# STATISTICS FOR ORDINARY ARTIN-SCHREIER COVERS AND OTHER $p$-RANK STRATA

ALINA BUCUR, CHANTAL DAVID, BROOKE FEIGON, MATILDE LALÍN

Abstract. We study the distribution of the number of points and of the zeroes of the zeta function in different $p$-strata of Artin-Schreier covers over $\mathbb{F}_q$ when $q$ is fixed and the genus goes to infinity. The $p$-strata considered include the ordinary family, the whole family and the family of curves with $p$-rank equal to $p-1$. While the zeta zeroes always approach the standard Gaussian distribution, the number of points over $\mathbb{F}_q$ has a distribution that varies with the specific family.

## Contents



## 1. Introduction

Besides their central place in number theory, algebraic curves over finite fields also play a pivotal role in applications via such fields as cryptography and error-correcting codes. In both theory and applications, a key property of an algebraic curve over a finite field is its *zeta function*, which determines and is determined by the number of points on the curve over the finite extensions of the base field. These zeta functions exhibit a strong analogy with other zeta functions occurring in number theory, such as the Riemann zeta function, with the added benefit that the analogue of the Riemann hypothesis is known by results of Weil.

In addition to studying curves individually, it is also profitable to study curves in families and ask aggregate questions over families. Historically, this generally involved varying the finite field, as in the work of Deligne. More recently, a series of results have emerged in which the finite field is fixed and other geometric parameters are allowed to vary. Examples include the work Kurlberg and Rudnick [KR09] that studies the distribution of the number of points on hyperelliptic curves as the genus grows. Similar statistics for the number of points

*Date*: April 16, 2013.

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 11M50, 14G15.

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

have been computed for cyclic $\ell$-covers of the projective line [BDFL10b, BDFL11, Xio10a], plane curves [BDFL10a], complete intersections in projective spaces [BK], general trigonal curves [Woo12], superelliptic curves [CWZ], curves on Hirzebruch surfaces [EW], and a subfamily of Artin-Schreier covers [Ent12].

A finer statistic for these curves is the distribution of the zeroes of the zeta function. (Note that the distribution of the points can be easily deduced from the distribution of the zeroes.) The problem of the distribution of the zeroes in the global and mesoscopic regimes was considered by Faifman and Rudnick [FR10] for hyperelliptic curves while [Xio10b], [Xio], and [BDFLS] treat the cases of cyclic $\ell$-covers, abelian covers of algebraic curves, and Artin-Schreier covers respectively. On the other hand, Entin [Ent12] uses the distributions of the number of points of a subfamily of Artin-Schreier covers to obtain some partial results towards the pair correlation problem for the zeroes.

Artin-Schreier curves represent a special family because they cannot be uniformly obtained by base-changing a scheme defined over $\mathbb{Z}$. This is intimately related to the fact that their zeta function has an expression in terms of *additive* characters of $\mathbb{F}_p$, and not in terms of multiplicative characters as is the case for the family of hyperelliptic curves and cyclic $\ell$-covers. On the other hand, the factor corresponding to a fixed additive character has a nice description as an exponential sum (3), which allows one to do a fair number of concrete computations. For instance, they can sometimes be used to show that the Weil bound on the number of points is sharp (especially in the supersingular case [Gar05, GV92]).

The $p$-rank induces a stratification on the moduli space of Artin-Schreier covers of genus $\mathfrak{g}$. We would like to remark that this stratification is not specific to the Artin-Schreier covers. Perhaps the best known example is the case of elliptic curves. The moduli space of elliptic curves only has two $p$-strata – $p$-rank 0 (ordinary) and $p$-rank 1 (supersingular) – and these two classes of elliptic curves behave fundamentally differently in many aspects. The ordinary stratum is Zariski dense in the moduli space, but there are only finitely many supersingular $\bar{\mathbb{F}}_q$-points in the moduli space of elliptic curves.

In the case of the Artin-Schreier covers, the picture is more complicated, as there are many intermediate strata besides the $p$-rank 0 and the maximal $p$-rank stratum. But it is still the case that the $p$-rank 0 stratum is the smallest stratum in the moduli space $\mathcal{AS}_{\mathfrak{g}}$ of Artin-Schreier covers of genus $\mathfrak{g}$. However, the supersingular locus is strictly contained in this stratum and it is not easy to locate the supersingular covers among those with $p$-rank 0. (See [Zhu].) On the other hand, the maximal $p$-rank stratum has the highest dimension. Whenever the ordinary locus is nonempty (i.e. there are covers with $p$-rank equal to the genus), the ordinary locus is irreducible. As it is noted in [PZ11, Example 2.9], in the case of $p \geq 3$ that we are interested in, the ordinary locus is nonempty whenever $2\mathfrak{g}/(p-1)$ is even. Otherwise, we can still talk about the stratum of maximal $p$-rank, but it will not be irreducible; the maximal rank will be strictly smaller than the genus (namely equal to $\mathfrak{g} - \frac{p-1}{2}$), and there is no ordinary locus.

Fix a finite field $\mathbb{F}_q$ of odd characteristic $p$. An Artin-Schreier cover is an Artin-Schreier curve for which we fix an automorphism of order $p$ and an isomorphism between the quotient and $\mathbb{P}^1$. Concretely, an $\mathbb{F}_q$-point of the moduli space of Artin-Schreier covers of genus $\mathfrak{g}$ consists, up to $\mathbb{F}_q$-isomorphism, of a curve of genus $\mathfrak{g}$ with affine model

$$C_f : y^p - y = f(x),$$

where $f(x) \in \mathbb{F}_q(x)$ is a rational function, together with the automorphism $y \mapsto y + 1$.

Let $p_1, \dots, p_{r+1}$ be the set of poles of $f(x)$ and let $d_j$ be the order of the pole $p_j$. Then the genus of $C_f$ is given by

$$\mathfrak{g}(C_f) = \frac{p-1}{2}\left(-2 + \sum_{j=1}^{r+1}(d_j + 1)\right) = \frac{p-1}{2}\left(r - 1 + \sum_{j=1}^{r+1} d_j\right). \tag{1}$$

(See [PZ11, Lemma 2.6].) The $p$-rank is the integer $s$ such that the cardinality of $\mathrm{Jac}(C_f)[p](\overline{\mathbb{F}_q})$ is $p^s$; by the Deuring-Shafarevich formula, we have $s = r(p-1)$ for some integer $r \geq 0$. We will write $\mathcal{AS}_{\mathfrak{g},s}$ for the stratum with $p$-rank equal to $s$ of the moduli space $\mathcal{AS}_{\mathfrak{g}}$. For example, $s = 0$ corresponds to one pole, which can always be moved to infinity. This corresponds to the case in which $f(x)$ is a polynomial that was considered in [Ent12, BDFLS]. However, this case only corresponds to a piece, namely $\mathcal{AS}_{\mathfrak{g},0}$, of the whole moduli space $\mathcal{AS}_{\mathfrak{g}}$ of Artin-Schreier covers of genus $\mathfrak{g}$. The next case is $s = p-1$, corresponding to two poles, which can always be moved to zero and infinity. Thus, this involves the case in which $f(x)$ is a

Laurent polynomial and its corresponding piece in the moduli space is $\mathcal{AS}_{\mathfrak{g},p-1}$. For details on the moduli space of Artin-Schreier curves and the $p$-rank stratification, we refer the reader to [PZ11].

The main object of this paper is the study of the distribution of the number of points and zeta zeroes for the ordinary locus $\mathcal{AS}_{\mathfrak{g},\mathfrak{g}}$ which only appears when $2\mathfrak{g}/(p-1)$ is even. In addition, we treat the cases of $\mathcal{AS}_{\mathfrak{g},p-1}$ of covers with $p$-rank equal to $p-1$ and the whole family $\mathcal{AS}_{\mathfrak{g}}$. More precisely, we have the following results.

**Theorem 1.1.** (1) *Assume that $2\mathfrak{g}/(p-1)$ is even. The average number of $\mathbb{F}_{q^k}$-points on an ordinary Artin-Schreier cover in $\mathcal{AS}_{\mathfrak{g},\mathfrak{g}}(\mathbb{F}_q)$ is*

$$\begin{cases} q^k+1+O\left(q^{(-1/2+\varepsilon)(1+\mathfrak{g}/(p-1))+2k}\right) & p\nmid k, \\ q^k+1+\frac{p-1}{1+q^{-1}-q^{-2}}+\sum_{u\mid\frac{k}{p}}\frac{p-1}{1+q^{-u}-q^{-2u}}\sum_{e\mid u}\mu(e)q^{u/e}+O\left(q^{(-1/2+\varepsilon)(1+\mathfrak{g}/(p-1))+2k}\right) & p\mid k. \end{cases}$$

(2) *The average number of $\mathbb{F}_{q^k}$-points on an Artin-Schreier cover in $\mathcal{AS}_{\mathfrak{g}}(\mathbb{F}_q)$ whose ramification divisor is supported at $r+1$ points and has degree $d$ is*

$$\begin{cases} q^k+1+O\left(q^{(\varepsilon-1)d+2k}\right) & p\nmid k, \\ q^k+1+(p-1)q^{k/p}+\frac{p-1}{1+q^{-1}}-(p-1)\sum_{u\mid\frac{k}{p}}\frac{1}{1+q^{u}}\sum_{e\mid u}\mu(e)q^{u/e}+O\left(q^{(\varepsilon-1)d+2k}\right) & p\mid k. \end{cases}$$

(3) *The average number of $\mathbb{F}_{q^k}$-points on an Artin-Schreier cover in $\mathcal{AS}_{\mathfrak{g},p-1}(\mathbb{F}_q)$ is*

$$\begin{cases} q^k+1 & p\nmid k, \\ q^k+1+(p-1)(q^{k/p}-1) & p\mid k. \end{cases}$$

By Weil's conjectures, the zeta function of $C_f$,

$$Z_{C_f}(u)=\exp\left(\sum_{k=1}^{\infty}N_k(C_f)\frac{u^k}{k}\right),$$

where $N_k(C_f)$ is the number of points on $C_f$ defined over $\mathbb{F}_{q^k}$, can be written as

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

where $P_{C_f}(u)$ is a polynomial of degree $2\mathfrak{g}=(p-1)(\Delta-1)$ with $\Delta=\left(r+\sum_{j=1}^{r+1}d_j\right)$. Using Lemma 2.1 and the additive characters of $\mathbb{F}_p$ to write a formula for $N_k(C_f)$, it follows easily that

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

where the product is taken over the *non-trivial* additive characters $\psi$ of $\mathbb{F}_p$, and $L(u,f,\psi)$ are certain $L$-functions (given later by (3)). Understanding the distribution of the zeroes of $Z_{C_f}(u)$ amounts to understanding the distribution of the zeroes of each of the $L(u,f,\psi)$ as $f$ runs in the relevant family of rational functions and the genus goes to infinity.

If we write

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

we have that $\alpha_j(f,\psi)=\sqrt{q}e^{2\pi i\theta_j(f,\psi)}$ 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 in the family. For an interval $\mathcal{I}\subset[-1/2,1/2)$, let

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

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 non-trivial subinterval $\mathcal{I}$ is asymptotic to $2\mathfrak{g}|\mathcal{I}|$, has variance asymptotic to $\frac{2(p-1)}{\pi^2}\log(\mathfrak{g}|\mathcal{I}|)$, and properly normalized has a Gaussian distribution.

**Theorem 1.2.** *Fix a finite field $\mathbb{F}_q$ of characteristic $p$. Let $\mathcal{AS}$ denote the family of Artin-Schreier covers, ordinary Artin-Schreier covers, or the $p$-rank $p-1$ Artin-Schreier covers. Then for any real numbers $a < b$ and $0 < |\mathcal{I}| < 1$ either fixed or $|\mathcal{I}| \to 0$ while $\mathfrak{g}|\mathcal{I}| \to \infty$,*

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

This result is analogous to what was obtained in [BDFLS] for $p$-rank 0 Artin-Schreier covers and is compatible with the philosophy of Katz and Sarnak [KS99]. In fact, Katz [Kat87] shows that the monodromy of the $L$-functions defined in (3) is given by $\mathrm{SL}\left(2\mathfrak{g}/(p-1)\right)$ when the dimension of the moduli space is big enough. Since the dimension grows with the genus, this occurs when $\mathfrak{g}$ is big enough. In particular, [DS94] implies that the limiting distribution as $\mathfrak{g} \to \infty$ is Gaussian.

## 2. Basic Artin-Schreier theory

Fix an odd prime $p$ and let $\mathbb{F}_q$ be a finite field of characteristic $p$ with $q$ elements. We consider, up to $\mathbb{F}_q$-isomorphism, pairs of curves with affine model

$$C_f : y^p - y = f(x)$$

with $f(x)$ a rational function together with the automorphism $y \mapsto y + 1$.

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 $\mathbb{F}_q$).

**Lemma 2.1.** *For each $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^n})$, the points in the fiber above $\alpha$ on the curve $C_f : y^p - y = f(x)$ are defined over $\mathbb{F}_{q^n}$ and the number of such points is*

$$\begin{cases} 1 & \text{if } f(\alpha) = \infty, \\ \\ p & \text{if } f(\alpha) \in \mathbb{F}_{q^n} \text{ with } \mathrm{tr}_n f(\alpha) = 0, \\ \\ 0 & \text{if } f(\alpha) \in \mathbb{F}_{q^n} \text{ with } \mathrm{tr}_n f(\alpha) \neq 0. \end{cases}$$

*Proof.* This is a simple application of Hilbert's Theorem 90. ☐

Let $\psi_k$, $k = 0, \dots, p-1$ be the additive characters of $\mathbb{F}_p$ given by

$$\psi_k(a) = e^{2\pi i k a/p}, \quad k = 0, \dots, p-1.$$

For each rational function $f \in \mathbb{F}_q(X)$ and non-trivial character $\psi$, we also define

$$S_n(f, \psi) = \sum_{\substack{x \in \mathbb{P}^1(\mathbb{F}_{q^n}) \\ f(x) \neq \infty}} \psi(\mathrm{tr}_n(f(x))).$$

Then, using the fact that for any $a \in \mathbb{F}_p$,

$$\sum_{k=0}^{p-1} \psi_k(a) = \begin{cases} p & a = 0, \\ 0 & a \neq 0, \end{cases}$$

it is easy to check that

$$P_{C_f}(u) = \prod_{\psi \neq \psi_0} L(u, f, \psi)$$

where

$$L(u,f,\psi)=\exp\left(\sum_{n=1}^{\infty}S_n(f,\psi)\frac{u^n}{n}\right). \tag{3}$$

Let $\mathcal{S}=\mathbb{F}_q[X,Z]$ be the homogeneous coordinate ring of $\mathbb{P}^1$ and denote $\mathcal{S}_d$ the $\mathbb{F}_q$-subspace of $\mathcal{S}$ of homogeneous polynomials of degree $d$. Notice that $\mathcal{S}_d$ contains the 0 polynomial and its size is exactly $q^{d+1}$.

Since Artin-Schreier covers can be embedded in $\mathbb{P}^1\times\mathbb{P}^1$, we can think of $C_f$ as the cover given by

$$C_{g,h}:y^p-y=\frac{g(X,Z)}{h(X,Z)},$$

where the fraction on the right hand side is obtained by homogenizing $f(x)$ in the usual way.

Given $f\in\mathcal{S}_d$, we will denote by $f^*(X)\in\mathbb{F}_q[X]$ the non-homogeneous polynomial resulting from $f(X,Z)$ by setting $Z=1$. We observe that $f^*$ is polynomial of degree at most $d$. Similarly, let $f_*(Z)\in\mathbb{F}_q[Z]$ be the non-homogeneous polynomial resulting from $f(X,Z)$ by setting $X=1$.

Given $\alpha=[\alpha_X:\alpha_Z]\in\mathbb{P}^1(\mathbb{F}_{q^k})$ and $h\in\mathcal{S}_d$ the value of $h(\alpha)$ can be zero or nonzero but if it is nonzero, it is not well defined. When we want to discuss an actual nonzero value we will be talking about $h^*(\alpha):=h(\alpha_X/\alpha_Z,1)$ which is defined for $\alpha\neq[1:0]=\infty$ and $h_*(\alpha):=h(1,\alpha_Z/\alpha_X)$ which is defined for $\alpha\neq[0:1]=0$.

We recall that the rational function $\frac{g}{h}$ can be evaluated in $[\alpha_X:\alpha_Z]$ as long as $g,h\in\mathcal{S}_d$ and $(g(\alpha_X,\alpha_Z),h(\alpha_X,\alpha_Z))\neq(0,0)$.

We now proceed to explicitly describe the families to be considered. The ordinary case occurs when the $p$-rank is maximal, in other words, when $r$ is maximal. For a given genus $\mathfrak{g}$, this happens when $d_i=1$ in formula (1) and $2\mathfrak{g}=(p-1)2r$. (Notice once again that this imposes a restriction on the possible values for the genus, as $2\mathfrak{g}/(p-1)$ must be even.) Thus, $f(x)$ is a rational function with exactly $r+1$ simple poles. This corresponds to the fact that $g(X,Z)$ and $h(X,Z)$ are both homogeneous polynomials of degree $r+1$ with no common factors and $h(X,Z)$ is square-free.

