Algebra & Number Theory

Volume 14
2020
No. 7

Nonvanishing of hyperelliptic zeta functions over finite fields

Jordan S. Ellenberg, Wanlin Li and Mark Shusterman

msp

ALGEBRA AND NUMBER THEORY 14:7 (2020)
https://doi.org/10.2140/ant.2020.14.1895

Nonvanishing of hyperelliptic zeta functions over finite fields

Jordan S. Ellenberg, Wanlin Li and Mark Shusterman

Fixing $t \in \mathbb{R}$ and a finite field $\mathbb{F}_q$ of odd characteristic, we give an explicit upper bound on the proportion of genus g hyperelliptic curves over $\mathbb{F}_q$ whose zeta function vanishes at $\frac{1}{2}+it$. Our upper bound is independent of g and tends to 0 as q grows.

An errata was submitted on 27 Aug 2021 and posted online on 1 Sep 2021.

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 of Chavdarov [1997] (and its improvement by Kowalski [2006]) 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

$$h_{q,s} := \sup_g \frac{|\{C \in \mathcal{H}_g(\mathbb{F}_q) : Z_C(s) = 0\}|}{|\mathcal{H}_g(\mathbb{F}_q)|} \tag{1.1}$$

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.

Theorem 1.2 (Theorem 3.2). *Fix a prime p, a real number t, and set $s = \frac{1}{2} + it$. Then as $k \to \infty$ we have*

$$h_{p^k,s} \ll p^{-k/276}. \tag{1.3}$$

In particular, $h_{p^k,s}$ tends to 0 as k tends to ∞.

This complements (but does not quite match) lower bounds on $h_{q,s}$ obtained by Li [2018].

Restricting q to powers of a fixed prime p is not always necessary. In case $s \neq \frac{1}{2}$, one can show (see [Ray 2018]) using transcendental number theory (six exponentials theorem [Lang 1966, Chapter 2,

MSC2010: 11M38.
Keywords: nonvanishing, L-functions, function fields, Dirichlet characters.

Section 1]) that there are only finitely many p for which p^{-s} is algebraic, so $h_{q,s}=0$ for any q not divisible by these p (as $Z_C(s)$ is a rational function in q^{-s}). Hence, it suffices to work with one characteristic at a time, as we do in the theorem above. For $s=\frac{1}{2}$, since the upper bound in Corollary 2.6 holds for any ℓ when q is a perfect square, we can conclude $\lim_{q\to\infty} h_{q,s}=0$ ranging over q which is an even power of a prime.

Additional motivation for Theorem 1.2 comes from the ability to write $Z_C(s)$ as a rational function in q^{-s}, with the numerator being a quadratic Dirichlet L-function. Interpreted in this language of Dirichlet characters, Theorem 1.2 improves (for all sufficiently large q) upon [Bui and Florea 2018, Corollary 2.1] $\left(\text{they give a lower bound of more than } 94.27\% \text{ nonvanishing at } s=\frac{1}{2}\right)$. Regarding the analogous vanishing problem for quadratic Dirichlet L-functions over $\mathbb{Z}$, we refer to the work of Soundararajan [2000].[1]

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 1.4 (Corollary 3.3). *Let A be a constant abelian variety defined over $\mathbb{F}_q(x)$. For each $f\in\mathbb{F}_{q^m}[x]$, 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 [Bui and Florea 2018, Corollary 2.2] and the analogous results over $\mathbb{Z}$ of Conrey, Ghosh and Gonek [Conrey et al. 1998], we bound the multiplicity of the zeros of Z_C, and obtain further information on nonvanishing at $s=\frac{1}{2}$.

Theorem 1.5. *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 *lengths, 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 and therefore gives an explicit set of size on order $X/\log X$ of Dirichlet characters of conductor at most X which have L-functions nonvanishing at the critical point. See the statement below.

