DISTRIBUTION OF ZETA ZEROES OF ARTIN–SCHREIER CURVES

ALINA BUCUR, CHANTAL DAVID, BROOKE FEIGON, MATILDE LALÍN, KANEENIKA SINHA

ABSTRACT. We study the distribution of the zeroes of the zeta functions of the family of Artin-Schreier curves over $\mathbb{F}_q$ when q is fixed and the genus goes to infinity. We consider both the global and the mesoscopic regimes, proving that when the genus goes to infinity, the number of zeroes with angles in a prescribed interval of $[-\pi, \pi)$ has a standard Gaussian distribution (when properly normalized).

1. INTRODUCTION

Recently there has been a great deal of interest in statistics for numbers of rational points on curves over finite fields, where the curve varies in a certain family but is always defined over a fixed finite field. This is in contrast to situations studied using Deligne's equidistribution theorem [Del74], which requires the size of the finite field to go to infinity, and which tends to produce statistics related to random matrices in certain monodromy groups. When one fixes the base field, one instead tends to encounter discrete probabilities, typically sums of independent identically distributed random variables. The first result in this direction is the work of Kurlberg and Rudnick for hyperelliptic curves [KR09]; other cases considered include cyclic p-fold covers of the projective line [BDFL10b, BDFL11] (for a slightly different approach see [Xio10a]), plane curves [BDFL10a], complete intersections in projective spaces [BK], and general trigonal curves [Woo].

The number of rational points on a curve over a finite field is determined by the zeta function, and statistical properties of the number of points may be interpreted as properties of the coefficients of the zeta function. A related but somewhat deeper question is to consider statistical properties of *zeroes* of the zeta function. In the case of hyperelliptic curves, these properties were studied by Faifman and Rudnick [FR10]. A related family was studied in [Xio10b].

In this paper, we make similar considerations for the family of *Artin-Schreier curves*; this family is interesting because the characteristic of the base field plays a more central role in the definition than in any of the other families mentioned so far. For instance, by viewing Artin-Schreier curves as cyclic covers of $\mathbb{P}^1$, one obtains a direct link between their zeta functions and certain exponential sums; while this is also the case for cyclic p-fold covers in characteristics other than p, the Artin-Schreier case admits a much more precise analysis. One example of how to exploit this additional precision is the work of Rojas-Leon and Wan [RLW11] refining the Weil bound for Artin-Schreier curves.

To explain our results in more detail, we introduce some notation. Fix an odd prime p and a finite field $\mathbb{F}_q$ of characteristic p. Each polynomial $f \in \mathbb{F}_q[X]$ whose degree d is not divisible by p defines an Artin-Schreier cover C_f of $\mathbb{P}^1$ with affine model

$$Y^p - Y = f(X). \tag{1}$$

Since f is a polynomial rather than a more general rational function, C_f has p-rank 0. For more details about the structure of the moduli space of Artin-Schreier curves and its p-rank strata, see [PZ11]. As usual, the Weil zeta function of C_f has the form

$$Z_{C_f}(u) = \frac{P_{C_f}(u)}{(1-u)(1-qu)}.$$

Here $P_{C_f}(u)$ is a polynomial of degree $2g = (d-1)(p-1)$ which factors as

Date: March 6, 2013.

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 11M50, 14G15.

Key words and phrases. Artin-Schreier curves, finite fields, distribution of zeroes of L-functions of curves.

$$P_{C_f}(u) = \prod_{\psi \neq 1} L(u, f, \psi), \tag{2}$$

where the product is taken over the non-trivial additive characters ψ of $\mathbb{F}_p$ and $L(u, f, \psi)$ are certain L-functions (see (4) for the formula). Computing the distribution of the zeroes of the zeta functions $Z_{C_f}(u)$ as C_f runs over the $\mathbb{F}_q$-points of the moduli space $\mathcal{AS}_{g,0}$ of Artin-Schreier curves of genus g and p-rank 0 amounts to computing the distribution of the zeroes of $\prod_{j=1}^{p-1} L(u, f, \psi^j)$ for a fixed non-trivial additive character ψ as f runs over polynomials of degree d. In fact, going over each $\mathbb{F}_q$-point of the moduli space $\mathcal{AS}_{g,0}$ once is equivalent to letting f vary over the set $\mathcal{F}'_d$ of polynomials of degree d containing no non-constant terms of degree divisible by p, as such terms can always be eliminated in a unique way without changing the resulting Artin-Schreier curve.

Some statistics for the zeroes in the family of Artin-Schreier curves were considered in the recent work of Entin [Ent], who employs the methods of Kurlberg and Rudnick [KR09] to study the variation of the number of points on such a family, then translates the results into information about zeroes. In the present work, we consider the global and mesoscopic regime, as was done by Faifman and Rudnick [FR10] for the family of hyperelliptic curves.

More precisely, we write

$$L(u, f, \psi) = \prod_{j=1}^{d-1} (1 - \alpha_j(f, \psi)u), \tag{3}$$

where $\alpha_j(f, \psi) = \sqrt{q} e^{2\pi i \theta_j(f,\psi)}$ and $\theta_j(f, \psi) \in [-1/2, 1/2)$. We study the statistics of the set of angles $\{\theta_j(f, \psi)\}$ as f varies. For an interval $\mathcal{I} \subset [-1/2, 1/2)$, let

$$N_{\mathcal{I}}(f, \psi) := \#\{1 \leq j \leq d-1 : \theta_j(f, \psi) \in \mathcal{I}\},$$

$$N_{\mathcal{I}}(f, \psi, \bar{\psi}) := N_{\mathcal{I}}(f, \psi) + N_{\mathcal{I}}(f, \bar{\psi}),$$

and

$$N_{\mathcal{I}}(C_f) := \sum_{j=1}^{p-1} N_{\mathcal{I}}(f, \psi^j).$$

We show that the number of zeroes with angle in a prescribed interval is asymptotic to $2g|\mathcal{I}|$ (Theorem 4.2), has variance asymptotic to $\left(2(p-1)/\pi^2\right) \log(g|\mathcal{I}|)$ and properly normalized has a Gaussian distribution.

Theorem 1.1. *Fix a finite field $\mathbb{F}_q$ of characteristic p. Let $\mathcal{F}'_d$ be the family of polynomials defined above. Then for any real numbers $a < b$ and $|\mathcal{I}|$ either fixed or $|\mathcal{I}| \to 0$ while $d|\mathcal{I}| \to \infty$,*

$$\lim_{d \to \infty} \mathrm{Prob}_{\mathcal{F}'_d} \left(a < \frac{N_{\mathcal{I}}(C_f) - (d-1)(p-1)|\mathcal{I}|}{\sqrt{\frac{2(p-1)}{\pi^2} \log(d|\mathcal{I}|)}} < b \right) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-x^2/2} dx.$$

As noted earlier, this result can also be stated in terms of the $\mathbb{F}_q$-points of $\mathcal{AS}_{g,0}$.

Corollary 1.2. *Fix a finite field $\mathbb{F}_q$ of characteristic p. Then for any real numbers $a < b$ and $|\mathcal{I}|$ either fixed or $|\mathcal{I}| \to 0$ while $g|\mathcal{I}| \to \infty$,*

$$\lim_{g \to \infty} \mathrm{Prob}_{\mathcal{AS}_{g,0}(\mathbb{F}_q)} \left(a < \frac{N_{\mathcal{I}}(C_f) - 2g|\mathcal{I}|}{\sqrt{\frac{2(p-1)}{\pi^2} \log\left(g|\mathcal{I}|\right)}} < b \right) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-x^2/2} dx.$$

Theorem 1.1 is obtained by computing the normalized moments of certain approximations of $N_{\mathcal{I}}(C_f) - (p-1)(d-1)|\mathcal{I}|$ given by Beurling-Selberg polynomials to verify that they fit the Gaussian moments. Our results are compatible with the following result for the distribution of zeroes of the L-functions $L(u, f, \psi)$ and $L(u, f, \bar{\psi})$.

Proposition 1.3. *Fix a finite field $\mathbb{F}_q$ of characteristic p. Then for any real numbers $a < b$ and $|\mathcal{I}|$ either fixed or $|\mathcal{I}| \to 0$ while $d|\mathcal{I}| \to \infty$,*

$$\lim_{d\to\infty} \mathrm{Prob}_{\mathcal{F}'_d}\left(a < \frac{N_{\mathcal{I}}(f,\psi,\bar{\psi}) - 2(d-1)|\mathcal{I}|}{\sqrt{\frac{4}{\pi^2}\log(d|\mathcal{I}|)}} < b\right) = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-x^2/2}dx.$$

We remark that this result is compatible with the philosophy of Katz and Sarnak, which predicts that when $q \to \infty$, the distribution of $N_{\mathcal{I}}(C_f)$ is the same as the distribution of $\hat{N}_{\mathcal{I}}(U)$, the number of eigenvalues of a $2g \times 2g$ matrix U in the monodromy group of C_f chosen uniformly at random with respect to the Haar measure. The monodromy groups of Artin-Schreier curves are computed by Katz in [Kat87, Kat90]. In the large matrix limit, which corresponds to the limit as $d \to \infty$ for the family of Artin-Schreier curves because $g = (p-1)(d-1)/2$, the statistics on $\hat{N}_{\mathcal{I}}(U)$ have been found to have Gaussian fluctuations in various ensembles of random matrices.

1.1. **Outline of the article.** This article is set up as follows. We begin by reviewing basic Artin-Schreier theory in Section 2. In Section 3 we prove two explicit formulas for the zeroes of $L(u, f, \psi)$ which we will need later to compute the moments. In Section 4 we prove a result about the number of zeroes of the zeta function for a fixed Artin-Schreier cover of $\mathbb{P}^1$. In Section 5 we recall some facts on Beurling-Selberg polynomials and use them to prove some technical statements about their coefficients. A certain sum of these trigonometric polynomials approximate the characteristic function of the interval $\mathcal{I}$. We use the explicit formula to reduce the problem of studying this sum of Beurling-Selberg polynomials to a problem about sums of characters of traces of a polynomial f evaluated at elements in extensions of $\mathbb{F}_q$. In Sections 6, 7 and 8 we analyze the first, second and third moments of this sum. These moments tell us the expectation and variance of the distribution. In Section 9 we compute the general moments of our approximating function and conclude that it has a standard Gaussian limiting distribution as the degree d of f goes to infinity for $\mathcal{I}$ either fixed or in the mesoscopic regime. Finally, in Section 10 we conclude the proof of Theorem 1.1 by proving that under normalization $N_{\mathcal{I}}(C_f) - (d-1)(p-1)|\mathcal{I}|$ converges in mean square and hence distribution to our approximating function.

1.2. **Acknowledgments.** The authors would like to thank Zeév Rudnick for many useful discussions while preparing this paper. The authors are also grateful to Andrew Granville and Rachel Pries for helpful conversations related to this work. The first, third and fifth named authors thank the Centre de Recherche Mathématique (CRM) and the Mathematical Sciences Research Institute (MSRI) for their hospitality.

