g(N)| \geq B_\epsilon \cdot N^{1/2-\epsilon}$ for $N > N_\epsilon$.*
2. *when e is odd and $q \neq 3$, $|g(N)| \geq B_\epsilon \cdot N^{1/3-\epsilon}$ for $N > N_\epsilon$.*

3. *when* $q = 3$, $|g(N)| \geq B_\epsilon \cdot N^{1/5-\epsilon}$ *for* $N > N_\epsilon$.

In particular, as $N \to \infty$, $|g(N)|$ *approaches infinity.*

The proof of this theorem is based on the realization that quadratic characters over $\mathbb{F}_q(t)$ whose L-functions vanish at $s = 1/2$ correspond to hyperelliptic curves over $\mathbb{F}_q$ whose Jacobians admit $q^{1/2}$ as a Frobenius eigenvalue. Using Honda–Tate theory and other previous results, such hyperelliptic curves exist for any finite field of odd characteristic. Since any hyperelliptic curve which admits a dominant map to one that having $q^{1/2}$ as a Frobenius eigenvalue will also admit the same property, to construct infinitely many such curves, it suffices to give a lower bound on the number of hyperelliptic curves which admit a dominant map to a fixed one. Thus, we have the following main proposition.

Proposition 1.2 ([Li18])**.** *Let* C_0 *be a hyperelliptic curve of genus* g *defined over* $\mathbb{F}_q$ *where* q *is odd. Assume the existence of a defining equation of* C_0 *as* $y^2 = f(x)$ *where* $\deg f = 2g+2$ *and* f *is reducible or* $\deg f = 2g+1$ *and* f *need not to be reducible. Then for any* $\epsilon > 0$*, there exist positive constants* B_ϵ *and* N_ϵ *such that the number of polynomials* $D \in \mathbb{F}_q[t]$ *satisfying*

- $|D| < N$
- *Curve* $C : s^2 = D(t)$ *admits a dominant map to* C_0

is at least $B_\epsilon \cdot N^{\frac{1}{g+1}-\epsilon}$ *for* $N > N_\epsilon$.

As maps between hyperelliptic curves over finite fields induce rational points on the base change of the target curve to the function field of the source, this proposition can be used to relate our result to ranks of constant elliptic curves in quadratic twist families. In particular, we obtain the following corollaries.

Corollary 1.3 ([Li18])**.** *Let* $E = E_0 \times \mathbb{F}_q(t)$ *be a constant elliptic curve over* $\mathbb{F}_q(t)$*. For any* $D \in \mathbb{F}_q[t]$*, let* E_D *denote the quadratic twist of* E *by* D*. Let* $P(N)$ *be the set* $\{D \in \mathbb{F}_q[t] :$ *monic, squarefree,* $|D| < N\}$*. Let* $R_m(N)$ *be the set* $\{D \in P(N) : \operatorname{rank} E_D \geq m\}$.

Then for any $\epsilon > 0$, there exist nonzero constants B_ϵ and N_ϵ such that

$$|R_2(N)| \geq B_\epsilon N^{1/2-\epsilon}$$

for any $N > N_\epsilon$.

Moreover, if the rank of $\mathrm{End}_{\mathbb{F}_q}(E_0)$ is 4, then we can replace $R_2(N)$ with $R_4(N)$ and the conclusion still holds.

Corollary 1.4 ([Li18]). *For q a square, let E be an elliptic curve over $\mathbb{F}_q$ where*

$$L(s, E) = 1 - 2q^{1/2-s} + q^{1-2s}.$$

Let

$$P'(g) = \{D \in \mathbb{F}_q[t] : \text{ monic, squarefree, of odd degree, } \deg D \leq 2g+1\}.$$

$$R'(g) = \{D \in P'(g) : E_D \text{ has rank } 0\}.$$

Then

$$\lim_{g\to\infty} \frac{|R'(g)|}{|P'(g)|} \geq 0.9427\cdots + o(1).$$

The last corollary gives strong evidence for the minimalist conjecture for this isogeny class of constant elliptic curves. Moreover, the minimalist conjecture for this class of elliptic curves is equivalent to the statement that *almost all* quadratic characters over function fields where the constant field is of square size satisfy the condition that the corresponding L-functions do not vanish at $s = 1/2$. The second part of this thesis is working towards this conjecture.

It is widely believed that not only for $s = 1/2$ but for any fixed $s = \frac{1}{2} + it$, almost all hyperelliptic curves do not have s as a zero of their zeta function. For example, it follows from the work of Chavdarov [Cha97] and Kowalski [Kow06] that for any fixed large g, the proportion of genus g hyperelliptic zeta functions vanishing at s tends to 0 as $q \to \infty$.

But we want to study the limit of this proportion as g grows to infinity. Joint with J.Ellenberg and M. Shusterman, in [ELS], fixing $t \in \mathbb{R}$ and a finite field $\mathbb{F}_q$ of odd characteristic, we give an upper bound on the proportion of genus g hyperelliptic curves over $\mathbb{F}_q$

whose zeta function vanishes at $\frac{1}{2} + it$ and this upper bound is independent of g and tends to 0 as q grows.

The main idea to prove this result is the study of L-functions modulo ℓ. The value of an L-function over $\mathbb{F}_q(x)$ at a complex number s can be expressed as a polynomial $P(T) \in \mathbb{Z}[T]$, where $T = q^{-s}$. So if we want to prove that $P(T)$ is nonvanishing, it suffices to prove that $P(T)$ is nonvanishing modulo ℓ for some prime ℓ. We show that, for suitably chosen ℓ, the vanishing mod ℓ of the L-function is related to the dimension of a certain Frobenius eigenspace in the ℓ-torsion of a hyperelliptic Jacobian over $\mathbb{F}_q$; the average size of this eigenspace can then be controlled by a modest generalization of the arguments in [EVW16].

While working towards this result, we observe that under some conditions on Weierstrass points, the L-function of χ_f is nonvanishing mod 2 at $s = 1/2$. Thus, we get the following theorem.

Theorem 1.5 ([ELS]). *Let C be a hyperelliptic curve of genus at least 2 over $\mathbb{F}_q$ and S be the set of Weierstrass points of C. The Frobenius acts on S by permuting the $2g+2$ Weierstrass points via some permutation π. Suppose that either*

- *g is even and π is a $(2g+2)$-cycle; or*
- *π is the product of two disjoint cycles of odd length.*

Then:

1. *The point $s = \frac{1}{2}$ is not a zero of Z_C.*
2. *All zeros of Z_C are of multiplicity at most 2. Moreover, if π is the product of two disjoint cycles of* coprime *odd length, all zeros of Z_C are simple.*

By giving an upper bound on the multiplicity of the zeros of Z_C, we obtain further information on nonvanishing at $s = \frac{1}{2}$. In the language of Dirichlet characters, this implies in particular the nonvanishing (at the central point) in the case of prime conductor of degree

not divisible by 4. (When the degree of the conductor is odd, one Weierstrass point is at ∞ and π consists of a fixed point and a cycle of length $2g+1$.) Thus there is an explicit set of size on order $X/\log X$ of Dirichlet characters of size at most X which have L-functions nonvanishing at the critical point; this improves on [AK13, Corollary 2.6] of Andrade and Keating and on [ABJ16, Corollary 2.8] of Andrade, Bae, and Jung, which give a proportion on order $(\log X)^{-2}$, and goes beyond the methods of [AB18].

The previous results are deduced from the study of Frobenius eigenvalues for hyperelliptic curves over finite finite fields. So in the third part of the thesis, we further move on to study the existence of smooth curves over finite fields whose Jacobians admit some certain Weil integer as a Frobenius eigenvalue. Joint with J. Bruce, in [BL18], we show that any abelian variety over a finite field is covered by a Jacobian whose dimension is bounded by an explicit constant. We do this by first proving an effective and explicit version of Poonen's Bertini theorem over finite fields, which allows us to show the existence of smooth curves arising as hypersurface sections of bounded degree and genus. Additionally, for simple abelian varieties we prove a better bound. The precise statement is the following.

Theorem 1.6 ([BL18])**.** *Fix $r, n \in \mathbb{N}$ with $n \geq 2$, and let $\mathbf{F}_q$ be a finite field of characteristic p. There exists an explicit constant*[1] *$C_{r,q}$ such that if $A \subset \mathbb{P}^r_{\mathbf{F}_q}$ is a non-degenerate abelian variety of dimension n, then for any $d \in \mathbb{N}$ satisfying*

$$C_{r,q}\zeta_A\left(n+\tfrac{1}{2}\right)\deg(A) \leq \frac{q^{\frac{d}{\max\{n+1,p\}}}(d+1)}{d^{n+1}+d^n+q^{\frac{d}{\max\{n+1,p\}}}},$$

there exists a smooth geometrically connected curve over $\mathbf{F}_q$ whose Jacobian J maps dominantly onto A, where

$$\dim J \leq \left\lfloor \frac{\deg(A)d^{n-1}-1}{r-1} \right\rfloor \left(\deg(A)d^{n-1} - \frac{\left\lfloor \frac{\deg(A)d^{n-1}-1}{r-1} \right\rfloor + 1}{2}(r-1) - 1 \right).$$

Moreover, if $A \subset \mathbb{P}^r_{\mathbf{F}_q}$ is simple, then for any $d \in \mathbb{N}$ satisfying

$$\deg(A) \leq \frac{(d-1)q^{\frac{1}{2}(d+1)(d+2)}}{d^{n-1}-1},$$

[1] See Proposition 4.13 for a more precise statement where the constant is explicitly stated.

there exists a smooth geometrically connected curve over $\mathbf{F}_q$ *whose Jacobian* J *maps dominantly onto* A*, where*

$$\dim J \leq \deg(A) d^{n-1} \left(\deg(A) d^{n-1} + 1 \right).$$

Acknowledgments

I would like to thank my advisor, Jordan Ellenberg, for all of his guidance and support during my graduate school years. In addition I'd like to thank the rest of my thesis committee: Nigel Boston, Daniel Erman, Melanie Matchett Wood and Tonghai Yang.

I would like to thank all of those who have helped in the writing of the three papers this thesis is based off of, in particular my collaborators, Juliette Bruce, Jordan Ellenberg and Mark Shusterman.

Chapter 2

Vanishing of hyperelliptic L-functions at the central point

[1]

2.1 Introduction

S. Chowla conjectured in [Cho65] that, for any real non-principal Dirichlet character χ, $L(s,\chi) \neq 0$ for all $s \in (0,1)$. In particular, his conjecture asserts that L-functions of quadratic characters never vanish at the central point $s = 1/2$.

Although this conjecture is still open, much progress has been made. K. Soundararajan [Sou00] proved that at least 87.5% of odd squarefree positive integers d have the property $L(1/2, \chi_{8d}) \neq 0$ where χ_{8d} denotes the quadratic character with conductor $8d$.

In this paper, we consider the analogue of Chowla's conjecture obtained by replacing the field of rational numbers with the field of rational functions over a finite field.

Let $q = p^e$ be a power of an odd prime p and $\mathbb{F}_q$ the finite field with q elements. Let $k = \mathbb{F}_q(t)$ denote the field of rational functions over $\mathbb{F}_q$. The primes of k are represented by monic irreducible polynomials in $\mathbb{F}_q[t]$ except the one prime at infinity.

A quadratic character of k corresponds to a squarefree polynomial in $\mathbb{F}_q[t]$. Explicitly, take $D \in \mathbb{F}_q[t]$ to be a squarefree polynomial and $K = k(\sqrt{D})$ the quadratic extension of k by joining $\sqrt{D}$. Then we can define a quadratic character χ_D as follows:

[1] This chapter is based on the contents of [Li18]

For P a prime of k,

$$\chi_D(P) = \begin{cases} 1 & P \text{ splits in } K \\ -1 & P \text{ is inert in } K \\ 0 & P \text{ ramifies in } K \end{cases}$$

We define the L-function associated to χ_D as

$$L(s, \chi_D) = \prod_P (1 - \chi_D(P)|P|^{-s})^{-1}$$

where the product is taken over the primes represented by polynomials P and $|P| = q^{degP}$.

Definition 2.1. *Define sets:*

$$P(N) = \{D \in \mathbb{F}_q[t] : D \text{ monic, squarefree, } |D| < N\}$$
$$g(N) = \{D \in P(N) : L(1/2, \chi_D) = 0\}.$$

Remark 2.2. Note that in the definition above, we have restricted ourselves to characters corresponding to monic squarefree polynomials which is half of all quadratic characters. But since we only study the density in this paper, such restriction won't affect our results.

Under this definition, the analogue of Chowla's conjecture states that $g(N)$ is empty for any N. There are some results towards this statement.

Bui and Florea [BF] showed for a fixed finite field $\mathbb{F}_q$ with odd characteristic, as $N \to \infty$,

$$|g(N)| \ll 0.057N + o(1)$$

where $N = q^{2n+1}$ for some $n > 0$.

The purpose of this paper is to show that the analogue of Chowla's conjecture over $\mathbb{F}_q(t)$ is not correct and to give a lower bound on the number of counterexamples with bounded height.

Theorem 2.3. *Let $q = p^e$ and let $g(N)$ be the set defined in Definition 2.1. For any $\epsilon > 0$, there exist nonzero constants B_ϵ and N_ϵ, such that*

1. *when e is even, $|g(N)| \geq B_\epsilon \cdot N^{1/2-\epsilon}$ for $N > N_\epsilon$.*
2. *when e is odd and $q \neq 3$, $|g(N)| \geq B_\epsilon \cdot N^{1/3-\epsilon}$ for $N > N_\epsilon$.*
3. *when $q = 3$, $|g(N)| \geq B_\epsilon \cdot N^{1/5-\epsilon}$ for $N > N_\epsilon$.*

In particular, as $N \to \infty$, $|g(N)|$ approaches infinity.

Remark 2.4. Although Chowla's conjecture is not strictly true over $\mathbb{F}_q(t)$, it may hold for *almost all* quadratic characters, i.e. it may be the case that $|g(N)|/N \to 0$ as $N \to \infty$.

Outline of the Chapter. In section 2, we give a geometric interpretation for the vanishing of a quadratic L-function at the central point. In section 3, we show a lower bound on the number of hyperelliptic curves which admit a dominant map to some fixed curve. In section 4, we describe an application of our main theorem to give a lower bound on the number of elliptic curves with elevated ranks in certain quadratic twist families. In section 5, we provide the proof of Theorem 2.3. In section 6, we present some of the data we collected using Magma on this problem.

2.2 Geometric Interpretation of Vanishing at the Central Point

Let D be a monic squarefree polynomial over $\mathbb{F}_q$. Then $y^2 = D$ is a hyperelliptic curve defined over $\mathbb{F}_q$ which we denote by C from now on. The field $K = k(\sqrt{D})$ as defined before is the function field of C.

Let $P(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of geometric Frobenius acting on the Jacobian $J(C)$.

Then we get

$$P(q^{-s}) = (1 - q^{-s})^{\lambda_D} L(s, \chi_D)$$

where

$$\lambda_D = \begin{cases} 1 & \deg D \text{ even} \\ 0 & \deg D \text{ odd} \end{cases}$$

By the Riemann Hypothesis for curves over finite fields, we have a factorization

$$P(x) = \prod_{j=1}^{2g}(1 - x\pi_j)$$

where g is the genus of C and π_j an algebraic integer with $|\pi_j| = q^{1/2}$ under every complex embedding.

The following lemma is now immediate.

Lemma 2.5. *Let D be a monic squarefree polynomial in $\mathbb{F}_q[t]$ and χ_D be the quadratic character associated to D. Let C be the hyperelliptic curve defined by $y^2 = D$, $P \in \mathbb{Z}[x]$ the characteristic polynomial of geometric Frobenius acting on the Jacobian of C and $\pi_1, \ldots, \pi_{2g}$ the eigenvalues of this action. Then the following statements are equivalent:*

- $L(1/2, \chi_D) = 0$.
- $P(q^{-1/2}) = 0$.
- $\pi_j = q^{1/2}$ *for some* j.

Algebraic integers with all Archimedean absolute values equal to $q^{1/2}$ are called Weil integers. The theorem of Honda–Tate states every Weil integer is an eigenvalue of the geometric Frobenius acting on some simple abelian variety over $\mathbb{F}_q$.

Theorem 2.6 (Honda–Tate [Eis], [Hon68])**.** *Let A be an abelian variety defined over $\mathbb{F}_q$ and π_A an eigenvalue of the geometric Frobenius endomorphism of A. The map $A \mapsto \pi_A$ defines a bijection between the $\mathbb{F}_q$-isogeny classes of abelian varieties defined and simple over $\mathbb{F}_q$ and Galois conjugacy classes of Weil integers.*

In particular, Honda–Tate guarantees the existence and uniqueness of an isogeny class of simple abelian varieties over $\mathbb{F}_q$ with $q^{1/2}$ being an eigenvalue of the Frobenius. We denote a representative of this class by A_q.

Now we want to find hyperelliptic curves whose Jacobians have $q^{1/2}$ as a Frobenius eigenvalue. Any curve C with a nonconstant map to A_q has A_q as an isogeny quotient of

$J(C)$, which implies C has $q^{1/2}$ as a Frobenius eigenvalue. A theorem of Tate guarantees the converse also holds.

Theorem 2.7 (Tate [Eis] , [Mum08])**.** *Let A and B be abelian varieties defined over $\mathbb{F}_q$ and let f_A, $f_B \in \mathbb{Z}[T]$ be characteristic polynomials of geometric Frobenius on A and B. Then the following are equivalent:*

1) B is $\mathbb{F}_q$-isogenous to a sub-abelian variety of A;

2) $f_B \mid f_A$ in $\mathbb{Q}[T]$.

Proposition 2.8. *Let C be a hyperelliptic curve defined over $\mathbb{F}_q$, then $q^{1/2}$ is an eigenvalue for geometric Frobenius acting on $J(C)$ if and only if A_q is $\mathbb{F}_q$-isogenous to a sub-abelian variety of $J(C)$.*

Proof. By the theorem of Honda–Tate, there is a unique isogeny class of simple abelian varieties over $\mathbb{F}_q$ having $q^{1/2}$ as a Frobenius eigenvalue, i.e. the class containing A_q. Since $J(C)$ can be decomposed up to isogeny uniquely as products of simple abelian varieties over $\mathbb{F}_q$, by the theorem of Tate, $q^{1/2}$ being a Frobenius eigenvalue for $J(C)$ is equivalent to $J(C)$ having a simple factor isogenous to A_q. □

Proposition 2.9. *$L(1/2, \chi_D) = 0$ if and only if the hyperelliptic curve $C : y^2 = D$ admits a nontrivial map to A_q.*

Proof. By Lemma 2.5 and Proposition 2.8, $L(1/2, \chi_D) = 0$ if and only if A_q is $\mathbb{F}_q$-isogenous to a sub-abelian variety of $J(C)$.

Thus, equivalently there is a dominant map $J(C) \to A_q$ over $\mathbb{F}_q$.

And as long as we have a map $C \to J(C)$ over $\mathbb{F}_q$ such that the image doesn't lie in any coset of the kernel of the projection to A_q, the composition gives a nonconstant morphism from C to A_q.

