Biased statistics for traces of cyclic p-fold covers over finite fields

Alina Bucur*, Chantal David†, Brooke Feigon‡ and Matilde Lalín§

February 25, 2010

Abstract

In this paper, we discuss in more detail some of the results on the statistics of the trace of the Frobenius endomorphism associated to cyclic p-fold covers of the projective line that were presented in [1]. We also show new findings regarding statistics associated to such curves where we fix the number of zeros in some of the factors of the equation in the affine model.

MSC: 11G20, 11T55, 11G25

To epsilon

1 Introduction

Let p be a prime and fix a prime power q such that $q \equiv 1 \pmod p$. In [1], we discussed the statistics for the distribution of the trace of the Frobenius endomorphism of curves C when C varies over irreducible components of the moduli space of cyclic p-fold covers of $\mathbb{P}^1(\mathbb{F}_q)$. To do so, we first consider all curves with affine models

$$Y^p = F(X), \qquad F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} \subseteq \mathbb{F}_q[X], \tag{1.1}$$

where

$$\mathcal{F}_{(d_1,\dots,d_{p-1})} = \{F = F_1F_2^2 \dots F_{p-1}^{p-1} : F_1,\dots,F_{p-1} \in \mathbb{F}_q[X] \text{ are monic, square-free, pairwise coprime, and } \deg F_i = d_i \text{ for } 1 \le i \le p-1\}.$$

Unless otherwise mentioned, all polynomials will be monic.

Roughly speaking, varying over all curves of an irreducible component of the moduli space of cyclic p-fold covers means to vary over models (1.1) with F in certain unions of sets of the type $\mathcal{F}_{(d_1,\dots,d_{p-1})}$, and statistics for the trace of Frobenius over the components of the moduli space can be deduced from the statistics associated to these sets (see Section 5).

Let $\mu_p \subseteq \mathbb{C}^*$ be the set of pth roots of unity, let $\mu_p^0 = \mu_p \cup \{0\}$, let ξ_p be a primitive pth root of unity, and let χ_p be a non-trivial character of order p of $\mathbb{F}_q$. Let C be the cyclic p-fold cover with affine model (1.1). Then, the number of affine points of C is

$$\sum_{x\in\mathbb{F}_q} 1 + \chi_p(F(x)) = q + S_p(F),$$

*Institute for Advanced Study, alina@math.ias.edu
†Concordia University, cdavid@mathstat.concordia.ca
‡University of Toronto, bfeigon@math.toronto.edu
§University of Alberta, mlalin@math.ualberta.ca

and the affine trace is

$$-S_p(F) = -\sum_{x\in\mathbb{F}_q} \chi_p(F(x)).$$

Theorem 1.1. *[1, Theorem 7.3] Let $\varepsilon_1, \dots, \varepsilon_{p-1} \in \mu_p^0$ such that m of the ε_i are zero. Then, as $d_1, \dots, d_{p-1} \to \infty$,*

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i,\ 1 \le i \le q\right\}\right|}{\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right|} \sim \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q-m}.$$

Furthermore, let $X_1, \dots, X_q$ be q i.i.d. random variables taking the value 0 with probability $(p-1)/(q+p-1)$ and each of the values in μ_p with equal probability $q/(p(q+p-1))$. Then, as $d_1, \dots, d_{p-1} \to \infty$,

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} \ : \ S_p(F) = t\right\}\right|}{\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right|} \sim \text{Prob}\left(\sum_{i=1}^q X_i = t\right)$$

for any $t \in \mathbb{Z}[\xi_p] \subset \mathbb{C}$.

The case $p = 2$ was proven in [2], and the case $p = 3$ was proven in [1]. The proof of the general case was sketched in [1], and we give more details in Section 3 of this paper. It may not be clear a priori where the random variables of Theorem 1.1 come from, but they can be explained by a simple heuristic. See [1] for more details.

As an intermediate step in the proof of Theorem 1.1, we have to consider the sets of polynomials

$$\mathcal{F}_{(d_1,\dots,d_{p-1})}^{(k_1,\dots,k_{p-1})} = \left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : F_i \text{ has } k_i \text{ roots over } \mathbb{F}_q, 1 \le i \le p-1\right\}.$$

Those spaces do not have a natural geometric interpretation as the sets of polynomials $\mathcal{F}_{(d_1,\dots,d_{p-1})}$ which parametrize irreducible components of moduli spaces, but they also lead to interesting results involving natural probabilities. We present those results in this paper. We first concentrate on the case $p = 3$ where the results are easier to explain, and then move on to the general case for any odd prime p.

Theorem 1.2. *Fix $0 \le k \le q$ and let*

$$\mathcal{F}_{(d_1,d_2)}^k = \left\{F = F_1F_2^2 \in \mathcal{F}_{(d_1,d_2)} : F_2 \text{ has } k \text{ roots over } \mathbb{F}_q\right\}.$$

Let $\varepsilon_1, \dots, \varepsilon_q \in \left\{0, 1, \xi_3, \xi_3^2\right\}$ such that m of the ε_i are zero. Then, as $d_1, d_2 \to \infty$,

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)}^k : \chi_3(F(x_i)) = \varepsilon_i,\ 1 \le i \le q\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}^k\right|} \sim \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{1}{q+1}\right)^{m-k} \left(\frac{q}{3(q+1)}\right)^{q-m}.$$

Let $X_1, \dots, X_q$ be random variables taking the value 0 with probability $1/(q+1)$ and any of the values $1, \xi_3, \xi_3^2$ with equal probability $q/(3(q+1))$ together with a bias counting the number of k-tuples of roots taken by the variables (as described in Section 2). Then, as $d_1, d_2 \to \infty$,

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)}^k \ : \ S_3(F) = t\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}^k\right|} \sim \text{Prob}\left(\sum_{i=1}^q X_i = t\right)$$

for any $t \in \mathbb{Z}[\xi_3] \subset \mathbb{C}$.

The proof of Theorem 1.2 is given in Section 2. We can interpret those results in the following way: Let $\mathcal{F}_d$ be the set of monic square-free polynomials F of degree d. It follows by exactly the same steps as Theorem 1.1 for $p=2$ that, as $d \to \infty$,

$$\frac{|\{F \in \mathcal{F}_d \,:\, S_3(F)=t\}|}{|\mathcal{F}_d|} \sim \text{Prob}\left(\sum_{i=1}^{q} X_i = t\right), \tag{1.2}$$

where $X_1, \dots, X_q$ are i.i.d. random variables variables taking the value 0 with probability $1/(q+1)$ and any of the values $1, \xi_3, \xi_3^2$ with equal probability $q/(3(q+1))$.[1] Then, if F_2 has no roots over $\mathbb{F}_q$ $(k=0)$, the polynomials $F \in \mathcal{F}^k_{(d_1,d_2)}$ lead to the same probability as the square-free polynomials. If F_2 has k roots over $\mathbb{F}_q$ $(1 \le k \le q)$, then the random variables $X_1, \dots, X_q$ of Theorem 1.2 are distributed in such a way that the probability that $X_i = \varepsilon_i$ for $1 \le i \le q$ depends on m, the number of zeros among $\varepsilon_1, \dots, \varepsilon_q$ (and the X_i are not i.i.d. in this case). More precisely, $\text{Prob}(X_i = \varepsilon_i, 1 \le i \le q)$ is $\binom{m}{k}T^{-1}$ times the probability associated with square-free polynomials, where $\binom{m}{k}$ is the number of k-tuples of zeros among $\varepsilon_1, \dots, \varepsilon_q$ and T is a normalizing factor insuring that the sum of the probabilities is 1 (see Section 2 for more details). We then say the probability $\text{Prob}(X_i = \varepsilon_i, 1 \le i \le q)$ in this case is the probability associated with the family of square-free polynomials biased by the number of zeros of $\varepsilon_1, \dots, \varepsilon_q$.

We now study the general case, where we take polynomials $F = F_1 F_2^2 \dots F_{p-1}^{p-1}$ in $\mathcal{F}_{(d_1,\dots,d_{p-1})}$ where some of the F_i have a prescribed number of roots.

Theorem 1.3. *Fix $1 \le v \le p-1$, and let $k_{v+1}, \dots, k_{p-1}$ be non-negative integers with $k = k_{v+1} + \dots + k_{p-1}$. We also suppose that $0 \le k \le q$. Let*

$$\mathcal{F}^{(*,k_{v+1},\dots,k_{p-1})}_{(d_1,\dots,d_{p-1})} = \left\{F \in \mathcal{F}_{d_1,\dots,d_{p-1}} : F_i \text{ has } k_i \text{ roots over } \mathbb{F}_q,\ v+1 \le i \le q\right\}.$$

Let $\varepsilon_1, \dots, \varepsilon_q \in \mu_p^0$ such that m of the ε_i are zero. Then, as $d_1, \dots, d_{p-1} \to \infty$,

$$\frac{\left|\left\{F \in \mathcal{F}^{(*,k_{v+1},\dots,k_{p-1})}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i,\ 1 \le i \le q\right\}\right|}{\left|\mathcal{F}^{(*,k_{v+1},\dots,k_{p-1})}_{(d_1,\dots,d_{p-1})}\right|} \sim \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{v}{q+v}\right)^{m-k} \left(\frac{q}{p(q+v)}\right)^{q-m}.$$

Let $X_1, \dots, X_q$ be q random variables taking the value 0 with probability $v/(q+v)$ and any of the values in μ_p with equal probability $q/(p(q+v))$ together with a bias counting the number of k-tuples of roots taken by the variables (as described in Section 3). Then, as $d_1, \dots, d_{p-1} \to \infty$,

$$\frac{\left|\left\{F \in \mathcal{F}^{(*,k_{v+1},\dots,k_{p-1})}_{(d_1,\dots,d_{p-1})} \,:\, S_p(F) = t\right\}\right|}{\left|\mathcal{F}^{(*,k_{v+1},\dots,k_{p-1})}_{(d_1,\dots,d_{p-1})}\right|} \sim \text{Prob}\left(\sum_{i=1}^{q} X_i = t\right)$$

for any $t \in \mathbb{Z}[\xi_p] \subset \mathbb{C}$.

