STATISTICS FOR BIQUADRATIC COVERS OF THE PROJECTIVE LINE OVER FINITE FIELDS.

ELISA LORENZO, GIULIO MELELEO, AND PIERMARCO MILIONE

ABSTRACT. We study the distribution of the traces of the Frobenius endomorphism of genus $g$ curves which are quartic non-cyclic covers of $\mathbb{P}^1_{\mathbb{F}_q}$, as the curve varies in an irreducible component of the moduli space. We show that for $q$ fixed, the limiting distribution of the trace of Frobenius equals the sum of $q + 1$ independent random discrete variables. We also show that when both $g$ and $q$ go to infinity, the normalized trace has a standard complex Gaussian distribution. Finally, we extend these computations to the general case of arbitrary covers of $\mathbb{P}^1_{\mathbb{F}_q}$ with Galois group isomorphic to $r$ copies of $\mathbb{Z}/2\mathbb{Z}$. For $r = 1$, we recover the already known hyperelliptic case.

1. Introduction

One of the most influential results in class field theory is Chebotarev’s density theorem. As it is well known, this result is a deep generalization of the Theorem of Dirichlet about equidistribution of rational primes in arithmetic progression and gives a complete understanding of the distribution of primes in a fixed Galois number field extension with respect to their splitting behavior (for an interesting discussion of the theorem and its original proof see [LS96]). In the function field case the parallel statement is carried over by the Sato-Tate conjecture for curves, which studies the distribution of the Frobenius endomorphism of the reduction modulo $p$ of a fixed curve, when the prime $p$ varies.

In order to complement this research line in other directions, several mathematicians were led to consider the following new general problem: given a family of curves, satisfying certain properties, of genus $g$ over $\mathbb{F}_q$, understand the distribution of the Frobenius endomorphism of the curves of the family. This is sometimes called the vertical Sato-Tate conjecture, since the prime $p$ is fixed and the curve varies in the family. This study can be done in two different ways, depending on whether we let the genus $g$ tend to infinity or the cardinality $q$ of the field. It is then interesting to compare both limit results.

When $g$ is fixed and $q$ goes to infinity the problem can be solved thanks to Deligne’s equidistribution theorem (cf. [KS99]) while for the complementary case different techniques are applied depending on the particular family considered. The fluctuation in the number of points at the $g$-limit has been studied for different families of curves, such as:

- Hyperelliptic curves, cf. [KR09], [BDFL09].

2010 Mathematics Subject Classification. 11G20,14H05,11M50.

Key words and phrases. Function fields, biquadratic curves, biquadratic covers, number of points over finite fields, arithmetic statistics.

The second author has been partially supported by the “National Group for Algebraic and Geometric Structures, and their Applications” (GNSAGA-INDAM). The third author has been partially supported by the Spanish Council under project MTM2012-33830 and by an ADR grant from the Universitat de Barcelona.
In the present paper, we study the distribution of the number of points over \( \mathbb{F}_q \) for a genus \( g \) curve \( C \) defined over \( \mathbb{F}_q \) which is a quartic non-cyclic cover of the projective line \( \mathbb{P}_1^{\mathbb{F}_q} \), at the \( q \)-limit (for a genus \( g \) fixed) and at the \( g \)-limit (with \( q \) fixed).

Let \( B_g(\mathbb{F}_q) \) be the family of such genus \( g \) curves and consider the following decomposition

\[
B_g(\mathbb{F}_q) = \bigcup_{g_1+g_2+g_3=g} B_{(g_1,g_2,g_3)}(\mathbb{F}_q)
\]

where \( B_{(g_1,g_2,g_3)}(\mathbb{F}_q) \) denotes the subfamily of curves \( C \in B_g(\mathbb{F}_q) \) such that the three hyperelliptic quotients of \( C \) have genera \( g_1, g_2 \) and \( g_3 \).

