Statistics for traces of cyclic trigonal curves over finite field

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

September 7, 2009

Abstract

We study the variation of the trace of the Frobenius endomorphism associated to a cyclic trigonal curve of genus g over $\mathbb{F}_q$ as the curve varies in an irreducible component of the moduli space. We show that for q fixed and g increasing, the limiting distribution of the trace of Frobenius equals the sum of $q+1$ independent random variables taking the value 0 with probability $2/(q+2)$ and $1, e^{2\pi i/3}, e^{4\pi i/3}$ each with probability $q/(3(q+2))$. This extends the work of Kurlberg and Rudnick who considered the same limit for hyperelliptic curves. We also show that when both g and q go to infinity, the normalized trace has a standard complex Gaussian distribution and how to generalize these results to p-fold covers of the projective line.

MSC: 11G20, 11T55, 11G25

To epsilon

Contents

[*] Massachusetts Institute of Technology, alina@math.mit.edu

[†] Concordia University, cdavid@mathstat.concordia.ca

[‡] University of Toronto, bfeigon@math.toronto.edu

[§] University of Alberta, mlalin@math.ualberta.ca

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. For any smooth projective curve C of genus g over $\mathbb{F}_q$, let $Z_C(T)$ be its zeta function. It was shown by Weil [8] that

$$Z_C(T) = \frac{P_C(T)}{(1-T)(1-qT)},$$

with

$$P_C(T) = \prod_{j=1}^{2g} (1 - \alpha_j(C)T),$$

and

$$|\alpha_j(C)| = q^{1/2}, \text{ for } 1 \leq j \leq 2g.$$

The trace of the Frobenius endomorphism (acting on the first cohomology group H^1) is then

$$\mathrm{Tr}(\mathrm{Frob}_C) = \sum_{j=1}^{2g} \alpha_j(C).$$

We study in this paper the variation of the trace of the Frobenius endomorphism Frob_C over moduli spaces of cyclic trigonal curves of genus g when g tends to infinity. This extends the work of Kurlberg and Rudnick who considered the same limit for the case of hyperelliptic curves [5]. All of the results extend further to the case of cyclic p-fold covers of $\mathbb{P}^1$ for p prime, as we indicate briefly in Section 7. However, we have chosen to focus on the trigonal case because it exhibits all of the essential features of the general case but with a somewhat lighter notational load. (Note that some of these features do not appear in [5], including reducibility of the moduli space, complex-valued random variables, and use of the Tauberian theorem.)

Before describing our main results, we describe a modified version of the main theorem of [5]. In the work of Kurlberg and Rudnick, the statistics are computed for the family of hyperelliptic curves $Y^2 = F(X)$ by running over all square-free polynomials F of a fixed degree d. This is not the same as running over the moduli space of hyperelliptic curves of a fixed genus, as not all points on the moduli space appear with the same multiplicity in this family. Also, the results of [5] are about the affine trace of the hyperelliptic curves, which differ slightly from $\mathrm{Tr}(\mathrm{Frob}_C)$. The geometric version of the work of Kurlberg and Rudnick is then the following theorem, which is proved in Section 6.

Theorem 1.1. *If q is fixed and $g \to \infty$, the distribution of the trace of the Frobenius endomorphism associated to C as C ranges over the moduli space $\mathcal{H}_g$ of hyperelliptic curves of genus g defined over $\mathbb{F}_q$ is that of a sum of $q+1$ i.i.d. random variables $X_1, \dots, X_{q+1}$ that take the value 0 with probability $1/(q+1)$ and ± 1 each with probability $1/(2(1+q^{-1}))$. More precisely, for any $s \in \mathbb{Z}$ with $|s| \leq q+1$, we have*

$$\frac{|\{C \in \mathcal{H}_g : \mathrm{Tr}(\mathrm{Frob}_C) = -s\}|'}{|\mathcal{H}_g|'} = \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right)\left(1 + O\left(q^{(3q-2-2g)/2}\right)\right).$$

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 $1/|\mathrm{Aut}(C)|$.

For the rest of the paper, we assume that $q \equiv 1 (\mathrm{mod}\ 3)$. For any cube-free polynomial $F \in \mathbb{F}_q[X]$, let C_F be the cyclic trigonal curve

$$C_F : Y^3 = F(X). \tag{1.1}$$

For cyclic trigonal curves, the genus is not a function of the degree of the polynomial F in (1.1), as it is for the hyperelliptic curves $Y^2 = F(X)$. Also, the moduli space of cyclic trigonal curves of genus g is not irreducible, and we look at the distribution of $\mathrm{Tr}(\mathrm{Frob}_C)$ on each irreducible component (Theorem 1.2). It turns out to be independent of the component when certain conditions are met.

Let $\mathcal{H}_{g,3}$ denote the moduli space of cyclic trigonal curves of genus g. Its irreducible components are determined by a finer geometric invariant, namely the signature. For $d_1+2d_2 \equiv 0 \pmod 3$, let $\mathcal{H}^{(d_1,d_2)}$ be the component of the moduli space with curves of signature $(r,s) = ((2d_1+d_2-3)/3, (d_1+2d_2-3)/3)$. Then

$$\mathcal{H}_{g,3} = \bigcup_{\substack{d_1+2d_2\equiv 0 \pmod 3,\\ g=d_1+d_2-2}} \mathcal{H}^{(d_1,d_2)},$$

where the union is disjoint and each component $\mathcal{H}^{(d_1,d_2)}$ is irreducible.

Fix a cubic character χ_3 of $\mathbb{F}_q$ (recall that $q \equiv 1 \,(\mathrm{mod}\, 3)$). It takes values $0, 1, \omega$ and ω^2, where ω is a primitive third root of unity in $\mathbb{C}$. Each cyclic trigonal curve C is endowed with a cyclic order 3 automorphism that splits the first cohomology group of C into two subspaces, $H^1_{\chi_3}$ and $H^1_{\overline{\chi}_3}$, on which the automorphism acts via χ_3 or via its conjugate. Since this automorphism commutes with the action of the Frobenius, it follows that

$$\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}}) = \overline{\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\overline{\chi}_3}})}.$$

So it is enough to study the distribution of the trace of the Frobenius on one of these two subspaces.

Theorem 1.2. *If q is fixed and $d_1, d_2 \to \infty$, the distribution of the trace of the Frobenius endomorphism associated to C as C ranges over the component $\mathcal{H}^{(d_1,d_2)}$ of cyclic trigonal curves defined over $\mathbb{F}_q$ is that of the sum of $q+1$ i.i.d. random variables $X_1, \dots, X_{q+1}$, where each X_i takes the value 0 with probability $2/(q+2)$ and $1, \omega, \omega^2$ each with probability $q/(3(q+2))$. More precisely, for any $s \in \mathbb{Z}[\omega] \subset \mathbb{C}$ with $|s| \le q+1$, we have for any $1 > \varepsilon > 0$,*

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,d_2)} : \mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}}) = -s\right\}\right|'}{\left|\mathcal{H}^{(d_1,d_2)}\right|'} = \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right)\left(1 + O\left(q^{-(1-\varepsilon)d_2+q} + q^{-(d_1-3q)/2}\right)\right).$$

It may not be clear where the probabilities attached to the random variables come from, but they are quite natural, as the heuristic in Section 8.2 shows.

We remark that in Theorem 1.2, and in all the results in our paper, the implied constants in the error terms are independent of q, even when q is fixed. Then, as was done in [5] for hyperelliptic curves, we can also study the case where q and d_1, d_2 tend to infinity. Since the trace takes complex values, the limiting distribution will be the *complex* Gaussian with mean 0 and variance 1, instead of the usual real-valued Gaussian one gets for hyperelliptic curves. We first compute the moments of $\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})/\sqrt{q+1}$ and compare them with the moments of the normalized sum of the i.i.d. random variables of Theorem 1.2.

Theorem 1.3. *For any positive integers j and k, let $M_{j,k}(q,(d_1,d_2))$ be the moments*

$$M_{j,k}(q,(d_1,d_2)) \;=\; \frac{1}{\left|\mathcal{H}^{(d_1,d_2)}\right|'} \sideset{}{'}\sum_{C\in\mathcal{H}^{(d_1,d_2)}} \left(\frac{-\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})}{\sqrt{q+1}}\right)^j \left(\frac{-\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\overline{\chi}_3}})}{\sqrt{q+1}}\right)^k.$$

Let ε and $X_1, \dots, X_{q+1}$ be as in Theorem 1.2. Then

$$M_{j,k}(q,(d_1,d_2)) = \mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} X_i\right)^j \left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} \overline{X_i}\right)^k\right)\left(1 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon(j+k)} + q^{-d_1/2+j+k}\right)\right).$$

Corollary 1.4. *When q, d_1, d_2 tend to infinity, the limiting distribution of the normalized trace* $\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})/\sqrt{q+1}$ *is a complex Gaussian with mean zero and variance one.*

We remark that when g is fixed and q tends to infinity, $\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})$ should be distributed as the trace of matrices in a group of random matrices determined by the monodromy group of the moduli space of C in the philosophy of Katz and Sarnak [4]. The monodromy groups for cyclic trigonal curves are computed in [1, Theorem 3.8]. Roughly speaking, the monodromy of each component $\mathcal{H}^{(d_1,d_2)}$ of signature (r,s) of the moduli space $\mathcal{H}_{g,3}$ is an extension of the group of sixth roots of unity $\boldsymbol{\mu}_6$ by the special unitary group $\mathrm{SU}(r,s)$. The monodromy for the component $\mathcal{H}^{(d,0)}$ is computed in [3, Theorem 5.4], and the result is an extension of $\boldsymbol{\mu}_6$ by $\mathrm{SL}(g)$.

The structure of this paper is as follows. In Section 2, we describe moduli spaces of cyclic trigonal curves, and present some notations and results which will be used in the rest of the paper. In Section 3, we describe how $\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})$ can be written as a sum of $q+1$ values of the cubic character of χ_3 of $\mathbb{F}_q$, and how to compute statistics of the trace by counting classes of the moduli spaces. The proof of Theorem 1.2 is concluded in Section 4. We compute the moments of $\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})/\sqrt{q+1}$ and prove Corollary 1.4 in Section 5, and we revisit the case of hyperelliptic curves in Section 6. In Section 7 we explain how the techniques employed in the study of cyclic trigonal case can be adapted to the general case of cyclic p-fold covers of $\mathbb{P}^1(\mathbb{F}_q)$. Finally, we present in Section 8 a heuristic model which predicts the results obtained in Theorems 1.1, 1.2 and 7.4.

2 Setting and notation

Fix $q \equiv 1 \pmod 3$. We will denote by ζ_q the (incomplete) zeta function of the rational function field $\mathbb{F}_q[X]$ given by

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

Let C be a cyclic trigonal curve over $\mathbb{F}_q$, i.e. a cyclic cover of order 3 of $\mathbb{P}^1$ defined over $\mathbb{F}_q$. Then, C has an affine model $Y^3 = F(X)$, where $F(X)$ is a polynomial in $\mathbb{F}_q[X]$. If $G(X) = H(X)^3F(X)$, then $Y^3 = F(X)$ and $Y^3 = G(X)$ are isomorphic over $\mathbb{F}_q$, so it suffices to consider curves $Y^3 = F(X)$ with $F(X)$ cube-free.

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

$$F(X) = \prod_{i=1}^{d_1}(X-a_i)\prod_{j=1}^{d_2}(X-b_j)^2,$$

where a_i, b_j are distinct elements of $\overline{\mathbb{F}}_q$.

Let C_F be the cyclic trigonal curve given by $Y^3 = F(X) = F_1(X)F_2(X)^2$, with F_1 and F_2 relatively prime, square-free, $\deg F_1 = d_1$, $\deg F_2 = d_2$ and $d = \deg F = d_1 + 2d_2$. The curve C_F has genus g if and only if $d_1+2d_2 \equiv 0 \pmod 3$ and $g = d_1+d_2-2$, or $d_1+2d_2 \equiv 1$ or $2 \pmod 3$ and $g = d_1+d_2-1$. Over $\overline{\mathbb{F}}_q$, one can reparametrize and choose an affine model for any cyclic trigonal curve with $d_1+2d_2 \equiv 0 \,(\mathrm{mod}\, 3)$. We already see that the relationship between the genus of the curve C_F and the degree of the polynomial F defining it is not as simple as in the hyperelliptic case, as the genus is not a function of the degree. Note that by interchanging F_1 and F_2, we are replacing F by F^2 (modulo a perfect cube) and the two curves $Y^3 = F_1(X)F_2(X)^2$ and $Y^3 = F_1(X)^2F_2(X)$ are isomorphic. Furthermore, the moduli space $\mathcal{H}_{g,3}$ of cyclic trigonal curves of fixed genus g splits into irreducible subspaces indexed by pairs of nonnegative integers d_1, d_2 with the property that $d_1 + 2d_2 \equiv 0 \pmod 3$, and the moduli space can be written as a disjoint union over its connected components

$$\mathcal{H}_{g,3} = \bigcup_{\substack{d_1+2d_2 \equiv 0 \pmod 3, \\ g = d_1+d_2-2}} \mathcal{H}^{(d_1,d_2)}. \tag{2.1}$$

Each component $\mathcal{H}^{(d_1,d_2)}$ is irreducible, and pairs (d_1, d_2) and (d_2, d_1) give the same component.

