ONE-LEVEL DENSITY OF THE FAMILY OF TWISTS OF AN ELLIPTIC CURVE
OVER FUNCTION FIELDS

ANTOINE COMEAU-LAPOINTE

ABSTRACT. We fix an elliptic curve $E/F_q(t)$ and consider the family $\{E \otimes \chi_D\}$ of $E$ twisted by quadratic Dirichlet characters. The one-level density of their $L$-functions is shown to follow orthogonal symmetry for test functions with Fourier transform supported inside $(-1, 1)$. As an application, we obtain an upper bound of $3/2$ on the average analytic rank. By splitting the family according to the sign of the functional equation, we obtain that at least $12.5\%$ of the family have rank zero, and at least $37.5\%$ have rank one. The Katz and Sarnak philosophy predicts that those percentages should both be $50\%$ and that the average analytic rank should be $1/2$. We finish by computing the one-level density of $E$ twisted by Dirichlet characters of order $\ell \neq 2$ coprime to $q$. We obtain a restriction of $(-1/2, 1/2)$ on the support with a unitary symmetry.

1. Introduction

We study the one-level density of the family of twists of an elliptic curve defined over $F_q(t)$. Over $\mathbb{Q}$, the one-level density of this family was studied by Heath-Brown [HB03] for quadratic twists. The first results obtained in the present paper are analogous to what he obtained. Under a hypothesis slightly stronger than the Riemann Hypothesis for elliptic curves, Fiorilli [Fio14] showed that the average analytic rank of this family is exactly $1/2$. For cubic Dirichlet $L$-functions over $\mathbb{Q}$, Cho and Park [CP18] computed the one-level density and obtained the restriction of $(-1, 1)$ on the support of the test functions along with a unitary symmetry. They also computed [CP19b] the $n$-level densities for the family of cubic twists of any given cuspidal representation of $GL_m(A_\mathbb{Q})$, and they showed that the symmetry is unitary. Over cubic Galois number fields, Meisner [Mei17] computed the one-level density of the associated $L$-functions and showed that the symmetry is unitary with a restriction of $(-1/2, 1/2)$ on the support. For the one-level density of Dirichlet $L$-functions of order $r$ over $\mathbb{Q}$, Cho and Park [CP19a] showed that the symmetry is unitary, and obtained the restriction of $(1,1)$ on the support. They also obtained the restriction of $(-1/m, 1/m)$ on the support for the family of twists of order $r$ of any given cuspidal representation of $GL_m(A_\mathbb{Q})$. All of the above results are under the Generalized Riemann Hypothesis. Over function fields, results are unconditional since the Weil’s conjectures has been proved.

Over $F_q(t)$, the one-level density of the family of quadratic Dirichlet $L$-functions was studied by Rudnick [Rud08] where he obtained a restriction of $(-2, 2)$ on the support, with a symplectic symmetry. Under further restrictions on the support, Bui and Florea [BF16] were able to compute lower order terms for the one-level density of this family. The first four moments of this family were obtained by Florea [Flo15], [Flo16]. For cubic Dirichlet $L$-functions over $F_q(t)$, David, Florea, and Lalín [DFL19] computed the mean values of the $L$-functions. They also proved that a positive proportion of these $L$-functions do not vanish at the central point [DFL20].

Throughout this paper, a prime $p \neq 2, 3$ is fixed and we fix $q = p^n$ for any integer $n \geq 1$. We also fix an elliptic curve $E : y^2 = x^3 + Ax + B$ over $F_q[t]$ under its minimal Weierstrass model such that it has at least one prime of multiplicative reduction, has additive reduction at infinity, and such that its $j$-invariant isn’t zero (see [Sil09] for background). We write $A$ instead of $A(t)$ for elements of $F_q[t]$. The conductor of $E$ is denoted by $N_E$.

Let $\mathcal{M}_N \subset F_q[t]$ be the set of monic polynomials of degree $N$ and let $\mathcal{H}_{N,C} \subset \mathcal{M}_N$ be the set of square-free polynomials of degree $N$ congruent to $C$ modulo $N_E$ where $C$ is coprime to $N_E$. We denote by $\mathcal{H}_N^*$ the
set of square-free polynomials of degree $N$ that are coprime to $N_E$. In particular, we have the partition $\mathcal{H}_N^* = \bigcup_{(C,N_E)=1} \mathcal{H}_{N,C}$. The main family of this paper is the set of quadratic twists of $E$. Each twist of $E$ is denoted by $E \otimes \chi_D$ where $\chi_D$ is the unique quadratic Dirichlet character of conductor $D$, where $D \in \mathcal{H}_N^*$. To each twist is associated a unitary matrix (up to conjugacy class) called the Frobenius of $E \otimes \chi_D$ denoted by

$$\Theta_D = \begin{pmatrix} e^{i\theta_{D,1}} & \cdots & e^{i\theta_{D,M}} \\ \vdots & \ddots & \vdots \\ e^{i\theta_{D,M}} & \cdots & e^{i\theta_{D,1}} \end{pmatrix} \tag{1.1}$$

where the $e^{i\theta_{D,j}}$ are called the Frobenius eigenvalues of $E \otimes \chi_D$ and $0 \leq \theta_{D,j} < 2\pi$. The average of traces of powers of $\Theta_D$ over $\mathcal{H}_{N,C}$ is defined by

$$\langle \text{tr} \Theta^n \rangle_{N,C} = \frac{1}{\lvert \mathcal{H}_{N,C} \rvert} \sum_{D \in \mathcal{H}_{N,C}} \sum_{j=1}^M e^{in\theta_{D,j}}.$$

We prove the following.

**Theorem 1.1.** For $\epsilon > 0$, $n > 0$, and $N > 4 \deg(N_E)$

$$\langle \text{tr} \Theta^n \rangle_{N,C} = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases} + O_{E,q} \left( (n + N)^{2\deg(N_E)+3} \left( \frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}} \right) + n^2 q^{-n/4} \right). \tag{1.2}$$

This is in agreement with the mean values over $O(M)$ given in [DS94]

$$\int_{O(M)} \text{tr} \Theta^n d\Theta = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases}$$

with respect to the Haar measure where $O(M)$ is the orthogonal group of dimension $M$.

As an application we compute the one-level density of the family. The Schwartz space $S(\mathbb{R})$ is a space of rapidly decreasing functions on $\mathbb{R}$ and is defined by

$$S(\mathbb{R}) := \{ f \in C^\infty(\mathbb{R}) \mid \forall \alpha, \beta \in \mathbb{N}, \| f \|_{\alpha, \beta} < \infty \} \text{ where } \| f \|_{\alpha, \beta} := \sup_{x \in \mathbb{R}} |x^\alpha f^{(\beta)}(x)|.$$

For an even function $\phi \in S(\mathbb{R})$ and $M \geq 0$, we define

$$F(\theta) := \sum_{k \in \mathbb{Z}} \phi \left( M \left( \frac{\theta}{2\pi} - k \right) \right)$$

which has period $2\pi$ and is localized on an interval of size $\approx 1/M$ around $0$ in $\mathbb{R}/2\pi \mathbb{Z}$. Let $\Theta$ be an $M \times M$ matrix with eigenvalues $e^{i\theta_j}$, where $0 \leq \theta_j < 2\pi$. We define

$$Z_\phi(\Theta) := \sum_{j=1}^M F(\theta_j).$$

The one-level density of the family $\mathcal{H}_{N,C}$ is the average

$$\langle Z_\phi \rangle_{N,C} := \frac{1}{\lvert \mathcal{H}_{N,C} \rvert} \sum_{D \in \mathcal{H}_{N,C}} Z_\phi(\Theta_D)$$

where $\Theta_D$ is given by (1.1). The one-level density picks up the $\theta_j$ near $0$ and it reveals the symmetry type of our family. We prove the following result on the one-level density.
Corollary 10.1. For \( \phi \in S(\mathbb{R}) \) an even function such that \( \text{supp}(\hat{\phi}) \subset (-1,1) \), we have for the one-level density of the family of quadratic twists of \( E \)

\[
\langle Z_\phi \rangle_{N,C} = \int_{O(M)} Z_\phi(\Theta) d\Theta + \mathcal{O}_{E,q}(1/N)
\]

where \( M = 2N + \deg(N_E) - 4 \).

As an application, we get an upper bound on the average analytic rank. The analytic rank of \( E \otimes \chi_D \) is defined as the number of \( \theta_{D,j} = 0 \) in \( \Theta_D \), and we denote it by \( r(E \otimes \chi_D) \). We define

\[
\langle r \rangle_{N,C} := \frac{1}{|H_{N,C}|} \sum_{D \in H_{N,C}} r(E \otimes \chi_D)
\]

and the average analytic rank is defined as

\[
r_C := \lim_{N \to \infty} \langle r \rangle_{N,C}
\]

if the limit exists. We prove the followings.

Theorem 11.1. We have \( r_C \leq \frac{3}{2} \).

In particular, the average analytic rank is \( \leq \frac{3}{2} \) in the whole family of twists \( D \in H_N \). By splitting the family according to congruence classes we get the following result on the non-vanishing at the central point.

Theorem 11.3. At least 12.5\% of the family of quadratic twists of \( E \) have rank zero and at least 37.5\% have rank one as \( N \to \infty \).

In the final section, we study the one-level density for the family of twists of \( E \) of order \( \ell \) coprime to \( q \). However, the results are too weak to produce any significant bound on the average analytic rank. We get the following restriction on the support of the Fourier transform of \( \phi \) where \( U(M) \) is the unitary group of dimension \( M \).

Theorem 12.1. For \( \phi \in S(\mathbb{R}) \) an even function such that \( \text{supp}(\hat{\phi}) \subset (-1/2,1/2) \), we have for the one-level density of the family of twists of \( E \) of order \( \ell \neq 2 \) and \( (\ell,q) = 1 \)

\[
\langle Z_\phi \rangle_{N,C} = \int_{U(M)} Z_\phi(\Theta) d\Theta + \mathcal{O}_{E,q,\ell}(1/N)
\]

where \( M = 2N + \deg(N_E) - 4 \).

The condition \( \text{supp}(\hat{\phi}) \subset (-1/2,1/2) \) for twists of \( E \) is the analogous result of the condition \( \text{supp}(\hat{\phi}) \subset (-1/m,1/m) \) for twists of a given cuspidal representation of \( \text{GL}_m(A_\mathbb{Q}) \) obtained by Cho and Park over \( \mathbb{Q} \) [CP19].