The main theorem of the paper is the following:

**Theorem.** In the limit when the three genera \( g_1, g_2, g_3 \) go to infinity

\[
\frac{|\{C \in B_{(g_1,g_2,g_3)}(\mathbb{F}_q) : \text{Tr}(\text{Frob}_C) = -M\}|}{|B_{(g_1,g_2,g_3)}(\mathbb{F}_q)|} = \text{Prob} \left( \sum_{j=1}^{q+1} X_j = M \right)
\]

where the \( X_j \) are i.i.d. random variables such that

\[
X_i = \begin{cases} 
-1 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\
1 & \text{with probability } \frac{4(q+3)}{6} \\
3 & \text{with probability } \frac{q}{4(q+3)}
\end{cases}
\]

**Outline.** In Section 2 we introduce the family of biquadratic curves and we give a parametrization of the family in terms of terms of coprime square-free polynomials. In Section 3 we compute the monodromy group of the family in the sense of Katz and Sarnak (cf. [KS99, Ch. 9]) and we obtain the corresponding distribution of the Frobenius traces at the \( q \)-limit. In Section 4 the main theorem is proven and in Section 5 the moments of the Frobenius traces are computed at the \( g \)-limit, proving that when both \( g \) and \( q \) go to infinity the normalized trace has a standard complex Gaussian distribution. Finally, in last section, main theorem is generalized for an arbitrary cover of the projective line with Galois group isomorphic to \( r \) copies of \( \mathbb{Z}/2\mathbb{Z} \).

**Notations.** We now fix some notations and conventions that will be valid in the sequel.

- \( p \neq 2 \) is a prime integer, and \( q \) is a positive power of \( p \).
- \( k = \mathbb{F}_q(t) \) is the function field of \( \mathbb{P}_1^{\mathbb{F}_q} \), and \( K/k \) is a finite extension.
- \( (f,g) \) denotes the greatest common divisor of two polynomials \( f, g \in \mathbb{F}_q[t] \).
- \( \deg(f) \) denotes the degree of a polynomial \( f \).
- \( \tilde{f} \) is the polynomial obtained inverting the order of the coefficients of \( f \).

**Acknowledgements.** This work was started in March 2014 at the Arizona Winter School “Arithmetic Statistic” and the authors would like to thank the organizers for creating such a stimulating working environment. Moreover, the authors are grateful to Alina Bucur and Chantal David for initiating them into this rich and appealing field of research in number theory and for several discussions and helpful comments during the preparation of the paper.
2. The family of biquadratic curves

We first define and give the basic properties of the family of biquadratic curves. We determine its genus in terms of the equations defining the curves, and we study the irreducible components of the coarse moduli space of biquadratic curves.

Recall that if $K/F_q(t)$ is a finite Galois extension such that $K \cap F_q = F_q$, then there exists a unique nonsingular projective curve $C$ with function field $F_q(C) = K$, together with a regular morphism $\varphi : C \to \mathbb{P}^1_{F_q}$ defined over $F_q$ (cf. [Har77, I, Th. 6.6, Th. 6.9]).

**Definition 2.1.** We will call biquadratic curve a smooth projective curve $C$, together with a regular morphism $\varphi : C \to \mathbb{P}^1_{F_q}$ defined over $F_q$, that induces a field extension with Galois group $\text{Gal}(F_q(C)/F_q(t)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since $\text{char}(k) \neq 2$, it is clear that every non-cyclic quartic extension of $k$ is of the form $K = k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$, for some $h_1(t), h_2(t) \in F_q[t]$ different non-constant polynomials, that we can take to be square-free. Moreover, if the leading coefficient $\text{lc}(h_i)$ is a square in $F_q$, then we can assume that this is equal to 1. Therefore, if $C$ is a biquadratic curve, then an affine model of $C$ in $\mathbb{A}^3_{F_q}$ is given by

$$C : \begin{cases} y_1^2 = h_1(t) \\ y_2^2 = h_2(t). \end{cases}$$

**Remark 2.2.** If $K := k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$ is a biquadratic extension of $k$, then there are exactly 3 different quadratic subextensions of $K$, namely $k(\sqrt{h_1}), k(\sqrt{h_2})$ and $k(\sqrt{h_1 h_2})$.

If we write $h_i = f_i f$ for $i = 1, 2$, with $f = (h_1, h_2)$, then clearly we have that $(f_1, f_2) = (f_1, f) = (f_2, f) = 1$ and these three subextensions are $k(\sqrt{f_1 f_2}), k(\sqrt{f_1 f_2})$ and $k(\sqrt{f_1 f_2})$.