We let

$$\mathcal{F}_d^{\mathrm{ord}}=\left\{(g(X,Z),h(X,Z)):g(X,Z),h(X,Z)\in\mathcal{S}_d,h\text{ square-free},(g,h)=1\right\},$$

with the understanding that $d=r+1$.

As $(g,h)$ range over $\mathcal{F}_d^{\mathrm{ord}}$, the cover $C_{g,h}$ ranges over each $\mathbb{F}_q$-point of $\mathcal{AS}_{\mathfrak{g},\mathfrak{g}}$ exactly $q-1$ times. Thus, our problem becomes the study of statistics for $C_{g,h}$ as $(g,h)$ varies over $\mathcal{F}_d^{\mathrm{ord}}$ and $d$ tends to infinity.

We will work with the full family of covers in $\mathcal{AS}_{\mathfrak{g}}$ as well. In this case we do not have the restriction of simple poles but we still require $g(X,Z)$ and $h(X,Z)$ not to have common factors.

$$\mathcal{F}_d^{\mathrm{full}}=\left\{(g(X,Z),h(X,Z)):g(X,Z),h(X,Z)\in\mathcal{S}_d,(g,h)=1\right\}.$$

We will then study the statistics as $d$ goes to infinity which is the same as $\mathfrak{g}$ going to infinity provided that the number of poles $r+1$ remains bounded.

Finally, we will consider another family given as follows. We say that $h$ has factorization type $v=(r_1^{d_{1,1}},\dots,r_1^{d_{1,\ell_1}},\dots,r_m^{d_{m,1}},\dots,r_m^{d_{m,\ell_m}})$ if

$$h=P_{1,1}^{d_{1,1}}\cdots P_{1,\ell_1}^{d_{1,\ell_1}}\cdots P_{m,1}^{d_{m,1}}\cdots P_{m,\ell_m}^{d_{m,\ell_m}},$$

where the $P_{i,j}$ are distinct irreducible polynomials of degree $r_i$ and $r_i\neq r_j$ if $i\neq j$. Thus the degree of $h$ is given by $d=\sum_{i=1}^m r_i\sum_{j=1}^{\ell_i}d_{i,j}$.

Let

$$\mathcal{F}_d^{v}=\{(g(X,Z),h(X,Z)):g(X,Z),h(X,Z)\in\mathcal{S}_d,(g,h)=1,h\text{ has factorization type }v\}.$$

In this case, formula (1) implies $2\mathfrak{g}=(p-1)\left(d-2+\sum_{i=1}^m\ell_ir_i\right)$. Here $\sum_{i=1}^m\ell_ir_i$ represents the number of poles and the $p$-rank is given by $(p-1)\left(\sum_{i=1}^m\ell_ir_i-1\right)$. We will assume the parameters $m$, $r_i$'s and $\ell_i$'s to be fixed. This implies that the covers considered are all in the same $p$-rank. However, in general, the set of the covers considered does not constitute the whole $p$-rank stratum. We will study the statistics as $d$ goes to infinity which is the same as $\mathfrak{g}$ going to infinity with a bound on the number of poles.

This family includes some important particular cases. Suppose that $v = (1^d)$. This corresponds to the case of only one pole of multiplicity $d$. This pole can always be moved to infinity (i.e., $h(X, Z) = Z^d$). After dehomogenizing with $Z = 1$, this gives the family of $p$-rank 0 covers $\mathcal{AS}_{\mathfrak{g},0}$:

$$\mathcal{F}_d^{\mathrm{rank}\,0} = \{g(x) : \deg(g) = d\}.$$

The statistics for this family were studied in [Ent12, BDFLS].

Another interesting case is with $v = (1^{d_1}, 1^{d_2})$. In this case we have two poles that can always be moved to zero and infinity (i.e., $h(X, Z) = X^{d_1} Z^{d_2}$). After dehomogenizing with $Z = 1$, this gives the family of $p$-rank $p-1$ covers $\mathcal{AS}_{\mathfrak{g},p-1}$ indexed by Laurent polynomials with bidegree $(d_2, d_1)$:

$$\mathcal{F}_{d_1+d_2}^{\mathrm{rank}\,p-1} = \{g(x)/x^{d_1} : \deg(g) = d_2\}.$$

The statistics for this family is very similar to the statistics for $\mathcal{AS}_{\mathfrak{g},0}$.

We will need to compute the number of elements in a family that satisfy certain values at certain points. The following notation will be useful.

**Definition 2.2.** *Let $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$. Let $\mathcal{F}_d$ be any of the families under consideration. We define*

$$\mathcal{F}_d(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n) = \{(g, h) \in \mathcal{F}_d : (\beta_{i,X} h - \beta_{i,Z} g)(\alpha_i) = 0, 1 \le i \le n\}.$$

We remark that when $\beta \neq \infty$ we identify $\beta = [\beta_X : \beta_Z]$ with $\frac{\beta_X}{\beta_Z} \in \mathbb{F}_{q^k}$ thus

$$(\beta_X h - \beta_Z g)(\alpha) = 0 \Longleftrightarrow \frac{g(\alpha)}{h(\alpha)} = \beta.$$

A particularly useful case is $\mathcal{F}_d(\alpha, \beta)$. We remark that this value does not depend on the value of $\beta$, provided that $\beta \neq \infty$, as we prove below.

**Lemma 2.3.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. Let $\beta \in \mathbb{F}_{q^u}$. Let $\mathcal{F}_d$ be any of the families under consideration. Then*

$$|\mathcal{F}_d(\alpha, \beta)| = |\mathcal{F}_d(\alpha, 0)|.$$

*Proof.* Recall that

$$\mathcal{F}_d(\alpha, \beta) = \{(g, h) \in \mathcal{F}_d : \beta_X h(\alpha) - \beta_Z g(\alpha) = 0\}.$$

Now let $g' = \beta_X h - \beta_Z g$. Since $\beta_Z \neq 0$ we have that $(g, h) = 1$ is equivalent to $(g', h) = 1$. Then $(g, h) \in \mathcal{F}_d(\alpha, \beta)$ if and only if $(g', h) \in \mathcal{F}_d(\alpha, 0)$. □

## 3. The ordinary case

In this section, we consider the family

$$\mathcal{F}_d^{\mathrm{ord}} = \{(g(X, Z), h(X, Z)) : g(X, Z), h(X, Z) \in \mathcal{S}_d, h \text{ square-free}, (g, h) = 1\}.$$

3.1. **Heuristics.** We want to calculate, for given $\alpha = [\alpha_X : \alpha_Z], \beta = [\beta_X : \beta_Z] \in \mathbb{P}^1(\mathbb{F}_{q^u})$ such that $\deg \alpha = u$, the probability that

$$(\beta_X h - \beta_Z g)(\alpha_X, \alpha_Z) = 0 \tag{4}$$

as $(g, h) \in \mathcal{F}_d^{\mathrm{ord}}$.

Locally at $\alpha$ this means that we want to look at pairs $(g^*, h^*)$ such that $(m_\alpha^*)^2 \nmid h^*$ (where $m_\alpha^* \in \mathbb{F}_q[X]$ denotes the minimal polynomial of $\alpha$ over $\mathbb{F}_q$) and $(g^*(\alpha), h^*(\alpha)) \not\equiv (0, 0) \pmod{(m_\alpha^*)^2}$.

Therefore

$$(g^*, h^*) \equiv (\gamma_1 + \delta_1 m_\alpha, \gamma_2 + \delta_2 m_\alpha) \pmod{(m_\alpha^*)^2},$$

with $\gamma_i, \delta_i \in \mathbb{F}_q[X]$, and if they are nonzero, $\deg \gamma_i, \deg \delta_i < u$. In addition, the conditions at $\alpha$ imply that $(\gamma_1, \gamma_2) \neq (0, 0)$ and $(\gamma_2, \delta_2) \neq (0, 0)$.

For each $\gamma_2 \neq 0$, there are $q^u$ choices for each of the other parameters, thus $q^{3u}(q^u - 1)$ total possibilities. If $\gamma_2 = 0$, then there are $q^u - 1$ choices for each of $\gamma_1$ and $\delta_2$, and $q^u$ choices for $\delta_1$, for a total of $q^u(q^u - 1)^2$ possibilities.

This yields a total of $q^u(q^u - 1)(q^{2u} + q^u - 1)$ possibilities for $\left(g^* \pmod{(m_\alpha^*)^2}, h^* \pmod{(m_\alpha^*)^2}\right)$.

Now if $\beta = [1:0] = \infty$, condition (4) reduces to $h^*(\alpha) = 0 \iff \gamma_2 = 0$. This leaves $q^u - 1$ choices for $\gamma_1$ and $\delta_2$ respectively and $q^u$ choices for $\delta_1$. Thus the probability that $g/h \in \mathcal{F}_d^{\mathrm{ord}}$ takes the value $\infty$ at a given point $\alpha$ is

$$\frac{q^u(q^u-1)^2}{q^u(q^u-1)(q^{2u}+q^u-1)} = \frac{q^{-u}(1-q^{-u})}{1+q^{-u}-q^{-2u}}.$$

In all other cases, including $\beta = 0$, we must have $h^*(\alpha) \neq 0$. So there are $q^u - 1$ choices for $\gamma_2$. Once we know $\gamma_2$, equation (4) fixes $\gamma_1(\alpha)$ (and therefore $\gamma_1$, since its degree is less than $u$), and we have $q^u$ choices for each of $\delta_1, \delta_2$. Thus the probability $g/h \in \mathcal{F}_d^{\mathrm{ord}}$ takes the value $\beta \neq \infty$ at a given point $\alpha$ is

$$\frac{q^{2u}(q^u-1)}{q^u(q^u-1)(q^{2u}+q^u-1)} = \frac{q^{-u}}{1+q^{-u}-q^{-2u}}.$$

Then, the heuristic confirms the result of Proposition 3.10, and the expected number of points of Theorem 1.1 for the family $\mathcal{F}_d^{\mathrm{ord}}$.

3.2. **The number of covers with local conditions.** In this subsection, we are going to compute the proportion of polynomials with certain fixed values. We will obtain the size of the family and the expected number of points as corollaries.

Unless otherwise indicated, we fix $\alpha_1, \dots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \dots, u_n$ over $\mathbb{F}_q$ and $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$ (i.e. none of the $\beta_i$'s is $\infty$). Also, $\beta_1, \dots, \beta_\ell$ are not zero, and $\beta_{\ell+1} = \cdots = \beta_n = 0$. Finally, none of the $\alpha_i$ are conjugate to each other, i.e. all the minimal polynomials $m_{\alpha_i}$ are distinct.

We start by making the following observation.

**Remark 3.1.** If $\alpha = [\alpha : 1] \in \mathbb{F}_{q^k}$ has degree $u$ over $\mathbb{F}_q$, then the map $\mathcal{S}_d \to \mathbb{F}_{q^u}, h \mapsto h^*(\alpha)$ is a linear map of $\mathbb{F}_q$-vector spaces. The map is surjective as long as $d \ge u$, and in this case its kernel has dimension $d+1-u$. If $d < u$ the elements $1, \alpha, \alpha^2, \dots, \alpha^d$ are linearly independent over $\mathbb{F}_q$. Therefore the image has dimension $d+1$ and thus the kernel has dimension 0. In other words the map is injective and the preimage of any element is either empty or a point.

If $\alpha = [1:0] = \infty$, then it has degree 1 over $\mathbb{F}_q$ and a condition fixing a value for $h(\alpha)$ can be rewritten in terms of $h_*(1)$ such that it does become linear and the reasoning above applies.

**Lemma 3.2.** *Fix $\alpha_1, \dots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \dots, u_n$ over $\mathbb{F}_q$ such that none of the $\alpha_i$ are conjugate to each other, and $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$ such that $\beta_1, \dots, \beta_\ell$ are not zero, and $\beta_{\ell+1} = \cdots = \beta_n = 0$. Fix $g \in \mathcal{S}_d$ such that $g(\alpha_i) = 0$ for $\ell+1 \le i \le n$, and $g(\alpha_i) \neq 0$ for $1 \le i \le \ell$. Then we have*

$$|\{h \in \mathcal{S}_d : (\beta_{i,X}h - \beta_{i,Z}g)(\alpha_i) = 0, 1 \le i \le n\}| = \begin{cases} q^{d+1-\sum_{i=1}^{\ell} u_i} & d \ge \sum_{i=1}^{\ell} u_i, \\ \\ 0 \text{ or } 1 & \text{otherwise.} \end{cases}$$

*If $g(\alpha_i) \neq 0$ for some $\ell+1 \le i \le n$, or $g(\alpha_i) = 0$ for some $1 \le i \le \ell$ then the above set is empty.*

*Proof.* For $\beta_i \neq 0$, the condition imposed over $h$ is $h(\alpha_i) = \frac{g(\alpha_i)}{\beta_i}$ while there is no condition imposed if $\beta_i = 0$. By the Chinese Remainder Theorem, imposing all the conditions together for $\alpha_1, \dots, \alpha_\ell$ is the same as imposing a condition for $h$ modulo the product $m_{\alpha_1} \cdots m_{\alpha_\ell}$. The result then follows from Remark 3.1. □

Let $D \in \mathcal{S}_d$. In all the following, the notation $(D)$ means the ideal generated by the polynomial $D$.

**Lemma 3.3.** *Fix $\alpha_1, \dots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \dots, u_n$ over $\mathbb{F}_q$ such that none of the $\alpha_i$ are conjugate to each other, and $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$ such that $\beta_1, \dots, \beta_\ell$ are not zero, and $\beta_{\ell+1} = \cdots = \beta_n = 0$. Fix $g \in \mathcal{S}_d$ such that $g(\alpha_i) = 0$ for $\ell+1 \le i \le n$, and $g(\alpha_i) \neq 0$ for $1 \le i \le \ell$. Then we have for any $\varepsilon > 0$*

$$\left| \left\{ h \in \mathcal{S}_d : (h,g) = 1, \ \frac{g(\alpha_i)}{h(\alpha_i)} = \beta_i, 1 \le i \le n \right\} \right| = q^{d+1-\sum_{i=1}^{\ell} u_i} \prod_{(P)|(g)} (1 - |P|^{-1}) + O\left(q^{\varepsilon d}\right).$$

*If $g(\alpha_i) \neq 0$ for some $\ell+1 \le i \le n$, or $g(\alpha_i) = 0$ for some $1 \le i \le \ell$ then the above set is empty.*

*Proof.* If $g(\alpha_i) \neq 0$ for some $\ell+1 \leq i \leq n$, or $g(\alpha_i) = 0$ for some $1 \leq i \leq \ell$, then it is clear that the above set is empty. We then suppose $g(\alpha_i) = 0$ for $\ell+1 \leq i \leq n$, and $g(\alpha_i) \neq 0$ for $1 \leq i \leq \ell$.

By inclusion-exclusion and Lemma 3.2 we have

$$\begin{aligned}
\left|\left\{h \in \mathcal{S}_d : (h,g)=1, \frac{g(\alpha_i)}{h(\alpha_i)} = \beta_i\right\}\right| &= \sum_{(D)|(g)} \mu(D) \sum_{\substack{h \in \mathcal{S}_d \\ D|h,\ \frac{g(\alpha_i)}{h(\alpha_i)} = \beta_i, 1 \leq i \leq \ell}} 1 \\
&= \sum_{\substack{(D)|(g) \\ \deg D \leq d - \sum_{i=1}^{\ell} u_i}} \mu(D) q^{d+1-\deg D - \sum_{i=1}^{\ell} u_i} + \sum_{\substack{(D)|(g) \\ d - \sum_{i=1}^{\ell} u_\ell < \deg D \leq d}} O(1) \\
&= q^{d+1-\sum_{i=1}^{\ell} u_i} \sum_{(D)|(g)} \mu(D) q^{-\deg D} + \sum_{\substack{(D)|(g) \\ d - \sum_{i=1}^{\ell} u_\ell < \deg D \leq d}} O(1) \\
&= q^{d+1-\sum_{i=1}^{\ell} u_i} \prod_{(P)|(g)} (1 - |P|^{-1}) + O\left(q^{\varepsilon d}\right)
\end{aligned}$$

where $\mu$ is the Möbius function.