To construct such a map, we just need to take the canonical class ω_C and define

$$C \to J(C)$$
$$P \mapsto (2g-2)P - \omega_C$$

Then the image of $C\left(\overline{\mathbb{F}}_q\right)$ under this map generates $J(C)$ as a group. Thus it is not contained in the kernel of $J(C) \to A_q$ and intersect the kernel non-trivially. This shows the existence of a nontrivial map from C to A_q.

Conversely, if there exists a nontrivial map from C to A_q, it factors through the Albanese variety of C which is the dual abelian variety of $J(C)$. Since Jacobian varieties are self-dual, this induces a nontrivial map from $J(C)$ to A_q. Since A_q is $\mathbb{F}_q$-simple, this map is surjective. This implies that the map from C to A_q is surjective as desired. □

Proposition 2.9 supplies a geometric condition equivalent to our algebraic statement $L(1/2, \chi_D) = 0$. All we need is to use this geometric condition to construct desired polynomials D.

2.3 Maps Between Hyperelliptic Curves

In this section, we prove the following result which provides a lower bound for the number of hyperelliptic curves of bounded genus covering a fixed hyperelliptic curve over a finite field of odd characteristic.

Proposition 2.10. *Let C_0 be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ where q is odd. Assume the existence of a defining equation of C_0 as $y^2 = f(x)$ where $\deg f = 2g+2$ and f is reducible or $\deg f = 2g+1$ and f need not to be reducible. Then for any $\epsilon > 0$, there exist positive constants B_ϵ and N_ϵ such that the number of polynomials $D \in \mathbb{F}_q[t]$ satisfying*

- $|D| < N$
- *Curve $C : s^2 = D(t)$ admits a dominant map to C_0*

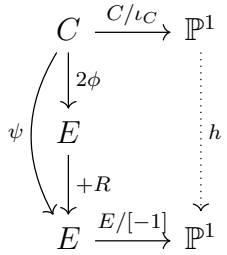
is at least $B_\epsilon \cdot N^{\frac{1}{g+1}-\epsilon}$ for $N > N_\epsilon$.

The restriction on the form of the defining equation of C_0 is only used for the proof of Proposition 2.10. Lemma 2.11 and 2.12 hold for general hyperelliptic curves.

The proposition is based on two lemmas relating maps between hyperelliptic curves to maps from $\mathbb{P}^1$ to $\mathbb{P}^1$. The treatment is slightly different when the base curve is an elliptic

curve and when the base curve has higher genus, we treat the two cases separately, in Lemma 2.11 and Lemma 2.12 respectively.

Lemma 2.11. *Let $\phi : C \to E$ be a dominant map from a hyperelliptic curve to an elliptic curve over a field k where char $k \neq 2$. Let C/ι_C be the degree 2 map from C to $\mathbb{P}^1$ induced by the hyperelliptic involution and $E/[-1]$ be the degree 2 map from E to $\mathbb{P}^1$ induced by the elliptic involution. Then there exists a dominant map $\psi : C \to E$ together with a map $h(x) : \mathbb{P}^1 \to \mathbb{P}^1$ and a point $R \in E(k)$ such that the following diagram commutes.*



Proof. Take any point P on C and denote $\overline{P} = \iota_C(P)$; then $P + \overline{P}$ is linearly equivalent to $P' + \overline{P'}$ for any point P' on C.

We have

$$\phi(P) + \phi(\overline{P}) = \phi(P') + \phi(\overline{P'}) = R$$

where R is a k-point of E.

Define ψ by the rule $\psi(P) = 2\phi(P) - R$.

Thus

$$\psi(P) + \psi(\overline{P}) = 2\phi(P) - R + 2\phi(\overline{P}) - R = O$$

which means it is equivariant for the two involutions as desired.

□

Lemma 2.12. *Let C_1 and C_2 be hyperelliptic curves with genus greater than 1 over a field k where char $k \neq 2$. Let $\psi : C_1 \to C_2$ be a dominant map from C_1 to C_2. Then there exists a rational function h over k such that the following diagram commutes:*

$$\begin{array}{ccc} C_1 & \xrightarrow{C_1/\iota_1} & \mathbb{P}^1 \\ \downarrow{\scriptstyle \psi} & & \vdots{\scriptstyle h} \\ C_2 & \xrightarrow{C_2/\iota_2} & \mathbb{P}^1 \end{array}$$

where ι_1 and ι_2 are the hyperelliptic involutions on C_1 and C_2.

Proof. Let C be a hyperelliptic curve of genus greater than 1 and let W be a Weierstrass point of C.Then the fiber over $2W$ in $\mathrm{Pic}^2(C)$ of the natural map $\mathrm{Sym}^2(C) \to \mathrm{Pic}^2(C)$ is given by divisors of form $P + \overline{P}$ where $\overline{P}$ denotes the image of P under the hyperelliptic involution.

Note that for an elliptic curve, every point is Weierstrass and thus $2W$ doesn't specify a unique divisor class in $\mathrm{Pic}^2(C)$.

Thus considering ψ induces a map from $\mathrm{Pic}^2(C_2)$ to $\mathrm{Pic}^2(C_1)$, a pair of conjugate points on C_1 get mapped to a pair of conjugate points on C_2. □

Proposition 2.13. *There exists a dominant map from a hyperelliptic curve $C : s^2 = D(t)$ where $D(t) \in \mathbb{F}_q[t]$ to a hyperelliptic curve $C_0 : y^2 = f(x)$ where $f(x) \in \mathbb{F}_q[x]$ if and only if the quadratic twist $Dy^2 = f(x)$ has a nontrivial rational point (x_0, y_0) over $\mathbb{F}_q(t)$.*

Proof. By the previous two lemmas 2.11 and 2.12, if a dominant map exists, C has a defining equation of the form $s^2 = f(h(t))$ for some rational function $h(t)$ in $\mathbb{F}_q(t)$. Thus, there exists $p(t) \in \mathbb{F}_q(t)$ such that

$$D(p(t))^2 = f(h(t))$$

which is saying

$$(x_0, y_0) = (h(t), p(t))$$

satisfies

$$Dy_0^2 = f(x_0).$$

On the other hand, if there exists a point (x_0, y_0) on the curve defined by $Dy^2 = f(x)$, then we have a dominant map $(t, s) \mapsto (x_0, y_0 s)$ from C to C_0. □

From Proposition 2.13, our question about squarefree polynomials $D \in \mathbb{F}_q[t]$ with curve defined by $s^2 = D(t)$ admitting a dominant map to a hyperelliptic curve of genus g defined by $y^2 = f(x)$ is exactly the same as asking for nontrivial solutions of the equation $Dy^2 = f(x)$ over the function field $\mathbb{F}_q(t)$.

Let

$$h(t) = u(t)/v(t) \in \mathbb{F}_q(t),$$

where $u(t)$, $v(t) \in \mathbb{F}_q[t]$ and $p(t) \in \mathbb{F}_q(t)$.

If we have $Dp^2 = f(h)$, then we get

$$Dp^2 v^{2g+2} = v^{2g+2} f(u/v) \in \mathbb{F}_q(t)[u, v]$$

which is a degree $2g+2$ homogeneous polynomial in u, v and is denoted by $F(u, v)$ from now on.

Thus D is the squarefree part of $F(u, v)$ in $\mathbb{F}_q[t]^*/(\mathbb{F}_q[t]^*)^2$ for some $u, v \in \mathbb{F}_q[t]$ and we can give a bound on the number of D by estimating the number of squarefree values taken by $F(u, v)$.

The main tool in our lower bound is a theorem of Poonen showing that squarefree polynomials over a localization of a polynomial ring take many squarefree values.

Proposition 2.14. *(Poonen [Poo03])*
Let P be a finite set of primes in $\mathbb{F}_q[t]$, A be the localization of $\mathbb{F}_q[t]$ by inverting the primes in P, $K = \mathbb{F}_q(t)$, $f \in A[x_1, \ldots, x_m]$ be a polynomial that is squarefree as an element of $K[x_1, \ldots, x_m]$ and for a choice of $x \in \mathbb{F}_q[t]^m$, we say that $f(x)$ is squarefree in A if $(f(x))$ is a product of distinct primes in A. For $a \in A$, define $|a| = |A/a|$ and for $a \in A^n$, define $|a| = \max |a_i|$. Let

$$S_f := \{x \in \mathbb{F}_q[t]^m : f(x) \text{ is squarefree in } A\}$$

and

$$\mu_{S_f} := \lim_{N \to \infty} \frac{|\{a \in S_f : |a| < N\}|}{N^m}$$

For each nonzero prime p of A, let c_p be the number of $x \in (A/p^2)^m$ that satisfy $f(x) = 0$ in A/p^2.

Then the limit μ_{S_f} exists and is equal to $\prod_p(1 - c_p/|p|^{2m})$.

Proof. This proposition follows Theorem 8.1 of [Poo03] by setting the "box" to be $\{u, v \in \mathbb{F}_q[t] : |u|, |v| < N\}$. □

Remark 2.15. *Proposition 2.14 only helps us if $\mu_{S_f} > 0$. In order to ensure this, it suffices to check that none of the factors $(1 - c_p/|p|^{2m})$ is zero where we take $m = 2$ for our case.*

If for some prime π in $\mathbb{F}_q(t)$, $1 - c_\pi/|\pi|^4 = 0$, then this means $F(u, v) \mod \pi^2$ vanishes for all $(u, v) \in (\mathbb{F}_q[t])^2$. Thus $F(u, v) \mod \pi$ vanishes for all $(u, v) \in (\mathbb{F}_q[t]/\pi)^2$. Since the coefficients of F are units in $\mathbb{F}_q[t]$, $F \mod \pi$ is not the zero polynomial. This implies it can at most have $\deg F|\mathbb{F}_q[t]/\pi|$ solutions over $\mathbb{F}_q[t]/\pi$. So

$$\deg F|\mathbb{F}_q[t]/\pi| \geq |\mathbb{F}_q[t]/\pi|^2$$

which is equivalent to $\deg F \geq |\pi|$.

Thus, we choose P_f be the set of primes P of $\mathbb{F}_q(t)$ such that $|P| < n$. Let A be the localization of $\mathbb{F}_q[t]$ by inverting primes in P_f. This implies $1 - c_p/|p|^4 \neq 0$ for any prime p in A. So is their product.

We now have all the tools we need for the proof of Proposition 2.10.

Proof of Proposition 2.10. Let $y^2 = f(x)$ be the defining equation for C_0 stated in the Proposition. Fix a factorization of $f(x)$ as follows:

If $\deg f = 2g + 2$, then by the condition of the proposition, f is squarefree and reducible. Fix a nontrivial factorization $f = f_1 f_2$ where $\gcd(f_1, f_2) = 1$.

If $\deg f = 2g + 1$, let the the factorization $f = f_1 f_2$ be the trivial one where $f_1 = f$ and $f_2 = 1$.

Let $n = 2g+2$. Given $u, v \in \mathbb{F}_q[t]$, define $F(u, v) = v^n f(u/v)$ which is a squarefree homogeneous polynomial in $\mathbb{F}_q[t][u, v]$. Then the factorization of f induces a natural factorization $F = F_1 F_2$ where

$$F_1(u, v) = v^{\deg f_1} f_1(u/v)$$

$$F_2(u,v) = v^{n-\deg f_1} f_2(u/v).$$

Recall Definition 2.1

$$P(N) = \{D \in \mathbb{F}_q[t] : D \text{ monic, squarefree, } |D| < N\}$$

Define set

$$G(N) = \{D \in P(N) : \text{curve } y^2 = D \text{ admits a dominant map to } C_0\}$$

Let the set A be defined as in Remark 2.15. Suppose u and v are elements of $\mathbb{F}_q[t]$ such that $F(u,v)$ is squarefree in A, take $D \in \mathbb{F}_q[t]$ to be the squarefree part of $F(u,v)$ in $\mathbb{F}_q[t]$; then the curve $Dy^2 = f(x)$ has a point $(u/v, a/v^{n/2})$ over $K = \mathbb{F}_q(t)$ where a is a unit in A. By Proposition 2.13, this implies curve $y^2 = D$ admits a dominant map to C_0.

For pairs (u,v) with $|u|, |v| < N^{1/n}$, we get $|F(u,v)| < N$.

Thus, we can define a subset of $G(N)$ as:

$$G'(N) = \{D \in P(N) : \exists u, v \in \mathbb{F}_q[t], |u|, |v| < N^{1/n} \text{ and } F(u,v) = a^2 D\}$$

where a is a unit in A.

Define set $W(N)$ as follows:

$$W(N) = \{(u,v) \in \mathbb{F}_q[t] : F(u,v) \text{ squarefree in } A, |u|, |v| < N^{1/n}\}.$$

We have an explicit surjective map from $W(N)$ to $G'(N)$.

$$\phi : (u,v) \mapsto D$$

where D is the squarefree part of $F(u,v)$ in $\mathbb{F}_q[t]$.

By Proposition 2.14,

$$\lim_{N\to\infty} \frac{|W(N)|}{N^{2/n}} \gg \mu_{S_f} > 0$$

Now to give a lower bound on the size of $G'(N)$, we need to give an upper bound on the size of each fiber of ϕ.

For each fixed $D \in G'(N)$, want to count pairs (u, v) with $F(u, v) = a^2 D$ for some unit a. Since $F = F_1 F_2$, for each a, there exist decompositions $D_1 D_2 = a^2 D$ such that

$$F_1(u, v) = D_1$$

$$F_2(u, v) = D_2$$

By construction, we have that F_1 and F_2 are coprime. So there are fewer than n^2 solutions for each pair of equations by Bezout's theorem and there are at most $d(a^2 D)$ such decompositions for each a where $d(a^2 D)$ denotes the number of factors of $a^2 D$ in $\mathbb{F}_q[t]$.

For each $(u, v) \in W(N)$, $|F(u, v)| \leq N$. Thus, we can give an upper bound for $d(a^2 D)$ by letting $c(N) = \max\{d(X) : X \in \mathbb{F}_q[t], |X| < N\}$.

For each fixed $D \in G'(N)$, the size of $\phi^{-1}(D)$ is bounded above by $n^2 c(N)$.

Then for any N,

$$|G'(N)| \geq \frac{|W(N)|}{n^2 c(N)}$$

Since $d(X) < |X|^\epsilon$ for any $\epsilon > 0$ and $X \in \mathbb{F}_q[t]$ when $|X|$ is sufficiently large, we get

$$|G(N)| \geq |G'(N)| \geq \frac{|W(N)|}{n^2 c(N)} \gg \frac{\mu_{S_f}}{c_\epsilon} N^{2/n - \epsilon}$$

where c_ϵ is a constant depending on ϵ.

□

2.4 A View Toward Ranks of Elliptic Curves

We start by recalling some standard definitions.

Definition 2.16. *An elliptic curve E defined over $\mathbb{F}_q(t)$ is constant if it can be defined by a Weierstrass form with coefficients in $\mathbb{F}_q$.*

An elliptic curve E defined over $\mathbb{F}_q(t)$ is isotrivial if there is a finite extension L of $\mathbb{F}_q(t)$ such that E becomes constant over L. Equivalently, E is isotrivial if and only if $j(E) \in \mathbb{F}_q$.

Proposition 2.17 (Proposition 6.1 of [Ulm11])**.** *Let E_0 be an elliptic curve over $k = \mathbb{F}_q$. Let K be the function field $k(C)$ of a curve C over k. Let $E_K = E_0 \times_k K$.*

There is a canonical isomorphism

$$E_K(K) \cong \mathrm{Mor}_k(C, E_0)$$

where Mor_k *denotes morphisms of* k*-schemes. Under this isomorphism,* $E_K(K)_{tor}$ *corresponds to the subgroup of constant morphisms.*

Corollary 2.18 (Corollary 6.2 of [Ulm11])**.** *Let* $J(C)$ *be the Jacobian of* C*. Then we have canonical isomorphisms of abelian groups*

$$E_K(K)/(E_K(K))_{tor} \cong \mathrm{Hom}_{k-av}(J(C), E_0) \cong \mathrm{Hom}_{k-av}(E_0, J(C))$$

where Hom_{k-av} *denotes morphisms of abelian varieties over* k*.*

Proposition 2.19. *Let* $E = E_0 \times \mathbb{F}_q(t)$ *be a constant elliptic curve over* $\mathbb{F}_q(t)$*. For any* $D \in \mathbb{F}_q[t]$*, let* E_D *denote the quadratic twist of* E *by* D*. Let* $P(N)$ *be the set* $\{D \in \mathbb{F}_q[t] :$ *monic, squarefree,* $|D| < N\}$ *as in Definition 2.1. Let* $R_m(N)$ *be the set* $\{D \in P(N) :$ $\operatorname{rank} E_D \geq m\}$*.*

Then for any $\epsilon > 0$*, there exist nonzero constants* B_ϵ *and* N_ϵ *such that*

$$|R_2(N)| \geq B_\epsilon N^{1/2-\epsilon}$$

for any $N > N_\epsilon$*.*

Moreover, if the rank of $\mathrm{End}_{\mathbb{F}_q}(E_0)$ *is* 4*, then we can replace* $R_2(N)$ *with* $R_4(N)$ *and the conclusion still holds.*

Proof. By Proposition 2.10, for any $\epsilon > 0$, there exists a nonzero constant B_ϵ such that at least $B_\epsilon N^{1/2-\epsilon}$ hyperelliptic curves $y^2 = D$ with $|D| < N$ admit a dominant map to E_0 when N is large.

By Proposition 2.17, Corollary 2.18 and Poincaré complete reducibility [Ulm11], for such D, $\operatorname{rank} E_D \geq \operatorname{rank} \mathrm{End}(E_0)$.

Since our ground field is of positive characteristic, the endomorphism ring of E_0 has rank 2 or 4. □

Proposition 2.20. *Let $E = E_0 \times \mathbb{F}_q(t)$ be a constant elliptic curve over $\mathbb{F}_q(t)$ where $E_0[2](\mathbb{F}_q) \neq O$. When $p \neq 2$, $q \neq 3, 9$ and $a^2 - 4q \notin \{-3, -4, -7\}$ where a is the trace of geometric Frobenius acting on the Tate module, we have the following.*

Let $P(N) = \{D \in \mathbb{F}_q[t] : \text{ monic, squarefree, } |D| < N\}$.

Let $R_m(N)$ be the set $\{D \in P(N) : \text{rank } E_D \geq m\}$.

Then for any $\epsilon > 0$, there exist nonzero constants B_ϵ and N_ϵ such that

$$|R_4(N)| \geq B_\epsilon N^{1/3-\epsilon}$$

for any $N > N_\epsilon$.

Moreover, if the rank of $\mathrm{End}_{\mathbb{F}_q}(E_0)$ is 4, then we can replace R_4 with R_8 and the conclusion holds.

Proof. By [HNR09], we know when the conditions on p, q, $a^2 - 4q$ in the statement of the proposition are satisfied, there exists a Jacobian variety isogenous to $E_0 \times E_0$ over $\mathbb{F}_q$. This Jacobian variety corresponds to a genus 2 curve C. We now show that C has a defining equation that satisfies the condition for Proposition 2.10.

Let $y^2 = f(x)$ be a defining equation for C and assume $\deg f = 6$.