2. Background

2.1. Elliptic curves. The degree of a polynomial \( A \in \mathbb{F}_q[t] \) is denoted by \( \deg(A) \). We define \( N_E \), the conductor of \( E \), by

\[
N_E = \prod_{P \in \mathbb{F}_q[t]} P^{f_P(E)}
\]

where

\[
f_P(E) := \begin{cases} 
0, & \text{if } E \text{ has good reduction at } P \\
1, & \text{if } E \text{ has multiplicative reduction at } P \\
2, & \text{if } E \text{ has additive reduction at } P 
\end{cases}
\]

including the prime at infinity. A good reduction means that \( E/P \), the reduction of \( E \) at a prime \( P \in \mathbb{F}_q[t] \), is an elliptic curve over \( \mathbb{F}_q[t]/(P) \cong \mathbb{F}_{q^{\deg(P)}} \), which is a finite field. By the Weil’s conjectures, its zeta function is equal to

\[
Z(E/P, u) = \frac{(1 - \alpha_P(E)u)(1 - \overline{\alpha_P(E)}u)}{(1 - u)(1 - q^{\deg(P)}u)}
\]
where \( \alpha_P(E) \) and \( \overline{\alpha}_P(E) \) may be swapped. We call those values the Frobenius eigenvalues of \( E \) at \( P \) and since we fixed \( E \), we simply write them as \( \alpha_P \) and \( \overline{\alpha}_P \). For primes of good reduction, they may be computed using

\[
a_P := \alpha_P + \overline{\alpha}_P = q^\deg(P) + 1 - \#(E/P)
\]

where \( \#(E/P) \) is the number of \( \mathbb{F}_{q^\deg(P)} \)-points of \( E/P \). When \( E/P \) isn’t an elliptic curve, we say that the reduction is bad. If the reduction is multiplicative, we have \( a_P = \pm 1 \), and if the reduction is additive, we have \( a_P = 0 \). We will often use the fact that \( |\alpha_P| = q^{\deg(P)/2} \) from the Weil’s conjectures for primes of good reduction.

2.2. \( L \)-functions. Let \( \chi \) be a primitive Dirichlet character on \( \mathbb{F}_q[t] \) (see [Ros13] for background). Its \( L \)-function is defined by

\[
L(\chi, u) := \prod_P (1 - \chi(P)u^\deg(P))^{-1}
\]

where the product is over the primes of \( \mathbb{F}_q[t] \) excluding the prime at infinity.

The \( L \)-function of \( E \) is defined by

\[
L(E, u) := \prod_{P \mid N_E} (1 - \alpha_P u^\deg(P))^{-1} (1 - \overline{\alpha}_P u^\deg(P))^{-1} \prod_{P \mid N_E} (1 - a_P u^\deg(P))^{-1}
\]

and the \( L \)-function of \( E \) twisted by \( \chi \) is defined by

\[
L(E \otimes \chi, u) := \prod_{P \mid N_E} (1 - \chi(P)\alpha_P u^\deg(P))^{-1} (1 - \chi(P)\overline{\alpha}_P u^\deg(P))^{-1} \prod_{P \mid N_E} (1 - \chi(P)a_P u^\deg(P))^{-1}
\]

excluding the prime at infinity.

A Dirichlet character is uniquely factored into

\[
\chi = \tilde{\chi}\chi_0
\]

where \( \tilde{\chi} \) is primitive and \( \chi_0 \) is principal with minimal modulus. For example, if \( \chi \) is primitive, then \( \chi_0 \equiv 1 \). If \( \tilde{\chi} \) is principal, then \( \chi_0 \equiv 1 \). A character is said to be even if it is trivial on \( \mathbb{F}_q[t] \). It is called odd otherwise.

We also split \( \mathcal{H}_N^+ = \mathcal{H}_{N,+} \cup \mathcal{H}_{N,-} \) depending on if the sign of the functional equation of \( L(E \otimes \chi_D, u) \) for \( D \in \mathcal{H}_N^+ \) is 1 or \(-1\) respectively.

2.3. Gauss sums. As done by Hayes [Hay66], we define the following function on \( \mathbb{F}_q(t) \)

\[
e_q(A) := e^{2\pi i \text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(A_1)}/p
\]

where \( A_1 \) is the coefficient of \( 1/t \) in the Laurent expansion of \( A \).

The Gauss sum of a primitive character \( \chi \) of conductor \( F \) is defined as

\[
G(\chi) := \sum_{A \mod F} \chi(A)e \left( \frac{A}{F} \right)
\]

and it does not depend on the choice of representatives.

We also define

\[
\tau(\chi) := \sum_{a \in \mathbb{F}_q^*} \chi(a)e^{2\pi i \text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)/p}.
\]

We denote by \( \omega(\chi) \) the sign of the functional equation of \( L(\chi, u) \) and it is given in Lemma 3.2. When \( \chi \) is quadratic, \( \omega(\chi) \) is always 1 (see [Rud08]).

We denote the orthogonal group of dimension \( M \) by \( O(M) \). The subgroup of matrices with determinant 1 is denoted by \( SO(M) \). Two different symmetry types exist depending on the parity of \( M \). They are denoted by \( SO(\text{even}) \) and \( SO(\text{odd}) \).
3. Duality

**Proposition 3.1** (Riemann Hypothesis). Let \( \chi \) be a primitive Dirichlet character of conductor \( F \neq 1 \) on \( \mathbb{F}_q[t] \). Then

\[
L(\chi, u) = (1 - u)^\lambda \prod_{j=1}^{M} (1 - q^{1/2} e^{i\theta_j} u)
\]

where \( M = \deg(F) - 1 \) and \( \lambda = 0 \) if \( \chi \) is odd or else \( M = \deg(F) - 2 \) and \( \lambda = 1 \).

**Proof.** We have by Theorem 9.16B of [Ros13]

\[
L(\chi, u) K_\infty(\chi, u) = \prod_{j=1}^{M} (1 - q^{1/2} e^{i\theta_j} u)
\]

where

\[
K_\infty(\chi, u) = (1 - \chi(P_\infty) u)^{-1}
\]

is the Euler factor of the prime at infinity. This implies \( L(\chi, u) \) have at most one zero on \( |u| = 1 \) and all others are on \( |u| = q^{-1/2} \).

We have the expansion

\[
L(\chi, u) = \sum_{h=0}^{\infty} \left( \sum_{D \in M_h} \chi(D) \right) u^h.
\]

When \( h \geq \deg(F) \), the polynomials become equidistributed modulo \( F \) so the coefficient of \( u^h \) is zero. We also have by [Ros13] that

\[
\sum_{D \in M_{\deg(F) - 1}} \chi(D) \neq 0
\]

meaning that \( L(\chi, u) \) is a polynomial of degree \( \deg(F) - 1 \).

When \( \chi \) is even

\[
(q - 1)L(\chi, 1) = \left( \sum_{a \in \mathbb{F}_q^*} \chi(a) \right)^{\deg(F) - 1} \left( \sum_{D \in M_{\deg(F) - 1}} \chi(D) \right) = \sum_{D \in \mathbb{F}_q[t]} \chi(D) = 0
\]

so a zero is forced at \( u = 1 \).

When \( \chi \) is odd, we refer to Tao’s blog [Tao19] Theorem 2 where it is stated that all zeros of \( L(\chi, u) \) have norm \( q^{-1/2} \).

We remark that Theorem 9.16B [Ros13] only holds for geometric extensions. To each character \( \chi \) is associated a cyclic field extension \( K_\chi/\mathbb{F}_q[t] \) of degree equals to the order of \( \chi \). It is called a geometric extension if its field of constants is \( \mathbb{F}_q \). A character associated to a field of constants extension has the form

\[
\chi_c(D) = \zeta^{\deg(D)}
\]

where \( \zeta \) is a root of unity in \( \mathbb{C} \). Those characters aren’t Dirichlet characters since they are not periodic to any modulo (\( \chi_c \) is never 0), which shows that \( K_\chi \) is geometric in the case of Dirichlet characters. \( \square \)

The following lemma can also be obtained using Poisson summation formula (see [BF16]). In this case, the character \( \chi \) doesn’t have to be primitive, but the summands become Gauss sums.

**Lemma 3.2** (Duality). Let \( \chi \) be a primitive Dirichlet character of conductor \( F \neq 1 \). Then

\[
\sum_{B \in M_j} \chi(B) = \omega(\chi) q^{-\deg(F)/2} \sum_{k=0}^{\deg(F) - 1 - j} \sigma(\chi) \sum_{B \in M_{\deg(F) - 1 - j - k}} \chi(B)
\]
where $\omega(\chi)$ is given by (3.2) and $\sigma_\chi(k)$ is given by (3.4). Furthermore, $\sigma_\chi(k)$ only depends on the parity of the character, $|\sigma_\chi(k)| \leq q$, and $|\omega(\chi)| = 1$.

**Proof.** This was proven by Rudnick ([Rud08] Proposition 7) for quadratic Dirichlet characters. We adjust his computations for arbitrary orders.

Assume first that $\chi$ is odd. By the above proposition

$$L(\chi, u) = \prod_{j=1}^M (1 - q^{1/2} e^{i\theta_j} u)$$

where $M = \deg(F) - 1$. Since

$$L(\chi, u) = \prod_{j=1}^M (1 - q^{1/2} e^{-i\theta_j} u)$$

we have

(3.1) $$L\left(\chi, \frac{1}{qu}\right) = \prod_{j=1}^M \left(1 - e^{-i\theta_j} \frac{1}{q^{1/2} u}\right)$$

$$= \prod_{j=1}^M e^{-i\theta_j} \prod_{j=1}^M (e^{i\theta_j} u q^{1/2} - 1)$$

$$= \frac{1}{\omega(\chi) u^M q^{M/2}} L(\chi, u)$$

where

(3.2) $$\omega(\chi) = \prod_{j=1}^M -e^{i\theta_j}.$$ 

Now, using

$$L(\chi, u) = \sum_{j=0}^M \left( \sum_{B \in M_j} \chi(B) \right) u^j$$

and the last equation, we get by comparing powers of $u$

$$\sum_{B \in M_{j}} \chi(B) = \omega(\chi) q^{j - M/2} \sum_{B \in M_{M-j}} \chi(B).$$

When $\chi$ is even, we have to deal with the extra factor $(1 - u)$. Let

$$\frac{L(\chi, u)}{1 - u} = \sum_{j=0}^M A_j u^j.$$ 

Since we removed the extra zero, we can use the above computation to get

$$A_j = \omega(\chi) q^{j - M/2} \overline{A}_{M-j}.$$ 

Also, we have

$$\sum_{B \in M_{j}} \chi(B) = A_j - A_{j-1}$$

which implies

(3.3) $$A_j = \sum_{k=0}^j \sum_{B \in M_k} \chi(B).$$

Then

$$\sum_{B \in M_{j}} \chi(B) = A_j - A_{j-1} = \omega(\chi) q^{j - 1 - M/2} (q \overline{A}_{M-j} - \overline{A}_{M+1-j})$$
and by Equation (3.3) above
\[
\sum_{B \in \mathcal{M}_j} \chi(B) = -\omega(\chi)q^{j-M/2-1} \left( \sum_{B \in \mathcal{M}_{M+1-j}} \chi(B) - (q-1) \sum_{k=0}^{M-j} \sum_{B \in \mathcal{M}_k} \chi(B) \right)
\]
where \( M = \deg(F) - 2 \). For ease of use we define
\[
(3.4) \quad \sigma_\chi(k) := \begin{cases} 
q^{1/2} & \text{if } k = 0 \\
0 & \text{otherwise}
\end{cases}
\]
when \( \chi \) is odd and
\[
(3.5) \quad \sigma_\chi(k) := \begin{cases} 
-1 & \text{if } k = 0 \\
q - 1 & \text{otherwise}
\end{cases}
\]
when \( \chi \) is even. \( \square \)

4. The explicit formula

**Proposition 4.1** (Riemann Hypothesis). For \( \chi \) a primitive Dirichlet character of conductor \( F \neq 1 \) coprime to \( N_E \)

\[
(4.1) \quad L(E \otimes \chi, u) = \prod_{j=1}^{M} (1 - qe^{i\theta_j}u)
\]

where \( M = 2 \deg(F) + \deg(N_E) - 4 \).