2. Basic Artin-Schreier theory

We now recall some more facts about Artin-Schreier curves. For each integer $n \geq 1$, denote by $\mathrm{tr}_n : \mathbb{F}_{q^n} \to \mathbb{F}_p$ the absolute trace map (not the trace to $\mathbb{F}_q$). For each polynomial $g \in \mathbb{F}_q[X]$ and non-trivial additive character ψ of $\mathbb{F}_p$, set

$$S_n(g,\psi) = \sum_{x\in\mathbb{F}_{q^n}} \psi(\mathrm{tr}_n(g(x))).$$

The L-functions that appear in (2) are given by

$$L(u,f,\psi) = \exp\left(\sum_{n=1}^{\infty} S_n(f,\psi)\frac{u^n}{n}\right) = \prod_P \left(1-\psi_f(P)u^{\deg P}\right)^{-1}, \tag{4}$$

where the product is taken over monic irreducible polynomials in $\mathbb{F}_q[X]$. In fact, throughout this paper P will denote such a polynomial and, if $n = \deg P$ we have

$$\psi_f(P) = \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ P(\alpha)=0}} \psi(f(\alpha)) = \psi(\mathrm{tr}_n(f(\alpha))) \text{ for any root } \alpha \text{ of } P.$$

To see that the exponential is equal to the product over primes in (4), one has to write the exponential as an Euler product over the closed points of $\mathbb{A}^1$. Namely, if we denote by $\mathcal{S}_n$ the set of closed points of $\mathbb{A}^1$ of

degree n, we can write

$$\begin{aligned} L(u,f,\psi) &= \exp\left(\sum_{n=1}^{\infty} S_n(f,\psi)\frac{u^n}{n}\right) \\ &= \exp\left(\sum_{n=1}^{\infty}\sum_{x\in\mathcal{S}_n}\sum_{k=1}^{\infty}\psi(\mathrm{tr}_{kn}(f(x)))\frac{u^{kn}}{k}\right). \end{aligned}$$

The denominator of the fraction is k, not kn, because each closed point $x \in \mathcal{S}_n$ produces n rational points of $\mathbb{F}_{q^n}$. Thus,

$$\begin{aligned} L(u,f,\psi) &= \prod_{n=1}^{\infty}\prod_{x\in\mathcal{S}_n}\exp\left(\sum_{k=1}^{\infty}\frac{\left(\psi(\mathrm{tr}_n(f(x)))u^n\right)^k}{k}\right) \\ &= \prod_{n=1}^{\infty}\prod_{x\in\mathcal{S}_n}(1-\psi(\mathrm{tr}_n(f(x)))u^n)^{-1} \\ &= \prod_{x \text{ closed point of } \mathbb{A}^1}(1-\psi(\mathrm{tr}_{\deg x}(f(x)))u^{\deg x})^{-1}, \end{aligned}$$

which is exactly the product over primes that appears in (4).

Note that for the trivial character $\psi = 1$, the same formula gives

$$L(u,f,1) = Z_{\mathbb{A}^1}(u) = \frac{1}{1-qu}.$$

The factor at infinity is then given by

$$\psi_f(\infty) = \begin{cases} 1 & \psi = 1, \\ 0 & \psi \neq 1. \end{cases}$$

Therefore we have

$$Z_{C_f}(u) = \prod_{\psi} L^*(u,f,\psi),$$

where $L^*(u,f,\psi)$ are the completed L-functions,

$$L^*(u,f,\psi) = \prod_v \left(1-\psi_f(P_v)u^{\deg P_v}\right)^{-1}.$$

Here the product is taken over all places v of $\mathbb{F}_q(X)$.

From now on we will fix a non-trivial additive character ψ of $\mathbb{F}_p$ given by a certain choice ζ of a primitive pth root of unity in $\mathbb{C}$. Then, all the other non-trivial characters of $\mathbb{F}_p$ are of the form $\sigma \circ \psi$ where σ is an automorphism of the cyclotomic field $\mathbb{Q}(\zeta)$. The reciprocals of zeroes of the $L(u,f,\sigma\circ\psi)$ are exactly the Galois conjugates $\sigma(\alpha_j(f,\psi))$, $1 \le j \le d-1$, of the reciprocals of the roots of $L(u,f,\psi)$. In order to compute the distribution of the zeroes of the Weil zeta functions Z_{C_f} as C_f runs over $\mathcal{AS}_{g,0}(\mathbb{F}_q)$ we are going to compute the distribution of the angles $\theta_j(f,\psi), \theta_j(f,\bar{\psi}), 1 \le j \le d-1$, for our specific choice of the additive character ψ, as f runs through $\mathcal{F}'_d$, where $g = (d-1)(p-1)/2$. Since the roots of $L(u,f,\psi)$ and $L(u,f,\bar{\psi})$ are conjugate, it suffices to work with symmetric intervals. The distribution of the roots of the whole zeta function is then obtained by combining the $(p-1)/2$ distributions for the various choices of ψ.

As discussed in the introduction, we will consider $\mathbb{F}_q$-points of the moduli space $\mathcal{AS}_{g,0}$ of Artin-Schreier curves of p-rank 0. That means that we need to consider, up to $\mathbb{F}_q$-isomorphism, curves with affine model $C_f : Y^p - Y = f(X)$ with $f(X)$ a polynomial of degree $d = 2g/(p-1)+1$ not divisible by p.

Using the $\mathbb{F}_q$-isomorphism $(X,Y) \mapsto (X, Y + aX^k)$, we get that C_f is isomorphic to C_g where $g(X) = f(X) + aX^k - a^pX^{kp}$. By using this isomorphism, we are reduced to considering the Artin-Schreier curves with model $C_f : Y^p - Y = f(X)$ where $f(X)$ is an element of the family $\mathcal{F}'_d$ defined in the introduction as

$$\mathcal{F}'_d = \left\{ a_dX^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{F}_q[X] : a_d \in \mathbb{F}_q^*, a_{pk} = 0, 1 \le k \le \left\lfloor \frac{d}{p} \right\rfloor \right\}. \tag{5}$$

Except for the isomorphisms described above, no two such affine models are isomorphic, and then considering all affine models $Y^p - Y = f(X)$ with $f(X) \in \mathcal{F}'_d$ is equivalent to considering all the points of $\mathcal{AS}_{g,0}(\mathbb{F}_q)$. Again, we refer the reader to [PZ11] for more details on the moduli space of Artin-Schreier curves.

In [Ent], the author is considering a slightly different family by also allowing twists, i.e. isomorphism over $\mathbb{F}_{q^p}$. This amounts to the models $C_f : Y^p - Y = f(X)$, with $f(X) \in \mathcal{F}''_d$, where

$$\mathcal{F}''_d = \left\{ a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 \in \mathbb{F}_q[X] : a_d \in \mathbb{F}_q^*, a_{pk} = 0, 0 \le k \le \left\lfloor \frac{d}{p} \right\rfloor \right\}.$$

Finally, we will denote by

$$\mathcal{F}_d = \left\{ a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 \in \mathbb{F}_q[X] : a_d \in \mathbb{F}_q^* \right\},$$

the set of all polynomials of degree d in $\mathbb{F}_q[X]$. We will also need the map $\mu : \mathcal{F}_d \to \mathcal{F}'_d$ defined by

$$\mu\left(\sum_{i=0}^{d} a_i X^i \right) = a_0 + \sum_{\substack{i=1 \\ i \neq kp, k \ge 1}}^{d} \left(\sum_{j=0}^{\lfloor \log_p(d/i) \rfloor} a_{ip^j}^{p^{-j}} \right) X^i. \tag{6}$$

This map is $q^{\lfloor \frac{d}{p} \rfloor}$-to-one and preserves the trace of $f(\alpha)$, which will allow us to work with $\mathcal{F}_d$ instead of $\mathcal{F}'_d$ when taking averages.

2.1. **Remark on the number of points.** For d large enough, the elements of $\mathcal{F}'_d$ have the same chance as any random polynomial of degree d in $\mathbb{F}_q[X]$ to take a given value in some extension of $\mathbb{F}_q$. Thus, if $p \nmid n$, as soon as $d - \lfloor d/p \rfloor > q^n$, the distribution of $\{\#C_f(\mathbb{F}_{q^n}); f \in \mathcal{F}'_d\}$ is given by a sum of i.i.d. random variables, one variable for each closed point of $\mathbb{P}^1$ of degree $e \mid n$. As long as we stay away from the point at infinity where $f(X)$ has a pole, the fiber above each closed point x of $\mathbb{P}^1$ contains pe rational points on the Artin-Schreier cover C_f if x happens to be in the kernel of the absolute trace map $\mathrm{tr}_n : \mathbb{F}_{q^n} \to \mathbb{F}_p$, and no points otherwise. Hence each random variable in the sum takes the value pe with probability $1/p$ and 0 with probability $1 - 1/p$. The average number of points is then $1 + q^n$, the constant 1 coming from the point at infinity where the polynomial $f(X)$ has a pole and the fiber above it contains just 1 point.

If $p \mid n$, the average is higher because there are certain points of $\mathbb{P}^1$ of degree e for which the fiber is forced to have pe points (i.e. the points of degree $e \mid \frac{n}{p}$). One adjusts the computation accordingly and obtains that the average number in $C_f(\mathbb{F}_{q^n})$ is now $1 + q^n + (p-1)q^{n/p}$. This is the essential reason behind Entin's result on the matter [Ent, Theorem 4], except that his count does not take into account the point at infinity.

3. Explicit Formulas

Let K be a positive integer, $e(\theta) = e^{2\pi i \theta}$ and let $h(\theta) = \sum_{|k| \le K} a_k e(k\theta)$ be a trigonometric polynomial. Then the coefficients a_k are given by the Fourier transform

$$a_k = \widehat{h}(k) = \int_{-1/2}^{1/2} h(\theta) e(-k\theta) d\theta.$$

We prove in this section two explicit formulas for $L(u, f, \psi)$, written as an exponential of a sum or as a product over primes as in (4). The first explicit formula (Lemma 3.1) will be used to compute the moments over the family $\mathcal{F}'_d$, and the second explicit formula (Lemma 3.2) will be used to prove a result about the number of zeroes for a fixed C_f (see Section 4).

Lemma 3.1. *Let $h(\theta) = \sum_{|k| \le K} \widehat{h}(k) e(k\theta)$ be a trigonometric polynomial. Let $\theta_j(f, \psi)$ be the eigenangles of the L-function $L(u, f, \psi)$. Then we have*

$$\sum_{j=1}^{d-1} h(\theta_j(f, \psi)) = (d-1)\widehat{h}(0) - \sum_{k=1}^{K} \frac{\widehat{h}(k) S_k(f, \psi) + \widehat{h}(-k) S_k(f, \overline{\psi})}{q^{k/2}}. \tag{7}$$

Proof. Recall from above that

$$L(u, f, \psi) = \exp\left(\sum_{n=1}^{\infty} S_n(f, \psi) \frac{u^n}{n} \right) = \prod_{j=1}^{d-1} (1 - \alpha_j(f, \psi) u).$$

Taking logarithmic derivatives, we have

$$\frac{d}{du}\sum_{j=1}^{d-1}\log(1-\alpha_j(f,\psi)u) = \frac{d}{du}\sum_{n=1}^{\infty} S_n(f,\psi)\frac{u^n}{n}.$$

Multiplying both sides by u, we get

$$\sum_{j=1}^{d-1}\frac{-\alpha_j(f,\psi)u}{1-\alpha_j(f,\psi)u} = \sum_{n=1}^{\infty} S_n(f,\psi)u^n,$$

that is,

$$-\sum_{j=1}^{d-1}\sum_{n=1}^{\infty}(\alpha_j(f,\psi)u)^n = \sum_{n=1}^{\infty} S_n(f,\psi)u^n.$$

Comparing coefficients,

$$-\sum_{j=1}^{d-1}(\alpha_j(f,\psi))^n = S_n(f,\psi).$$

Thus, for $n>0$, we get

$$-\sum_{j=1}^{d-1} e^{2\pi i n\theta_j(f,\psi)} = \frac{S_n(f,\psi)}{q^{n/2}}. \tag{8}$$