Denote the roots of f by $x_1, \ldots, x_6$. Then the 2-torsion group of $J(C)$ is generated by divisors $(x_1, 0) - (x_i, 0)$ where $i = 2, 3, 4, 5$. Thus, using this basis, from the action on $x_1, \ldots, x_6$, we get the matrix representation of the Frobenius action on $J(C)[2] \simeq (\mathbb{F}_2)^4$. If Frobenius acts on the roots transitively, then the characteristic polynomial of the action on the $\mathbb{F}_2$ vector space is $x^4 + x^2 + 1$.

Since we know the characteristic polynomial of Frobenius acting on the Tate module of $J(C)$ is $(1 - ax + qx^2)^2$, we see that the action of Frobenius on $J(C_0)[2]$ has characteristic polynomial $x^4 + 1$ when a is even. And a is even if and only if condition $E_0[2](\mathbb{F}_q) \neq O$ holds. Thus Frobenius doesn't act transitively on the Weierstrass points of curve C.

Since Frobenius doesn't act transitively on the Weierstrass points of C, it has a defining equation of the form $y^2 = f(x)$ where f is not irreducible.

By Proposition 2.10, for any $\epsilon > 0$, at least $B_\epsilon N^{1/3-\epsilon}$ hyperelliptic curves $y^2 = D$ with $|D| < N$ admit a dominant map to this fixed genus 2 curve when N is sufficiently large.

For these D, rank $E_D \geq 2$ rank $End(E_0)$.

Since our ground field is of positive characteristic, End(E_0) has rank 2 or 4 which gives rank 4 and 8 for quadratic twists E_D. □

From the geometric interpretation of L-functions, we know $L(1/2, \chi_D) = 0$ if and only if there exists a dominant map from the hyperelliptic curve defined by $C : y^2 = D$ to E_0. Using the statements above, this condition is equivalent to the quadratic twist of the constant elliptic curve $E_0 \times \mathbb{F}_q(t)$ by D having positive rank.

More precisely, we have the following proposition.

Proposition 2.21. *For q a square, let E_0 be an elliptic curve which admits $\sqrt{q}$ as a Frobenius eigenvalue.*

Denote by E the base change of E_0 to the function field $\mathbb{F}_q(t)$.

Denote by E_D be the quadratic twist of E by D where D is a squarefree polynomial in $\mathbb{F}_q[t]$.

Recall the definitions

$$P(N) = \{D \in \mathbb{F}_q[t] : D \text{ monic, squarefree, } |D| < N\}$$
$$g(N) = \{D \in P(N) : L(1/2, \chi_D) = 0\}$$

Let $R_m(N)$ be the set $\{D \in P(N) : \text{rank } E_D \geq m\}$.

Then $g(N) = R_2(N)$.

Proof. Let D be a monic, squarefree polynomial in $\mathbb{F}_q[t]$ and C the hyperelliptic curve defined by $y^2 = D$. Let K be the function field $k(C)$ of C and $E_K = E_0 \times_k K$.

Let $J(C)$ be the Jacobian of C. Assume that $J(C)$ is isogenous to $E_0^m \times A$ over k where A is an Abelian variety admitting no nonzero morphisms to E_0.

Then by Corollary 2.18, $E_K(K)/E_K(K)_{tor} \simeq (\text{End}(E_0))^m$. Since E_0 is defined over $\mathbb{F}_q$, rank End(E_0) is at least 2; we conclude that rank $E_K \geq 2m$.

We have rank $E_K(K) =$ rank $E_D(\mathbb{F}_q(t))$ + rank $E(\mathbb{F}_q(t))$. But rank $E(\mathbb{F}_q(t))$ is always 0 since $\mathbb{F}_q(t)$ is the function field of $\mathbb{P}^1$ and there is no nonconstant map from $\mathbb{P}^1$ to an elliptic curve.

Thus rank $E_D =$ rank $E_K \geq 2m$.

As was studied before, $L(1/2, \chi_D) = 0$ if and only if C admits a dominant map to E_0. This is equivalent to $m > 0$ and rank $E_D \geq 2$. □

Thus, by Proposition 2.21, results on quadratic characters can be used to give lower bounds on the number of elliptic curves with rank ≥ 2 in quadratic twist families of constant elliptic curves.

There are lots of heuristics and results on the study of ranks of elliptic curves in a quadratic twist family over number fields ([PPVMW], [BMSW07]). For example, with a fixed $E/\mathbb{Q}$, let d range over fundamental discriminants in $\mathbb{Z}$. Define set

$$N(X) = \{d < X : \text{rank}(E_d) \geq 2 \text{ and is even } \}$$

Then it is conjectured by Sarnak that

$$|N(X)| = X^{3/4+o(1)}$$

Following Katz-Sarnak philosophy, Conrey, Keating, Rubinstein, and Snaith [CKRS02] made the previous conjecture more precise. They conjectured that there exist constants c_E, e_E such that

$$|N(X)| = (c_E + o(1))X^{3/4}(\ln(X))^{e_E}$$

Gouvêa and Mazur [GM91] proved under the parity conjecture, for any $\epsilon > 0$, there exists a constant X_ϵ such that for all $X \geq X_\epsilon$,

$$|N(X)| > X^{1/2-\epsilon}$$

In the same spirit, Karl Rubin and Alice Silverberg [RS01] showed unconditionally that if either

- $E[2]$ has a non-trivial Galois equivariant automorphism and $\mathrm{End}_{\mathbb{C}}(E) \neq \mathbb{Z}[i]$, or
- E has a rational subgroup of odd prime order p and $\mathbb{Z}[\sqrt{-p}] \nsubseteq \mathrm{End}_{\mathbb{C}}(E)$.

one has, for $X \gg 1$,

$$|\{d < X : \mathrm{rank}(E_d) \geq 2\}| \gg X^{1/3}$$

They also showed the existence of a family of elliptic curves E over $\mathbb{Q}$ such that

$$|\{d < X : \mathrm{rank}(E_d) \geq 3\}| \gg X^{1/6}$$

Goldfeld[Gol79] conjectures that the average rank of quadratic twists of an elliptic curve is $1/2$, to be more precise,

$$\lim_{X\to\infty} \frac{\sum_{|d|<X} \mathrm{rank}(E_d)}{|\{d : |d| < X, \text{squarefree}\}|} = \frac{1}{2}$$

What underlies this conjecture is a widely held belief that 50% of the elliptic curves have rank 0 and 50% have rank 1. This is a combination of parity principle and minimalist philosophy.

In our case, the parity principle does not apply, since all the quadratic twists in our family have even rank.

Thus, we don't expect the average rank of this family to approach $1/2$. But still, we would expect minimalist philosophy which means 0% of elliptic curves in this family have rank ≥ 2.

And this expectation is supported by Bui and Florea's result mentioned in the first section for the odd degree case.

Corollary 2.22. *For q a square, let E be an elliptic curve over $\mathbb{F}_q$ where*

$$L(s, E) = 1 - 2q^{1/2-s} + q^{1-2s}.$$

Let

$$P'(g) = \{D \in \mathbb{F}_q[t] : \text{ monic, squarefree, of odd degree, } \deg D \leq 2g + 1\}.$$

$$R'(g) = \{D \in P'(g) : E_D \text{ has rank } 0\}.$$

Then

$$\lim_{g\to\infty} \frac{|R'(g)|}{|P'(g)|} \geq 0.9427\cdots + o(1).$$

Proof. This follows from Prop 2.21 and Corollary 2.1 of [BF]. □

2.5 Proof of the Main Theorem

In this section, we will use Proposition 2.10 as our main tool to prove the three statements of Theorem 2.3.

Proof of 2.3 (1). Following the theorem of Honda–Tate, when q is a square, the simple Abelian varieties defined over $\mathbb{F}_q$ with $q^{1/2}$ being a Frobenius eigenvalue are elliptic curves. We will pick one such curve and call it E with a Weierstrass form.

When q is a square, $C : y^2 = D$ admits a dominant map to E if and only if $L(1/2, \chi_D) = 0$.

By Proposition 2.10, since E has genus 1 with an odd defining equation, for any $\epsilon > 0$, there are at least $B_\epsilon N^{1/2-\epsilon}$ polynomials with $|D| < N$ satisfying the condition where B_ϵ is a nonzero constant.

So we get for polynomials $D \in \mathbb{F}_q[t]$ with $|D| < N$, for any $\epsilon > 0$, there are at least $B_\epsilon N^{1/2-\epsilon}$ which have the property that $L(1/2, \chi_D) = 0$ for N large.

□

Proof of Theorem 2.3 (2). When q is not a square, the simple $\mathbb{F}_q$ Abelian varieties with $q^{1/2}$ as a Frobenius eigenvalue form an isogeny class of Abelian surfaces. They are exactly the Weil restriction of scalars of the class of elliptic curves defined over $\mathbb{F}_{q^2}$ which have q as a Frobenius eigenvalue.

By results of Howe, Nart and Ritzenthaler [HNR09], for all $q > 3$, there is an abelian variety A_q having $\sqrt{q}$ as a Frobenius eigenvalue which is the Jacobian of a smooth genus-2 curve. It will play the same role in this section as the elliptic curve E for the case when q is a square.

Now in this case, we still have that for a polynomial $D \in \mathbb{F}_q[x]$ to have $L(1/2, \chi_D) = 0$, A_q is isogenous over $\mathbb{F}_q$ to a subabelian variety of the Jacobian of curve C given by $y^2 = D$.

Unlike the previous case, a map $J(C) \to A_q$ won't induce a map from C to C_0.

However, the existence of a map $C \to C_0$ would guarantee $J(C_0) = A_q$ to be isogenous to a subabelian variety of $J(C)$.

In order to use Proposition 2.10, we need C_0 to have a defining equation of the form $y^2 = f(x)$ where $\deg f = 6$ and f is reducible.

We will show that C_0 has such an equation for all q; that is, for each q and each C_0 whose Jacobian is isogenous to A_q, the q-th Frobenius doesn't act transitively on the Weierstrass points of C_0.

Denote the roots of f by $x_1, \ldots, x_6$. Then the 2-torsion group of $J(C_0)$ is generated by divisors $(x_1, 0) - (x_i, 0)$ where $i = 2, 3, 4, 5$. Thus, using this basis, from the action on $x_1, \ldots, x_6$, we get the matrix representation of the Frobenius action on $J(C_0)[2] \simeq (\mathbb{F}_2)^4$. If Frobenius acts on the roots transitively, then the characteristic polynomial of the action on the $\mathbb{F}_2$ vector space is $x^4 + x^2 + 1$.

Since we know the characteristic polynomial of Frobenius acting on the Tate module of $J(C_0)$ is $x^4 - 2qx^2 + q^4$, we see that the action of Frobenius on $J(C_0)[2]$ has characteristic polynomial $x^4 + 1$. Thus Frobenius doesn't act transitively on the Weierstrass points.

Since Frobenius doesn't act transitively on the Weierstrass points of C_0, it has a defining equation of the form $y^2 = f(x)$ where f is not irreducible. By applying Proposition 2.10, for any $\epsilon > 0$, there are at least $B_\epsilon N^{1/3-\epsilon}$ polynomials with $|D| < N$ with the curve defined by $y^2 = D$ admitting a dominant map to C_0 where B_ϵ is a nonzero constant.

We thus conclude that $g(N)$ is at least $B_\epsilon N^{1/3-\epsilon}$ for N large. □

Proof of Theorem 2.3 (3). We used Magma to go through all hyperelliptic curves defined by monic squarefree polynomial over $\mathbb{F}_3$ and found that the curve C defined by $y^2 = x(x^8 - 1)$ admits $\sqrt{3}$ as a Frobenius eigenvalue. Since C has an odd defining equation and is of genus 4, by applying Proposition 2.10, we conclude for any $\epsilon > 0$, at least $B_\epsilon N^{1/5-\epsilon}$ hyperelliptic curves admit a dominant map to C where B_ϵ is a nonzero constant and N is large. □

2.6 Data and Remarks

To get a direct view of our main problem, we used Magma to list all monic squarefree polynomials up to a certain degree over some finite fields and evaluate the L-functions corresponding to the hyperelliptic curves defined by these polynomials at the central point to get a count on the ones with value 0. We have listed the data over fields $\mathbb{F}_5$ and $\mathbb{F}_9$ in the following tables. For field $\mathbb{F}_3$, there was only one curve of genus 4 given by a degree 9 defining equation found during the enumeration for polynomials of degree up to 12.

In the following tables, the first column is the degree d of polynomials. Second column is the number of polynomials of degree d whose corresponding L-function vanishes at $s = 1/2$. The set of such polynomials is denoted as $g'(q^d)$. Note that the set $g(q^d)$ studied in the paper is the union of $g'(q^k)$ for all $k \leq d$. The third column lists the total number of degree d monic squarefree polynomials. The last column is the value $log(g'(q^d))/log(q^d - q^{d-1})$. By our main theorem, it has a lim inf of at least $1/3$ for $\mathbb{F}_5$ and $1/2$ for $\mathbb{F}_9$ as $d \to \infty$.

$\mathbb{F}_5$			
Degree d	$\lvert g'(5^d)\rvert$	$5^d - 5^{d-1}$	$\frac{log(\lvert g'(5^d)\rvert)}{log(5^d - 5^{d-1})}$
3	0	100	
4	0	500	
5	1	2500	0
6	0	12500	
7	10	62500	0.2085
8	5	312500	0.1272

For degree 9 and 10, due to the large number of monic squarefree polynomials, we randomly sampled 5000000 data points for each and got the following data. The sample set is denoted by S. If we estimate the density $|g'(5^d)|/(5^d - 5^{d-1})$ to be equal to the same density $|S \cap g'(5^d)|/|S|$, then we get an approximation for $\frac{log(|g'(5^d)|)}{log(5^d - 5^{d-1})}$ which was put in the last column.

$\mathbb{F}_5$			
Degree d	$\lvert S \cap g'(5^d)\rvert$	$\lvert S\rvert$	$\frac{log(\lvert g'(5^d)\rvert)}{log(5^d - 5^{d-1})}$
9	317	5000000	0.3222
10	89	5000000	0.3109

Over $\mathbb{F}_5$, we see there exists a genus 2 curve defined by a degree 5 polynomial with Frobenius eigenvalue $\sqrt{5}$. This polynomial is $x(x^4 - 1)$. Unlike hyperelliptic curves defined over larger fields, this curve doesn't have an even degree model. That explains why there is no quadratic character with conductor 5^6 whose L-function vanishes at $s = 1/2$.

$\mathbb{F}_9$			
Degree d	$\lvert g'(9^d)\rvert$	$9^d - 9^{d-1}$	$\frac{log(\lvert g'(9^d)\rvert)}{log(9^d - 9^{d-1})}$
3	6	648	0.2768
4	18	5832	0.3333
5	216	52488	0.4946
6	180	472392	0.3975
7	8658	4251528	0.5940

Similarly,for degree 8, 9 and 10, 5000000 data points for each were randomly sampled and we got the following data. The last column is the approximation gotten the same way as the case of field $\mathbb{F}_5$ listed above.

$\mathbb{F}_9$			
Degree d	$\lvert S \cap g'(9^d)\rvert$	$\lvert S\rvert$	$\frac{log(\lvert g'(9^d)\rvert)}{log(9^d - 9^{d-1})}$
8	2660	5000000	0.5682
9	3262	5000000	0.6269
10	532	5000000	0.5814

From this table, we can see over $\mathbb{F}_9$, characters defined by odd degree polynomials are more likely to have their L-function vanish at $s = 1/2$. Thus, what this data tells us is that hyperelliptic curves defined over $\mathbb{F}_{p^2}$ with a Frobenius eigenvalue p is more likely to have a rational Weierstrass point.

One explanation for this phenomenon is the observation that elliptic curves defined over $\mathbb{F}_{p^2}$ with Frobenius eigenvalues p and p have full 2 torsion group over $\mathbb{F}_{p^2}$. This is because the pth Frobenius acts on Tate module T_l by multiplication by p; thus, if $p \equiv 1 \mod l$ then the action is trivial on $E[l]$. And this is equivalent to l-torsion points being defined over the ground field.

Thus the elliptic curve E we used in the proof of Theorem 2.3 part 1 is defined by $y^2 = x(x-1)(x-\lambda)$ where $\lambda \in \mathbb{F}_q$. And the hyperelliptic curves C which admit a dominant map to E have defining equations of the form $y^2 = F(x) = u(x)(u(x) - v(x))(u(x) - \lambda v(x))v(x)$.

For C to have a rational Weierstrass point is equivalent to $F(x)$ having a rational root. As we can see, instead of being a random polynomial over $\mathbb{F}_q$, $F(x)$ admits a factorization into four factors; this should increase the likelihood of its having an $\mathbb{F}_q$ rational root.

Chapter 3

Nonvanishing of hyperelliptic zeta functions over finite fields

[1]

3.1 Introduction

Let p be an odd prime, set $q = p^k$ for some positive integer k, and denote by $\mathbb{F}_q$ the finite field with q elements. To (the smooth completion of) any hyperelliptic curve C over $\mathbb{F}_q$ one associates a zeta function $Z_C(s)$. Weil has shown that $Z_C(s) = 0$ implies that $s = \frac{1}{2} + it$ for some $t \in \mathbb{R}$.

It is widely believed that for any fixed $s = \frac{1}{2} + it$, the 'vast majority' of (hyperelliptic) curves do not have s as a zero of their zeta function. For example, it follows from the work [Cha97] of Chavdarov (and its improvement by Kowalski [Kow06]) that for any fixed (large enough) g, the proportion of genus g hyperelliptic zeta functions vanishing at s tends to 0 as $q \to \infty$.

Here we are concerned with the growing g regime. Namely, for fixed q (and s), we give an upper bound on

$$h_{q,s} := \sup_g \frac{\left|\{C \in \mathcal{H}_g(\mathbb{F}_q) : Z_C(s) = 0\}\right|}{\left|\mathcal{H}_g(\mathbb{F}_q)\right|} \tag{3.1}$$

where $\mathcal{H}_g(\mathbb{F}_q)$ is the family of genus g hyperelliptic curves over $\mathbb{F}_q$. Our bound is better once q is large, as given by our main result.

[1] This chapter is based on the contents of [ELS]

Theorem 3.1 (Theorem 3.9)**.** *For any $t \in \mathbb{R}$ and $s = \frac{1}{2} + it$, we have*

$$\lim_{k\to\infty} h_{p^k,s} = 0. \tag{3.2}$$

Restricting q to powers of a fixed prime p is not strictly necessary. In case $s \neq \frac{1}{2}$, one can show (using transcendental number theory) that there are only a few p for which p^{-s} is algebraic, so $h_{q,s} = 0$ for any q not divisible by these p. For $s = \frac{1}{2}$, a modification of our arguments is needed (in order to obtain our theorem with possibly varying characteristic).

Additional motivation for Theorem 3.1 comes from the ability to write $Z_C(s)$ as a rational function in q^{-s}, with the numerator being (essentially) a quadratic Dirichlet L-function. Interpreted in this language of Dirichlet characters, Theorem 3.1 improves (for all sufficiently large q) upon [BF, Corollary 2.1] of Bui and Florea (they give a nonzero nonvanishing proportion at $s = \frac{1}{2}$). Regarding the analogous vanishing problem for quadratic Dirichlet L-functions over $\mathbb{Z}$, we refer to the work [Sou00] of Soundararajan and references therein[2] .