**Proof.** Let \( \ell \) be the order of \( \chi \). We first assume \( \ell \) to be prime. Let \( K_\chi/F_q[t] \) be the cyclic field extension associated to \( \chi \). By Artin’s conjecture, which has been proven over function fields, we have

\[
L(E/K_\chi, u) = L(E, u) \prod_{i=1}^{l-1} L(E \otimes \chi^i, u)
\]

and all of these functions are entire. When no field is specified in the parameters of the \( L \)-function, the Euler product is assumed to be over \( F_q[t] \), otherwise it is over the specified field. By [CFJ15] Theorem 1.1 (ii)

\[
L(E/K_\chi, u) = \prod_{j=1}^{L} (1 - qe^{i\theta_j}u)
\]

where \( L = \deg_K(\mathcal{N}_E) + 2(2g - 2) \) and \( g \) is the genus of \( K_\chi \). The function \( \deg_K(\mathcal{N}_E) \) is defined on primes of \( K_\chi \) by \( \deg_K(p) := \log_q[K_\chi/(p)] \) and extended using \( \deg_K(pq) = \deg_K(p) + \deg_K(q) \). In particular, for \( P \) a prime of \( F_q[t] \), we have \( \deg_K(P) = \ell \cdot \deg(P) \). The conductor \( \mathcal{N}_E \) is the conductor of \( E \) over \( K_\chi \). Since \( (F, N_E) = 1 \), only the prime at infinity might ramify in \( K_\chi/F_q[t] \). We recall that we assume \( P_\infty^2 \mid N_E \) where \( P_\infty \) is the prime at infinity of \( F_q[t] \).

If \( \chi \) is even, the prime at infinity is not ramified in \( K_\chi/F_q[t] \). This means \( \deg_K(\mathcal{N}_E) = \ell \cdot \deg(N_E) \). We also have \( 2g = (\ell - 1)(\deg(F) - 2) \) and \( L(E, u) \) has degree \( \deg(N_E) - 4 \) ([Bru92], Appendix). This implies \( M = 2 \deg(F) + \deg(N_E) - 4 \) since the twisted \( L \)-functions have the same number of zeros since \( \ell \) is prime.

If \( \chi \) is odd, the prime at infinity is ramified in \( K_\chi/F_q[t] \). We denote by \( p_\infty \) the prime at infinity of \( K_\chi/F_q[t] \). We have \( P_\infty = (p_\infty)^\ell \). However, \( P_\infty^2 \mid N_E \). We have \( P_\infty^2 \mid N_E \) instead, so the conductors \( N_E \) and \( \mathcal{N}_E \) are not equal and we have \( \deg(K_\chi(\mathcal{N}_E) = \ell \cdot \deg(N_E) - 2(\ell - 1) \). Also, \( 2g = (\ell - 1)(\deg(F) - 1) \). This implies \( M = 2 \deg(F) + \deg(N_E) - 4 \). The result can be generalized to composite orders using induction.

We remark that the theorems we have used in this proof include the prime at infinity in their definition of the \( L \)-function. Since we have assumed that \( E \) has additive reduction at infinity, it makes no difference that we exclude the prime at infinity in our definition. \( \square \)
Lemma 4.2 (Explicit Formula). For $\chi$ a primitive Dirichlet character of conductor $F \neq 1$ coprime to $N_E$,

$$\sum_{d|n} \sum_{P \in \mathcal{P}_{n/d}} (n/d)(\alpha^d_P + \overline{\alpha}^d_P)\chi^d(P) = -q^n \sum_{j=1}^{M} e^{in\theta_j}$$

where $\alpha^d_P + \overline{\alpha}^d_P$ is replaced by $a^d_P$ for primes dividing $N_E$.

Proof. We get the result by comparing the coefficients of the powers of $u$ in the logarithmic derivative of (4.1) to those coming from the logarithmic derivative of the Euler product. \qed

5. Average of traces

The main theorem of this paper is the following.

Theorem 5.1. For $\epsilon > 0$, $n > 0$, and $N > 4\deg(N_E)$

$$\langle \text{tr } \Theta^n \rangle_{N,C} = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases} + O_{E,q} \left( (n + N)^{2\deg(N_E) + 3} \left( \frac{1}{q^{n/8}} + \frac{1}{q^N} + \frac{q^{n/2}}{q^{(1-\epsilon)N}} \right) + n^2 q^{-n/4} \right).$$

Proof. By the explicit formula (Lemma 4.2)

$$\langle \text{tr } \Theta^n \rangle_{N,C} = \frac{-1}{q^n |H_{N,C}|} \sum_{d|n} \sum_{\deg(P) = n/d} (n/d)(\alpha^d_P + \overline{\alpha}^d_P) \sum_{D \in H_{N,C}} \chi^d(D)(P)$$

Combining each estimate of Sections 7, 8, and 9 concludes the proof. \qed

6. The sieve

We sieve for two conditions, the polynomials must be square-free and congruent to $C$ modulo $N_E$ for some $C$ coprime to $N_E$. We use the techniques of [BF16] Lemma 2.2. The notation $A | B^\infty$ means that if a prime divides $A$, then it must divide $B$.

Lemma 6.1.

$$\sum_{D \in H_{N,C}} \chi_D(P) = \frac{1}{|\mathbb{F}_q[t]/(N_E)|^*} \sum_{\psi \mod N_E} \bar{\psi}(C) \sum_{k=0}^{N} \sum_{m=0}^{k} \alpha_\psi(m) \mu(Q_1)\psi(Q_1)\chi_{Q_1}(P)\psi_2(Q_2) \sum_{D \in M_{N-k}} \psi(D)\chi_D(P)$$

where $\alpha_\psi := \psi^2$, $\psi = \hat{\psi}\psi_0$ and $\psi_2 = \hat{\psi}_2\psi_0$ as in Equation (2.1). The modulus of $\hat{\psi}$ is denoted by $M_\psi$ and the modulus of $(\psi_2)$ is denoted by $N_\psi$. The function $\alpha_\psi$ is given by (6.5) and $|\alpha_\psi(m)| \leq m^{2\deg(N_E)} q^{m/2}$.

Proof. Polynomials $D \in \mathbb{F}_q[t]$ that are congruent to $C$ mod $N_E$ are picked up using

$$\frac{1}{|\mathbb{F}_q[t]/(N_E)|^*} \sum_{\psi \mod N_E} \bar{\psi}(C)\psi(D) = \begin{cases} 1 & \text{if } D \equiv C \mod N_E \\ 0 & \text{otherwise} \end{cases}$$

where the sum is over all Dirichlet characters modulo $N_E$. So

$$\sum_{D \in H_{N,C}} \chi_D(P) = \frac{1}{|\mathbb{F}_q[t]/(N_E)|^*} \sum_{\psi \mod N_E} \bar{\psi}(C) \sum_{D \in H_N} \psi(D)\chi_D(P)$$

and we write the generating series as

$$\sum_{h=0}^{\infty} \left( \sum_{D \in H_h} \psi(D)\chi_D(P) \right) u^h = \prod_{Q \text{ prime}} \left( 1 + \psi(Q)\chi_Q(P)u^{\deg(Q)} \right)$$
Also \( \prod \)\( \frac{\prod_Q (1 - \psi_2(Q) \chi_Q(P) u^{-2\deg(Q)})}{\prod_Q (1 - \psi(Q) \chi_Q(P) u^{-\deg(Q)})} \)
\( = \frac{\prod_Q (1 - \hat{\psi}(Q) \chi_Q(P) u^{\deg(Q)})^{-1} \prod_Q |M_q| (1 - \hat{\psi}(Q) \chi_Q(P) u^{\deg(Q)})}{\prod_Q (1 - \hat{\psi}_2(Q) u^{2\deg(Q)})^{-1} \prod_Q |P_{N_q}| (1 - \hat{\psi}_2(Q) u^{2\deg(Q)})} \).

We now expand all four products. We first have

\[
\prod_Q (1 - \hat{\psi}(Q) \chi_Q(P) u^{\deg(Q)})^{-1} = \sum_{h=0}^{\infty} \left( \sum_{D \in M_h} \hat{\psi}(D) \chi_D(P) \right) u^h.
\]

Also
\[
\prod_Q (1 - \hat{\psi}_2(Q) u^{2\deg(Q)})^{-1} = L(\hat{\psi}_2, u^2).
\]

We assume first that \( \hat{\psi}_2 \) isn’t trivial. We use Proposition 3.1 to expand
\[
\frac{1}{L(\hat{\psi}_2, u^2)} = (1 - u^2)^{-\lambda} \prod_{j=1}^{M} (1 - q^{1/2} e^{i \theta_j \psi} u^2)^{-1}
\]
\( = \left( \sum_{h=0}^{\infty} u^{2h} \right)^{\lambda} \prod_{j=1}^{M} \sum_{h=0}^{\infty} q^{h/2} e^{i \theta_j \psi} u^{2h}.\)

We expand again to get

\[
\frac{1}{L(\hat{\psi}_2, u^2)} = \sum_{h=0}^{\infty} \alpha_\psi(h) u^h
\]
and bounding trivially gives \( |\alpha_\psi(h)| \leq h^{\deg(N_E)} q^{h/4}.\)

If \( \hat{\psi}_2 \) is trivial, then \( 1/L(\hat{\psi}_2, u^2) = 1 - qu^2 \) and so \( \alpha_\psi(0) = 1, \alpha_\psi(2) = -q, \) and it is 0 everywhere else, which is the case of [BF16] Lemma 2.2. We use the bound \( |\alpha_\psi(h)| \leq h^{\deg(N_E)} q^{h/2} \) to deal with both cases at once.

For the two remaining products, we use
\[
(1 - \hat{\psi}_2(Q) u^{2\deg(Q)})^{-1} = \sum_{h=0}^{\infty} \hat{\psi}_2(Q^h) u^{2h \deg(Q)}
\]
to get

\[
\frac{\prod_{Q | M_q} (1 - \hat{\psi}(Q) \chi_Q(P) u^{\deg(Q)})}{\prod_{Q | P_{N_q}} (1 - \hat{\psi}_2(Q) u^{2\deg(Q)})} \sum_{h=0}^{\infty} \left( \sum_{Q_1 | M_q} \mu(Q_1) \hat{\psi}(Q_1) \chi_{Q_1}(P) \hat{\psi}_2(Q_2) \right) u^h.
\]

We multiply the series (6.4), (6.5), and (6.6) and compare powers of \( u \) in Equation (6.3). We put the result into Equation (6.2) to conclude.

We now compute the size of \( \mathcal{H}_{N,C} \) in a similar fashion, but we use Perron’s formula instead of multiplying the generating series together.

**Lemma 6.2.** For \( (C, N_E) = 1 \) and any \( \epsilon > 0 \)
\[
|\mathcal{H}_{N,C}| = \frac{1}{|\mathcal{F}_q[1]/(N_E)|^*} (1 - q^{-1}) \prod_{Q | N_E} (1 + q^{-\deg(Q)})^{-1} q^{N+1} + O_{E,q,\epsilon}(q^{N(1/4+\epsilon)}).
\]
In particular, the family $\mathcal{H}_E$ is equidistributed in the invertible congruence classes modulo $N_E$ as $N \to \infty$. Furthermore, $|\mathcal{H}_{N,C}| \approx_{E,q} q^N$.