The proof of Theorem 1.3 is given in Section 4. We can interpret the results as we did for the case of $p=3$. If $v=1$ and $k=0$, then the probability for the set of polynomials $F_1 F_2^2 \dots F_{p-1}^{p-1}$ is the same as for the square-free polynomials. If $v=1$ and $1 \le k \le q$, then the probability $\text{Prob}(X_i = \varepsilon_i, 1 \le i \le q)$ in this case is the probability associated with the family of square-free polynomials biased by the number

[1] The difference between (1.2) and Theorem 1.1 with $p=2$ is that in the former case, we consider the trace $S_3(F)$ and in the latter case, the trace $S_2(F)$. Both results follow directly from a count on how many polynomials in $\mathcal{F}_d$ take a prescribed set of values.

of zeros of $\varepsilon_1, \ldots, \varepsilon_q$. When $v = 2$ and $k = 0$, then the probability $\mathrm{Prob}(X_i = \varepsilon_i, 1 \le i \le q)$ in this case is the probability associated with the family of polynomials $F_1F_2^2$ with F_1, F_2 monic, square-free and co-prime. If $v = 2$ and $1 \le k \le q$, the probability $\mathrm{Prob}(X_i = \varepsilon_i, 1 \le i \le q)$ in this case is the probability associated with the family of polynomials of the form $F_1F_2^2$ biased by the number of zeros of $\varepsilon_1, \ldots, \varepsilon_q$. The general case follows similarly.

We can give a more geometric version of Theorem 1.1 in terms of the moduli space of cyclic p-fold covers. For any prime p, let $\mathcal{H}_{g,p}$ denote the moduli space of cyclic p-fold covers of genus g. It breaks into a disjoint union of irreducible components $\mathcal{H}^{(d_1,\ldots,d_{p-1})}$ indexed by the inertia type of the branch points of $F(X)$, and

$$\mathcal{H}_{g,p} = \bigcup_{\substack{d_1+2d_2+\cdots+(p-1)d_{p-1}\equiv 0 \pmod p \\ 2g=(p-1)(d_1+\cdots+d_{p-1}-2)}} \mathcal{H}^{(d_1,\ldots,d_{p-1})}, \tag{1.3}$$

where the union is disjoint and each component $\mathcal{H}^{(d_1,\ldots,d_{p-1})}$ is irreducible (see Section 5 for more details). We remark that for $p = 2$, there is just one component in the above decomposition and the moduli space is irreducible.

Consider the first étale cohomology group with $\mathbb{Q}_\ell$ coefficients, where ℓ is a prime with $\ell \equiv 1 \bmod p$ (so that $\mathbb{Q}_\ell$ contains the pth roots of unity). The group of order p generated by the cyclic automorphism acts on the curve C and therefore on the first cohomology group, which gives us a representation of the aforementioned cyclic group on this $\mathbb{Q}_\ell$-vector space. Since the group is abelian and we have enough roots of unity in $\mathbb{Q}_\ell$, the representation splits into a direct sum of 1-dimensional representations. Since these are 1-dimensional representations, they correspond to multiplication by some scalar. In order to find the scalar, one can use the Lefschetz–Verdier fixed point formula from which it follows that our cyclic automorphism acts on these subspaces by multiplication by different powers of χ_p and the dimensions of isotypical subspaces are equal. For more details, see [3]. However, the Riemann–Hurwitz formula shows that the trivial character appears with multiplicity 0. This shows that the cyclic automorphism of order p splits the first cohomology group of C into $p-1$ subspaces $H^1_{\chi_p}, H^1_{\chi_p^2}, \ldots, H^1_{\chi_p^{p-1}}$ on which the automorphism acts by multiplication by $\chi_p, \chi_p^2, \ldots, \chi_p^{p-1}$ respectively. Futhermore, the action of the cyclic automorphism is defined over the base field $\mathbb{F}_q$ (since this contains the pth roots of unity) and Frobenius fixes $\mathbb{F}_q$. Thus the two actions (of Frobenius and of the cyclic automorphism) commute and it suffices to study the trace of the Frobenius on one of these subspaces, say $\mathrm{Tr}(\mathrm{Frob}_C|_{H^1_{\chi_p}})$. Moving to another subspace corresponds to a new choice of the character χ_p.

Theorem 1.4. *[1, Theorem 7.4] If q is fixed and $d_1, \ldots, d_{p-1} \to \infty$, the distribution of the trace of the Frobenius endomorphism associated to C as C ranges over the component $\mathcal{H}^{(d_1,\ldots,d_{p-1})}$ of cyclic p-fold covers of $\mathbb{P}^1(\mathbb{F}_q)$ is that of the sum of $q+1$ i.i.d. random variables $X_1, \ldots, X_{q+1}$, where each X_i takes the value 0 with probability $(p-1)/(q+p-1)$ and each value in μ_p with probability $q/(p(q+p-1))$. More precisely, for any $t \in \mathbb{Z}[\xi_p] \subset \mathbb{C}$ with $|t| \le q+1$ and any $1 > \varepsilon > 0$, we have, as $d_1, \ldots, d_{p-1} \to \infty$,*

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,\ldots,d_{p-1})} : \mathrm{Tr}(\mathrm{Frob}_C|_{H^1_{\chi_p}}) = -t\right\}\right|'}{\left|\mathcal{H}^{(d_1,\ldots,d_{p-1})}\right|'} \sim \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = t\right).$$

In the last theorem, and in the rest of the paper, the $'$ notation, applied both to summation and cardinality, means that curves C on the moduli spaces are counted with the usual weights $1/|\mathrm{Aut}(C)|$ (as in the mass formula). The proof of Theorem 1.4 is given in Section 5.

2 Cyclic trigonal curves and proof of Theorem 1.2

For $p = 3$, a cyclic p-fold cover of $\mathbb{P}^1(\mathbb{F}_q)$ is called a cyclic trigonal curve, and every cyclic trigonal curve has an affine model of the form $Y^3 = F(X)$ where $F(X) = F_1(X)F_2(X)^2 \in \mathcal{F}_{(d_1,d_2)}$.

Let $0 \le k \le q$. We consider in this section the sets of polynomials

$$\mathcal{F}^k_{(d_1,d_2)} = \left\{ F = F_1F_2^2 \in \mathcal{F}_{(d_1,d_2)} : F_2 \text{ has } k \text{ roots over } \mathbb{F}_q \right\}.$$

Fix $q \equiv 1 \pmod 3$. In all this section, ξ_3 denotes a non-trivial third root of unity in $\mathbb{C}^*$, and χ_3 a non-trivial cubic character of $\mathbb{F}_q$. We will denote by ζ_q the (incomplete) zeta function of the rational function field $\mathbb{F}_q[X]$ given by

$$\zeta_q(s) = \sum_F |F|^{-s} = \prod_P \left(1 - |P|^{-s}\right)^{-1} = (1 - q^{1-s})^{-1}.$$

Proposition 2.1. *[1, Proposition 4.3] Let $0 \le \ell \le q$, let $x_1, \ldots, x_\ell$ be distinct elements of $\mathbb{F}_q$, and $a_1, \ldots, a_\ell \in \mathbb{F}_q^*$. Then for any $1 > \varepsilon > 0$, we have*

$$|\{F \in \mathcal{F}_{(d_1,d_2)} : F(x_i) = a_i, 1 \le i \le \ell\}| = \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{q}{(q+2)(q-1)}\right)^\ell \left(1 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon\ell} + q^{-d_1/2+\ell}\right)\right),$$

where

$$K = \prod_P \left(1 - \frac{1}{(|P|+1)^2}\right), \tag{2.1}$$

and the product runs over all monic irreducible polynomials of $\mathbb{F}_q[X]$.

In particular, taking $\ell = 0$, we have

$$\left|\mathcal{F}_{(d_1,d_2)}\right| = \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2} \left(1 + O\left(q^{-(1-\varepsilon)d_2} + q^{-d_1/2}\right)\right). \tag{2.2}$$

The statistics for the number of polynomials $F \in \mathcal{F}^k_{(d_1,d_2)}$ taking prescribed values then follow easily from the previous proposition.