As we explain in the last section, our theorem can be rephrased as an upper bound for the number of quadratic twists of a constant abelian variety which have positive rank.

Corollary 3.2 (Corollary 3.10)**.** *Let A be a constant abelian variety defined over $\mathbb{F}_q(x)$. For each $f \in \mathbb{F}_{q^m}[x]$ where q^m is the m-th power of q, denote by A_f the quadratic twist of $A \otimes \mathbb{F}_{q^m}(x)$ by f. Let $R_{n,m}$ be the set $\{f \in \mathbb{F}_{q^m}[x],$ squarefree, of $\deg n : A_f$ has positive rank$\}$. Then,*

$$\lim_{m\to\infty} \limsup_{n\to\infty} \frac{|R_{n,m}|}{q^{m(n+1)}} = 0.$$

Motivated by [BF, Corollary 2.2] and the analogous results over $\mathbb{Z}$ of Conrey, Ghosh and Gonek from [CGG98], we bound the multiplicity of the zeros of Z_C, and obtain further information on nonvanishing at $s = \frac{1}{2}$.

Theorem 3.3. *Let C be a hyperelliptic curve of genus at least 2 over $\mathbb{F}_q$ and S be the set of Weierstrass points of C. The Frobenius acts on S by permuting the $2g + 2$ Weierstrass points via some permutation π. Suppose that either*

[2]Results in [BF] and [Sou00] were stated at point $s = 1/2$ but the methods can be extended to prove the statement for any point on the critical line.

- *g is even and π is a $(2g+2)$-cycle; or*
- *π is the product of two disjoint cycles of odd length.*

Then:

1. *The point $s = \frac{1}{2}$ is not a zero of Z_C.*
2. *All zeros of Z_C are of multiplicity at most 2. Moreover, if π is the product of two disjoint cycles of* coprime *odd length, all zeros of Z_C are simple.*

In the language of Dirichlet characters, this implies in particular the nonvanishing (at the central point) in the case of prime conductor of degree not divisible by 4. (When the degree of the conductor is odd, one Weierstrass point is at ∞ and π consists of a fixed point and a cycle of length $2g+1$.) Thus there is an explicit set of size on order $X/\log X$ of Dirichlet characters of size at most X which have L-functions nonvanishing at the critical point; this improves on [AK13, Corollary 2.6] of Andrade and Keating and on [ABJ16, Corollary 2.8] of Andrade, Bae, and Jung, which give a proportion on order $(\log X)^{-2}$, and goes beyond the methods of [AB18]. For the analogous problem over $\mathbb{Z}$, we refer to the recent work [BP18] of Baluyot and Pratt.

In fact, there is nothing special about hyperelliptic curves in Theorem 3.3. A similar "genus-theory" argument allows us to handle the case of cyclic p-covers of $\mathbb{P}^1$ for odd p.

Theorem 3.4. *Let ℓ be an odd prime and let C be a $(\mathbb{Z}/\ell\mathbb{Z})$-cover of $\mathbb{P}^1/\mathbb{F}_q$ branched at a set $S \subset \mathbb{P}^1(\overline{\mathbb{F}}_q)$. Let π be the permutation induced by Frobenius on S, and suppose that π is the union of disjoint cycles of order $k_1, k_2, \ldots, k_r$, all prime to ℓ.*

1. *Suppose the k_i are mutually coprime, and either $r = 2$ or q is not congruent to 1 modulo ℓ. Then every zero of Z_C is simple.*
2. *Define κ_i to be k_i if k_i is odd and $k_i/2$ if k_i is even. Suppose that either*
   - *q is congruent to 1 modulo ℓ and $r = 2$; or*
   - *There is no i such that q^{κ_i} is congruent to 1 modulo ℓ.*

Then the point $s = \frac{1}{2}$ is not a zero of Z_C.

We remark that this theorem, like Theorem 3.3 above, provides a set of size on order $X/\log(X)^a$ of order-ℓ Dirichlet characters of conductor at most X whose zeta functions are non-vanishing at $s = 1/2$, for some power $a \in (0, 1]$. This lower bound improves upon Corollary 1.3 of [DFL] for the case $\ell = 3$.

The main idea that connects all the theorems in this paper is the study of L-functions modulo ℓ. The value of an L-function over $\mathbb{F}_q(x)$ at a complex number s can be expressed as a polynomial $P(T) \in \mathbb{Z}[T]$, where $T = q^{-s}$. So if we want to prove that $P(T)$ is nonvanishing, it suffices to prove that $P(T)$ is nonvanishing modulo ℓ for some prime ℓ. For Theorem 3.1, we will show that, for suitably chosen ℓ, the vanishing mod ℓ of the L-function is related to the dimension of a certain Frobenius eigenspace in the ℓ-torsion of a hyperelliptic Jacobian over $\mathbb{F}_q$; the average size of this eigenspace can then be controlled by a modest generalization of the arguments in [EVW16]. For Theorem 3.3, on the other hand, we argue that under the given condition on Weierstrass points the L-function of χ_f is nonvanishing mod 2 at $s = 1/2$. For the similar Theorem 3.4, the ℓ is again the order of the Dirichlet character in question.

3.2 Main Theorem and Proof

3.2.1 Setup and Notations

Throughout the paper, $\mathbb{F}_q$ is a finite field of odd characteristic p. Let $Q_{n,q}$ be the set of squarefree polynomials over $\mathbb{F}_q$ of degree n. For each $f \in Q_{n,q}$, write J_f for the Jacobian of the hyperelliptic curve

$$y^2 = f(x)$$

and $P_f(x) \in \mathbb{Z}[x]$ for the characteristic polynomial of Frobenius acting on the ℓ-adic Tate module of J_f. Let ℓ be a prime not equal to the characteristic of $\mathbb{F}_q$ and let a be an element of $(\mathbb{Z}/\ell\mathbb{Z})^*$. The elements R of $J_f[\ell](\overline{\mathbb{F}}_q)$ which satisfy

$$\mathrm{Frob}_q \cdot R = aR.$$

form a finite-dimensional vector space over $\mathbb{Z}/\ell\mathbb{Z}$ and we denote by $m_a(f)$ the number of nonzero elements of this vector space. Note that $m_1(f)$ is just the number of $\mathbb{F}_q$-rational nontrivial ℓ-torsion points of J_f. Let $Q_{n,q}^{a,\ell}$ be the set of squarefree polynomials over $\mathbb{F}_q$ of degree n such that $m_a(f)$ is greater than 0.

Let α be an algebraic integer with minimal polynomial $g_\alpha(x) \in \mathbb{Z}[x]$ and absolute value $\sqrt{q}$ under all complex embeddings. Let $Q_{n,q}^{\alpha}$ be the subset of $Q_{n,q}$ defined by $\{f \in Q_{n,q} \mid P_f(\alpha^{-1}) = 0\}$. With notation introduced as above, if $g_\alpha(a) = 0 \bmod \ell$, then $|Q_{n,q}^{\alpha}| \leq |Q_{n,q}^{a,\ell}|$.

3.2.2 Rational points on twisted Hurwitz spaces over finite fields

Our main tool will be the following result about the average size of the subspace of $\mathrm{Jac}(C)[\ell](\overline{\mathbb{F}}_q)$ on which Frobenius acts by some specified scalar a, as C ranges over hyperelliptic curves over $\mathbb{F}_q$. More precisely, we study the variation as we range over $y^2 = f(x)$ with f ranging over squarefree polynomials in $\mathbb{F}_q[x]$; this amounts to the same, since each isomorphism class of hyperelliptic curves is represented in this form the same number of times (assuming, of course, that the isomorphism classes are weighted inversely to the number of automorphisms they possess.)

Proposition 3.5. *With notation as Section 3.2.1, there exists a constant C_ℓ only depending on ℓ such that*

$$\left| \frac{\sum_{f \in Q_{n,q}} m_a(f)}{|Q_{n,q}|} - 1 \right| \leq C_\ell q^{-1/2}$$

for all n, q sufficiently large.

When $a = 1$ and n is odd, this is essentially Theorem 8.8 of [EVW16], and indeed the proof of Proposition 3.5 is a modification of the proof of that theorem.

The reader may note that [EVW16, Thm 8.8] requires not only that q is not a multiple of ℓ but that q is not congruent to 1 modulo ℓ. We face no such restriction here. That's because [EVW16, Thm 8.8] computes arbitrary moments of the Cohen-Lenstra distribution, whereas we are only studying the analogue of the average size of the ℓ-part of the class group. In the language of [EVW16, Thm 8.8], we are only considering the case $A = \mathbb{Z}/\ell\mathbb{Z}$. The

difference is as follows. In the proof, we will end up estimating the number of $\mathbb{F}_q$-points on a moduli space over $\mathbb{F}_p$, and the result will depend on that space having just one geometrically irreducible component defined over $\mathbb{F}_q$. In the more general setting treated in [EVW16, Thm 8.8], that space has many geometric components, all but one of which have fields of definition containing μ_ℓ; so when q is congruent to 1 mod ℓ there are multiple $\mathbb{F}_q$-rational components. In the case treated here, the moduli space in question is geometrically irreducible, so this issue does not arise.

Proof. We begin by observing that $\sum_{f \in Q_{n,q}} m_a(f)$ can be interpreted as the number of $\mathbb{F}_q$-rational points of a certain moduli space.

To this end we briefly recall the setup of [EVW16, Section 7].

Let k be a field, let G be a finite group with trivial center, and let c be a conjugacy-closed subset of $G \backslash e$. By a *tame G-cover of $\mathbb{P}^1$ with monodromy type c* we mean a triple (X, f, ϕ) where

- X is a smooth proper geometrically connected curve X/k;
- $f : X \to \mathbb{P}^1$ is a tamely ramified finite cover;
- The image of tame inertia at each branch point of f excepting ∞ lies in c;
- f is Galois with group G; that is, $\mathrm{Aut}(f)$ acts transitively on the geometric fibers of f and ϕ is an automorphism from G to $\mathrm{Aut}(f)$.

Then, as in [EVW16, Section 7] (more or less immediate from a theorem of Romagny and Wewers [RW06]), there is a scheme $\mathsf{Hn}^c_{G,n}$ over $\mathbb{Z}[1/|G|]$ whose k-points (as long as k has characteristic prime to $|G|$) are in bijection with the isomorphism classes of tame G-covers of $\mathbb{P}^1$ which have n branch points on $\mathbb{A}^1$ with monodromy type c. (We do not specify whether or how the cover is branched at ∞.)[3] In fact ([RW06, Theorem 2.1]) the set $\mathsf{Hn}^c_{G,n}(S)$ corresponds to isomorphism classes of tame G-covers over S, suitably defined; we will not

[3]The somewhat artificial special treatment of ∞ in this definition, as in [EVW16], stems from the need to compare with topology, where branched covers of the disc are technically easier to handle than branched covers of the sphere.

need to spell out that definition here. We emphasize that by an isomorphism between two covers $f : X \to \mathbb{P}^1$ and $f' : X' \to \mathbb{P}^1$ we mean a morphism $\psi : X \to X'$ with $f' \circ \psi = f$, not a pair (ψ, ι) with ι a nontrivial automorphism of $\mathbb{P}^1$ and $f' \circ \psi = \iota \circ f$. In other words, our $\mathbb{P}^1$ is "labeled".

From now on, we suppose that k is $\mathbb{F}_q$, that G is the dihedral group $(\mathbb{Z}/\ell\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, and that c is the conjugacy class of an involution in G. We will now explain the relationship between the space of G-covers and the ℓ-torsion in the Jacobian of hyperelliptic curves. The key point is that, for any algebraic curve C, the set of surjections $\mathrm{Jac}(C)[\ell] \to (\mathbb{Z}/\ell\mathbb{Z})^k$ is naturally identified with the set of étale $(\mathbb{Z}/\ell\mathbb{Z})^k$ covers of C. For details, see Section 3.9 of [Mil08].

If $f : X \to \mathbb{P}^1$ is a G-cover, the product structure of G allows us to factor f as

$$X \xrightarrow{g} C \xrightarrow{h} \mathbb{P}^1$$

where h is a hyperelliptic cover and g is a Galois cover with group $(\mathbb{Z}/\ell\mathbb{Z})$; that is, g is endowed with an isomorphism $\phi : \mathbb{Z}/\ell\mathbb{Z} \to \mathrm{Aut}(g)$. What's more, the fact that the monodromy in f is of type c implies that g is an etale cover, at least away from the points of C over $\infty \in \mathbb{P}^1$.

What happens over ∞ is slightly more delicate. The double cover h is branched at n points on $\mathbb{A}^1$, but the total number of branch points of h must be even. Thus, if n is odd, h is branched at ∞. The monodromy around ∞ in the cover $X \to \mathbb{P}^1$ is thus an element of G projecting to the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$. Such an element must be an involution, and it follows that g is unramified at ∞. If n is even, on the other hand, it is possible for g to be ramified. We thus wish to restrict our attention to those G-covers $X \to C$ which are unramified over ∞. These are parametrized by a closed and open subscheme of $\mathsf{Hn}^c_{G,n}$ (indeed, it is the second term in the disjoint union in the paragraph following (7.3.1) of [EVW16]). Let X_n be this subscheme of $\mathsf{Hn}^c_{G,n}$ when n is even, and $\mathsf{Hn}^c_{G,n}$ when n is odd. We have explained how every point of $X_n(k)$ gives rise to a triple $(g, \phi, h)/k$ up to isomorphism, and in fact it is not hard to check that the converse holds as well. (This is essentially the last paragraph of the proof of [EVW16, Proposition 8.7].)

If a is an element of $(\mathbb{Z}/\ell\mathbb{Z})^*$, we denote by $\langle a \rangle$ the automorphism of X_n which sends (g, ϕ, h) to $(g, a\phi, h)$. We then write X_n^a for the twist of X_n by the homomorphism

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to \mathrm{Aut}(X_n)$$

which sends Frob_q to a. (Reference: [Poo17, §4.5].)

Lemma 3.6. *With notation as in Section 3.2.1,*

$$\sum_{f \in Q_{n,q}} m_a(f) = (q-1)|X_n^a(\mathbb{F}_q)|$$

Proof. A point of $X_n^a(\mathbb{F}_q)$ is a point of $X_n(\overline{\mathbb{F}}_q)$ such that $\mathrm{Frob}_q \cdot x = \langle a \rangle \cdot x$. In other words, it is a triple $(g, \phi, h)/\overline{\mathbb{F}}_q$ such that $\mathrm{Frob}_q \cdot (g, \phi, h)$ is isomorphic to $(g, a\phi, h)$. The fact that the isomorphism class of h is fixed by Frobenius implies that C is isomorphic (over $\overline{\mathbb{F}}_q$) to $y^2 = f(x)$ for a unique monic squarefree polynomial f of degree n (namely, the one which vanishes precisely at the branch locus of h, which is an $\mathbb{F}_q$-rational divisor.)

Fixing such an h, and thus such a C, we now consider the set of points of $X_n^a(\mathbb{F}_q)$ lying over this h. First of all, the choices of $(g, \phi) \in X_n^a(\overline{\mathbb{F}}_q) = X_n(\overline{\mathbb{F}}_q)$ for a specified h are in bijection with the $\ell^{2g(C)} - 1$ surjections from $J(C)[\ell](\overline{\mathbb{F}}_q)$ to $\mathbb{Z}/\ell\mathbb{Z}$. Two such surjections s, s' are isomorphic (that is, are parametrized by the same point of $X_n^a(\overline{\mathbb{F}}_q)$) if and only if $s = \pm s'$. The action of Frobenius on the set of surjections sends s to $a^{-1} \mathrm{Frob}_q s$; so s descends to a point of $X_n^a(\mathbb{F}_q)$ if and only if $\mathrm{Frob}_q \cdot s = \pm as$. We conclude that the number of points of $X_n^a(\mathbb{F}_q)$ lying over h is $(1/2)(m_a(f) + m_{-a}(f))$.

Now if f in $Q_{n,q}$ is *not* monic then $f = \epsilon F$ for some $\epsilon \in \mathbb{F}_q^*$ and some monic F. The curve C_f is isomorphic to C_F if ϵ is a quadratic residue and to the nontrivial quadratic twist of C_F otherwise. In the former case, $m_a(f) = m_a(F)$, and in the latter, $m_a(f) = m_{-a}(F)$. In particular, the quantity $(1/2)(m_a(f) + m_{-a}(f))$ is the same for all $q-1$ nonzero multiples of F. We conclude that

$$\sum_{f \in Q_{n,q}} (1/2)(m_a(f) + m_{-a}(f)) = (q-1)|X_n^a(\mathbb{F}_q)|$$

Moreover, taking ϵ to be a non-residue in $\mathbb{F}_q^*$,

$$\sum_{f\in Q_{n,q}} m_a(f) = \sum_{f\in Q_{n,q}} m_a(\epsilon f) = \sum_{f\in Q_{n,q}} m_{-a}(f)$$

from which we obtain

$$\sum_{f\in Q_{n,q}} m_a(f) = (q-1)|X_n^a(\mathbb{F}_q)|$$

as desired. □

We now argue exactly as in the proof of [EVW16, Theorem 8.8].

Since $|Q_{n,q}| = (q-1)(q^n - q^{n-1})$, it suffices to prove that

$$|q^{-n}|X_n^a(\mathbb{F}_q)| - 1| \leq C_\ell q^{-1/2}$$

for some C_ℓ depending only on ℓ and for all n, q sufficiently large. Via the Grothendieck-Lefschetz trace formula, we have

$$|X_n^a(\mathbb{F}_q)| = \sum_i (-1)^i \mathrm{Tr}(\mathrm{Frob}_q\,|H^i_{c,\text{ét}}((X_n^a)_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\lambda). \tag{3.3}$$

where λ is a prime greater than $\max\{2\ell, q, n\}$.

Note that the étale cohomology is that of the base change of X_n^a to $\overline{\mathbb{F}}_q$, where it becomes isomorphic to the untwisted space X_n; so at this point the choice of a becomes completely irrelevant! The moduli space X_n is a closed and open subscheme of $\mathsf{Hn}^c_{G,n}$, so its Betti numbers are bounded by those of $\mathsf{Hn}^c_{G,n}$; by [EVW16, (7.8.1)] we have

$$\dim H^{2n-i}_{\text{ét}}((X_n^a)_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \leq (C')^{2n-i}$$

where C' is a constant depending only on ℓ and n, q are both sufficiently large. The eigenvalue of Frobenius on $H^i_{c,\text{ét}}((X_n^a)_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\lambda)$ is bounded in absolute value by $q^{i/2}$; so the contribution of all $i < 2n$ to (3.3) is bounded above by $C_\ell q^{n-1/2}$ for some C_ℓ only depending on ℓ and all sufficiently large n, q. See [EVW16, Section 1.8].