Proof. We deal with the congruence condition using (6.1). So

$$\sum_{D \in \mathcal{H}_{N,C}} 1 = \frac{1}{|\mathcal{H}_E|/(N_E^{*1})} \sum_{\psi \text{ mod } N_E} \overline{\psi}(C) \sum_{D \in \mathcal{H}_N} \psi(D)$$

and we write the generating series as

$$\mathcal{L}(\psi, u) := \sum_{h=0}^{\infty} \left( \sum_{D \in \mathcal{H}_h} \psi(D) \right) u^h = \prod_{Q \text{ prime}} \left( 1 + \psi(Q) u^{\deg(Q)} \right)$$

$$= \prod_Q (1 - \psi(Q) u^{2\deg(Q)}) \prod_Q (1 - \psi(Q) u^{\deg(Q)})$$

$$= \prod_Q (1 - \psi(Q) u^{2\deg(Q)})^{-1} \prod_Q (1 - \psi(Q) u^{\deg(Q)})$$

$$= \frac{L(\psi, u) \prod_{Q \mid M_\psi} (1 - \psi(Q) u^{\deg(Q)})}{L(\psi_2, u^2) \prod_{Q \mid N_\psi} (1 - \psi_2(Q) u^{2\deg(Q)})}$$

where $\psi_2 = \psi^2$, $\psi_0 = \hat{\psi} \psi_0$ and $\psi_2 = \hat{\psi}_2(\psi_2)_0$ as in Equation (2.1). The modulus of $\psi_0$ is denoted by $M_\psi$ and the modulus of $(\psi_2)_0$ is denoted by $N_\psi$. Perron’s formula works by dividing the generating series by $u^{N+1}$ in order to create a pole at $u = 0$ such that its residue is the $N$th coefficient of the series. Here

$$\frac{\mathcal{L}(\psi, u)}{u^{N+1}} = \sum_{h=0}^{\infty} \left( \sum_{D \in \mathcal{H}_h} \psi(D) \right) u^{h-N-1}.$$

This sum is the Laurent expansion of $\frac{\mathcal{L}(\psi, u)}{u^{N+1}}$ at $u = 0$, so the residue at $u = 0$ is the coefficient of $u^{-1}$, which is

$$\sum_{D \in \mathcal{H}_N} \psi(D).$$

We’re going to use Cauchy’s residue theorem by integrating on the complex circle $C_\epsilon : |u| = q^{-1/4-\epsilon}$ the following function

$$\mathcal{L}(\psi, u) = \frac{L(\psi, u) \prod_{Q \mid M_\psi} (1 - \psi(Q) u^{\deg(Q)})}{L(\psi_2, u^2) \prod_{Q \mid N_\psi} (1 - \psi_2(Q) u^{2\deg(Q)})} \frac{1}{u^{N+1}}$$

If $\hat{\psi}$ is trivial

$$L(\hat{\psi}, u) = \frac{1}{1 - qu}$$

and it has a unique simple pole at $u = 1/q$. If $\hat{\psi}$ isn’t trivial, then

$$L(\hat{\psi}, u) = (1-u)^{K_\psi} \prod_{j=1}^{K_\psi} (1-q^{1/2} e^{i\theta_j} u)$$

where $K_\psi \leq \deg(N_E)$ and it has no poles. If $\hat{\psi}_2$ is trivial

$$L(\hat{\psi}_2, u^2) = 1 - qu^2$$

and it has no poles. If $\hat{\psi}_2$ isn’t trivial

$$\frac{1}{L(\psi_2, u^2)} = (1-u)^{-\lambda_{\psi_2}} \prod_{j=1}^{K_{\psi_2}} (1 - q^{1/2} e^{i\theta_{\psi_2,j}} u^2)^{-1}$$
where $K_{\psi_2} \leq \deg(N_E)$ and it has poles of norm $q^{-1/4}$. The two remaining products of (6.8) have poles and zeros of norm one.

We define

$$A(E, q, \epsilon) := \sup_{\psi \mod N_E} \sup_{u = q^{-1/4 - \epsilon}} \left| \frac{L(\psi, u) \prod_{Q|M_\psi} (1 - \hat{\psi}(Q) u^{2\deg(Q)})}{L(\psi_2, u^2) \prod_{Q|N_\psi} (1 - \hat{\psi_2}(Q) u^{2\deg(Q)})} \right|.$$ 

We have $A(E, q, \epsilon) < \infty$ since these functions have no poles on $C_\epsilon$. We also have $|1/u^{N+1}| = q^{1/4 + \epsilon} + 1/4 + \epsilon$ on $C_\epsilon$, so

(6.9) \[ \left| \oint_{C_\epsilon} \frac{L(\psi, u)}{u^{N+1}} \right| \leq 2\pi A(E, q, \epsilon) q^{(1/4 + \epsilon)} \ll \epsilon_{E, q, \epsilon} q^{1/4 + \epsilon}. \]

If $\hat{\psi}$ is trivial, then $\psi$ is the principal character modulo $N_E$. In this case, we have by Cauchy's residue theorem

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{L(\psi, u)}{u^{N+1}} = \text{Res}_{u = 0} L(\psi, u) u^{N+1} + \text{Res}_{u = 1/q} L(\psi, u) u^{N+1} = \sum_{D \in \mathcal{H}_N} \psi(D) + (1 - q^{-1}) \prod_{Q|N_E} (1 + q^{-\deg(Q)})^{-1} q^{N+1}$$

since $\hat{\psi}_2$ is also trivial, and $M_\psi$ and $N_\psi$ are both equal to the product of all the primes dividing $N_E$.

If $\psi$ isn’t the principal character modulo $N_E$, then there is only a pole at $u = 0$ and

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{L(\psi, u)}{u^{N+1}} = \sum_{D \in \mathcal{H}_N} \psi(D).$$

We use those two results along with (6.9) in (6.7) to get

$$\sum_{D \in \mathcal{H}_{N, C}} 1 = \frac{1}{|\mathcal{F}_q(t)/(N_E)|^2} (1 - q^{-1}) q^{N+1} \prod_{Q|N_E} (1 + q^{-\deg(Q)})^{-1} + \mathcal{O}_{E, q, \epsilon}(q^{1/4 + \epsilon}).$$

By Proposition 1.4. and 1.6. [Ros13] we have $|\mathcal{F}_q(t)/(N_E)|^2 \approx q^{\deg(N_E)}$, so we can conclude

$|\mathcal{H}_{N, C}| \approx \epsilon_{E, q, \epsilon} q^N$. 

\[\square\]

7. CONTRIBUTION OF THE PRIMES

The contribution of the primes in Equation (5.1) corresponds to the terms with $d = 0$, which is

$$S_C(N, n) := \frac{-1}{q^n|\mathcal{H}_{N, C}|} \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha} P) \sum_{D \in \mathcal{H}_{N, C}} \chi_D(P).$$

We start with a lemma that will be useful for bounding some quantities coming from the sieve.

Lemma 7.1.

$$\sum_{\substack{Q \mid N_E \\text{\degree} Q = N \\text{\degree}}} 1 \leq (N + 1)^{\deg(N_E)}$$

Proof. In the worst case scenario, $N_E$ is a product of distinct primes of degree one. We use induction on the degree of $N_E$. If $N_E$ is prime, then there is only the possibility $Q = N_E$, the lemma is true in this case.

Now we assume the lemma is true for $\deg(N_E) = k$. Let $\deg(N_E) = k + 1$ and fix a prime $P_0$ that divides $N_E$. We split the terms depending on the powers of $P_0$ dividing them

$$\sum_{\substack{Q \mid N_E \\text{\degree} Q = N \\text{\degree}}} 1 = \sum_{j=0}^{N} \sum_{\substack{Q \mid (N_E/P_0)^{j} \\text{\degree} Q = N-j \\text{\degree}}} 1 \leq (N + 1)^{k+1}$$

11
and this concludes the induction. □

**Proposition 7.2.** For any \( \epsilon > 0 \) and \( N > 4 \deg(N_E) \)

\[
S_C(N, n) \ll_{E,q} (n + N)^{N^2 \deg(N_E) + 3} \left( \frac{1}{q^{N/8}} + \frac{1}{q^{rN}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}} \right).
\]

**Proof.** We apply the sieve (Proposition 6.1) and quadratic reciprocity \( \chi_D(P) = (-1)^{\deg(D)\deg(P)(q-1)/2} \chi_P(D) \) to write

\[
S_C(N, n) = \sum_{P \in \mathcal{P}_n} n(\alpha_P + \alpha_P) \left( \frac{1}{|F_q[t]/(N_E)|!} \right) \sum_{\psi \bmod N_E} \overline{\psi}(C) \sum_{k \geq cN} \alpha_\psi(m) \sum_{\ell = 0}^{\lfloor \frac{k-m}{N} \rfloor} \sum_{Q_1 | M_\psi} \sum_{Q_2 | N_\psi} (-1)^{n(N-k)(q-1)/2} \mu(Q_1) \hat{\psi}(Q_1) \chi_Q(P) \hat{\psi}_2(Q_2 P^\ell) \sum_{D \in \mathcal{M}_{N-k}} \hat{\psi} \chi_P(D)
\]

where we split the sum over \( Q_2 \) according to powers of \( P \), so we define \( N_\psi := N_\psi/P \) if \( P \mid N_\psi \), and \( \tilde{N}_\psi := N_\psi \) if \( P \nmid N_\psi \). Assume first that \( n \leq N/4 \). The degree of the conductor of \( \hat{\psi} \chi_P \) is then bounded by \( N/4 + \deg(N_E) \). Then, when \( N - k \geq N/4 + \deg(N_E) \), the sum over the monic polynomials is zero, so it is bounded by \( q^{N/4+\deg(N_E)} \). Using Lemma 6.2 and Lemma 7.1 and noticing \( Q_1 \) has at most \( 2^{\deg(N_E)} \) possibilities gives

\[
S_C(N, n) \ll_{E,q} N^{\deg(N_E)+3} q^{N/8}
\]

by bounding everything else trivially. Therefore, the contribution of the primes of low degrees tends to zero as \( N \to \infty \).

Now, assume \( n > N/4 \). We also assume \( N > 4 \deg(N_E) \) so that \( \hat{\psi} \chi_P \) is primitive. We split into two cases depending on whether \( k \geq \epsilon N \) or \( k < \epsilon N \) for any \( \epsilon > 0 \).