[1] Results in [Bui and Florea 2018] and [Soundararajan 2000] were stated at point $s=\frac{1}{2}$ but the methods can be extended to prove the statement for any point on the critical line.

Corollary 1.6. *Let χ be a quadratic character over $\mathbb{F}_q(x)$ with conductor $f \in \mathbb{F}_q[x]$. If f is irreducible and $4 \nmid \deg f$, then $L\left(\frac{1}{2}, \chi\right) \neq 0$.*

In particular, the number of quadratic characters with irreducible conductor of size at most X whose L-function does not vanish at $s = \frac{1}{2}$ is $\gg X/\log X$ as $X \to \infty$. This result improves on the work of Andrade and Keating [2013, Corollary 2.6] and of Andrade, Bae, and Jung [Andrade et al. 2016, Corollary 2.8], which give a proportion on order $(\log X)^{-2}$, and goes beyond the methods of Andrade and Baluyot [2020]. For the analogous problem over $\mathbb{Z}$, we refer to the recent work of Baluyot and Pratt [2018].

In fact, there is nothing special about hyperelliptic curves in Theorem 1.5. A similar "genus-theory" argument allows us to handle the case of cyclic ℓ-covers of $\mathbb{P}^1$ for an odd prime ℓ.

Theorem 1.7. *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 $S \subset \mathbb{P}^1(\bar{\mathbb{F}}_q)$. Let π be the permutation induced by Frobenius on S, and suppose that π is the composition of disjoint cycles of orders $k_1, k_2, \ldots, k_r$, 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 1.5 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 nonvanishing at $s = \frac{1}{2}$, for some power $a \in (0, 1]$. See Corollary 1.8 for example. This lower bound improves, for $\ell = 3$, upon Corollary 1.3 of recent work by David, Florea and Lalin [2019] which gives a lower bound of the form $X^{1-\epsilon}$ (for any $\epsilon > 0$).

Corollary 1.8. *Let ℓ be an odd prime different from the characteristic of a fixed finite field $\mathbb{F}_q$. The number of ℓ-cyclic Dirichlet characters over $\mathbb{F}_q(x)$ with conductor at most X and whose L-function does not vanish at $s = \frac{1}{2}$ is $\gg X/(\log X)^{1/2}$ as $X \to \infty$.*

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 $P(T) \in \mathbb{Z}[T]$ evaluated at $T = q^{-s}$. 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 1.2, 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 point count on a moduli space over a finite field, which is a modest generalization and explication of the arguments in [Ellenberg et al. 2016] and [Lipnowski and Tsimerman 2019] respectively. For Theorem 1.5, 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 $s = \frac{1}{2}$. For the similar Theorem 1.7, the ℓ is again the order of the Dirichlet character in question.

2. Main theorem and proof

2A. ***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 geometric 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 $J_f[\ell](\bar{\mathbb{F}}_q)$ 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 f over $\mathbb{F}_q$ of degree n such that $m_a(f)$ is greater than 0.

Let α be a q-Weil number of weight 1 with minimal polynomial $g_\alpha(x) \in \mathbb{Z}[x]$. Namely, it is an algebraic integer whose absolute values under all complex embeddings equal $\sqrt{q}$. 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 $|Q_{n,q}^{\alpha}| \le |Q_{n,q}^{a,\ell}|$.

2B. ***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 $\mathrm{Jac}(C)[\ell](\bar{\mathbb{F}}_q)$ 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 2.1. *Let $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. With notation as in Section 2A, there exist constants C_ℓ, N_ℓ, Q_ℓ only depending on ℓ such that*

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

for all $n \ge N_\ell$ and $q \ge Q_\ell$.

Remark 2.2. While this paper was in proof, we learned that Proposition 2.1 follows from the proof of Theorem 1.1 of [Lipnowski and Tsimerman 2019], which is in fact more general, and the arguments used are essentially the same as those here. We have left the proof of Proposition 2.1 in the present paper

because the form in which we present the proof here is conducive to proving the explicit bounds for the stable range obtained in Proposition 2.7 below. It would be interesting to address the questions of explicit bounds for the stable range in the more general situations considered by [loc. cit.], where the group-theoretic part of the proof of Proposition 2.7 would presumably be more complicated.