$\square$

**Definition 3.4.** *Let $g \in \mathcal{S}_d$. Set*

$$A_d^g = \{h \in \mathcal{S}_d : h \text{ square free and } (h,g) = 1\}.$$

*Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$. We define*

$$A_d^g(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) = \{h \in A_d^g : (\beta_{i,X} h - \beta_{i,Z} g)(\alpha_i) = 0, 1 \leq i \leq n\}.$$

**Lemma 3.5.** *Fix $\alpha_1, \ldots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \ldots, u_n$ over $\mathbb{F}_q$ such that none of the $\alpha_i$ are conjugate to each other. Let $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \leq i \leq n$ such that $\beta_1, \ldots, \beta_\ell$ are not zero, and $\beta_{\ell+1} = \cdots = \beta_n = 0$. Fix $g \in \mathcal{S}_d$ such that $g(\alpha_i) = 0$ for $\ell+1 \leq i \leq n$ and $g(\alpha_i) \neq 0$ for $1 \leq i \leq \ell$. Then*

$$|A_d^g(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)| = \frac{q^{d+1-\sum_{i=1}^{\ell} u_i}}{\zeta_q(2) \prod_{i=1}^{\ell} (1 - q^{-2u_i})} \prod_{(P)|(g)} (1 + |P|^{-1})^{-1} + O\left(q^{(1/2+\varepsilon)d}\right).$$

*If $g(\alpha_i) \neq 0$ for some $\ell+1 \leq i \leq n$, or $g(\alpha_i) = 0$ for some $1 \leq i \leq \ell$ then the above set is empty.*

*Proof.* It is clear that $A_d^g(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ is empty if the condition on the values $g(\alpha_i)$ of the lemma are not satisfied, and we then suppose that $g(\alpha_1), \ldots, g(\alpha_\ell) \neq 0$, and $g(\alpha_{\ell+1}) = \cdots = g(\alpha_n) = 0$.

By inclusion-exclusion,

$$\begin{aligned}
|A_d^g(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)| &= \sideset{}{'}\sum_{\substack{(D):(D,g)=1 \\ \deg(D) \leq d/2}} \mu(D) \left|\left\{h_1 \in \mathcal{S}_{d-2\deg(D)} : (h_1, g) = 1, \frac{g(\alpha_i)}{h_1(\alpha_i)} = D^2(\alpha_i)\beta_i\right\}\right| \\
&= q^{d+1-\sum_{i=1}^{\ell} u_i} \prod_{(P)|(g)} (1 - |P|^{-1}) \sideset{}{'}\sum_{\substack{(D):(D,g)=1 \\ \deg(D) \leq d/2}} \mu(D)|D|^{-2} + \sideset{}{'}\sum_{\substack{(D):(D,g)=1 \\ \deg D \leq d/2}} O\left(q^{\varepsilon d}\right)
\end{aligned}$$

by Lemma 3.3, where we have written $\sideset{}{'}\sum_{(D)}$ for the sum over polynomials $D$ such that $D(\alpha_i) \neq 0$ for $1 \leq i \leq \ell$.

But

$$\sideset{}{'}\sum_{(D):(D,g)=1} \mu(D)|D|^{-2s} = \prod_{\substack{(P):P\nmid g \\ P(\alpha_i) \neq 0, 1 \leq i \leq \ell}} (1 - |P|^{-2s}) = \prod_{(P):P \nmid g m_{\alpha_1} \ldots m_{\alpha_\ell}} (1 - |P|^{-2s}),$$

where we made use of the fact that $(g, m_{\alpha_i}) = 1$ since $g(\alpha_i) \neq 0$. This can be rewritten as

$$\frac{1}{\zeta_q(2s)} \prod_{(P)|(g m_{\alpha_1} \ldots m_{\alpha_\ell})} (1 - |P|^{-2s})^{-1} = \frac{1}{\zeta_q(2s) \prod_{i=1}^{\ell} (1 - q^{-2su_i})} \prod_{(P)|(g)} (1 - |P|^{-2s})^{-1}.$$

Therefore

$$\sum_{\substack{(D):(D,g)=1\\ \deg(D)\le d/2}}{}' \mu(D)|D|^{-2} = \frac{1}{\zeta_q(2)\ \prod_{i=1}^{\ell}(1-q^{-2u_i})}\prod_{(P)|(g)}(1-|P|^{-2})^{-1} + O\left(q^{-d/2}\right)$$

and

$$|A_d^g(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)| \quad = \quad \frac{q^{d+1-\sum_{i=1}^{\ell}u_i}}{\zeta_q(2)\prod_{i=1}^{\ell}(1-q^{-2u_i})}\prod_{(P)|(g)}(1+|P|^{-1})^{-1} + O\left(q^{(1/2+\varepsilon)d}\right).$$

□

**Proposition 3.6.** *Fix $\alpha_1,\dots,\alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1,\dots,u_n$ over $\mathbb{F}_q$ such that none of the $\alpha_i$ are conjugate to each other. Let $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1\le i\le n$. Then*

$$|\mathcal{F}_d^{\mathrm{ord}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)| = \frac{H(1)q^{2d+2-\sum_{i=1}^{n}u_i}}{\zeta_q(2)^2\prod_{i=1}^{n}(1+q^{-u_i}-q^{-2u_i})} + O\left(q^{(3/2+\varepsilon)d}\right),$$

*where*

$$H(1) = \prod_{(P)}\left(1+\frac{1}{(|P|+1)(|P|^2-1)}\right).$$

*Proof.* Denote by $m_{\alpha_i}$ the homogenized minimal polynomial of $\alpha_i$ over $\mathbb{F}_q$. We have

$$|\mathcal{F}_d^{\mathrm{ord}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)| = \sum_{g\in\mathcal{S}_d}|A_d^g(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)|.$$

Assume without loss of generality that $\beta_1,\dots,\beta_\ell$ are not zero, and $\beta_{\ell+1}=\dots=\beta_n=0$. By Lemma 3.5, the above sum equals

$$\begin{aligned}|\mathcal{F}_d^{\mathrm{ord}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)| &= \sum_{\substack{g\in\mathcal{S}_d\\ g(\alpha_i)\neq 0, 1\le i\le\ell\\ g(\alpha_i)=0,\ell+1\le i\le n}}\left(\frac{q^{d+1-\sum_{i=1}^{\ell}u_i}}{\zeta_q(2)\prod_{i=1}^{\ell}(1-q^{-2u_i})}\prod_{(P)|(g)}(1+|P|^{-1})^{-1} + O\left(q^{(1/2+\varepsilon)d}\right)\right)\\ &= \frac{q^{d+1-\sum_{i=1}^{n}u_i}}{\zeta_q(2)\prod_{i=1}^{\ell}(1-q^{-2u_i})}\sum_{\substack{g\in\mathcal{S}_d\\ g(\alpha_i)\neq 0, 1\le i\le\ell\\ g(\alpha_i)=0,\ell+1\le i\le n}}\prod_{(P)|(g)}(1+|P|^{-1})^{-1} + O\left(q^{(3/2+\varepsilon)d}\right).\end{aligned}$$

Set

$$b(g) = \prod_{(P)|(g)}(1+|P|^{-1})^{-1}$$

and

$$G(s) = \sum_{(g)\neq 0}\frac{b(g)}{|g|^s}.$$

Since $b(g)$ is a multiplicative function, it follows that $G(s)$ has an Euler product of the form

$$\begin{aligned}G(s) &= \prod_{(P)}\left(\sum_{k=0}^{\infty}b(P^k)|P|^{-ks}\right)\\ &= \prod_{(P)}\left(1+\frac{b(P)|P|^{-s}}{1-|P|^{-s}}\right)\\ &= \prod_{(P)}\left(1+\frac{|P|^{-s}}{(1-|P|^{-s})(1+|P|^{-1})}\right).\end{aligned}$$

Thus

$$G(s) = \frac{\zeta_q(s)}{\zeta_q(2s)}H(s),$$

where

$$H(s)=\prod_{(P)}\left(1-\frac{|P|^{-s}(1-|P|^{1-s}-|P|^{-s})}{(|P|+1)(1-|P|^{-2s})}\right),$$

which converges for $\mathrm{Re}(s)>1/2$. In addition, $G(s)$ has a simple pole at $s=1$ with residue

$$\frac{H(1)}{\zeta_q(2)\log q}=\frac{1}{\zeta_q(2)\log q}\prod_{(P)}\left(1+\frac{1}{(|P|+1)(|P|^2-1)}\right).$$

Define the additional Dirichlet series

$$\begin{aligned}
G_1(s) &= \sum_{\substack{(m_{\alpha_i})\nmid(g),1\le i\le\ell\\(m_{\alpha_i})\mid(g),\ell+1\le i\le n}}\frac{b(g)}{|g|^s}=\prod_{(P)\neq(m_{\alpha_i}),1\le i\le n}\left(1+\frac{|P|^{-s}}{(1-|P|^{-s})(1+|P|^{-1})}\right)\\
&\quad\times\prod_{(P)=(m_{\alpha_i}),\ell+1\le i\le n}\left(\sum_{k=1}^{\infty}b(P^k)|P|^{-ks}\right)\\
&= G(s)\prod_{i=1}^{n}\left(1+\frac{q^{-u_is}}{(1-q^{-u_is})(1+q^{-u_i})}\right)^{-1}\prod_{i=\ell+1}^{n}\frac{q^{-u_is}}{(1-q^{-u_is})(1+q^{-u_i})}\\
&= G(s)\prod_{i=1}^{\ell}\frac{(1-q^{-u_is})(1+q^{-u_i})}{1+q^{-u_i}-q^{-u_i(s+1)}}\prod_{i=\ell+1}^{n}\frac{q^{-u_is}}{1+q^{-u_i}-q^{-u_i(s+1)}}.
\end{aligned}$$

Thus, $G_1(s)$ has a simple pole at $s=1$ with residue

$$\rho=\frac{H(1)}{\zeta_q(2)\log q}\prod_{i=1}^{\ell}\frac{1-q^{-2u_i}}{1+q^{-u_i}-q^{-2u_i}}\prod_{i=\ell+1}^{n}\frac{q^{-u_i}}{1+q^{-u_i}-q^{-2u_i}},$$

and

$$G_1(s)-\frac{\rho}{s-1}$$

is holomorphic for $\mathrm{Re}(s)>1/2$. Then, using Theorem 17.1 of [Ros02] which is the function field version of the Wiener–Ikehara Tauberian Theorem, we get that

$$\sum_{\substack{(g),g\in\mathcal{S}_d\\(m_{\alpha_i})\nmid(g),1\le i\le\ell\\(m_{\alpha_i})\mid(g),\ell+1\le i\le n}}b(g)=\frac{H(1)q^{d+1}}{\zeta_q(2)}\prod_{i=1}^{\ell}\frac{1-q^{-2u_i}}{1+q^{-u_i}-q^{-2u_i}}\prod_{i=\ell+1}^{n}\frac{q^{-u_i}}{1+q^{-u_i}-q^{-2u_i}}+O\left(q^{(1/2+\varepsilon)d}\right).$$

Using the line above in the formula for $|\mathcal{F}_d^{\mathrm{ord}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)|$, we get

$$\begin{aligned}
&|\mathcal{F}_d^{\mathrm{ord}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)|\\
&=\frac{q^{d+1-\sum_{i=1}^{\ell}u_i}}{\zeta_q(2)\prod_{i=1}^{\ell}(1-q^{-2u_i})}\frac{H(1)q^{d+1}}{\zeta_q(2)}\prod_{i=1}^{\ell}\frac{1-q^{-2u_i}}{1+q^{-u_i}-q^{-2u_i}}\prod_{i=\ell+1}^{n}\frac{q^{-u_i}}{1+q^{-u_i}-q^{-2u_i}}+O\left(q^{(3/2+\varepsilon)d}\right)\\
&=\frac{H(1)q^{2d+2-\sum_{i=1}^{n}u_i}}{\zeta_q(2)^2\prod_{i=1}^{n}(1+q^{-u_i}-q^{-2u_i})}+O\left(q^{(3/2+\varepsilon)d}\right).
\end{aligned}$$

□

The previous result may be used to obtain the number of covers in the whole ordinary family by specializing to $n=0$.

**Corollary 3.7.**

$$|\mathcal{F}_d^{\mathrm{ord}}|=\frac{H(1)q^{2d+2}}{\zeta_q(2)^2}+O\left(q^{(3/2+\varepsilon)d}\right).$$

By combining Proposition 3.6 and Corollary 3.7, we obtain the following result.

**Proposition 3.8.** *Fix $\alpha_1, \ldots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \ldots, u_n$ over $\mathbb{F}_q$ such that none of the $\alpha_i$ are conjugate to each other. Let $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$. Then*

$$\begin{aligned}\frac{|\mathcal{F}_d^{\text{ord}}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)|}{|\mathcal{F}_d^{\text{ord}}|} &= \frac{q^{-\sum_{i=1}^n u_i}}{\prod_{i=1}^n (1 + q^{-u_i} - q^{-2u_i})} + O\left(q^{(-1/2+\varepsilon)d}\right) \\ &= q^{-\sum_{i=1}^n u_i}\left(1 + O\left(\sum_{i=1}^n q^{-u_i}\right)\right) + O\left(q^{(-1/2+\varepsilon)d}\right).\end{aligned}$$

We finish this section by computing the expected number of points in an ordinary Artin-Schreier cover. For this, we need to compute the case $n = 1$, i.e., $|\mathcal{F}_d^{\text{ord}}(\alpha, \beta)|$.

**Corollary 3.9.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. Let $\beta \in \mathbb{P}^1(\mathbb{F}_{q^u})$. Then*

$$|\mathcal{F}_d^{\text{ord}}(\alpha, \beta)| = \begin{cases} \frac{H(1)q^{2d+2-u}(1-q^{-u})}{\zeta_q(2)^2(1+q^{-u}-q^{-2u})} + O\left(q^{(3/2+\varepsilon)d+u}\right) & \beta = \infty, \\ \\ \frac{H(1)q^{2d+2-u}}{\zeta_q(2)^2(1+q^{-u}-q^{-2u})} + O\left(q^{(3/2+\varepsilon)d}\right) & \beta \in \mathbb{F}_{q^u}. \end{cases}$$

*Proof.* The case of $\beta \in \mathbb{F}_{q^u}$ is a simple consequence of Proposition 3.6. For $\beta = [1:0]$, we have, by Lemma 2.3 that

$$\begin{aligned}|\mathcal{F}_d^{\text{ord}}(\alpha, \infty)| &= |\mathcal{F}_d^{\text{ord}}| - \sum_{\beta \in \mathbb{F}_{q^u}} |\mathcal{F}_d^{\text{ord}}(\alpha, \beta)| \\ &= |\mathcal{F}_d^{\text{ord}}| - q^u |\mathcal{F}_d^{\text{ord}}(\alpha, 0)| \\ &= \frac{H(1)q^{2d+2-u}(1-q^{-u})}{\zeta_q(2)^2(1+q^{-u}-q^{-2u})} + O\left(q^{(3/2+\varepsilon)d+u}\right).\end{aligned}$$

□

By combining Proposition 3.8 and Corollaries 3.7 and 3.9, we obtain the following result.

**Proposition 3.10.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ with degree $u$ over $\mathbb{F}_q$. Let $\beta \in \mathbb{P}^1(\mathbb{F}_{q^u})$. Then*

$$\frac{|\mathcal{F}_d^{\text{ord}}(\alpha, \beta)|}{|\mathcal{F}_d^{\text{ord}}|} = \begin{cases} \frac{q^{-u}(1-q^{-u})}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d+u}\right) & \beta = \infty, \\ \\ \frac{q^{-u}}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d}\right) & \beta \in \mathbb{F}_{q^u}. \end{cases}$$

**Lemma 3.11.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. The expected number of $\mathbb{F}_{q^k}$-points in the fiber above $\alpha$ is*

$$\begin{cases} 1 + O\left(q^{(-1/2+\varepsilon)d+u}\right) & \text{if } p \nmid \frac{k}{u}, \\ \\ 1 + \frac{p-1}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d+u}\right) & \text{if } p \mid \frac{k}{u}. \end{cases}$$

*Proof.* By Lemma 2.1 and Proposition 3.10, the expected number of $\mathbb{F}_{q^k}$-points in the fiber above $\alpha$ is

$$\frac{q^{-u}(1-q^{-u})}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d+u}\right) + \sum_{\beta \in \mathbb{F}_{q^u}, \text{tr}_k(\beta)=0} p\left(\frac{q^{-u}}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d}\right)\right).$$

If $p \nmid \frac{k}{u}$, then $\text{tr}_k(\beta) = 0$ iff $\text{tr}_u(\beta) = 0$ and there are $\frac{q^u}{p}$ points in $\mathbb{F}_{q^u}$ with that property.

If $p \mid \frac{k}{u}$, then $\text{tr}_k(\beta) = \frac{k}{u}\text{tr}_u(\beta) = 0$ for all $\beta \in \mathbb{F}_{q^u}$ and therefore the expected number of points in the fiber is

$$\frac{q^{-u}(1-q^{-u})}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d+u}\right) + \frac{p}{1+q^{-u}-q^{-2u}} + O\left(q^{(-1/2+\varepsilon)d+u}\right).$$

□

For our main result, we recall that an ordinary Artin-Schreier cover has $r+1$ simple poles. This corresponds to taking $d = r+1$. We are ready to prove the first part of Theorem 1.1.