For $n<0$, taking complex conjugates, we have by (3) and (8)

$$\begin{aligned}-\sum_{j=1}^{d-1} e^{2\pi i n\theta_j(f,\psi)} &= \overline{-\sum_{j=1}^{d-1} e^{2\pi i|n|\theta_j(f,\psi)}} = \overline{-\sum_{j=1}^{d-1}\frac{\alpha_j(f,\psi)^{|n|}}{q^{|n|/2}}}\\ &= \overline{\frac{S_{|n|}(f,\psi)}{q^{|n|/2}}} = \frac{S_{|n|}(f,\overline{\psi})}{q^{|n|/2}} = \frac{S_{|n|}(f,\psi^{-1})}{q^{|n|/2}}.\end{aligned}$$

Thus,

$$\begin{aligned}\sum_{j=0}^{d-1} h(\theta_j(f,\psi)) &= \sum_{j=1}^{d-1}\sum_{k=-K}^{K}\widehat{h}(k)e(k\theta_j(f,\psi))\\ &= (d-1)\widehat{h}(0) + \sum_{j=1}^{d-1}\sum_{k=1}^{K}\widehat{h}(k)e(k\theta_j(f,\psi)) + \sum_{j=1}^{d-1}\sum_{k=-K}^{-1}\widehat{h}(k)e(k\theta_j(f,\psi))\\ &= (d-1)\widehat{h}(0) - \sum_{k=1}^{K}\widehat{h}(k)\left(\frac{S_k(f,\psi)}{q^{k/2}}\right) - \sum_{k=-K}^{-1}\widehat{h}(k)\left(\frac{S_{-k}(f,\overline{\psi})}{q^{-k/2}}\right)\\ &= (d-1)\widehat{h}(0) - \sum_{k=1}^{K}\frac{\widehat{h}(k)S_k(f,\psi)+\widehat{h}(-k)S_k(f,\overline{\psi})}{q^{k/2}}.\end{aligned}$$

□

Lemma 3.2. *Let $\theta_j(f,\psi)$ be the eigenangles of the L-function $L(u,f,\psi)$. Then for any $n\geq 1$,*

$$-\sum_{j=1}^{d-1} e^{2\pi i n\theta_j(f,\psi)} = \sum_{\deg(M)=n}\frac{\Lambda(M)\psi_f(M)}{q^{n/2}}$$

where M runs over monic polynomials in $\mathbb{F}_q[X]$,

$$\Lambda(M) = \begin{cases}\deg P & \text{if } M = P^k \text{ for some } k\geq 1 \text{ and } P \text{ irreducible,}\\ 0 & \text{otherwise,}\end{cases}$$

and $\psi_f(P^k) = \psi_f(P)^k$.

Proof. Comparing equations (4) and (3), we have

$$\prod_{j=1}^{d-1}(1-\alpha_j(f,\psi)u)=\prod_{P}(1-\psi_f(P)u^{\deg P})^{-1},$$

where the product on the right hand side is taken over monic irreducible polynomials in $\mathbb{F}_q[X]$. Taking logarithmic derivatives and multiplying by u, we deduce that

$$-\sum_{j=1}^{d-1}\sum_{n=1}^{\infty}(\alpha_j(f,\psi)u)^n=\sum_{M}\Lambda(M)u^{\deg M}\psi_f(M).$$

Comparing the coefficients of u^n, we get

$$-\sum_{j=1}^{d-1}\alpha_j(f,\psi)^n=\sum_{\deg(M)=n}\Lambda(M)\psi_f(M),$$

and the result follows by dividing both sides by $q^{n/2}$. □

4. The distribution of zeroes of $L(u,f,\psi)$

In this section we use the Erdös-Turán inequality (see [Mon94], Corollary 1.1) to prove a result on the number of eigenangles $\theta_j(f,\psi)$ in an interval $\mathcal{I}$ for a fixed L-function $L(u,f,\psi)$.

Theorem 4.1. *[P. Erdös, P. Turán] Let $x_1,x_2,\dots,x_N$ be real numbers lying in the unit interval $[-1/2,1/2)$. For any interval $\mathcal{I}\subseteq[-1/2,1/2)$, let $A(\mathcal{I},N,\{x_n\})$ denote the number of elements from the above set in $\mathcal{I}$. Let $|\mathcal{I}|$ denote the length of the interval. There exist absolute constants B_1 and B_2 such that for any $K\geq 1$,*

$$|A(\mathcal{I},N,\{x_n\})-N|\mathcal{I}||\leq\frac{B_1N}{K+1}+B_2\sum_{k=1}^{K}\frac{1}{k}\left|\sum_{n=1}^{N}e^{2\pi ikx_n}\right|.$$

We now prove the following theorem, which is the analogue of Proposition 5.1 in [FR10].

Theorem 4.2. *For any $\mathcal{I}\subseteq[-1/2,1/2)$, let $N_{\mathcal{I}}(f,\psi):=\#\{1\leq j\leq d-1:\theta_j(f,\psi)\in\mathcal{I}\}$. Then*

$$N_{\mathcal{I}}(f,\psi)=(d-1)|\mathcal{I}|+O\left(\frac{d}{\log d}\right).$$

Proof. By the Erdös-Turán inequality and Lemma 3.2, we have

$$\begin{aligned}|N_{\mathcal{I}}(f,\psi)-(d-1)|\mathcal{I}||&\ll\frac{d}{K}+\sum_{k=1}^{K}\frac{1}{k}\left|\sum_{\deg M=k}\frac{\Lambda(M)\psi_f(M)}{q^{k/2}}\right|\\&\ll\frac{d}{K}+\sum_{k=1}^{K}\frac{1}{q^{k/2}}\sum_{\substack{M=P^a,\,a\geq 1\\ \deg M=k}}1.\end{aligned}$$

Applying the function-field analogue of the prime number theorem, the above expression is $\ll\frac{d}{K}+\frac{q^{K/2}}{K}$. Choosing $K=\left[\frac{\log d}{\log q}\right]$, we deduce the theorem. □

5. Beurling-Selberg functions

By the functional equation, the conjugate of a root of $Z_{C_f}(u)$ is also a root so we can restrict to considering symmetric intervals. Let $\mathcal{I}=[-\beta/2,\beta/2]\subset[-1/2,1/2)$. We are going to approximate the characteristic function of $\mathcal{I}$, $\chi_{\mathcal{I}}$, with Beurling-Selberg polynomials $I_K^{\pm}$. We will use the following properties of the coefficients of Beurling-Selberg polynomials (see [Mon94], ch 1.2).

(a) The $I_K^{\pm}$ are trigonometric polynomials of degree $\leq K$, i.e.,

$$I_K^{\pm}(x)=\sum_{|k|\leq K}\widehat{I}_K^{\pm}(k)e(kx).$$

(b) The Beurling-Selberg polynomials bound the characteristic function from below and above:

$$I_K^- \le \chi_{\mathcal{I}} \le I_K^+.$$

(c) The integral of Beurling-Selberg polynomials is close to the length of the interval:

$$\int_{-1/2}^{1/2} I_K^{\pm}(x)dx = \int_{-1/2}^{1/2} \chi_{\mathcal{I}}(x)dx \pm \frac{1}{K+1}.$$

(d) The $I_K^{\pm}$ are even (since we are taking the interval $\mathcal{I}$ to be symmetric about the origin). It then follows that the Fourier coefficients are also even, i.e. $\widehat{I}_K^{\pm}(-k) = \widehat{I}_K^{\pm}(k)$ for $|k| \le K$.

(e) The nonzero Fourier coefficients are also close to those of the characteristic function:

$$|\widehat{I}_K^{\pm}(k) - \widehat{\chi}_{\mathcal{I}}(k)| \le \frac{1}{K+1} \quad \Longrightarrow \quad \widehat{I}_K^{\pm}(k) = \frac{\sin(\pi k|\mathcal{I}|)}{\pi k} + O\left(\frac{1}{K+1}\right), \quad k \ge 1.$$

This implies the following bound:

$$|\widehat{I}_K^{\pm}(k)| \le \frac{1}{K+1} + \min\left\{|\mathcal{I}|, \frac{\pi}{|k|}\right\}, \quad 0 < |k| \le K;$$

Proposition 5.1. *(Proposition 4.1,* [FR10]*) For $K \ge 1$ such that $K|\mathcal{I}| > 1$, we have*

$$\begin{aligned}
\sum_{k\ge 1} \widehat{I}_K^{\pm}(2k) &= O(1), \\
\sum_{k\ge 1} \widehat{I}_K^{\pm}(k)^2 k &= \frac{1}{2\pi^2}\log(K|\mathcal{I}|) + O(1), \\
\sum_{k\ge 1} \widehat{I}_K^{+}(k)\widehat{I}_K^{-}(k) k &= \frac{1}{2\pi^2}\log(K|\mathcal{I}|) + O(1).
\end{aligned}$$

Note that for a given K these sums are actually finite, since the Beurling-Selberg polynomials $I_K^{\pm}$ have degree at most K.

Proof. The first two statements are proven in Proposition 4.1 of [FR10]. Since

$$\widehat{I}_K^{\pm}(k) = \frac{\sin(\pi k|\mathcal{I}|)}{\pi k} + O\left(\frac{1}{K}\right),$$

holds for both $\widehat{I}_K^{+}(k)$ and $\widehat{I}_K^{-}(k)$, the third statement follows by exactly the same proof as the second statement. □

We will also need the following estimates.

Proposition 5.2. *For $\alpha_1, \dots, \alpha_r, \gamma_1, \dots, \gamma_r > 0$, and $\beta_1, \dots, \beta_r \in \mathbb{R}$, we have,*

$$\sum_{k_1,\dots,k_r \ge 1} \widehat{I}_K^{\pm}(k_1)^{\alpha_1} \dots \widehat{I}_K^{\pm}(k_r)^{\alpha_r} k_1^{\beta_1} \dots k_r^{\beta_r} q^{-\gamma_1 k_1 - \dots - \gamma_r k_r} = O(1).$$

For $\alpha_1, \alpha_2, \gamma > 0$, and $\beta \in \mathbb{R}$,

$$\sum_{k\ge 1} \widehat{I}_K^{\pm}(k)^{\alpha_1} \widehat{I}_K^{\pm}(2k)^{\alpha_2} k^{\beta} q^{-\gamma k} = O(1).$$

Proof. Since $\left|\widehat{I}_K^{\pm}(k)\right| \le \frac{1}{K+1} + \min\left\{|\mathcal{I}|, \frac{\pi}{|k|}\right\}$, we obtain

$$\left| \sum_{k_1,\dots,k_r \ge 1} \widehat{I}_K^{\pm}(k_1)^{\alpha_1} \dots \widehat{I}_K^{\pm}(k_r)^{\alpha_r} k_1^{\beta_1} \dots k_r^{\beta_r} q^{-\gamma_1 k_1 - \dots - \gamma_r k_r} \right| \ll \sum_{k_1,\dots,k_r \ge 1} k_1^{\beta_1} \dots k_r^{\beta_r} q^{-\gamma_1 k_1 - \dots - \gamma_r k_r}$$

Since $\sum_{k\ge 1} k^{\beta} q^{-\gamma k} = O(1)$ for $q > 1$ and $\gamma > 0$, we get that the right hand side above is also equal to $O(1)$. The second equation is proved in a similar way. □

6. First Moment

Recall that $N_{\mathcal{I}}(f,\psi)$ denotes the number of angles $\theta_j(f,\psi)$ of the zeroes of the L-function $L(u,f,\psi)$ in the interval $\mathcal{I}$.

From now on, for a function $\phi : \mathcal{F}'_d \to \mathbb{C}$, we denote its average by

$$\langle \phi(f) \rangle := \frac{1}{|\mathcal{F}'_d|} \sum_{f \in \mathcal{F}'_d} \phi(f).$$

We want to compute the first moment

$$\langle N_{\mathcal{I}}(f,\psi) \rangle = \frac{1}{|\mathcal{F}'_d|} \sum_{f \in \mathcal{F}'_d} N_{\mathcal{I}}(f,\psi).$$

We will do so by proving the following result.