When $a = 1$ and n is odd, Proposition 2.1 is essentially Theorem 8.8 of [Ellenberg et al. 2016], and indeed the proof here is a modification of the proof of that theorem.

The reader may note that [Ellenberg et al. 2016, Theorem 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 [loc. cit., Theorem 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 [loc. cit., Theorem 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 [loc. cit., Theorem 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 [Ellenberg et al. 2016, Section 7].

Let k be a field, let G be a finite group with trivial center, denote by e the identity element of G, 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 $\mathrm{Aut}(f)$.

Here 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".

Then, as in [Ellenberg et al. 2016, Section 7] (more or less immediate from a theorem of Romagny and Wewers [2006]), 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 ∞.)[2] In fact [Romagny and Wewers 2006, Theorem 2.1], for a scheme S, the set $\mathsf{Hn}^c_{G,n}(S)$ corresponds to isomorphism classes of tame G-covers over S, suitably defined; we will not need to spell out that definition here. Once the n branch points are chosen on $\mathbb{A}^1$ there are finitely many choices for f and ϕ. Thus the dimension of $\mathsf{Hn}^c_{G,n}$ equals to n.

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 [Milne 2008].

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 étale 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 as C is a smooth proper hyperelliptic curve. 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 [Ellenberg et al. 2016]). 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. In both cases, $\dim X_n = n$. 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 [Ellenberg et al. 2016, 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

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

which sends Frob_q to a [Poonen 2017, Section 4.5].

Lemma 2.3. *With notation as in Section 2A,*

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

[2] The somewhat artificial special treatment of ∞ in this definition, as in [Ellenberg et al. 2016], 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.

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 the branch locus of h is an $\mathbb{F}_q$-rational divisor. Let $f(x) \in \mathbb{F}_q[x]$ be the unique monic squarefree polynomial which vanishes precisely at the branch locus of h. Then C is isomorphic (over $\overline{\mathbb{F}}_q$) to the smooth completion of the hyperelliptic curve defined by $y^2 = f(x)$.

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, ϕ) such that $(g, \phi, h) \in X_n^a(\overline{\mathbb{F}}_q) = X_n(\overline{\mathbb{F}}_q)$ 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 $\left(\frac{1}{2}\right)(m_a(f) + m_{-a}(f))$.

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 $\left(\frac{1}{2}\right)(m_a(f) + m_{-a}(f))$ is the same for all $q - 1$ nonzero multiples of F. We conclude that

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

Moreover, taking ϵ to be a nonresidue 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 [Ellenberg et al. 2016, Theorem 8.8].

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

$$|q^{-n}|X_n^a(\mathbb{F}_q)| - 1| \le C_\ell q^{-1/2} \tag{2.4}$$

for some C_ℓ depending only on ℓ and for all $n > N_\ell, q > Q_\ell$.

Via the Grothendieck–Lefschetz trace formula, we have

$$|X_n^a(\mathbb{F}_q)| = \sum_i (-1)^i \,\mathrm{Tr}(\mathrm{Frob}_q \mid H^i_{c,\text{ét}}((X_n^a)_{\overline{\mathbb{F}}_q}; \mathbb{Q}_\lambda). \tag{2.5}$$

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; in particular, the choice of a affects the action of Frobenius on the étale cohomology, but not the étale Betti numbers, bounds on which are the main engine of the argument.

We begin by computing the main term:

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

This follows immediately from the fact that $(X_n^a)_{\bar{\mathbb{F}}_q} \cong (X_n)_{\bar{\mathbb{F}}_q}$ is irreducible. When n is odd, this is shown in the proof of [Ellenberg et al. 2016, Theorem 8.8] as a consequence of a big monodromy theorem of J.K. Yu. (This is actually the only place where we need n to be large, and indeed $n = 3$ would be enough.) 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 [loc. cit., Section 2.2], 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 $\mathrm{Hn}^c_{G,n-1}$, which we know to be irreducible since $n-1$ is odd. This implies that X_n is irreducible.