**Theorem 3.12.** *The expected number of $\mathbb{F}_{q^k}$-points on an ordinary Artin-Schreier cover defined over $\mathbb{F}_q$ is*

$$\begin{cases} q^k + 1 + O\left(q^{(-1/2+\varepsilon)(r+1)+2k}\right) & p \nmid k, \\ q^k + 1 + \frac{p-1}{1+q^{-1}-q^{-2}} + \sum_{u \mid \frac{k}{p}} \frac{p-1}{1+q^{-u}-q^{-2u}} \pi(u) u + O\left(q^{(-1/2+\varepsilon)(r+1)+2k}\right) & p \mid k, \end{cases}$$

*where $\pi(u)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree $u$.*

*Proof.* If $p \nmid k$, the result follows by adding the result of Lemma 3.11 over all $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$. If $p \mid k$ we still get the term $q^k + 1$ and an additional term given by

$$\sum_{u \mid \frac{k}{p}} \sum_{\alpha, \deg \alpha = u} \frac{p-1}{1+q^{-u}-q^{-2u}} = \frac{p-1}{1+q^{-1}-q^{-2}} + \sum_{u \mid \frac{k}{p}} \frac{p-1}{1+q^{-u}-q^{-2u}} \pi(u) u,$$

where the first term on the right hand side accounts for the case $\alpha = \infty$. □

**Remark 3.13.** When $k = p$, we obtain

$$q^p + 1 + \frac{(p-1)(q+1)}{1+q^{-1}-q^{-2}} + O\left(q^{(-1/2+\varepsilon)(r+1)+2p}\right).$$

## 4. Full Space

In this case, we consider the family

$$\mathcal{F}_d^{\text{full}} = \left\{ (g(X,Z), h(X,Z)) : g(X,Z), h(X,Z) \in \mathcal{S}_d, (g,h) = 1 \right\}.$$

**Proposition 4.1.** *Fix $\alpha_1, \dots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \dots, u_n$ such that none of the $\alpha_i$ are conjugate to each other. Let $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$. Then we have*

$$|\mathcal{F}_d^{\text{full}}(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n)| = \frac{q^{2d+2-\sum_{i=1}^n u_i}}{\zeta_q(2)} \prod_{i=1}^n \left( \frac{1}{1+q^{-u_i}} \right) + O\left(q^{(1+\varepsilon)d}\right).$$

*Proof.* Assume without loss of generality that $\beta_1, \dots, \beta_\ell$ are not zero, and $\beta_{\ell+1} = \dots = \beta_n = 0$. We have, by Lemma 3.3, that

$$\begin{aligned} |\mathcal{F}_d^{\text{full}}(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n)| &= \sum_{g \in \mathcal{S}_d} \left| \left\{ h \in \mathcal{S}_d : (h,g) = 1, \frac{g(\alpha_i)}{h(\alpha_i)} = \beta_i, 1 \le i \le n \right\} \right| \\ &= \sum_{g \in \mathcal{S}_d} q^{d+1-\sum_{i=1}^\ell u_i} \prod_{(P) \mid (g)} (1 - |P|^{-1}) + O\left(q^{(1+\varepsilon)d}\right). \end{aligned}$$

We set

$$b(g) = \prod_{(P) \mid (g)} (1 - |P|^{-1}),$$

and

$$G(s) = \sum_{(g) \neq 0} \frac{b(g)}{|g|^s}.$$

Since $b(g)$ is a multiplicative function, it follows that $G(s)$ has an Euler product of the form

$$\begin{aligned} G(s) &= \prod_{(P)} \left( \sum_{k=0}^\infty b(P^k) |P|^{-ks} \right) = \prod_{(P)} \left( 1 + \frac{b(P)|P|^{-s}}{1-|P|^{-s}} \right) \\ &= \prod_{(P)} \left( 1 + \frac{(1-|P|^{-1})|P|^{-s}}{1-|P|^{-s}} \right) = \prod_{(P)} \left( \frac{1-|P|^{-1-s}}{1-|P|^{-s}} \right). \end{aligned}$$

Therefore

$$G(s) = \frac{\zeta_q(s)}{\zeta_q(1+s)},$$

is analytic for $\mathrm{Re}(s) > 0$, except for a simple pole at $s = 1$ with residue $\frac{(q-1)}{\zeta_q(2) \log q}$.

Now define the Dirichlet series

$$
\begin{aligned}
G_1(s) &= \sum_{\substack{(m_{\alpha_i})\nmid(g),1\le i\le\ell\\(m_{\alpha_i})|(g),\ell+1\le i\le n}} \frac{b(g)}{|g|^s} = \prod_{(P)\neq(m_{\alpha_i}),1\le i\le n}\left(\frac{1-|P|^{-1-s}}{1-|P|^{-s}}\right)\\
&\quad\times\prod_{(P)=(m_{\alpha_i}),\ell+1\le i\le n}\left(\sum_{k=1}^{\infty} b(P^k)|P|^{-ks}\right)\\
&= G(s)\prod_{i=1}^{n}\left(\frac{1-q^{-u_i(1+s)}}{1-q^{-u_is}}\right)^{-1}\prod_{i=\ell+1}^{n}\left(\frac{q^{-u_is}(1-q^{-u_i})}{1-q^{-u_is}}\right)\\
&= G(s)\prod_{i=1}^{\ell}\frac{1-q^{-u_is}}{1-q^{-u_i(1+s)}}\prod_{i=\ell+1}^{n}\frac{q^{-u_is}(1-q^{-u_i})}{1-q^{-u_i(1+s)}}.
\end{aligned}
$$

Thus $G_1(s)$ is analytic for $\mathrm{Re}(s)>0$, except for a simple pole at $s=1$ with residue

$$
\frac{1}{\zeta_q(2)\log q}\prod_{i=1}^{\ell}\frac{1}{1+q^{-u_i}}\prod_{i=\ell+1}^{n}\frac{q^{-u_i}}{1+q^{-u_i}}.
$$

Then, using again Theorem 17.1 of [Ros02], we get that

$$
\begin{aligned}
|\mathcal{F}_d^{\mathrm{full}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)| &= q^{d+1-\sum_{i=1}^{\ell}u_i}\sum_{\substack{(g),g\in\mathcal{S}_d\\(m_{\alpha_i})\nmid(g),1\le i\le\ell\\(m_{\alpha_i})|(g),\ell+1\le i\le n}} b(g)+O\left(q^{(\varepsilon+1)d}\right)\\
&= \frac{q^{2d+2-\sum_{i=1}^{\ell}u_i}}{\zeta_q(2)}\prod_{i=1}^{\ell}\left(\frac{1}{1+q^{-u_i}}\right)\prod_{i=\ell+1}^{n}\left(\frac{q^{-u_i}}{1+q^{-u_i}}\right)+O\left(q^{(\varepsilon+1)d}\right).
\end{aligned}
$$

□

We may now proceed to compute the number of covers in the whole family by setting $n=0$ in the previous result.

**Corollary 4.2.**

$$
|\mathcal{F}_d^{\mathrm{full}}| = \frac{q^{2d+2}}{\zeta_q(2)}+O\left(q^{(1+\varepsilon)d}\right).
$$

By combining Proposition 4.1 and Corollary 4.2, we obtain the following result.

**Proposition 4.3.** *Fix $\alpha_1,\dots,\alpha_n\in\mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1,\dots,u_n$ such that none of the $\alpha_i$ are conjugate to each other. Let $\beta_i\in\mathbb{F}_{q^{u_i}}$ for $1\le i\le n$. Then we have*

$$
\begin{aligned}
\frac{|\mathcal{F}_d^{\mathrm{full}}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)|}{|\mathcal{F}_d^{\mathrm{full}}|} &= \prod_{i=1}^{n}\left(\frac{q^{-u_i}}{1+q^{-u_i}}\right)+O\left(q^{(\varepsilon-1)d}\right)\\
&= q^{-\sum_{i=1}^{n}u_i}\left(1+O\left(\sum_{i=1}^{n}q^{-u_i}\right)\right)+O\left(q^{(\varepsilon-1)d}\right).
\end{aligned}
$$

We finish the section by computing the expected number of points in the full Artin-Schreier family.

**Corollary 4.4.** *Fix $\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. Let $\beta\in\mathbb{P}^1(\mathbb{F}_{q^u})$. Then*

$$
|\mathcal{F}_d^{\mathrm{full}}(\alpha,\beta)| = \frac{q^{2d+2-u}}{\zeta_q(2)(1+q^{-u})}+\begin{cases}O\left(q^{(\varepsilon+1)d+u}\right) & \beta=\infty,\\[2ex] O\left(q^{(\varepsilon+1)d}\right) & \beta\in\mathbb{F}_{q^u}.\end{cases}
$$

*Proof.* The case of $\beta \in \mathbb{F}_{q^u}$ easily follows from Proposition 4.1. For $\beta = [1:0]$, we have, by Lemma 2.3 that

$$\begin{aligned} |\mathcal{F}_d^{\text{full}}(\alpha,\infty)| &= |\mathcal{F}_d^{\text{full}}| - \sum_{\beta\in\mathbb{F}_{q^u}} |\mathcal{F}_d^{\text{full}}(\alpha,\beta)| \\ &= |\mathcal{F}_d^{\text{full}}| - q^u|\mathcal{F}_d^{\text{full}}(\alpha,0)| \\ &= \frac{q^{2d+2-u}}{\zeta_q(2)(1+q^{-u})} + O\left(q^{(\varepsilon+1)d+u}\right). \end{aligned}$$

□

We then obtain the following result.

**Proposition 4.5.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. Let $\beta \in \mathbb{P}^1(\mathbb{F}_{q^u})$. Then*

$$\frac{|\mathcal{F}_d^{\text{full}}(\alpha,\beta)|}{|\mathcal{F}_d^{\text{full}}|} = \frac{q^{-u}}{1+q^{-u}} + \begin{cases} O\left(q^{(\varepsilon-1)d+u}\right) & \beta=\infty, \\ O\left(q^{(\varepsilon-1)d}\right) & \beta\in\mathbb{F}_{q^u}. \end{cases}$$

**Lemma 4.6.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. The expected number of $\mathbb{F}_{q^k}$-points in the fiber above $\alpha$ is*

$$\begin{cases} 1+O\left(q^{(\varepsilon-1)d+u}\right) & \text{if } p\nmid \frac{k}{u}, \\ 1+\frac{p-1}{1+q^{-u}}+O\left(q^{(\varepsilon-1)d+u}\right) & \text{if } p\mid \frac{k}{u}. \end{cases}$$

*Proof.* By Lemma 2.1 and Proposition 4.5, we have

$$\frac{q^{-u}}{1+q^{-u}} + O\left(q^{(\varepsilon-1)d+u}\right) + \sum_{\beta\in\mathbb{F}_{q^u},\operatorname{tr}_k(\beta)=0} p\left(\frac{q^{-u}}{1+q^{-u}} + O\left(q^{(\varepsilon-1)d}\right)\right).$$

If $p\nmid \frac{k}{u}$, then $\operatorname{tr}_k(\beta)=0$ iff $\operatorname{tr}_u(\beta)=0$ and there are $\frac{q^u}{p}$ points in $\mathbb{F}_{q^u}$ with that property.

If $p\mid \frac{k}{u}$, then $\operatorname{tr}_k(\beta)=\frac{k}{u}\operatorname{tr}_u(\beta)=0$ for all $\beta\in\mathbb{F}_{q^u}$ and therefore the expected number of points in the fiber is

$$\frac{q^{-u}}{1+q^{-u}} + O\left(q^{(\varepsilon-1)d+u}\right) + \frac{p}{1+q^{-u}} + O\left(q^{(\varepsilon-1)d+u}\right).$$

□

We are ready to prove Theorem 1.1 (2).

**Theorem 4.7.** *The expected number of $\mathbb{F}_{q^k}$-points on an Artin-Schreier cover in $\mathcal{AS}_{\mathfrak{g}}$ defined over $\mathbb{F}_q$ is*

$$\begin{cases} q^k+1+O\left(q^{(\varepsilon-1)d+2k}\right) & p\nmid k, \\ q^k+1+(p-1)q^{k/p}+\frac{p-1}{1+q^{-1}}-(p-1)\sum_{u\mid\frac{k}{p}}\frac{1}{1+q^u}\pi(u)u+O\left(q^{(\varepsilon-1)d+2k}\right) & p\mid k. \end{cases}$$

*Proof.* The result for $p\nmid k$ follows from Lemma 4.6. If $p\mid k$ we still get the term $q^k+1$ and an additional term given by

$$\begin{aligned} \sum_{u\mid\frac{k}{p}}\sum_{\alpha,\deg\alpha=u}\frac{p-1}{1+q^{-u}} &= \frac{p-1}{1+q^{-1}}+(p-1)\sum_{u\mid\frac{k}{p}}\frac{q^u}{1+q^u}\pi(u)u \\ &= \frac{p-1}{1+q^{-1}}+(p-1)q^{k/p}-(p-1)\sum_{u\mid\frac{k}{p}}\frac{1}{1+q^u}\pi(u)u. \end{aligned}$$

□

**Remark 4.8.** When $k=p$, we obtain

$$q^p+1+(p-1)q+O\left(q^{(\varepsilon-1)d+2p}\right).$$

## 5. Prescribed factorization type

Recall that

$$\mathcal{F}_d^v = \{(g(X,Z), h(X,Z)) : g(X,Z), h(X,Z) \in \mathcal{S}_d, (g,h) = 1, h \text{ has factorization type } v\},$$

where $v = (r_1^{d_{1,1}}, \ldots, r_1^{d_{1,\ell_1}}, \ldots, r_m^{d_{m,1}}, \ldots, r_m^{d_{m,\ell_m}})$ and

$$h = P_{1,1}^{d_{1,1}} \cdots P_{1,\ell_1}^{d_{1,\ell_1}} \cdots P_{m,1}^{d_{m,1}} \cdots P_{m,\ell_m}^{d_{m,\ell_m}},$$

where the $P_{i,j}$ are distinct irreducible polynomials of degree $r_i$ and $r_i \neq r_j$ if $i \neq j$. The degree of $h$ is then given by $d = \sum_{i=1}^m r_i \sum_{j=1}^{\ell_i} d_{i,j}$.

We will first compute the expected number of points for this family. We need the following result.

**Lemma 5.1.** *Fix a polynomial $h \in \mathcal{S}_d$. Then, if $h \neq 0$*

$$|\{g \in \mathcal{S}_d : (g,h) = 1\}| = q^{d+1} \prod_{(P)|(h)} (1 - |P|^{-1}).$$

We remark that this Lemma follows directly from the proof of Lemma 3.3.

**Proposition 5.2.** *Fix $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u$ over $\mathbb{F}_q$. Let $\beta \in \mathbb{P}^1(\mathbb{F}_{q^u})$. Then, if $u \leq d$,*

$$\frac{|\mathcal{F}_d^v(\alpha,\beta)|}{|\mathcal{F}_d^v|} = \begin{cases} q^{-u} & \deg(\alpha) = u \neq r_i, \beta \neq \infty, \\ 0 & \deg(\alpha) = u \neq r_i, \beta = \infty, \\ \frac{q^{-r_i}(\pi(r_i) - \ell_i)}{\pi(r_i)} & \deg(\alpha) = r_i, \beta \neq \infty, \\ \frac{\ell_i}{\pi(r_i)} & \deg(\alpha) = r_i, \beta = \infty. \end{cases}$$

*If $u > d$ the above quotient is $O(q^{-d})$.*

*Proof.* We first consider the size of the whole family. By Lemma 5.1 we have

$$\begin{aligned} |\mathcal{F}_d^v| &= \sum_{\deg P_{i,j} = r_i, \text{all different}} |\{g \in \mathcal{S}_d \,:\, (g,h) = 1\}| \\ &= q^{d+1} \prod_{i=1}^m (1 - q^{-r_i})^{\ell_i} \sum_{\deg P_{i,j} = r_i, \text{all different}} 1. \end{aligned} \tag{5}$$

If $\deg(\alpha) = u \neq r_i$, and $\beta \in \mathbb{F}_{q^u}$, then by Lemma 2.3 it suffices to find $|\mathcal{F}_d^v(\alpha,\beta)|$ for $\beta = 0$. If this is the case, then we need $g(\alpha) = 0$, or that $m_\alpha \mid g$.

$$\begin{aligned} |\mathcal{F}_d^v(\alpha,\beta)| &= \sum_{\deg P_{i,j} = r_i, \text{all different}} |\{g \in \mathcal{S}_d \,:\, (g,h) = 1, m_\alpha \mid g\}| \\ &= q^{d+1-u} \prod_{i=1}^m (1 - q^{-r_i})^{\ell_i} \sum_{\deg P_{i,j} = r_i, \text{all different}} 1. \end{aligned}$$

If $\deg(\alpha) = u \neq r_i$, and $\beta = \infty$, we get a contradiction and thus

$$|\mathcal{F}_d^v(\alpha,\infty)| = 0.$$

Now assume that $\deg(\alpha) = u = r_{i_0}$, for some $i_0$ and that $\beta \in \mathbb{F}_{q^u}$. By Lemma 2.3 we can again assume that $\beta = 0$. In this case we need to impose the condition that $h(\alpha) \neq 0$. Therefore,

$$|\mathcal{F}_d^v(\alpha,\beta)| = q^{d+1-r_{i_0}} \prod_{i=1}^m (1 - q^{-r_i})^{\ell_i} \sum_{\deg P_{i,j} = r_i, P_{i_0,j} \neq m_\alpha, \text{all different}} 1.$$

Finally, if $\deg(\alpha) = r_{i_0}$ for some $i_0$ and $\beta = \infty$, we need that $h(\alpha) = 0$ and $g(\alpha) \neq 0$.

$$|\mathcal{F}_d^v(\alpha,\infty)| = q^{d+1}\prod_{i=1}^m (1-q^{-r_i})^{\ell_i} \sum_{\deg P_{i,j}=r_i, \exists P_{i_0,j}=m_\alpha, \text{all different}} 1.$$

The result now follows from the identity

$$|\{\deg P_{i,j} = r_i, \text{all different}\}| = \prod_{i=1}^m \binom{\pi(r_i)}{\ell_i}.$$

□

We are now ready to prove the main result of this section.