Theorem 6.1. *As $d \to \infty$,*

$$\langle N_{\mathcal{I}}(f,\psi) - (d-1)|\mathcal{I}| \rangle = O(1).$$

Remark 6.2. Recall that in Theorem 4.2 we showed that

$$N_{\mathcal{I}}(f,\psi) - (d-1)|\mathcal{I}| = O\left(\frac{d}{\log d}\right).$$

Theorem 6.1, on the other hand, gives us a far better estimate for the average of $\langle N_{\mathcal{I}}(f,\psi) - (d-1)|\mathcal{I}| \rangle$ than we could have derived from Theorem 4.2.

For the proof of Theorem 6.1, we will use the Beurling-Selberg approximation of the characteristic function of the interval $\mathcal{I}$. By property **(b)** of the Beurling-Selberg polynomials,

$$\sum_{j=1}^{d-1} I_K^-(\theta_j(f,\psi)) \le N_{\mathcal{I}}(f,\psi) \le \sum_{j=1}^{d-1} I_K^+(\theta_j(f,\psi)).$$

With the explicit formula of Lemma 3.1 and property **(c)**, we write

$$\sum_{j=1}^{d-1} I_K^{\pm}(\theta_j(f,\psi)) \quad = \quad (d-1)|\mathcal{I}| - S^{\pm}(K,f,\psi) \pm \frac{d-1}{K+1}$$

where

$$S^{\pm}(K,f,\psi) := \sum_{k=1}^{K} \frac{\widehat{I}_K^{\pm}(k) S_k(f,\psi) + \widehat{I}_K^{\pm}(-k) S_k(f,\bar{\psi})}{q^{k/2}}. \tag{9}$$

This gives

$$-S^-(K,f,\psi) - \frac{d-1}{K+1} \le N_{\mathcal{I}}(f,\psi) - (d-1)|\mathcal{I}| \le -S^+(K,f,\psi) + \frac{d-1}{K+1}. \tag{10}$$

In order to complete the proof it remains to estimate $\langle S^{\pm}(K,f,\psi) \rangle$. We will need the following results from [Ent]. As we remarked in Section 2, we are using a slightly different description for the family of Artin-Schreier curves since we do not allow twists. Because of that, our results are slightly simpler than those stated in [Ent]. We have also modified the original notation so that it fits the generalization that we pursue in the next sections.

Lemma 6.3. *(*[Ent]*, Lemma 5.2)Let h be an integer, $p \nmid h$. Assume $k < d$ and $\alpha \in \mathbb{F}_{q^k}$. Then*

$$\langle h\psi(\mathrm{tr}_k\, f(\alpha)) \rangle = \begin{cases} 1 & p \mid k,\ \alpha \in \mathbb{F}_{q^{k/p}}, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If $p \mid k$ and $\alpha \in \mathbb{F}_{q^{k/p}}$ then $\mathrm{tr}_k(f(\alpha)) = p\,\mathrm{tr}_{\frac{k}{p}}(f(\alpha)) = 0$ so $\langle \psi(\mathrm{tr}_k f(\alpha))\rangle = 1$. For the remaining case we first note that the average is the same if we average over the family $\mathcal{F}_d$ of degree d polynomials (without the condition $a_{pk} = 0$). This is due to the existence of the map μ defined by (6).

Denote by u the degree of α over $\mathbb{F}_q$. Since $u \le k < d$ the map

$$\tau : \mathcal{F}_d \to \mathbb{F}_{q^u}$$

defined by $\tau(f) = f(\alpha)$ is $(q-1)q^{d-u}$-to-one. Thus as f ranges over $\mathcal{F}_d$, $f(\alpha)$ takes each value in $\mathbb{F}_{q^u}$ an equal number of times. Since $p \nmid \frac{k}{u}$, $\mathrm{tr}_k(f(\alpha)) = \frac{k}{u}\,\mathrm{tr}_u(f(\alpha))$ also takes every value in $\mathbb{F}_p$ the same number of times as f ranges over $\mathcal{F}_d$ and the same is true for $h\,\mathrm{tr}_k(f(\alpha))$. Thus each pth root of unity occurs the same number of times in $\psi(h\,\mathrm{tr}_k(f(\alpha)))$ as f ranges over $\mathcal{F}_d$ and so the average is 0. □

The lemma has the following consequence.

Corollary 6.4. *(*[Ent]*, Corollary 5.3) Let h be an integer, $p \nmid h$. Assume $k < d$ and set*

$$M_{1,d}^{k,1,h} := \left\langle q^{-k/2} \sum_{\alpha \in \mathbb{F}_{q^k}} \psi(h\,\mathrm{tr}_k f(\alpha)) \right\rangle.$$

Then

$$M_{1,d}^{k,1,h} = e_{p,k} q^{-(1/2-1/p)k},$$

where

$$e_{p,k} = \begin{cases} 0 & p \nmid k, \\ 1 & p \mid k. \end{cases}$$

We also denote

$$M_{1,d}^{k,-1,h} := \left\langle q^{-k/2} \sum_{\alpha \in \mathbb{F}_{q^k}} \psi(-h\,\mathrm{tr}_k f(\alpha)) \right\rangle.$$

Clearly, $M_{1,d}^{k,-1,h} = \overline{M_{1,d}^{k,1,h}}$.

Notice that changing h allows us to vary the character from ψ to ψ^h. This will be useful later.

Proof. (Theorem 6.1) We have that

$$\begin{aligned} \left\langle S^{\pm}(K,f,\psi)\right\rangle &= \sum_{k=1}^{K} \frac{\widehat{I}_K^{\pm}(k)\left\langle S_k(f,\psi)\right\rangle + \widehat{I}_K^{\pm}(-k)\left\langle S_k(f,\bar{\psi})\right\rangle}{q^{k/2}} \\ &= \sum_{k=1}^{K} \widehat{I}_K^{\pm}(k) M_{1,d}^{k,1,1} + \widehat{I}_K^{\pm}(-k) M_{1,d}^{k,-1,1} \\ &= 2\sum_{k=1}^{K} \widehat{I}_K^{\pm}(k) e_{p,k} q^{-(1/2-1/p)k} \end{aligned}$$

and the result follows from property **(e)** and (10) taking $K = cd$ with $c < 1$. □

Remark 6.5. We denote by

$$C(K) := \sum_{k=1}^{K} \widehat{I}_K^{\pm}(k) e_{p,k} q^{-(1/2-1/p)k}$$

and

$$C := \sum_{k=1}^{\infty} \frac{\sin(\pi k|\mathcal{I}|)}{\pi k} e_{p,k} q^{-(1/2-1/p)k}.$$

These terms will reappear in the computation of the higher moments. Note that, since $p > 2$, the above infinite series converges absolutely. By Proposition 5.2, $C(K) = O(1)$. By property **(e)** of the Beurling-Selberg polynomials, $C = C(K) + O(1/K)$.

7. Second moment

Let

$$S^{\pm}(K, C_f) = \sum_{h=1}^{p-1} S^{\pm}(K, f, \psi^h), \tag{11}$$

where $S^{\pm}(K, f, \psi)$ is defined in (9).

In the next sections, we are computing the moments of $S^{\pm}(K, C_f)$. We show that they fit the Gaussian moments when properly normalized (Theorem 9.6). We will then use this result to show that

$$\frac{N_{\mathcal{I}}(C_f) - (p-1)(d-1)|\mathcal{I}|}{\sqrt{\frac{2(p-1)}{\pi^2}\log(d|\mathcal{I}|)}}$$

converges to a normal distribution as $d \to \infty$ since it converges in mean square to

$$\frac{S^{\pm}(K, C_f)}{\sqrt{\frac{2(p-1)}{\pi^2}\log(d|\mathcal{I}|)}}.$$

The following lemma is generalization of Lemma 6.2 in [Ent], that also takes into account the difference in our family of Artin-Schreier curves.

Recall that $\psi^j(\alpha) = \psi(j\alpha)$ for $\alpha \in \mathbb{F}_p$. We have the following

Lemma 7.1. *Let $p \nmid h_1 h_2$ and let $e_1, e_2 \in \{-1, 1\}$. Assume $k_1, k_2 > 0$, $k_1 + k_2 < d$. Let $\alpha_1 \in \mathbb{F}_{q^{k_1}}$, $\alpha_2 \in \mathbb{F}_{q^{k_2}}$ with monic minimal polynomials g_1, g_2 of degrees u_1, u_2 over $\mathbb{F}_q$ respectively. We have*

$$\langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2)) \rangle = \begin{cases} 1, & g_1 = g_2,\ p \mid \frac{e_1 h_1 k_1 + e_2 h_2 k_2}{u_1},\ p \nmid \frac{k_1 k_2}{u_1 u_2} \text{ or } p \mid \left(\frac{k_1}{u_1}, \frac{k_2}{u_2}\right) \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $p \mid \frac{k_2}{u_2}$ then $\operatorname{tr}_{k_2} f(\alpha_2) = p \operatorname{tr}_{\frac{k_2}{p}} f(\alpha_2) = 0$, so

$$\langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2)) \rangle = \langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1)) \rangle .$$

By Lemma 6.3, this equals 0 if $p \nmid \frac{k_1}{u_1}$ and 1 if $p \mid \frac{k_1}{u_1}$ as $p \nmid e_1 h_1$.

The only remaining case is when $p \nmid \frac{k_1 k_2}{u_1 u_2}$. We first suppose that $g_1 \neq g_2$. We note that we will have the same value if we average over $\mathcal{F}_d$ rather than $\mathcal{F}'_d$ due to the existence of the map μ defined by (6). Since $u_1 + u_2 \leq k_1 + k_2 < d$, the map

$$\tau : \mathcal{F}_d \to \mathbb{F}_q[X]/(g_1 g_2) \simeq \mathbb{F}_{q^{u_1}} \times \mathbb{F}_{q^{u_2}}$$

is exactly $(q-1)q^{d-u_1-u_2}$-to-one. Hence as f ranges over $\mathcal{F}_d$, $(f(\alpha_1), f(\alpha_2))$ takes every value in $\mathbb{F}_{q^{u_1}} \times \mathbb{F}_{q^{u_2}}$ the same number of times. Now, since $p \nmid \frac{e_1 h_1 k_1}{u_1}$ and $p \nmid \frac{e_2 h_2 k_2}{u_2}$,

$$(\operatorname{tr}_{k_1} f(\alpha_1), \operatorname{tr}_{k_2} f(\alpha_2)) = \left(\frac{e_1 h_1 k_1}{u_1} \operatorname{tr}_{u_1}(f(\alpha_1)), \frac{e_2 h_2 k_2}{u_2} \operatorname{tr}_{u_2}(f(\alpha_2)) \right)$$

also takes every value in $\mathbb{F}_p \times \mathbb{F}_p$ the same number of times as f ranges over $\mathcal{F}_d$. Then

$$\psi\left(e_1 h_1 \operatorname{tr}_{k_1}(f(\alpha_1)) + e_2 h_2 \operatorname{tr}_{k_2}(f(\alpha_2))\right) = \psi\left(e_1 h_1 \frac{k_1}{u_1} \operatorname{tr}_{u_1}(f(\alpha_1)) + e_2 h_2 \frac{k_2}{u_2} \operatorname{tr}_{u_2}(f(\alpha_2)) \right)$$

assumes every pth root of unity equally many times as we average over $\mathcal{F}_d$ and so the average is 0.