We now turn to the error term. The moduli space X_n is a closed and open subscheme of $\mathrm{Hn}^c_{G,n}$, so its Betti numbers are bounded by those of $\mathrm{Hn}^c_{G,n}$; by [loc. cit., (7.8.1)] we have

$$\dim H^{2n-i}_{c,\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \le K_\ell (B_\ell)^i$$

where K_ℓ, B_ℓ are constants depending only on ℓ.

Using the Deligne bound [1980], the eigenvalue of Frobenius on $H^i_{c,\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda)$ is bounded in absolute value by $q^{i/2}$; so the absolute value of the contribution of all $i < 2n$ to (2.5) is bounded above by the sum of a geometric series which converges for all $q > B_\ell^2$. In particular, as in [Ellenberg et al. 2016, Section 1.8], this contribution is at most

$$K_\ell B_\ell q^{-1/2}(1 - B_\ell q^{-1/2})^{-1} q^n.$$

So if we take $Q_\ell = 4B_\ell^2$ and $q > Q_\ell$, we may take $C_\ell = 2K_\ell B_\ell$ and conclude

$$|X_n^a(\mathbb{F}_q) - q^n| = \left| \sum_{i=0}^{2n-1} (-1)^i \,\mathrm{Tr}(\mathrm{Frob}_q \mid H^i_{c,\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \right| < C_\ell q^{n-1/2}$$

which proves (2.4) and thus the desired result. □

Proposition 2.1 allows us to bound the proportion of hyperelliptic curves whose étale cohomology has a Frobenius eigenvalue congruent to a mod ℓ. Recall from Section 2A that $Q^{a,\ell}_{n,q}$ is the set of squarefree polynomials over $\mathbb{F}_q$ of degree n such that $m_a(f)$ is greater than 0.

Corollary 2.6. *There are constants C'_ℓ, Q_ℓ, N_ℓ such that for any $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ we have*

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

for all $n \ge N_\ell$, $q \ge Q_\ell$.

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,

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

By Proposition 2.1, 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 $C'_\ell = C_\ell/(\ell-1)$. □

So far, we have used the results of [Ellenberg et al. 2016] as they appear in that paper. However, for the present application, it is useful to compute explicit values C_ℓ, Q_ℓ for which Corollary 2.6 holds. We do so by going back to the main body of [loc. cit.] and working out explicit bounds for quantities that are given in [loc. cit., (7.8.1)] only as unspecified constants.

Proposition 2.7. *Corollary 2.6 holds with* $C'_\ell = 2(\ell-1)^{-1}(4\ell)^{138}$ *and* $Q_\ell = 4\cdot(4\ell)^{156}$.

Proof. By the proof of Corollary 2.6, we may take C'_ℓ to be $C_\ell/(\ell-1)$, where C_ℓ is the constant appearing in the statement of Proposition 2.1. Moreover, we may take C_ℓ to be $2K_\ell B_\ell$ and Q_ℓ to be $4B_\ell^2$, where B_ℓ, K_ℓ are the constants appearing in the proof of Proposition 2.1 controlling the exponential growth of the Betti numbers of the relevant Hurwitz space. We now explain how to bound B_ℓ explicitly.