Corollary 2.2. *[1, Corollary 4.4] Let $x_1, \ldots, x_q$ be an enumeration of elements in $\mathbb{F}_q$. Let $a_1 = \ldots = a_m = 0$, and $a_{m+1}, \ldots, a_q \in \mathbb{F}_q^*$. Then, for $1 > \varepsilon > 0$,*

$$\begin{aligned}\left|\left\{F \in \mathcal{F}^k_{(d_1,d_2)} \;:\; F(x_i) = a_i,\; 1 \le i \le q\right\}\right| &= \binom{m}{k} \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{1}{q+2}\right)^m \left(\frac{q}{(q+2)(q-1)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{-(1-\varepsilon)(d_2-k)+\varepsilon q} + q^{-(d_1+k-m)/2+q}\right)\right).\end{aligned}$$

Corollary 2.3. *Let $x_1, \ldots, x_q$ be an enumeration of elements in $\mathbb{F}_q$. Let $a_1 = \ldots = a_m = 0$, and $a_{m+1}, \ldots, a_q \in \mathbb{F}_q^*$. Then, for $1 > \varepsilon > 0$,*

$$\begin{aligned}\frac{\left|\left\{F \in \mathcal{F}^k_{(d_1,d_2)} : F(x_i) = a_i, 1 \le i \le q\right\}\right|}{\left|\mathcal{F}^k_{(d_1,d_2)}\right|} &= \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{1}{q+1}\right)^{m-k} \left(\frac{q}{(q-1)(q+1)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{-(1-\varepsilon)(d_2-k)+\varepsilon q} + q^{-(d_1+k-3q)/2}\right)\right),\end{aligned}$$

and

$$\frac{\left|\left\{F \in \mathcal{F}^k_{(d_1,d_2)} : \chi(F(x_i)) = \varepsilon_i, 1 \le i \le q\right\}\right|}{\left|\mathcal{F}^k_{(d_1,d_2)}\right|} = \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{1}{q+1}\right)^{m-k} \left(\frac{q}{3(q+1)}\right)^{q-m} \times \left(1 + O\left(q^{-(1-\varepsilon)(d_2-k)+\varepsilon q} + q^{-(d_1+k-3q)/2}\right)\right).$$

Proof. We first use Corollary 2.2 to compute $\left|\mathcal{F}^k_{(d_1,d_2)}\right|$. Let $M(a_1,\dots,a_q)$ be the number of values of a_i which are zero. Then

$$\left|\mathcal{F}^k_{(d_1,d_2)}\right| = \sum_{m=k}^{q} \sum_{\substack{(a_1,\dots,a_q)\in(\mathbb{F}_q)^q \\ M(a_1,\dots,a_q)=m}} \left|\left\{F \in \mathcal{F}^k_{(d_1,d_2)} : F(x_i) = a_i, 1 \le i \le q\right\}\right|.$$

By Corollary 2.2, the main term of the above sum equals

$$\begin{aligned}\frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{q}{q+2}\right)^q \sum_{m=k}^{q}\binom{q}{m}\binom{m}{k}q^{-m} &= \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{q}{q+2}\right)^q \binom{q}{k}\sum_{m=k}^{q}\binom{q-k}{m-k}q^{-m} \\ &= \binom{q}{k}\frac{Kq^{d_1+d_2-k}}{\zeta_q(2)^2(1+q^{-1})^k}\left(\frac{q+1}{q+2}\right)^q.\end{aligned}$$

Taking the maximal value of the error term for m between k and q, this gives

$$\left|\mathcal{F}^k_{(d_1,d_2)}\right| = \binom{q}{k}\frac{Kq^{d_1+d_2-k}}{\zeta_q(2)^2(1+q^{-1})^k}\left(\frac{q+1}{q+2}\right)^q \left(1 + O\left(q^{-(1-\varepsilon)(d_2-k)+\varepsilon q} + q^{-(d_1+k-3q)/2}\right)\right). \quad (2.3)$$

The first assertion follows by dividing the result of Corollary 2.2 by $\left|\mathcal{F}^k_{(d_1,d_2)}\right|$, and the second assertion by remarking that for $\varepsilon_i = 0$, then $\chi(F(x_i)) = \varepsilon_i$ if and only if $F(x_i) = 0$, and for $\varepsilon_i = 1$, then $\chi(F(x_i)) = \varepsilon_i$ if and only if $F(x_i)$ is one of the $(q-1)/3$ cubes in $\mathbb{F}_q^*$, and similarly for $\varepsilon_i = \xi_3, \xi_3^2$. □

Taking $d_1, d_2 \to \infty$ in Corollary 2.3, this proves the first statement of Theorem 1.2.

We can also describe the asymptotic of Corollary 2.3 in terms of a natural probability.

Let X be the random variable taking the value 0 with probability $1/(q+1)$, and any value $\in \left\{1, \xi_3, \xi_3^2\right\}$ with probability $q/(3(q+1))$, as in Theorem 1.2. For each q-tuple $(\varepsilon_1,\dots,\varepsilon_q) \in \left\{0, 1, \xi_3, \xi_3^2\right\}^q$, let m be the number of i such that $\varepsilon_i = 0$. Let $X_1,\dots,X_q$ be random variables distributed as X with a bias counting the (unordered) k-tuples $\{i_1,\dots,i_k\} \subseteq \{1,\dots,q\}$ such that $\varepsilon_{i_1} = \dots = \varepsilon_{i_k} = 0$. More precisely, let

$$\text{Prob}\left(X_i = \varepsilon_i : 1 \le i \le q\right) = \binom{m}{k}\frac{1}{T}\left(\frac{1}{q+1}\right)^m \left(\frac{q}{3(q+1)}\right)^{q-m}, \quad (2.4)$$

where

$$\begin{aligned} T &= \sum_{(\varepsilon_1,\dots,\varepsilon_q)\in\left\{0,1,\xi_3,\xi_3^2\right\}^q} \binom{m}{k}\left(\frac{1}{q+1}\right)^m\left(\frac{q}{3(q+1)}\right)^{q-m} \\ &= \sum_{m=k}^{q}\binom{m}{k}3^{q-m}\binom{q}{m}\left(\frac{1}{q+1}\right)^m\left(\frac{q}{3(q+1)}\right)^{q-m} \\ &= \binom{q}{k}\sum_{m=k}^{q}\binom{q-k}{q-m}\left(\frac{1}{q+1}\right)^m\left(\frac{q}{q+1}\right)^{q-m} \\ &= \binom{q}{k}\left(\frac{1}{q+1}\right)^k. \end{aligned}$$

Using the value of T in (2.4), we get

$$\operatorname{Prob}\left(X_i=\varepsilon_i : 1\le i\le q\right) = \frac{\binom{m}{k}}{\binom{q}{k}}\left(\frac{1}{q+1}\right)^{m-k}\left(\frac{q}{3(q+1)}\right)^{q-m}, \tag{2.5}$$

which is the probability appearing in Corollary 2.3.

The second statement of Theorem 1.2 follows by summing the probabilities for all tuples $(\varepsilon_1,\dots,\varepsilon_q)$ such that $\varepsilon_1+\dots+\varepsilon_q=t$.

3 General p-fold covers and proof of Theorem 1.1

We recall that

$$\mathcal{F}_{(d_1,\dots,d_{p-1})}=\left\{F=F_1F_2^2\dots F_{p-1}^{p-1} : F_i \text{ monic, square-free, pairwise coprime, } \deg F_i=d_i, 1\le i\le p-1\right\}.$$

The proof of the following proposition was sketched in [1]. We give more details here. For $F,G\in\mathbb{F}_q[X]$, let $\gcd(F,G)$ denote their greatest common divisor.

Proposition 3.1. *[1, Proposition 7.1] Fix $0\le\ell\le q$, $x_1,\dots,x_\ell$ distinct points in $\mathbb{F}_q$ and $a_1,\dots,a_\ell$ nonzero elements of $\mathbb{F}_q$. Then, for each $r\ge1$ and $\varepsilon>0$,*

$$\begin{aligned}\left|\left\{F\in\mathcal{F}_{(d_1,\dots,d_r)} : F(x_i)=a_i, 1\le i\le\ell\right\}\right| &= \frac{L_{r-1}q^{d_1+\dots+d_r}}{\zeta_q(2)^r}\left(\frac{q}{(q+r)(q-1)}\right)^\ell \\ &\quad\times\left(1+O\left(q^{\varepsilon\ell}\sum_{h=2}^{r}q^{\varepsilon(d_h+\dots+d_r)-d_h}+q^{-d_1/2+\ell}\right)\right),\end{aligned}$$

where

$$L_{r-1}:=K_1\dots K_{r-1},$$

with

$$K_j:=\prod_P\left(1-\frac{j}{(|P|+1)(|P|+j)}\right),\quad j\ge1,$$

and $K_0=L_0=1$. Furthermore, taking $\ell=0$, this gives

$$\left|\mathcal{F}_{(d_1,\dots,d_r)}\right| = \frac{L_{r-1}q^{d_1+\dots+d_r}}{\zeta_q(2)^r}\left(1+O\left(\sum_{h=2}^{r}q^{\varepsilon(d_h+\dots+d_r)-d_h}+q^{-d_1/2}\right)\right). \tag{3.1}$$

Proof. If $r=1$, $\mathcal{F}_{(d_1)}$ is the set of square-free polynomials, and this is Lemma 5 in [2], where the empty sum $q^{-d_2}+\cdots+q^{-d_r}$ of the error term is understood to be 0. We then suppose that $r\geq 2$. Let

$$\mathcal{G}_{d_1,\ldots,d_r}=\left\{(F_1,\ldots,F_r)\in\mathbb{F}_q[X]^r : F_i \text{ monic, square-free, pairwise coprime, } \deg(F_i)=d_i, 1\leq i\leq r\right\}.$$

By Lemma 4.2 in [1],

$$\begin{aligned}
&\left|\left\{F\in\mathcal{F}_{(d_1,\ldots,d_r)} : F(x_i)=a_i, 1\leq i\leq\ell\right\}\right| \\
&\quad=\sum_{\substack{(F_2,\ldots,F_r)\in\mathcal{G}_{d_2,\ldots,d_r}\\ \prod_{j=2}^r F_j(x_i)\neq 0, 1\leq i\leq\ell}} S_{d_1}^{F_2\ldots F_r}(\ell) \\
&\quad=\frac{q^{d_1-\ell}}{\zeta_q(2)(1-q^{-2})^\ell}\sum_{\substack{(F_2,\ldots,F_r)\in\mathcal{G}_{d_2,\ldots,d_r}\\ \prod_{j=2}^r F_j(x_i)\neq 0, 1\leq i\leq\ell}}\prod_{P|F_2\ldots F_r}(1+|P|^{-1})^{-1}+\sum_{\substack{(F_2,\ldots,F_r)\in\mathcal{G}_{d_2,\ldots,d_r}\\ \prod_{j=2}^r F_j(x_i)\neq 0, 1\leq i\leq\ell}} O\left(q^{d_1/2}\right) \\
&\quad=\frac{q^{d_1-\ell}}{\zeta_q(2)(1-q^{-2})^\ell}\sum_{\deg F_r=d_r}\cdots\sum_{\deg F_2=d_2} b(F_2\ldots F_r)+O\left(q^{d_1/2+d_2+\ldots+d_r}\right),
\end{aligned}\tag{3.2}$$

where, following the notation from Lemma 4.2 in [1],

$$S_d^U(\ell)=\left|\{F\in\mathcal{F}_d : (F,U)=1, F(x_i)=a_i, 1\leq i\leq\ell\}\right|,$$

and we define

$$b(F)=\begin{cases}\mu^2(F)\prod_{P|F}(1+|P|^{-1})^{-1} & F(x_i)\neq 0, 1\leq i\leq\ell,\\ 0 & \text{otherwise,}\end{cases}$$

for any polynomial $F\in\mathbb{F}_q[X]$. (Here the product is over all the monic irreducible polynomials $P\in\mathbb{F}_q[X]$ dividing F.)