Two such extensions $k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$ and $k(\sqrt{h'_1(t)}, \sqrt{h'_2(t)})$ are the same if and only if we have the equality of sets:

$$\left\{ h_1, h_2, \frac{h_1 h_2}{(h_1, h_2)^2} \right\} = \left\{ h'_1, h'_2, \frac{h'_1 h'_2}{(h'_1, h'_2)^2} \right\}.$$

**Remark 2.3.** Recall that if $\pi : C \to \mathbb{P}^1$, whose affine plane model is $y^2 = F(t)$, with $F(t)$ a square-free polynomial over $F_q$, then the point at infinity is ramified in the cover $\pi$ iff the degree $d$ of $F$ is odd. Indeed, if we take take $u = \frac{1}{t}$, then the function field of $C$ is:

$$k(C) = k(\sqrt{F(t)}) = k(\sqrt{F(1/u)}) = k(\sqrt{u^d F(u)})$$

and then it is clear that $t = \infty$ ramifies iff the point $u = 0$ ramifies, i.e. iff $d$ is odd.

**Proposition 2.4.** Let $h_1(t), h_2(t) \in F_q[t]$ be different square-free polynomials, and let $C$ be the curve whose function field is $k(C) = k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$. For every $i = 1, 2$, write $h_i = f_i f$, with $f = (h_1, h_2)$, and define $h_3 := f_1 f_2$.

If we denote by $C_i$ the hyperelliptic curve whose affine plane model is given by the equation $y^2 = h_i(t)$, for $i = 1, 2, 3$, then we have the following formula for the genus of $C$:

$$g(C) = g(C_1) + g(C_2) + g(C_3)$$

Moreover, if we denote by $n := \deg(f)$ and $n_i := \deg(f_i)$,

$$g(C) = g(n, n_2, n) := n_1 + n_2 + n + e_{\infty} - 4,$$

where $e_{\infty}$ is the number of ramified points at infinity.
where
\[ e_\infty := \begin{cases} 2, & \text{if } n \equiv n_1 \equiv n_2 \equiv 0 \pmod{2} \\ 1, & \text{otherwise} \end{cases} \]

**Proof.** Let us denote by \( R := \text{Ram}(\pi) \) the subset of all points of \( \mathbb{P}^1_{\mathbb{F}_q} \) which are ramified in the cover \( \pi : C \to \mathbb{P}^1_{\mathbb{F}_q} \). Riemann-Hurwitz formula (cf. [Ros02, Theorem 7.16]) implies that 
\[ 2g(C) - 2 = 4(2 \cdot 0 - 2) + 2|R|. \]
So, \( g(C) = |R| - 3 \). Again, for the hyperelliptic cover \( \pi_i : C_i \to \mathbb{P}^1 \) and the ramification sets \( R_i := \text{Ram}(\pi_i) \), gives \( g(C_i) = \frac{|R_i|}{2} - 1 \). Now, the definition of \( h_3 \) implies that
\[ 2|R_1 \cup R_2 \cup R_3| = |R_1| + |R_2| + |R_3|. \]
Thus, the formula \( g(C) = g(C_1) + g(C_2) + g(C_3) \) holds.

We can also apply Riemann-Hurwitz formula to the morphism \( \pi \), and so we have:
\[ 2g - 2 = 4(2 \cdot 0 - 2) + 2 \cdot (n_1 + n_2 + n_3 + e_\infty - 1). \]
\[ \square \]

Now, we introduce some sets of polynomials that will be useful:
\[
\begin{align*}
V_d &= \{ F \in \mathbb{F}_q[t] : F \text{ monic, } \deg(F) = d \} \\
F_d &= \{ F \in \mathbb{F}_q[t] : F \text{ monic, square-free, } \deg(F) = d \} \\
\tilde{F}_d &= \{ F \in \mathbb{F}_q[t] : F \text{ square-free, } \deg(F) = d \} \\
F_{n,n_1,n_2} &= \{ (f, f_1, f_2) \in F_n \times F_{n_1} \times F_{n_2} : (f, f_1) = (f, f_2) = (f_1, f_2) = 1 \} \\
\tilde{F}_{n,n_1,n_2} &= \{ (f, f_1, f_2) \in F_n \times \tilde{F}_{n_1} \times \tilde{F}_{n_2} : (f, f_1) = (f_1, f_2) = 1 \}
\end{align*}
\]

**Definition 2.5.** We denote by \( B_g(\mathbb{F}_q) \) the family of biquadratic curves defined over \( \mathbb{F}_q \) and of fixed genus \( g \). It can be written as a disjoint union of subfamilies indexed by unordered 3-tuples of positive integers \( g_1, g_2, g_3 \), i.e.
\[
B_g(\mathbb{F}_q) = \bigcup_{g_1 + g_2 + g_3 = g} B_{(g_1,g_2,g_3)}(\mathbb{F}_q),
\]
where \( B_{(g_1,g_2,g_3)}(\mathbb{F}_q) \) denotes the family of curves over the set of polynomials \( \tilde{F}_{n,n_1,n_2} \) such that \( g_i = \left\lfloor \frac{n_i + n_{i-1}}{2} \right\rfloor \) for \( i = 1, 2 \) and \( g_3 = \left\lfloor \frac{n_1 + n_2 - 1}{2} \right\rfloor \).