In [Ellenberg et al. 2016, 7.8.1], the bound

$$\dim H^i_{\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \leq K_\ell (B_\ell)^i$$

arises from two facts. First, there is a stability theorem [loc. cit., 6.2], which tells us in this context that

$$\dim H^i_{\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) = \dim H^i_{\text{ét}}((X_{n+D}^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \tag{2.8}$$

for all $n > Ai + B$, where A, B, and D are constants we shall specify. Second, there is an absolute bound [loc. cit., 2.5] which tells us that

$$\dim H^i_{\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \leq (4\ell)^n.$$

These two facts together imply that

$$\dim H^i_{\text{ét}}((X_n^a)_{\bar{\mathbb{F}}_q}; \mathbb{Q}_\lambda) \leq (4\ell)^{Ai+B+D}$$

so we may take $B_\ell = (4\ell)^A$ and $K_\ell = (4\ell)^{B+D}$. It remains to compute A, B, and D.

The key object of computation is the ring R defined in [Ellenberg et al. 2016, Section 3]. This ring is defined for any finite group G and any conjugacy-closed subset of G; we will consider here just the case relevant to us, which is that where G is the dihedral group of order 2ℓ and c is the class of involutions in G. The set of n-tuples of involutions $(\tau_1, \ldots, \tau_n) \in G^n$ carries a natural action of the n-strand braid

group; the ring R is a graded $\mathbb{Q}$-algebra whose degree-n part is spanned by the set of orbits of that action, which set we denote Σ_n. The multiplication in R is given by concatenation of n-tuples.

The key fact about R is that it contains a central element U with the property that $R[U]$ and R/UR both have finite degree (that is, they are supported in only finitely many grades.) In the dihedral case, R and U are particularly easy to describe. For any n, there is map from Σ_n to G sending $(\tau_1, \dots, \tau_n)$ to the product $\tau_1 \cdots \tau_n$, which is called the *boundary monodromy*. Each n-tuple in Σ_n also has a *monodromy group*; namely, the group generated by $\tau_1, \dots, \tau_n$. The possible monodromy groups are just the order-2 subgroups of G and G itself. It is not hard to check that, for all $n \geq 4$, the elements of Σ_n are determined by their boundary monodromy and their monodromy group; to be precise, Σ_n consists of ℓ orbits consisting of the single element $(\tau, \tau, \dots, \tau)$ as τ ranges over the ℓ involutions, and ℓ more orbits, each of which consists of all n-tuples with monodromy group G and boundary monodromy g, as g ranges over the index-2 cyclic subgroup of G (when n is even) or its nontrivial coset (when n is odd.) In particular, $\dim R_n = 2\ell$ for all $n \geq 4$. We may take U to be the degree-2 central operator

$$U = \sum_{\tau \in c} (\tau, \tau)$$

and check that U induces an isomorphism from R_n to R_{n+2} for all $n \geq 4$. In particular, $\deg R[U]$ and $\deg R/UR$ are both at most 4, where by the degree of a graded ring we mean the highest grade represented in its support.

This combinatorial information about the dihedral group is what goes into the computation of constants in [Ellenberg et al. 2016]. The constant D in [loc. cit., 6.1] is just the degree of U, which is 2. The stability result in [loc. cit., 6.1] is derived from a general theorem [loc. cit., 4.2] about R-modules. The R-module M governing the H^i of Hurwitz space, to which we apply [loc. cit., 4.2] is the one called M_i in [loc. cit., 6.1]. So (using the constants appearing in those theorems) stability begins when $n = \max(h_0, h_1) + A_0$, where h_j is the quantity denoted $\deg H_j(\mathcal{K}(M_i)$ in [loc. cit., 6.1]. In turn, as asserted in the first paragraph of the proof of [loc. cit., 6.1], we have

$$\deg H_j(\mathcal{K}(M_i)) \leq A_2 + A_0(3i + j).$$

So we find that (2.8) holds for all $n \leq A_2 + A_0(3i + 1) + A_0 = 3A_0 i + (2A_0 + A_2)$. In other words, we may take $A = 3A_0$ and $B = 2A_0 + A_2$.