We now evaluate

$$M_r:=\sum_{\deg F_r=d_r}\cdots\sum_{\deg F_2=d_2} b(F_2\ldots F_r).$$

We notice that b is multiplicative and that $b(F_2\ldots F_r)=0$ if the F_i are not relatively prime in pairs. Then we have

$$M_r=\sum_{\deg(F_r)=d_r}\ \sum_{\substack{\deg(F_{r-1})=d_{r-1}\\ \gcd(F_{r-1},F_r)=1}}\cdots\sum_{\substack{\deg(F_2)=d_2\\ \gcd(F_2,F_r)=1,\ldots,\gcd(F_2,F_3)=1}} b(F_2)\ldots b(F_r).$$

For any $j\geq 1$, let

$$c_j^U(F)=\begin{cases}\mu^2(F)\prod_{P|F}(1+j|P|^{-1})^{-1} & F(x_i)\neq 0, 1\leq i\leq\ell,\ \gcd(F,U)=1,\\ 0 & \text{otherwise.}\end{cases}\tag{3.3}$$

Notice that in particular, $b(F)=c_1^1(F)$. Then we can write

$$M_r=\sum_{\deg(F_r)=d_r} c_1^1(F_r)\sum_{\deg(F_{r-1})=d_{r-1}} c_1^{F_r}(F_{r-1})\ldots\sum_{\deg(F_2)=d_2} c_1^{F_3\ldots F_r}(F_2).$$

Using Lemma 3.2 with $j = 1$, we have

$$\sum_{\deg(F_2)=d_2} c_1^{F_3\dots F_r}(F_2) = \frac{K_1 q^{d_2}}{\zeta_q(2)} \left(\frac{q+1}{q+2}\right)^{\ell} \left(\prod_{P|F_3\dots F_r} \left(\frac{|P|+1}{|P|+2}\right)\right) \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_r+\ell)-d_2}\right)\right) \tag{3.4}$$

Using (3.4) in (3.2), this proves the theorem for $r = 2$. For $r \geq 3$, we first have to evaluate

$$\sum_{\deg(F_3)=d_3} c_1^{F_4\dots F_r}(F_3) \sum_{\deg(F_2)=d_2} c_1^{F_3\dots F_r}(F_2)$$

$$= \frac{K_1 q^{d_2}}{\zeta_q(2)} \left(\frac{q+1}{q+2}\right)^{\ell} \sum_{\deg(F_3)=d_3} c_1^{F_4\dots F_r}(F_3) \left(\prod_{P|F_3\dots F_r} \left(\frac{|P|+1}{|P|+2}\right)\right) \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_r+\ell)-d_2}\right)\right)$$

$$= \frac{K_1 q^{d_2}}{\zeta_q(2)} \left(\frac{q+1}{q+2}\right)^{\ell} \left(\prod_{P|F_4\dots F_r} \left(\frac{|P|+1}{|P|+2}\right)\right) \sum_{\substack{\deg(F_3)=d_3 \\ F_3(x_i)\neq 0, 1\leq i\leq \ell \\ \gcd(F_3, F_4\dots F_r)=1}} \mu^2(F_3) \prod_{P|F_3} \frac{|P|}{|P|+2} \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_r+\ell)-d_2}\right)\right)$$

$$= \frac{K_1 q^{d_2}}{\zeta_q(2)} \left(\frac{q+1}{q+2}\right)^{\ell} \left(\prod_{P|F_4\dots F_r} \left(\frac{|P|+1}{|P|+2}\right)\right) \sum_{\deg(F_3)=d_3} c_2^{F_4\dots F_r}(F_3) \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_r+\ell)-d_2}\right)\right).$$

Using Lemma 3.2 with $j = 2$, this gives

$$\sum_{\deg(F_3)=d_3} c_1^{F_4\dots F_r}(F_3) \sum_{\deg(F_2)=d_2} c_1^{F_3\dots F_r}(F_2)$$

$$= \frac{K_1 K_2 q^{d_2+d_3}}{\zeta_q(2)^2} \left(\frac{q+1}{q+3}\right)^{\ell} \prod_{P|F_4\dots F_r} \left(\frac{|P|+1}{|P|+3}\right) \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_r+\ell)-d_2} + q^{\varepsilon(d_3+\dots+d_r+\ell)-d_3}\right)\right).$$

Using the last equality in (3.2), this proves the Proposition with $r = 3$. In general, continuing in this way up to the last sum $\sum_{\deg F_r = d_r}$, we obtain the result. □

Lemma 3.2. *Assume the hypotheses of Proposition 3.1 and let U be a polynomial of degree u with $U(x_i) \neq 0$ for $1 \leq i \leq \ell$. Let $j \geq 1$, and let $c_j^U(F)$ be defined as in* (3.3)*. Then for any $1 > \varepsilon > 0$,*

$$\sum_{\deg(F)=d} c_j^U(F) = \frac{K_j\, q^d}{\zeta_q(2)} \left(\frac{q+j}{q+j+1}\right)^{\ell} \left(\prod_{P|U} \left(\frac{|P|+j}{|P|+j+1}\right)\right) \left(1 + O\left(q^{\varepsilon(d+u+\ell)-d}\right)\right).$$

Proof. We will use the function field version of the Wiener-Ikehara Tauberian Theorem. This is Theorem 17.1 in [5]. For our application, it is important to get an error term which is independent of U and q and for this we need a more precise statement of the Tauberian Theorem than in [5] so we will go through the proof here.

First, we consider the Dirichlet series

$$G_j(s) = \sum_F \frac{c_j^U(F)}{|F|^s} = \prod_{\substack{P \\ P(x_i)\neq 0, 1\leq i\leq \ell, P\nmid U}} \left(1 + \frac{1}{|P|^s} \cdot \frac{|P|}{|P|+j}\right)$$

$$= \frac{\zeta_q(s)}{\zeta_q(2s)} H_j(s) \left(1 + \frac{1}{q^{s-1}(q+j)}\right)^{-\ell} \prod_{P|U} \left(1 + \frac{1}{|P|^s} \cdot \frac{|P|}{|P|+j}\right)^{-1},$$

where

$$H_j(s) = \prod_P \left(1 - \frac{j}{(|P|^s+1)(|P|+j)}\right).$$

In the above, we have used the hypothesis that $U(x_i) \neq 0$, and therefore the primes $P|U$ are different from the primes $X - x_i$ for $1 \leq i \leq \ell$. Notice that $H_j(s)$ converges absolutely for $\mathrm{Re}(s) > 0$, and $G_j(s)$ is meromorphic for $\mathrm{Re}(s) > 0$ with simple poles at the points s where $\zeta_q(s) = (1 - q^{1-s})^{-1}$ has poles, that is, $s_n = 1 + i\frac{2\pi n}{\log q}$, with $n \in \mathbb{Z}$. Notice that $H_j(1) = K_j$, and $\mathrm{Res}_{s=1}\zeta_q(s) = \frac{1}{\log q}$. Thus $G_j(s)$ has a simple pole at $s = 1$ with residue

$$\frac{K_j}{\zeta_q(2)\log q}\left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|U}\left(\frac{|P|+j}{|P|+j+1}\right)\right). \tag{3.5}$$

Define $Z(u)$ by $Z(q^{-s}) = G_j(s)$. Thus

$$Z(u) = \frac{1-qu^2}{1-qu}\left(1 + \frac{uq}{q+j}\right)^{-\ell} \prod_P \left(1 - \frac{j}{(u^{-\deg P}+1)(q^{\deg P}+j)}\right) \prod_{P|U}\left(1 + \frac{u^{\deg P}q^{\deg P}}{q^{\deg P}+j}\right)^{-1}.$$

Fix any ε such that $1 > \varepsilon > 0$. Then $Z(u)$ is a meromorphic function on the disk $\{u \mid |u| \leq q^{-\varepsilon}\}$ with a simple pole at $u = q^{-1}$. Let $C = \{u \in \mathbb{C} \mid |u| = q^{-\varepsilon}\}$, oriented counterclockwise. For any $0 < \delta < q^{-1}$, let $C_\delta = \{u \in \mathbb{C} \mid |u| = \delta\}$, oriented clockwise. Notice that $\frac{Z(u)}{u^{d+1}}$ is a meromorphic function between the two circles, with a simple pole at $u = q^{-1}$ with residue

$$\begin{aligned}
\mathrm{Res}_{u=q^{-1}}\frac{Z(u)}{u^{d+1}} &= \lim_{u\to q^{-1}}(u-q^{-1})\frac{Z(u)}{u^{d+1}} \\
&= -\frac{K_j}{\zeta_q(2)}\left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|U}\left(\frac{|P|+j}{|P|+j+1}\right)\right) q^d.
\end{aligned}$$