It remains to show that

$$\mathrm{Tr}(\mathrm{Frob}_q\,|H^{2n}_{c,\text{ét}}((X_n^a)_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\lambda) = q^n.$$

But this is equivalent to $(X_n^a)_{\overline{\mathbb{F}}_q} \cong (X_n)_{\overline{\mathbb{F}}_q}$ being irreducible. When n is odd, this is shown in the proof of [EVW16, Theorem 8.8] as a consequence of a big monodromy theorem of J.K. Yu. When n is even, we argue as follows. The map from X_n to the configuration space $\mathrm{Conf}^n \mathbb{A}^1$ sending a G-cover to its branch locus is a finite cover, and irreducibility of X_n is equivalent to the monodromy group of this cover acting transitively on the fiber. It suffices to check that this holds on a closed subvariety of the base. So write Z for the subvariety of $\mathrm{Conf}^n \mathbb{A}^1$ consisting of those configurations containing some specified point $p_0 \in \mathbb{P}^1(F_q)$, and let Y be the preimage of Z in X_n. An automorphism of $\mathbb{P}^1$ taking p_0 to ∞ now identifies Y with $\mathsf{Hn}^c_{G,n-1}$, which we know to be irreducible since $n-1$ is odd. This implies that X_n is irreducible, completing the proof. □

Proposition 3.5 allows us to bound the proportion of hyperelliptic curves whose étale homology has a Frobenius eigenvalue congruent to a mod ℓ. Recall from Section 3.2.1 that $Q_{n,q}^{a,\ell}$ is the set of squarefree polynomials over $\mathbb{F}_q$ of degree n such that $m_a(f)$ is greater than 0.

Corollary 3.7. *There is a constant C'_ℓ such that*

$$\frac{|Q_{n,q}^{a,\ell}|}{|Q_{n,q}|} \leq \frac{1}{\ell - 1} + C'_\ell q^{-1/2}$$

for all n, q sufficiently large.

Proof. Write δ for the quantity $|Q_{n,q}|^{-1}|Q_{n,q}^{a,\ell}|$ to be bounded.

Since $m_a(f)$ is the number of nonzero elements of a vector space over $\mathbb{Z}/\ell\mathbb{Z}$, it is at least $\ell - 1$ if it is greater than 0. In particular,

$$|Q_{n,q}|^{-1} \sum_{f \in Q_{n,q}} m_a(f) \geq |Q_{n,q}|^{-1}(\ell - 1)|Q_{n,q}^{a,\ell}| = (l-1)\delta$$

By Proposition 3.5, we now have

$$(\ell - 1)\delta < 1 + C_\ell q^{-1/2}$$

for all sufficiently large n, q, which yields the desired result by taking $C'_\ell = C_\ell/(\ell - 1)$. □

3.3 Application to nonvanishing of L-functions

We can use the above reasoning to bound the number of quadratic L-functions over function fields which vanish at a specified point on the critical line. For the rest of this section we fix an odd prime p and consider only fields of characteristic p. We note that, if χ_f is a quadratic character of $\mathbb{F}_q(x)$, then $L(s, \chi_f)$ can vanish only at a point s such that q^s is an algebraic integer whose complex absolute values all have magnitude $\sqrt{q}$. We first recall the following lemma relating the vanishing of the L-function of a quadratic character in terms of the Frobenius eigenvalues of a hyperelliptic curve;

Lemma 3.8. *Let f be a monic squarefree polynomial in $\mathbb{F}_q[x]$ and χ_f be the quadratic character with conductor f. Let C be the hyperelliptic curve defined by $y^2 = f(x)$ and let $P \in \mathbb{Z}[x]$ be the characteristic polynomial of geometric Frobenius acting on the Jacobian of C. Then for any $s \neq 0$, $L(s, \chi_f) = 0$ if and only if $P(q^s) = 0$.*

This is immediate from the description of P as the numerator of the L-function $L(s, \chi_f)$.

Theorem 3.9. *For any squarefree polynomial $f \in Q_{n,q}$, let $L(s, \chi_f)$ be the Dirichlet L-function associated to the quadratic character χ_f as was defined in Section 3.2.1. Then for any $s \neq 0$,*

$$\lim_{q\to\infty} \limsup_{n\to\infty} \frac{|\{f \in Q_{n,q} \mid L(s, \chi_f) = 0\}|}{|Q_{n,q}|} = 0.$$

Proof. By Lemma 3.8, $L(s, \chi_f) = 0$ is equivalent to $P(q^{-s}) = 0$ where $P(x) \in \mathbb{Z}[x]$ is the characteristic polynomial of Frobenius acting on the Jacobian of the hyperelliptic curve defined by $y^2 = f(x)$. Thus, the set $\{f \in Q_{n,q} \mid L(s, \chi_f) = 0\}$ is the same as $Q_{n,q}^{q^s}$.

Let $l \neq p$ be any prime where $g_{p^s}(x)$, the minimal polynomial of p^s, splits completely. By Chebotarev density theorem, there are infinitely many such primes. Let $a \in \mathbb{Z}/l\mathbb{Z}$ such that $g_{p^s}(a) = 0 \bmod l$. If $q = p^m$, then any f with $L(\chi_f, s) = 0$ has $m_{a^m}(f) > 0$. So

$$\frac{|Q_{n,q}^{q^s}|}{|Q_{n,q}|} \leq \frac{|Q_{n,q}^{a^m,\ell}|}{|Q_{n,q}|}$$

and now we can apply Corollary 3.7 to conclude that, for all sufficiently large m, we have

$$\limsup_{n\to\infty} \frac{|Q_{n,q}^{q^s}|}{|Q_{n,q}|} \leq \frac{1}{\ell - 1} + C'_\ell q^{-1/2}$$

The theorem now follows, since we can choose ℓ to be as large as we like. □

Results on the vanishing of quadratic L-functions over function fields can be used to study the rank distribution of quadratic twist families of constant abelian varieties. In the following corollary, we show as the constant field grows to infinity, the probability for a quadratic twist of a constant abelian variety to have positive rank goes to 0 as q grows. In the elliptic curve case, this agrees with the general "Minimalist Conjecture" philosophy, which holds that positive ranks should be a density-0 phenomenon except when forced by parity considerations from the functional equation (in this setting the functional equation never forces positive rank, and the rank is always even.)

Corollary 3.10. *Let A be an abelian variety defined over a finite field $\mathbb{F}_q$. For each $f \in Q_{n,q^m}$ where q^m is the m-th power of q, denote by A_f the quadratic twist of $A \times_{\mathbb{F}_q} \mathbb{F}_{q^m}(x)$ by f. Let $R_{n,m}$ be the set $\{f \in Q_{n,q^m} : A_f$ has positive rank$\}$. Then*

$$\lim_{m\to\infty} \limsup_{n\to\infty} \frac{|R_{n,m}|}{|Q_{n,q^m}|} = 0.$$

Proof. Let $P(x)$ be the characteristic polynomial of Frobenius acting on the Tate module of A and let q^{-s} be one of its roots. Then $\operatorname{rank} A_f > 0$ is equivalent to $L(s, \chi_f) = 0$. (See [Li18, Proposition 4.6] for a similar statement with the same proof.) Thus, the statement is a direct application of Theorem 3.9. □

We now prove Theorem 3.3, which makes use of the mod 2 Galois representations on $J(C)$ rather than the representations modulo odd primes.

Proof of Theorem 3.3. Let $x_1, ..., x_{2g+2}$ be the set of Weierstrass points of C. The 2-torsion subgroup $J(C)[2]$ is spanned by the degree-0 2-torsion divisors $x_i - x_j$. That is, the group of divisors of the form $\sum a_i x_i$ with $\sum a_i = 0$ surjects onto $J(C)[2]$. Note also that $x_1 + \ldots + x_{2g+2} - (2g+2)x_1$ is a principle divisor and thus $x_1 + \ldots + x_{2g+2}$ is 0 in $J(C)[2]$. See

[Gro12, Secion 4] for detailed discussion. This identifies $J(C)[2]$ with an explicit subquotient of $\mathbb{F}_2^{2g+2}$; namely, $J(C)[2]$ is the quotient of the subspace $(a_1, \ldots, a_{2g+2}) : \sum a_i = 0$ by the 1-dimensional subspace spanned by $(1, \ldots, 1)$.

This identification is equivariant for the Frobenius action on both sides, so it allows us to describe the mod 2 Galois representation afforded by $J(C)$ in terms of the permutation π which Frobenius induces on $x_1, \ldots, x_{2g+2}$. To be precise, the action of S_{2g+2} on $J(C)[2]$ is a representation $\rho : S_{2g+2} \to \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, and the action of Frobenius on $J(C)[2]$ is given by $\rho(\pi)$.

The conditions on π given in Theorem 3.3 are equivalent to the condition that π^2 is a product of two disjoint odd cycles. Thus, the action of π^2 in its permutation representation $\mathbb{F}_2^{2g+2}$ has eigenvalues given by μ_k and μ_{2g+2-k}; passing to the subquotient $J(C)[2]$ removes two eigenspaces of $\rho(\pi^2)$ with the eigenvalue 1. So the eigenvalues of Frob^2 on $J(C)[2]$ are the multiset $\mu'_k \cup \mu'_{2g+2-k}$, where μ'_n denotes the nontrivial n'th roots of unity. We see in particular that $\rho(\pi^2)$ does not have 1 as an eigenvalue. But if the zeta function Z_C had a zero at $1/2$, then $\sqrt{q}$ would be a Frobenius eigenvalue on C, which would mean that q was an eigenvalue of Frob^2; we have shown that Frob^2 has no eigenvalue congruent to 1 mod 2, which rules this out. This proves (1).

What's more, the multiset $\mu'_k \cup \mu'_{2g+2-k}$ contains any eigenvalue at most twice, and if $(k, 2g+2-k) = 1$, no eigenvalue appears more than once. This proves (2) (or rather, it proves (2) for the zeta function of $C/\mathbb{F}_{q^2}$, from which (2) is immediate.)

□

The proof of Theorem 3.4 is very similar, but we treat it separately in order to make the hyperelliptic case above more readable.

Proof of Theorem 3.4. Let $x_1, \ldots, x_m$ be the ramification points of the $(\mathbb{Z}/\ell\mathbb{Z})$-cover of $\mathbb{P}^1$ in S, where $m = k_1 + k_2$. The Jacobian $J(C)$ of C carries an action of $\mathbb{Z}[(\mathbb{Z}/\ell\mathbb{Z})]$; write $\lambda \in \mathbb{Z}[(\mathbb{Z}/\ell\mathbb{Z})]$ for $\zeta - 1$, where ζ is a generator of $(\mathbb{Z}/\ell\mathbb{Z})$. A Riemann-Hurwitz computation

shows that the genus of C is $(m-2)(\ell-1)/2$, so the Tate module $T_\ell J(C)$ is a free $\mathbb{Z}_\ell[\zeta_\ell]$-module of rank $m-2$, and $J(C)[\lambda]$ has dimension $m-2$.

The λ-torsion subgroup of $J(C)$ is spanned by the degree-0 λ-torsion divisors $x_i - x_j$. That is, the group of divisors of the form $\sum a_i x_i$ with $\sum a_i = 0$ surjects onto $J(C)[\lambda]$. This surjection is not an isomorphism; there is a 1-dimensional kernel, which we can describe as follows. Over $\overline{\mathbb{F}}_q$, the curve C has an affine model of the form $y^\ell = f(x)$ with f a rational function with no zeroes or poles at ∞. Then the principal divisor associated to y is $\sum a_i x_i$ where $a_i = \mathrm{ord}_{x_i} f$. We have now expressed $J(C)[\lambda]$ as an explicit subquotient of $\mathbb{F}_\ell^m$.

This identification is equivariant for the Frobenius action on both sides, so it allows us to describe the mod ℓ Galois representation afforded by $J(C)$ in terms of the permutation π which Frobenius induces on $x_1, \ldots, x_m$.

The action of π splits $x_1, \ldots, x_m$ into cycles of length $k_1, \ldots, k_r$, which by hypothesis are prime to ℓ. So the eigenvalues of π in its action on $\mathbb{F}_\ell^m$ are the union (as multisets) $\bigcup_{j=1}^r \mu_{k_j}$. Now the composition factors of $\mathbb{F}_\ell^m$ as a representation of the cyclic group $\langle \pi \rangle$ are $J(C)[\lambda]$, $\mathbb{F}_\ell div(y)$, and the $\mathbb{F}_\ell$ to which $\mathbb{F}_\ell^m$ maps by summing coordinates. But π acts trivially on the latter two factors. We conclude that the eigenvalues of π in its action on $J(C)[\lambda]$ are the multiset $\bigcup_{j=1}^s \mu'_{k_j}$ together with $r-2$ copies of 1, where μ'_n denotes the nontrivial n'th roots of unity.[4]

If the zeta function Z_C had a zero at $1/2$, then $\sqrt{q}$ would be a Frobenius eigenvalue of C, which would mean that $\sqrt{q}$ modulo ℓ was an eigenvalue of the action of π on $J(C)[\lambda]$. If q is congruent to 1 modulo ℓ and $r = 2$, this is ruled out by the fact that $r - 2 = 0$ and $\bigcup_{j=1}^r \mu'_{k_j}$ contains no copy of 1. If q is not congruent to 1 mod ℓ, then $\sqrt{q}$ cannot be contained in $\bigcup_{j=1}^r \mu'_{k_j}$ because of our hypothesis on q^{κ_i}. Thus we have proved that $s = 1/2$ is not a root of Z_C.

[4] What if $r = 1$? This isn't possible. If π is an m-cycle, then the coefficients of the $\mathbb{F}_q$-rational divisor D must all be equal to the same constant a, which means am is congruent to 0 mod ℓ, which means m is a multiple of ℓ; but by hypothesis no cycle has length a multiple of ℓ.

If $k_1, \ldots, k_r$ are mutually coprime, then $\bigcup_{j=1}^{r} \mu'_{k_j}$ has no repeated values. So the only possible multiple eigenvalue of Frobenius on $J(C)[\ell]$ is 1, and this eigenvalue appears multiple times only if $r \geq 3$. This completes the proof.

□

Chapter 4

Effective Bounds on the Dimensions of Jacobians Covering Abelian Varieties

[1]

Over an infinite field, every abelian variety is covered by the Jacobian variety of a smooth connected curve. In fact, given an embedding of the abelian variety, one can even provide an effective upper bound on the dimension of the Jacobian variety using the dimension and degree of the abelian variety (see [Mil08, Section III]). We show that an analogous effective statement holds over a finite field.

Theorem 4.1. *Fix $r, n \in \mathbb{N}$ with $n \geq 2$, and let $\mathbf{F}_q$ be a finite field of characteristic p. There exists an explicit constant*[2] *$C_{r,q}$ such that if $A \subset \mathbb{P}^r_{\mathbf{F}_q}$ is a non-degenerate abelian variety of dimension n, then for any $d \in \mathbb{N}$ satisfying*

$$C_{r,q}\zeta_A\left(n+\tfrac{1}{2}\right)\deg(A) \leq \frac{q^{\frac{d}{\max\{n+1,p\}}}(d+1)}{d^{n+1}+d^n+q^{\frac{d}{\max\{n+1,p\}}}},$$

there exists a smooth geometrically connected curve over $\mathbf{F}_q$ whose Jacobian J maps dominantly onto A, where

$$\dim J \leq \left\lfloor \frac{\deg(A)d^{n-1}-1}{r-1} \right\rfloor \left(\deg(A)d^{n-1} - \frac{\left\lfloor \frac{\deg(A)d^{n-1}-1}{r-1} \right\rfloor + 1}{2}(r-1) - 1 \right).$$

Moreover, if $A \subset \mathbb{P}^r_{\mathbf{F}_q}$ is simple, then for any $d \in \mathbb{N}$ satisfying

$$\deg(A) \leq \frac{(d-1)q^{\frac{1}{2}(d+1)(d+2)}}{d^{n-1}-1},$$

[1] This chapter is based on the contents of [BL18]

[2] See Proposition 4.13 for a more precise statement where the constant is explicitly stated.

there exists a smooth geometrically connected curve over $\mathbf{F}_q$ *whose Jacobian* J *maps dominantly onto* A*, where*

$$\dim J \leq \deg(A)d^{n-1}\left(\deg(A)d^{n-1}+1\right).$$

Over an infinite field the fact that every abelian variety is covered by the Jacobian variety of a smooth connected curve is long known. The key idea, which we review (and slightly extend) in Proposition 4.4, is this: if $A \subset \mathbb{P}^r_{\mathbf{k}}$ is an embedded n-dimensional abelian variety, and C is a smooth curve which arises as the intersection of A with a linear subspace $L \subset \mathbb{P}^r_{\mathbf{k}}$ of codimension $n-1$, then $\mathrm{Jac}(C)$ will cover A. It is thus sufficient to find a linear subspace of codimension $n-1$ which intersects A in a smooth curve. Over an infinite field, such a linear space exists by Bertini's Theorem.

When the base field $\mathbf{k}$ is a finite field, the situation is substantially more subtle. For instance, it need no longer be the case that there exists even a single hyperplane in $\mathbb{P}^r_{\mathbf{k}}$ that has a smooth intersection with A. Poonen's Bertini Theorem shows that while one cannot necessarily find smooth hyperplane sections, smooth hypersurface sections always exist if the degree of the hypersurface is allowed to be arbitrarily high [Poo04, Theorem 1.1]. By induction, there exist homogeneous polynomials $f_1, \ldots, f_{n-1}$ of high enough degree such that $A \cap \mathbb{V}(f_1, \ldots, f_{n-1})$ is a smooth connected curve. This implies the existence of a Jacobian variety mapping dominantly onto A when $\mathbf{k}$ is a finite field.

While Poonen's result is enough to show existence, it is not enough to provide the explicit bounds appearing in Theorem A. For example, one does not necessarily know what the degrees of $f_1, \ldots, f_{n-1}$ may be. In fact, since the construction of the f_k is inductive, it may be the case that the choice of $f_1, \ldots, f_{k-1}$ affects the degree of f_k. Existence was also proved over finite fields independently by Gabber using different methods [Gab01, Corollary 2.5]; however, this also does not provide explicit bounds.

We prove Theorem A by first proving an effective version of Poonen's result with explicit bounds.

Theorem 4.2. *Fix $r, n \in \mathbb{N}$ with $n \geq 2$, and let $\mathbf{F}_q$ be a finite field of characteristic p. For any $1 \leq k \leq n-1$ there exists an explicit constant*[3] *$C_{r,q}$ such that if $X \subset \mathbb{P}^r_{\mathbf{F}_q}$ is a smooth quasi-projective subscheme of dimension n, then for any $d \in \mathbb{N}$ satisfying*

$$C_{r,q} \deg(X) \zeta_X\left(n+\tfrac{1}{2}\right) < \frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}{d^n + d^{n+\frac{2k-1}{n}} + q^{\frac{d}{\max\{n+1,p\}}}},$$

there exist homogeneous polynomials $f_1, \ldots, f_k \in \mathbf{F}_q[x_0, \ldots, x_r]$ of degree d such that $X \cap \mathbb{V}(f_1, \ldots, f_k)$ is smooth of dimension $n-k$. Moreover, if X is projective and geometrically connected then $X \cap \mathbb{V}(f_1, \ldots, f_k)$ is also geometrically connected.

Our proof of this theorem builds upon work of Bucur and Kedlaya [BK12], which in part allows us to choose all of the hypersurfaces at once instead of going through an inductive argument. We prove non-trivial bounds on the error terms and the Euler product appearing in [BK12, Theorem 1.2], which allow us to deduce the explicit bound appearing in Theorem B.