If $g_1 = g_2$, then α_1 and α_2 are conjugates over $\mathbb{F}_q$ and so are $f(\alpha_1), f(\alpha_2)$. Then $\operatorname{tr}_{u_1} f(\alpha_1) = \operatorname{tr}_{u_1} f(\alpha_2)$. This implies

$$e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2) = e_1 h_1 \frac{k_1}{u_1} \operatorname{tr}_{u_1} f(\alpha_1) + e_2 h_2 \frac{k_2}{u_1} \operatorname{tr}_{u_1} f(\alpha_2) = \frac{e_1 h_1 k_1 + e_2 h_2 k_2}{u_1} \operatorname{tr}_{u_1} f(\alpha_1),$$

which is zero when $p \mid \frac{e_1 h_1 k_1 + e_2 h_2 k_2}{u_1}$. If p does not divide $\frac{e_1 h_1 k_1 + e_2 h_2 k_2}{u_1}$ then

$$\langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2)) \rangle = \left\langle \psi\left(\frac{e_1 h_1 k_1 + e_2 h_2 k_2}{u_1} \operatorname{tr}_{u_1} f(\alpha_1) \right) \right\rangle = 0$$

by Lemma 6.3.

□

For positive integers k_1, k_2, h_1, h_2 with $p \nmid h_1 h_2$ and $e_1, e_2 \in \{-1, 1\}$, let

$$\begin{aligned} M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} &:= \left\langle q^{-(k_1+k_2)/2} \sum_{\substack{\alpha_1 \in \mathbb{F}_{q^{k_1}} \\ \alpha_2 \in \mathbb{F}_{q^{k_2}}}} \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2)) \right\rangle \\ &= q^{-(k_1+k_2)/2} \sum_{\substack{\alpha_1 \in \mathbb{F}_{q^{k_1}} \\ \alpha_2 \in \mathbb{F}_{q^{k_2}}}} \langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2)) \rangle . \end{aligned}$$

Then we have the following analogue of Theorem 8 in [Ent].

Theorem 7.2. *Assume $k_1 \geq k_2 > 0$ and $k_1 + k_2 < d$. Let $0 < h_1, h_2 \leq (p-1)/2$. Then*

$$\begin{aligned} M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} &= \delta_{k_1,2k_2} O\left(k_1 q^{-k_2/2}\right) + O\left(k_1 q^{-k_2/2-k_1/6} + q^{-(1/2-1/p)(k_1+k_2)}\right) \\ &\quad + \begin{cases} \delta_{k_1,k_2} k_1 \left(1 + O\left(q^{-k_1/2}\right)\right), & (e_1,e_2) = (1,-1), h_1 = h_2, \\ 0, & \text{otherwise,} \end{cases} \end{aligned}$$

where

$$\delta_{k_1,k_2} = \begin{cases} 1, & k_1 = k_2, \\ 0, & k_1 \neq k_2. \end{cases}$$

Before proceeding with the proof, we would like to make a few remarks. In the instances when we apply this result, we will choose $K = cd$, for $0 < c < 1/2$, and therefore $k_1, k_2 \leq K$ will imply that $k_1 + k_2 < d$, and will be able to apply Theorem 7.2 for all values of k_1, k_2 under consideration. Also note that the condition $k_1 \geq k_2 > 0$ does not restrict the validity of the statement, since $M_{2,d}^{(k_2,k_1),(1,-1),(h_1,h_2)} = \overline{M_{2,d}^{(k_1,k_2),(1,-1),(h_2,h_1)}}$.

Proof. From Lemma 7.1,

$$M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} = q^{-(k_1+k_2)/2} \left(e_{p,e_1 h_1 k_1 + e_2 h_2 k_2} \sum_{\substack{m \mid (k_1,k_2) \\ mp \nmid k_1,k_2 \\ mp \mid (e_1 h_1 k_1 + e_2 h_2 k_2)}} \pi(m) m^2 + e_{p,k_1} e_{p,k_2} q^{(k_1+k_2)/p} \right),$$

where $\pi(m)$ denotes the number of monic irreducible polynomials of degree m over $\mathbb{F}_q[X]$. The prime number theorem for function fields (see [Ros02], Theorem 2.2) states that $\pi(m) = \frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right)$.

When $k_1 = k_2$, the conditions on the summation indices become $m \mid k_1$, $mp \nmid k_1$, and $mp \mid (e_1 h_1 + e_2 h_2) k_1$, a contradiction unless $p \mid (e_1 h_1 + e_2 h_2)$. Due to the range in which the h_1, h_2 take values, this can only happen when $e_1 = -e_2$ and $h_1 = h_2$. In this case, one gets

$$\sum_{\substack{m \mid k_1 \\ mp \nmid k_1}} \pi(m) m^2 = k_1 q^{k_1} + O\left(k_1 q^{k_1/2}\right).$$

On the other hand, when $k_1 = 2k_2$, one gets

$$\sum_{\substack{m \mid k_2 \\ mp \nmid k_2 \\ mp \mid (2e_1 h_1 + e_2 h_2) k_2}} \pi(m) m^2 = O(k_2 q^{k_2}) = O\left(k_1 q^{k_1/2}\right).$$

Finally, if $k_1 > k_2$ but $k_1 \neq 2k_2$, we have $(k_1, k_2) \leq k_1/3$ and

$$\sum_{\substack{m \mid (k_1,k_2) \\ mp \nmid k_1,k_2 \\ mp \mid (e_1 h_1 k_1 + e_2 h_2 k_2)}} \pi(m) m^2 = O\left(k_1 q^{k_1/3}\right).$$

This concludes the proof of the theorem. □

Finally, we are able to compute the covariances.

Theorem 7.3. *Let $0 < h_1, h_2 \le (p-1)/2$. Then for any K with $\max\{1, 1/|\mathcal{I}|\} < K < d/2$,*

$$\left\langle S^{\pm}(K, f, \psi^{h_1}) S^{\pm}(K, f, \psi^{h_2}) \right\rangle = \left\langle S^{\pm}(K, f, \psi^{h_1}) S^{\mp}(K, f, \psi^{h_2}) \right\rangle = \begin{cases} \frac{1}{\pi^2} \log(K|\mathcal{I}|) + O(1), & h_1 = h_2 \\ O(1), & h_1 \neq h_2. \end{cases}$$

Proof. By definition,

$$\begin{aligned} &\left\langle S^{\pm}(K, f, \psi^{h_1}) S^{\pm}(K, f, \psi^{h_2}) \right\rangle \\ &= \sum_{k_1, k_2 = 1}^{K} \widehat{I}_K^{\pm}(k_1) \widehat{I}_K^{\pm}(k_2) M_{2,d}^{(k_1,k_2),(1,1),(h_1,h_2)} + \widehat{I}_K^{\pm}(k_1) \widehat{I}_K^{\pm}(-k_2) M_{2,d}^{(k_1,k_2),(1,-1),(h_1,h_2)} \\ &\quad + \widehat{I}_K^{\pm}(-k_1) \widehat{I}_K^{\pm}(k_2) M_{2,d}^{(k_1,k_2),(-1,1),(h_1,h_2)} + \widehat{I}_K^{\pm}(-k_1) \widehat{I}_K^{\pm}(-k_2) M_{2,d}^{(k_1,k_2),(-1,-1),(h_1,h_2)}. \end{aligned}$$

Then, by repeated use of Theorem 7.2 and Proposition 5.2, the summation over k_1, k_2 is $O(1)$ if $h_1 \neq h_2$. If $h_1 = h_2$ then

$$\begin{aligned} \left\langle S^{\pm}(K, f, \psi^{h_1})^2 \right\rangle &= 2 \sum_{k_1 = 1}^{K} \widehat{I}_K^{\pm}(k_1) \widehat{I}_K^{\pm}(-k_1) k_1 + O(1) = 2 \sum_{k_1 \ge 1} \widehat{I}_K^{\pm}(k_1)^2 k_1 + O(1) \\ &= \frac{1}{\pi^2} \log(K|\mathcal{I}|) + O(1) \end{aligned}$$

by applying Proposition 5.1. The proof for $\left\langle S^{\pm}(K, f, \psi^{h_1}) S^{\mp}(K, f, \psi^{h_2}) \right\rangle$ follows along exactly the same lines. □

Corollary 7.4. *For any K with $\max\{1, 1/|\mathcal{I}|\} < K < d/2$,*

$$\langle S^{\pm}(K, C_f)^2 \rangle = \langle S^{+}(K, C_f) S^{-}(K, C_f) \rangle = \frac{2(p-1)}{\pi^2} \log(K|\mathcal{I}|) + O(1).$$

Proof. First we note that

$$\langle S^{\pm}(K, C_f)^2 \rangle = \sum_{h_1, h_2 = 1}^{p-1} \left\langle S^{\pm}(K, f, \psi^{h_1}) S^{\pm}(K, f, \psi^{h_2}) \right\rangle.$$

Notice that by Theorem 7.3, the mixed average contributes $\frac{1}{\pi^2} \log(K|\mathcal{I}|) + O(1)$ for each term where $h_1 = h_2$ or $h_1 = p - h_2$. The proof for $\langle S^{+}(K, C_f) S^{-}(K, C_f) \rangle$ is identical. □

8. Third moment

Let k_1, k_2, k_3 be positive integers, e_1, e_2, e_3 take values ± 1, and h_1, h_2, h_3 be integers such that $p \nmid h_i$. Denote $\mathbf{k} = (k_1, k_2, k_3)$, $\mathbf{e} = (e_1, e_2, e_3)$, and $\mathbf{h} = (h_1, h_2, h_3)$. For every $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}} \times \mathbb{F}_{q^{k_3}}$, set

$$m_{3,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = \langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2 h_2 \operatorname{tr}_{k_2} f(\alpha_2) + e_3 h_3 \operatorname{tr}_{k_3} f(\alpha_3)) \rangle,$$

and

$$M_{3,d}^{\mathbf{k},\mathbf{e},\mathbf{h}} = \sum_{\substack{\alpha_i \in \mathbb{F}_{q^{k_i}} \\ i=1,2,3}} q^{-(k_1+k_2+k_3)/2} m_{3,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}).$$

In an analogous manner to Section 7, one can prove the following.

Lemma 8.1. *Let $p \nmid h_1 h_2 h_3$ and let $e_1, e_2, e_3 \in \{-1, 1\}$. Assume $k_1, k_2, k_3 > 0$ and $k_1 + k_2 + k_3 < d$. For $i = 1, 2, 3$ α_i be an element of $\mathbb{F}_{q^{k_i}}$ with minimal polynomial g_i over $\mathbb{F}_q$ of degree u_i. We have $m_{3,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = 1$ in any of the following cases*

- $g_1 = g_2 = g_3, p \mid \frac{(e_1 h_1 k_1 + e_2 h_2 k_2 + e_3 h_3 k_3)}{u_1}, p \nmid \frac{k_1 k_2 k_3}{u_1 u_2 u_3}$.
- $g_{j_1} = g_{j_2}, p \mid \frac{(e_{j_1} h_{j_1} k_{j_1} + e_{j_2} h_{j_2} k_{j_2})}{u_{j_1}}, p \nmid \frac{k_{j_1} k_{j_2}}{u_{j_1} u_{j_2}}, p \mid \frac{k_{j_3}}{u_{j_3}}$, *where (j_1, j_2, j_3) is any permutation of $(1, 2, 3)$.*
- $p \mid \frac{k_i}{u_i}, i = 1, 2, 3$.

Otherwise $m_{3,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = 0$.