Finally, the values of A_0 and A_2 are given in [Ellenberg et al. 2016, 4.5.3]. They are defined in terms of $A(R) = \max(\deg R[U], \deg R/UR)$, which for us is 4. Now $A_0 = 6A(R) + \deg U = 26$ and $A_2 = A(R) + \deg U = 6$. Thus, $A = 78$ and $B = 58$. Since $D = 2$, we conclude that we may take $B_\ell = (4\ell)^{78}$ and $K_\ell = (4\ell)^{60}$. So we have $Q_\ell = 4 \cdot (4\ell)^{156}$ and $C'_\ell = 2(\ell - 1)^{-1}(4\ell)^{138}$, as claimed. □

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 a q-Weil number of weight 1. 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 3.1. *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 zeta function of C, and the connection of the latter to $L(s, \chi_f)$ (see, for instance, [Rudnick 2010, Section 2]).

Theorem 3.2. *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 2A. Then for any $s \neq 0$,*

$$\limsup_{n\to\infty} \frac{|\{f \in Q_{n,q} \mid L(s, \chi_f) = 0\}|}{|Q_{n,q}|} \ll q^{-1/276}$$

where the limit is taken over all powers q of a fixed odd prime number p.

Proof. Fix an odd prime number p, and let q be a power of p. By Lemma 3.1, $L(s, \chi_f) = 0$ 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 $Q_{n,q}^{q^s}$.

By Chebotarev's density theorem, we can (for large enough q) find a prime

$$\ell = \frac{1}{4}\left(\frac{q}{4}\right)^{1/276}(1 + o(1))$$

mod which g_{p^s}, the minimal polynomial of p^s, splits completely. Let $a \in \mathbb{Z}/l\mathbb{Z}$ such that $g_{p^s}(a) = 0 \bmod \ell$. If $q = p^t$, then any f with $L(\chi_f, s) = 0$ has $m_{a^t}(f) > 0$. So

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

and now we can apply Corollary 2.6 to conclude using the second equation of Section 2A that, for all sufficiently large t, 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 required bound follows from Proposition 2.7. □

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 that as the constant field grows (so the characteristic is not changing), the probability for a quadratic twist of a constant abelian variety to have positive rank goes to 0. 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 3.3. *Let A be an abelian variety defined over a finite field $\mathbb{F}_q$ of odd characteristic. For each $f \in Q_{n,q^m}$, 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 rank $A_f > 0$ is equivalent to $L(s, \chi_f) = 0$. (See [Li 2018, Proposition 4.6] for a similar statement with the same proof.) Thus, the statement is a direct application of Theorem 3.2. □

We now prove Theorem 1.5, which makes use of the mod 2 Galois representations on $J(C)$ rather than the representations modulo odd primes.

Proof of Theorem 1.5. Let $x_1, \dots, x_{2g+2}$ 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 $x_1 + \cdots + x_{2g+2} - (2g+2)x_1$ is a principal divisor and thus $x_1 + \cdots + x_{2g+2}$ is 0 in $J(C)[2]$. See [Gross 2012, Section 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 $(a_1, \dots, a_{2g+2}) : \sum a_i = 0$ by the 1-dimensional subspace spanned by $(1, \dots, 1)$.

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 $x_1, \dots, x_{2g+2}$. 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 1.5 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} for some odd $1 \le k \le 2g+1$; 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 $\frac{1}{2}$, 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.) □

Proof of Corollary 1.6. By assumption, f is an irreducible polynomial over $\mathbb{F}_q$. So when $\deg f = n$ is even, Frobenius acts on the set of Weierstrass points of $C_f : y^2 = f(x)$ as a n-cycle. If $\deg f = n$ is odd, then Frobenius acts on the set of Weierstrass points of C_f as a disjoint union of a $(n-1)$-cycle and a

1-cycle. In either case, when $4 \nmid \deg f$ we can apply Theorem 1.5 to conclude that Z_{C_f} does not vanish at $\frac{1}{2}$ and so behaves $L(s, \chi_f)$.