From this effective Bertini theorem over finite fields applied to abelian varieties, we deduce Theorem A as follows: first we use Theorem B to produce a smooth connected curve C on A whose degree is explicitly bounded and which arises as an intersection $C = A \cap V(f_1, \ldots, f_{n-1})$. Then we use Proposition 4.4 to show that $\mathrm{Jac}(C)$ covers A, and finally we use a classical theorem of Castelnuovo to bound the genus of C.

In the case when the abelian variety A is simple, the condition of $A \cap \mathbb{V}(f_1, \ldots, f_{n-1})$ being smooth can be dropped, and this allows us to lower the degree and genus bounds. To construct an explicit smooth curve whose Jacobian dominates A, we just need a curve (not necessarily smooth or even reduced) given by the intersection of A with hypersurfaces. Using recent work of the first author and Erman, characterizing the probability that randomly choosing homogeneous polynomials $f_1, \ldots, f_{n-1}$ of degree d that intersect A in a (not necessarily smooth) curve [BE16, Theorem B, Proposition 5.1], we show that when A is simple, hypersurfaces of smaller degree suffice. This results in the better bound seen in Theorem A.

Since we work with non-smooth curves in the case where A is simple, we cannot use Castelnuovo's bound for the genus. We thus prove a more general degree-genus bound

[3] See Proposition 4.10 for a more precise statement where the constant is explicitly stated.

that holds for any connected, reduced curve. The key idea of this proof is to combine a Hilbert function argument with the Gruson-Lazarsfeld-Peskine bound on Castelnuovo-Mumford regularity of any such curve [GLP83, Gia06].

As an application of Theorem A, we show the existence of a smooth connected curve with bounded genus whose Jacobian has an arbitrary number of copies of an elliptic curve as isogeny factors.

Corollary 4.3. *Let $\mathbf{F}_q$ be a finite field and for any $n \in \mathbb{N}$, there exists an explicit constant $B_{n,q}$ such that for any E, an elliptic curve over $\mathbf{F}_q$, there exists a smooth geometrically connected curve C of genus $g \leq B_{n,q}$ defined over $\mathbf{F}_q$ such that $\mathrm{Jac}(C)$ admits E^n as an isogeny factor.*

This chapter is organized as follows. §4.2 gathers background results about abelian varieties. In §4.3 we prove Theorem B. In §4.4 we use Theorem B to prove the general statement in Theorem A. §4.5 concludes the proof of Theorem A by handling the case of simple abelian varieties. §4.6 presents the proof of Corollary 4.3.

Conventions

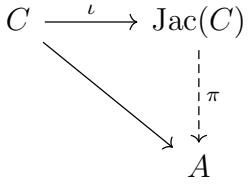
We let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the natural numbers and $\mathbb{Z}$ be the integers. Throughout the paper, $\mathbf{k}$ will denote a field, and $\mathbf{F}_q$ will be a finite field of characteristic p for some prime $p > 0$. By a curve over a field $\mathbf{k}$, we refer to a complete separated equidimensional scheme of finite type over $\mathbf{k}$ of dimension one. By equidimensional we mean that all of the irreducible components have the same dimension and that there are no embedded components. We will say a scheme X over a field $\mathbf{k}$ is smooth if its structure morphism is smooth. We discuss the Jacobian variety associated to a smooth connected curve C as defined in [Mil08, Section III.1, pg. 86] and we denote the Jacobian variety of such a curve C by $\mathrm{Jac}(C)$. By abelian variety over a field $\mathbf{k}$, we mean a geometrically reduced, separated, group scheme of finite type over $\mathbf{k}$ that is both complete and geometrically connected [Mil08, Section I.1, pg. 8]. When

discussing a polynomial ring $\mathbf{k}[x_0, \ldots, x_r]$ over a field $\mathbf{k}$, we will always assume it has the standard $\mathbb{N}$-grading where $\deg(x_i) = 1$ for all i.

4.2 Background on Abelian Varieties

Here we collect some classical results regarding abelian varieties, each adapted from [Mil08, Section III].

Let A be an abelian variety and C be a smooth connected curve together with a map $C \to A$. By the universal property of Jacobians, one has the following diagram:



where $\iota : C \to \mathrm{Jac}(C)$ is an Abel-Jacobi map for C. In general, the map π need not be surjective. However, if the curve C arises as a complete intersection on A – i.e. if there exist homogeneous polynomials $f_1, \ldots, f_{n-1}$ on $\mathbb{P}^r_{\mathbf{k}}$ such that $C = A \cap \mathbb{V}(f_1, \ldots, f_{n-1})$ – then the map π is surjective. This is the content of the following proposition.

Proposition 4.4. *Let $A \subset \mathbb{P}^r_{\mathbf{k}}$ be an abelian variety of dimension n over a field $\mathbf{k}$. If $f_1, \ldots, f_{n-1} \in \mathbf{k}[x_0, \ldots, x_r]$ are homogeneous polynomials such that $C := A \cap \mathbb{V}(f_1, \ldots, f_{n-1})$ is a smooth geometrically connected curve, then the induced map $\pi : \mathrm{Jac}(C) \to A$ is surjective.*

The case where the f_i's are linear forms is Theorem 10.1 in [Mil08, Section III], and the key adaptation here is allowing hypersurfaces of higher degree. To do this, we need the following lemma, which is adapted from Lemma 10.3 in [Mil08, Section III].

Lemma 4.5. *Let $X \subset \mathbb{P}^r_{\mathbf{k}}$ be a projective subscheme of dimension ≥ 2 defined over a field $\mathbf{k}$, and $X' = X \cap H$ be a hypersurface section of X. Let Y be a geometrically normal, geometrically integral, projective scheme. If $\psi : Y \to X$ is a finite map then $\psi^{-1}(X')$ is geometrically connected.*

Proof. Since the hypotheses are stable under base change, it is enough to assume that $\mathbf{k}$ is algebraically closed and show that $\psi^{-1}(X')$ is connected. Since X' is the restriction of an ample divisor on $\mathbb{P}^r_{\mathbf{k}}$ to X, it remains ample. Since ψ is a finite morphism, it is quasi-affine. Thus $\psi^{-1}(X')$ is the support of an ample divisor [TS18, Lemma 0892]. Finally, since $\mathbf{k}$ is algebraically closed and Y is integral and normal we may apply Corollary 7.9 of [Har77, Section III], which implies the desired claim. □

Proof of Proposition 4.4. Consider the image of π, which we denote by A_1. Compositing with a translation on A wouldn't affect surjectivity of the map. Without loss of generality, we assume π is a group homomorphism. Thus, A_1 is an abelian subvariety of A. Towards a contradiction, suppose that $A_1 \neq A$. If this was the case, then there exists an abelian subvariety $A_2 \subset A$ such that the map $\phi : A_1 \times A_2 \to A$ given by $(a_1, a_2) \mapsto a_1 + a_2$ is an isogeny [Mil08, Proposition I.10.1].

Now let $m \in \mathbb{N}$ be relatively prime to the characteristic of $\mathbf{k}$, and consider the map ψ:

$$A_1 \times A_2 \xrightarrow{1\times m} A_1 \times A_2 \xrightarrow{\phi} A, \qquad \psi = \phi \circ (1\times m)$$

given by the composition of two isogenies. Let proj : $A_1 \times A_2 \to A_2$ be the projection map. We wish to show that $\mathrm{proj}(\psi^{-1}(C))$ is equal to $\mathrm{proj}(\psi^{-1}(O))$ where O is the identity element of A. The key point is that since $C \subset A_1 \subset A$ if $\phi(a_1, a_2) \in C$ then $a_1 + a_2 \in A_1$ implying that $a_2 = (a_1 + a_2) - a_1$ is contained in A_1. Phrased differently $\phi^{-1}(C)$ is equal to $\{(a_1 - a_2, a_2) \mid a_1 \in C, \ \ a_2 \in A_1 \cap A_2\}$. The equality now follows from the fact that the kernel of ϕ is $\{(a, -a) \mid a \in A_1 \cap A_2\}$.

Since ϕ is an isogeny the kernel of ϕ, which is $\{(a, -a) \mid a \in A_1 \cap A_2\}$, is finite. Thus, $A_1 \cap A_2$ is a finite set, and moreover, $A_1 \cap A_2$ is non-empty since the identity element of A is contained in $A_1 \cap A_2$. As m is relatively prime to the characteristic of our ground field, multiplication by m is a finite map of degree m^{2n} where n is the dimension of A_2. Thus, $\mathrm{proj}(\psi^{-1}(C))$ is a finite set of size $m^{2n}|A_1 \cap A_2| > 1$, which implies that $\psi^{-1}(C)$ is not geometrically connected. However, applying Lemma 4.5 repeatedly shows that $\psi^{-1}(C)$

is geometrically connected, providing a contradiction. So, we conclude $A_1 = A$ and π is surjective. □

4.3 Effective Bertini Theorem over Finite Fields

In this section we establish an effective Bertini Theorem over finite fields, proving Theorem B. This section also contains a technical version of Theorem B, Proposition 4.10, where all constants are explicitly stated.

A key ingredient in the proof of these results is recent work of Bucur and Kedlaya [BK12] which characterizes the probability that the intersection of an n-dimensional quasi-projective subscheme X with k randomly chosen hypersurfaces of given degrees is smooth of dimension $n-k$. While Bucur and Kedlaya's result is not itself effective, it does contain an explicit error term. We carefully analyze this error term to produce an effective Bertini Theorem.

Before stating their result and using it to prove Theorem B, we fix a bit of notation. Let $S = \mathbf{F}_q[x_0, \ldots, x_r]$ be the homogeneous coordinate ring of $\mathbb{P}^r_{\mathbf{F}_q}$. Given a tuple $\mathbf{d} = (d_1, \ldots, d_k) \in \mathbb{N}^k$ we set

$$S_{\mathbf{d}} = S_{d_1} \oplus S_{d_2} \oplus \cdots \oplus S_{d_k},$$

where S_{d_i} is the $\mathbf{F}_q$-vector space of homogeneous polynomials of degree d_i in S. Further, given an element $f_{F'/F} = (f_1, \ldots, f_k) \in S_{\mathbf{d}}$ we write $\mathbb{V}(f_{F'/F})$ for $\mathbb{V}(f_1, \ldots, f_k) \subset \mathbb{P}^r_{\mathbf{F}_q}$. The probability that k uniformly chosen vectors in $\mathbf{F}_q^n$ are linearly independent is denoted as follows

$$L(q, n, k) = \prod_{j=0}^{k-1} \left(1 - q^{-(n-j)}\right).$$

With this notation in hand we now state Bucur and Kedlaya's result.

Theorem 4.6. [BK12, Theorem 1.2] *Let $X \subset \mathbb{P}^r_{\mathbf{F}_q}$ be a smooth quasi-projective subscheme of dimension $n \geq 0$ over a finite field $\mathbf{F}_q$ of characteristic p. Choose an integer $k \in \{1, \ldots, n-1\}$, a degree sequence $\mathbf{d} = (d_1 \leq d_2 \leq \cdots \leq d_k)$, and set*

$$\mathcal{P}_{\mathbf{d}} = \left\{ f_{F'/F} \in S_{\mathbf{d}} \;\middle|\; \begin{array}{c} X \cap \mathbb{V}(f_{F'/F}) \text{ has dimension } n-k \\ \text{and is smooth} \end{array} \right\}.$$

Then

$$\left|\frac{\#\mathcal{P}_{\mathbf{d}}}{\#S_{\mathbf{d}}} - \prod_{x\in X}\left(1-q^{-k\deg(x)}+q^{-k\deg(x)}L\left(q^{\deg(x)},n,k\right)\right)\right| \tag{4.1}$$
$$\leq 2^{n+2}\deg(X)kq^{-\delta}+(r+1)kr^n\deg(X)(n+1)d_k^n q^{\frac{-d_1}{\max\{n+1,p\}}},$$

where

$$\delta=(2k-1)\left(1+\left\lfloor\frac{1}{n}\log_q\frac{d_1+1}{(n+1)2^{n+1}}\right\rfloor\right).$$

To prove Theorem B, we need to control the Euler product appearing in the above theorem. In general this is difficult. For example, [BK12, pg. 544] presents numerical evidence suggesting it cannot be interpreted as a zeta function. But we are able to provide a lower bound for it in terms of a zeta function value.

Proposition 4.7. *Let $X\subset\mathbb{P}^r_{\mathbf{F}_q}$ be a smooth quasi-projective subscheme of dimension $n\geq 0$ defined over a finite field $\mathbf{F}_q$. Fix $1\leq k\leq n-1$. If $q\geq 3$ then*

$$\zeta_X\left(n+\tfrac{1}{2}\right)^{-1}\leq\prod_{x\in X}\left(1-q^{-k\deg(x)}+q^{-k\deg(x)}L\left(q^{\deg(x)},n,k\right)\right),$$

and if $q=2$ then

$$2^{-\#X(\mathbf{F}_2)}\zeta_X\left(n+\tfrac{1}{2}\right)^{-1}\leq\prod_{x\in X}\left(1-q^{-k\deg(x)}+q^{-k\deg(x)}L\left(q^{\deg(x)},n,k\right)\right).$$

To prove this proposition, we need two lemmas.

Lemma 4.8. *If $\{a_i\}_{i=1}^t$ is a sequence of real numbers such that $0<a_i<1$ then*

$$1-\sum_{i=1}^t a_i\leq\prod_{i=1}^t(1-a_i)<1.$$

Proof. The upper bound is immediate from the fact that $0<1-a_i<1$ for all i. For the lower bound we proceed by induction on t with the case when $t=1$ being clear. In the general case by induction we assume

$$1-\sum_{i=1}^{t-1}a_i\leq\prod_{i=1}^{t-1}(1-a_i),$$

and multiplying both sides by $(1-a_t)$ gives

$$1-\sum_{i=1}^{t} a_i \leq 1-\sum_{i=1}^{t} a_i + a_t\left(\sum_{i=1}^{t-1} a_i\right) = \left(1-\sum_{i=1}^{t-1} a_i\right)(1-a_t) \leq \prod_{i=1}^{t}(1-a_i),$$

which completes the inductive step. □

Lemma 4.9. *Fix $1 \leq k \leq n-1$. If either $q \geq 3$ and $t \geq 1$ or if $q = 2$ and $t > 1$ then*

$$1 - q^{-\left(n-k+\frac{1}{2}\right)t} \leq L\left(q^t, n, k\right).$$

Moreover, if $q = 2$ and $t = 1$ we have

$$\tfrac{1}{2}\left(1 - 2^{-\left(n-k+\frac{1}{2}\right)}\right) \leq L\left(2, n, k\right).$$

Proof. Combining the definition of $L\left(q^t, n, k\right)$ with Lemma 4.8 we know that

$$1-\sum_{i=0}^{k-1} q^{-(n-i)t} \leq \prod_{i=0}^{k-1}\left(1-q^{-(n-i)t}\right) = L\left(q^t, n, k\right).$$

Since the left-hand side is a geometric sum we may rewrite this inequality as

$$1-\frac{q^{-(n-k+1)t}-q^{-(n+1)t}}{1-q^{-t}} = 1-\sum_{i=0}^{k-1} q^{-(n-i)t} \leq L\left(q^t, n, k\right),$$

which we may further simplify to

$$1-\frac{q^{-(n-k+1)t}}{1-q^{-t}} \leq 1-\frac{q^{-(n-k+1)t}-q^{-(n+1)t}}{1-q^{-t}} \leq L\left(q^t, n, k\right).$$

Now we shift to showing that in the cases when $q \geq 3$ and $t \geq 1$ or $q = 2$ and $t > 1$

$$1 - q^{-\left(n-k+\frac{1}{2}\right)t} \leq 1-\frac{q^{-(n-k+1)t}}{1-q^{-t}}.$$

Rearranging the terms, one sees the above inequality is equivalent to

$$\frac{q^{-\frac{t}{2}}}{1-q^{-t}} = \frac{q^{-(n-k+1)}q^{\left(n-k+\frac{1}{2}\right)t}}{1-q^{-t}} \leq 1. \tag{4.2}$$

Notice the above inequality is equivalent to $q^t - q^{\frac{t}{2}} - 1 \geq 0$ Since $x^2 - x - 1 \geq 0$ for all $x \geq \frac{1}{2}(1+\sqrt{5})$ it is thus enough for $q^{\frac{t}{2}} \geq \frac{1}{2}(1+\sqrt{5})$, however, is true since $q \geq 3$ and $t \geq 1$ and so $q^{\frac{t}{2}} \geq \sqrt{3} > \frac{1}{2}(1+\sqrt{5})$.

Finally we focus on the remaining case, when $q = 2$ and $t = 1$. From our work above we know

$$1 - \frac{q^{-(n-k+1)t}}{1-q^{-t}} \leq 1 - \frac{q^{-(n-k+1)t} - q^{-(n+1)t}}{1-q^{-t}} \leq L\left(q^t, n, k\right),$$

and so it is enough to show that

$$\tfrac{1}{2}\left(1 - 2^{-\left(n-k+\frac{1}{2}\right)}\right) \leq 1 - 2^{-(n-k)} = 1 - \frac{2^{-(n-k+1)}}{1-2^{-1}}.$$

Rearranging the terms, this inequality is equivalent to

$$1 \leq 2^{n-1-k} + 2^{-\frac{3}{2}}.$$

The right-hand side is minimized when $k = n-1$, in which case it is equal to $1 + 2^{-\frac{3}{2}}$, and so the desired inequality holds for all $1 \leq k \leq n-1$. □

Proof of Proposition 4.7. By Lemma 4.9, if $q \geq 3$ then

$$\begin{aligned}
&\zeta_X\left(n+\tfrac{1}{2}\right)^{-1} \\
&\qquad = \prod_{x\in X}\left(1 - q^{-\left(n+\frac{1}{2}\right)\deg(x)}\right) \\
&\qquad = \prod_{x\in X}\left(1 - q^{-k\deg(x)} + q^{-k\deg(x)}\left(1 - q^{-\left(n-k+\frac{1}{2}\right)\deg(x)}\right)\right) \\
&\qquad \leq \prod_{x\in X}\left(1 - q^{-k\deg(x)} + q^{-k\deg(x)} L\left(q^{\deg(x)}, n, k\right)\right).
\end{aligned}$$

Similarly in the $q = 2$ case for points $x \in X$ of degree not one Lemma 4.9 tells us that

$$\prod_{\substack{x\in X\\ \deg(x)\neq 1}}\left(1 - q^{-\left(n+\frac{1}{2}\right)\deg(x)}\right) \leq \prod_{\substack{x\in X\\ \deg(x)\neq 1}}\left(1 - q^{-k\deg(x)} + q^{-k\deg(x)} L\left(q^{\deg(x)}, n, k\right)\right). \tag{4.3}$$

On the other hand for points $x \in X$ of degree one Lemma 4.9 implies that

$$\prod_{\substack{x\in X\\ \deg(x)=1}} \tfrac{1}{2}\left(1-q^{-\left(n+\frac{1}{2}\right)}\right) = \prod_{\substack{x\in X\\ \deg(x)=1}} \left(\tfrac{1}{2}-\tfrac{1}{2}q^{-k\deg(x)}+\tfrac{1}{2}q^{-k\deg(x)}\left(1-q^{-\left(n-k+\frac{1}{2}\right)\deg(x)}\right)\right) \tag{4.4}$$

$$\leq \prod_{\substack{x\in X\\ \deg(x)=1}} \left(1-q^{-k\deg(x)}+\tfrac{1}{2}q^{-k\deg(x)}\left(1-q^{-\left(n-k+\frac{1}{2}\right)\deg(x)}\right)\right) \tag{4.5}$$

$$\leq \prod_{\substack{x\in X\\ \deg(x)=1}} \left(1-q^{-k\deg(x)}+q^{-k\deg(x)}L\left(q^{\deg(x)},n,k\right)\right). \tag{4.6}$$

Multiplying Inequality (4.3) and Inequality (4.4) gives the result in the case when $q=2$. □

We now prove the following proposition, which is a more precise version of Theorem B.