Theorem 8.2. *Assume* $k_1 \geq k_2 \geq k_3 > 0$ *and* $k_1 + k_2 + k_3 < d$. *Then*

$$\begin{aligned}
& M_{3,d}^{\mathbf{k},\mathbf{e},\mathbf{h}} \\
= \; & M_{1,d}^{k_1,e_1,h_1} M_{2,d}^{(k_2,k_3),(e_2,e_3),(h_1,h_2)} + M_{1,d}^{k_2,e_2,h_3} M_{2,d}^{(k_1,k_3),(e_1,e_3),(h_1,h_3)} + M_{1,d}^{k_3,e_3,h_3} M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} \\
& -2M_{1,d}^{k_1,e_1,h_1} M_{1,d}^{k_2,e_2,h_2} M_{1,d}^{k_3,e_3,h_3} \\
& +O\left(\delta_{k_1,k_2,k_3} k_1^2 q^{-k_1/2} + \delta_{k_1,k_2,2k_3} k_1^2 q^{-3k_1/4} + \delta_{k_1,2k_2,2k_3} k_1^2 q^{-k_1/2} + k_1^2 q^{-k_1/6-k_2-k_3}\right) \\
= \; & e_{p,k_1} q^{-(1/2-1/p)k_1} M_{2,d}^{(k_2,k_3),(e_2,e_3),(h_2,h_3)} + e_{p,k_2} q^{-(1/2-1/p)k_2} M_{2,d}^{(k_1,k_3),(e_1,e_3),(h_1,h_3)} \\
& +e_{p,k_3} q^{-(1/2-1/p)k_3} M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} \\
& +O\left(\delta_{k_1,k_2,k_3} k_1^2 q^{-k_1/2} + \delta_{k_1,k_2,2k_3} k_1^2 q^{-3k_1/4} + \delta_{k_1,2k_2,2k_3} k_1^2 q^{-k_1/2} + k_1^2 q^{-k_1/6-k_2-k_3} + q^{-(1/2-1/p)(k_1+k_2+k_3)}\right).
\end{aligned}$$

Proof. We can use induction in the same way as we used it in the proof of Lemma 8.1. The only new term to be considered is given by the case $g_1 = g_2 = g_3, pu_1 \mid (e_1h_1k_1 + e_2h_2k_2 + e_3h_3k_3)$. This term yields

$$q^{-(k_1+k_2+k_3)/2} e_{p,e_1h_1k_1+e_2h_2k_2+e_3h_3k_3} \sum_{\substack{m \mid (k_1,k_2,k_3) \\ mp \nmid k_1,k_2,k_3 \\ mp \mid (e_1h_1k_1+e_2h_2k_2+e_3h_3k_3)}} \pi(m) m^3.$$

Suppose that $k_1 \geq k_2 \geq k_3$. If $k_1 = k_3$, we have

$$\sum_{\substack{m \mid k_1 \\ mp \nmid k_1 \\ mp \mid (e_1h_1+e_2h_2+e_3h_3)k_1}} \pi(m) m^3 = O\left(k_1^2 q^{k_1}\right).$$

If $k_1 = 2k_3$, $k_2 = k_1$ or $k_2 = k_3$, we have

$$\sum_{\substack{m \mid (k_1,k_2,k_3) \\ mp \nmid k_3 \\ mp \mid (e_1h_1k_1+e_2h_2k_2+e_3h_3k_3)}} \pi(m) m^3 = O\left(k_1^2 q^{k_1/2}\right).$$

Finally, for the other cases,

$$\sum_{\substack{m \mid (k_1,k_2,k_3) \\ mp \nmid k_1,k_2,k_3 \\ mp \mid (e_1h_1k_1+e_2h_2k_2+e_3h_3k_3)}} \pi(m) m^3 = O\left(k_1^2 q^{k_1/3}\right).$$

□

Theorem 8.3. *Let* $0 < h_1, h_2, h_3 \leq (p-1)/2$. *For any* K *with* $\max\{1, 1/|\mathcal{I}|\} < K < d/3$,

$$\begin{aligned}
& \left\langle S^{\pm}(K, f, \psi^{h_1}) S^{\pm}(K, f, \psi^{h_2}) S^{\pm}(K, f, \psi^{h_3}) \right\rangle \\
= \; & \begin{cases} \frac{3C}{\pi^2} \log(K|\mathcal{I}|) + O(1) & h_1 = h_2 = h_3, \\ \frac{C}{\pi^2} \log(K|\mathcal{I}|) + O(1) & h_{j_1} = h_{j_2} \neq h_{j_3},\ (j_1, j_2, j_3) \text{ a permutation of } (1,2,3), \\ O(1) & h_i \text{ distinct.} \end{cases}
\end{aligned}$$

where C *is the constant defined in Remark* 6.5.

Corollary 8.4. *For any* K *with* $\max\{1, 1/|\mathcal{I}|\} < K < d/3$,

$$\langle S^{\pm}(K, C_f)^3 \rangle = \frac{6C(p-1)^2}{\pi^2} \log(K|\mathcal{I}|) + O(1).$$

9. General Moments

Let $n, k_1, \dots, k_n$ be positive integers, let $e_1, \dots, e_n$ take values ± 1 and let $h_1, \dots, h_n$ be integers such that $p \nmid h_i$, $1 \le i \le n$. Let $\mathbf{k} = (k_1, \dots, k_n)$, $\mathbf{e} = (e_1, \dots, e_n)$ and $\mathbf{h} = (h_1, \dots, h_n)$. Let $\alpha_i \in \mathbb{F}_{q^{k_i}}$, $1 \le i \le n$, and let $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$. We define

$$m_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = \langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + \cdots + e_n h_n \operatorname{tr}_{k_n} f(\alpha_n)) \rangle$$

and

$$M_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}} = \sum_{\substack{\alpha_i \in \mathbb{F}_{q^{k_i}} \\ i=1,\dots,n}} q^{-(k_1+\cdots+k_n)/2} m_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}).$$

We are computing in this section the general moments

$$\left\langle S^{\pm}(K, f, \psi)^n \right\rangle = \sum_{k_1,\dots,k_n=1}^{K} \sum_{e_1,\dots,e_n=\pm 1} I_K^{\pm}(e_1 k_1) \dots I_K^{\pm}(e_n k_n) M_{n,d}^{\mathbf{k},\mathbf{e}}$$

and

$$\left\langle S^{\pm}(K, f, \psi^{h_1}) \dots S^{\pm}(K, f, \psi^{h_n}) \right\rangle = \sum_{k_1,\dots,k_n=1}^{K} \sum_{e_1,\dots,e_n=\pm 1} I_K^{\pm}(e_1 k_1) \dots I_K^{\pm}(e_n k_n) M_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}.$$

Lemma 9.1. *Assume $k_1, \dots, k_n > 0$, $k_1 + \cdots + k_n < d$. Let $g_1, \dots, g_s$ of degree $u_1, \dots, u_s$ respectively be all the distinct minimal polynomials over $\mathbb{F}_q$ of $\alpha_1, \dots, \alpha_n$ (we allow the possibility that some α_i's are conjugate to each other, thus $s \le n$), and let*

$$\epsilon_i = \frac{1}{u_i} \sum_{\alpha_j \in R(g_i)} k_j e_j h_j, \quad 1 \le i \le s,$$

where $R(g)$ is the set of roots of g. Then

$$m_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = \begin{cases} 1 & \text{if } p \mid \epsilon_i \text{ for } 1 \le i \le s, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. As before, we can take the average over the family $\mathcal{F}_d$ of polynomials of degree d without the condition that $a_{kp} = 0$ for $1 \le k \le d/p$. Renumbering, suppose that α_i has minimal polynomial g_i for $1 \le i \le s$.

Since $\sum_{i=1}^{s} u_i \le \sum_{i=1}^{s} k_i < d$, the map

$$\tau : \mathcal{F}_d \to \mathbb{F}_q[X]/(g_1 \dots g_s) \simeq \mathbb{F}_{q^{u_1}} \times \cdots \times \mathbb{F}_{q^{u_s}}$$

is exactly $(q-1)q^{d-(u_1+\cdots+u_s)}$-to-one, and as f ranges over $\mathcal{F}_d$, $(f(\alpha_1), \dots, f(\alpha_s))$ takes every value in $\mathbb{F}_{q^{u_1}} \times \cdots \times \mathbb{F}_{q^{u_s}}$ the same number of times. Now, $(\operatorname{tr}_{u_1} f(\alpha_1), \dots, \operatorname{tr}_{u_s} f(\alpha_s))$ also takes every value in $(\mathbb{F}_p)^s$ the same number of times as f ranges over $\mathcal{F}_d$, and the same holds for any linear combination

$$\gamma_1 \operatorname{tr}_{u_1} f(\alpha_1) + \cdots + \gamma_s \operatorname{tr}_{u_s} f(\alpha_s),$$

unless p divides every γ_i. This shows that each pth root of unity occurs as many times as

$$\psi\left(\gamma_1 \operatorname{tr}_{u_1} f(\alpha_1) + \cdots + \gamma_s \operatorname{tr}_{u_s} f(\alpha_s)\right)$$

when p does not divide all the γ_i. We now determine the coefficients γ_i for

$$m_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = \sum_{f \in \mathcal{F}_d} \psi\left(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + \cdots + e_n h_n \operatorname{tr}_{k_n} f(\alpha_n)\right).$$

Recall that $\operatorname{tr}_{k_i} f(\alpha_i) = \frac{k_i}{u_i} \operatorname{tr}_{u_i} f(\alpha_i)$ for $i = 1, \dots, s$. Let

$$\epsilon_i = \frac{1}{u_i} \sum_{\alpha_j \in R(g_i)} e_j h_j k_j, \quad 1 \le i \le s.$$

Then $\gamma_i = \epsilon_i$, i.e.,

$$m_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = \sum_{f \in \mathcal{F}_d} \psi\left(\epsilon_1 \operatorname{tr}_{u_1} f(\alpha_1) + \cdots + \epsilon_s \operatorname{tr}_{u_s} f(\alpha_s)\right),$$

which implies that $m_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha})$ takes the value 1 if $p \mid \epsilon_i$ for $1 \le i \le s$, and 0 otherwise. □

Recall that $\pi(m)$ denotes the number of monic irreducible polynomials in $\mathbb{F}_q[X]$.

Lemma 9.2. *Assume $k_1, \dots, k_n > 0$, $k_1 + \cdots + k_n < d$. Then $M_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$ is bounded by a sum of terms made of products of elementary terms of the type*

$$q^{-(j_1+\cdots+j_r)/2} \sum_{\substack{m|(j_1,\dots,j_r) \\ mp|\sum_{i=1}^r e_i h_i j_i}} \pi(m) m^r$$

where the indices $j_1, \dots, j_r$ of the elementary terms appearing in each product are in bijection with $k_1, \dots, k_n$.

Let $N_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$ be the sum of the terms made exclusively of products of elementary terms

$$q^{-(j_1+j_2)/2} \sum_{\substack{m|(j_1,j_2) \\ mp|e_1h_1j_1+e_2h_2j_2}} \pi(m) m^2.$$

If n is odd, these terms will also be multiplied by an elementary term

$$e_{p,j} q^{-j/2} \sum_{\substack{m|j \\ mp|ej}} \pi(m) m = e_{p,j} \sum_{m|\frac{j}{p}} \pi(m) m = e_{p,j} \#\mathbb{F}_{q^{j/p}} = e_{p,j} q^{j/p}.$$

Let $E_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$ be the sum of all the other terms appearing in $M_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$. Then, $M_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}} = N_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}} + O\left(E_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}\right)$.