**Theorem 5.3.** *The expected number of $\mathbb{F}_{q^k}$-points on an Artin-Schreier cover with poles given by the factorization type $v$ defined over $\mathbb{F}_q$ is*

$$\begin{cases} q^k+1 & p \nmid k, \\ \\ q^k+1+(p-1)q^{k/p}+(p-1)\left(1-\sum_{r_i|k}\ell_i r_i\right) & p \mid k. \end{cases}$$

*Proof.* We can assume that $p \nmid d_i$. This is because the $\mathbb{F}_q$-isomorphisms $(x,y) \mapsto (x, y+ax^k)$ allow us to eliminate all the terms in $h$ such that $x$ appears to a power multiple of $p$.

By Lemma 2.1, the final count becomes

$$\begin{aligned}
&\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})} \frac{|\mathcal{F}_d^v(\alpha,\infty)|}{|\mathcal{F}_d^v|} + \sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})}\sum_{\beta\in\mathbb{F}_{q^{\deg(\alpha)}},\operatorname{tr}_k(\beta)=0} p\frac{|\mathcal{F}_d^v(\alpha,\beta)|}{|\mathcal{F}_d^v|}\\
&=\sum_{r_i|k}\frac{\ell_i}{\pi(r_i)}\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k}),\deg(\alpha)=r_i} 1+\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})}\sum_{\beta\in\mathbb{F}_{q^{\deg(\alpha)}},\operatorname{tr}_k(\beta)=0} pq^{-\deg(\alpha)}\\
&-\sum_{r_i|k}\frac{\ell_i}{\pi(r_i)}\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k}),\deg(\alpha)=r_i}\sum_{\beta\in\mathbb{F}_{q^{r_i}},\operatorname{tr}_k(\beta)=0} pq^{-r_i}.
\end{aligned}$$

If $p \nmid k$, then $\operatorname{tr}_k(\beta) = 0$ if and only if $\operatorname{tr}_u(\beta) = 0$ and there are $\frac{q^u}{p}$ in $\mathbb{F}_{q^u}$ with that property. Thus we obtain $q^k+1$. If $p \mid k$, then since $p \nmid r_i$, if $r_i \mid k$ then $p \mid \frac{k}{r_i}$ and $\operatorname{tr}_k(\beta) = 0$ for $\beta \in \mathbb{F}_{q^{r_i}}$. The final count then becomes

$$\begin{aligned}
&\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})}\sum_{\beta\in\mathbb{F}_{q^{\deg(\alpha)}},\operatorname{tr}_k(\beta)=0} pq^{-\deg(\alpha)}+\sum_{r_i|k}\frac{\ell_i}{\pi(r_i)}\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^{r_i}}),\deg\alpha=r_i}\left(1-\sum_{\beta\in\mathbb{F}_{q^{r_i}},\operatorname{tr}_k(\beta)=0} pq^{-r_i}\right)\\
&=q^k+1+(p-1)(q^{k/p}+1)-\sum_{r_i|k}\frac{\ell_i}{\pi(r_i)}\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^{r_i}}),\deg\alpha=r_i}(p-1)\\
&=q^k+1+(p-1)q^{k/p}+(p-1)\left(1-\sum_{r_i|k}\ell_i r_i\right).
\end{aligned}$$

□

Now suppose that we take the $p$-rank 0 family. We recall that this corresponds to $v = (1^d)$. A simple application of Theorem 5.3 yields the following.

**Theorem 5.4.** *The expected number of $\mathbb{F}_{q^k}$-points on a p-rank 0 Artin-Schreier cover in $\mathcal{AS}_{\mathfrak{g},0}$ defined over $\mathbb{F}_q$ is*

$$\begin{cases} q^k+1 & p \nmid k, \\ \\ q^k+1+(p-1)q^{k/p} & p \mid k. \end{cases}$$

This recovers the result from [Ent12].

Finally we consider the family of curves with $p$-rank equal to $p-1$. It corresponds to $v=(1^{d_1},1^{d_2})$. Again, by applying Theorem 5.3 we get the third part of Theorem 1.1.

**Theorem 5.5.** *The expected number of $\mathbb{F}_{q^k}$-points on a p-rank p Artin-Schreier cover in $\mathcal{AS}_{\mathfrak{g},p-1}$ defined over $\mathbb{F}_q$ is*

$$\begin{cases} q^k+1 & p \nmid k, \\ \\ q^k+1+(p-1)(q^{k/p}-1) & p \mid k. \end{cases}$$

We now proceed to the case where we fix several values, which will be needed for the computation of the moments.

**Proposition 5.6.** *Let $\alpha_1,\dots,\alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1,\dots,u_n$ over $\mathbb{F}_q$ such that none of the $\alpha_i$ are conjugate to each other. Let $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$. Then*

$$\frac{|\mathcal{F}_d^v(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)|}{|\mathcal{F}_d^v|} = \prod_{i=1}^m (1-\tau(r_i,\ell_i;u_1,\dots,u_n))q^{-(u_1+\cdots+u_n)} + O(q^{(\varepsilon-1)d}),$$

*where $0 \le \tau(r_i,\ell_i;u_1,\dots,u_n) \le 1$ is a constant that depends on the number of $u_j$'s that are equal to $r_i$ and is equal to zero if $u_j \ne r_i$ for any $j$.*

*Proof.* Without loss of generality we can assume that $\beta_1,\dots,\beta_\ell$ are not zero and that $\beta_{\ell+1}=\cdots=\beta_n=0$. We have that

$$\begin{aligned} & |\mathcal{F}_d^v(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)| \\ (6) \quad = & \sum_{\substack{\deg P_{i,j}=r_i, \text{all different} \\ P_{i,j}\neq m_\alpha}} \left| \left\{ g_1 \in \mathcal{S}_{d-\sum_{j=\ell+1}^n u_j} \,:\, (g_1,h)=1, \frac{g_1(\alpha_i)\prod_{j=\ell+1}^n m_{\alpha_j}(\alpha_i)}{h(\alpha_i)} = \beta_i,\, 1\le i \le \ell \right\} \right|. \end{aligned}$$

Notice that $\beta_i^{-1} \in \mathbb{F}_{q^{u_i}}^*$ for $1 \le i \le \ell$. By Lemma 3.3,

$$\begin{aligned} & \left| \left\{ g_1 \in \mathcal{S}_{d-\sum_{j=\ell+1}^n u_j} \,:\, (g_1,h)=1, \frac{h(\alpha_i)}{g_1(\alpha_i)\prod_{j=\ell+1}^n m_{\alpha_j}(\alpha_i)} = \beta_i^{-1}\, 1\le i \le \ell \right\} \right| \\ = \; & q^{d+1-\sum_{i=1}^n u_i} \prod_{(P)|(h)} (1-|P|^{-1}) + O\left(q^{\varepsilon d}\right) \\ = \; & q^{d+1-\sum_{i=1}^n u_i} \prod_{j=1}^m (1-q^{-r_j})^{\ell_j} + O\left(q^{\varepsilon d}\right). \end{aligned}$$

On the other hand, $|\{\deg P_{i,j}=r_i, \text{all different}, P_{i,j}\neq m_\alpha\}|$ is a product of binomials of the form

$$\binom{\pi(r_i)-s_i}{\ell_i},$$

where $s_i$ corresponds to the number of $u_j$'s that equal the particular $r_i$.

This gives that

$$\frac{|\{\deg P_{i,j}=r_i, \text{all different}, P_{i,j}\neq m_\alpha\}|}{|\{\deg P_{i,j}=r_i, \text{all different}\}|}$$

is a product of terms of the form

$$(1-\tau(r_i,\ell_i;u_1,\ldots,u_n)) = \frac{\binom{\pi(r_i)-s_i}{\ell_i}}{\binom{\pi(r_i)}{\ell_i}} = \frac{(\pi(r_i)-\ell_i)(\pi(r_i)-\ell_i-1)\cdots(\pi(r_i)-\ell_i-s_i+1)}{\pi(r_i)(\pi(r_i)-1)\cdots(\pi(r_i)-s_i+1)}.$$

By dividing equation (6) by equation (5), we get

$$\frac{|\mathcal{F}_d^v(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n)|}{|\mathcal{F}_d^v|} = q^{-\sum_{i=1}^n u_i}\prod_{i=1}^m(1-\tau(r_i,\ell_i;u_1,\ldots,u_n)) + O(q^{(\varepsilon-1)d}),$$

where the constant satisfies the desired properties. □

## 6. Beurling–Selberg functions

In this section we start the development of the tools needed to prove Theorem 1.2. 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 $0<\beta<1$ and set $\mathcal{I}=[-\beta/2,\beta/2]\subset[-1/2,1/2)$. Our goal is to estimate the quantity

$$N_{\mathcal{I}}(f,\psi) := \#\left\{1\le j\le \frac{2\mathfrak{g}}{p-1} : \theta_j(f,\psi)\in\mathcal{I}\right\} = \sum_{j=1}^{2\mathfrak{g}/(p-1)} \chi_{\mathcal{I}}(\theta_j(f,\psi)),$$

where $\chi_{\mathcal{I}}$ denotes the characteristic function of $\mathcal{I}$. We are going to approximate $\chi_{\mathcal{I}}$ with Beurling–Selberg polynomials $I_K^{\pm}$.

In what follows, we use the standard notation $e(x):=e^{2\pi i x}$. Let $K$ be a positive integer, 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

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

Here is a list of a series of useful properties of the Beurling–Selberg polynomials (see [Mon94], ch 1.2) that will be used in this paper.

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

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

(b) The Beurling–Selberg polynomials yield upper and lower bounds for the characteristic function:

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

(c) The integral of Beurling–Selberg polynomials approximates the length of the interval:

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

(d) The $I_K^{\pm}$ are even (because the interval $\mathcal{I}$ is symmetric about the origin). Therefore 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 of the Beurling–Selberg polynomials approximate those of the characteristic function:

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

Therefore we obtain the following bound:

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

We now list some results that will be useful in future sections.

**Proposition 6.1.** *(Proposition 4.1,* [FR10]*) For $K \geq 1$ such that $K|\mathcal{I}| > 1$, we have*

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

We remark that for a given $K$ the above sums are actually finite, since the Beurling–Selberg polynomials $I_K^{\pm}$ have degree at most $K$. We will also need the following estimates.

**Proposition 6.2.** *(Proposition 5.2,* [BDFLS]*) For $\alpha_1,\dots,\alpha_r,\gamma_1,\dots,\gamma_r > 0$, and $\beta_1,\dots,\beta_r \in \mathbb{R}$, we have,*

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

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

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

## 7. Set-up for the distribution of the zeroes

We state here an explicit formula that will be used to relate $L(u,f,\psi)$ to the Beurling–Selberg polynomials. Recall that $2\mathfrak{g} = (p-1)(\Delta-1)$.

**Lemma 7.1.** *(*[BDFLS]*, Lemma 3.1) Let $h(\theta) = \sum_{|k|\leq K} \widehat{h}(k)e(k\theta)$ be a trigonometric polynomial. Let $\theta_j(f,\psi)$ be the eigenangles of the L-function $L(u,f,\psi)$. Then we have*

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

*where*

$$S_k(f,\psi) = \sum_{\substack{x\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(x)\neq\infty}} \psi(\mathrm{tr}_k(f(x))).$$

We use the Beurling–Selberg approximation of the characteristic function of the interval $\mathcal{I}$ to rewrite $N_{\mathcal{I}}(f,\psi)$ and $N_{\mathcal{I}}(C_f)$ where $f$ varies over one of the families $\mathcal{F}_d$. By Property (b) of the Beurling–Selberg polynomials, we have

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

and using the explicit formula of Lemma 7.1 and Property (c), we have

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

where

$$S^{\pm}(K,f,\psi) := \sum_{k=1}^{K} \frac{\widehat{I}_K^{\pm}(k)S_k(f,\psi) + \widehat{I}_K^{\pm}(-k)S_k(f,\bar{\psi})}{q^{k/2}}. \tag{8}$$

This gives

$$-S^{-}(K,f,\psi) - \frac{\Delta-1}{K+1} \leq N_{\mathcal{I}}(f,\psi) - (\Delta-1)|\mathcal{I}| \leq -S^{+}(K,f,\psi) + \frac{\Delta-1}{K+1}, \tag{9}$$

and

$$-\sum_{h=1}^{p-1} S^-(K,f,\psi^h) - \frac{2\mathfrak{g}}{K+1} \quad \leq \quad N_{\mathcal{I}}(C_f) - 2\mathfrak{g}|\mathcal{I}| \leq -\sum_{h=1}^{p-1} S^+(K,f,\psi^h) + \frac{2\mathfrak{g}}{K+1}. \tag{10}$$

In the next section we are going to compute the moments

$$\frac{1}{|\mathcal{F}_d|}\sum_{f\in\mathcal{F}_d} S^{\pm}(K,f,\psi^h)^n \quad \text{and} \quad \frac{1}{|\mathcal{F}_d|}\sum_{f\in\mathcal{F}_d} S^{\pm}(K,C_f)^n$$

where

$$S^{\pm}(K,C_f)^n = \sum_{h_1,\dots,h_n=1}^{p-1} S^{\pm}(K,f,\psi^{h_1})\dots S^{\pm}(K,f,\psi^{h_n}). \tag{11}$$

We will show that they approach the Gaussian moments when properly normalized. We will then use this result to show that

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

converges to a normal distribution as $\mathfrak{g}\to\infty$ since it converges in mean square to

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

## 8. Moments

Our goal is to compute the moments of $S^{\pm}(K,C_f)$ when $f$ varies in any of the families of curves $\mathcal{F}_d^{\mathrm{ord}}$, $\mathcal{F}_d^{\mathrm{full}}$, and $\mathcal{F}_d^{v}$.

**Definition 8.1.** *Let*

$$E_{\mathcal{F}_d}(u) = \begin{cases} (1+q^{-u}-q^{-2u})^{-1} & \mathcal{F}_d = \mathcal{F}_d^{\mathrm{ord}}, \\ (1+q^{-u})^{-1} & \mathcal{F}_d = \mathcal{F}_d^{\mathrm{full}}, \\ \dfrac{\pi(r_i)-\ell_i}{\pi(r_i)} & \mathcal{F}_d = \mathcal{F}_d^{v} \text{ and } u = r_i \text{ for some } i, \\ 1 & \mathcal{F}_d = \mathcal{F}_d^{v} \text{ and } u \neq r_i \text{ for any } i. \end{cases}$$

*More generally, we have*

$$E_{\mathcal{F}_d}(u_1,\dots,u_n) = \begin{cases} \prod_{i=1}^{n} E_{\mathcal{F}_d}(u_i) & \mathcal{F}_d = \mathcal{F}_d^{\mathrm{ord}}, \mathcal{F}_d^{\mathrm{full}}, \\ \prod_{i=1}^{m} (1-\tau(r_i,\ell_i;u_1,\dots,u_n)) & \mathcal{F}_d = \mathcal{F}_d^{v}, \end{cases}$$

*where $\tau(r_i,\ell_i;u_1,\dots,u_n)$ is as defined in Proposition 5.6.*

**Remark 8.2.** Let $\mathcal{F}_d$ be any one of the families considered. Then

$$E_{\mathcal{F}_d}(u) = 1 + O\left(uq^{-u}\right).$$

The estimate can be improved to $E_{\mathcal{F}_d}(u) = 1+O\left(q^{-u}\right)$ for $\mathcal{F}_d^{\mathrm{ord}}$ and $\mathcal{F}_d^{\mathrm{full}}$. In the case of $\mathcal{F}_d^{v}$, we are assuming that the $\ell_i$ are fixed constants and using the estimate $\pi(m) = \frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right)$ (see [Ros02], Theorem 2.2).

In addition, we have that

$$E_{\mathcal{F}_d}(u_1,\dots,u_n) \ll 1.$$

From now on we will use the notation $\alpha_1 \sim \alpha_2$ to indicate that $\alpha_1$ and $\alpha_2$ are Galois conjugate, and $\alpha_1 \not\sim \alpha_2$ for the opposite statement.

Then, for all the families under consideration we have the following result.