Proposition 4.10. *Let $X \subset \mathbb{P}^r_{\mathbf{F}_q}$ be a smooth quasi-projective subscheme of dimension $n \geq 2$ defined over a finite field $\mathbf{F}_q$ of characteristic p. Fix $1 \leq k \leq n-1$. Under either of the following circumstances*

1. *$q \geq 3$, and $d \in \mathbb{N}$ satisfies the inequality*

$$k2^{n+2k+1+\frac{2k-1}{n}}(n+1)^{1+\frac{2k-1}{n}}(r+1)r^n \deg X \zeta_X\left(n+\tfrac{1}{2}\right) < \frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}{d^n+d^{n+\frac{2k-1}{n}}+q^{\frac{d}{\max\{n+1,p\}}}}, \tag{4.7}$$

2. *or $q=2$, and $d \in \mathbb{N}$ satisfies the inequality*

$$k2^{n+2k+1+\frac{2k-1}{n}+\#X(\mathbf{F}_2)}(n+1)^{1+\frac{2k-1}{n}}(r+1)r^n \deg X \zeta_X\left(n+\tfrac{1}{2}\right) < \frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}{d^n+d^{n+\frac{2k-1}{n}}+q^{\frac{d}{\max\{n+1,p\}}}},$$

there exist homogeneous polynomials $f_1,\ldots,f_k \in \mathbf{F}_q[x_0,\ldots,x_r]$ of degree d such that $X \cap \mathbb{V}(f_1,\ldots,f_k)$ is smooth of dimension $n-k$. Moreover, if X is projective and geometrically connected then $X \cap \mathbb{V}(f_1,\ldots,f_k)$ is also geometrically connected.

Proof. Setting $d = d_1 = d_2 \cdots = d_k$ we wish to show that $\frac{\#\mathcal{P}_{\mathbf{d}}}{\#S_{\mathbf{d}}} > 0$, which since $\frac{\#\mathcal{P}_{\mathbf{d}}}{\#S_{\mathbf{d}}} \geq 0$ is equivalent to showing that $\frac{\#\mathcal{P}_{\mathbf{d}}}{\#S_{\mathbf{d}}} \neq 0$. By Theorem 4.6:

$$\left| \frac{\#\mathcal{P}_{\mathbf{d}}}{\#S_{\mathbf{d}}} - \prod_{x \in X} \left(1 - q^{-k \deg(x)} + q^{-k \deg(x)} L\left(q^{\deg(x)}, n, k\right)\right) \right| \tag{4.8}$$

$$\leq 2^{n+2} \deg(X) k q^{-\delta} + (r+1) k r^n \deg(X)(n+1) d_k^n q^{\frac{-d_1}{\max\{n+1,p\}}}, \tag{4.9}$$

and so to show that $\frac{\#\mathcal{P}_{\mathbf{d}}}{\#S_{\mathbf{d}}} \neq 0$ it is enough to show that

$$2^{n+2} \deg(X) k q^{-\delta} + (r+1) k r^n \deg(X)(n+1) d^n q^{\frac{-d}{\max\{n+1,p\}}} \tag{4.10}$$

$$< \prod_{x \in X} \left(1 - q^{-k \deg(x)} + q^{-k \deg(x)} L\left(q^{\deg(x)}, n, k\right)\right). \tag{4.11}$$

Using Proposition 4.7 to bound the right-hand side of the above inequality it is enough to show that:

$$\begin{aligned} 2^{n+2} \deg(X) k q^{-\delta} + (r+1) k r^n \deg(X)(n+1) d^n q^{\frac{-d}{\max\{n+1,p\}}} & \\ < \zeta_X\left(n + \tfrac{1}{2}\right)^{-1} \qquad (q \neq 2) & \\ 2^{n+2} \deg(X) k q^{-\delta} + (r+1) k r^n \deg(X)(n+1) d^n q^{\frac{-d}{\max\{n+1,p\}}} & \\ < 2^{-\#X(\mathbf{F}_2)} \zeta_X\left(n + \tfrac{1}{2}\right)^{-1} \qquad (q = 2). & \end{aligned} \tag{4.12}$$

We now proceed by bounding the left-hand side of Inequality (4.12). Since r, k, and n are positive constants and $r \geq 1$, the left-hand side of Inequality (4.12) satisfies the following:

$$2^{n+2} \deg(X) k q^{-\delta} + (r+1) k r^n \deg(X)(n+1) d^n q^{\frac{-d}{\max\{n+1,p\}}} \tag{4.13}$$

$$\leq k 2^{n+2} (n+1)(r+1) r^n \deg X \left[q^{-\delta} + d^n q^{\frac{-d}{\max\{n+1,p\}}}\right]. \tag{4.14}$$

With δ as in Theorem 4.6 we may bound δ as follows:

$$\frac{2k-1}{n} \log_q \frac{d+1}{(n+1)2^{n+1}} \tag{4.15}$$

$$= (2k-1)\left(1 + \frac{1}{n} \log_q \frac{d+1}{(n+1)2^{n+1}} - 1\right) \tag{4.16}$$

$$\leq (2k-1)\left(1 + \left\lfloor \frac{1}{n} \log_q \frac{d+1}{(n+1)2^{n+1}} \right\rfloor\right) \tag{4.17}$$

$$= \delta. \tag{4.18}$$

This allows us to bound $q^{-\delta}$ from above, giving an upper bound for the right-hand side of Inequality (4.13):

$$k2^{n+2}(n+1)(r+1)r^n \deg X \left[q^{-\delta} + d^n q^{\frac{-d}{\max\{n+1,p\}}}\right] \tag{4.19}$$

$$\leq k2^{n+2}(n+1)(r+1)r^n \deg X \left[\left(\tfrac{(n+1)2^{n+1}}{d+1}\right)^{\frac{2k-1}{n}} + d^n q^{\frac{-d}{\max\{n+1,p\}}}\right]. \tag{4.20}$$

Since n is a positive constant, we may give an upper bound to the right-hand side of Inequality (4.19) by "pulling out" $((n+1)2^{n+1})^{\frac{2k-1}{n}}$. Further since $d \geq 1$ we may bound $(d+1)^{\frac{2k-1}{n}}$ below by $d^{\frac{2k-1}{n}} + 1$. This allows us to bound the right-hand side of Inequality (4.19) from above by the following:

$$k2^{n+2k+1+\frac{2k-1}{n}}(n+1)^{1+\frac{2k-1}{n}}(r+1)r^n \deg X \left[\frac{d^n + d^{n+\frac{2k-1}{n}} + q^{\frac{d}{\max\{n+1,p\}}}}{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}\right]. \tag{4.21}$$

Combining Inequalities (4.13), (4.19), and (4.21) we get our final upper bound for the left-hand side of Inequality (4.12):

$$2^{n+2}\deg X k q^{-\delta} + (r+1)kr^n \deg X (n+1)d^n q^{\frac{-d}{\max\{n+1,p\}}} \tag{4.22}$$

$$\leq k2^{n+2k+1+\frac{2k-1}{n}}(n+1)^{1+\frac{2k-1}{n}}(r+1)r^n \deg X \left[\frac{d^n + d^{n+\frac{2k-1}{n}} + q^{\frac{d}{\max\{n+1,p\}}}}{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}\right]. \tag{4.23}$$

So by Inequalities (4.12) and (4.22) if $d \in \mathbb{N}$ satisfies:

$$k2^{n+2k+1+\frac{2k-1}{n}}(n+1)^{1+\frac{2k-1}{n}}(r+1)r^n \deg X \left[\frac{d^n + d^{n+\frac{2k-1}{n}} + q^{\frac{d}{\max\{n+1,p\}}}}{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}\right]$$
$$< \zeta_X\left(n+\tfrac{1}{2}\right)^{-1} \qquad (q \neq 2)$$

$$k2^{n+2k+1+\frac{2k-1}{n}}(n+1)^{1+\frac{2k-1}{n}}(r+1)r^n \deg X \left[\frac{d^n + d^{n+\frac{2k-1}{n}} + q^{\frac{d}{\max\{n+1,p\}}}}{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{2k-1}{n}}+1\right)}\right]$$
$$< 2^{-\#X(\mathbf{F}_2)}\zeta_X\left(n+\tfrac{1}{2}\right)^{-1} \qquad (q = 2).$$

then such d also satisfies Inequality (4.10) meaning that $\frac{\#\mathcal{P}_\mathbf{d}}{\#S_\mathbf{d}} > 0$.

Finally, since X is smooth it is geometrically reduced [TS18, Lemma 056T]. In particular, if X is geometrically connected then it is geometrically integral. Thus, if X is also projective, then since $n \geq 2$ and $n - k \geq 1$ we may inductively apply [Har77, Section III, Corollary 7.9] to deduce that $X \cap \mathbb{V}(f_1, \ldots, f_k)$ is geometrically connected. □

Remark 4.11. *The inequalities appearing in Proposition 4.10 are eventually true for d sufficiently large since the right-hand sides tend to infinity as $d \to \infty$ while the left-hand side is independent of d.*

Proof of Theorem B. Since $\#X(\mathbf{F}_2) \leq \#\mathbb{P}^r(\mathbf{F}_2) = 2^{r+1} - 1$, we can bound $\#X(\mathbf{F}_2)$ in terms of just r. Thus, by Proposition 4.10 if we let

$$C_{r,q} = \begin{cases} 2^{3r-1}(r+1)^5 r^r & \text{if } q \neq 2 \\ 2^{3r+2^{r+1}-1}(r+1)^5 r^r & \text{if } q = 2 \end{cases}$$

there exists homogeneous polynomials $f_1, \ldots, f_k \in \mathbf{F}_q[x_0, \ldots, x_r]$ of degree d such that $X \cap \mathbb{V}(f_1, \ldots, f_k)$ is smooth of dimension $n-k$, which is geometrically connected if X is projective and geometrically connected. □

Remark 4.12. *Regarding Theorem B, Poonen has pointed out to us, in personal communication, that by using a noetherian induction argument, one can show the existence of a bound dependent solely on r and the degree of X. While such a bound would be ineffective, it would be independent of q and n.*

4.4 Smooth Curves of Bounded Genus and Degree

We now bound the degree and genus of the smooth curves $C \subset X$ we constructed in the previous section.

Proposition 4.13. *Let $X \subset \mathbb{P}^r_{\mathbf{F}_q}$ be a smooth projective subscheme of dimension $n \geq 2$ defined over a finite field $\mathbf{F}_q$ of characteristic p. Under either of the following circumstances*

1. *$q \geq 3$, and $d \in \mathbb{N}$ satisfies the inequality*

$$2^{3n+3}\deg(X)n^4r^{n+1}\zeta_X\left(n+\tfrac{1}{2}\right) \leq \frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{1}{2}}+1\right)}{d^{n+2}+d^n+q^{\frac{d}{\max\{n+1,p\}}}},$$

2. *or $q = 2$, and $d \in \mathbb{N}$ satisfies the inequality*

$$2^{3n+\#X(\mathbf{F}_2)+3}\deg(X)n^4r^{n+1}\zeta_X\left(n+\tfrac{1}{2}\right) \leq \frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{1}{2}}+1\right)}{d^{n+2}+d^n+q^{\frac{d}{\max\{n+1,p\}}}},$$

there exist homogeneous polynomials $f_1,\ldots,f_{n-1} \in \mathbf{F}_q[x_0,\ldots,x_r]$ of degree d such that $X \cap \mathbb{V}(f_1,\ldots,f_{n-1})$ is a smooth curve and $\deg(C) = \deg(X)d^{n-1}$. Moreover, if X is projective and geometrically connected then $X \cap \mathbb{V}(f_1,\ldots,f_{n-1})$ is also geometrically connected.

Proof. As $n, r \geq 1$ note that $(n-1)(n+1)^{3-\frac{3}{n}}(r+1)r^n \leq 4n^4r^{n+1}$, and so

$$\begin{aligned}
&2^{3n-\frac{3}{n}+1}\deg(X)(n-1)(n+1)^{3-\frac{3}{n}}(r+1)r^n\zeta_X\left(n+\frac{1}{2}\right)\\
\leq&2^{3n+3}\deg(X)n^4r^{n+1}\zeta_X\left(n+\tfrac{1}{2}\right)\\
&2^{3n-\frac{3}{n}+\#X(\mathbf{F}_2)+1}\deg(X)(n-1)(n+1)^{3-\frac{3}{n}}(r+1)r^n\zeta_X\left(n+\tfrac{1}{2}\right)\\
\leq&2^{3n+\#X(\mathbf{F}_2)+3}\deg(X)n^4r^{n+1}\zeta_X\left(n+\tfrac{1}{2}\right).
\end{aligned}$$

Moreover, we see that

$$\frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{\frac{1}{2}}+1\right)}{d^{n+2}+d^n+q^{\frac{d}{\max\{n+1,p\}}}} \leq \frac{q^{\frac{d}{\max\{n+1,p\}}}\left(d^{2-\frac{3}{n}}+1\right)}{d^n+d^{n+2-\frac{3}{n}}+q^{\frac{d}{\max\{n+1,p\}}}}.$$

Thus, given $d \in \mathbb{N}$ as in the statement of this proposition then applying Proposition 4.10 in the case when $k = n-1$ there exist the desired homogeneous polynomials $f_1,\ldots,f_{n-1} \in \mathbf{F}_q[x_0,\ldots,x_r]$ of degree d such that $X \cap \mathbb{V}(f_1,\ldots,f_{n-1})$ is a smooth curve. Further, Bezout's Theorem [Ful98, Proposition 8.4] implies

$$\deg(C) = \deg(X)\prod_{i=1}^{n-1}\deg(f_i) = \deg(X)d^{n-1}.$$

Finally, as stated in Proposition 4.10 if X is projective and geometrically connected then $X \cap \mathbb{V}(f_1,\ldots,f_{n-1})$ is geometrically connected.

□

To show the existence of smooth connected curves with bounded genus, we use a classical theorem of Castelnuovo which gives an upper bound on the genus of an irreducible, smooth, non-degenerate curve $X \subset \mathbb{P}^r$ in terms of $\deg X$ and r. (Recall a scheme $X \subset \mathbb{P}^r$ is non-degenerate if it is not contained in any hyperplane.)

Proposition 4.14. *Let $X \subset \mathbb{P}^r_{\mathbf{F}_q}$ be a smooth non-degenerate projective geometrically connected subscheme of dimension $n \geq 2$ defined over a finite field $\mathbf{F}_q$ of characteristic p. If $d \geq 2$ is a natural number satisfying the condition in Proposition 4.13, then there exists a smooth geometrically connected non-degenerate curve $C \subset X$ such that*

$$g(C) \leq \left\lfloor \frac{\deg(X)d^{n-1}-1}{r-1} \right\rfloor \left(\deg(X)d^{n-1} - \frac{\left\lfloor \frac{\deg(X)d^{n-1}-1}{r-1} \right\rfloor + 1}{2}(r-1) - 1 \right).$$

Proof. By Proposition 4.13, for such $d \geq 2$ there exists a smooth geometrically connected curve $C \subset X$ with $\deg(C) = \deg(X)d^{n-1}$. To show that C is non-degenerate it is enough, by induction, to show that $X \cap \mathbb{V}(f_1)$ is non-degenerate. If $X \cap \mathbb{V}(f_1)$ were degenerate, and so contained in a linear subspace $L \subset \mathbb{P}^r_{\mathbf{F}_q}$, then $X \cap \mathbb{V}(f_1) \subset X \cap L$, and since X itself is non-degenerate both $X \cap \mathbb{V}(f_1)$ and $X \cap L$ have dimension $n-1$. However, by Bezout's Theorem [Ful98, Proposition 8.4] the degree of $X \cap \mathbb{V}(f_1)$ is equal to $\deg(X)d$, which since $d \geq 2$ is strictly larger than $\deg(X \cap L) = \deg(X)$, giving a contradiction. Finally, applying Castelnuovo's genus bound [Har81, pg. 40] to C gives the stated result. □

We conclude this section with the proof of the statement in Theorem A for general abelian varieties.

Proof of Theorem A (General Case). Since $n \leq r$ by Propositions 4.4 and 4.14, it is enough to show that if $q = 2$ then $\#A(\mathbf{F}_2)$ is bounded by a constant depending only on n and r. This follows immediately from the Weil bounds [AH16, pg. 3], which states that $\#A(\mathbf{F}_2)$ is bounded above by $(3+2\sqrt{2})^n$. Thus, the result follows with $C_{r,q}$ defined as:

$$C_{r,q} = \begin{cases} 2^{3r+3}r^{r+5} & \text{if } q \neq 2 \\ 2^{3r+3+(3+2\sqrt{2})^r}r^{r+5} & \text{if } q = 2 \end{cases}.$$

□

Remark 4.15. *Notice the dependence of $C_{r,q}$ on q is really only dependence on whether or not $q = 2$. Thus, one can easily make $C_{r,q}$ independent of q by adding in the appropriate factors of 2.*

4.5 The Case when A is Simple

When A is a simple abelian variety, our general bound can be simplified as was stated in the second part of Theorem A. This is possible because when A is simple, almost any curve on A, even if it is reducible, non-reduced, or non-smooth, gives rise to a covering of A by a Jacobian.

In particular, suppose that $C \subset A$ is any curve on A. By taking an irreducible component of C considered with the reduced subscheme structure without loss of generality we may assume that C is irreducible and reduced. Now taking the normalization of this irreducible reduced curve C results in a smooth irreducible curve $\tilde{C}$, which maps non-trivially to A. The universal property of Jacobian varieties in turn gives a nonconstant map $\mathrm{Jac}(\tilde{C}) \to A$, and as A is simple this map must be surjective.

Thus, in the simple case, constructing curves whose Jacobians dominate A is easier. One only needs the existence of a (possibly non-smooth, non-reduced, or reducible) curve C contained in A. So it is sufficient to find homogeneous polynomials $f_1, \ldots, f_{n-1}$, which cut out any curve on A. This allows us to choose the $f_1, \ldots, f_{n-1}$ to be of smaller degree, improving bound.