Thus by the Cauchy integral formula,

$$\frac{1}{2\pi i}\oint_{C_\delta + C}\frac{Z(u)}{u^{d+1}}du = -\frac{K_j}{\zeta_q(2)}\left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|U}\left(\frac{|P|+j}{|P|+j+1}\right)\right) q^d. \tag{3.6}$$

Now we observe that

$$Z(u) = \sum_{n=0}^\infty \left(\sum_{\deg F = n} c_j^U(F)\right) u^n.$$

Thus

$$\frac{1}{2\pi i}\oint_{C_\delta}\frac{Z(u)}{u^{d+1}}du = -\sum_{\deg F = d} c_j^U(F). \tag{3.7}$$

Combining (3.6) and (3.7) we see that

$$\sum_{\deg F=d} c_j^U(F) = \frac{K_j}{\zeta_q(2)}\left(\frac{q+j}{q+j+1}\right)^\ell \left(\prod_{P|U}\left(\frac{|P|+j}{|P|+j+1}\right)\right) q^d + \frac{1}{2\pi i}\oint_C \frac{Z(u)}{u^{d+1}}du.$$

Let M be the maximum value of $|Z(u)|$ on C. Then clearly

$$\left|\frac{1}{2\pi i}\oint_C \frac{Z(u)}{u^{d+1}}du\right| \leq Mq^{\varepsilon d}$$

so

$$\sum_{\deg(F)=d} c_j^U(F) = \frac{K_j}{\zeta_q(2)}\left(\frac{q+j}{q+j+1}\right)^{\ell}\left(\prod_{P|U}\left(\frac{|P|+j}{|P|+j+1}\right)\right)q^d + O(Mq^{\varepsilon d}). \tag{3.8}$$

To conclude the proof we note that

$$\begin{aligned} M &= \max_{|q^{-s}|=q^{-\varepsilon}} |H_j(s)| \left|\left(1+\frac{1}{q^{s-1}(q+j)}\right)^{-\ell}\prod_{P|U}\left(1+\frac{1}{|P|^s}\cdot\frac{|P|}{|P|+j}\right)^{-1}\right| \\ &\ll (1-q^{-\varepsilon})^{-\ell}\prod_{P|U}(1-|P|^{-\varepsilon})^{-1} \ll q^{\varepsilon\ell}\prod_{P|U}|P|^{\varepsilon} \leq q^{\varepsilon\ell}|U|^{\varepsilon} = q^{\varepsilon(u+\ell)}. \end{aligned} \tag{3.9}$$

By (3.9), the absolute error term in (3.8) is $O\left(q^{\varepsilon(d+u+\ell)}\right)$ and we get the result.

□

Proposition 3.1 will be used with $r = p-1$.
Denote

$$\mathcal{F}_{(d_1,\dots,d_{p-1})}^{(k_1,\dots,k_{p-1})} = \left\{F = F_1\dots F_{p-1}^{p-1} \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : F_i \text{ has } k_i \text{ roots in } \mathbb{F}_q, 1 \leq i \leq p-1\right\}.$$

Corollary 3.3. *Fix $0 \leq m \leq q$. Choose $x_1,\dots,x_q$ an enumeration of the points of $\mathbb{F}_q$, and values $a_1 = \dots = a_m = 0$, $a_{m+1},\dots,a_q \in \mathbb{F}_q^*$. Pick a partition $m = k_1+\dots+k_{p-1}$. Then, for any $\varepsilon > 0$,*

$$\begin{aligned} &\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})}^{(k_1,\dots,k_{p-1})} : F(x_i) = a_i, 1 \leq i \leq q\right\}\right| \\ &= \binom{m}{k_1,\dots,k_{p-1}}\frac{L_{p-2}q^{d_1+\dots+d_{p-1}}}{\zeta_q(2)^{p-1}}\left(\frac{1}{q+p-1}\right)^m\left(\frac{q}{(q+p-1)(q-1)}\right)^{q-m} \\ &\times\left(1+O\left(q^{\varepsilon q}\sum_{h=2}^{p-1}q^{\varepsilon(d_h+\dots+d_{p-1}-(k_h+\dots+k_{p-1}))-(d_h-k_h)}+q^{-(d_1-k_1)/2+q}\right)\right). \end{aligned}$$

Proof. Let F be a polynomial in $F_{(d_1,\dots,d_{p-1})}^{(k_1,\dots,k_{p-1})}$ such that $F(x_i) = a_i$ for $1 \leq i \leq q$. Then, F can be written as

$$F(X) = \prod_{j=1}^{m}(X-x_j)^{b_j}G(X),$$

where the b_j are positive integers with the property that for any $1 \leq i \leq p-1$, the number of b_j's such that $b_j = i$ is k_i and $G \in F_{(d_1-k_1,\dots,d_{p-1}-k_{p-1})}$ is such that $G(x_i) \neq 0$ for $1 \leq i \leq q$. There are then $\binom{m}{k_1,\dots,k_{p-1}}$ choices for the b_j's. After this choice of b_j's, we choose the values $\alpha_i = G(x_i)$ for $1 \leq i \leq m$.

This gives,

$$\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})}^{(k_1,\dots,k_{p-1})} : F(x_i) = a_i, 1 \le i \le q\right\}\right|$$
$$= \binom{m}{k_1,\dots,k_{p-1}} \sum_{\substack{(\alpha_1,\dots,\alpha_m)\\ \in(\mathbb{F}_q^*)^m}} \left|\left\{G \in \mathcal{F}_{(d_1-k_1,d_2-k_2,\dots,d_{p-1}-k_{p-1})} :\ G(x_i) = a_i \prod_{j=1}^{m}(x_i - x_j)^{-b_j}\right.\right.$$
$$\left.\left.\text{for } m+1 \le i \le q, \text{ and } G(x_i) = \alpha_i \text{ for } 1 \le i \le m\right\}\right|.$$

The result is proved by using Proposition 3.1 with $r = p-1$ in the last expression. □

Corollary 3.4. *Choose $x_1,\dots,x_q$ an enumeration of the points of $\mathbb{F}_q$. Fix $0 \le m \le q$, $a_1 = \ldots = a_m = 0$ and $a_{m+1},\dots,a_q \in \mathbb{F}_q^*$. Then for any $\varepsilon > 0$,*

$$\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : F(x_i) = a_i, 1 \le i \le q\right\}\right| = \frac{L_{p-2}q^{d_1+\ldots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{(q+p-1)(q-1)}\right)^{q-m}$$
$$\times \quad \left(1 + O\left(q^{\varepsilon q+(1-\varepsilon)m}\sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right).$$

Let $\varepsilon_1,\dots,\varepsilon_q \in \mu_p^0$ and let m be the number of values of ε_i which are 0. Then for any $\varepsilon > 0$,

$$\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i, 1 \le i \le q\right\}\right| = \frac{L_{p-2}q^{d_1+\ldots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q-m}$$
$$\times \quad \left(1 + O\left(q^{\varepsilon q+(1-\varepsilon)m}\sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right).$$

Proof. Adding over all the $p-1$-partitions of m and using Corollary 3.3 and the identity

$$\sum_{k_1+\ldots+k_{p-1}=m} \binom{m}{k_1,\dots,k_{p-1}} = (p-1)^m,$$

which follows from the Multinomial Theorem, we get the first assertion. For the second assertion, we note that if $\varepsilon \in \mu_p$, there are $\frac{q-1}{p}$ elements $\alpha \in \mathbb{F}_q^*$ such that $\chi_p(\alpha) = \varepsilon$. □

Finally, Theorem 1.1 follows by dividing $\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i, 1 \le i \le q\right\}\right|$ (Corollary 3.4) by $\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right|$ (Proposition 3.1). This gives

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i,\ 1 \le i \le q\right\}\right|}{\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right|} = \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q-m}$$
$$\times \left(1 + O\left(q^{\varepsilon q+(1-\varepsilon)m}\sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right).$$

Notice that the order in which we perform the nested sum in equation (3.2) is arbitrary. Thus, we can assume, without loss of generality, that $d_2 \ge \cdots \ge d_{p-1}$ while proving Proposition 3.1. As a result, the error terms in all the statements of this section go to zero for $d_1,\dots,d_{p-1} \to \infty$ as long as ε is small enough, for example, $0 < \varepsilon < 1/r$ in Proposition 3.1 and $0 < \varepsilon < 1/(p-1)$ in the other statements.

4 General p-fold covers and proof of Theorem 1.3

Let v be a fixed integer such that $0 \le v \le p-1$. We now study the distribution of the traces $S_p(F)$ when F varies over polynomials in

$$\mathcal{F}_{(d_1,\dots,d_{p-1})}^{(*,k_{v+1},\dots,k_{p-1})} = \left\{F \in \mathcal{F}_{d_1,\dots,d_{p-1}} : F_i \text{ has } k_i \text{ roots over } \mathbb{F}_q, v+1 \le i \le p-1\right\}.$$

Then, if $F \in \mathcal{F}_{(d_1,\dots,d_{p-1})}^{(*,k_{v+1},\dots,k_{p-1})}$, the number of roots is fixed for $F_{v+1},\dots,F_{p-1}$ only. We will always write $k = k_{v+1} + \cdots + k_{p-1}$ for the total number of fixed roots. Notice that for $v = 0$ we necessarily have $k = m$.

Using Corollary 3.3, we obtain the following three results.