**Lemma 8.3.** *Let $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree $u$ over $\mathbb{F}_q$. Let $\beta \in \mathbb{F}_{q^u}$. Let $\mathcal{F}_d$ be any of the families under consideration. Then*

$$\frac{|\mathcal{F}_d(\alpha,\beta)|}{|\mathcal{F}_d|} = \frac{|\mathcal{F}_d(\alpha,0)|}{|\mathcal{F}_d|} = \frac{E_{\mathcal{F}_d}(u)}{q^u} + O\left(q^{-d/2}\right). \tag{12}$$

*Let $\alpha_1, \alpha_2 \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, u_2$ respectively over $\mathbb{F}_q$. Let $\beta_1 \in \mathbb{F}_{q^{u_1}}$, $\beta_2 \in \mathbb{F}_{q^{u_2}}$. Let $\mathcal{F}_d$ be any of the families under consideration. Then, if $\alpha_1 \not\sim \alpha_2$,*

$$\frac{|\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)|}{|\mathcal{F}_d|} = \frac{E_{\mathcal{F}_d}(u_1,u_2)}{q^{u_1+u_2}} + O\left(q^{-d/2}\right), \tag{13}$$

*where $E_{\mathcal{F}_d}(u_1,u_2)$ does not depend on the values of $\beta_1, \beta_2$.*

*If $\alpha_1 \sim \alpha_2$, and $\beta_1 \sim \beta_2$ by the same automorphism,*

$$\frac{|\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)|}{|\mathcal{F}_d|} = \frac{|\mathcal{F}_d(\alpha_1,\beta_1)|}{|\mathcal{F}_d|} = \frac{E_{\mathcal{F}_d}(u_1)}{q^{u_1}} + O\left(q^{-d/2}\right). \tag{14}$$

*Otherwise, we get zero.*

*Let $\alpha_1, \dots, \alpha_n \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degrees $u_1, \dots, u_n$ over $\mathbb{F}_q$ and let $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le n$.*

*If none of the $\alpha_i$ are conjugate to each other. Then*

$$\frac{|\mathcal{F}_d(\alpha_1,\dots,\alpha_n,\beta_1,\dots\beta_n)|}{|\mathcal{F}_d|} = \frac{E_{\mathcal{F}_d}(u_1,\dots,u_n)}{q^{u_1+\cdots+u_n}} + O(q^{-d/2}), \tag{15}$$

*where $E_{\mathcal{F}_d}(u_1,\dots,u_n)$ does not depend on the values of $\beta_1,\dots,\beta_n$.*

*If some of the $\alpha_i$'s are conjugate to others, then we get zero, unless the corresponding $\beta_i$'s are conjugate by the same automorphisms and in that case we get formula* (15)*, where the $u_i$'s correspond to the degrees for each of the* different *conjugacy classes of the $\alpha_i$'s.*

*Proof.* This follows from Propositions 3.8, 3.10, 4.3, 4.5, 5.2 and 5.6. □

We recall that for a family $\mathcal{F}$, a function $G$ depending on $f$, and a vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$, we have the notation

$$\begin{aligned}\langle G(f)\rangle_{\mathcal{F}} &:= \frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} G(f),\\ \langle G(f)\rangle_{\mathcal{F},\boldsymbol{\alpha}} &:= \frac{1}{|\mathcal{F}|}\sum_{\substack{f\in\mathcal{F}\\ f(\alpha_i)\neq\infty, 1\le i\le n}} G(f).\end{aligned}$$

The main idea in the computations of moments is that if we sum the value of a non-trivial additive character $\psi$ evaluated at a linear combination of the traces $\operatorname{tr}_{u_i}(\beta_i)$ over all $\beta_i \in \mathbb{F}_{q^{u_i}}$ for $1 \le i \le s$, then the sum will be 0 unless each coefficient is divisible by $p$.

**Lemma 8.4.** *Let $m_1, \dots, m_s \in \mathbb{Z}$, and $\psi$ a non-trivial additive character of $\mathbb{F}_p$. Then,*

$$\sum_{\beta_i\in\mathbb{F}_{q^{u_i}}\ 1\le i\le s} \psi(m_1 \operatorname{tr}_{u_1}(\beta_1) + \cdots + m_s \operatorname{tr}_{u_s}(\beta_s)) = \begin{cases} q^{u_1+\cdots+u_s} & p \mid m_i \text{ for } 1 \le i \le s,\\ 0 & \text{otherwise.}\end{cases}$$

8.1. **First moment.**

**Lemma 8.5.** *Let $h$ be an integer such that $p \nmid h$, $e \in \{-1, 1\}$, and $k > 0$. Let $\alpha \in \mathbb{F}_{q^k}$ of degree $u$ over $\mathbb{F}_q$. Let $\mathcal{F}_d$ be any of the families under consideration. We have,*

$$\langle \psi(eh \operatorname{tr}_k f(\alpha))\rangle_{\mathcal{F}_d,\alpha} = \begin{cases} E_{\mathcal{F}_d}(u) + O\left(q^{u-d/2}\right) & p \mid \frac{k}{u},\\ O\left(q^{u-d/2}\right) & \text{otherwise.}\end{cases}$$

*Proof.* By reversing the order of summation, we obtain

$$\langle \psi(eh\,\mathrm{tr}_k\, f(\alpha))\rangle_{\mathcal{F}_d,\alpha} \quad = \quad \sum_{\beta\in\mathbb{F}_{q^u}} \psi(eh\,\mathrm{tr}_k(\beta))\frac{|\mathcal{F}_d(\alpha,\beta)|}{|\mathcal{F}_d|}.$$

We now apply Lemma 8.3 in order to obtain

$$\frac{E_{\mathcal{F}_d}(u)}{q^u}\sum_{\beta\in\mathbb{F}_{q^u}} \psi\left(\frac{ehk}{u}\,\mathrm{tr}_u(\beta)\right) + O\left(q^{u-d/2}\right).$$

Lemma 8.4 implies that the main term is zero unless $p \mid \frac{k}{u}$. This completes the proof of the statement. □

For positive integers $k, h$ with $p \nmid h$ and $e \in \{-1, 1\}$, set

$$\begin{aligned} M_{1,d}^{k,e,h} &:= \left\langle q^{-k/2} \sum_{\substack{\alpha\in\mathbb{F}_{q^k}\\ f(\alpha)\neq\infty}} \psi(eh\,\mathrm{tr}_k\, f(\alpha))\right\rangle_{\mathcal{F}_d} \\ &= q^{-k/2}\sum_{\alpha\in\mathbb{F}_{q^k}} \langle \psi(eh\,\mathrm{tr}_k\, f(\alpha))\rangle_{\mathcal{F}_d,\alpha}. \end{aligned}$$

Lemma 8.5 has the following consequence.

**Theorem 8.6.** *Let $h$ be an integer such that $p \nmid h$ and let $\mathcal{F}_d$ be any of the families under consideration. Then*

$$\begin{aligned} M_{1,d}^{k,e,h} &= e_{p,k}\left(E_{\mathcal{F}_d}(k/p)\, q^{-(1/2-1/p)k} + O\left(q^{-(1/2-1/2p)k}\right)\right) + O\left(q^{3k/2-d/2}\right) \\ &= O\left(q^{-(1/2-1/p)k} + q^{3k/2-d/2}\right), \end{aligned}$$

*where*

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

*Proof.* By Lemma 8.5, we have that

$$\begin{aligned} M_{1,d}^{k,e,h} &= q^{-k/2} \sum_{\substack{u,pu\mid k\\ \alpha\in\mathbb{F}_{q^k},\deg(\alpha)=u}} E_{\mathcal{F}_d}(u) + q^{-k/2}\sum_{\alpha\in\mathbb{F}_{q^k}} O(q^{\deg(\alpha)-d/2}) \\ &= \frac{e_{p,k}}{q^{k/2}}\sum_{m,pm\mid k} E_{\mathcal{F}_d}(m)\pi(m)m + O\left(q^{3k/2-d/2}\right). \end{aligned}$$

Finally, if $p \mid k$, the estimates from Remark 8.2 yield

$$\sum_{m,pm\mid k} E_{\mathcal{F}_d}(m)\pi(m)m = E_{\mathcal{F}_d}(k/p)\, q^{k/p} + O\left(q^{k/2p}\right).$$

□

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

**Theorem 8.7.** *Let $h$ be an integer such that $p \nmid h$ and let $\mathcal{F}_d$ be any of the families under consideration. Then for any $K$ with* $\max\{1, 1/|\mathcal{I}|\} < K < d/3$,

$$\left\langle S^{\pm}(K, f, \psi^h)\right\rangle_{\mathcal{F}_d} = O(1).$$

*Proof.* We have that

$$\begin{aligned}\left\langle S^{\pm}(K,f,\psi^h)\right\rangle_{\mathcal{F}_d} &= \sum_{k=1}^{K}\frac{\widehat{I}_K^{\pm}(k)\left\langle S_k(f,\psi^h)\right\rangle_{\mathcal{F}_d}+\widehat{I}_K^{\pm}(-k)\left\langle S_k(f,\bar{\psi}^h)\right\rangle_{\mathcal{F}_d}}{q^{k/2}}\\ &= \sum_{k=1}^{K}\widehat{I}_K^{\pm}(k)M_{1,d}^{k,1,h}+\widehat{I}_K^{\pm}(-k)M_{1,d}^{k,-1,h}\\ &= \sum_{k=1}^{K}\widehat{I}_K^{\pm}(k)O\left(q^{-(1/2-1/p)k}+q^{3k/2-d/2}\right).\end{aligned}$$

and the result follows from Proposition 6.2. □

**Theorem 8.8.** *Let $\mathcal{F}_d$ be any of the families under consideration. Then,*

$$\begin{aligned}\langle N_{\mathcal{I}}(f,\psi)\rangle_{\mathcal{F}_d}=\frac{1}{|\mathcal{F}_d|}\sum_{f\in\mathcal{F}_d}N_{\mathcal{I}}(f,\psi) &= (\Delta-1)|\mathcal{I}|+O(1)\\ \langle N_{\mathcal{I}}(C_f)\rangle_{\mathcal{F}_d}=\frac{1}{|\mathcal{F}_d|}\sum_{f\in\mathcal{F}_d}N_{\mathcal{I}}(C_f) &= 2\mathfrak{g}|\mathcal{I}|+O(1).\end{aligned}$$

*Proof.* This follows from Theorem 8.7 and equations (9) and (10) using $K=\varepsilon d$ for any $0<\varepsilon<1/3$. □

8.2. **Second moment.**

**Lemma 8.9.** *Let $h_1,h_2$ be integers such that $p\nmid h_1h_2$, $e_1,e_2\in\{-1,1\}$ and $k_1,k_2>0$. Let $\alpha_1\in\mathbb{F}_{q^{k_1}}$, $\alpha_2\in\mathbb{F}_{q^{k_2}}$ of degrees $u_1,u_2$ respectively over $\mathbb{F}_q$. For any of the families under consideration, we have,*

$$\begin{aligned}&\langle\psi(e_1h_1\operatorname{tr}_{k_1}f(\alpha_1)+e_2h_2\operatorname{tr}_{k_2}f(\alpha_2))\rangle_{\mathcal{F}_d,(\alpha_1,\alpha_2)}\\ &=\begin{cases}E_{\mathcal{F}_d}(u_1)+O\left(q^{u_1-d/2}\right) & \alpha_1\sim\alpha_2,\ p\mid\dfrac{e_1h_1k_1+e_2h_2k_2}{u_1},\\ O\left(1+q^{u_1+u_2-d/2}\right) & \alpha_1\not\sim\alpha_2,\ p\mid\left(\frac{k_1}{u_1},\frac{k_2}{u_2}\right),\\ O\left(q^{u_1+u_2-d/2}\right) & \textit{otherwise.}\end{cases}\end{aligned}$$

*Proof.* Reversing the order of summation, we write

$$\begin{aligned}&\langle\psi(e_1h_1\operatorname{tr}_{k_1}f(\alpha_1)+e_2h_2\operatorname{tr}_{k_2}f(\alpha_2))\rangle_{\mathcal{F}_d,(\alpha_1,\alpha_2)}\\ &=\sum_{\beta_1\in\mathbb{F}_{q^{u_1}},\beta_2\in\mathbb{F}_{q^{u_2}}}\psi(e_1h_1\operatorname{tr}_{k_1}\beta_1+e_2h_2\operatorname{tr}_{k_2}\beta_2)\frac{|\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)|}{|\mathcal{F}_d|}.\end{aligned}\tag{16}$$

Assume that $\alpha_1\not\sim\alpha_2$. By Lemma 8.3 we can write (16) as

$$\frac{E_{\mathcal{F}_d}(u_1,u_2)}{q^{u_1+u_2}}\sum_{\beta_1\in\mathbb{F}_{q^{u_1}},\beta_2\in\mathbb{F}_{q^{u_2}}}\psi\left(\frac{e_1h_1k_1}{u_1}\operatorname{tr}_{u_1}\beta_1+\frac{e_2h_2k_2}{u_2}\operatorname{tr}_{u_2}\beta_2\right)+O\left(q^{u_1+u_2-d/2}\right).$$

Then Lemma 8.4 implies that the sum is zero unless $p\mid\frac{k_1}{u_1}$ and $p\mid\frac{k_2}{u_2}$.

Now assume that $\alpha_1\sim\alpha_2$. Then $f(\alpha_1)\sim f(\alpha_2)$ and $\operatorname{tr}_{u_1}f(\alpha_1)=\operatorname{tr}_{u_1}f(\alpha_2)$. By Lemma 8.3 we can write (16) as

$$\frac{E_{\mathcal{F}_d}(u_1)}{q^{u_1}}\sum_{\beta_1\in\mathbb{F}_{q^{u_1}}}\psi\left(\frac{e_1h_1k_1+e_2h_2k_2}{u_1}\operatorname{tr}_{u_1}\beta_1\right)+O\left(q^{u_1-d/2}\right).$$

Then Lemma 8.4 implies that the sum is zero unless $p\mid\frac{e_1h_1k_1+e_2h_2k_2}{u_1}$.

□

**Lemma 8.10.** *Let $h_1, h_2$ be integers such that $p \nmid h_1h_2$, $e_1, e_2 \in \{-1, 1\}$ and $k_1, k_2 > 0$, $k_1 \geq k_2$. Let $\mathcal{F}_d$ be any of the families under consideration. Then,*

$$\sum_{\substack{m|(k_1,k_2)\\ mp\nmid k_1,k_2\\ mp|(e_1h_1k_1+e_2h_2k_2)}} E_{\mathcal{F}_d}(m)\pi(m)m^2 = \begin{cases} E_{\mathcal{F}_d}(k_1)k_1q^{k_1} + O\left(k_1q^{k_1/2}\right) & k_1 = k_2, p \mid (e_1h_1 + e_2h_2),\\ 0 & k_1 = k_2, p \nmid (e_1h_1 + e_2h_2),\\ O\left(k_1q^{k_1/2}\right) & k_1 = 2k_2,\\ O\left(k_1q^{k_1/3}\right) & k_1 \neq k_2, 2k_2. \end{cases}$$

*Proof.* For the first case when $k_1 = k_2$, the conditions on the summation indices become $m \mid k_1$, $mp \nmid k_1$, and $mp \mid (e_1h_1 + e_2h_2)k_1$, a contradiction unless $p \mid (e_1h_1 + e_2h_2)$. In this case, one gets

$$\sum_{\substack{m|k_1\\ mp\nmid k_1}} E_{\mathcal{F}_d}(m)\pi(m)m^2 = E_{\mathcal{F}_d}(k_1)k_1q^{k_1} + O\left(k_1q^{k_1/2}\right),$$

where we have used the estimates for $\pi(m)$ and $E_{\mathcal{F}_d}(m)$ discussed in Remark 8.2.

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

$$\sum_{\substack{m|k_2\\ mp\nmid k_2\\ mp|(2e_1h_1+e_2h_2)k_2}} E_{\mathcal{F}_d}(m)\pi(m)m^2 = O\left(k_1q^{k_1/2}\right).$$

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

$$\sum_{\substack{m|(k_1,k_2)\\ mp\nmid k_1,k_2\\ mp|(e_1h_1k_1+e_2h_2k_2)}} E_{\mathcal{F}_d}(m)\pi(m)m^2 = O\left(k_1q^{k_1/3}\right).$$

This completes the proof. □

For positive integers $k_1, k_2, h_1, h_2$ with $p \nmid h_1h_2$ and $e_1, e_2 \in \{-1, 1\}$, let

$$\begin{aligned} M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} &:= \left\langle q^{-(k_1+k_2)/2} \sum_{\substack{\alpha_1\in\mathbb{F}_{q^{k_1}},\alpha_2\in\mathbb{F}_{q^{k_2}}\\ f(\alpha_1)\neq\infty, f(\alpha_2)\neq\infty}} \psi(e_1h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2h_2 \operatorname{tr}_{k_2} f(\alpha_2)) \right\rangle_{\mathcal{F}_d} \\ &= q^{-(k_1+k_2)/2} \sum_{\substack{\alpha_1\in\mathbb{F}_{q^{k_1}}\\ \alpha_2\in\mathbb{F}_{q^{k_2}}}} \langle \psi(e_1h_1 \operatorname{tr}_{k_1} f(\alpha_1) + e_2h_2 \operatorname{tr}_{k_2} f(\alpha_2))\rangle_{\mathcal{F}_d,(\alpha_1,\alpha_2)}. \end{aligned}$$

Using Lemma 8.10, we can prove the following analogue of Theorem 8 in [Ent12].