The family \( B_g(\mathbb{F}_q) \) of biquadratic curves defined over \( \mathbb{F}_q \) is a coarse moduli space over \( \mathbb{Z}[1/2] \) (cf. [PG05b, Lemma 3.1]). A detailed geometric study of this moduli space can be found in [PG05b] and [PG05a].

**Remark 2.6.** One has the following equalities:
\[
|B_{(g_1,g_2,g_3)}(\mathbb{F}_q)|' = \sum_{C \in B_{(g_1,g_2,g_3)}(\mathbb{F}_q)} 1 = \sum_{F \in \tilde{F}_{n,n_1,n_2}} \frac{1}{|\text{Aut}(C)|} = \frac{|\tilde{F}_{n,n_1,n_2}|}{q(q^2 - 1)},
\]
where the ' notation, applied both to cardinality and summation, means that each one of the curves \( C \) in the moduli spaces is counted with the usual weight \( \frac{1}{|\text{Aut}(C)|} \).
Remark 2.7. Notice that $|\mathcal{F}_{(n,n_1,n_2)}| = (q-1)^2 |\mathcal{F}_{(n_1,n_2)}|$ and that we can see the set $\mathcal{F}_{(n,n_1,n_2)}$ as the set of the quadratic twists of elements in $\mathcal{F}_{(n_1,n_2)}$ given by the equations

$$C' : \begin{cases} y_1^2 = \alpha_1 f_1(t) \\ y_2^2 = \alpha_2 f_2(t) \end{cases}$$

where $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$.

3. Monodromy group of the family

A useful reference for this section is [KS99, Ch. 9]. Let $S$ be an open set of $\text{Spec} \mathbb{F}_q$ and let $\mathcal{C} \to S$ be a smooth proper morphism of schemes such that the geometric fibers $C_x \otimes \mathbb{F}_q$ are smooth projective curves of genus $g$ over $\mathbb{F}_q$.

Fix a prime integer $\ell \neq p$. Then, there exists an $\ell$-adic representation

$$\rho_\ell : \pi_1(S) \to \text{GL}_{2g}(\mathbb{Q}_\ell)$$

with the following interpolation property: for every closed point $x : \text{Spec} \mathbb{F}_q \to S$ the induced representation

$$\text{Gal}(\mathbb{F}_q/\mathbb{F}_q) \cong \pi_1(\text{Spec} \mathbb{F}_q) \to \pi_1(S) \to \text{GL}_{2g}(\mathbb{Q}_\ell)$$

is isomorphic to the $\ell$-adic representation

$$\rho_{C_x, \ell} : \text{Gal}(\mathbb{F}_q/\mathbb{F}_q) \to \text{Aut}(H^1_{et}(C_x \otimes \mathbb{F}_q, \mathbb{Q}_\ell)) \cong \text{GL}_{2g}(\mathbb{Q}_\ell) .$$

Once fixed an embedding $\iota : \mathbb{Q}_\ell \to \mathbb{C}$, we have a $2g$-dimensional complex representation $\iota \cdot \rho_\ell$. The image of this representation is a subgroup of $\text{GL}_{2g}(\mathbb{C})$ called the monodromy group of the family.

For every integer $d \geq 1$, the set of polynomials $\mathcal{F}_d$ defined in Section 2 can be algebraically realized as a Zariski-open subset of $A^d_{\mathbb{F}_q}$. This could be done redefining it in the following way:

$$\mathcal{F}_d := \{ (a_0, \ldots, a_{d-1}) \in A^d_{\mathbb{F}_q} \mid D(a_0, \ldots, a_{d-1}) \neq 0 \},$$

where $D : A^d_{\mathbb{F}_q} \to A^1_{\mathbb{F}_q}$ is the continuos function such that $D(a_0, a_1, \ldots, a_{d-1})$ denotes the discriminant of the monic polynomial $a_0 + a_1 t + \ldots + t^d \in \mathbb{F}_q[t]$.