For any $X = q^{2g+2}$, the set of irreducible polynomials of odd degree at most $2g+1$ gives quadratic characters with bounded conductor whose L-function does not vanish at the central point $s = \frac{1}{2}$. By the prime number theorem for function fields, the number of irreducible polynomials in $\mathbb{F}_q[x]$ of degree at most n is $\gg q^n/n$. This gives the lower bound in statement. □

The proof of Theorem 1.7 is very similar to that of Theorem 1.5, but we treat it separately in order to make the hyperelliptic case above more readable.

Proof of Theorem 1.7. 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 $m = k_1 + \cdots + k_r$. 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 $\zeta_\ell - 1$, where ζ_ℓ 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 $a_i = \operatorname{ord}_{x_i} f$. 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 π-trivial one-dimensional representation onto 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.[3]

If the zeta function Z_C had a zero at $\frac{1}{2}$, 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 $s = \frac{1}{2}$ is not a root of Z_C.

[3] 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 $k_1, \dots, k_r$ 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. □

Proof of Corollary 1.8. Consider curves over $\mathbb{F}_q$ with defining equations of the form $y^\ell = f(x)$ where $f \in \mathbb{F}_q[x]$ is monic, squarefree of degree n and n is a multiple of ℓ. This gives $\ell - 1$ cyclic Dirichlet characters of conductor f and order ℓ. Such a curve C_f admits a $\mathbb{Z}/\ell\mathbb{Z}$ cover of $\mathbb{P}^1_{\mathbb{F}_q}$ branched at the vanishing loci of f.

Let d be the order of the image of q in $(\mathbb{Z}/\ell\mathbb{Z})^*$ and let $k_1, k_2, \dots, k_r$ be the degrees of the factors of f. By Theorem 1.7, if $d \nmid k_i$ for any $i \in \{1, 2, \dots, r\}$, then the point $s = \frac{1}{2}$ is not a zero of Z_C thus not a zero for the Dirichlet L-functions corresponding to the curve. Thus, a count on this family of polynomials would give a lower bound on the set of desired Dirichlet characters.

By [Bolker and Gleason 1980, Theorem 2], the number of elements in S_n with no cycle length divisible by d is

$$T_d(n) = \prod_{j=1}^{n} (j - \theta_d(j))$$

where $\theta_d(j) = 0$ if $d \nmid j$ and 1 if $d \mid j$. So the number of monic, squarefree polynomials of degree n over $\mathbb{F}_q$ where none of its factor has degree divisible by d is $\gg (T_d(n)/n!)(q^n - q^{n-1})$. Since $T_d(n) \geq T_2(n)$ for any $d \geq 2$, we have

$$\frac{T_d(n)}{n!} \geq \frac{((n-1)!!)^2}{n!} \geq \frac{C}{n^{1/2}}$$

where !! stands for double factorial and C is a nonzero constant. As $X = q^n$, we get the desired result. □

Acknowledgments

The authors are grateful to Chantal David, Zeev Rudnick, Alexandra Florea, and Emmanuel Kowalski for helpful comments and suggestions. Ellenberg was partially supported by NSF grant DMS-1700885 and by a fellowship from the Simons Foundation. We thank the referees for the valuable feedback and comments.

References

[Andrade and Baluyot 2020] J. Andrade and S. Baluyot, "Small zeros of Dirichlet L-functions of quadratic characters of prime modulus", *Res. Number Theory* **6**:2 (2020), 1–20. MR

[Andrade and Keating 2013] J. C. Andrade and J. P. Keating, "Mean value theorems for L-functions over prime polynomials for the rational function field", *Acta Arith.* **161**:4 (2013), 371–385. MR Zbl

[Andrade et al. 2016] J. C. Andrade, S. Bae, and H. Jung, "Average values of L-series for real characters in function fields", *Res. Math. Sci.* **3** (2016), art. id. 38. MR Zbl

[Baluyot and Pratt 2018] S. Baluyot and K. Pratt, "Dirichlet L-functions of quadratic characters of prime conductor at the central point", preprint, 2018. arXiv