Lemma 4.1. *Let $1 \le v \le p-1$. Fix m such that $0 \le k \le m \le q$. Choose $x_1,\dots,x_q$ an enumeration of the points of $\mathbb{F}_q$, and values $a_1 = \ldots = a_m = 0$, $a_{m+1},\dots,a_q \in \mathbb{F}_q^*$. Then, for any $\varepsilon > 0$, we have*

$$\begin{aligned}
&\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})}^{(*,k_{v+1},\dots,k_{p-1})} : F(x_i) = a_i, 1 \le i \le q\right\}\right| \\
&= \binom{m}{m-k, k_{v+1},\dots,k_{p-1}} v^{m-k} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{1}{q+p-1}\right)^m \left(\frac{q}{(q+p-1)(q-1)}\right)^{q-m} \\
&\times \left(1 + O\left(q^{\varepsilon q + (1-\varepsilon)m} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1+k-m)/2+q}\right)\right).
\end{aligned}$$

Notice that the case $v = 0$ was already covered in Corollary 3.3.

Proof. We first write

$$\begin{aligned}
&\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})}^{(*,k_{v+1},\dots,k_{p-1})} : F(x_i) = a_i, 1 \le i \le q\right\}\right| \\
&= \sum_{k_1+\cdots+k_v = m-k} \left|\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})}^{(k_1,\dots,k_{p-1})} : F(x_i) = a_i, 1 \le i \le q\}\right|. \qquad (4.1)
\end{aligned}$$

By Corollary 3.3, the main term of (4.1) is

$$\frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{1}{q+p-1}\right)^m \left(\frac{q}{(q+p-1)(q-1)}\right)^{q-m} \sum_{k_1+\cdots+k_v=m-k} \binom{m}{k_1,\dots,k_{p-1}},$$

and then we use the fact that

$$\begin{aligned}
\sum_{k_1+\cdots+k_v=m-k} \binom{m}{k_1,\dots,k_{p-1}} &= \sum_{k_1+\cdots+k_v=m-k} \binom{m-k}{k_1,\dots,k_v} \binom{m}{m-k, k_{v+1},\dots,k_{p-1}} \\
&= v^{m-k} \binom{m}{m-k, k_{v+1},\dots,k_{p-1}}.
\end{aligned}$$

By using a bound on the error term of Corollary 3.3 which is valid for all $k_1,\dots,k_v$ such that $k_1+\cdots+k_v = m-k$, the result follows. □

Lemma 4.2. *As defined above, let $1 \le v \le p-1$ and $k = k_{v+1} + \cdots + k_{p-1}$ with $0 \le k \le q$. Then, for any $\varepsilon > 0$,*

$$\left|\mathcal{F}^{(*,k_{v+1},\ldots,k_{p-1})}_{(d_1,\ldots,d_{p-1})}\right| = \binom{q}{q-k, k_{v+1}, \ldots, k_{p-1}} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}(q+v)^k} \left(\frac{q+v}{q+p-1}\right)^q \times \left(1 + O\left(q^q \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1+k-3q)/2}\right)\right).$$

For $v = 0$, we obtain

$$\left|\mathcal{F}^{(k_1,\ldots,k_{p-1})}_{(d_1,\ldots,d_{p-1})}\right| = \binom{q}{q-k, k_1, \ldots, k_{p-1}} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}-k}}{\zeta_q(2)^{p-1}} \left(\frac{q}{q+p-1}\right)^q \times \left(1 + O\left(q^{\varepsilon q} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1}-(k_h+\cdots+k_{p-1}))-(d_h-k_h)} + q^{-(d_1-k_1)/2+q}\right)\right).$$

Proof. We have

$$\left|\mathcal{F}^{(*,k_{v+1},\ldots,k_{p-1})}_{(d_1,\ldots,d_{p-1})}\right| = \sum_{m=k}^{q} \binom{q}{m} (q-1)^{q-m} \left|\left\{F \in \mathcal{F}^{(*,k_{v+1},\ldots,k_{p-1})}_{(d_1,\ldots,d_{p-1})} : F(x_i) = a_i, 1 \le i \le q\right\}\right|. \tag{4.2}$$

For $v \ge 1$ we use Lemma 4.1 and the chicken, chicken, chicken identity

$$\binom{q}{m}\binom{m}{m-k, k_{v+1}, \ldots, k_{p-1}} = \binom{q}{q-k, k_{v+1}, \ldots, k_{p-1}}\binom{q-k}{q-m}.$$

Then, the main term of $\left|\mathcal{F}^{(*,k_{v+1},\ldots,k_{p-1})}_{(d_1,\ldots,d_{p-1})}\right|$ is

$$\begin{aligned}
&\frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{q}{q+p-1}\right)^q v^{-k} \sum_{m=k}^{q} \binom{q}{m}\binom{m}{m-k, k_{v+1}, \ldots, k_{p-1}} v^m q^{-m} \\
&= \binom{q}{q-k, k_{v+1}, \ldots, k_{p-1}} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{q}{q+p-1}\right)^q v^{-k} \sum_{m=k}^{q} \binom{q-k}{q-m} v^m q^{-m} \\
&= \binom{q}{q-k, k_{v+1}, \ldots, k_{p-1}} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{q+v}{q+p-1}\right)^q (q+v)^{-k}.
\end{aligned}$$

Replacing m by the maximal value $m = q$ in the error term of Lemma 4.1, the result follows for $v \neq 0$.

If $v = 0$ we use Corollary 3.3 in equation (4.2) (in this case, the sum in equation (4.2) has one term for $m = k$). The main term of $\left|\mathcal{F}^{(k_1,\ldots,k_{p-1})}_{(d_1,\ldots,d_{p-1})}\right|$ is

$$\begin{aligned}
&= \binom{q}{k}(q-1)^{q-k}\binom{k}{k_1, \ldots, k_{p-1}} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{1}{q+p-1}\right)^k \left(\frac{q}{(q+p-1)(q-1)}\right)^{q-k} \\
&= \binom{q}{q-k, k_1, \ldots, k_{p-1}} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{1}{q+p-1}\right)^k \left(\frac{q}{q+p-1}\right)^{q-k},
\end{aligned}$$

and the error term is the same as in Corollary 3.3.

□

Proposition 4.3. *As defined above, let $1 \leq v \leq p-1$ and $k = k_{v+1} + \cdots + k_{p-1}$ with $0 \leq k \leq q$. Fix m such that $0 \leq k \leq m \leq q$. Choose $x_1, \ldots, x_q$ an enumeration of the points of $\mathbb{F}_q$, and values $a_1 = \ldots = a_m = 0$, $a_{m+1}, \ldots, a_q \in \mathbb{F}_q^*$. Then for any $\varepsilon > 0$,*

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})} : F(x_i) = a_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})}\right|} = \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{v}{q+v}\right)^{m-k} \left(\frac{q}{(q-1)(q+v)}\right)^{q-m}$$
$$\times \left(1 + O\left(q^q \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1+k-3q)/2}\right)\right),$$

and

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})}\right|} = \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{v}{q+v}\right)^{m-k} \left(\frac{q}{p(q+v)}\right)^{q-m}$$
$$\times \left(1 + O\left(q^q \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1+k-3q)/2}\right)\right).$$

If $v = 0$, we need $m = k$, and in this case

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(k_1,\ldots,k_{p-1})} : F(x_i) = a_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(k_1,\ldots,k_{p-1})}\right|} = \frac{1}{\binom{q}{k}(q-1)^{q-k}}$$
$$\times \left(1 + O\left(q^{\varepsilon q} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1}-(k_h+\cdots+k_{p-1}))-(d_h-k_h)} + q^{-(d_1-k_1)/2+q}\right)\right),$$

and

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(k_1,\ldots,k_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(k_1,\ldots,k_{p-1})}\right|} = \frac{1}{\binom{q}{k}p^{q-k}}$$
$$\times \left(1 + O\left(q^{\varepsilon q} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1}-(k_h+\cdots+k_{p-1}))-(d_h-k_h)} + q^{-(d_1-k_1)/2+q}\right)\right).$$

Proof. For $v > 0$, the first assertion follows by dividing the result of Lemma 4.1 by the result of Lemma 4.2, and the second assertion by observing that $\chi_p(F(a_i)) = \xi_p$ if and only if $F(a_i)$ takes $(q-1)/p$ possible values in $\mathbb{F}_q^*$. For $v = 0$ we use Corollary 3.3 instead of Lemma 4.1. □

The result of Theorem 1.3 then follows by taking $d_1, \ldots, d_{p-1} \to \infty$ in Proposition 4.3.

We now compare the result of Proposition 4.3 with a probabilistic model. Let X be the random variable taking value 0 with probability $\frac{v}{q+v}$, and any value in μ_p with probability $\frac{q}{p(q+v)}$. For each q-tuple $(\varepsilon_1, \ldots, \varepsilon_q) \in \mu_p^0$, let m be the number of i such that $\varepsilon_i = 0$. Let $X_1, \ldots, X_q$ be random variables distributed as X with a bias counting the (unordered) k-sets $\{i_1, \ldots, i_k\}$ where $\varepsilon_{i_j} = 0$ for $j = 1, \ldots, k$, i.e.,

$$\operatorname{Prob}(X_i = \varepsilon_i \ : \ 1 \leq i \leq q) = \binom{m}{k} \frac{1}{T} \left(\frac{v}{q+v}\right)^m \left(\frac{q}{p(q+v)}\right)^{q-m},$$

where

$$\begin{aligned} T &= \sum_{(\varepsilon_1,\ldots,\varepsilon_q)\in(\mu_p^0)^q} \binom{m}{k} \left(\frac{v}{q+v}\right)^m \left(\frac{q}{p(q+v)}\right)^{q-m} \\ &= \sum_{m=k}^{q} \binom{q}{m} p^{q-m} \binom{m}{k} \left(\frac{v}{q+v}\right)^m \left(\frac{q}{p(q+v)}\right)^{q-m} \\ &= \binom{q}{k} \sum_{m=k}^{q} \binom{q-k}{q-m} \left(\frac{v}{q+v}\right)^m \left(\frac{q}{q+v}\right)^{q-m} \\ &= \binom{q}{k} \left(\frac{v}{q+v}\right)^k. \end{aligned}$$

Thus, we obtain

$$\operatorname{Prob}(X_i = \varepsilon_i \ : \ 1 \leq i \leq q) \quad = \quad \frac{\binom{m}{k}}{\binom{q}{k}} \left(\frac{v}{q+v}\right)^{m-k} \left(\frac{q}{p(q+v)}\right)^{q-m}, \tag{4.3}$$

which are the probabilities in Proposition 4.3 for $v \neq 0$. The second statement of Theorem 1.3 then follows from Proposition 4.3 by summing the probabilities for all tuples $(\varepsilon_1, \ldots, \varepsilon_q)$ such that $\varepsilon_1 + \cdots + \varepsilon_q = t$.