Let $\mathcal{H}_g$ denote the family of genus $g$ hyperelliptic curves over $\mathcal{F}_d$, whose fiber over the polynomial $F \in \mathcal{F}_d$ is given by the curve whose affine plane model is $y^2 = F(t)$. In [KS99, 10.1], it is proved that the monodromy group either of the family $\mathcal{H}_g$ over $\mathcal{F}_{2g+1}$ and of the family $\mathcal{H}_g$ over $\mathcal{F}_{2g+2}$ is $G_{\text{geom}} = \text{Sp}_{2g}(\mathbb{C})$.

Proposition 3.1. The monodromy group of the family $\mathcal{B}_{g_1,g_2,g_3}(\mathbb{F}_q)$ is the biggest possible, namely it is the symplectic group $\text{Sp}_{2g}(\mathbb{C})$.

Proof. The set of polynomials $\mathcal{F}_{[n,n_1,n_2]}$ defined in Section 2 can be realized as a Zariski-open subset of $A^n_{\mathbb{F}_q} \times A^{n_1+1}_{\mathbb{F}_q} \times A^{n_2+1}_{\mathbb{F}_q}$.

The family of genus $g$ curves over $\mathcal{F}_{[n,n_1,n_2]}$, whose fiber over the pair $(f, f_1, f_2) \in \mathcal{F}_{[n,n_1,n_2]}$ is given by the curve whose affine model is $y_1^2 = f f_1(t), y_2^2 = f f_2(t)$, is exactly the subfamily of genus $g$ biquadratic curves $\mathcal{B}_{g_1,g_2,g_3}(\mathbb{F}_q)$ defined in Section 2.
Let $N := \max(n, n_2, n_3)$. By the symmetry of the parametrization we can assume for example that $N = n$ and then we fix two square-free polynomials $f_1, f_2$ of degrees $n_1, n_2$ such that $f_1f_2$ is square-free. Therefore we can consider the open immersion

$$ f \in \{ F \in \mathcal{F}_n : F_{f_1}, F_{f_2} \text{ square - free} \} \mapsto (f, f_1, f_2) \in \mathcal{F}_{[n,n_1,n_2]}.$$ 

The monodromy group of the family $\mathcal{H}_g$ of hyperelliptic curves over this subset of $\mathcal{F}_n$ is the same as if we consider the family over all $\mathcal{F}_n$. Finally, the monodromy group of the family $B_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ can only increase and, after results of [KS99] 10.1, it is the biggest possible.

Applying Deligne’s equidistribution theorem (cf. [KS99] 9.3.9.2) and random matrix theory (cf. [DS94] 4), we have the following distribution result at the $q$-limit for the family $B_{(g_1,g_2,g_3)}(\mathbb{F}_q)$:

**Corollary 3.2.** Let $g \geq 3$ be a fixed integer. When $q$ goes to $\infty$, the classes of the Frobenius automorphisms $\{ \text{Frob}_C \} \subset B_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ acting on the first étale cohomology group $H^1_{et}(C, \mathbb{Q}_\ell)$ are equidistributed with respect to the Haar measure associated to the maximal compact subgroup of $\text{Sp}_{2g}(\mathbb{C})$, i.e.

$$\lim_{q \to \infty} \langle \text{Tr} \text{Frob}_C^n \rangle = \begin{cases} 2g & n = 0 \\ -\eta_n & 1 \leq |n| \leq 2g \\ 0 & |n| > 2g \end{cases}$$

where

$$\eta_n := \begin{cases} 1 & n \text{ even} \\ 0 & n \text{ odd} \end{cases}.$$ 

4. **The Distribution for $n = 1$**

Let $\chi$ denote the quadratic character in $\mathbb{F}_q$, we set, for any element $(f, f_1, f_2)$ in $\tilde{\mathcal{F}}_{(n,n_1,n_2)}$,

$$S(f, f_1, f_2) = \sum_{x \in \mathbb{F}_q} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x))),$$

and

$$\tilde{S}(f, f_1, f_2) = \sum_{x \in \mathbb{F}_q} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x))),$$

where for the point at infinity we define

$$\chi(F(\infty)) = \begin{cases} 0 & \deg(F) \text{ odd} \\ 1 & \deg(F) \text{ even, leading coefficient is a square in } \mathbb{F}_q \\ -1 & \deg(F) \text{ even, leading coefficient is not a square in } \mathbb{F}_q \end{cases}$$