[Bolker and Gleason 1980] E. D. Bolker and A. M. Gleason, "Counting permutations", *J. Combin. Theory Ser. A* **29**:2 (1980), 236–242. MR Zbl

[Bui and Florea 2018] H. M. Bui and A. Florea, "Zeros of quadratic Dirichlet L-functions in the hyperelliptic ensemble", *Trans. Amer. Math. Soc.* **370**:11 (2018), 8013–8045. MR Zbl

[Chavdarov 1997] N. Chavdarov, "The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy", *Duke Math. J.* **87**:1 (1997), 151–180. MR Zbl

[Conrey et al. 1998] J. B. Conrey, A. Ghosh, and S. M. Gonek, "Simple zeros of the Riemann zeta-function", *Proc. Lond. Math. Soc.* (3) **76**:3 (1998), 497–522. MR Zbl

[David et al. 2019] C. David, A. Florea, and M. Lalin, "The mean values of cubic L-functions over function fields", preprint, 2019. arXiv

[Deligne 1980] P. Deligne, "La conjecture de Weil, II", *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252. MR Zbl

[Ellenberg et al. 2016] J. S. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields", *Ann. of Math.* (2) **183**:3 (2016), 729–786. MR Zbl

[Gross 2012] B. H. Gross, "Hanoi lectures on the arithmetic of hyperelliptic curves", *Acta Math. Vietnam.* **37**:4 (2012), 579–588. MR Zbl

[Kowalski 2006] E. Kowalski, "The large sieve, monodromy and zeta functions of curves", *J. Reine Angew. Math.* **601** (2006), 29–69. MR Zbl

[Lang 1966] S. Lang, *Introduction to transcendental numbers*, Addison-Wesley, Reading, MA, 1966. MR Zbl

[Li 2018] W. Li, "Vanishing of hyperelliptic L-functions at the central point", *J. Number Theory* **191** (2018), 85–103. MR Zbl

[Lipnowski and Tsimerman 2019] M. Lipnowski and J. Tsimerman, "Cohen–Lenstra heuristics for étale group schemes and symplectic pairings", *Compos. Math.* **155**:4 (2019), 758–775. MR Zbl

[Milne 2008] J. S. Milne, "Abelian varieties", version 2.0, course notes, 2008, available at https://www.jmilne.org/math/CourseNotes/av.html.

[Poonen 2017] B. Poonen, *Rational points on varieties*, Graduate Studies in Math. **186**, Amer. Math. Soc., Providence, RI, 2017. MR Zbl

[Ray 2018] A. Ray, Reply to "Algebraic exponential values", MathOverflow, 2018, available at https://mathoverflow.net/q/314221.

[Romagny and Wewers 2006] M. Romagny and S. Wewers, "Hurwitz spaces", pp. 313–341 in *Groupes de Galois arithmétiques et différentiels*, edited by D. Bertrand and P. Dèbes, Sémin. Congr. **13**, Soc. Math. France, Paris, 2006. MR Zbl

[Rudnick 2010] Z. Rudnick, "Traces of high powers of the Frobenius class in the hyperelliptic ensemble", *Acta Arith.* **143**:1 (2010), 81–99. MR Zbl

[Soundararajan 2000] K. Soundararajan, "Nonvanishing of quadratic Dirichlet L-functions at $s = \frac{1}{2}$", *Ann. of Math.* (2) **152**:2 (2000), 447–488. MR Zbl

Communicated by Andrew Granville
Received 2019-02-22 Revised 2019-12-18 Accepted 2020-02-06

ellenber@math.wisc.edu *Department of Mathematics, University of Wisconsin, Madison, WI, United States*

wanleen@gmail.com *Department of Mathematics, MIT, Cambridge, MA, United States*

mshusterman@wisc.edu *Department of Mathematics, University of Wisconsin, Madison, WI, United States*

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 7 2020