Proof. We first remark that the number of $(\alpha_1, \dots, \alpha_t) \in \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_t}}$ which are conjugate over $\mathbb{F}_q$ is

$$\sum_{m|(k_1,\dots,k_t)} \pi(m) m^t.$$

Using Lemma 9.1, we then have to count the contribution coming from the $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ such that $p \mid \epsilon_i$ for $1 \le i \le s$. Let $\mathcal{P}$ be the set of partitions of n in s subsets $T_1, \dots, T_s$. Let $k(T_j)$ be the gcd of the k_i such that $i \in T_j$ and let $s(T_j) = \sum_{i \in T_j} e_i h_i k_i$. Then, for any such partition, the number of $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_n}}$ such that α_i is a root of g_j when $i \in T_j$ is less than or equal to

$$\sum_{\substack{m|k(T_1) \\ mp|s(T_1)}} \pi(m) m^{|T_1|} \cdots \sum_{\substack{m|k(T_s) \\ mp|s(T_s)}} \pi(m) m^{|T_s|}.$$

This proves the first statement of the lemma. We remark that the above count is an over-count, as it may also count polynomials $g_1, \dots, g_s$ which are not distinct. For example, the number of $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{F}_{q^{j_1}} \times \cdots \times \mathbb{F}_{q^{j_4}}$ with minimal polynomials $g_1 = g_2, g_3 = g_4$ and $g_1 \neq g_3$ is

$$q^{-(j_1+\cdots+j_4)/2} \left(\sum_{\substack{m|(j_1,j_2) \\ mp|e_1h_1j_1+e_2h_2j_2}} \pi(m) m^2 \sum_{\substack{m|(j_3,j_4) \\ mp|e_3h_3j_3+e_4h_4j_4}} \pi(m) m^2 - \sum_{\substack{m|(j_1,\dots,j_4) \\ mp|e_1h_1j_1+\cdots+e_4h_4j_4}} \pi(m) m^4 \right),$$

which can be written as a term in $N_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$ and a term in $E_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$. The general case is similar. Suppose that $n = 2\ell$ is even. Then, using inclusion-exclusion, the number of $(\alpha_1, \dots, \alpha_n) \in (\mathbb{F}_{q^{k_1}}, \dots, \mathbb{F}_{q^{k_n}})$ such that α_i and $\alpha_{\ell+i}$ have minimal polynomial g_i, and all the g_i are distinct can be written as

$$q^{-(k_1+\cdots+k_{2\ell})/2} \left(\sum_{\substack{m|(k_1,k_{\ell+1}) \\ mp|e_1h_1k_1+e_{\ell+1}h_{\ell+1}k_{\ell+1}}} \pi(m) m^2 \cdots \sum_{\substack{m|(k_\ell,k_{2\ell}) \\ mp|e_\ell h_\ell k_\ell+e_{2\ell}h_{2\ell}k_{e\ell}}} \pi(m) m^2 \right) + S(k_1, \dots, k_n)$$

where $S(k_1, \dots, k_n)$ is a sum of terms in $E_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$.

The case of $n = 2\ell + 1$ follows similarly, taking into account that one has to multiply by the factor $e_{p,k_n} q^{-k_n/2} \sum_{\substack{m|k_n \\ mp|ek_n}} \pi(m) m$. □

We now compute

$$\left\langle S^{\pm}(K, f, \psi^{h_1}) \dots S^{\pm}(K, f, \psi^{h_n}) \right\rangle = \sum_{\substack{k_1,\dots,k_n=1 \\ e_1,\dots,e_n=\pm 1}}^{K} I_K^{\pm}(e_1 k_1) \dots I_K^{\pm}(e_n k_n) M_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}.$$

We will use $K = cd$ where $0 < c < 1/n$. Then, $k_i \le K$ implies that $k_1 + \cdots + k_n < d$, and we can apply the lemmas above.

Using Lemma 9.2, we have to compute sums of the type

$$\sum_{k=1}^{K} \widehat{I}_K^{\pm}(k) q^{-(1/2-1/p)k} = C(K) = O(1), \tag{12}$$

and for $r \ge 2$

$$\sum_{k_1,\dots,k_r=1}^{K} \widehat{I}_K^{\pm}(e_1 k_1) \dots \widehat{I}_K^{\pm}(e_r k_r) q^{-(k_1+\cdots+k_r)/2} \sum_{\substack{m \mid (k_1,\dots,k_r) \\ mp \mid \sum_{i=1}^{f} e_i h_i k_i}} \pi(m) m^r.$$

If $r = 2$, we have when $p \mid e_1 h_1 k_1 + e_2 h_2 k_2$

$$\begin{aligned} &\sum_{k_1,k_2=1}^{K} \widehat{I}_K^{\pm}(e_1 k_1) \widehat{I}_K^{\pm}(e_2 k_2) q^{-(k_1+k_2)/2} \sum_{\substack{m \mid (k_1,k_2) \\ mp \mid (e_1 h_1 k_1 + e_2 h_2 k_2)}} \pi(m) m^2 \\ &= \begin{cases} \frac{1}{2\pi^2} \log\left(K|\mathcal{I}|\right) + O(1) & e_1 h_1 + e_2 h_2 \equiv 0 \bmod p, \\ O(1) & \text{otherwise} \end{cases} \end{aligned} \tag{13}$$

as we computed in the proof of Theorems 7.2 and 7.3. (In those theorems we had the extra condition $mp \nmid k_1, k_2$ in the sum, but those additional terms only add an $O(1)$ to the final sum, and we can ignore them.)

For the other terms, we have

Lemma 9.3. *Let $r > 2$, then*

$$S := \sum_{k_1,\dots,k_r=1}^{K} \widehat{I}_K^{\pm}(k_1) \dots \widehat{I}_K^{\pm}(k_r) q^{-(k_1+\cdots+k_r)/2} \sum_{\substack{m \mid (k_1,\dots,k_r) \\ mp \nmid (k_1,\dots,k_r)}} \pi(m) m^r = O(1)$$

Proof. Suppose for the moment that $k_1 \ge \cdots \ge k_r$. If $k_1 = k_r$, we have

$$\sum_{\substack{m \mid (k_1,\dots,k_r) \\ mp \nmid (k_1,\dots,k_r)}} \pi(m) m^f = O\left(k_1^r q^{k_1}\right).$$

If $k_1 = 2k_r$, and all the other k_i are equal to k_1 or k_r, we have

$$\sum_{\substack{m \mid (k_1,\dots,k_r) \\ mp \nmid (k_1,\dots,k_r)}} \pi(m) m^r = O\left(k_1^r q^{k_1/2}\right).$$

In all the other cases,

$$\sum_{\substack{m \mid (k_1,\dots,k_r) \\ mp \nmid (k_1,\dots,k_r)}} \pi(m) m^r = O\left(k_1^r q^{k_1/3}\right).$$

Putting things together, we get

$$\begin{aligned} S &\ll \sum_{k=1}^{K} \widehat{I}_K^{\pm}(k)^r k^r q^{-(r-2)k/2} + \sum_{\ell=1}^{r-1} \sum_{k=1}^{K} \widehat{I}_K^{\pm}(2k)^{\ell} \widehat{I}_K^{\pm}(k)^{r-\ell} k^r q^{(1-r/2-\ell/2)k} \\ &\quad + \sum_{k_1,\dots,k_r=1}^{K} \widehat{I}_K^{\pm}(k_1) \dots \widehat{I}_K^{\pm}(k_r) k_1^r q^{-k_1/6-(k_2+\cdots+k_r)/2} \\ &\ll 1 \end{aligned}$$

by Proposition 5.2. □

Theorem 9.4. *For any K with $\max\{1, 1/|\mathcal{I}|\} < K < d/n$*

$$\left\langle S^{\pm}(K,f,\psi)^n \right\rangle = \begin{cases} \frac{(2\ell)!}{\ell!(2\pi^2)^\ell} \log^\ell(K|\mathcal{I}|) \left(1 + O\left(\log^{-1}(K|\mathcal{I}|)\right)\right) & n = 2\ell, \\ C \frac{(2\ell+1)!}{\ell!(2\pi^2)^\ell} \log^\ell(K|\mathcal{I}|) \left(1 + O\left(\log^{-1}(K|\mathcal{I}|)\right)\right) & n = 2\ell+1, \end{cases}$$

where C is defined in Remark 6.5.

Proof. By Lemmas 9.2 and 9.3, we observe that the leading term in $S^{\pm}(K,f,\psi)^n$ will come from the contributions $N_{n,d}^{\mathbf{k},\mathbf{e}}$. By equation (13), if $n = 2\ell$, the leading terms are of the form

$$\left(\frac{1}{2\pi^2} \log(K|\mathcal{I}|)\right)^\ell$$

and if $n = 2\ell + 1$, the leading terms are of the form

$$C \left(\frac{1}{2\pi^2} \log(K|\mathcal{I}|)\right)^\ell.$$

The final coefficient is obtained by counting the numbers of ways to choose the ℓ (or $\ell+1$) coefficients $k_i's$ with positive sign ($e_i = 1$) and to pair them with those with negative sign ($e_j = -1$).

□

As $S^{\pm}(K,f,\psi) = S^{\pm}(K,f,\bar{\psi})$, it is sufficient to study the sum of $S^{\pm}(K,f,\psi^j)$ for j up to $(p-1)/2$ rather than $p-1$.

We let

$$\delta_n(C) = \begin{cases} 1 & n = 2\ell \\ C & n = 2\ell + 1. \end{cases}$$

Theorem 9.5. *Let $\ell = \lfloor \frac{n}{2} \rfloor$. Let $0 < h_1, \ldots, h_n \leq (p-1)/2$. Then for any K with $\max\{1, 1/|\mathcal{I}|\} < K < d/n$,*

$$\left\langle S^{\pm}(K,f,\psi^{h_1}) \ldots S^{\pm}(K,f,\psi^{h_n}) \right\rangle = \delta_n(C) \frac{\Delta(h_1,\ldots,h_n)}{(2\pi^2)^\ell} \log^\ell(K|\mathcal{I}|) \left(1 + O\left(\log^{-1}(K|\mathcal{I}|)\right)\right)$$

where C is defined in Remark 6.5 *and*

$$\Delta(h_1,\ldots,h_n) = \#\{(e_1,\ldots,e_n) \in \{-1,1\}, \sigma \in \mathbb{S}_n |\, e_1 h_{\sigma(1)} + e_2 h_{\sigma(2)} \equiv \ldots, \equiv e_{2\ell-1} h_{\sigma(2\ell-1)} + e_{2\ell} h_{\sigma(2\ell)} \equiv 0 \bmod p\}$$

where $\mathbb{S}_n$ denotes the permutations of the set of n elements.

Proof. By Lemmas 9.2 and 9.3, we observe that the leading term in $S^{\pm}(K,f,\psi^{h_1}) \ldots S^{\pm}(K,f,\psi^{h_n})$ will come from the contributions $N_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}}$. By Theorem 7.3, if $n = 2\ell$, the leading terms are of the form

$$\left(\frac{1}{2\pi^2} \log(K|\mathcal{I}|)\right)^\ell$$

and if $n = 2\ell + 1$, the leading terms are of the form

$$C \left(\frac{1}{2\pi^2} \log(K|\mathcal{I}|)\right)^\ell.$$

The final coefficient is obtained by counting the numbers of ways to choose the ℓ (or $\ell+1$) coefficients k_i with positive sign ($e_i = 1$) and to pair them with k_j with negative sign ($e_j = -1$) in such a way that p divides $e_i h_i + e_j h_j$.

□

We note that if $n = 2\ell$,

$$\sum_{h_1,\ldots,h_n=1}^{(p-1)/2} \Delta(h_1,\ldots,h_n) = \frac{(p-1)^\ell (2\ell)!}{2^\ell \ell!}. \tag{14}$$

There are $\frac{(2\ell)!}{\ell!2^\ell}$ ways of choosing pairs $\{e_i, e_j\}$ (because the order does not count inside the pair). For each pair either e_i or e_j can be negative and the other one positive so there are a total 2^ℓ choices for the signs. Finally, for each pair there are $((p-1)/2)$ possible values for h_i and this determines h_j.