We start with the case \( k \geq \epsilon N \). We want to bring the sum over \( P \) inside in order to use the explicit formula (Lemma 4.2). The sum is then

\[
\sum_{\psi \bmod N_E} \overline{\psi}(C) \sum_{k \geq cN} \alpha_\psi(m) \sum_{\ell = 0}^{\lfloor \frac{k-m}{N} \rfloor} \sum_{Q_1 | M_\psi} \sum_{Q_2 | N_\psi} (-1)^{n(N-k)(q-1)/2} \mu(Q_1) \hat{\psi}(Q_1) \hat{\psi}_2(Q_2) \sum_{D \in \mathcal{M}_{N-k}} \hat{\psi} \chi_P(D) \sum_{P \in \mathcal{P}_n} n(\alpha_P + \alpha_P) \chi_Q(P) \hat{\psi}_2(P^\ell)
\]

where we reapplied quadratic reciprocity on \( \chi_P(D) \). Let \( \Psi := \chi_{DQ} \hat{\psi}_2 \) and \( \Psi = \hat{\psi} \Psi_0 \) as in (2.1). The explicit formula for \( L(E \otimes \hat{\Psi}, u) \) gives the bound

\[
\sum_{d | n} \sum_{P \in \mathcal{P}_{n/d}} (n/d)(\alpha_P^d + \alpha_P^d \hat{\psi}^d(P) \ll_{E,q} N q^n.
\]

It is important to mention here that the conductor of \( \hat{\psi} \) might not be coprime to \( N_E \). The Riemann hypothesis is still valid for \( L(E \otimes \hat{\Psi}, u) \), but the number of zeros given in Proposition 4.1 could be changed by a quantity bounded by \( 2 \deg(N_E) \), which is why the bound remains valid. This bound also holds when \( \hat{\psi} \) is trivial, since then we get \( L(E, u) \) which has \( \deg(N_E) - 4 \) zeros of norm \( 1/q \). Now, since

\[
\sum_{d | n} \sum_{P \in \mathcal{P}_{n/d}} (n/d)(\alpha_P^d + \alpha_P^d \hat{\psi}^d(P) =
\]

12
\[
\sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) + \sum_{d | n} \sum_{P \in \mathcal{P}_{n/d}} (n/d)(\alpha_P^d + \overline{\alpha}_P^d)\hat{\Psi}^d(P)
\]

and
\[
\sum_{d | n} \sum_{P \in \mathcal{P}_{n/d}} (n/d)(\alpha_P^d + \overline{\alpha}_P^d)\hat{\Psi}^d(P) = O(nq^n)
\]

we have
\[
(7.4) \quad \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) \ll_E q^n(N + n).
\]

Also, we have
\[
\sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) = \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) - \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P)
\]

where \(K_{\Phi}\) is the modulus of \(\Psi\). We have assumed \(n > N/4\) and \(N > 4\deg(N_E)\), so only \(\chi_d\) can contribute to \(K_{\Phi}\), and it contributes at most two different primes. So
\[
\sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) = \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) + O(nq^{n/2}).
\]

Then
\[
\sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\hat{\Psi}(P) \ll_E q^n(N + n).
\]

This sum is exactly the sum over \(\mathcal{P}_n\) in (7.3). We use \(|\alpha\psi(m)| \leq q^{k/2}N^{\deg(N_E)}\) from Lemma 6.1 since \(m \leq k\) and we bound everything else trivially as we did for (7.2). We get that (7.3) is bounded by
\[
(7.5) \quad \ll_E, q \frac{(n + N)N^{2\deg(N_E)+3}}{q^{n/2}}
\]

which goes to zero as \(N \to \infty\).

For the case \(k < \epsilon N\), we apply duality (Lemma 3.2) to (7.1) to get
\[
(7.6) \quad \frac{-1}{q^n[H_{N,E}]} \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P) \left| [\mathbb{F}_q[t]/(N_E)]^* \right| \sum_{\psi \equiv \overline{\psi} \mod N_E} \psi(C) \sum_{k=0}^{\lfloor \frac{\epsilon N}{\pi} \rfloor} \sum_{m=0}^{k} \alpha_\psi(m) \sum_{\ell=0}^{\left\lfloor \frac{\epsilon N}{\pi} \right\rfloor} (-1)^{n(N-k)(q-1)/2} \mu(Q_1)\hat{\psi}(Q_1)\chi_\ell(P)\hat{\psi}(Q_2)\tilde{\psi}(Q_2)P^{\ell}
\]

\[
\omega(\hat{\psi}\chi_P)q^{N-k-(n+\deg(C_\psi))/2} \sum_{r=0}^{n+\deg(C_\psi)-1-N+k} \sigma_{\psi,\chi_P}(r) \sum_{D \in \mathcal{M}_{n+\deg(C_\psi)-1-N+k-r} D \in \mathcal{M}_{n+\deg(C_\psi)-1-N+k-r}} \overline{\psi}\chi_P(D)
\]

where \(C_\psi\) is the conductor of \(\hat{\psi}\).

The goal is again to sum over \(\mathcal{P}_n\) first in order to use the explicit formula (Lemma 4.2). To bring the sum inside, we must deal with \(\omega(\hat{\psi}\chi_P)\) to remove its dependency on \(P\).

Definitions related to Gauss sums can be found at the end of Section 2. Corollary 2.4 [DFL19] states that for primitive characters of conductor \(F\)
\[
\omega(\chi) = \begin{cases} \frac{1}{\pi}q^{-(\deg(F)-1)/2}G(\chi) & \text{if } \chi \text{ odd} \\ q^{-\deg(F)/2}G(\chi) & \text{if } \chi \text{ even} \end{cases}
\]
and adjusting Lemma 2.12 (i) [DFL19] for general Dirichlet characters gives
\[ G(\hat{\psi}(P)) = \hat{\psi}(P)\chi_P(C_{\hat{\psi}})G(\hat{\psi})G(\chi_P) \]
because \(\deg(P)\) is large enough for \(P\) to be coprime to \(C_{\hat{\psi}}\). Then, assuming the most complicated case where all characters are odd
\[ \omega(\hat{\psi}(P)) = \frac{1}{\chi(\hat{\psi}(P))}q^{-\deg(C_{\hat{\psi}})+n-1/2}G(\hat{\psi}(P)) \]
\[ = \frac{1}{\chi(\hat{\psi}(P))}q^{-\deg(C_{\hat{\psi}})+n-1/2}\hat{\psi}(P)\chi_P(C_{\hat{\psi}})G(\hat{\psi})G(\chi_P) \]
\[ = \frac{1}{\chi(\hat{\psi}(P))}q^{-1/2}\hat{\psi}(P)\chi_P(C_{\hat{\psi}})\omega(\hat{\psi})\tau(\hat{\psi})\omega(\chi_P)\tau(\chi_P). \]

If \(\deg(P)\) is even, then \(\chi_P(a) = 1\) for all \(a \in \mathbb{F}_q^*\) and if \(\deg(P)\) is odd, \(\chi_P(a) = 1\) if \(a\) is a square in \(\mathbb{F}_q^*\) and \(\chi_P(a) = -1\) otherwise. This implies \(\tau(\hat{\psi}(P)) \) and \(\tau(\chi_P)\) does not depend on the actual \(P\), only on its degree, since the sum defining these quantities is over \(\mathbb{F}_q^*\). We recall \(\omega(\chi_P) = 1\) since \(\chi_P\) is quadratic. This implies
\[ \omega_n(\hat{\psi}) := \frac{\omega(\hat{\psi}(P))}{\psi(\chi_P)\chi_P(C_{\hat{\psi}})} \]
only depends on \(\deg(P) = n\), hence the notation.

The other quantity that might depend on \(P\) is \(\sigma_{\hat{\psi}(P)}(r)\). We recall that it only depends on the parity of the character, and by the discussion above, the parity of \(\hat{\psi}(P)\) only depends on \(\hat{\psi}\) and the degree of \(P\). We therefore use the notation \(\sigma_{\hat{\psi},n}(r) := \sigma_{\hat{\psi}(P)}(r)\).

Replacing in (7.6) gives
\[ (7.7) -1 \frac{1}{q^n|\mathcal{H}_{N,C}|} \left[ \left( \frac{\mathbb{F}_q[t]}{(N_E)} \right)^* \right] \sum_{\psi \operatorname{mod} N_E} \overline{\psi}(C) \sum_{k=0}^{\lceil n \rceil} \sum_{m=0}^{k} \sum_{\ell=0}^{k-m} \sum_{Q_1 \mid M_{Q \psi}^\infty} \sum_{Q_2 \mid N_{\psi}^\infty} \mu(Q_1)\hat{\psi}(Q_1)\hat{\psi}(Q_2)\omega_n(\hat{\psi})q^{n-k-(n+\deg(C_{\hat{\psi}}))/2} \sum_{r=0}^{n+\deg(C_{\hat{\psi}})-1-N+k} (-1)^r(n-r-1)(q-1)^2 \]
\[ \sigma_{\hat{\psi},n}(r) = \sum_{D \in \mathcal{D}_{N_E \deg(C_{\hat{\psi}})-1-N+k}} \overline{\psi}(D) \sum_{P \in \mathcal{P}_n} n(\alpha_P + \overline{\alpha_P})\chi_D(P)\hat{\psi}(P)\chi_C(P)\hat{\psi}(D) \]

after applying quadratic reciprocity on \(\chi_D(D)\) and \(\chi_P(C_{\hat{\psi}})\). We use (7.4) to bound the sum over \(\mathcal{P}_n\). We have an extra \(\hat{\psi}\chi_C\) in the character, so it adds at most \(2\deg(N_E)\) to the degree of the conductor. Bounding everything else trivially, we have that (7.7) is
\[ \ll q^{N/6} q^{2\deg(N_E)+3} q^{n/2} q^{-N+\epsilon N/2}. \]
Combining this bound with (7.2) and (7.5) concludes to proof.

8. Contribution of the squares

The contribution of the squares comes from the terms with even \(d\) in Equation (5.1).

Proposition 8.1.
\[ \frac{-1}{q^n|\mathcal{H}_{N,C}|} \sum_{d \mid n} \sum_{\deg(P) \mid n/d} \frac{(n/d)(\alpha_P^d + \overline{\alpha_P^d})}{2 \mid d} \chi_D^d(P) = \begin{cases} 1 + O_E(n^2 q^{-n/4}), & \text{if } 2 \mid n \\ 0, & \text{if } 2 \nmid n \end{cases} \]
where \(\alpha_P^d + \overline{\alpha_P^d}\) is replaced by \(a_P^d\) for bad primes.
Proof. If $2 \nmid n$, there are no terms, hence no contribution.

When $2 \mid n$, we rewrite the sum as

$$(8.1) \quad \frac{-1}{q^{2m}|\mathcal{H}_{N,C}} \sum_{d | m} \sum_{d | m \deg(P) = m/d} (m/d) \left( \alpha_{P}^{2d} + \alpha_{P}^{2d} \right) \sum_{D \in \mathcal{H}_{N,C}} \chi_{D}^{2d}(P)$$

where $m := n/2$. The character equals $1_{P,D}$ because its power is even. A simple sieving gives

$$\sum_{D \in \mathcal{H}_{N,C}} 1 = \sum_{j=0}^{[N/\deg(P)]} (-1)^j \sum_{D \in \mathcal{H}_{N-j \deg(P), C \setminus D}} 1$$

if $(P, N_E) = 1$ so that $P$ is invertible modulo $N_E$. If $P \mid N_E$, then

$$\sum_{D \in \mathcal{H}_{N,C}} 1 = [\mathcal{H}_{N,C}]$$

since every $D$ is coprime to $N_E$ because $(C, N_E) = 1$. In the case $(P, N_E) = 1$, the sum with $j = 0$ is exactly $[\mathcal{H}_{N,C}]$. When $j > 0$

$$\sum_{j=1}^{[N/\deg(P)]} (-1)^j \sum_{D \in \mathcal{H}_{N-j \deg(P), C \setminus D}} 1 \asymp \sum_{j=1}^{[N/\deg(P)]} (-1)^j q^{N-j \deg(P)} \ll q^{N-\deg(P)} \sum_{j=0}^{\infty} q^{-j} \ll q^{N-\deg(P)}.$$  

Then

$$(8.2) \quad \sum_{D \in \mathcal{H}_{N,C}} \chi_{D}^{2d}(P) = [\mathcal{H}_{N,C}] + \mathcal{O}(q^{-\deg(P)})$$

which holds in both cases.