The components can also be described by their signature (r, s). The signature and (d_1, d_2) are related by $d_1 = 2r - s + 1$ and $d_2 = 2s - r + 1$, or equivalently $r = (2d_1 + d_2 - 3)/3$ and $s = (d_1 + 2d_2 - 3)/3$. Each unordered pair $\{r, s\}$ represents a different component of the moduli space of cyclic trigonal curves. We refer the reader to [1] for the details.

In view of the previous observations, we will write

$$F(X) = F_1(X)F_2(X)^2,$$

where F_1 and F_2 are relatively prime monic square-free polynomials with $\deg F_1 = d_1$ and $\deg F_2 = d_2$.

We will use the following sets of polynomials:

$$\begin{array}{rcl}
V_d &=& \{F \in \mathbb{F}_q[X] \ : \ F \text{ monic}, \deg F = d\} \\
\mathcal{F}_d &=& \{F \in \mathbb{F}_q[X] : F \text{ monic, square-free and} \deg F = d\} \\
\widehat{\mathcal{F}}_d &=& \{F \in \mathbb{F}_q[X] : F \text{ square-free and} \deg F = d\} \\
\mathcal{F}_{(d_1,d_2)} &=& \{F = F_1F_2^2 : F_1, F_2 \text{ monic, square-free and coprime}, \deg F_1 = d_1, \deg F_2 = d_2\} \\
\mathcal{F}^k_{(d_1,d_2)} &=& \left\{F = F_1F_2^2 \in \mathcal{F}_{(d_1,d_2)} : F_2 \text{ has } k \text{ roots in } \mathbb{F}_q\right\} \\
\widehat{\mathcal{F}}_{(d_1,d_2)} &=& \left\{F = \alpha F_1F_2^2 \ : \ \alpha \in \mathbb{F}_q^*, F_1F_2^2 \in \mathcal{F}_{(d_1,d_2)}\right\} \\
\mathcal{F}_{[d_1,d_2]} &=& \mathcal{F}_{(d_1,d_2)} \cup \mathcal{F}_{(d_1-1,d_2)} \cup \mathcal{F}_{(d_1,d_2-1)} \\
\widehat{\mathcal{F}}_{[d_1,d_2]} &=& \widehat{\mathcal{F}}_{(d_1,d_2)} \cup \widehat{\mathcal{F}}_{(d_1-1,d_2)} \cup \widehat{\mathcal{F}}_{(d_1,d_2-1)}.
\end{array}$$

As a matter of convention, from now on, all our polynomials will be monic unless otherwise stated. Also, we will use P to denote monic irreducible polynomials.

We transcribe here the relevant results from the work of Kurlberg and Rudnick [5].

Lemma 2.1. *[5, Lemma 3] The number of square-free monic polynomials of degree d is*

$$|\mathcal{F}_d| = \begin{cases} q^d(1-q^{-1}) & d \geq 2, \\ q^d & d = 0, 1. \end{cases}$$

Lemma 2.2. *[5, Lemma 4] For $0 \leq \ell \leq q$, let $x_1, \dots, x_\ell \in \mathbb{F}_q$ be distinct elements, and let $a_1, \dots, a_\ell \in \mathbb{F}_q$. If $d \geq \ell$, then*

$$|\{F \in V_d : F(x_1) = a_1, \dots, F(x_\ell) = a_\ell\}| = q^{d-\ell}.$$

Lemma 2.3. *[5, Lemma 5] Let $d \geq 2$ and $\ell \leq q$ be positive integers, let $x_1, \dots, x_\ell \in \mathbb{F}_q$ be distinct elements, and let $a_1, \dots, a_\ell \in \mathbb{F}_q$ be nonzero elements. Then*

$$|\{F \in \mathcal{F}_d : F(x_1) = a_1, \dots, F(x_\ell) = a_\ell\}| = \frac{q^{d-\ell}}{\zeta_q(2)(1-q^{-2})^\ell} + O\left(q^{d/2}\right).$$

Lemma 2.4. *[5, Proposition 6] Let $x_1, \ldots, x_{\ell+m} \in \mathbb{F}_q$ be distinct elements, let $a_1, \ldots, a_\ell \in \mathbb{F}_q^*$, and let $a_{\ell+1} = \cdots = a_{\ell+m} = 0$. Then*

$$|\{F \in \mathcal{F}_d : F(x_i) = a_i, 1 \leq i \leq m+\ell\}| = \frac{(1-q^{-1})^m q^{d-(m+\ell)}}{\zeta_q(2)(1-q^{-2})^{m+\ell}} \left(1 + O\left(q^{(3m+2\ell-d)/2}\right)\right).$$

and

$$\frac{|\{F \in \mathcal{F}_d : F(x_i) = a_i, 1 \leq i \leq m+\ell\}|}{|\mathcal{F}_d|} = \frac{(1-q^{-1})^m q^{-(m+\ell)}}{(1-q^{-2})^{m+\ell}} \left(1 + O\left(q^{(3m+2\ell-d)/2}\right)\right).$$

We will also use the following Lemma which follows easily from Lemma 2.4.

Lemma 2.5. *Fix $0 \leq k \leq q$. Then*

$$|\mathcal{F}_d^k| = \frac{\binom{q}{k} q^{d-k}}{\zeta_q(2)(1+q^{-1})^q} \left(1 + O\left(q^{(k+2q-d)/2}\right)\right).$$

Proof. In the Lemma 2.4, set $m = k$ and $\ell = q-k$. In this way, we guarantee that there are exactly k zeros. Now we also have $\binom{q}{k}$ options for choosing the zeros, and $(q-1)^\ell$ options for choosing the nonzero values. Combining all of this with Lemma 2.4, we get the formula. □

3 The geometric point of view

We prove in this section that Theorem 1.2 follows from the following theorem which will be proved in Section 4. Recall that χ_3 is a fixed cubic character of $\mathbb{F}_q$ and ω is a primitive third root of unity in $\mathbb{C}$.

Theorem 3.1. *Let $x_1, \ldots, x_q$ be the elements of $\mathbb{F}_q$ and let $\varepsilon_1, \ldots, \varepsilon_q \in \{0, 1, \omega, \omega^2\}$. Let m be the number of values of ε_i which are 0. Then for any $\varepsilon > 0$*

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

$$\begin{aligned} \left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \;:\; \chi_3(F(x_i)) = \varepsilon_i,\; 1 \leq i \leq q\right\}\right| &= \frac{K q^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q} + q^{-(d_1-m)/2+q}\right)\right), \end{aligned} \tag{3.1}$$

and

$$\begin{aligned} \frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \;:\; \chi_3(F(x_i)) = \varepsilon_i,\; 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}\right|} &= \left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q} + q^{-(d_1-m)/2+q}\right)\right), \end{aligned}$$

where K is the constant

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

For any polynomial $F \in \mathcal{F}_{(d_1,d_2)}$, let

$$S_3(F) = \sum_{x \in \mathbb{F}_q} \chi_3(F(x)). \tag{3.2}$$

Then, the number of affine points on the curve $Y^3 = F(X)$ is given by

$$\sum_{x \in \mathbb{F}_q} 1 + \chi_3(F(x)) + \overline{\chi_3(F(x))} = q + S_3(F) + \overline{S_3(F)}.$$

Using Theorem 3.1, we can immediately deduce a result for the distribution of the affine trace $-(S_3(F) + \overline{S_3(F)})$ when we vary over the family of curves $C_F : Y^3 = F(X)$ for $F(X) \in \mathcal{F}_{(d_1,d_2)}$. This is the "non-geometric version" of Theorem 1.2 which corresponds to Theorem 1 of [5]. When comparing Theorem 1.2 and Corollary 3.2, it is interesting to remark that the point at infinity appearing in the trace of the Frobenius on $H^1_{\chi_3}$, and not in the affine trace, behaves like any other point.

Corollary 3.2. *Let $X_1, \dots, X_q$ be q i.i.d. random variables taking the value 0 with probability $2/(q+2)$ and any of the values $1, \omega, \omega^2$ with probability $q/(3(q+2))$. Then for any $\varepsilon > 0$,*

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ S_3(F) = s\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}\right|} \quad = \quad \text{Prob}\left(\sum_{i=1}^{q} X_i = s\right)\left(1 + O\left(q^{-(1-\varepsilon)d_2+q} + q^{-(d_1-3q)/2}\right)\right)$$

for any $s \in \mathbb{Z}[\omega] \subset \mathbb{C}$.

Proof. Using (3.2), we write

$$\begin{aligned}
&\frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ S_3(F) = s\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}\right|} \\
&= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_q) \in \{0,1,\omega,\omega^2\} \\ \varepsilon_1 + \cdots + \varepsilon_q = s}} \frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ \chi_3(F(x_i)) = \varepsilon_i, \ 1 \le i \le q\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}\right|} \\
&= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_q) \in \{0,1,\omega,\omega^2\} \\ \varepsilon_1 + \cdots + \varepsilon_q = s}} \left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q-m} \left(1 + O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q} + q^{-(d_1-m)/2+q}\right)\right) \\
&= \text{Prob}\left(\sum_{i=1}^{q} X_i = s\right)\left(1 + O\left(q^{-(1-\varepsilon)(d_2-q)+\varepsilon q} + q^{-(d_1-q)/2+q}\right)\right).
\end{aligned}$$

□

Proof of Theorem 1.2. We now proceed to the proof of Theorem 1.2, assuming Theorem 3.1. When we write a cyclic trigonal curve as

$$C_F : Y^3 = F(X) \tag{3.3}$$

where $F(X)$ is cube-free, we are choosing an affine model of the curve. To compute the statistics for the components $\mathcal{H}^{(d_1,d_2)}$ of the moduli space $\mathcal{H}_{g,3}$, we need to work with families 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 cube-free polynomials in $\mathbb{F}_q[X]$, and not only monic ones. We fix a genus g, and a component $\mathcal{H}^{(d_1,d_2)}$ for this genus as in equation (2.1). For each point of this component, we want to count its affine models $C' : Y^3 = G(X)$ with $G \in \widehat{\mathcal{F}}_{[d_1,d_2]}$.

For $g \geq 5$, the 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 $C' : Y^3 = G(X)$ where $G \in \widehat{\mathcal{F}}_{[d_1,d_2]}$. This shows that

$$|\mathcal{H}^{(d_1,d_2)}|' = \sum_{C \in \mathcal{H}^{(d_1,d_2)}}{}' 1 = \sum_{C \in \mathcal{H}^{(d_1,d_2)}} \frac{1}{|\mathrm{Aut}(C)|} \quad = \quad \frac{|\widehat{\mathcal{F}}_{[d_1,d_2]}|}{q(q^2-1)}. \tag{3.4}$$

We denote

$$\widehat{S}_3(F) \quad = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x)),$$

where the value of F at the point at infinity is defined below. Fix an enumeration of the points on $\mathbb{P}^1(\mathbb{F}_q)$, $x_1, \dots, x_{q+1}$, such that x_{q+1} denotes the point at infinity. Then

$$F(x_{q+1}) = \begin{cases} \text{leading coefficient of } F & F \in \widehat{\mathcal{F}}_{(d_1,d_2)}, \\ 0 & F \in \widehat{\mathcal{F}}_{(d_1-1,d_2)} \cup \widehat{\mathcal{F}}_{(d_1,d_2-1)}. \end{cases}$$

Therefore, $\widehat{S}_3(F) + \overline{\widehat{S}_3(F)}$ is equal to

$$S_3(F) + \overline{S_3(F)} + \begin{cases} 2 & F \in \widehat{\mathcal{F}}_{(d_1,d_2)} \text{ and leading coefficient of } F \text{ is a cube}, \\ -1 & F \in \widehat{\mathcal{F}}_{(d_1,d_2)} \text{ and leading coefficient of } F \text{ is not a cube}, \\ 0 & F \in \widehat{\mathcal{F}}_{(d_1-1,d_2)} \cup \widehat{\mathcal{F}}_{(d_1,d_2-1)}. \end{cases}$$

Then, the number of points on the projective curve C_F with affine model (3.3) is given by

$$\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} 1 + \chi_3(F(x)) + \overline{\chi_3(F(x))} = q + 1 + \widehat{S}_3(F) + \overline{\widehat{S}_3(F)}$$

and

$$\mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_3}}) \quad = \quad -\widehat{S}_3(F) \tag{3.5}$$

$$\mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\overline{\chi_3}}}) \quad = \quad -\overline{\widehat{S}_3(F)}. \tag{3.6}$$

As in (3.4), we write

$$\left|\left\{C \in \mathcal{H}^{(d_1,d_2)} : \mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_3}}) = -s\right\}\right|' = \sum_{\substack{C \in \mathcal{H}^{(d_1,d_2)} \\ \mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_3}}) = -s}} \frac{1}{|\mathrm{Aut}(C)|}. \tag{3.7}$$

It then follows from (3.4), (3.5) and (3.7) that

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,d_2)} : \mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_3}}) = -s\right\}\right|'}{\left|\mathcal{H}^{(d_1,d_2)}\right|'} \quad = \quad \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,d_2]} \ : \ \widehat{S}_3(F) = s\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,d_2]}\right|}. \tag{3.8}$$

We now rewrite (3.8) in terms of polynomials in $\mathcal{F}_{(d_1,d_2)}$. We first compute

$$\begin{aligned} |\widehat{\mathcal{F}}_{[d_1,d_2]}| &= (q-1)\left(\left|\mathcal{F}_{(d_1,d_2)}\right| + \left|\mathcal{F}_{(d_1-1,d_2)}\right| + \left|\mathcal{F}_{(d_1,d_2-1)}\right|\right) \\ &= \frac{K}{\zeta_q(2)^2}\frac{(q+2)(q-1)}{q}q^{d_1+d_2}\left(1+O\left(q^{-(1-\varepsilon)d_2}+q^{-d_1/2}\right)\right) \end{aligned} \tag{3.9}$$

by Theorem 3.1.