Then, for the curve $C \in B_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ defined by $(f, f_1, f_2)$ we have that

$$\#C(\mathbb{F}_q) = q + 1 + \tilde{S}(f, f_1, f_2).$$

Hence, we have the equality

$$\frac{|\{ C \in B_{(g_1,g_2,g_3)}(\mathbb{F}_q) : \text{Tr}(\text{Frob}_C) = -M \}|'}{|B_{(g_1,g_2,g_3)}(\mathbb{F}_q)|'} = \frac{|\{(f, f_1, f_2) \in \tilde{\mathcal{F}}_{[n,n_1,n_2]} : \tilde{S}(f, f_1, f_2) = M \}|}{|\tilde{\mathcal{F}}_{[n,n_1,n_2]}|}$$

The goal of this section is to prove the following theorem, which is a more precise statement of the theorem in the Introduction.
Theorem 4.1. In the limit when the three degrees $n, n_1, n_2$ go to infinity

$$\frac{|\{(f, f_1, f_2) \in \mathcal{F}_{[n,n_1,n_2]} : \hat{S}(f,f_1,f_2) = M\}|}{|\mathcal{F}_{[n,n_1,n_2]}|} = \text{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right)$$

where the $X_j$ are i.i.d. random variables such that

$$X_i = \begin{cases} 
-1 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\
1 & \text{with probability } \frac{q}{4(q+3)} \\
3 & \text{with probability } \frac{1}{4(q+3)}
\end{cases}$$

More precisely,

$$\frac{|\{(f, f_1, f_2) \in \mathcal{F}_{[n,n_1,n_2]} : \hat{S}(f,f_1,f_2) = M\}|}{|\mathcal{F}_{[n,n_1,n_2]}|} = \text{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right)\left(1 + O(q^{-\min(n,n_1,n_2)+3})\right)$$

The proof of the Theorem runs as in [KR09] (resp. [BDFL09]) for the equivalent statement for hyperelliptic curves (resp. $l$-cyclic covers).

Lemma 4.2. ([BDFL09] Lemma 4.2) For $0 \leq l \leq q$ let $x_1, \ldots, x_l$ be distinct elements of $\mathbb{F}_q$. Let $U \in \mathbb{F}_q[l]$ be such that $U(x_i) \neq 0$ for $i = 0, \ldots, l$. Let $a_1, \ldots, a_l \in \mathbb{F}_q^\times$. The number of elements in the set

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

is the number

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

Lemma 4.3. For $0 \leq l \leq q$ let $x_1, \ldots, x_l$ be distinct elements of $\mathbb{F}_q$. Let $U \in \mathbb{F}_q[l]$ be such that $U(x_i) \neq 0$ for $i = 0, \ldots, l$. Let $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{F}_q^\times$. The number of elements in the set

$$\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_1, U) = (f_2, U) = 1, f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}$$

is the number

$$R_{n_1,n_2}^U(l) = \frac{q^{n_1+n_2-2l}L}{\zeta_q(2)(1-q^{-2})} \left(\frac{1+2q^{-1}}{(1+q^{-1})^2}\right)^l \prod_{D \mid U} \left(\frac{1}{1+2|D|^{-1}}\right) \left(1 + O(q^{-n_1-n_2+2})\right),$$

where $L := \prod_{P \mid \mathbb{F}_q} \left(1 - \frac{|P|^{-2}}{(1+|P|^{-1})^2}\right)$.

Proof. By inclusion-exclusion principle (same notations as in [GGL95] Theorem 13.5]), with $f(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_1, U) = 1, D(f_1, f_2), f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}|$,

$$g(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_1, U) = 1, (f_1, f_2) = D, f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}|,$$

we have

$$R_{n_1,n_2}^U(l) = g(1) = \sum_{D, D(x_i) = 0, (D,U) = 1} \mu(D)f(D).$$

But notice that when $(D,U) = 1$

$$f(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1-\deg(D)} \times \mathcal{F}_{n_2-\deg(D)} : (f_1, U D) = 1, f_1(x_i) = a_i, f_2(x_i) = b_i, 1 \leq i \leq l\}|,$$
hence Lemma 4.2 implies

\[ f(D) = S^{U \delta}_{n_1-\deg(D)}(l) \cdot S^{U \delta}_{n_2-\deg(D)}(l) = \frac{q^{n_1+n_2-2l-2\deg(D)}}{\zeta_q(2)(1-q^{-2})^{2l}} \prod_{P \mid U} \left( 1 + \left| P \right|^{-1} \right)^{-2} \left( 1 + O(q^{l-\min(n_1,n_2)} \frac{\min(n_1,n_2)}{2}) \right). \]