**Theorem 8.11.** *Let $0 < h_1, h_2 \leq (p-1)/2$, $e_1, e_2 \in \{-1, 1\}$, $k_1 \geq k_2 > 0$, and let $\mathcal{F}_d$ be any of the families under consideration. Then*

$$\begin{aligned} M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} &= \begin{cases} \delta_{k_1,k_2}\left(E_{\mathcal{F}_d}(k_1)k_1 + O\left(k_1q^{-k_1/2} + k_1q^{(k_1-d/2)}\right)\right) & e_1 = -e_2,\ h_1 = h_2,\\ 0 & \textit{otherwise}, \end{cases} \\ &\quad + \delta_{k_1,2k_2}O\left(k_1q^{-k_2/2} + k_1q^{k_2/2-d/2}\right) \\ &\quad + O\left(k_1q^{-k_2/2-k_1/6} + k_1q^{k_1/6-k_2/2-d/2}\right) \\ &\quad + O\left(q^{(1/p-1/2)(k_1+k_2)} + q^{3(k_1+k_2)/2-d/2}\right) \end{aligned}$$

*where*

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

*Proof.* From Lemma 8.9, we have

$$
\begin{aligned}
M_{2,d}^{(k_1,k_2),(e_1,e_2),(h_1,h_2)} &= \frac{e_{p,e_1h_1k_1+e_2h_2k_2}}{q^{(k_1+k_2)/2}} \sum_{\substack{m|(k_1,k_2)\\ mp\nmid k_1,k_2\\ mp|(e_1h_1k_1+e_2h_2k_2)}} \pi(m)m^2\left(E_{\mathcal{F}_d}(m)+O(q^{m-d/2})\right)\\
&\quad +O\left(\frac{e_{p,k_1}e_{p,k_2}}{q^{(k_1+k_2)/2}} \sum_{\substack{\deg\alpha_1=u_1,\deg\alpha_2=u_2\\ p|\frac{k_1}{u_1},p|\frac{k_2}{u_2}}} \left(1+q^{u_1+u_2-d/2}\right)\right)\\
&\quad +O\left(\frac{1}{q^{(k_1+k_2)/2}} \sum_{\substack{\deg\alpha_1=u_1,\deg\alpha_2=u_2\\ u_1|k_1,u_2|k_2}} q^{u_1+u_2-d/2}\right).
\end{aligned}
$$

It is easy to see that the last two terms are

$$O\left(q^{(1/p-1/2)(k_1+k_2)}+q^{3(k_1+k_2)/2-d/2}\right).$$

For the first term, we use Lemma 8.10. As a final observation, the condition $p \mid e_1h_1+e_2h_2$ translates into $h_1=h_2$ and $e_1=-e_2$ because of the restriction on the possible values for $h_1,h_2$. This concludes the proof of the theorem. □

Using Lemma 8.10, we can prove the following result which will also be used in the general moments.

**Proposition 8.12.** *Let $h_1,h_2$ be integers such that $p\nmid h_1h_2$, $e_1,e_2\in\{-1,1\}$ and $k_1,k_2>0$. Let $\mathcal{F}_d$ be any of the families under consideration. Then,*

$$
\begin{aligned}
&\sum_{k_1,k_2=1}^{K} \widehat{I}_K^{\pm}(e_1k_1)\widehat{I}_K^{\pm}(e_2k_2)q^{-(k_1+k_2)/2} \sum_{\substack{m|(k_1,k_2)\\ mp\nmid k_1,k_2\\ mp|(e_1h_1k_1+e_2h_2k_2)}} E_{\mathcal{F}_d}(m)\pi(m)m^2\\
&= \begin{cases} \dfrac{1}{2\pi^2}\log\left(K|\mathcal{I}|\right)+O(1) & p\mid(e_1h_1+e_2h_2),\\[2ex] O(1) & \textit{otherwise.}\end{cases}
\end{aligned}
$$

*Proof.* Using Lemma 8.10, we have the sum is

$$
\begin{aligned}
&e_{p,e_1h_1+e_2h_2}\sum_{k_1=1}^{K}\widehat{I}_K^{\pm}(k_1)\widehat{I}_K^{\pm}(-k_1)\left(E_{\mathcal{F}_d}(k_1)k_1+O\left(k_1q^{-k_1/2}\right)\right)+O\left(\sum_{k_1=1}^{K}k_1q^{-k_1/4}+\sum_{k_1,k_2=1}^{K}k_1q^{-k_1/6}q^{-k_2/2}\right)\\
&=e_{p,e_1h_1+e_2h_2}\sum_{k_1=1}^{K}\widehat{I}_K^{\pm}(k_1)\widehat{I}_K^{\pm}(-k_1)E_{\mathcal{F}_d}(k_1)k_1+O(1).
\end{aligned}
$$

Now the estimates from Remark 8.2 and Proposition 6.1 yield

$$
\begin{aligned}
\sum_{k_1=1}^{K}\widehat{I}_K^{\pm}(k_1)\widehat{I}_K^{\pm}(-k_1)E_{\mathcal{F}_d}(k_1)k_1 &= \sum_{k_1=1}^{K}\widehat{I}_K^{\pm}(k_1)\widehat{I}_K^{\pm}(-k_1)k_1+O\left(\sum_{k_1=1}^{K}k_1^2q^{-k_1}\right)\\
&= \frac{1}{2\pi^2}\log(K|\mathcal{I}|)+O(1),
\end{aligned}
$$

which finishes the proof of the statement.

□

Finally, we are able to compute the covariances.

**Theorem 8.13.** *Let $0 < h_1, h_2 \leq (p-1)/2$, and let $\mathcal{F}_d$ be any of the families under consideration. Then for any $K$ with $1/|\mathcal{I}| < K < d/6$,*

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

*Proof.* By definition,

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

Using Theorem 8.11 to replace the terms above, we first remark that the contribution of the last two error terms from Theorem 8.11 to the sum is

$$\ll \sum_{k_1,k_2=1}^{K} k_1 q^{-k_2/2-k_1/6} + k_1 q^{k_1/6-k_2/2-d/2} + q^{(1/p-1/2)(k_1+k_2)} + q^{3(k_1+k_2)/2-d/2} \ll 1$$

provided that $d > 6K$.

Similarly, the contribution of the error terms for $k_1 = k_2$ and $k_1 = 2k_1$ is bounded by

$$\ll \sum_{k=1}^{K} kq^{-k/2} + kq^{k-d/2} \ll 1$$

provided that $d > 2K$. Finally, the main term comes from summing $E_{\mathcal{F}_d}(k_1)k_1$ when $k_1 = k_2$, and this occurs only when $h_1 = h_2$ and $\{e_1, e_2\} = \{1, -1\}$. Proceeding as in the proof of Proposition 8.12, we then get that

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

The proof for $\left\langle S^{\pm}(K,f,\psi^{h_1})S^{\mp}(K,f,\psi^{h_2})\right\rangle_{\mathcal{F}_d}$ follows exactly along the same lines. □

**Corollary 8.14.** *For any $K$ with $1/|\mathcal{I}| < K < d/6$,*

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

*Proof.* First we note that

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

Notice that by Theorem 8.13, 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 $\langle S^{+}(K,C_f)S^{-}(K,C_f)\rangle_{\mathcal{F}_d}$ is identical. □

8.3. **General moments.** Let $n, k_1, \dots, k_n$ be positive integers, let $e_1, \dots, e_n$ take values $\pm 1$, 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 $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$. Let $\mathcal{F}_d$ be any of the families under consideration. Then, we define

$$\begin{aligned} m_n^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) &= \langle \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + \dots + e_n h_n \operatorname{tr}_{k_n} f(\alpha_n)) \rangle_{\mathcal{F}_d, \boldsymbol{\alpha}} \\ &= \frac{1}{|\mathcal{F}_d|} \sum_{\substack{f \in \mathcal{F}_d \\ f(\alpha_i) \neq \infty, 1 \le i \le n}} \psi(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + \dots + e_n h_n \operatorname{tr}_{k_n} f(\alpha_n)), \end{aligned}$$

and

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

**Lemma 8.15.** *Let $\mathcal{F}_d$ be any of the families under consideration. Let $C_1, \dots, C_s$ be the distinct conjugacy classes of the $\alpha_1, \dots, \alpha_n$. Let $u_i$ be the degree of the elements of $C_i$. For $i = 1, \dots, s$, let*

$$\eta_i = \frac{1}{u_i} \sum_{\alpha_j \in C_i} e_j h_j k_j.$$

*Then*

$$m_n^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) = \begin{cases} E_{\mathcal{F}_d}(u_1, \dots, u_s) + O\left(q^{u_1+\dots+u_s-d/2}\right) & \text{if } p \mid \eta_i \text{ for } 1 \le i \le s, \\ O\left(q^{u_1+\dots+u_s-d/2}\right) & \text{otherwise.} \end{cases}$$

*Proof.* Renumbering, suppose that $\alpha_i \in C_i$ for $1 \le i \le s$. Since $\operatorname{tr}_{k_i} f(\alpha_i) = \frac{k_i}{u_i} \operatorname{tr}_{u_i} f(\alpha_i)$ for $i = 1, \dots, s$, by the definition of $\eta_i$, we have that

$$\begin{aligned} m_n^{\mathbf{k},\mathbf{e},\mathbf{h}}(\boldsymbol{\alpha}) &= \frac{1}{|\mathcal{F}_d|} \sum_{\substack{f \in \mathcal{F}_d \\ f(\alpha_i) \neq \infty, 1 \le i \le n}} \psi\left(e_1 h_1 \operatorname{tr}_{k_1} f(\alpha_1) + \dots + e_n h_n \operatorname{tr}_{k_n} f(\alpha_n)\right) \\ &= \frac{1}{|\mathcal{F}_d|} \sum_{\substack{f \in \mathcal{F}_d \\ f(\alpha_i) \neq \infty, 1 \le i \le n}} \psi\left(\eta_1 \operatorname{tr}_{u_1} f(\alpha_1) + \dots + \eta_s \operatorname{tr}_{u_s} f(\alpha_s)\right) \\ &= \sum_{\beta_i \in \mathbb{F}_{q^{u_i}},\, 1 \le i \le s} \psi\left(\eta_1 \operatorname{tr}_{u_1} \beta_1 + \dots + \eta_s \operatorname{tr}_{u_s} \beta_s\right) \frac{|\mathcal{F}_d(\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s)|}{|\mathcal{F}_d|} \\ &= \frac{E_{\mathcal{F}_d}(u_1, \dots, u_s)}{q^{u_1+\dots+u_s}} \sum_{\beta_i \in \mathbb{F}_{q^{u_i}},\, 1 \le i \le s} \psi\left(\eta_1 \operatorname{tr}_{u_1} \beta_1 + \dots + \eta_s \operatorname{tr}_{u_s} \beta_s\right) + O\left(q^{u_1+\dots+u_s-d/2}\right) \end{aligned}$$

by Lemma 8.3. The result now follows from Lemma 8.4. $\square$

**Lemma 8.16.** *$M_n^{\mathbf{k},\mathbf{e},\mathbf{h}}$ is bounded by a sum of terms $q^{-(k_1+\dots+k_n)/2} T(k_1, \dots, k_n)$, where each $T(k_1, \dots, k_n)$ is a product of elementary terms of the type*

$$\sum_{\substack{m \mid (j_1, \dots, j_r) \\ mp \mid \sum_{i=1}^r e_i h_i j_i}} \pi(m) m^r$$

*such that the indices $j_1, \dots, j_r$ of the elementary terms appearing in each $T(k_1, \dots, k_n)$ are in bijection with $k_1, \dots, k_n$.*

*For $n = 2\ell$ even, let $N_n^{\mathbf{k},\mathbf{e},\mathbf{h}}$ be the sum of all possible terms $q^{-(k_1+\dots+k_n)/2} T(k_1, \dots, k_n)$ where the $T(k_1, \dots, k_n)$ are made exclusively of the following nested sums*

$$\sum_{\substack{m_1 \mid (j_1, j_{\ell+1}) \\ m_1 p \mid e_1 h_1 j_{\ell+1} + e_{\ell+1} h_{\ell+1} j_{\ell+1}}} \pi(m_1) m_1^2 \cdots \sum_{\substack{m_\ell \mid (j_\ell, j_{2\ell}) \\ m_\ell p \mid e_\ell h_\ell j_{2\ell} + e_{2\ell} h_{2\ell} j_{2\ell}}} \pi(m_\ell) m_\ell^2 E_{\mathcal{F}_d}(m_1, \dots, m_\ell). \tag{17}$$

*If $n = 2\ell+1$ is odd, let $N_n^{\mathbf{k},\mathbf{e},\mathbf{h}}$ be the sum of all possible terms $q^{-(k_1+\cdots+k_n)/2}T(k_1,\ldots,k_n)$ where $T(k_1,\ldots,k_n)$ are made exclusively of the following nested sums*

(18)

$$\sum_{\substack{m_1|(j_1,j_{\ell+1})\\ m_1p|e_1h_1j_{\ell+1}+e_{\ell+1}h_{\ell+1}j_{\ell+1}}} \pi(m_1)m_1^2\cdots \sum_{\substack{m_\ell|(j_\ell,j_{2\ell})\\ m_\ell p|e_\ell h_\ell j_{2\ell}+e_{2\ell}h_{2\ell}j_{2\ell}}} \pi(m_\ell)m_\ell^2 \sum_{\substack{m_{\ell+1}|j_{2\ell+1}\\ m_{\ell+1}p|e_{2\ell+1}h_{2\ell+1}j_{2\ell+1}}} \pi(m_{\ell+1})m_{\ell+1}E_{\mathcal{F}_d}(m_1,\ldots,m_\ell,m_{\ell+1}).$$

*Let $L_n^{\mathbf{k},\mathbf{e},\mathbf{h}}$ be the sum of all the other terms $q^{-(k_1+\cdots+k_n)/2}T(k_1,\ldots,k_n)$ as defined above. Then,*

$$M_n^{\mathbf{k},\mathbf{e},\mathbf{h}} = N_{n,d}^{\mathbf{k},\mathbf{e},\mathbf{h}} + O\left(L_n^{\mathbf{k},\mathbf{e},\mathbf{h}}\right) + O\left(q^{3(k_1+\cdots+k_n)/2-d/2}\right).$$

*Proof.* Using Lemma 8.15, we first write

$$M_n^{\mathbf{k},\mathbf{e},\mathbf{h}} = q^{-(k_1+\cdots+k_n)/2} \sum_{\substack{\alpha_i\in\mathbb{F}_{q^{k_i}},\ i=1,\ldots,n\\ (\alpha_1,\ldots,\alpha_n)\in\mathcal{A}}} E_{\mathcal{F}_d}(u_1,\ldots,u_s) + O\left(q^{3(k_1+\cdots+k_n)/2-d/2}\right),$$

where the set $\mathcal{A}$ of admissible $(\alpha_1,\ldots,\alpha_n)$ are those where $p \mid \eta_i,\ i=1,\ldots,s$. To count the number of admissible $(\alpha_1,\ldots,\alpha_n)$, we first fix a partition of $\{1,\ldots,n\}$ in $s$ classes $C_1,\ldots C_s$. Let $k(C_w)$ be the gcd of the $k_i$ such that $i\in C_w$ and let $\delta(C_w)=\sum_{i\in C_w} e_ih_ik_i$. Then, for any such partition, the number of $(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}_{q^{k_1}}\times\cdots\times\mathbb{F}_{q^{k_n}}$ such that $\alpha_i$ and $\alpha_j$ are conjugate when $i,j$ are in the same class $C_w$ and which are counted in $\mathcal{A}$ is bounded by

$$\prod_{i=1}^{s}\sum_{\substack{m|k(C_i)\\ mp|\delta(C_i)}}\pi(m)m^{|C_i|}, \tag{19}$$

where we have used the fact that the number of $(\alpha_1,\ldots,\alpha_t)\in\mathbb{F}_{q^{k_1}}\times\cdots\times\mathbb{F}_{q^{k_t}}$ which are conjugate over $\mathbb{F}_q$ is given by

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

Since $E_{\mathcal{F}}(u_1,\ldots,u_s)\ll 1$ by Remark 8.2, we get the first result of the statement by summing (19) over all partitions of $\{1,\ldots,n\}$ in $s$ classes $C_1,\ldots C_s$.

Suppose that $n=2\ell$ is even. Then, using inclusion-exclusion, the number of $(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}_{q^{k_1}}\times\cdots\times\mathbb{F}_{q^{k_n}}$ such that $\alpha_i$ and $\alpha_j$ are conjugate, if and only if $i\equiv j (\mathrm{mod}\ell)$ can be written as

$$\left(\sum_{\substack{m_1|(k_1,k_{\ell+1})\\ m_1p|e_1h_1k_1+e_{\ell+1}h_{\ell+1}k_{\ell+1}}}\pi(m_1)m_1^2\cdots\sum_{\substack{m_\ell|(k_\ell,k_{2\ell})\\ m_\ell p|e_\ell h_\ell k_\ell+e_{2\ell}h_{2\ell}k_{e\ell}}}\pi(m_\ell)m_\ell^2E_{\mathcal{F}_d}(m_1,\ldots,m_\ell)\right)+S(k_1,\ldots,k_n)$$

where $S(k_1,\ldots,k_n)$ is a sum of terms in $L_n^{\mathbf{k},\mathbf{e},\mathbf{h}}$. (We have to do inclusion-exclusion to remove the cases where conjugate values of $\alpha$ belong to two different classes $C_w$.)