Now (8.1) is equal to

$$\frac{-1}{q^{2m}} \sum_{d | m \deg(P) = m/d} (m/d) \left( \alpha_{P}^{2d} + \alpha_{P}^{2d} \right) + \mathcal{O}(m^2 q^{-m}).$$

We retrieve the double sum by looking at the symmetric square of $L(E, u)$, which is defined by

$$L(\text{Sym}^2 E, u) := \prod_{P \mid N_E} \left( 1 - \alpha_{P}^{2d} u^{\deg(P)} \right)^{-1} \left( 1 - \alpha_{P}^{2d} \bar{u}^{d \deg(P)} \right)^{-1} \left( 1 - \bar{u}^{2d} u^{d \deg(P)} \right)^{-1} \left( 1 - \bar{u}^{2d} \bar{u}^{d \deg(P)} \right)^{-1}.$$

It is related to the variety

$$\text{Sym}^2 E : y^2 = (x^3 + Ax + B)(z^3 + Az + B).$$

It is known that ([CFJ15] Theorem 1.1)

$$L(\text{Sym}^2 E, u) = \prod_{j=1}^{M} (1 - q^{3/2} e^{i \theta_{\text{Sym}^2 E,j} u})$$

for some $M < \infty$ depending on $E$. The explicit formula for $L(\text{Sym}^2 E, u)$ is then

$$\sum_{d | m \deg(P) = m/d} (m/d) \left( \alpha_{P}^{2d} + q^{d \deg(P)} \alpha_{P}^{2d} \right) + \mathcal{O}(m^2 q^{-m}) = \sum_{j=1}^{M} e^{i \theta_{\text{Sym}^2 E,j}} q^{3m/2}$$

where we replace $\alpha_{P}^{2d} + q^{d \deg(P)} \alpha_{P}^{2d}$ by $\alpha_{P}^{2d}$ for bad primes. We have

$$\sum_{d | m \deg(P) = m/d} (m/d) q^{d \deg(P)} = q^{2m}$$
and
\[ \sum_{d|m \, \text{deg}(P)=m/d} (m/d) q^{d \cdot \text{deg}(P)} = \sum_{d|m \, \text{deg}(P)=m/d} (m/d) q^{d \cdot \text{deg}(P)} + \sum_{P \, \text{bad}} \sum_{d|m \, \text{deg}(P)=m/d} (m/d) q^{d \cdot \text{deg}(P)}. \]

Since there are at most \( \deg(N_E) \) bad primes
\[ \sum_{d|m \, \text{deg}(P)=m/d} (m/d) q^{d \cdot \text{deg}(P)} \ll \deg(N_E) mq^m. \]

This implies
\[ \sum_{d|m \, \text{deg}(P)=m/d} (m/d) \left( \alpha_P^{2d} + \overline{\alpha_P}^{2d} \right) = -q^{2m} + O_E(q^{3m/2}) \]
where we replace \( \alpha_P^{2d} + \overline{\alpha_P}^{2d} \) by \( a_P^{2d} \) for bad primes and this concludes the proof. \( \square \)

9. CONTRIBUTION OF HIGHER POWERS

Proposition 9.1.
\[ \frac{1}{q^n|H_{N,C}|} \sum_{d|m \, \text{deg}(P)=n/d} \sum_{n/d > 2} (n/d)(\alpha_P^d + \overline{\alpha_P}^d) \sum_{D \in H_{N,C}} \chi_D^d(P) \ll n^2 q^{-n/6}. \]

Proof. We bound everything trivially. \( \square \)

10. ONE-LEVEL DENSITY

Corollary 10.1. For \( \phi \in S(\mathbb{R}) \) an even function such that \( \text{supp}(\hat{\phi}) \subset (-1,1) \), we have
\[ \langle Z \phi \rangle_{N,C} = \int_{O(M)} Z\phi(\Theta) d\Theta + O_E, q(1/N) \]
where \( M = 2N + \deg(N_E) - 4 \).

Proof. The Fourier expansion of \( Z\phi(\Theta) \) is
\[ Z\phi(\Theta) = \int_{\mathbb{R}} \phi(x) dx + \frac{1}{M} \sum_{n \neq 0} \hat{\phi} \left( \frac{n}{M} \right) \text{tr} \Theta^n. \]
Since \( \text{tr} \Theta^{-n} = \text{tr} \Theta^n \), our main result is valid when \( n < 0 \). Averaging over \( H_{N,C} \) and applying Theorem 5.1 gives
\[ \langle Z \phi \rangle_{N,C} = \hat{\phi}(0) + \frac{1}{M} \sum_{n \neq 0} \hat{\phi} \left( \frac{n}{M} \right) \eta_n + O_E, q \left( \frac{1}{M} \sum_{n=1}^{\infty} \hat{\phi} \left( \frac{n}{M} \right) \left((n+N)N^2 \deg(N_E)+3 \left( \frac{1}{q^{N/8}} + \frac{1}{q^N} + \frac{q^{n/2}}{q^{(1-\epsilon)N}} \right) + n^2 q^{-n/4} \right) \right) \]
where
\[ \eta_n = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd.} \end{cases} \]
By Equation (1.2)
\[ \hat{\phi}(0) + \frac{1}{M} \sum_{n \neq 0} \hat{\phi} \left( \frac{n}{M} \right) \eta_n = \int_{O(M)} Z\phi(\Theta) d\Theta. \]
For the error term, we have that
\[ (n+N)N^2 \deg(N_E)+3 \left( \frac{1}{q^{N/8}} + \frac{1}{q^N} + \frac{q^{n/2}}{q^{(1-\epsilon)N}} \right) \]
tends to zero as $N \to \infty$ provided that $n < 2(1 - 2\epsilon)N$. The range of $n$ is controlled by restricting the support of $\hat{\phi}$, so it must be inside $(-1, 1)$ since $M \sim 2N$ as $N \to \infty$. For the second term of the error, notice that
\[
\sum_{n=1}^{\infty} n^2 q^{-n/4}
\]
converges, so
\[
\frac{1}{M} \sum_{n=1}^{\infty} \hat{\phi} \left( \frac{n}{M} \right) n^2 q^{-n/4}
\]
tends to zero as $N \to \infty$. □

**Remark.** By (6) [You04], we cannot distinguish between the symmetry types $O$, $SO$(even), and $SO$(odd) since they all have the same one-level density when the support of $\hat{\phi}$ is contained inside $(-1, 1)$.

11. **Average rank and non-vanishing**

One application of the one-level density is getting a bound on the average analytic rank.

**Theorem 11.1.** The family $\mathcal{H}_{N,C}$ of quadratic twists of an elliptic curve over $\mathbb{F}_q[t]$ has average analytic rank $r_C \leq 3/2$.

**Proof.** We adjust [You04] Section 5.5. We use Corollary 10.1 with
\[
\phi_n(x) = \left( \frac{\sin(\pi \nu x)}{\pi \nu x} \right)^2
\]
\[
\hat{\phi}_n(y) = \frac{1}{\nu} \left( 1 - |y| \right)
\]
where $\hat{\phi}_n$ is supported in $[-\nu, \nu]$ and is the Fourier transform of $\phi_n$. Since $\phi_n(0) = 1$ and $\phi_n(x) \geq 0$, we have $F(0) \geq 1$ and $F'(\theta) \geq 0$, where we defined $F'(\theta)$ in Section 2. This implies $\text{ord}_{u=1/q} L(E \otimes \chi_D, u) \leq Z_{\phi_n}(\Theta_D)$, so $r_{N,C} \leq (Z_{\phi_n})_{N,C}$. By Corollary 10.1
\[
r_{N,C} \leq \int_{O(M)} Z_{\phi_n}(\Theta) d\Theta + \mathcal{O}_{E,q}(1/N).
\]
By Equation (10.1), we need to evaluate
\[
\hat{\phi}_n(0) + \frac{1}{M} \sum_{n \neq 0} \hat{\phi}_n \left( \frac{n}{M} \right) \eta_n = \frac{1}{\nu} + \frac{2}{M \nu} \sum_{n=1}^{\lfloor M\nu/2 \rfloor} \left( 1 - \frac{2n}{M \nu} \right)
\]
\[
= \frac{1}{\nu} + \frac{2}{M \nu} \left( \frac{\lfloor M\nu/2 \rfloor}{2} - \frac{2}{M \nu} \sum_{n=1}^{\lfloor M\nu/2 \rfloor} n \right)
\]
\[
= \frac{1}{\nu} + \frac{2}{M \nu} \left( M\nu/2 + \mathcal{O}(1) - \frac{2}{M \nu} \left( \frac{M^2 \nu^2}{8} + \mathcal{O}(M \nu) \right) \right)
\]
\[
= \frac{1}{\nu} + \frac{1}{2} + \mathcal{O} \left( \frac{1}{M \nu} \right).
\]
Setting $\nu = 1 - \epsilon$ for any $\epsilon > 0$, we have
\[
r_{N,C} \leq \frac{1}{1 - \epsilon} + \frac{1}{2} + \mathcal{O}_{E,q}(1/N)
\]
meaning that
\[
\limsup_{N \to \infty} r_{N,C} \leq 3/2 + o(1).
\]
If the limit exists, then
\[
r_C \leq 3/2.
\]
We remark that unlike [BF16], we cannot optimize the choice of the test function in order to improve our result as in [ILS99] Appendix A, Corollary 2 since the symmetry is orthogonal. □
Let $\epsilon$ and $\epsilon_D$ be the sign of the functional equation of $L(E, u)$ and $L(E \otimes \chi_D, u)$ respectively. They are both $\pm 1$.

**Lemma 11.2.** The order of the central zero $\text{ord}_{u=1/q} L(E \otimes \chi_D, u)$ is even or odd depending on whether $\epsilon_D = 1$ or $\epsilon_D = -1$ respectively.

**Proof.** Since $L(E, u) \in \mathbb{Z}[u]$, we also have $L(E \otimes \chi_D, u) \in \mathbb{Z}[u]$ because $\chi_D$ is quadratic. The functional equation is then

$$L(E \otimes \chi_D, 1 - q^2 u) = \frac{1}{\epsilon_D(1 - q^2u)^M} L(E \otimes \chi_D, u)$$

where $M$ is the number of zeros of $L(E \otimes \chi_D, u)$. Applying the functional equation twice shows that $\epsilon_D = \pm 1$.

If $(1/q) e^{i \theta_j}$ is a zero of $L(E \otimes \chi_D, u)$, then $(1/q) e^{-i \theta_j}$ is also a zero by the functional equation. This means all zeros come in pairs except those at $u = -1/q$ and $u = 1/q$. We have

$$\epsilon_D = \prod_{i=1}^{M} (-e^{i \theta_j}) = (-1)^M (-1)^{\text{ord}_{u=-1/q} L(E \otimes \chi_D, u)}$$

So for example if $\epsilon_D = 1$ and $M$ is even, then $\text{ord}_{u=-1/q} L(E \otimes \chi_D, u)$ must be even and $\text{ord}_{u=1/q} L(E \otimes \chi_D, u)$ must be even too. The argument is the same for the other cases. $\square$

**Theorem 11.3.** At least 12.5% of the family of quadratic twists of an elliptic curve have rank zero and at least 37.5% have rank one as $N \to \infty$.