So, one has

\[ R^U_{n_1,n_2}(l) = \sum_{D, D(x_i) \neq 0, (D, U) = 1} \mu(D) f(D) = \frac{q^{n_1+n_2-2l}}{\zeta_q(2)(1-q^{-2})^{2l}} \prod_{P \mid U} \left( 1 + \left| P \right|^{-1} \right)^{-2} \sum_{D(x_i) \neq 0, (D, U) = 1} \mu(D) \left| D \right|^{-2} \prod_{P \mid D} \left( 1 + \left| P \right|^{-1} \right)^{-2} \left( 1 + O(q^{l-\min(n_1,n_2)}) \right). \]

Now, we observe that

\[ \sum_{D(x_i) \neq 0, (D, U) = 1} \mu(D) \left| D \right|^{-2} \prod_{P \mid D} \left( 1 + \left| P \right|^{-1} \right)^{-2} = \]

\[ \sum_{D, D(x_i) \neq 0, (D, U) = 1} \mu(D) \left| D \right|^{-2} \prod_{P \mid D} \left( 1 + \left| P \right|^{-1} \right)^{-2} + O(q^{-2\min(n_1,n_2)}), \]

where we have that

\[ \sum_{D, D(x_i) \neq 0, (D, U) = 1} \mu(D) \left| D \right|^{-2} \prod_{P \mid D} \left( 1 + \left| P \right|^{-1} \right)^{-2} = \]

\[ = \left( \frac{1+2q^{-1}}{1+q^{-1}} \right)^{-l} \prod_{P \mid U} \left( \frac{1+2\left| P \right|^{-1}}{1+\left| P \right|^{-1}} \right)^{-1} \prod_{P \text{ prime}} \left( 1 - \frac{\left| P \right|^{-2}}{1+\left| P \right|^{-1}} \right) = \]

\[ = \left( \frac{1+2q^{-1}}{1+q^{-1}} \right)^{-l} \prod_{P \mid U} \left( \frac{1+2\left| P \right|^{-1}}{1+\left| P \right|^{-1}} \right)^{-1} L. \]

We can prove that \( 0 < L < 1 \) (see next Remark 4.4). So, finally

\[ R^U_{n_1,n_2}(l) = \frac{q^{n_1+n_2-2l}L}{\zeta_q(2)(1-q^{-2})^{2l}} \left( \frac{1+2q^{-1}}{1+q^{-1}} \right)^{-l} \prod_{P \mid U} \left( \frac{1}{1+2\left| P \right|^{-1}} \right) \left( 1 + O(q^{l-\min(n_1,n_2)} \frac{\min(n_1,n_2)}{2}) \right). \]

\[ \square \]

**Remark 4.4.** We need to prove that the infinite product \( \prod_{P \text{ prime}} \left( 1 - \frac{\left| P \right|^{-2}}{(1+\left| P \right|^{-1})^2} \right) \) converges to a real number \( L \) such that \( 0 < L < 1 \). The Prime Polynomial Theorem implies that this is equivalent to prove that the infinite product

\[ \prod_{\nu \geq 1} \left( 1 - \frac{1}{(q^\nu + 1)^2} \right)^{q^\nu} \]

converges to a real number \( \tilde{L} \) such that \( 0 < \tilde{L} < 1 \) (remember that \( q \geq 3 \)).
Because \((1 - \frac{1}{(q^{r+1})^{2}})^{\frac{1}{2r}} < 1\), we have that \(\tilde{L} < 1\). In order to prove that \(0 < \tilde{L}\), and since for \(z \in (0, 1)\) we have \(\log(1 - z) \geq \frac{-z}{1 - z}\), it is enough to prove that

\[
\sum_{\nu \geq 1} \frac{q^{\nu}}{\nu} \left( \frac{1}{(q^{r+1})^{2}} - 1 \right) = - \sum_{\nu \geq 1} \frac{1}{\nu} \cdot \frac{1}{q^{\nu} + 2}
\]

is convergent. Indeed, we have

\[
0 \leq \sum_{\nu \geq 1} \frac{1}{\nu} \cdot \frac{1}{q^{\nu} + 2} \leq \sum_{\nu \geq 1} \frac{1}{\nu^{3/2}} = \log \frac{3}{2}.
\]

Thus,

\[
\prod_{\nu \geq 1} \left( 1 - \frac{1}{(q^{r} + 1)^{2}} \right)^{\frac{1}{2r}} \geq \frac{2}{3}.
\]