Fix a $(q+1)$-tuple $(\varepsilon_1,\dots,\varepsilon_{q+1})$ where $\varepsilon_i \in \{0,1,\omega,\omega^2\}$ 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_3 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 $\widehat{\mathcal{F}}_{[d_1,d_2]}$.

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

In this case, only polynomials from $\widehat{\mathcal{F}}_{(d_1-1,d_2)} \cup \widehat{\mathcal{F}}_{(d_1,d_2-1)}$ can have $\chi_3(F(x_{q+1})) = \varepsilon_{q+1}$. Also, the number of zeros among $\varepsilon_1,\dots,\varepsilon_q$ is now $m-1$. Thus using (3.1)

$$\begin{aligned} &\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,d_2]} : \chi_3(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right| \\ &= \sum_{\alpha\in\mathbb{F}_q^*} \left|\left\{F \in \mathcal{F}_{(d_1-1,d_2)} \cup \mathcal{F}_{(d_1,d_2-1)} : \chi_3(F(x_i)) = \varepsilon_i\chi_3^{-1}(\alpha), 1 \le i \le q\right\}\right| \\ &= 2(q-1)\left(\frac{Kq^{d_1+d_2-1}}{\zeta_q(2)^2}\left(\frac{2}{q+2}\right)^{m-1}\left(\frac{q}{3(q+2)}\right)^{q-m+1}\right) \\ &\times\left(1+O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q}+q^{-(d_1-m)/2+q}\right)\right). \end{aligned} \tag{3.10}$$

Case 2: $\varepsilon_{q+1} = 1, \omega$, or ω^2.

In this case, only polynomials from $\widehat{\mathcal{F}}_{(d_1,d_2)}$ can have $\chi_3(F(x_{q+1})) = \varepsilon_{q+1}$, and there are m values of $\varepsilon_1,\dots,\varepsilon_q$ which are zero. Thus

$$\begin{aligned} &\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,d_2]} : \chi_3(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right| \\ &= \sum_{\substack{\alpha\in\mathbb{F}_q^* \\ \chi_3(\alpha)=\varepsilon_{q+1}}} \left|\left\{F \in \mathcal{F}_{(d_1,d_2)} : \chi_3(F(x_i)) = \varepsilon_i\varepsilon_{q+1}^{-1}, 1 \le i \le q\right\}\right| \\ &= \frac{q-1}{3}\frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{2}{q+2}\right)^{m}\left(\frac{q}{3(q+2)}\right)^{q-m} \\ &\times\left(1+O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q}+q^{-(d_1-m)/2+q}\right)\right), \end{aligned} \tag{3.11}$$

which is the same as (3.10).

Then, it follows from (3.9), (3.10) and (3.11) that

$$\begin{aligned} \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,d_2]} \ : \ \chi_3(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,d_2]}\right|} &= \left(\frac{2}{q+2}\right)^{m}\left(\frac{q}{3(q+2)}\right)^{q+1-m} \\ &\times \left(1+O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q}+q^{-(d_1-m)/2+q}\right)\right). \end{aligned}$$

Putting everything together, we obtain

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,d_2)} \ : \ \mathrm{Tr}(\mathrm{Frob}_C) = -s\right\}\right|'}{\left|\mathcal{H}^{(d_1,d_2)}\right|'} = \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,d_2]} \ : \ \widehat{S}_3(F) = s\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,d_2]}\right|}$$

$$= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_{q+1}) \\ \varepsilon_1+\cdots+\varepsilon_{q+1}=s}} \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{[d_1,d_2]} \ : \ \chi_3(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right|}{\left|\widehat{\mathcal{F}}_{[d_1,d_2]}\right|}$$

$$= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_{q+1}) \\ \varepsilon_1+\cdots+\varepsilon_{q+1}=s}} \left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q+1-m} \left(1 + O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q} + q^{-(d_1-m)/2+q}\right)\right)$$

$$= \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right) \left(1 + O\left(q^{-(1-\varepsilon)(d_2-q)+\varepsilon q} + q^{-(d_1-q)/2+q}\right)\right)$$

where $X_1, \dots, X_{q+1}$ $q+1$ are i.i.d. random variables that take the value 0 with probability $2/(q+2)$ and $1, \omega, \omega^2$ each with probability $q/(3(q+2))$. □

We concentrate on the proof of Theorem 3.1 in the next section.

4 Distribution of the trace for cube-free polynomials

In this section we prove Theorem 3.1 by obtaining asymptotic formulas for $|\mathcal{F}_{(d_1,d_2)}|$ and $\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} : F(x_i) = a_i, 1 \le i \le q\right\}\right|$ for $d_1, d_2 \to \infty$. We begin with two lemmas that count the number of polynomials that obtain specified nonzero values and are relatively prime to a fixed polynomial.

Lemma 4.1. *For $\min\{d, q\} \ge \ell \ge 0$ let $x_1, x_2, \dots, x_\ell \in \mathbb{F}_q$ be distinct elements. Let $U \in \mathbb{F}_q[X]$ be such that $U(x_i) \ne 0$ for $i = 1, \dots, \ell$. Let $a_1, a_2, \dots, a_\ell \in \mathbb{F}_q^*$, then*

$$|\{F \in V_d : (F, U) = 1, F(x_i) = a_i, 1 \le i \le \ell\}| = q^{d-\ell} \prod_{P|U} (1 - q^{-\deg P}).$$

Note that when $\ell = 0$, there is no condition imposed at any point in $\mathbb{F}_q$.

Proof. By inclusion-exclusion we have

$$|\{F \in V_d : (F, U) = 1, F(x_i) = a_i, 1 \le i \le \ell\}| = \sum_{D|U} \mu(D) \sum_{\substack{F \in V_d \\ D|F \\ F(x_i)=a_i}} 1,$$

where μ is the Möebius function. Using the fact that $U(x_i) \ne 0$ this equals

$$\sum_{D|U} \mu(D) \sum_{\substack{G \in V_{d-\deg D} \\ G(x_i)=a_i D(x_i)^{-1}}} 1.$$

By Lemma 2.2 this equals

$$\sum_{D|U} \mu(D) q^{d-\deg D-\ell} = q^{d-\ell} \sum_{D|U} \mu(D) q^{-\deg D}.$$

The function $f(D) = \mu(D)q^{-\deg D}$ is multiplicative, so is $g(U) = \sum_{D|U} f(D)$, and

$$g(P^e) = 1 - q^{-\deg P}$$

for $e \geq 1$. Applying this to the last equation,

$$|\{F \in V_d : (F,U) = 1, F(x_i) = a_i, 1 \leq i \leq \ell\}| = q^{d-\ell} \prod_{P|U} (1 - q^{-\deg P}).$$

□

Our proof of the next lemma follows the same steps as the proof of Lemma 2.3 (Lemma 5 in [5]), with the added condition that the polynomials we are counting are relatively prime to a fixed polynomial.

Lemma 4.2. *For $q \geq \ell \geq 0$ let $x_1, \dots, x_\ell \in \mathbb{F}_q$ be distinct elements. Let $U \in \mathbb{F}_q[X]$ be such that $U(x_i) \neq 0$ for $i = 1, \dots, \ell$. Let $a_1, \dots, a_\ell \in \mathbb{F}_q^*$. Let $S_d^U(\ell)$ be the number of elements in the set*

$$\{F \in \mathcal{F}_d : (F,U) = 1,\ F(x_i) = a_i,\ 1 \leq i \leq \ell\}.$$

Then

$$S_d^U(\ell) = \frac{q^{d-\ell}}{\zeta_q(2)(1-q^{-2})^\ell} \prod_{P|U} (1 + q^{-\deg P})^{-1} + O\left(q^{d/2}\right).$$

Proof. By inclusion-exclusion we have

$$S_d^U(\ell) = \sum_{\substack{D,\, \deg D \leq d/2 \\ (D,U)=1}} \mu(D) \left|\left\{F \in V_{d-2\deg(D)} : (F,U) = 1, D(x_i)^2 F(x_i) = a_i, 1 \leq i \leq \ell\right\}\right|.$$

We denote by $\tilde{\sum}$ the sum over all polynomials D such that $D(x_i) \neq 0$ for $1 \leq i \leq \ell$. Then

$$S_d^U(\ell) = \tilde{\sum_{\substack{\deg D \leq d/2 \\ (D,U)=1}}} \mu(D) \left|\left\{F \in V_{d-2\deg(D)} : (F,U) = 1, F(x_i) = a_i D(x_i)^{-2}, 1 \leq i \leq \ell\right\}\right|.$$

For $d - 2\deg D \geq \ell$, by Lemma 4.1 we have

$$\left|\left\{F \in V_{d-2\deg D} : (F,U) = 1, F(x_i) = a_i D(x_i)^{-2}, 1 \leq i \leq \ell\right\}\right| = q^{d-2\deg D-\ell} \prod_{P|U} (1 - q^{-\deg P}).$$

Therefore

$$S_d^U(\ell) = q^{d-\ell} \prod_{P|U} (1 - q^{-\deg P}) \tilde{\sum_{\substack{\deg D < (d-\ell)/2 \\ (D,U)=1}}} \mu(D) q^{-2\deg D} + \text{ Error.} \tag{4.1}$$

There is at most one F of degree less than or equal to ℓ that takes ℓ prescribed values at ℓ distinct points, thus

$$\text{Error } \ll \sum_{(d-\ell)/2 \leq \deg D \leq d/2} 1 = q^{d/2} \left(\frac{1 - q^{-\ell/2-1}}{1 - q^{-1}}\right) = O(q^{d/2}). \tag{4.2}$$

Now we observe that

$$\overset{\sim}{\sum_{\substack{\deg D<(d-\ell)/2\\(D,U)=1}}}\mu(D)q^{-2\deg D}=\overset{\sim}{\sum_{\substack{D\\(D,U)=1}}}\mu(D)q^{-2\deg D}+O(q^{(\ell-d)/2}) \tag{4.3}$$

and

$$\overset{\sim}{\sum_{\substack{D\\(D,U)=1}}}\mu(D)|D|^{-2s}=\prod_{\substack{P,P(x_i)\neq 0\\P\nmid U}}(1-|P|^{-2s}).$$

Using that $U(x_i)\neq 0$, we find that

$$\overset{\sim}{\sum_{\substack{D\\(D,U)=1}}}\mu(D)|D|^{-2s}=\frac{1}{\zeta_q(2s)(1-q^{-2s})^{\ell}}\prod_{P|U}(1-|P|^{-2s})^{-1}. \tag{4.4}$$

By (4.1), (4.2), (4.3) and (4.4) we have

$$\begin{aligned}S_d^U(\ell)&=q^{d-\ell}\prod_{P|U}(1-q^{-\deg P})\left(\frac{1}{\zeta_q(2)(1-q^{-2})^{\ell}}\prod_{P|U}(1-|P|^{-2})^{-1}+O(q^{(\ell-d)/2})\right)+O(q^{d/2})\\&=\frac{q^{d-\ell}}{\zeta_q(2)(1-q^{-2})^{\ell}}\prod_{P|U}(1+q^{-\deg P})^{-1}+O\left(q^{d/2}\right).\end{aligned}$$

□

We now use Lemma 4.2 along with the function field version of the Tauberian Theorem to count the number of polynomials in $\mathcal{F}_{(d_1,d_2)}$ that take a prescribed set of nonzero values on ℓ points.