**Proof.** By (1.2) [BFKRG19]

$$\epsilon_D = \alpha \cdot \epsilon \cdot \chi_{M_E}(D)$$

for $D \in \mathcal{H}_N$ where $M_E$ is the product of the primes of multiplicative reduction of $E$, $\alpha = \pm 1$ depending only on the degree of $D$, and $\chi_{M_E}$ is the unique quadratic Dirichlet character of conductor $M_E$. We recall that we assume $M_E \neq 1$. Since $\chi_{M_E}$ is periodic modulo $M_E$ and since $M_E \mid N_E$, we have that $\chi_{M_E}$ is constant on $\mathcal{H}_{N,C}$.

We recall that we split $\mathcal{H}_N = \mathcal{H}_{N,+} \cup \mathcal{H}_{N,-}$ depending on if $\epsilon_D = 1$ or $\epsilon_D = -1$ respectively.

Let $\chi_{N_E}(D) := 1_{(D, N_E)=1} \chi_{M_E}(D)$, which is a Dirichlet character modulo $N_E$ since $M_E \mid N_E$. We have $\chi_{N_E} = \chi_{M_E}$ on $\mathcal{H}_N^*$ since all elements are coprime to $N_E$. By Lemma 6.2, $\mathcal{H}_N^*$ becomes equidistributed modulo $N_E$ as $N$ grows, and since $\chi_{N_E} = 1$ on half of $\left(\mathbb{F}_q[t]/(N_E)\right)^*$ and $\chi_{N_E} = -1$ on the other half, we have

$$(11.1) \quad |\mathcal{H}_{N,+}| \sim |\mathcal{H}_{N,-}| \sim \frac{|\mathcal{H}_N|}{2} \quad \text{as } N \to \infty.$$ 

By Theorem 11.1, assuming all limits exist, the average analytic rank is $\leq 3/2$ for both $\mathcal{H}_{N,+}$ and $\mathcal{H}_{N,-}$, since both sets are disjoint unions of congruence classes modulo $N_E$. Then, by Lemma 11.2, the rank must be zero for at least 25% of the twists of $\mathcal{H}_{N,+}$, and for $\mathcal{H}_{N,-}$, the rank must be one for at least 75% of the twists in order to satisfy the bound as $N \to \infty$. We must divide these quantities by two to conclude. $\square$

**Remark 1.** We have the relation

$$\epsilon_D = (-1)^M \det \Theta_D = (-1)^{\text{deg}(N_E)} \det \Theta_D$$

where $M$ is the number of zeros of $L(E \otimes \chi_D, u)$. When $\text{deg}(N_E)$ is even, the matrices $\Theta_D$ with $D \in \mathcal{H}_{N,+}$ lie in $\text{SO}(M)$ and the matrices $\Theta_D$ with $D \in \mathcal{H}_{N,-}$ lie in $\text{O}(M) \setminus \text{SO}(M)$. Since $M$ is even, the twists from $\mathcal{H}_{N,+}$ have $\text{SO}(\text{even})$ symmetry, and the twists from $\mathcal{H}_{N,-}$ have $\text{SO}(\text{odd})$ symmetry.

When $\text{deg}(N_E)$ is odd, the matrices $\Theta_D$ with $D \in \mathcal{H}_{N,-}$ lie in $\text{SO}(M)$ and the matrices $\Theta_D$ with $D \in \mathcal{H}_{N,+}$ lie in $\text{O}(M) \setminus \text{SO}(M)$. Since $M$ is odd, the twists from $\mathcal{H}_{N,-}$ have $\text{SO}(\text{odd})$ symmetry, and the twists from $\mathcal{H}_{N,+}$ have $\text{SO}(\text{even})$ symmetry.

By (11.1), the twists from $\mathcal{H}_N$ have orthogonal symmetry. See (6) [You04] for a table of statistics of
Remark 2. The Katz and Sarnak philosophy predicts that Corollary 10.1 should hold without any restriction on the support of $\hat{\varphi}$. However, it is important to integrate over the appropriate symmetry group, since it matters when the support of $\hat{\varphi}$ is greater than $(-1, 1)$. Then, we expect the average analytic rank of the family of twists from $H_N^*$ to be $1/2$. For the family of twists from $H_{N,+}$, we expect an average analytic rank of zero, and for $H_{N,-}$ we expect an average of one. In other words, we expect half of the twists from $H_N^*$ to have rank zero, and the other half to have rank one.

Remark 3. The contribution of the primes can be trivially bounded using the Riemann hypothesis (Proposition 4.1)

$$S(N, n) := \sum_{D \in H_N^*} \sum_{\deg(P) = n} (n/d)(\alpha_P + \sigma_P)\chi_D(P) = \mathcal{O}_{E,q}(Nq^{n+N}).$$

The analogue of Hypothesis M from [Fio14] is

$$S(N, n) = o_{E,q}(q^{n+N}).$$

This bound implies that the contribution of the primes goes to zero as $N \to \infty$ for any $n$, which is what we need to remove the restriction on the support of $\hat{\varphi}$ and to show that the average analytic rank is $1/2$.

12. TRIVIAL BOUND FOR ARBITRARY ORDER

We now study the one-level density when the order $\ell \neq 2$ of the Dirichlet characters is coprime to $q$. Using the Lindelöf hypothesis, we obtain the following restriction on the support of the Fourier transform of the test functions

$$\text{supp} \hat{\varphi} \subset \left(-\frac{1}{2}, 1\right).$$

This is the analogue of $\text{supp} \hat{\varphi} \subset (-1, 1)$ for cubic Dirichlet $L$-functions. It is not clear how to use duality to extend the support in this case, as was done for quadratic characters. By restricting to a subfamily (of density zero), David and Gülöglü [DG20] were able to increase the support for cubic Dirichlet $L$-functions over $\mathbb{Q}(\zeta_3)$.

**Theorem 12.1.** For $\varphi \in \mathcal{S}(\mathbb{R})$ an even function such that $\text{supp}(\hat{\varphi}) \subset (-1/2, 1/2)$, we have for the one-level density of the family of twists of order $\ell \neq 2$ and $(\ell, q) = 1$

$$\langle Z_{\varphi} \rangle_{N,C} = \int_{U(M)} Z_{\varphi}(\Theta)d\Theta + \mathcal{O}_{E,q,\ell}(1/N)$$

where $M = 2N + \deg(N_E) - 4$.

**Proof.** Let $a > 1$ be a divisor of $\ell$ and let $k$ be the smallest integer such that $a \mid q^k - 1$, so $k$ depends on $a$. We fix an isomorphism $\psi$ from the $a$-roots of unity in $\mathbb{F}_{q^k}$ to those in $\mathbb{C}$ and we define the $a$-power residue symbol as

$$\left(\frac{A}{q}\right)_a := \psi\left(A^{\frac{\deg(q)}{a} - 1}\mod q\right)$$

for $A, q \in \mathbb{F}_{q^k}[t]$ where $q$ is prime. If $q \mid A$, the symbol equals zero by definition. This symbol is a Dirichlet character of modulus $q$ of order $a$ over $\mathbb{F}_{q^k}$. Let $\text{Frob}_q$ act on $\mathbb{F}_{q^k}[t]$ by raising each coefficient to the $q$th power. On $\mathbb{F}_{q^k} \subset \mathbb{F}_{q^k}[t]$, this operator permutes the $a$-roots of unity and can be associated via $\psi$ to some $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})$ which generates a normal cyclic subgroup $H \leq \text{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})$ of order $k$. Furthermore, we have

$$\left(\frac{\text{Frob}_q(A)}{\text{Frob}_q(q)}\right)_a = \sigma \left(\frac{A}{q}\right)_a.$$

Now, over $\mathbb{F}_{q^k}[t]$, a prime modulus has primitive Dirichlet characters of order $a$ if and only if its degree is divisible by $k$. In other words, the modulus must split totally in the extension $\mathbb{F}_{q^k}[t]$. Moduli of prime powers $\geq 2$ do not have primitive characters of order $a$. For each prime $Q$ such that $k \mid \deg(Q)$, we define $\chi_{a,Q,i}$ for $1 \leq i \leq \phi(a)$ to be the collection of characters of order $a$ with conductor $Q$, and they are
Gal\((\mathbb{Q}(\zeta_n)/\mathbb{Q})\) conjugates. We extend this definition to composite conductors by multiplicativity. In the following generating series, we consider all primitive characters of order \(a \mid \ell\) of conductor of degree \(h\) for \(a > 1\). In the Euler product, we include for each prime all of its possible characters of order \(a > 1\) dividing \(\ell\). Let \(|u| = q^{-1/2-\epsilon}\) for any \(\epsilon > 0\). We have

\[
\mathcal{L}_P(u) := \sum_{h=0}^{\infty} \left( \sum_{\substack{\chi \text{ of order } a|\ell \text{ primitive} \\ \deg(\text{cond}(\chi)) = h \\ \text{cond}(\chi), N_E = 1 \\ a > 1}} \chi(P) \right) u^h
\]

\[
= \prod_{Q \text{ prime}} \prod_{Q|N_E} \left( 1 + \sum_{a|\ell \atop a > 1} \sum_{i=1}^{\phi(a)} \chi_{a, Q, i}(P) u^{\deg(Q)} \right)^{-1}
\]

The error comes from the fact that the terms \(u^j \deg(Q)\) with \(j \geq 2\) in the product are negligible over \(C_\epsilon : |u| = q^{-1/2-\epsilon}\), since there are at most \(q^m\) primes of degree \(m\) and the sum

\[
\sum_{m=1}^{\infty} q^m q^{-(1-2\epsilon)m}
\]

converges absolutely. We also have

\[
\prod_{Q \text{ prime}} \prod_{Q|N_E} \left( 1 + \sum_{a|\ell \atop a > 1} \sum_{i=1}^{\phi(a)} \chi_{a, Q, i}(P) u^{\deg(Q)} \right)^{-1} \ll_{E, \ell, q} 1
\]

over \(C_\epsilon\). Now, we fix \(a > 1\) dividing \(\ell\) and we collect the primes \(Q\) having characters of order \(a\). Let \(k\) be the smallest integer such that \(a \mid q^k - 1\). When we write “\(q\) totally split” under the product, we mean that the prime in \(\mathbb{F}_q[t]\) under \(q\) splits completely in \(\mathbb{F}_{q^k}[t]\). We have

\[
\prod_{Q \text{ prime}} \prod_{Q|N_E} \left( 1 + \sum_{a|\ell \atop a > 1} \sum_{i=1}^{\phi(a)} \chi_{a, Q, i}(P) u^{\deg(Q)} \right)^{-1} \ll_{E, \ell, q} 1
\]

by defining

\[
\chi_{a, q, i}(A) := \sigma_i \left( \frac{A}{q^k} \right)_a
\]

where the \(\sigma_i\) are a set of representatives of \(\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/H\) where \(H\) was defined above. Since \(\text{Frob}_q(P) = P\), and since a character of conductor \(q\) of order \(a\) over \(\mathbb{F}_{q^k}[t]\) restricted to \(\mathbb{F}_q[t]\) gives a character of conductor \(Q\) of order \(a\) over \(\mathbb{F}_q[t]\), we have a one-to-one correspondence between these characters. By the \(a\)-power
reciprocity law ([Ros13] Theorem 3.5)

\[
\prod_{\substack{q \in \mathbb{F}_q[t] \\
q \text{ prime}}}(1 - \chi_{a,q,i}(P)u^{k\deg(q)})^{-1} = L_q^+(\chi_{a,P,i}, (-1)^{\frac{k-1}{2}\deg(P)}u^{k}) \quad \prod_{\substack{q \in \mathbb{F}_q[t] \\
q \text{ prime}}}(1 - \chi_{a,q,i}(P)u^{k\deg(q)})
\]

where the index \(q^k\) indicates that the L-function is taken over \(\mathbb{F}_q[t]\). When \(q\) is not totally split, we have \(k \deg(q) \geq 2 \deg(Q)\), so the last product converges absolutely on \(C_{\epsilon}\) since the number of primes above a given prime \(Q\) is bounded by \(\ell\). Finally, by the Lindelöf hypothesis ([DFL19] Lemma 2.6), we have for any \(\delta > 0\)

\[
L_q^+(\chi_{a,P,i}, u^k) \ll_{\epsilon, \delta} q^{\delta \deg(P)} \quad \text{for } |u| \leq q^{-1/2}.
\]