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

**Theorem 8.17.** *Let $\mathcal{F}_d$ be any of the families under consideration. For any $K$ with $1/|\mathcal{I}|<K<d/n$*

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

*More generally, let $0<h_1,\ldots,h_n\le(p-1)/2$. Then for any $K$ with $1/|\mathcal{I}|<K<d/n$,*

$$\left\langle S^{\pm}(K,f,\psi^{h_1})\ldots S^{\pm}(K,f,\psi^{h_n})\right\rangle_{\mathcal{F}_d} = \begin{cases} \frac{\Theta(h_1,\ldots,h_n)}{(2\pi^2)^\ell}\log^\ell(K|\mathcal{I}|)\left(1+O\left(\log^{-1}(K|\mathcal{I}|)\right)\right) & n=2\ell,\\ O\left(\log^\ell(K|\mathcal{I}|)\right) & n=2\ell+1.\end{cases}$$

*The constant $\Theta(h_1, \dots, h_n)$ is given by*

$$\#\{(e_1, \dots, e_n) \in \{-1, 1\}, \sigma \in \mathbb{S}_n \ : \ e_1 h_{\sigma(1)} + e_2 h_{\sigma(2)} \equiv \cdots \equiv e_{2\ell-1} h_{\sigma(2\ell-1)} + e_{2\ell} h_{\sigma(2\ell)} \equiv 0 \,(\operatorname{mod} p)\}$$

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

*Proof.* We have that

$$\left\langle S^{\pm}(K, f, \psi^{h_1}) \dots S^{\pm}(K, f, \psi^{h_n}) \right\rangle_{\mathcal{F}_d} = \sum_{\substack{k_1, \dots, k_n = 1 \\ e_1, \dots, e_n = \pm 1}}^{K} I_K^{\pm}(e_1 k_1) \dots I_K^{\pm}(e_n k_n) M_n^{\mathbf{k}, \mathbf{e}, \mathbf{h}},$$

and we use Lemma 8.16 to replace $M_n^{\mathbf{k}, \mathbf{e}, \mathbf{h}}$ in the sum. The error term satisfies

$$\sum_{\substack{k_1, \dots, k_n = 1 \\ e_1, \dots, e_n = \pm 1}}^{K} I_K^{\pm}(e_1 k_1) \dots I_K^{\pm}(e_n k_n) O\left(q^{3(k_1 + \cdots + k_n)/2 - d/2}\right) \ll \left(\sum_{k=1}^{K} q^{3k/2 - d/2n}\right)^n \ll 1$$

when $d > 3nK$.

For the main term, we have to consider the sum of the terms $T(k_1, \dots, k_n)$ from Lemma 8.16. For each fixed $T(k_1, \dots, k_n)$, we write the sum over $k_1, \dots, k_n$ as $s$ nested sums $\Sigma_1 \dots \Sigma_s E_{\mathcal{F}_d}(m_1, \dots, m_s)$ where $\Sigma_w$ is a sum over the $k_i$ such that $i \in C_w$, and $|E_{\mathcal{F}_d}(m_1, \dots, m_s)| \ll 1$. If $|C_w| = 1$, then we have a sum

$$\sum_{k=1}^{K} \widehat{I}_K^{\pm}(k) q^{-k/2} \sum_{\substack{m | k \\ mp | e_k}} \pi(m) m \ll 1, \tag{20}$$

because of Theorem 8.7. For $r = |C_w| \geq 2$, we have a sum of the type

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

When $r = |C_w| > 2$, we will show in Lemma 8.18 that the contribution from the terms of the sum over $k_1, \dots, k_r$ is bounded. Assuming this result, we have by Lemma 8.16 that the leading term in $S^{\pm}(K, f, \psi)^n$ will come from the contributions $N_{n,d}^{\mathbf{k}, \mathbf{e}, \mathbf{h}}$.

If $n = 2\ell$, the leading terms are of the form

$$\sum_{k_1, \dots, k_r = 1}^{K} \widehat{I}_K^{\pm}(e_1 k_1) \dots \widehat{I}_K^{\pm}(e_r k_r) q^{-(k_1 + \cdots + k_r)/2} \sum_{\substack{m_1 | (k_1, k_{\ell+1}) \\ m_1 p | e_1 h_1 k_{\ell+1} + e_{\ell+1} h_{\ell+1} k_{\ell+1}}} \pi(m_1) m_1^2 \cdots \sum_{\substack{m_\ell | (k_\ell, k_{2\ell}) \\ m_\ell p | e_\ell h_\ell k_{2\ell} + e_{2\ell} h_{2\ell} k_{2\ell}}} \pi(m_\ell) m_\ell^2$$

$$\times E_{\mathcal{F}_d}(m_1, \dots, m_\ell)$$

By Definition 8.1 and Remark 8.2 combined with Proposition 8.12, for $\mathcal{F}_d = \mathcal{F}_d^{\text{ord}}, \mathcal{F}_d^{\text{full}}$ the above sum gives

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

For $\mathcal{F}_d^v$, we have that $E_{\mathcal{F}_d}(m_1, \dots, m_\ell) = 1$ unless some of the $m_j$'s equal some of the $r_i$'s. Since the $r_i$'s are fixed constants, this simply introduces an error term of the form $O\left(\log\left(K|\mathcal{I}|\right)\right)^{\ell-1}$ which does not change the final result.

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

$$O\left(\log\left(K|\mathcal{I}|\right)\right)^\ell.$$

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

**Lemma 8.18.** *Let $r > 2$, then*

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

*Proof.* Suppose that $k_1 \geq \cdots \geq k_r$. We use repeatedly the estimates from Remark 8.2. If $k_1 = k_r$, we have

$$\sum_{\substack{m|(k_1,\dots,k_r)\\ mp\nmid(k_1,\dots,k_r)}} \pi(m)m^r = O\left(k_1^{r-1}q^{k_1}\right).$$

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

$$\sum_{\substack{m|(k_1,\dots,k_r)\\ mp\nmid(k_1,\dots,k_r)}} \pi(m)m^r = O\left(k_1^{r-1}q^{k_1/2}\right).$$

In all the other cases, the estimate is

$$\sum_{\substack{m|(k_1,\dots,k_r)\\ mp\nmid(k_1,\dots,k_r)}} \pi(m)m^r = O\left(k_1^{r-1}q^{k_1/3}\right).$$

Putting things together, we get

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

by Proposition 6.2. □

**Remark 8.19.** We note that if $n = 2\ell$,

$$\sum_{h_1,\dots,h_n=1}^{(p-1)/2} \Theta(h_1,\dots,h_n) = \frac{(p-1)^{\ell}(2\ell)!}{2^{\ell}\ell!}. \tag{21}$$

There are $\frac{(2\ell)!}{\ell!2^{\ell}}$ ways of choosing unordered pairs of the form $\{e_i, e_j\}$. Inside each pair, exactly one of $\{e_i, e_j\}$ is positive and the other is negative, so there are a total $2^{\ell}$ choices for the signs. Finally, for each pair there are $(p-1)/2$ possible values for $h_i$ which automatically determines the value of $h_j$.

**Remark 8.20.** By Theorem 8.17, the moments are given by sums of products of covariances. Thus, they are the same as the moments of a multivariate normal distribution. Moreover, the generating function of the moments converges due to (21). Therefore, our random variables are jointly normal. Since the variables are uncorrelated (cf. Theorem 8.13), it follows that our random variables are independent.

Recall that

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

**Theorem 8.21.** *Assume that $K = \mathfrak{g}/\log\log(\mathfrak{g}|\mathcal{I}|)$, $\mathfrak{g} \to \infty$ and either $|\mathcal{I}|$ is fixed or $|\mathcal{I}| \to 0$ while $\mathfrak{g}|\mathcal{I}| \to \infty$. Then*

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

*has a standard Gaussian limiting distribution when $\mathfrak{g} \to \infty$.*

*Proof.* First we compute the moments and then we normalize them.

With our choice of $K$ we have

$$\frac{\log(K|\mathcal{I}|)}{\log(\mathfrak{g}|\mathcal{I}|)} = 1 - \frac{\log\log\log(\mathfrak{g}|\mathcal{I}|)}{\log(\mathfrak{g}|\mathcal{I}|)} \to 1 \text{ as } \mathfrak{g} \to \infty.$$

Because of this, $\log(K|\mathcal{I}|)$ can be replaced by $\log(\mathfrak{g}|\mathcal{I}|)$ in our formulas.

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

$$S^{\pm}(K,C_f)^n = \left(2\sum_{h=1}^{(p-1)/2} S^{\pm}(K,f,\psi^h)\right)^n = 2^n \sum_{h_1,\dots,h_n=1}^{(p-1)/2} S^{\pm}(K,f,\psi^{h_1})\dots S^{\pm}(K,f,\psi^{h_n}).$$

Therefore, the moment is given by

$$\left\langle S^{\pm}(K,C_f)^n\right\rangle_{\mathcal{F}_d} = 2^n \sum_{h_1,\dots,h_n=1}^{(p-1)/2} \langle S^{\pm}(K,f,\psi^{h_1})\dots S^{\pm}(K,f,\psi^{h_n})\rangle_{\mathcal{F}_d}.$$

First assume that $n = 2\ell$. By Theorem 8.17, this is asymptotic to

$$\frac{2^n}{(2\pi^2)^\ell}\log^\ell(\mathfrak{g}|\mathcal{I}|)\sum_{h_1,\dots,h_n=1}^{(p-1)/2}\Theta(h_1,\dots,h_n).$$

Finally we use equation (21) to conclude that when $n = 2\ell$,

$$\left\langle S^{\pm}(K,C_f)^n\right\rangle_{\mathcal{F}_d} = \frac{2^n(p-1)^\ell(2\ell)!}{2^\ell\ell!(2\pi^2)^\ell}\log^\ell(\mathfrak{g}|\mathcal{I}|) = \frac{(2\ell)!}{\ell!\pi^{2\ell}}(p-1)^\ell\log^\ell(\mathfrak{g}|\mathcal{I}|).$$

In particular, the variance is asymptotic to $\frac{2(p-1)}{\pi^2}\log(\mathfrak{g}|\mathcal{I}|)$.

Now assume that $n$ is odd, $n = 2\ell+1$. Theorem 8.17 yields

$$\left\langle S^{\pm}(K,C_f)^n\right\rangle_{\mathcal{F}_d} = O\left(\log^\ell(\mathfrak{g}|\mathcal{I}|)\right).$$

Hence the normalized moment converges to

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

for $n = 2\ell$, and to zero for $n$ odd. Hence, we have obtained the moments of the standard Gaussian distribution. □

## 9. The distribution of zeroes

We prove in this section that

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

converges in mean square to

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

Then, using Theorem 8.21, we get the result of Theorem 1.2 since convergence in mean square implies convergence in distribution.

**Lemma 9.1.** *Let $\mathcal{F}_d$ be any of the families under consideration. Assume that $K = \mathfrak{g}/\log\log(\mathfrak{g}|\mathcal{I}|)$, $\mathfrak{g}\to\infty$ and either $|\mathcal{I}|$ is fixed or $|\mathcal{I}|\to 0$ while $\mathfrak{g}|\mathcal{I}|\to\infty$. Then*

$$\left\langle\left|\frac{N_{\mathcal{I}}(C_f) - 2\mathfrak{g}|\mathcal{I}| + S^{\pm}(K,C_f)}{\sqrt{(2(p-1)/\pi^2)\log(\mathfrak{g}|\mathcal{I}|)}}\right|^2\right\rangle_{\mathcal{F}_d}\to 0.$$

*Proof.* From equation (10), using the Beurling–Selberg polynomials and the explicit formula (Lemma 7.1), we deduce that

$$\frac{-2\mathfrak{g}}{K+1}\le N_{\mathcal{I}}(C_f) - 2\mathfrak{g}|\mathcal{I}| + S^{-}(K,C_f)\le S^{-}(K,C_f) - S^{+}(K,C_f) + \frac{2\mathfrak{g}}{K+1}$$

and

$$\frac{-2\mathfrak{g}}{K+1}\le -N_{\mathcal{I}}(C_f) + 2\mathfrak{g}|\mathcal{I}| - S^{+}(K,C_f)\le S^{-}(K,C_f) - S^{+}(K,C_f) + \frac{2\mathfrak{g}}{K+1}.$$

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

$$\begin{aligned}
&\left\langle \left(N_{\mathcal{I}}(C_f) - 2\mathfrak{g}|\mathcal{I}| + S^{\pm}(K,C_f)\right)^2 \right\rangle_{\mathcal{F}_d} \\
\leq\ & \max\left\{ \left(\frac{2\mathfrak{g}}{K+1}\right)^2, \left\langle \left( S^-(K,C_f) - S^+(K,C_f) + \frac{2\mathfrak{g}}{K+1}\right)^2 \right\rangle_{\mathcal{F}_d} \right\} \\
&\leq \left(\frac{2\mathfrak{g}}{K+1}\right)^2 \\
+\ & \max\left\{ 0, \left\langle \left(S^-(K,C_f) - S^+(K,C_f)\right)^2 \right\rangle_{\mathcal{F}_d} + \frac{4\mathfrak{g}}{K+1} \left\langle S^-(K,C_f) - S^+(K,C_f) \right\rangle_{\mathcal{F}_d} \right\}.
\end{aligned}$$

Now Theorem 8.7 implies that

$$\left\langle S^-(K,C_f) - S^+(K,C_f) \right\rangle_{\mathcal{F}_d} \;=\; \left\langle S^-(K,C_f) \right\rangle_{\mathcal{F}_d} - \left\langle S^+(K,C_f) \right\rangle_{\mathcal{F}_d} = O(1).$$

For the remaining term we note that

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

By Corollary 8.14, this equals

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

Therefore,

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

and

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

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

9.1. **Acknowledgments.** The authors would like to thank Rachel Pries for many useful discussions while preparing this paper. A substantial part of this work was completed during a SQuaREs program at the American Institute for Mathematics. The first and third named authors thank the Centre de Recherche Mathématique (CRM) for their hospitality. The fourth author thanks the Graduate Center at CUNY for its hospitality.

This work was supported by the National Science Foundation of U.S. [DMS-1201446 to B. F.], PSC-CUNY [to B.F.], the Simons Foundation [#244988 to A. B.], the UCSD Hellman Fellows Program [2012-2013 Hellman Fellowship to A. B.], the Natural Sciences and Engineering Research Council of Canada [Discovery Grant 155635-2008 to C. D., 355412-2008 to M. L.] and the Fonds de recherche du Québec - Nature et technologies [144987 to M. L., 166534 to C. D. and M. L.]

## 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.

[BDFLS] Alina Bucur, Chantal David, Brooke Feigon, Matilde Lalín, and Kaneenika Sinha. Distribution of zeta zeroes of Artin-Schreier covers. *Math. Res. Lett.*. To appear, arXiv:1111.4701v2.

[BK] Alina Bucur and Kiran S. Kedlaya. The probability that a complete intersection is smooth. *J. Théor des Nombres de Bordeaux* 24, No. 3: 541–556, 2012.

[CWZ] GilYoung Cheong, Melanie Matchett–Wood, and Azeem Zaman. The distribution of points on superelliptic curves over finite fields. *Proc. Amer. Math. Soc.* To appear, arXiv:1210.0456.

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

[DS94] Persi Diaconis and Mehrdad Shahshahani. On the eigenvalues of random matrices. Studies in applied probability. *J. Appl. Probab.* 31A (1994): 49–62.

[Ent12] Alexei Entin. On the distribution of zeroes of Artin-Schreier $L$-functions. *Geom. Funct. Anal.* 22 (2012), no. 5, 1322–1360.

[EW] Daniel Erman, Melanie Matchett–Wood. Semiample Bertini theorems over finite fields. Preprint, arXiv:arXiv:1209.5266v1.

[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.

[Gar05] Arnaldo Garcia. On curves over finite fields. *Arithmetic, geometry and coding theory (AGCT 2003)* Sémin. Congr., 11, Soc. Math. France: 75–110, 2005.

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

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[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.

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

[GV92] Gerard van der Geer and Marcel van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Math.* 84 (1992) no. 3: 333–367.

[Woo12] Melanie Matchett Wood. The distribution of the number of points on trigonal curves over $\mathbb{F}_q$. *Int. Math. Res. Not. IMRN*, 2012, No. 23, 5444–5456 (2012).

[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.

[Xio] Maosheng Xiong. Distribution of zeta zeroes for abelian covers of algebraic curves over a finite field Preprint, arXiv:1301.7124.

[Zhu] Hui June Zhu. Some families of supersingular Artin-Schreier curves in characteristic $>$ 2. Preprint, arXiv:arXiv:0809.0104.



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