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

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

where

$$K=\prod_P\left(1-\frac{1}{(|P|+1)^2}\right), \tag{4.5}$$

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

In particular, we have

$$\left|\mathcal{F}_{(d_1,d_2)}\right|\;=\;\frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(1+O\left(q^{-(1-\varepsilon)d_2}+q^{-d_1/2}\right)\right). \tag{4.6}$$

Proof. First we observe that

$$\begin{aligned}\left|\left\{F\in\mathcal{F}_{(d_1,d_2)}:F(x_i)=a_i,1\leq i\leq\ell\right\}\right|&=\sum_{\substack{F_2\in\mathcal{F}_{d_2}\\F_2(x_i)\neq0,1\leq i\leq\ell}}\;\sum_{\substack{F_1\in\mathcal{F}_{d_1}\\F_1(x_i)=a_iF_2(x_i)^{-2},1\leq i\leq\ell\\(F_1,F_2)=1}}1\\&=\sum_{\substack{F\in\mathcal{F}_{d_2}\\F_2(x_i)\neq0,1\leq i\leq\ell}}S_{d_1}^{F_2}(\ell).\end{aligned}$$

Using Lemma 4.2 we have that

$$\begin{aligned}&\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \;:\; F(x_i) = a_i,\; 1 \le i \le \ell\right\}\right| \\ &= \frac{q^{d_1-\ell}}{\zeta_q(2)(1-q^{-2})^{\ell}} \sum_{\substack{F_2 \in \mathcal{F}_{d_2} \\ F_2(x_i) \ne 0, 1 \le i \le \ell}} \prod_{P \mid F_2} (1 + q^{-\deg P})^{-1} + \sum_{\substack{F_2 \in \mathcal{F}_{d_2} \\ F_2(x_i) \ne 0, 1 \le i \le \ell}} O\left(q^{d_1/2}\right).\end{aligned}$$

Then by Lemma 2.1 and Lemma 2.3,

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

where for any polynomial F

$$b(F) = \begin{cases} \mu^2(F) \prod_{P \mid F} (1 + |P|^{-1})^{-1} & F(x_i) \ne 0, 1 \le i \le \ell, \\ 0 & \text{otherwise.} \end{cases} \tag{4.7}$$

To evaluate $\sum_{\deg F = d_2} b(F)$, we consider the Dirichlet series

$$\begin{aligned} G(s) = \sum_F \frac{b(F)}{|F|^s} &= \prod_{\substack{P \\ P(x_i) \ne 0, 1 \le i \le \ell}} \left(1 + \frac{1}{|P|^s} \cdot \frac{|P|}{|P|+1}\right) \\ &= \frac{\zeta_q(s)}{\zeta_q(2s)} H(s) \left(1 + \frac{1}{q^{s-1}(q+1)}\right)^{-\ell}, \end{aligned}$$

where

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

Notice that $H(s)$ converges absolutely for $\mathrm{Re}(s) > 0$, and $G(s)$ 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 $H(1) = K$, where K is the constant given in (4.5) and $\mathrm{Res}_{s=1}\zeta_q(s) = \frac{1}{\log q}$. Thus $G(s)$ has a simple pole at $s = 1$ with residue

$$\frac{K}{\zeta_q(2) \log q} \left(\frac{q+1}{q+2}\right)^{\ell}.$$

Using Theorem 17.1 in [6], which is the function field version of the Wiener-Ikehara Tauberian Theorem, we get that

$$\sum_{\deg F = d_2} b(F) = \frac{K}{\zeta_q(2)} \left(\frac{q+1}{q+2}\right)^{\ell} q^{d_2} + O_q(q^{\varepsilon d_2}). \tag{4.8}$$

We remark that it is important for Theorem 1.3 and Corollary 1.4 to get an error term which is independent of q. From the proof of Theorem 17.1 in [6], one sees that the hidden constant in the error term of (4.8) is bounded by

$$\max_{|q^{-s}| = q^{-\varepsilon}} |H(s)| \left| \left(1 + \frac{1}{q^{s-1}(q+1)}\right)^{-\ell} \right| \ll \left(1 - q^{-\varepsilon}\right)^{-\ell} = \left(\frac{q^{\varepsilon}}{q^{\varepsilon} - 1}\right)^{\ell} \ll q^{\varepsilon \ell}.$$

Thus we have

$$\sum_{\deg F=d_2} b(F)=\frac{K}{\zeta_q(2)}\left(\frac{q+1}{q+2}\right)^{\ell} q^{d_2}+O\left(q^{\varepsilon(d_2+\ell)}\right). \tag{4.9}$$

Replacing (4.9) in (4.7), we get

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

□

Before we obtain the number of $\mathcal{F}_{(d_1,d_2)}$ that take any set of prescribed (zero or nonzero) values, we first need an intermediary step involving the number of zeros in F_2. We recall that $F\in\mathcal{F}^k_{(d_1,d_2)}$ is the set of monic polynomials $F=F_1F_2^2\in\mathcal{F}_{(d_1,d_2)}$ such that F_2 has exactly k zeros over $\mathbb{F}_q$.

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

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

Proof. The k roots of F_2 must be among the $x_{\ell+1},\dots,x_{\ell+m}$, and the remaining elements of $x_{\ell+1},\dots x_{\ell+m}$ must be roots of F_1. Thus we can write

$$F(x)=\prod_{j=1}^{k}(x-x_{i_j})^2\prod_{v=1}^{m-k}(x-x_{i_v})G(x),$$

with $G(x)\in\mathcal{F}_{(d_1-m+k,d_2-k)}$, $G(x_i)\neq 0$ for $\ell+1\le i\le \ell+m$ and $G(x_i)=a_i\prod_{j=1}^{k}(x_i-x_{i_j})^{-2}\prod_{v=1}^{m-k}(x_i-x_{i_v})^{-1}$ for $1\le i\le\ell$. Thus,

$$\begin{aligned}&\left|\left\{F\in\mathcal{F}^k_{(d_1,d_2)}: F(x_i)=a_i, 1\le i\le \ell+m\right\}\right|\\ &=\sum_{\substack{\{i_1,\dots,i_k\}\\ \subset\{\ell+1,\dots,\ell+m\}}}\ \sum_{\substack{(\alpha_1,\dots,\alpha_m)\\ \in(\mathbb{F}_q^*)^m}}\left|\left\{G\in\mathcal{F}_{(d_1-m+k,d_2-k)}:\ G(x_i)=a_i\prod_{j=1}^{k}(x_i-x_{i_j})^{-2}\prod_{v=1}^{m-k}(x_i-x_{i_v})^{-1},\right.\right.\\ &\qquad\qquad 1\le i\le\ell,\ G(x_{\ell+i})=\alpha_i, 1\le i\le m\}|.\end{aligned}$$

By Proposition 4.3 this equals

$$\binom{m}{k}\frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{1}{q+2}\right)^{m}\left(\frac{q}{(q+2)(q-1)}\right)^{\ell}\left(1+O\left(q^{-(1-\varepsilon)(d_2-k)+\varepsilon q}+q^{-(d_1+k-m)/2+q}\right)\right).$$

□

Corollary 4.5. *Let $x_1, \dots, x_q$ be the elements of $\mathbb{F}_q$, and let $a_1, \dots, a_q \in \mathbb{F}_q$ such that m of the a_i are 0. Then for $\varepsilon > 0$*

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

and

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

Proof. We sum over k in Corollary 4.4.

$$\begin{aligned}&\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ F(x_i) = a_i, \ 1 \le i \le q\right\}\right| \\ &= \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{1}{q+2}\right)^m \left(\frac{q}{(q+2)(q-1)}\right)^{q-m} \sum_{k=0}^{m}\binom{m}{k}\left(1 + O\left(q^{-(1-\varepsilon)(d_2-k)+\varepsilon q} + q^{-(d_1+k-m)/2+q}\right)\right) \\ &= \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{2}{q+2}\right)^m \left(\frac{q}{(q+2)(q-1)}\right)^{q-m} \left(1 + O\left(q^{-(1-\varepsilon)(d_2-m)+\varepsilon q} + q^{-(d_1-m)/2+q}\right)\right).\end{aligned}$$

For the second identity, we divide by (4.6). □

To complete the proof of Theorem 3.1 we note that if $\varepsilon \in \{1, \omega, \omega^2\}$, there are $\frac{q-1}{3}$ elements $\alpha \in \mathbb{F}_q$ such that $\chi_3(\alpha) = \varepsilon$.

5 Moments

In this section, we compute the moments of $\text{Tr}(\text{Frob}_C\,|_{H^1_{\chi_3}})/\sqrt{q+1}$ and prove Theorem 1.3. Our proof follows the same steps as the proof of the equivalent result (for the case of hyperelliptic curves) in [5].

Proof of Theorem 1.3. Working as in Section 3, we first rewrite

$$M_{j,k}(q,(d_1,d_2)) \quad = \quad \frac{1}{\left|\widehat{\mathcal{F}}_{[d_1,d_2]}\right|}\sum_{F \in \widehat{\mathcal{F}}_{[d_1,d_2]}}\left(\frac{\widehat{S}_3(F)}{\sqrt{q+1}}\right)^j \left(\frac{\overline{\widehat{S}_3(F)}}{\sqrt{q+1}}\right)^k.$$

Since every $F \in \widehat{\mathcal{F}}_{[d_1,d_2]}$ can be written uniquely as $F = \alpha G$ for some $\alpha \in \mathbb{F}_q^*$ and $G \in \mathcal{F}_{[d_1,d_2]}$, and

$$\widehat{S}_3(F) = \chi_3(\alpha)\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)}\chi_3(G(x_i)) = \chi_3(\alpha)\widehat{S}_3(G),$$

we have

$$\begin{aligned}M_{j,k}(q,(d_1,d_2)) &= \frac{1}{\left|\widehat{\mathcal{F}}_{[d_1,d_2]}\right|}\sum_{\alpha \in \mathbb{F}_q^*}\chi_3(\alpha)^{j-k}\sum_{F \in \mathcal{F}_{[d_1,d_2]}}\left(\frac{\widehat{S}_3(F)}{\sqrt{q+1}}\right)^j \left(\frac{\overline{\widehat{S}_3(F)}}{\sqrt{q+1}}\right)^k \\ &= \frac{1}{\left|\mathcal{F}_{[d_1,d_2]}\right|}\sum_{F \in \mathcal{F}_{[d_1,d_2]}}\left(\frac{\widehat{S}_3(F)}{\sqrt{q+1}}\right)^j \left(\frac{\overline{\widehat{S}_3(F)}}{\sqrt{q+1}}\right)^k\end{aligned}$$

when $j \equiv k \pmod 3$ and $M_{j,k}(q,(d_1,d_2)) = 0$ when $j \not\equiv k \pmod 3$.

Assume from now on that $j \equiv k \pmod 3$. Then,

$$\begin{aligned} M_{j,k}(q,(d_1,d_2)) &= \frac{(q+1)^{-(j+k)/2}}{\left|\mathcal{F}_{[d_1,d_2]}\right|} \sum_{F\in\mathcal{F}_{[d_1,d_2]}} \left(\sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x))\right)^j \left(\sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \overline{\chi_3(F(x))}\right)^k \\ &= \frac{(q+1)^{-(j+k)/2}}{\left|\mathcal{F}_{[d_1,d_2]}\right|} \sum_{\substack{x_1,\dots,x_j\in\mathbb{P}^1(\mathbb{F}_q)\\ y_1,\dots,y_k\in\mathbb{P}^1(\mathbb{F}_q)}} \sum_{F\in\mathcal{F}_{[d_1,d_2]}} \chi_3(F(x_1)\dots F(x_j))\overline{\chi_3(F(y_1)\dots F(y_k))} \end{aligned}$$

(5.1)

$$= (q+1)^{-(j+k)/2} \sum_{\ell=1}^{j}\sum_{m=1}^{k} d(j,k,\ell,m) \sum_{(\mathbf{x},\mathbf{y},\mathbf{b},\mathbf{c})\in P_{j,k,\ell,m}} \frac{1}{\left|\mathcal{F}_{[d_1,d_2]}\right|} \sum_{F\in\mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{\ell} \chi_3(F(x_i))^{b_i} \prod_{i=1}^{m} \overline{\chi_3(F(y_i))^{c_i}}$$

where

$$\begin{aligned} P_{j,k,\ell,m} &= \Big\{(\mathbf{x},\mathbf{y},\mathbf{b},\mathbf{c}) \,:\, \mathbf{x}=(x_1,\dots,x_\ell)\in\mathbb{P}^1(\mathbb{F}_q)^\ell, x_i\text{'s distinct}, \mathbf{y}=(y_1,\dots,y_m)\in\mathbb{P}^1(\mathbb{F}_q)^m \\ &\qquad y_i\text{'s distinct}, \mathbf{b}=(b_1,\dots,b_\ell)\in\mathbb{Z}_{>0}^\ell, \mathbf{c}=(c_1,\dots,c_m)\in\mathbb{Z}_{>0}^m, \sum_{i=1}^{\ell} b_i = j, \sum_{i=1}^{m} c_i = k\Big\}, \end{aligned}$$

and $d(j,k,\ell,m)$ is a certain combinatorial factor. We do not need exact formulas for the $d(j,k,\ell,m)$, but note that

$$\sum_{\ell=1}^{j}\sum_{m=1}^{k} d(j,k,\ell,m) \sum_{(\mathbf{x},\mathbf{y},\mathbf{b},\mathbf{c})\in P_{j,k,\ell,m}} 1 = (q+1)^{j+k}.$$