Proposition 4.16. *Let $X \subset \mathbb{P}^r_{\mathbf{F}_q}$ be a smooth projective subscheme of dimension n defined over a finite field $\mathbf{F}_q$. If $d \in \mathbb{N}$ satisfies the following inequality*

$$\deg(X) \leq \frac{(d-1)q^{\frac{1}{2}(d+1)(d+2)}}{d^{n-1}-1},$$

then there exist homogeneous polynomials $f_1, \ldots, f_{n-1} \in \mathbf{F}_q[x_0, ..., x_r]$ of degree d such that $C = X \cap \mathbb{V}(f_1, ..., f_{n-1})$ is a curve and $\deg(C) = \deg(X)d^{n-1}$.

Proof. By combining the given inequality on d with Proposition 5.1 of [BE16] in the case when $k = n-2$ we can find homogeneous polynomials $f_1, ..., f_{n-1}$ of degree d where $X \cap V(f_1, ..., f_{n-1})$ has dimension 1. Bezout's Theorem [Ful98, Proposition 8.4] then gives $\deg(C) = \deg(X) \prod_{i=1}^{n-1} \deg(f_i) = \deg(X) d^{n-1}$. □

To finish the proof of Theorem A, we must be able to bound the genus of the normalization $\tilde{C}$ in terms of the degree of C. As the genus of $\tilde{C}$ is bounded above by the arithmetic genus of C [Har77, Exercise IV.1.8] it is enough to bound the arithmetic genus of C. (We write $p_a(C)$ for the arithmetic genus of a curve C.)

As before, the idea is to use a degree-genus bound. However, since the curves arising in Proposition 4.16 need not be smooth we cannot use Castelnuovo's genus bound. Instead we prove a less sharp, but more general bound by combining a lower bound on the Hilbert function/polynomial with a bound on the Castelnuovo-Mumford regularity.

Lemma 4.17. *If $C \subset \mathbb{P}^r_{\mathbf{k}}$ is a curve with homogeneous coordinate ring R, then* $\dim R_d \geq d+1$ *for any $d \in \mathbb{N}$.*

Proof. Since base change does not affect the Hilbert function, without loss of generality, we may suppose that $\mathbf{k}$ is algebraically closed. Since $\mathbf{k}$ is infinite, there exists a linear form $\ell \in R$, which gives rise to the short exact sequence

$$0 \longrightarrow R(-1) \xrightarrow{\cdot \ell} R \longrightarrow R/\langle \ell \rangle \longrightarrow 0.$$

Using the additivity of the Hilbert function, we see that $\dim R_d = \sum_{k=0}^{d} \dim (R/\langle \ell \rangle)_k$ for any $d \in \mathbb{N}$, and since $R/\langle \ell \rangle$ is one-dimensional, the result now follows by noting that $\dim(R/\langle \ell \rangle)_k \geq 1$ for all $k \geq 0$. □

With this lemma in hand, we prove a more general genus-degree bound that applies to all geometrically connected reduced equidimensional curves.

Lemma 4.18. *If $C \subset \mathbb{P}^r_{\mathbf{k}}$ is a geometrically connected reduced curve, then*

$$p_a(C) \leq \deg(C)(\deg(C)+1) - 2.$$

Proof. Since the hypotheses are stable under base change, without loss of generality, we may suppose that $\mathbf{k}$ is algebraically closed and that C is connected. Let R be the homogeneous coordinate ring of the curve C. The Hilbert polynomial $P_C(t)$ of the curve C is equal to $\deg(C)t + 1 - p_a(C)$. For any $t \geq \operatorname{reg}(C)$, the Hilbert function and Hilbert polynomial agree [Eis05, Theorem 4.2]. Thus, if $t \geq \operatorname{reg}(C)$ then by Lemma 4.17:

$$t + 1 \leq \dim R_t = P_C(t) = \deg(C)t + 1 - p_a(C).$$

Results of Giaimo imply that $\operatorname{reg}(C) \leq \deg(C) + 2$ [Gia06]. Plugging $t = \deg(C) + 2$ into the above inequality yields:

$$\deg(C) + 3 \leq \dim R_{\deg(C)+2} = \deg(C)\left(\deg(C) + 2\right) + 1 - p_a(C).$$

The result now follows from rearranging the above inequality. □

Remark 4.19. *Not only does the bound from Lemma 4.18 apply to non-smooth curves, it also applies to degenerate curves, i.e. curves lying in a hyperplane in $\mathbb{P}^r_{\mathbf{k}}$. In fact, such curves attain the maximal values, as any degree d planar curve will have the maximal possible arithmetic genus.*

Finally, we conclude the proof of Theorem A.

Proof of Theorem A (Simple Case). By Proposition 4.16, there exist homogeneous polynomials $f_1, \ldots, f_{n-1} \in \mathbf{F}_q[x_0, x_1, \ldots, x_r]$ of degree d such that $C = A \cap \mathbb{V}(f_1, f_2, \ldots, f_{n-1})$ is a curve with $\deg(C) = \deg(A)d^{n-1}$. Let $C'_{\text{red}} \subset C$ be an irreducible component of C considered with the reduced subscheme structure. As noted in the beginning of this section, if $\tilde{C}'_{\text{red}}$ is the normalization of C'_{red}, then since A is simple the map $\operatorname{Jac}(\tilde{C}'_{\text{red}}) \to A$ coming from the universal property of Jacobians is surjective. Hence it is enough to bound the genus of $\tilde{C}'_{\text{red}}$.

Towards this, note that $\deg(C'_{\text{red}}) \leq \deg(C)$, and so $\deg(C'_{\text{red}}) \leq \deg(A)d^{n-1}$. Applying Lemma 4.18 and Exercise IV.1.8 in [Har77] to C'_{red}, we see that

$$p_a\left(\tilde{C}'_{\text{red}}\right) \leq p_a\left(C'_{\text{red}}\right) \leq \deg(A)^2 d^{2n-2} + \deg(A)d^{n-1} - 2.$$

Since $\tilde{C}'_{\text{red}}$ is an irreducible smooth curve, its geometric genus is equal to its arithmetic genus, and so

$$g\left(\tilde{C}'_{\text{red}}\right) = p_a\left(\tilde{C}'_{\text{red}}\right) \leq \deg(A)^2 d^{2n-2} + \deg(A) d^{n-1} - 2.$$

□

4.6 Application

As an application of Theorem A, we show the existence of abelian varieties of the form $E^n \times A$ for arbitrary $n \in \mathbb{N}$, where E is an elliptic curve, in the Torelli locus. Recall the Torelli locus $\mathcal{T}_g$ is the image of the Torelli map

$$\begin{aligned} \mathcal{M}_g &\longrightarrow \mathcal{A}_g \\ C &\longmapsto \text{Jac}(C) \end{aligned}$$

between the moduli space of (geometrically irreducible, complete, smooth) curves of genus g and the moduli space of principally polarized abelian varieties of dimension g.

Since the dimension of $\mathcal{M}_g$ is $3g-3$ and the dimension of $\mathcal{A}_g$ is $g(g+1)/2$, the Torelli locus is a proper subscheme of $\mathcal{A}_g$ for $g \geq 4$. In general describing this locus is hard, and relatively little is known. For example, given a principally polarized abelian variety of dimension greater than or equal to 4 over a finite field, it is difficult to determine whether it can be realized as the Jacobian variety of a smooth curve.

Further, since the codimension of $\mathcal{T}_g$ grows with g, for any given stratification of $\mathcal{A}_g$, we expect the Torelli locus to only intersect the relatively generic strata. For example, if we fix an elliptic curve E over $\mathbf{F}_q$ then we may stratify $\mathcal{A}_g$ by the number of copies of E each abelian variety has as isogeny factors. That is to say each stratum has the form $\{E^n\} \times \mathcal{A}_{g-n}$ for $0 \leq n \leq g$. Then we expect the intersection $\mathcal{T}_g \cap \{E^n\} \times \mathcal{A}_{g-n}$ to often be empty for larger n. In particular, we expect the Jacobian of some smooth genus g curve over $\mathbf{F}_q$ to have E^n as an isogeny factor only if n is small relative to g. This is supported by the results in [EHR14].

Proposition 4.20. [EHR14, Corollary 1.3] *Let E be an elliptic curve over a finite field $\mathbf{F}_q$ of characteristic p and $n \in \mathbb{N}$. Let C be a smooth curve of genus g defined over $\mathbf{F}_q$. If E^n is an isogeny factor of $\mathrm{Jac}(C)$ then*

$$g - \sqrt{\frac{\log\log g}{6\log q}} \geq n.$$

Proof. By Corollary 1.3 in [EHR14], $\mathrm{Jac}(C)$ has a simple factor A with dimension at least $\sqrt{\frac{\log\log g}{6\log q}}$. Thus, the dimension of the isogeny factor which decomposes as copies of E is at most $g - \dim A$. □

The previous proposition can be viewed as a lower bound for the genus of curves with a prescribed isogeny factor for their Jacobians. Phrased differently, it says that for g less than the explicit bound in the proposition, the intersection of $\{E^n\} \times \mathcal{A}_{g-n}$ and $\mathcal{T}_g$ is empty.

On the other hand, our Theorem A can be used to construct curves with a prescribed isogeny factor with bounded genus. In particular, Corollary 4.3 implies that while unlikely, there does exist $g \leq B_{n,q}$ such that $\{E^n\} \times \mathcal{A}_{g-n}$ intersects $\mathcal{T}_g$.

Proof of Corollary 4.3. Let E be an elliptic curve defined over $\mathbf{F}_q$. Apply Theorem A in the case when $A = E^n$, with the polarization induced by divisor $E^{n-1} \times \{O\} + E^{n-2} \times \{O\} \times E + \ldots + \{O\} \times E^{n-1}$. There exists a smooth geometrically connected curve C defined over $\mathbf{F}_q$ whose genus satisfies the bound appearing in Theorem A, and $\mathrm{Jac}(C)$ maps dominantly onto E^n. This means $\mathrm{Jac}(C)$ admits a factor isogenous to E^n. Since there are finitely many elliptic curves defined over $\mathbf{F}_q$ we may let $B_{n,q}$ be the maximum of all such constants. □

Remark 4.21. *Recall the a number of an abelian variety A over a field $\mathbf{k}$ of characteristic $p > 0$ is defined as $\dim_{\bar{\mathbf{k}}} \mathrm{Hom}(\alpha_p, A[p])$ where $\alpha_p = \mathrm{Spec}\,\mathbf{k}[x]/\langle x^p \rangle$. The previous corollary allows one to show the existence of Jacobian varieties over $\mathbf{F}_q$ of bounded dimension with an a number at least n.*

In particular, if in Corollary 4.3 we take E to be a supersingular elliptic curve, then with C as in the corollary the a number of $\mathrm{Jac}(C)$ is at least n. Previous results in this

direction, see [Pri], *mainly come from constructing special families of curves over* $\overline{\mathbf{F}}_p$, *thus only providing existence over algebraically closed fields.*

Bibliography

[ABJ16] Julio C. Andrade, Sunghan Bae, and Hwanyup Jung, *Average values of L-series for real characters in function fields*, Res. Math. Sci. **3** (2016), Paper No. 38, 47, DOI 10.1186/s40687-016-0087-4. MR3567720 ↑5, 31

[AB18] J. Andrade and S. Baluyot, *Small zeros of Dirichlet L-functions of quadratic characters of prime modulus* (2018). ArXiv pre-print. ↑5, 31

[AK13] Julio C. Andrade and Jonathan P. Keating, *Mean value theorems for L-functions over prime polynomials for the rational function field*, Acta Arith. **161** (2013), no. 4, 371–385, DOI 10.4064/aa161-4-4. MR3150889 ↑5, 31

[AH16] Yves Aubry and Safia Haloui, *On the number of rational points on Prym varieties over finite fields*, Glasg. Math. J. **58** (2016), no. 1, 55–68, DOI 10.1017/S0017089515000063. MR3426428 ↑59

[BH12] Salman Baig and Chris Hall, *Experimental data for Goldfeld's conjecture over function fields*, Exp. Math. **21** (2012), no. 4, 362–374, DOI 10.1080/10586458.2012.671638. MR3004252 ↑

[BP18] S. Baluyot and K. Pratt, *Dirichlet L-functions of quadratic characters of prime conductor at the central point* (2018). ArXiv pre-print. ↑31

[BMSW07] Baur Bektemirov, Barry Mazur, William Stein, and Mark Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 2, 233–254, DOI 10.1090/S0273-0979-07-01138-X. MR2291676 ↑22

[BE16] Juliette Bruce and Daniel Erman, *A probabilistic approach to systems of parameters and Noether normalization* (2016). ArXiv pre-print: https://arxiv.org/abs/1604.01704. ↑46, 61

[BL18] Juliette Bruce and Wanlin Li, *Effective Bounds on the Dimensions of Jacobians Covering Abelian Varieties* (2018). ArXiv pre-print: https://arxiv.org/abs/1804.11015. ↑5, 44

[BK12] Alina Bucur and Kiran S. Kedlaya, *The probability that a complete intersection is smooth*, J. Théor. Nombres Bordeaux **24** (2012), no. 3, 541–556 (English, with English and French summaries). ↑46, 50, 51

[BF] H. M. Bui and Alexandra Florea, *Zeros of quadratic Dirichlet L-functions in the hyperelliptic ensemble*, preprint, available on arXiv at http://arxiv.org/abs/1605.07092. ↑1, 8, 24, 30

[Cha97] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180, DOI 10.1215/S0012-7094-97-08707-X. MR1440067 ↑3, 29

[Cho65] S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Norske Vid. Selsk. Forh. (Trondheim) **38** (1965), 62–64. MR0186643 ↑1, 7

[CGG98] J. B. Conrey, A. Ghosh, and S. M. Gonek, *Simple zeros of the Riemann zeta-function*, Proc. London Math. Soc. (3) **76** (1998), no. 3, 497–522, DOI 10.1112/S0024611598000306. MR1616809 ↑30

[CKRS02] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–315. MR1956231 ↑22

[DFL] C. David, A. Florea, and M. Lalin, *The mean values of cubic L-functions over function fields*, arXiv preprint, https://arxiv.org/abs/1901.00817. ↑32

[Dok13] Tim Dokchitser, *Notes on the parity conjecture*, Elliptic curves, Hilbert modular forms and Galois deformations, Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013, pp. 201–249, DOI 10.1007/978-3-0348-0618-3_5. MR3184338 ↑

[Eis05] David Eisenbud, *The geometry of syzygies*, Graduate Texts in Mathematics, vol. 229, Springer-Verlag, New York, 2005. A second course in commutative algebra and algebraic geometry. MR2103875 ↑62

[Eis] K. Eisenträger, *The Theorem of Honda and Tate*, In "Notes on complex multiplication", available at www.math.stanford.edu/conrad/. ↑10, 11

[EHR14] Noam D. Elkies, Everett W. Howe, and Christophe Ritzenthaler, *Genus bounds for curves with fixed Frobenius eigenvalues*, Proc. Amer. Math. Soc. **142** (2014), no. 1, 71–84. MR3119182 ↑63, 64

[ELS] Jordan S. Ellenberg, Wanlin Li, and Mark Shusterman, *Nonvanishing of hyperelliptic zeta functions over finite fields*, preprint, available on arXiv at https://arxiv.org/abs/1901.08202. ↑3, 4, 29

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), no. 3, 729–786, DOI 10.4007/annals.2016.183.3.1. MR3488737 ↑4, 32, 33, 34, 35, 37, 38

[Ful98] William Fulton, *Intersection theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 2, Springer-Verlag, Berlin, 1998. ↑58, 59, 61

[Gab01] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. **11** (2001), no. 6, 1192–1200. MR1878318 ↑45

[Gia06] Daniel Giaimo, *On the Castelnuovo-Mumford regularity of connected curves*, Trans. Amer. Math. Soc. **358** (2006), no. 1, 267–284. MR2171233 ↑47, 62

[Gol79] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118. MR564926 ↑23

[GM91] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23, DOI 10.2307/2939253. MR1080648 ↑22

[Gro12] Benedict H. Gross, *Hanoi lectures on the arithmetic of hyperelliptic curves*, Acta Math. Vietnam. **37** (2012), no. 4, 579–588. MR3058664 ↑41

[GLP83] L. Gruson, R. Lazarsfeld, and C. Peskine, *On a theorem of Castelnuovo, and the equations defining space curves*, Invent. Math. **72** (1983), no. 3, 491–506, DOI 10.1007/BF01398398. MR704401 ↑47

[Har81] Joe Harris, *A bound on the geometric genus of projective varieties*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **8** (1981), no. 1, 35–68. MR616900 ↑59

[Har77] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977. With a view toward algebraic geometry. ↑49, 57, 61, 62

[Hon68] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95, DOI 10.2969/jmsj/02010083. MR0229642 ↑10

[HNR09] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 1, 239–289 (English, with English and French summaries). MR2514865 ↑20, 24

[Kat12] Nicholas M. Katz, *Report on the irreducibility of L-functions*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 321–353. MR2867923 ↑

[Kow06] E. Kowalski, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math. **601** (2006), 29–69, DOI 10.1515/CRELLE.2006.094. MR2289204 ↑3, 29

[Li18] Wanlin Li, *Vanishing of hyperelliptic L-functions at the central point*, J. Number Theory **191** (2018), 85–103. MR3825462 ↑1, 2, 3, 7, 40

[Mil08] James S. Milne, *Abelian Varieties (v2.00)*, 2008. Available at www.jmilne.org/math/. ↑35, 44, 47, 48, 49

[Mum08] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin; Corrected reprint of the second (1974) edition. MR2514037 ↑11

[PPVMW] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, preprint, available on arXiv at https://arxiv.org/abs/1602.01431. ↑22

[Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127. ↑45

[Poo03] ———, *Squarefree values of multivariable polynomials*, Duke Math. J. **118** (2003), no. 2, 353–373, DOI 10.1215/S0012-7094-03-11826-8. MR1980998 ↑15, 16

[Poo17] ———, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR3729254 ↑36

[Pri] Rachel Pries, *Current results on Newton polygons of curves*. to appear as Chapter 6, Questions in Arithmetic Algebraic Geometry, Advanced Lectures in Mathematics Book Series. ↑65

[RW06] Matthieu Romagny and Stefan Wewers, *Hurwitz spaces*, Groupes de Galois arithmétiques et différentiels, Sémin. Congr., vol. 13, Soc. Math. France, Paris, 2006, pp. 313–341 (English, with English and French summaries). MR2316356 ↑34

[RS01] Karl Rubin and Alice Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experiment. Math. **10** (2001), no. 4, 559–569. MR1881757 ↑22

[Sch80] J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. Assoc. Comput. Mach. **27** (1980), no. 4, 701–717, DOI 10.1145/322217.322225. MR594695 ↑

[Sou00] K. Soundararajan, *Nonvanishing of quadratic Dirichlet L-functions at $s = \frac{1}{2}$*, Ann. of Math. (2) **152** (2000), no. 2, 447–488, DOI 10.2307/2661390. MR1804529 ↑1, 7, 30

[TS18] The Stacks project authors, *The Stacks project*, 2018. ↑49, 57

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144, DOI 10.1007/BF01404549. MR0206004 ↑

[Ulm11] Douglas Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280. MR2882692 ↑18, 19

[Zip79] Richard Zippel, *Probabilistic algorithms for sparse polynomials*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin-New York, 1979, pp. 216–226. MR575692 ↑