Recall that

$$S^\pm(K, C_f) = \sum_{j=1}^{p-1} S^\pm(K, f, \psi^j).$$

Theorem 9.6. *Assume that $K = d/\log\log(d|\mathcal{I}|)$, $d \to \infty$ and either $|\mathcal{I}|$ is fixed or $|\mathcal{I}| \to 0$ while $d|\mathcal{I}| \to \infty$. Then*

$$\frac{S^\pm(K, C_f)}{\sqrt{\frac{2(p-1)}{\pi^2}\log(d|\mathcal{I}|)}}$$

has a standard Gaussian limiting distribution when $d \to \infty$.

Proof. First we compute the moments and then we normalize them. Let $\ell = \lfloor \frac{n}{2} \rfloor$. We note that with our choice of K we have

$$\frac{\log(K|\mathcal{I}|)}{\log(d|\mathcal{I}|)} = 1 - \frac{\log\log\log(d|\mathcal{I}|)}{\log(d|\mathcal{I}|)}.$$

Therefore, we can replace $\log(K|\mathcal{I}|)$ by $\log(d|\mathcal{I}|)$ in our formulas.

Recall that $S^\pm(K, f, \psi^j) = S^\pm(K, f, \psi^{p-j})$, then

$$S^\pm(K, C_f)^n = \left(2\sum_{j=1}^{(p-1)/2} S^\pm(K, f, \psi^j)\right)^n = 2^n \sum_{j_1,\dots,j_n=1}^{(p-1)/2} S^\pm(K, f, \psi^{j_1}) \dots S^\pm(K, f, \psi^{j_n}).$$

Therefore, we can compute the moment

$$\left\langle S^\pm(K, C_f)^n \right\rangle = 2^n \sum_{j_1,\dots,j_n=1}^{(p-1)/2} \langle S^\pm(K, f, \psi^{j_1}) \dots S^\pm(K, f, \psi^{j_n}) \rangle$$

and then by Theorem 9.5 this is asymptotic to

$$\frac{2^n \delta_n(C)}{(2\pi^2)^\ell} \log^\ell(d|\mathcal{I}|) \sum_{j_1,\dots,j_n=1}^{(p-1)/2} \Delta(j_1, \dots, j_n).$$

Finally we use equation (14) to conclude that when $n = 2\ell$,

$$\left\langle S^\pm(K, C_f)^n \right\rangle = \frac{2^n (p-1)^\ell (2\ell)!}{2^\ell \ell! (2\pi^2)^\ell} \log^\ell(d|\mathcal{I}|) = \frac{(2\ell)!}{\ell! \pi^{2\ell}} (p-1)^\ell \log^\ell(d|\mathcal{I}|)$$

and the variance is asymptotic to $\frac{2(p-1)}{\pi^2}\log(d|\mathcal{I}|)$.

Hence the normalized moment converges to 0 for n odd and for n even,

$$\lim_{d\to\infty} \frac{\left\langle S^\pm(K, C_f)^{2\ell} \right\rangle}{\left(\sqrt{\frac{2(p-1)}{\pi^2}\log(d|\mathcal{I}|)}\right)^{2\ell}} = \frac{(2\ell)!}{\ell! 2^\ell}.$$

□

10. Proof of main theorem

We prove in this section that

$$\frac{N_{\mathcal{I}}(C_f) - 2g|\mathcal{I}|}{\sqrt{(2(p-1)/\pi^2)\log(d|\mathcal{I}|)|}}$$

converges in mean square to

$$\frac{S^\pm(K, C_f)}{\sqrt{(2(p-1)/\pi^2)\log(d|\mathcal{I}|)}}.$$

Then, using Theorem 9.6, we get the result of Theorem 1.1 since convergence in mean square implies convergence in distribution.

Lemma 10.1. *Assume that $K = d/\log\log(d|\mathcal{I}|)$, $d \to \infty$ and either $|\mathcal{I}|$ is fixed or $|\mathcal{I}| \to 0$ while $d|\mathcal{I}| \to \infty$. Then*

$$\left\langle \left| \frac{N_{\mathcal{I}}(C_f) - (d-1)(p-1)|\mathcal{I}| + S^{\pm}(K, C_f)}{\sqrt{(2(p-1)/\pi^2)\log(d|\mathcal{I}|)}} \right|^2 \right\rangle \to 0$$

Proof. From equation (10) from Section 6, using the Beurling-Selberg polynomials and the explicit formula (Lemma 3.1), we deduce that

$$\frac{-(p-1)(d-1)}{K+1} \leq N_{\mathcal{I}}(C_f) - (p-1)(d-1)|\mathcal{I}| + S^-(K, C_f) \leq S^-(K, C_f) - S^+(K, C_f) + \frac{(p-1)(d-1)}{K+1}$$

and

$$\frac{-(p-1)(d-1)}{K+1} \leq -N_{\mathcal{I}}(C_f) + (p-1)(d-1)|\mathcal{I}| - S^+(K, C_f) \leq S^-(K, C_f) - S^+(K, C_f) + \frac{(p-1)(d-1)}{K+1}.$$

Using these two inequalities to bound the absolute value of the central term, we obtain

$$\begin{aligned}
& \left\langle \left(N_{\mathcal{I}}(C_f) - (p-1)(d-1)|\mathcal{I}| + S^{\pm}(K, C_f)\right)^2 \right\rangle \\
\leq \quad & \max\left\{ \left(\frac{(p-1)(d-1)}{K+1} \right)^2, \left\langle \left(S^-(K, C_f) - S^+(K, C_f) + \frac{(p-1)(d-1)}{K+1} \right)^2 \right\rangle \right\} \\
& \leq \left(\frac{(p-1)(d-1)}{K+1} \right)^2 \\
+ \quad & \max\left\{ 0, \left\langle \left(S^-(K, C_f) - S^+(K, C_f)\right)^2 \right\rangle + 2\frac{(p-1)(d-1)}{K+1} \left\langle S^-(K, C_f) - S^+(K, C_f) \right\rangle \right\}.
\end{aligned}$$

Now using the estimate in the proof of Theorem 6.1, we have that

$$\left\langle S^-(K, C_f) - S^+(K, C_f) \right\rangle \quad = \quad \left\langle S^-(K, C_f) \right\rangle - \left\langle S^+(K, C_f) \right\rangle = O(1).$$

For the remaining term we note that

$$\begin{aligned}
& \left\langle \left(S^-(K, C_f) - S^+(K, C_f)\right)^2 \right\rangle \\
= \quad & \left\langle \left(S^-(K, C_f)\right)^2 \right\rangle + \left\langle \left(S^+(K, C_f)\right)^2 \right\rangle - 2 \left\langle \sum_{j_1, j_2 = 1}^{p-1} S^-(K, f, \psi^{j_1}) S^+(K, f, \psi^{j_2}) \right\rangle.
\end{aligned}$$

By Corollary 7.4, this equals

$$\frac{4(p-1)}{\pi^2}\log(d|\mathcal{I}|) + O(1) - \frac{4(p-1)}{\pi^2}\log(d|\mathcal{I}|) + O(1) = O(1).$$

Therefore,

$$\left\langle \left(N_{\mathcal{I}}(C_f) - (p-1)(d-1)|\mathcal{I}| + S^{\pm}(K, C_f)\right)^2 \right\rangle = O\left(\left(\frac{(p-1)(d-1)}{K+1} \right)^2 \right)$$

and

$$\left\langle \left(\frac{N_{\mathcal{I}}(C_f) - (p-1)(d-1)|\mathcal{I}| + S^{\pm}(K, C_f)}{\sqrt{(2(p-1)/\pi^2)\log(d|\mathcal{I}|)}} \right)^2 \right\rangle \to 0$$

when d tends to infinity and $K = d/\log\log(d|\mathcal{I}|)$. □

Remark 10.2. Proposition 1.3 is proved in a similar way. For this, one uses Theorem 9.4 to examine the moments of

$$\frac{S^{\pm}(K, f, \psi) + S^{\pm}(K, f, \bar{\psi})}{\sqrt{\frac{4}{\pi^2}\log(d|\mathcal{I}|)}} = \frac{2S^{\pm}(K, f, \psi)}{\sqrt{\frac{4}{\pi^2}\log(d|\mathcal{I}|)}}.$$

References

[BDFL10a] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Fluctuations in the number of points on smooth plane curves over finite fields. *J. Number Theory*, 130(11):2528–2541, 2010.

[BDFL10b] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Statistics for traces of cyclic trigonal curves over finite fields. *Int. Math. Res. Not. IMRN*, (5):932–967, 2010.

[BDFL11] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Biased statistics for traces of cyclic p-fold covers over finite fields. In *WIN–Women in Numbers: Research Directions in Number Theory*, volume 60 of *Fields Institute Communications Series*, pages 121–143. Amer. Math. Soc., Providence, RI, 2011.

[BK] Alina Bucur and Kiran Kedlaya. The probability that a complete intersection is smooth. *Journal de Theorie des Nombres de Bordeaux*. To appear, arXiv:1003.5222v2.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[Ent] Alexei Entin. On the distribution of zeroes of Artin-Schreier L-functions. Preprint, arXiv:1105.5517.

[FR10] Dmitry Faifman and Zeév Rudnick. Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field. *Compos. Math.*, 146(1):81–101, 2010.

[Kat87] Nicholas M. Katz. On the monodromy groups attached to certain families of exponential sums. *Duke Math. J.*, 54(1):41–56, 1987.

[Kat90] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.

[KR09] Pär Kurlberg and Zeév Rudnick. The fluctuations in the number of points on a hyperelliptic curve over a finite field. *J. Number Theory*, 129(3):580–587, 2009.

[Mon94] Hugh L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[PZ11] Rachel Pries and Hui June Zhu. The p-rank stratification of Artin-Schreier curves. *Ann. Inst. Fourier (Grenoble)*, 61, 2011.

[RLW11] Antonio Rojas-León and Daqing Wan. Improvements of the Weil bound for Artin-Schreier curves. *Math. Ann.*, 351(2):417–442, 2011.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Woo] Melanie Matchett Wood. The distribution of the number of points on trigonal curves over $\mathbb{F}_q$. Preprint, arXiv:1108.2526v1.

[Xio10a] Maosheng Xiong. The fluctuations in the number of points on a family of curves over a finite field. *J. Théor. Nombres Bordeaux*, 22(3):755–769, 2010.

[Xio10b] Maosheng Xiong. Statistics of the zeros of zeta functions in a family of curves over a finite field. *Int. Math. Res. Not. IMRN*, (18):3489–3518, 2010.

Alina Bucur: Department of Mathematics, University of California at San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093, USA

E-mail address: alina@math.ucsd.edu

Chantal David: Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montreal, QC H3G 1M8, Canada

E-mail address: cdavid@mathstat.concordia.ca

Brooke Feigon: Department of Mathematics, The City College of New York, CUNY, NAC 8/133, New York, NY 10031, USA

E-mail address: bfeigon@ccny.cuny.edu

Matilde Lalín: Département de mathématiques et de statistique, Université de Montréal. CP 6128, succ. Centre-ville. Montreal, QC H3C 3J7, Canada

E-mail address: mlalin@dms.umontreal.ca

Kaneenika Sinha: Department of Mathematics and Statistics, Indian Institute of Science Education and Research, Kolkata PO: BCKV Main Campus, Mohanpur - 741252, Nadia, West Bengal, India

E-mail address: kaneenika@iiserkol.ac.in