We now fix a vector $(\mathbf{x},\mathbf{y},\mathbf{b},\mathbf{c})\in P_{j,k,\ell,m}$, and we compute

$$\frac{1}{\left|\mathcal{F}_{[d_1,d_2]}\right|} \sum_{F\in\mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{\ell} \chi_3(F(x_i))^{b_i} \prod_{i=1}^{m} \overline{\chi_3(F(y_i))^{c_i}}.$$

Suppose that $\{x_1,\dots,x_\ell,y_1,\dots,y_m\} = \{z_1,\dots,z_h\}$, in other words, that $\mathbf{x}$ and $\mathbf{y}$ have $\ell+m-h$ coordinates in common. To simplify the notation, we will denote by f_i the corresponding exponent for z_i which is equal to some b_i, c_i or $b_i - c_i$ depending on whether the value z_i appears in $\{x_1,\dots,x_\ell\}$, $\{y_1,\dots,y_m\}$, or in both sets. We also adopt the convention that f_i could be equal to 0, in which case $\chi_3(F(z_i))^{f_i} = 1$ if $F(z_i)\neq 0$ and $\chi_3(F(z_i))^{f_i} = 0$ if $F(z_i) = 0$. With this notation, we want to compute

(5.2)
$$\frac{1}{\left|\mathcal{F}_{[d_1,d_2]}\right|} \sum_{F\in\mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i}.$$

There are two cases.

Case 1: Suppose that z_t is the point at infinity, for some $1\le t\le h$. Then, only polynomials in $\mathcal{F}_{(d_1,d_2)}$ have a nonzero contribution to (5.2) and $\chi_3(F(z_t))^{f_t} = 1$. This gives that

$$\sum_{F\in\mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} \;=\; \sum_{\substack{a_i\in\mathbb{F}_q^*\\ 1\le i\le h, i\neq t}} \prod_{\substack{i=1\\ i\neq t}}^{h} \chi_3(a_i)^{f_i} \sum_{\substack{F\in\mathcal{F}_{(d_1,d_2)}\\ F(z_i)=a_i, 1\le i\le h, i\neq t}} 1.$$

Suppose that all f_i for $1 \leq i \leq h$ and $i \neq t$ are multiples of 3. Then, using Proposition 4.3, we get

$$\sum_{F \in \mathcal{F}_{(d_1,d_2)}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} = \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{q}{q+2}\right)^{h-1} \left(1 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon(h-1)} + q^{-d_1/2+h-1}\right)\right). \tag{5.3}$$

Suppose that there exists a f_i with $1 \leq i \leq h$ and $i \neq t$ such that f_i is not a multiple of 3. Without loss of generality, suppose that $f_1 \equiv 1 \,(\mathrm{mod}\, 3)$ and $t \neq 1$. Then, using again Proposition 4.3, we get

$$\begin{aligned}
\sum_{F \in \mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} &= \sum_{\substack{a_i \in \mathbb{F}_q^* \\ 1 \leq i \leq h, i \neq t \\ \chi_3(a_1)=1}} \prod_{\substack{i=2 \\ i \neq t}}^{h} \chi_3(a_i)^{f_i} \sum_{\substack{F \in \mathcal{F}_{(d_1,d_2)} \\ F(z_i)=a_i, 1 \leq i \leq h, i \neq t}} 1 \\
&\quad + \omega \sum_{\substack{a_i \in \mathbb{F}_q^* \\ 1 \leq i \leq h, i \neq t \\ \chi_3(a_1)=\omega}} \prod_{\substack{i=2 \\ i \neq t}}^{h} \chi_3(a_i)^{f_i} \sum_{\substack{F \in \mathcal{F}_{(d_1,d_2)} \\ F(z_i)=a_i, 1 \leq i \leq h, i \neq t}} 1 + \omega^2 \sum_{\substack{a_i \in \mathbb{F}_q^* \\ 1 \leq i \leq h, i \neq t \\ \chi_3(a_1)=\omega^2}} \prod_{\substack{i=2 \\ i \neq t}}^{h} \chi_3(a_i)^{f_i} \sum_{\substack{F \in \mathcal{F}_{(d_1,d_2)} \\ F(z_i)=a_i, 1 \leq i \leq h, i \neq t}} 1 \\
&= \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{q}{q+2}\right)^{h-1} \left(0 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon(h-1)} + q^{-d_1/2+h-1}\right)\right). \qquad (5.4)
\end{aligned}$$

We remark that $j \equiv k \,(\mathrm{mod}\, 3)$ and $f_i \equiv 0 \,(\mathrm{mod}\, 3)$ for $1 \leq i \leq h$, $i \neq t$ is equivalent to $f_i \equiv 0 \,(\mathrm{mod}\, 3)$ for $1 \leq i \leq h$.

Using (5.3) and (5.4), and dividing by

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

we get that

$$\begin{aligned}
&\frac{1}{\left|\mathcal{F}_{[d_1,d_2]}\right|} \sum_{F \in \mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} \\
&= \left(\frac{q}{q+2}\right)^{h} \left(\delta(\mathbf{f},h) + O\left(q^{-(1-\varepsilon)d_2+\varepsilon(h-1)} + q^{-d_1/2+h-1}\right)\right), \qquad (5.5)
\end{aligned}$$

where $\delta(\mathbf{f},h) = 1$ if $f_i \equiv 0 \,(\mathrm{mod}\, 3)$ for $1 \leq i \leq h$ and 0 otherwise.

Case 2: Suppose that $z_1, \ldots, z_h \in \mathbb{F}_q$. Then any $F \in \mathcal{F}_{[d_1,d_2]}$ can contribute to (5.2). Repeating the reasoning above, we get

$$\sum_{F \in \mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} = \sum_{\substack{a_i \in \mathbb{F}_q^* \\ 1 \leq i \leq h}} \prod_{i=1}^{h} \chi_3(a_i)^{f_i} \sum_{\substack{F \in \mathcal{F}_{[d_1,d_2]} \\ F(z_i)=a_i, 1 \leq i \leq h}} 1.$$

Suppose that all f_i for $1 \leq i \leq h$ are multiples of 3. Then, using Proposition 4.3, we get

$$\sum_{F \in \mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} = \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2} \left(\frac{q}{q+2}\right)^{h-1} \left(1 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon h} + q^{-d_1/2+h}\right)\right).$$

If not all f_i are multiples of 3, reasoning as in Case 1, we get

$$\sum_{F\in\mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(z_i))^{f_i} = \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{q}{q+2}\right)^{h-1}\left(0+O\left(q^{-(1-\varepsilon)d_2+\varepsilon h}+q^{-d_1/2+h}\right)\right)$$

and

$$\begin{aligned} &\frac{1}{\left|\mathcal{F}_{[d_1,d_2]}\right|}\sum_{F\in\mathcal{F}_{[d_1,d_2]}} \prod_{i=1}^{h} \chi_3(F(x_i))^{f_i} \\ &= \left(\frac{q}{q+2}\right)^{h}\left(\delta(\mathbf{f},h)+O\left(q^{-(1-\varepsilon)d_2+\varepsilon h}+q^{-d_1/2+h}\right)\right). \end{aligned} \tag{5.6}$$

We then have the same result for Case 1 and Case 2, and replacing (5.5) or (5.6) in (5.1), we have

$$\begin{aligned} M_{j,k}(q,(d_1,d_2)) &= \left((q+1)^{-(j+k)/2}\sum_{\ell=1}^{j}\sum_{m=1}^{k} d(j,k,\ell,m) \sum_{\substack{(\mathbf{x},\mathbf{y},\mathbf{b},\mathbf{c})\in P_{j,k,\ell,m}\\ 3\mid f_i}} \left(\frac{q}{q+2}\right)^{h}\right) \\ &\times \left(1+O\left(q^{-(1-\varepsilon)d_2+\varepsilon(j+k)}+q^{-d_1/2+(j+k)}\right)\right), \end{aligned} \tag{5.7}$$

where h and f_i are understood as before.

We now compute the corresponding moment of the normalized sum of the random variables $X_1,\dots,X_{q+1}$, i.e.

$$\begin{aligned} &\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1}X_i\right)^{j}\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1}\overline{X_i}\right)^{k}\right) \\ = &\frac{1}{(q+1)^{(j+k)/2}}\sum_{\ell=1}^{j}\sum_{m=1}^{k} d(j,k,\ell,m)\sum_{(\mathbf{u},\mathbf{v},\mathbf{b},\mathbf{c})\in A_{j,k,\ell,m}} \mathbb{E}\left(X_{u_1}^{b_1}\cdots X_{u_\ell}^{b_\ell}\overline{X_{v_1}}^{c_1}\cdots\overline{X_{v_m}}^{c_m}\right) \end{aligned}$$

where

$$\begin{aligned} A_{j,k,\ell,m} = &\{(\mathbf{u},\mathbf{v},\mathbf{b},\mathbf{c}) \,:\, \mathbf{u}=(u_1,\dots,u_\ell), 1\le u_i\le q+1, u_i\text{'s distinct}, \mathbf{v}=(v_1,\dots,v_m), \\ &1\le v_i\le q+1, v_i\text{'s distinct}, \mathbf{b}=(b_1,\dots,b_\ell)\in\mathbb{Z}_{>0}^{\ell}, \mathbf{c}=(c_1,\dots,c_m)\in\mathbb{Z}_{>0}^{m}, \\ &\left.\sum_{i=1}^{\ell}b_i=j, \sum_{i=1}^{m}c_i=k\right\}. \end{aligned}$$

Since

$$\mathbb{E}(X_i^b\overline{X_i}^c) = \begin{cases} 0 & b\not\equiv c \pmod 3, \\ \dfrac{1}{1+2q^{-1}} & b\equiv c \pmod 3 \end{cases}$$

and $X_1, \ldots, X_{q+1}$ are independent, we get

$$\begin{aligned} & \mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} X_i\right)^j \left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} \overline{X_i}\right)^k\right) \\ (5.8) \qquad = \; & \frac{1}{(q+1)^{(j+k)/2}} \sum_{\ell=1}^{j}\sum_{m=1}^{k} d(j,k,\ell,m) \sum_{\substack{(\mathbf{u},\mathbf{v},\mathbf{b},\mathbf{c})\in A_{j,k,\ell,m} \\ 3\mid f_i}} \left(\frac{q}{q+2}\right)^h . \end{aligned}$$

Since the number of terms in the sums over the sets $P_{j,k,\ell,m}$ such that $3 \mid f_i$ and $A_{j,k,\ell,m}$ such that $3 \mid f_i$ are the same, comparing (5.7) and (5.8), we have

$$\begin{aligned} M_{j,k}(q,(d_1,d_2)) \; &= \; \mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} X_i\right)^j \left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} \overline{X_i}\right)^k\right) \\ & \times \; \left(1 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon(j+k)} + q^{-d_1/2+j+k}\right)\right). \end{aligned}$$

□

Proof of Corollary 1.4. First we study the distribution of the normalized sum of the i.i.d. random variables $(X_1 + \ldots + X_{q+1})/\sqrt{q+1}$ as $q \to \infty$. Since the X_j's take complex values, we first write each of them as $X_j = A_j + \sqrt{-1}B_j$ and identify it with the $\mathbb{R}^2$ vector $\begin{pmatrix} A_j \\ B_j \end{pmatrix}$.