Finally, we remark that the probability for $\mathcal{F}_{(d_1,\ldots,d_{p-1})}$ can be written as the mixed probability involving the probabilities for all the $\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})}$ as

$$\begin{aligned} &\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\ldots,d_{p-1})} : \chi(F(x_i)) = \varepsilon_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}\right|} \\ &= \sum_{\substack{0\leq k_i \leq d_i \\ v<i\leq p-1}} \frac{\left|\left\{F \in \mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})} : \chi(F(x_i)) = \varepsilon_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})}\right|} \frac{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}^{(*,k_{v+1},\ldots,k_{p-1})}\right|}{\left|\mathcal{F}_{(d_1,\ldots,d_{p-1})}\right|}. \end{aligned}$$

5 The geometric point of view

We prove in this section that Theorem 1.4 is a consequence of Theorem 1.1.

Let C be a cyclic p-fold cover of $\mathbb{P}^1(\mathbb{F}_q)$. Then, C has an affine model of the form $Y^p = F(X)$, where $F(X)$ is a polynomial in $\mathbb{F}_q[X]$. If $G(X) = H(X)^p F(X)$, then $Y^p = F(X)$ and $Y^p = G(X)$ are isomorphic over $\mathbb{F}_q$, so it suffices to consider curves $Y^p = F(X)$ where $F(X)$ is a polynomial which is pth-power free.

Let $F \in \mathbb{F}_q[X]$ be pth-power free and monic. Recall that pth-power free over $\mathbb{F}_q$ is the same as pth-power free over $\overline{\mathbb{F}}_q$. So F factors in $\overline{\mathbb{F}}_q[X]$ as

$$F(X) = \prod_{i=1}^{d_1}(X - a_{1,i}) \prod_{i=1}^{d_2}(X - a_{2,i})^2 \cdots \prod_{i=1}^{d_{p-1}}(X - a_{p-1,i})^{p-1}$$

where the $a_{i,j}$ are distinct elements of $\overline{\mathbb{F}}_q$.

Let C_F be the cyclic p-fold cover given by $Y^p = F(X) = F_1(X)F_2(X)^2 \dots F_{p-1}(X)^{p-1}$ where the F_i are square-free, relatively prime, and $\deg F_i = d_i$ for $1 \le i \le p-1$ and $d = \deg F = d_1 + 2d_2 + \cdots + (p-1)d_{p-1}$. The number of branch points on C_F is $R = d_1 + \cdots + d_{p-1}$ if $d \equiv 0 \pmod p$ or $R = d_1 + \cdots + d_{p-1} + 1$ otherwise (as the point at infinity is a branch point in the latter case), and the Riemann-Hurwitz formula implies that the genus is $g = (p-1)(R-2)/2$. Then, the curve C_F has genus g if $d = d_1 + 2d_2 + \cdots + (p-1)d_{p-1} \equiv 0 \pmod p$ and $2g = (p-1)(d_1 + \cdots + d_{p-1} - 2)$, or if $d = d_1 + 2d_2 + \cdots + (p-1)d_{p-1} \not\equiv 0 \pmod p$ and $2g = (p-1)(d_1 + \cdots + d_{p-1} - 1)$.

Over $\overline{\mathbb{F}}_q$, one can reparametrize and choose an affine model for any cyclic p-fold cover with $d_1 + 2d_2 + \cdots + (p-1)d_{p-1} \equiv 0 \pmod p$. Furthermore, the moduli space $\mathcal{H}_{g,p}$ of cyclic p-fold covers of $\mathbb{P}^1(\mathbb{F}_q)$ of a fixed genus g splits into irreducible subspaces indexed by equivalence classes of $(p-1)$-tuples of nonnegative integers $(d_1, \dots, d_{p-1})$ with the property that $d_1 + 2d_2 + \cdots + (p-1)d_{p-1} \equiv 0 \pmod p$. We will not expand on the equivalence relations here, but we would like the reader to note that in the $p = 3$ case, they amount to interchanging d_1 and d_2. The moduli space can be written as a disjoint union over its connected components,

$$\mathcal{H}_{g,p} = \bigcup \mathcal{H}^{(d_1,\dots,d_{p-1})}, \tag{5.1}$$

where each component $\mathcal{H}^{(d_1,\dots,d_{p-1})}$ is irreducible. For more details about these Hurwitz spaces, see [4].

From now on, we assume that $d_1 + 2d_2 + \cdots + (p-1)d_{p-1} \equiv 0 \mod p$, and we define

$$\begin{aligned}
\mathcal{F}^j_{(d_1,\dots,d_{p-1})} &= \{F = F_1F_2^2 \dots F_{p-1}^{p-1} \in \mathcal{F}_{(d_1,\dots,d_{j-1},d_j-1,d_{j+1},\dots,d_{p-1})}\} \text{ for } 1 \le j \le p-1, \\
\mathcal{F}^0_{(d_1,\dots,d_{p-1})} &= \mathcal{F}_{(d_1,\dots,d_{p-1})}, \\
\mathcal{F}_{[d_1,\dots,d_{p-1}]} &= \cup_{j=0}^{p-1} \mathcal{F}^j_{(d_1,\dots,d_{p-1})}.
\end{aligned}$$

For any set $\mathcal{F}$ of monic polynomials in $\mathbb{F}_q[X]$, we denote by $\widehat{\mathcal{F}}$ the set of polynomials αF where $\alpha \in \mathbb{F}_q$ and $F \in \mathcal{F}$. This defines the sets $\widehat{\mathcal{F}}_{(d_1,\dots,d_{p-1})}$, $\widehat{\mathcal{F}}^j_{(d_1,\dots,d_{p-1})}$ and $\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$ which are used in this section.

When we write a cyclic p-fold cover of $\mathbb{P}^1$ as

$$C_F : Y^p = F(X) \tag{5.2}$$

where $F(X)$ is pth-power free, we choose an affine model of the curve. To compute the statistics for the components $\mathcal{H}^{(d_1,\dots,d_{p-1})}$ of the moduli space $\mathcal{H}_{g,p}$, we need to work with families of models where we count each curve, seen as a projective variety of dimension 1, up to isomorphism, with the same multiplicity. To do so, we have to consider all pth-power free polynomials in $\mathbb{F}_q[X]$, and not only monic ones. We fix a genus g, and a component $\mathcal{H}^{(d_1,\dots,d_{p-1})}$ for this genus as in the decomposition (5.1). For each curve of this component, we want to count its different affine models $C' : Y^p = G(X)$. Since C' is obtained from an automorphism of $\mathbb{P}^1(\mathbb{F}_q)$, this means that $G \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$ (since $G \in \widehat{\mathcal{F}}_{(d_1,\dots,d_{p-1})}$ if the roots of F are sent to the roots of G, and $G \in \widehat{\mathcal{F}}^j_{(d_1,\dots,d_{p-1})}$ if a root of F_j is sent to the point at infinity).

Assume that C has genus $g > (p-1)^2$ and there are two ways of writing C as a cyclic p-fold cover, i.e. two maps $\phi_{1,2} : C \to \mathbb{P}^1$. They induce a map $\phi : C \to \mathbb{P}^1 \times \mathbb{P}^1$, $\phi = (\phi_1, \phi_2)$. The image of ϕ is a curve rationally equivalent to n_1 times the horizontal fiber plus n_2 times the vertical fiber, where $n_i \in \{1, p\}$ since it has to divide the degree of the projections. The adjunction formula says that the arithmetic genus of the image is equal to $(n_1-1)(n_2-1) \leq (p-1)^2$. Hence the geometric genus is at most $(p-1)^2$, which is strictly less then the genus of C itself. Hence the map ψ from C to the image of ϕ cannot be an isomorphism, in fact it must have degree > 1. But both ϕ_i factor through ψ, hence the degree of ψ can be only either 1 or p. Since we already excluded 1, it follows that the degree is p, which in turn implies that $n_1 = n_2 = 1$. Hence $\mathrm{im}(\phi)$ must be the graph of an automorphism $\mathbb{P}^1 \to \mathbb{P}^1$, and ϕ_1 and ϕ_2 are therefore related by this automorphism.

Hence all curves C' isomorphic to C are obtained from the automorphisms of $\mathbb{P}^1(\mathbb{F}_q)$, namely the $q(q^2-1)$ elements of $\mathrm{PGL}_2(\mathbb{F}_q)$. By running over the elements of $\mathrm{PGL}_2(\mathbb{F}_q)$, we obtain $q(q^2-1)/|\mathrm{Aut}(C)|$ different models $C' : Y^p = G(X)$ where $G \in \widehat{\mathcal{F}}_{[d_1,\ldots,d_{p-1}]}$. This shows that

$$\left|\mathcal{H}^{(d_1,\ldots,d_{p-1})}\right|' = \sum_{C \in \mathcal{H}^{(d_1,\ldots,d_{p-1})}} \frac{1}{|\mathrm{Aut}(C)|} = \frac{\left|\widehat{\mathcal{F}}_{[d_1,\ldots,d_{p-1}]}\right|}{q(q^2-1)}, \tag{5.3}$$

where, as before, the $'$ notation means that the curves C on the moduli space are counted with the usual weights $1/|\mathrm{Aut}(C)|$.