Combining everything gives

\[
\mathcal{L}_P(u) \ll_{\epsilon, \delta, \epsilon, \ell} q^{\delta \deg(P)}
\]
on \(C_{\epsilon}\). We now apply Perron’s formula

\[
\sum_{\substack{\chi \text{ of order } a|\ell \\
\chi \text{ primitive} \\
\deg(\text{cond}(\chi))=h \\
(\text{cond}(\chi),N_E)=1 \\
a>1}} \chi(P) = \frac{1}{2\pi i} \oint_{C_{\epsilon}} \frac{\mathcal{L}_P(u)}{u^{h}} \frac{du}{u}.
\]

Since \(\mathcal{L}_P(u)\) is entire inside \(C_{\epsilon}\) and since \(|1/u^{h+1}| \leq q^{(1/2+\epsilon)h+1}\), we have

\[
\sum_{\substack{\chi \text{ of order } a|\ell \\
\chi \text{ primitive} \\
\deg(\text{cond}(\chi))=h \\
(\text{cond}(\chi),N_E)=1 \\
a>1}} \chi(P) \ll_{\epsilon, \delta, \epsilon, \ell} q^{h/2}q^{\epsilon h}q^{\delta \deg(P)}
\]

for any \(\epsilon, \delta > 0\). Since this holds for any \(\ell\), we may isolate the characters of order \(\ell\)

\[
\sum_{\substack{\chi \text{ of order } \ell \\
\chi \text{ primitive} \\
\deg(\text{cond}(\chi))=h \\
(\text{cond}(\chi),N_E)=1}} \chi(P) \ll_{\epsilon, \delta, \epsilon, \ell} q^{h/2}q^{\epsilon h}q^{\delta \deg(P)}.
\]

As in the quadratic case, the average of traces is given by

\[
\langle \text{tr } \Theta^n \rangle_N = \frac{1}{q^n|\mathcal{F}_N|} \sum_{d|n} \sum_{\deg(P)=n/d} (n/d)(\alpha_P^d + \overline{\alpha}_P^d) \sum_{\substack{\chi \text{ order } \ell \\
\chi \text{ primitive} \\
\deg(\text{cond}(\chi))=N \\
(\text{cond}(\chi),N_E)=1}} \chi^d(P)
\]

where \(\mathcal{F}_N\) denotes the family of primitive twists of order \(\ell\) of conductor of degree \(N\) coprime to \(N_E\). Using \(|\mathcal{F}_N| \propto q^N\) and the above, we have

\[
\langle \text{tr } \Theta^n \rangle_N \ll_{\epsilon, \ell} n^2q^{n/2} - N^2q^{\epsilon(n+N)}
\]
since \(\chi^2\) isn’t principal and higher powers are trivially bounded. This translates to a restriction of \((-1/2, 1/2)\) on the support of the test function for the one-level density. The symmetry is unitary since there is no contribution. \(\square\)

**Remark.** In this section, the number of zeros of the L-functions do not depend on the parity of the characters. However, if we were to remove the elliptic curve, the genus would change depending on the parity of the characters for conductors of fixed degree. See [DFL19] Lemma 2.9 for example. We can control the parity of the characters here by fixing \(s := (\ell, q - 1)\) and \(\chi\) a character of order \(s\) on \(\mathbb{F}_q^*\). The indexing of the collection \(\{\chi_{a,Q,i}\}_{1 \leq i \leq \phi(a)}\) of characters over \(\mathbb{F}_q^*[t]\) described above is now important. We set \(\chi_{a,Q,1}\) to be any character from the collection such that it is equal to \(\tilde{\chi}^{t_n, \deg(Q)}\) when restricted to \(\mathbb{F}_q^*\) where
\(t_a = (\ell, q - 1)/(a, q - 1)\). Then, we set the other characters as \(\chi_{a,Q,i} := \chi_{a,Q,1}\) where \(b_{a,i}\) is the \(i\)th element of \((\mathbb{Z}/a\mathbb{Z})^*\). To keep track of the values of the characters over \(\mathbb{F}_q^*\), we modify the Euler product as

\[
\prod_{Q \text{ prime} \mod N_E} \left(1 + \sum_{a|Q} \sum_{i=1}^{\phi(a)} \chi_{a,Q,i}(P) \zeta_{s}^{rta_{b_{a,i}} \deg(Q)} q^{\deg(Q)} \right)
\]

where \(\zeta_s\) is the \(s\)th complex root of unity and \(0 \leq r \leq s - 1\). Doing so will change the \(L\)-function obtained above as

\[
L_{q^h}(\chi_{a:P,i}, (-1)^{\frac{a^h-1}{a}} q^{\deg(P)} (\zeta_s q_{s}^{rb_{a:i}} q^{\deg(P)})
\]

so it doesn’t change the bound we obtained

\[
\sum_{\chi \text{ of order } \ell \mod \chi \text{ primitive } \deg(\text{cond}(\chi)) = h \mod (\text{cond}(\chi), N_E) = 1} \chi(P) q^{rb(\chi)} \ll q^{\delta/2} q^{h \delta} q^{\deg(P)}
\]

where \(0 \leq b(\chi) \leq s - 1\) is the unique number such that

\[\chi|_{\mathbb{F}_q^*} = \zeta^{b(\chi)}.\]

We can now control the congruence of \(b(\chi)\) modulo \(s\) by summing over all \(r\)

\[
\sum_{\chi \text{ of order } \ell \mod \chi \text{ primitive } \deg(\text{cond}(\chi)) = h \mod (\text{cond}(\chi), N_E) = 1} \chi(P) q^{rb(\chi)}
\]

so the bound also holds for this sum. By denoting the genus by \(g\) and the degree of the conductor by \(h\), we have \(g = h - 1\) if \(\chi\) is odd and \(g = h - 2\) if \(\chi\) is even for Dirichlet \(L\)-functions. We know that \(\chi\) is even if and only if \(b(\chi) \equiv 0 \mod s\), so controlling the congruence gives us control over the genus.

13. Acknowledgments

I would like to thank Chantal David, my doctoral thesis advisor, for the idea of this project, for her support, her help, and the various improvements she suggested. I would also like to thank the Fonds de recherche Nature et technologies du Québec for their financial support.

References

[BCD+16] Alina Bucur, Edgar Costa, Chantal David, João Guerreiro, and David Lowry-Duda. Traces, high powers and one level density for families of curves over finite fields. arXiv e-prints, page arXiv:1610.00164, Oct 2016.

[BF16] Hung M. Bui and Alexandra Florea. Zeros of quadratic Dirichlet \(L\)-functions in the hyperelliptic ensemble. arXiv, 2016.

[BFKR19] H. M. Bui, Alexandra Florea, Jonathan P. Keating, and Edva Roditty-Gershon. Moments of quadratic twists of elliptic curve \(L\)-functions over function fields. arXiv, 2019.

[Bru92] Armand Brumer. The average rank of elliptic curves I. Inventiones mathematicae, 109(1):445–472, Dec 1992.

[CFJ15] Byungchul Cha, Daniel Fiorilli, and Florent Jouve. Independence of the zeros of elliptic curve \(L\)-functions over function fields. arXiv, 2015.

[CP18] Peter J. Cho and Jeongho Park. Low-lying zeros of cubic Dirichlet \(L\)-functions and the ratios conjecture, 2018.

[CP19a] Peter J. Cho and Jeongho Park. Dirichlet characters and low-lying zeros of \(L\)-functions, 2019.

[CP19b] Peter J. Cho and Jeongho Park. n-level densities for twisted cubic Dirichlet \(L\)-functions. Journal of Number Theory, 196:139 – 155, 2019.

[DFL19] Chantal David, Alexandra Florea, and Matilde Lalín. The mean values of cubic \(L\)-functions over function fields. preprint, 2019.

[DFL20] Chantal David, Alexandra Florea, and Matilde Lalín. Non-vanishing for cubic \(L\)-functions, 2020.

[DG20] Chantal David and Ahmet Guloglu. One-level density and non-vanishing for cubic Dirichlet \(L\)-functions over the Eisenstein field, 2020.
[DS94] P. Diaconis and M. Shahshahani. On the eigenvalues of random matrices. *Studies in applied probability. J. Appl. Probab.* 31A, 1994.

[Fio14] Daniel Fiorilli. A conditional determination of the average rank of elliptic curves. 2014.

[Flo15] Alexandra Florea. The second and third moment of $L(\frac{1}{2}, \chi)$ in the hyperelliptic ensemble, 2015.

[Flo16] Alexandra Florea. The fourth moment of quadratic Dirichlet $L$-functions over function fields, 2016.

[Hay66] David Hayes. The expression of a polynomial as a sum of three irreducibles. *Acta Arithmetica*, 11(4):461–488, 1966.

[HB03] D. R. Heath-Brown. The average analytic rank of elliptic curves. *arXiv*, 2003.

[ILS99] Henryk Iwaniec, Wenzhi Luo, and Peter Sarnak. Low lying zeros of families of $L$-functions. *arXiv Mathematics e-prints*, page math/9901141, January 1999.

[KS99] Nicholas M. Katz and Peter Sarnak. Zeroes of zeta functions and symmetry. *Bull. Amer. Math. Soc.*, 36(1):1–26, January 1999.

[Mei15] Patrick Meisner. Distribution of points on cyclic curves over finite fields, 2015.

[Mei17] Patrick Meisner. One level density for cubic galois number fields. 2017.

[Ros13] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2013.

[Rud08] Zeev Rudnick. Traces of high powers of the Frobenius class in the hyperelliptic ensemble. *arXiv*, November 2008.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[Tao19] Terence Tao. A function field analogue of Riemann zeta statistics. *Blog post*, pages https://terrytao.wordpress.com/2019/05/17/a–function–field–analogue–of–riemann–zeta–statistics/, 2019.

[You04] Matthew P. Young. Low-lying zeros of families of elliptic curves. *arXiv*, 2004.