Since $\mathbb{E}(|X_j|^2) = (1+2q^{-1})^{-1}$ and $\mathbb{E}(X_j) = \mathbb{E}(X_j^2) = 0$, we have

$$\mathbb{E}(A_j) = \mathbb{E}(B_j) = \mathbb{E}(A_jB_j) = 0$$

and

$$\mathbb{E}(A_j^2) = \mathbb{E}(B_j^2) = \frac{1}{2}\mathbb{E}(|X_j|^2).$$

The Triangular Central Limit Theorem holds for two-dimensional vector valued random variables as long as the covariance matrix is invertible. Since for us the covariance matrix not only is invertible, but also is diagonal with nonzero diagonal entries, we obtain that

$$\frac{1}{q+1}\sum_{j=1}^{q+1}\begin{pmatrix} A_j \\ B_j \end{pmatrix} \to \mathbf{N}_{\mathbb{R}^2}\left(0, \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}\right),$$

the two-dimensional Gaussian with mean 0 and covariance matrix $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$, whose probability density is given by

$$\frac{1}{\pi}e^{-x^2-y^2}\,dxdy.$$

Note that this measure is invariant under multiplication by -1. Going back to the complex valued random variables, we obtain that, as q approaches infinity, the normalized sum $(X_1+\ldots+X_{q+1})/\sqrt{q+1}$ approaches the complex Gaussian with mean zero and variance one. The probability measure of this Gaussian is given by

$$\frac{1}{\pi}e^{-|z|^2}dz.$$

Theorem 1.3 tells us that, as $q, d_1, d_2 \to \infty$, the moments $M_{j,k}(q,(d_1,d_2))$ approach the moments of the complex Gaussian for all j and k. Since the Gaussian is invariant under the change of sign, the limiting value distribution of $\mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_3}})/\sqrt{q+1}$ is the complex Gaussian distribution with mean 0 and variance 1. □

6 Hyperelliptic curves: the geometric point of view

We now revisit the results of Kurlberg and Rudnick [5] for hyperelliptic curves from the geometric point of view. The results of this section are similar to the results of Section 3 for the case of hyperelliptic curves.

Lemma 6.1. *The number of square-free polynomials of degree d is*

$$\left|\widehat{\mathcal{F}}_d\right| = \begin{cases} q^{d+1}(1-q^{-1})^2 & d \geq 2, \\ q^{d+1}(1-q^{-1}) & d = 0, 1. \end{cases}$$

Proof. This follows from Lemma 2.1 since $\left|\widehat{\mathcal{F}}_d\right| = (q-1)\left|\mathcal{F}_d\right|$. □

Proof of Theorem 1.1. Consider the hyperelliptic curve with affine model

$$C: \quad Y^2 = F(X),$$

where $F \in \widehat{\mathcal{F}}_d$. It has genus g if and only if d is either $2g+1$ or $2g+2$. In terms of the polynomial F, the trace of the Frobenius is equal to

$$-\widehat{S}_2(F) = -\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_2(F(x)),$$

where the value of F at the point at infinity is given by the value of $X^{2g+2}F(1/X)$ at zero. By running over all $F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, one counts each point in the moduli space $\mathcal{H}_g$ exactly $q(q^2-1)$ times. (As usual, a point C in the moduli space is counted with weight $1/|\mathrm{Aut}(C)|$.) With the notation from the introduction,

$$\frac{|\{C \in \mathcal{H}_g : \mathrm{Tr}(\mathrm{Frob}_C) = -s\}|'}{|\mathcal{H}_g|'} = \frac{\left|\left\{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \widehat{S}_2(F) = s\right\}\right|}{\left|\widehat{\mathcal{F}}_{2g+1}\right| + \left|\widehat{\mathcal{F}}_{2g+2}\right|}$$

Fix $x_1, \dots, x_{q+1}$ an enumeration of the points on $\mathbb{P}^1(\mathbb{F}_q)$ such that x_{q+1} denotes the point at infinity. Then

$$\chi_2(F(x_{q+1})) = \begin{cases} 0 & F \in \widehat{\mathcal{F}}_{2g+1}, \\ 1 & F \in \widehat{\mathcal{F}}_{2g+2}, \text{ leading coefficient is a square in } \mathbb{F}_q, \\ -1 & F \in \widehat{\mathcal{F}}_{2g+2}, \text{ leading coefficient is not a square in } \mathbb{F}_q. \end{cases}$$

Pick $(\varepsilon_1, \dots, \varepsilon_{q+1}) \in \{0, \pm 1\}^{q+1}$. Denote m the number of zeros in this $(q+1)$-tuple. We need to evaluate the probability that the character χ_2 takes exactly these values as F ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$. Namely we will show that the results of [5] imply that

$$\begin{aligned} &\frac{\left|\left\{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_2(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right|}{\left|\widehat{\mathcal{F}}_{2g+1}\right| + \left|\widehat{\mathcal{F}}_{2g+2}\right|} \\ &= \frac{2^{m-q-1} q^{-m}}{(1+q^{-1})^{q+1}} \left(1 + O\left(q^{m/2+q-g-1}\right)\right). \end{aligned} \tag{6.1}$$

Case 1: $\varepsilon_{q+1} = 0$. The numbers of zeros among $\varepsilon_1, \dots, \varepsilon_q$ is now $m-1$. Since there are no polynomials in $\widehat{\mathcal{F}}_{2g+2}$ with $\chi_2(F(x_{q+1})) = 0$, only $\widehat{\mathcal{F}}_{2g+1}$ contributes. There are $q-1$ possibilities for the leading coefficient of such a polynomial and thus

$$\begin{aligned} &\left|\left\{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_2(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right| \\ &= \sum_{\alpha \in \mathbb{F}_q^*} \left|\left\{F \in \mathcal{F}_{2g+1} : \chi_2(F(x_i)) = \varepsilon_i \chi_2(\alpha), 1 \le i \le q\right\}\right|. \end{aligned}$$

Taking into account that there are $\frac{q-1}{2}$ squares in $\mathbb{F}_q$ and the same number of non-squares, and using Lemma 2.4 the above expression can be written as

$$\begin{aligned} &(q-1)\left(\frac{q-1}{2}\right)^{q-m+1} \frac{(1-q^{-1})^m q^{2g+1-q}}{(1-q^{-2})^q} \left(1 + O\left(q^{m/2+q-g-1}\right)\right) \\ &\qquad = \frac{2^{m-1-q}(1-q^{-1})^{q+2} q^{2g+3-m}}{(1-q^{-2})^q} \left(1 + O\left(q^{m/2+q-g-1}\right)\right). \end{aligned} \tag{6.2}$$

With Lemma 6.1, we compute

$$\left|\widehat{\mathcal{F}}_{2g+1}\right| + \left|\widehat{\mathcal{F}}_{2g+2}\right| = q^{2g+3}(1-q^{-1})(1-q^{-2}), \tag{6.3}$$

and dividing (6.2) by (6.3) we get (6.1).

Case 2: $\varepsilon_{q+1} = \pm 1$.

This is the complementary situation, namely there are m zeros among $\varepsilon_1, \dots, \varepsilon_q$ and only $\widehat{\mathcal{F}}_{2g+2}$ contributes. By the same argument as before, and taking into account that there are $\frac{q-1}{2}$ leading coefficients that would give $\varepsilon_{q+1} = 1$ and the same number that would yield $\varepsilon_{q+1} = -1$,

$$\begin{aligned} &\left|\left\{F \in \widehat{\mathcal{F}}_{2g+2} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_2(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\right\}\right| \\ &= \frac{q-1}{2} \left|\left\{F \in \mathcal{F}_{2g+2} : \chi_2(F(x_i)) = \varepsilon_i \varepsilon_{q+1}, 1 \le i \le q\right\}\right|. \end{aligned}$$

By Lemma 2.4, and by taking into account the number of squares and non-squares in $\mathbb{F}_q$ this equals

$$\begin{aligned} &\left(\frac{q-1}{2}\right)^{q+1-m} \frac{(1-q^{-1})^{m+1} q^{2g+2-q}}{(1-q^{-2})^q} \left(1 + O\left(q^{m/2+q-g-1}\right)\right) \\ &\qquad = \frac{2^{m-1-q}(1-q^{-1})^{q+2} q^{2g+3-m}}{(1-q^{-2})^q} \left(1 + O\left(q^{m/2+q-g-1}\right)\right), \end{aligned}$$

which is the same as (6.2). The formula (6.1) follows as before.

On the other hand for $X_1, \dots, X_{q+1}$ as in Theorem 1.1

$$\mathrm{Prob}\,(X_i = \varepsilon_i, 1 \le i \le q+1) = \frac{2^{m-q-1} q^{-m}}{(1+q^{-1})^{q+1}} \tag{6.4}$$

and the theorem follows by summing (6.1) and (6.4) over all $(q+1)$-tuples $(\varepsilon_1, \dots, \varepsilon_{q+1})$ such that $\varepsilon_1 + \cdots + \varepsilon_{q+1} = s$ as done at the end of Section 3.

□

We remark that the probability of hitting a certain $(q+1)$-tuple does not depend on the entry at the point we designated as the point at infinity. Therefore that point behaves the same as the affine points, which is exactly what one would expect from a geometric standpoint.

6.1 Moments

We want to compute the moments of $\mathrm{Tr}(\mathrm{Frob}_C)/\sqrt{q+1}$. Namely, denote the k-th moment by

$$M_k(q,g) = \frac{1}{|\mathcal{H}_g|'} \sum_{C \in \mathcal{H}_g}{}' \left(\frac{\mathrm{Tr}(\mathrm{Frob}_C)}{\sqrt{q+1}} \right)^k .$$

For a given curve $C \in \mathcal{H}_g$, its quadratic twist C' also has genus g and they are not isomorphic over $\mathbb{F}_q$. So both $\mathrm{Tr}(\mathrm{Frob}_C)$ and $\mathrm{Tr}(\mathrm{Frob}_{C'}) = -\mathrm{Tr}(\mathrm{Frob}_C)$ appear in our sum. This implies that for k odd we have $M_k(q,g) = 0$.

Theorem 6.2. *If g, q both tend to infinity, then the moments of $\mathrm{Tr}(\mathrm{Frob}_C)/\sqrt{q+1}$, as C runs over the moduli space $\mathcal{H}_g$ of hyperelliptic curves of genus g, are asymptotically Gaussian with mean 0 and variance 1. In particular the limiting value distribution is a standard Gaussian.*

As before, by looking at curves of the form

$$Y^2 = F(X)$$

as F ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$ we run over each point in $\mathcal{H}_g$ exactly $q(q^2-1)$ times. The trace of Frobenius of the curve with the above affine model is given by $\widehat{S}_2(F)$. As a result, for k even, we can write the k-th moment as

$$\begin{aligned} M_k(q,g) &= (-1)^k \frac{1}{\left|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}\right|} \sum_{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}} \left(\frac{\widehat{S}_2(F)}{\sqrt{q+1}} \right)^k \\ &= \frac{(q+1)^{-k/2}}{\left|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}\right|} \sum_{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}} \left(\sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_2(F(x)) \right)^k \\ &= \frac{1}{(q+1)^{k/2}} \sum_{x_1, \dots, x_k \in \mathbb{P}^1(\mathbb{F}_q)} \frac{1}{\left|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}\right|} \sum_{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}} \chi_2(F(x_1) \cdots F(x_k)) \\ &= \frac{1}{(q+1)^{k/2}} \sum_{\ell=1}^{k} c(k,\ell) \sum_{(\mathbf{x},\mathbf{b}) \in P_{k,\ell}} \frac{1}{\left|\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}\right|} \sum_{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}} \chi_2 \left(\prod_{i=1}^{l} F(x_i)^{b_i} \right), \end{aligned}$$

where

$$P_{k,\ell} = \left\{ (\mathbf{x}, \mathbf{b}) : \mathbf{x} = (x_1, \dots, x_\ell) \in \mathbb{P}^1(\mathbb{F}_q)^\ell, x_i\text{'s distinct }, \mathbf{b} = (b_1, \dots, b_\ell) \in \mathbb{Z}_{>0}^\ell, \sum_{i=1}^{l} b_i = k \right\},$$

and $c(k,\ell)$ is a certain combinatorial factor. We do not need exact formulas for the $c(k,\ell)$, but note that

$$\sum_{l=1}^{k} c(k,\ell) \sum_{(\mathbf{x},\mathbf{b}) \in P_{k,\ell}} 1 = (q+1)^k. \tag{6.5}$$

Fix a vector $(\mathbf{x}, \mathbf{b}) \in P_{k,\ell}$. There are two cases.

Case 1: x_j is the point at infinity, for some $1 \le j \le \ell$.

Then only polynomials in $\widehat{\mathcal{F}}_{2g+2}$ have a nonzero contribution and we can write

$$\sum_{F \in \widehat{\mathcal{F}}_{2g+2}} \chi_2 \left(\prod_{i=1}^{\ell} F(x_i)^{b_i} \right) = \sum_{a_j \in \mathbb{F}_q^*} \chi_2(a_j)^{b_j} \sum_{G \in \mathcal{F}_{2g+2}} \prod_{i \neq j} \chi_2(G(x_i))^{b_i}.$$

Note that G ranges over *monic* polynomials of degree $2g+2$ and we can write the above expression becomes

$$\sum_{a_j \in \mathbb{F}_q^*} \chi_2(a_j)^{b_j} \sum_{G \in \mathcal{F}_{2g+2}} \prod_{i \neq j} \chi_2(G(x_i))^{b_i} = \sum_{\substack{a_i \in \mathbb{F}_q^* \\ 1 \le i \le l}} \sum_{\substack{G \in \mathcal{F}_{2g+2} \\ G(x_i) = a_i, i \neq j}} \prod_{i=1}^{\ell} \chi_2(a_i)^{b_i}.$$

Thus, by Lemma 2.3, the contribution to the moment of such a term is

$$\begin{cases} O\left(q^{1+\ell+g}\right) & \text{if any of the } b_i\text{'s is odd,} \\ \dfrac{q^{2g+3}(1-q^{-1})^{\ell+1}}{(1-q^{-2})^{\ell-1}} + O\left(q^{1+\ell+g}\right) & \text{if all the } b_i\text{'s are even.} \end{cases}$$

Case 2: $x_1, \dots, x_\ell \in \mathbb{F}_q$.