For $1 \leq j \leq p-1$, we denote

$$\widehat{S}_p^j(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_p^j(F(x)),$$

where the value of F at the point at infinity is given by the value at zero of $X^{d_1+2d_2+\cdots+(p-1)d_{p-1}} F(1/X)$. Fix an enumeration of the points on $\mathbb{P}^1(\mathbb{F}_q)$, $x_1, \ldots, x_{q+1}$, such that x_{q+1} denotes the point at infinity. Then

$$F(x_{q+1}) = \begin{cases} \text{leading coefficient of } F & F \in \widehat{\mathcal{F}}_{(d_1,\ldots,d_{p-1})}, \\ 0 & F \in \cup_{j=1}^{p-1} \widehat{\mathcal{F}}^j_{(d_1,\ldots,d_{p-1})}. \end{cases}$$

The number of points on the projective curve C_F with affine model (5.2) is given by

$$\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \left(1 + \sum_{j=1}^{q-1} \chi_p^j(F(x))\right) = q + 1 + \sum_{j=1}^{p-1} \widehat{S}_p^j(F)$$

and

$$\mathrm{Tr}(\mathrm{Frob}_C \mid_{H^1_{\chi_p^j}}) = -\widehat{S}_p^j(F), \quad 1 \leq j \leq p-1. \tag{5.4}$$

It follows easily from the definitions above that

$$\sum_{j=1}^{p-1} \widehat{S}_p^j(F) = \sum_{j=1}^{p-1} S_p^j(F) + \begin{cases} p-1 & F \in \widehat{\mathcal{F}}_{(d_1,\ldots,d_{p-1})} \text{ and leading coefficient of } F \text{ is a } p\text{th-power}, \\ -1 & F \in \widehat{\mathcal{F}}_{(d_1,\ldots,d_{p-1})} \text{ and leading coefficient of } F \text{ is not a } p\text{th-power}, \\ 0 & F \in \cup_{j=1}^{p-1} \widehat{\mathcal{F}}^j_{(d_1,\ldots,d_{p-1})}. \end{cases}$$

As in (5.3), we write

$$\left|\left\{C \in \mathcal{H}^{(d_1,\dots,d_{p-1})} : \mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_p}}) = -t\right\}\right|' = \sum_{\substack{C\in\mathcal{H}^{(d_1,\dots,d_{p-1})}\\ \mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_p}})=-t}} \frac{1}{|\mathrm{Aut}(C)|}. \tag{5.5}$$

It then follows from (5.3), (5.4) and (5.5) that

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,\dots,d_{p-1})} : \mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_p}}) = -t\right\}\right|'}{\left|\mathcal{H}^{(d_1,\dots,d_{p-1})}\right|'} = \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]} \ : \ \widehat{S}_p(F) = t\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}\right|}. \tag{5.6}$$

We first compute

$$\begin{aligned}
\left|\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}\right| &= (q-1)\sum_{j=0}^{p-1}\left|\mathcal{F}^{j}_{(d_1,\dots,d_{p-1})}\right| \\
&= \frac{(q-1)(q+p-1)}{q}\frac{L_{p-2}q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \qquad (5.7)\\
&\times \left(1+O\left(\sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h+1} + q^{-(d_1-1)/2}\right)\right)
\end{aligned} \tag{5.8}$$

by Proposition 3.1.

Fix a $(q+1)$-tuple $(\varepsilon_1,\dots,\varepsilon_{q+1})$ where $\varepsilon_i \in \mu_p^0$ for $1 \le i \le q+1$. Denote by m the number of i such that $\varepsilon_i = 0$. We want to evaluate the probability that the character χ_p takes exactly these values at the points $F(x_1),\dots,F(x_{q+1})$ where x_{q+1} is the point at infinity of $\mathbb{P}^1(\mathbb{F}_q)$, as F ranges over $\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}$.

Case 1: $\varepsilon_{q+1} = 0$.

In this case, only polynomials from $\bigcup_{j=1}^{p-1}\widehat{\mathcal{F}}^{j}_{(d_1,\dots,d_{p-1})}$ can have $\chi_p(F(x_{q+1})) = \varepsilon_{q+1}$. Also, the number of zeros among $\varepsilon_1,\dots,\varepsilon_q$ is now $m-1$. Thus, using Corollary 3.4,

$$\begin{aligned}
&\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]} : \chi_p(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right| \\
&= \sum_{\alpha\in\mathbb{F}_q^*}\left|\left\{F \in \cup_{j=1}^{p-1}\mathcal{F}^{j}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i\chi_p^{-1}(\alpha), 1 \le i \le q\right\}\right| \\
&= \frac{(q-1)(p-1)}{q}\left(\frac{L_{p-2}q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}}\left(\frac{p-1}{q+p-1}\right)^{m-1}\left(\frac{q}{p(q+p-1)}\right)^{q-m+1}\right) \\
&\times \left(1+O\left(q^{\varepsilon q+(1-\varepsilon)m}\sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right).
\end{aligned} \tag{5.9}$$

Case 2: $\varepsilon_{q+1} \in \mu_p$.

In this case, only polynomials from $\widehat{\mathcal{F}}_{(d_1,\dots,d_{p-1})}$ can have $\chi_p(F(x_{q+1})) = \varepsilon_{q+1}$, and there are m values of $\varepsilon_1, \dots, \varepsilon_q$ which are zero. Thus,

$$
\begin{aligned}
&\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]} : \chi_p(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right| \\
&= \sum_{\substack{\alpha \in \mathbb{F}_q^* \\ \chi_p(\alpha) = \varepsilon_{q+1}}} \left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i \varepsilon_{q+1}^{-1}, 1 \le i \le q\right\}\right| \\
&= \frac{q-1}{p} \frac{L_{p-2} q^{d_1+\cdots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q-m} \\
&\times \left(1 + O\left(q^{\varepsilon q + (1-\varepsilon)m} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right),
\end{aligned} \tag{5.10}
$$

which is the same as (5.9).

Then, it follows from (5.7), (5.9) and (5.10) that

$$
\begin{aligned}
\frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]} \ : \ \chi_p(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}\right|} &= \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q+1-m} \\
&\times \left(1 + O\left(q^{\varepsilon q + (1-\varepsilon)m+1} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right).
\end{aligned}
$$

Putting everything together, we obtain

$$
\begin{aligned}
&\frac{\left|\left\{C \in \mathcal{H}^{(d_1,\dots,d_{p-1})} \ : \ \mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_p}}) = -t\right\}\right|'}{\left|\mathcal{H}^{(d_1,\dots,d_{p-1})}\right|'} = \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]} \ : \ \widehat{S}_p(F) = t\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}\right|} \\
&= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_{q+1}) \\ \varepsilon_1+\cdots+\varepsilon_{q+1}=t}} \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]} \ : \ \chi_p(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,\dots,d_{p-1}]}\right|} \\
&= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_{q+1}) \\ \varepsilon_1+\cdots+\varepsilon_{q+1}=t}} \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q+1-m} \\
&\times \left(1 + O\left(q^{\varepsilon q + (1-\varepsilon)m+1} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-m)/2+q}\right)\right) \\
&= \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = t\right) \left(1 + O\left(q^{q+1} \sum_{h=2}^{p-1} q^{\varepsilon(d_h+\cdots+d_{p-1})-d_h} + q^{-(d_1-3q)/2}\right)\right)
\end{aligned}
$$

where $X_1, \dots, X_{q+1}$ are i.i.d. random variables that take the value 0 with probability $(p-1)/(q+p-1)$ and any value in μ_p with probability $q/(p(q+p-1))$. Taking $d_1, \dots, d_{p-1} \to \infty$, this proves Theorem 1.4.

Acknowledgments. This work was initiated at the Banff workshop "Women in Numbers" organized by Kristin Lauter, Rachel Pries, and Renate Scheidler in November 2008, and the authors would like to thank the organizers and BIRS for a great workshop and excellent working conditions. The authors also wish to thank Eduardo Dueñez, Nicholas Katz, Kiran Kedlaya, Pär Kurlberg, Lea Popovic, Rachel Pries, and Zeév Rudnick for helpful discussions related to this work.

This work was supported by the Natural Sciences and Engineering Research Council of Canada [B.F., Discovery Grant 155635-2008 to C.D., 355412-2008 to M.L.]; the National Science Foundation of U.S. [DMS-0652529 to A.B.]; and the University of Alberta [Faculty of Science Startup grant to M.L.]

References

[1] A. Bucur, C. David, B. Feigon, and M. Lalín; Statistics for traces of cyclic trigonal curves over finite fields, accepted for publication, *Int. Math. Res. Not. IMRN.*

[2] P. Kurlberg and Z. Rudnick; The fluctuations in the number of points on a hyperelliptic curve over a finite field. *J. Number Theory* 129 (2009), no. 3, 580–587.

[3] M. Raynaud; Caractéristique d'Euler-Poincaré d'un faisceaux et cohomologie des variétés abeliennes, *Seminaire Bourbaki* **9**, Exp. 286 (1995), 129–147.

[4] M. Romagny and S. Wewers; Hurwitz Spaces, *Groupes de Galois arithmétiques et différentiels*, 313–341, Sémin. Congr., 13, *Soc. Math. France, Paris,* 2006.

[5] M. Rosen; Number Theory in Function Fields, Graduate Texts in Mathematics, 210. *Springer-Verlag, New York*, 2002. xii+358 pp.