Then both $\widehat{\mathcal{F}}_{2g+1}$ and $\widehat{\mathcal{F}}_{2g+2}$ contribute. Repeating the reasoning from before, the contribution is

$$O\left(q^{3/2+\ell+g}\right)$$

unless all the b_i's are even. In which case

$$\sum_{F \in \widehat{\mathcal{F}}_{2g+1}} \chi_2 \left(\prod_{i=1}^{\ell} F(x_i)^{b_i} \right) = \frac{q^{2g+2}(1-q^{-1})^{\ell+2}}{(1-q^{-2})^{\ell}} + O\left(q^{1+\ell+g}\right)$$

and

$$\sum_{F \in \widehat{\mathcal{F}}_{2g+2}} \chi_2 \left(\prod_{i=1}^{\ell} F(x_i)^{b_i} \right) = \frac{q^{2g+3}(1-q^{-1})^{\ell+2}}{(1-q^{-2})^{\ell}} + O\left(q^{3/2+\ell+g}\right).$$

Adding them up, we get a total contribution of

$$\frac{q^{2g+3}(1-q^{-1})^{\ell+1}}{(1-q^{-2})^{\ell-1}} + O\left(q^{3/2+\ell+g}\right).$$

In both cases, the main term is the same, and dividing by

$$\left|\widehat{\mathcal{F}}_{2g+1}\right| + \left|\widehat{\mathcal{F}}_{2g+2}\right| = q^{2g+3}(1-q^{-1})(1-q^{-2})$$

we obtain that

$$M_k(q,g) = \frac{1}{(q+1)^{k/2}} \sum_{l=1}^{k} c(k,\ell) \sum_{\substack{(\mathbf{x},\mathbf{b})\in P_{k,\ell} \\ b_i \text{ even}}} (1+q^{-1})^{-\ell} + O((q+1)^{-k/2}(q+1)^k q^{-3/2+k-g}),$$

where the error term is estimated using (6.5).

On the other hand, the corresponding moment of the normalized sum of our random variables is

$$\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} X_i\right)^k\right) = \frac{1}{(q+1)^{k/2}} \sum_{\ell=1}^{k} c(k,\ell) \sum_{(\mathbf{i},\mathbf{b})\in A_{k,\ell}} \mathbb{E}\left(X_{i_1}^{b_1}\cdots X_{i_\ell}^{b_\ell}\right),$$

where

$$A_{k,\ell} = \left\{(\mathbf{i},\mathbf{b}); \mathbf{i} = (i_1,\dots,i_\ell), 1 \le i_j \le q+1, i_j\text{'s distinct }, \mathbf{b} = (b_1,\dots,b_\ell), \sum_{j=1}^{\ell} b_j = k\right\}$$

is clearly isomorphic to $P_{k,\ell}$.

Since

$$\mathbb{E}(X_i^b) = \begin{cases} 0 & b \text{ odd} \\ \dfrac{1}{1+q^{-1}} & b \text{ even} \end{cases}$$

and $X_1,\dots,X_{q+1}$ are independent, we get

$$M_k(q,g) = \mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1} X_i\right)^k\right) + O\left(q^{(3k-3-2g)/2}\right). \tag{6.6}$$

Since the moments of a sum of bounded i.i.d. random variables converge to the Gaussian moments [2, Section 30], it follows that, as $q,g\to\infty$, $M_k(q,g)$ agrees with Gaussian moments for all k. Hence the limiting value distribution of $\mathrm{Tr}(\mathrm{Frob}_C)/\sqrt{q+1}$ is a standard Gaussian distribution with mean 0 and variance 1.

7 General case

In this section we briefly sketch the proof of our results for the case of curves C that have a cyclic p-to-1 map to $\mathbb{P}^1(\mathbb{F}_q)$, where $q \equiv 1 \pmod p$ and p is an odd prime. As we mentioned in the introduction, the proof of the general case follows from the same techniques as in the cyclic trigonal case.

Denote by $\mathcal{F}_{(d_1,\dots,d_r)}$ the set of polynomials of the form $F(X) = F_1(X)F_2^2(X)\cdots F_r^r(X)$ with $F_1,\dots,F_r$ monic, square-free and pairwise coprime polynomials of degrees $d_1,\dots,d_r$, respectively. We note that when $r = p-1$ this is the set of monic p-th power-free polynomials. For fixed $x_1,\dots,x_\ell$ distinct points in $\mathbb{F}_q$ and $a_1,\dots,a_\ell \in \mathbb{F}_q^*$,

$$\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_r)} : F(x_i) = a_i\right\}\right| = \frac{q^{d_1-\ell}}{\zeta_q(2)(1-q^{-2})^\ell} \sum_{\deg F_2 = d_2} \cdots \sum_{\deg F_r = d_r} b(F_2\dots F_r) + O\left(q^{d_1/2+d_2+\dots+d_r}\right),$$

where $b(F)$ is the quantity defined in (4.7). Here we used the fact that $b(F)$ is multiplicative and $b(F_1 \dots F_r) = 0$ if the F_i are not relatively prime in pairs.

Using the Tauberian theorem and an induction argument on r, we obtain the following result which mirrors Proposition 4.3.

Proposition 7.1. *Fix $0 \leq \ell \leq q$, $x_1, \dots, x_\ell$ distinct points in $\mathbb{F}_q$ and $a_1, \dots, a_l$ nonzero elements of $\mathbb{F}_q$. For each $r \geq 2$,*

$$\begin{aligned}\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_r)} : F(x_i) = a_i, 1 \leq i \leq \ell\right\}\right| &= \frac{L_{r-1} q^{d_1+\dots+d_r}}{\zeta_q(2)^r} \left(\frac{q}{(q+r)(q-1)}\right)^\ell \\ &\times \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_r+\ell)}\left(q^{-d_2} + \dots + q^{-d_r}\right) + q^{-d_1/2+\ell}\right)\right),\end{aligned}$$

where

$$L_{r-1} = \prod_{j=1}^{r-1} \prod_P \left(1 - \frac{j}{(|P|+1)(|P|+j)}\right).$$

Denote

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

Proceeding as in the proof of Corollary 4.4, we obtain the following.

Corollary 7.2. *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 $\varepsilon > 0$,*

$$\begin{aligned}&|\{F \in \mathcal{F}^{(k_1,\dots,k_{p-1})}_{(d_1,\dots,d_{p-1})} : F(x_i) = a_i, 1 \leq i \leq q\}| \\ &= \binom{m}{k_1, \dots, k_{p-1}} \frac{L_{p-2} q^{d_1+\dots+d_{p-1}}}{\zeta_q(2)^{p-1}} \left(\frac{1}{q+p-1}\right)^m \left(\frac{q}{(q+p-1)(q-1)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_{p-1}+k_1-m+q)}\left(q^{-(d_2-k_2)} + \dots + q^{-(d_{p-1}-k_{p-1})}\right) + q^{-(d_1-k_1)/2+q}\right)\right).\end{aligned}$$

Summing over all such possible partitions of m, just as we did in the proof of Corollary 4.5, and using the Multinomial Theorem, we obtain that

$$\begin{aligned}&\frac{\left|\left\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : F(x_i) = a_i, 1 \leq i \leq q\right\}\right|}{\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right|} = \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{(q+p-1)(q-1)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_{p-1}+q)+(1-\varepsilon)m}\left(q^{-d_2} + \dots + q^{-d_{p-1}}\right) + q^{-(d_1-m)/2+q}\right)\right).\end{aligned}$$

Taking into account the number of elements in each p-power residue class in $\mathbb{F}_q$, we arrive at the following result, which corresponds to Theorem 3.1 from the cyclic trigonal case.

Theorem 7.3. *Choose $x_1, \dots, x_q$ an enumeration of the points of $\mathbb{F}_q$. Fix $\varepsilon_1, \dots, \varepsilon_q \in \mathbb{C}$, such that m of them are 0 and the rest are p-th roots of unity. Then for any $\varepsilon > 0$,*

$$\begin{aligned}&\frac{\left|\{F \in \mathcal{F}_{(d_1,\dots,d_{p-1})} : \chi_p(F(x_i)) = \varepsilon_i, 1 \leq i \leq q\}\right|}{\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right|} = \left(\frac{p-1}{q+p-1}\right)^m \left(\frac{q}{p(q+p-1)}\right)^{q-m} \\ &\times \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_{p-1}+q)+(1-\varepsilon)m}\left(q^{-d_2} + \dots + q^{-d_{p-1}}\right) + q^{-(d_1-m)/2+q}\right)\right).\end{aligned}$$

Proceeding as in Section 3, one can prove that the point at infinity behaves like any other point of $\mathbb{P}^1(\mathbb{F}_q)$. For a curve C with affine model $Y^p = F(X)$, $F = F_1 F_2^2 \dots F_{p-1}^{p-1}$ the number of branch points is $R = d_1 + \dots + d_{p-1}$ if $\deg F \equiv 0 \pmod p$ or $R = d_1 + \dots + d_{p-1} + 1$ otherwise. The genus of such a curve is always $g = (p-1)(R-2)/2$. The moduli space breaks into a disjoint union of irreducible components

$$\mathcal{H}_g = \bigcup \mathcal{H}^{(d_1,\dots,d_{p-1})}.$$

Here the components are indexed by tuples $(d_1, \dots, d_{p-1})$ with the properties that $(p-1)(d_1 + \dots + d_{p-1} - 2) = 2g$ and $d_1 + 2d_2 + \dots + (p-1)d_{p-1} \equiv 0 \pmod p$, taking into account the fact that two such tuples give the same component under certain equivalence relations (in the case $p = 3$ this amounts to switching d_1 and d_2). We also remark that, just as in the cyclic trigonal case, for a curve C of genus $g > (p-1)^2$, the cyclic p-to-1 map to $\mathbb{P}^1(\mathbb{F}_q)$ is uniquely determined up to isomorphisms of $\mathbb{P}^1(\mathbb{F}_q)$. So when the genus passes this threshold, counting all possible affine models for curves of a fixed inertia type (with the appropriate weights) will count each curve with the same multiplicity. Namely,

$$\left|\mathcal{H}^{(d_1,\dots,d_{p-1})}\right|' = \frac{1}{q(q^2-1)} \left(\left|\mathcal{F}_{(d_1,\dots,d_{p-1})}\right| + \left|\mathcal{F}_{(d_1-1,\dots,d_{p-1})}\right| + \dots + \left|\mathcal{F}_{(d_1,\dots,d_{p-1}-1)}\right| \right).$$

Similar to the cyclic trigonal curves, the curves C are endowed with an automorphism of order p that splits the first cohomology group H^1 into subspaces $H^1_{\chi_p}, H^1_{\chi_p^2}, \dots, H^1_{\chi_p^{p-1}}$ on which the automorphism acts by multiplication by $\chi_p, \dots, \chi_p^{p-1}$ respectively (for a choice of an order p character χ_p). Since this automorphism commutes with the action of Frobenius, it suffices to study the trace of Frobenius on one of these subspaces, say $H^1_{\chi_p}$. Moving to another subspace amounts to a new choice of χ_p.

The trace of Frobenius of the curve C with affine model

$$C : Y^p = F(X)$$

on each subspace of H^1 is then given by

$$\mathrm{Tr}(\mathrm{Frob}_C \mid_{H^1_{\chi_p^j}}) = - \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_p^j(F(x)) = -\widehat{S}_j(F) \qquad 1 \le j \le p-1$$

where the value of F at the point at infinity is the value at zero of $X^{\deg F} F(1/X)$ if $\deg F \equiv 0 \pmod p$ and 0 otherwise. The number of points of C over $\mathbb{F}_q$ (including the points at infinity) is then

$$q + 1 + \left(\widehat{S}_1(F) + \dots + \widehat{S}_{p-1}(F) \right).$$

Following the argument from the proof of Theorem 1.2, one can show that the projective trace is distributed just like the affine trace.

Theorem 7.4. *Let $X_1, \dots, X_{q+1}$ be complex i.i.d. random variables taking the value 0 with probability $(p-1)/(q+p-1)$ and each of the p-th roots of unity in $\mathbb{C}$ with probability $q/(p(q+p-1))$. As $d_1, \dots, d_{p-1} \to \infty$,*

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,\dots,d_{p-1})} : \mathrm{Tr}(\mathrm{Frob}_C \mid_{H^1_{\chi_p}}) = -s\right\}\right|'}{\left|\mathcal{H}^{(d_1,\dots,d_{p-1})}\right|'}$$
$$= \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right) \left(1 + O\left(q^{\varepsilon(d_2+\dots+d_{p-1})+q}\left(q^{-d_2} + \dots + q^{-d_{p-1}}\right) + q^{-(d_1-3q)/2}\right)\right)$$

for any $s \in \mathbb{C}$, $|s| \le q+1$ and $0 > \varepsilon > 1$.

Note that our random variables are complex-valued and have the property that

$$\mathbb{E}(X_i^b \overline{X_i}^c) = \begin{cases} 0 & b \not\equiv c \,(\operatorname{mod} p), \\ \dfrac{q}{q+p-1} & b \equiv c \,(\operatorname{mod} p). \end{cases}$$

Computing the mixed moments of the trace, one sees that they approach the moments of the normalized sum of random variables $(X_1 + \ldots + X_{q+1})/\sqrt{q+1}$. Namely, for each $j, k \geq 0$, denote

$$M_{j,k}(q, (d_1, \ldots, d_{p-1})) = \frac{1}{|\mathcal{H}^{(d_1,\ldots,d_{p-1})}|'} \sum_{C \in \mathcal{H}^{(d_1,\ldots,d_{p-1})}} \left(\frac{-\operatorname{Tr}(\operatorname{Frob}_C |_{H^1_{\chi_p}})}{\sqrt{q+1}} \right)^j \left(\frac{-\operatorname{Tr}(\operatorname{Frob}_C |_{H^1_{\overline{\chi}_p}})}{\sqrt{q+1}} \right)^k.$$

A similar computation to the one in the proof of Theorem 1.3 yields

$$\begin{aligned} M_{j,k}(q, (d_1, \ldots, d_{p-1})) &= \mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}} \sum_{i=1}^{q+1} X_i \right)^j \left(\frac{1}{\sqrt{q+1}} \sum_{i=1}^{q+1} \overline{X_i} \right)^k \right) \\ &\times \left(1 + O\left(q^{\varepsilon(d_2+\cdots+d_{p-1}+j+k)} \left(q^{-d_2} + \cdots + q^{-d_{p-1}} \right) + q^{-d_1/2+j+k} \right) \right). \end{aligned} \tag{7.1}$$

Writing each random variable X_j in terms of its real and imaginary part, $X_j = A_j + \sqrt{-1}B_j$, we obtain that $\mathbb{E}(A_j) = \mathbb{E}(B_j) = 0$ and $\mathbb{E}(A_j^2) = \mathbb{E}(B_j^2) = q/(2(q+p-1))$. Applying the Triangular Central Limit Theorem, we obtain, by the same arguments as in the proof of Corollary 1.4, that the limiting distribution of the normalized $(X_1 + \ldots + X_{q+1})/\sqrt{q+1}$ is a complex Gaussian with mean 0 and variance 1. Together with (7.1) this fact implies the following result.

Theorem 7.5. *As $q, d_1, \ldots, d_{p-1} \to \infty$,*

$$\frac{1}{\sqrt{q+1}} \operatorname{Tr}(\operatorname{Frob}_C |_{H^1_{\chi_p}})$$

has a complex Gaussian distribution with mean 0 and variance 1 as C varies in $\mathcal{H}^{(d_1,\ldots,d_{p-1})}(\mathbb{F}_q)$.

8 Heuristic

We give in this section a heuristic which explains the probabilities occurring in Theorems 1.1, 1.2 and 7.4.

8.1 Heuristic for hyperelliptic curves

We first give a heuristic explaining the results of Lemma 2.4 (Proposition 6 in [5]). To model square-free polynomials, we consider polynomials with no double root in $\mathbb{F}_q$. That is, fix points $x_1, \ldots, x_{\ell+m}$ and count the monic polynomials of degree d that are not divisible by $(X - x_i)^2$ for any $1 \leq i \leq \ell+m$. Assume that $d \gg \ell+m$. Then by the Chinese Remainder Theorem, the number of such polynomials is the number of monic polynomials of degree d multiplied by a factor of $(1 - q^{-2})$ for each condition. There are $\ell + m$ conditions, so there are $q^d(1 - q^{-2})^{\ell+m}$ polynomials of degree d which are not divisible by $(X - x_i)^2$

for any $1 \leq i \leq \ell + m$. We now fix $a_1, \dots, a_\ell \in \mathbb{F}_q^*$ and $a_{\ell+1}, \dots, a_{\ell+m} = 0$, and count the number of polynomials defined above satisfying $F(x_i) = a_i$. For $i \geq \ell + 1$, we want $F(X) \equiv 0 \bmod (X - x_i)$, and there are $(q-1)$ such residues modulo $(X - x_i)^2$ among the $q^2 - 1$ residues not congruent to 0 modulo $(X - x_i)^2$. For $i \leq \ell$, we want $F(X) \equiv a_i \bmod (X - x_i)$, and there are q such residues modulo $(X - x_i)^2$ among the $q^2 - 1$ residues not congruent to 0 modulo $(X - x_i)^2$. Using the Chinese Remainder Theorem, this shows that

$$\frac{\left|\left\{F \in \mathbb{F}_q[X] : \deg F = d, F \text{ monic}, (X - x_i)^2 \nmid F, F(x_i) = a_i\right\}\right|}{\left|\left\{F \in \mathbb{F}_q[X] : \deg F = d, F \text{ monic}, (X - x_i)^2 \nmid F\right\}\right|}$$

$$= \left(\frac{q-1}{q^2-1}\right)^m \left(\frac{q}{q^2-1}\right)^\ell = \frac{(1-q^{-1})^m q^{-(\ell+m)}}{(1-q^{-2})^{\ell+m}},$$

which is the main term in Lemma 2.4. Then in some way, imposing the square-free condition cuts uniformly across these sets, and being square-free is an event independent of imposing values at a finite number of points. The error term occurs because if one interprets the square-free condition as a collection of conditions indexed by irreducible polynomials, these individual conditions are only jointly independent in small numbers.

We now illustrate how the above heuristic also explains the probabilities of Theorem 1.1. This is very similar to the computation of Section 6. As there, we now use the set of (not necessarily monic) polynomials of degree $2g+1$ and $2g+2$. There are $q^{2g+3}(1-q^{-2})^{\ell+m+1}$ such polynomials $F \in \mathbb{F}_q[X]$ with no double zeros at the points $x_1, \dots, x_{\ell+m}$. Denoting the point at infinity by $x_{\ell+m+1}$, we have to compute

$$\frac{\left|\left\{F \in \mathbb{F}_q[X] : \begin{array}{l} 2g+1 \leq \deg F \leq 2g+2, (X - x_i)^2 \nmid F, 1 \leq i \leq \ell + m \\ F(x_i) = a_i, 1 \leq i \leq \ell + m + 1 \end{array}\right\}\right|}{\left|\left\{F \in \mathbb{F}_q[X] : 2g+1 \leq \deg F \leq 2g+2, (X - x_i)^2 \nmid F, 1 \leq i \leq \ell + m\right\}\right|}. \tag{8.1}$$

If $F(x_{\ell+m+1}) = 0$, which is equivalent to $\deg(F) = 2g+1$, then the numerator of (8.1) is equal to $q^{2g+1-2(\ell+m)}(q-1)q^\ell(q-1)^m$. Similarly, if $F(x_{\ell+m+1}) \neq 0$, which is equivalent to $\deg(F) = 2g+2$, the numerator of (8.1) is equal to $q^{2g+2-2(\ell+m)}q^\ell(q-1)^m$. This shows that (8.1) is equal to

$$\begin{cases} \left(\frac{1}{q+1}\right)^{m+1} \left(\frac{q}{q^2-1}\right)^\ell & \text{if } F(x_{\ell+m+1}) = 0, \\ \left(\frac{1}{q+1}\right)^m \left(\frac{q}{q^2-1}\right)^{\ell+1} & \text{if } F(x_{\ell+m+1}) \neq 0. \end{cases}$$

This is the geometric version of the main term in Lemma 2.4. To see that, let $x_1, \dots, x_{q+1}$ be the points of $\mathbb{P}^1(\mathbb{F}_q)$, let $a_1, \dots, a_{q+1} \in \mathbb{F}_q$ and let m be the number of zeros among the values $a_1, \dots, a_{q+1}$. Then (8.1) writes as

$$\left(\frac{1}{q+1}\right)^m \left(\frac{q}{q^2-1}\right)^{q+1-m} = \frac{(1-q^{-1})^m q^{-(q+1)}}{(1-q^{-2})^{q+1}},$$

and the probabilities of Theorem 1.1 follow with the usual argument.

8.2 Heuristic for general case

The same heuristic can be used to explain the result one gets for curves C that have a cyclic p-to-1 map to $\mathbb{P}^1(\mathbb{F}_q)$,

Lemma 8.1. *The number of $(p-1)$-tuples $(F_1, \dots, F_{p-1})$ of nonzero residues modulo $(X-t)^2$ such that $(X-t)$ does not divide F_i and F_j for any $i \neq j$ is $q^{p-2}(q-1)^{p-1}(q+p-1)$.*

Proof. Denote by $\mathcal{S}_t$ the set of such tuples. The total number of $(p-1)$-tuples of nonzero residues modulo $(X-t)^2$ is $(q^2-1)^{p-1}$. For each integer $1 \leq k \leq p-1$, denote

$$\mathcal{B}_k = \left\{(F_1, \dots, F_{p-1}) : (X-t) \text{ divides exactly } k \text{ of the } F_i,\ (X-t)^2 \text{ does not divide any } F_i\right\}.$$

Then

$$|\mathcal{S}_t| = (q^2-1)^{p-1} - \sum_{k=2}^{p-1} |\mathcal{B}_k|.$$

It is easy to see that $|\mathcal{B}_k| = \binom{p-1}{k}(q-1)^k(q^2-q)^{p-1-k}$, and the lemma follows by using the binomial formula. □

The number of $(p-1)$-tuples in $\mathcal{S}_t$ such that $F = F_1F_2^2 \dots F_{p-1}^{p-1}$ takes the value $a \in \mathbb{F}_q^*$ is equal to $q^{p-1}(q-1)^{p-2}$. It follows that the number of $(p-1)$-tuples in $\mathcal{S}_t$ such that $F = F_1F_2^2 \dots F_{p-1}^{p-1}$ takes the value 0 is equal to $|\mathcal{S}_t| - q^{p-1}(q-1)^{p-1} = (p-1)q^{p-2}(q-1)^{p-1}$. Therefore the probability that $F = F_1F_2^2 \dots F_{p-1}^{p-1}$ takes a value $a \in \mathbb{F}_q$ at a point t is

$$\begin{cases} \dfrac{p-1}{q+p-1} & \text{if } a = 0, \\[2ex] \dfrac{q}{(q-1)(q+p-1)} & \text{if } a \in \mathbb{F}_q^*. \end{cases} \tag{8.2}$$

This explains the result of Corollary 4.5 and Theorem 7.3.

Finally, for Theorems 1.2 and 7.4, we note that taking the point at infinity into consideration works just like in Section 8.1 and we get that for any enumeration $x_0, \dots, x_q$ of $\mathbb{P}^1(\mathbb{F}_q)$ and any $\varepsilon_0, \dots, \varepsilon_q$ that are either zero or p-th roots of unity,

$$\operatorname{Prob}\left(\chi(F(x_i)) = \varepsilon_i, 0 \leq i \leq q\right) = \operatorname{Prob}\left(X_i = \varepsilon_i, 0 \leq i \leq q\right),$$

where $X_0, \dots, X_q$ are i.i.d. random variables taking the value 0 with probability $(p-1)/(q+p-1)$ and each root of unity with probability $q/(p(q+p-1))$.

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 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] Achter, Jeffrey D. and Pries, Rachel. "The integral monodromy of hyperelliptic and trielliptic curves." *Math. Ann.* 338 (2007), no. 1, 187–206.

[2] Billingsley, Patrick. *Probability and measure*, third ed., Wiley Series in Probability and Mathematical Statistics, John Wiley and Sons Inc., New York (1995).

[3] Katz, Nicholas M. "Affine Cohomological Transforms, Perversity, and Monodromy." *J. Amer. Math. Soc.* 6 (1993), no. 1, 149–222.

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

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

[6] Rosen, Michael. *Number Theory in Function Fields*, Graduate Text in Mathematics 210, Springer, 2002.

[7] Stroock, Daniel W. *Probability theory, an analytic view*, Cambridge University Press, Cambridge, 1993.

[8] Weil, André. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann et Cie., Paris, 1948. iv+85 pp.