**Proposition 4.5.** Let \(0 \leq l \leq q\), let \(x_1, \ldots, x_l\) be distinct elements of \(\mathbb{F}_q\), and \(a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{F}_q^*\). Then, for any \(1 > \epsilon > 0\), we have

\[
|\{(f, f_1, f_2) \in \mathcal{F}_{(n_1, n_2)} : f(x_i) f_1(x_i) = a_i, f(x_i) f_2(x_i) = b_i, 1 \leq i \leq l\}| =
\]

\[
= \frac{KLq^{n_1+n_2+n-2l}}{\zeta_q^3(2)} \left( \frac{q^3}{(q-1)^2(q+3)} \right)^l \left( 1 + O(q^{-(1-\epsilon)n+cl} + q^{-\min(1,n_2)^2+l}) \right),
\]

where \(K := \prod_P (1 - \frac{2}{(P+1)(P+2)})\).

**Proof.** First we observe that

\[
|\{(f, f_1, f_2) \in \mathcal{F}_{(n_1, n_2)} : f(x_i) f_1(x_i) = a_i, f(x_i) f_2(x_i) = b_i, 1 \leq i \leq l\}| =
\]

\[
= \sum_{f \in \mathcal{F}_n} \sum_{f_1 \in \mathcal{F}_{n_1}} \sum_{f_2 \in \mathcal{F}_{n_2}} 1 =
\]

\[
= \sum_{f \in \mathcal{F}_n, f(x_i) \neq 0} \sum_{f_1 \in \mathcal{F}_{n_1}} \sum_{f_2 \in \mathcal{F}_{n_2}} 1 =
\]

\[
= \sum_{f \in \mathcal{F}_n, f(x_i) \neq 0} R_{n_1, n_2}^l (l).
\]

Using Lemma 4.3 we have that

\[
|\{(f, f_1, f_2) \in \mathcal{F}_{(n_1, n_2)} : f(x_i) f_1(x_i) = a_i, f(x_i) f_2(x_i) = b_i, 1 \leq i \leq l\}| =
\]

\[
= \frac{q^{n_1+n_2-2l}L}{\zeta_q^2(2)(1 - q^{-2})^2} \left( \frac{1}{1 + 2q^{-1}} \right)^l \sum_{U \in \mathcal{F}_n, \deg(U) \neq 0} \prod_{P | U} \frac{1}{1 + 2P^{-1}} + O(q^{n_1+n_2-\min(1,n_2)^2-l}) =
\]

\[
= \frac{q^{n_1+n_2-2l}L}{\zeta_q^2(2)(1 - q^{-2})^2} \left( \frac{1}{1 + 2q^{-1}} \right)^l \sum_{\deg(U) = n} c(U) + O(q^{n_1+n_2-\min(1,n_2)^2-l}),
\]

where for any polynomial \(U\), we define

\[
c(U) = \begin{cases} 
\mu^2(U) \prod_{P | U} \frac{1}{1 + 2P^{-1}}, & U(x_i) \neq 0 \\
0, & \text{otherwise.}
\end{cases}
\]
In order to evaluate $\sum_{\deg(U)=n} c(U)$, we consider the Dirichlet series
\[
G(w) = \sum_{U} \frac{c(U)}{|U|^w} = \prod_{P, \deg P = 0} \left(1 + \frac{1}{|P|^w} \cdot \frac{|P|}{(|P| + 2)}\right) = \frac{\zeta_q(w)}{\zeta_q(2w)} H(w) \left(1 + \frac{1}{q^{w-1}(q + 2)}\right)^{-1},
\]
where
\[
H(w) = \prod_{P} (1 - \frac{2}{(1 + |P|^w)(|P| + 2)})
\]
Notice that $H(w)$ converges absolutely for $\text{Re}(w) > 0$, and $G(w)$ is meromorphic for $\text{Re}(w) > 0$ with simple poles at the points $w$ where $\zeta_q(w) = (1 - q^{1-w})^{-1}$ has poles, that is, $1 + \frac{i2\pi n}{\log q}$. Thus, $G(w)$ has a simple pole at $w = 1$ with residue
\[
\frac{K}{\zeta_q(2) \log(q)} \left(\frac{q + 3}{q + 2}\right)^{-1},
\]
where $K = H(1)$.

Using Theorem 17.1 of [Ros02], which is the function field version of the Wiener-Ikehara Tauberian Theorem, we get that
\[
\sum_{\deg(U)=n} c(U) = \frac{K}{\zeta_q(2)} \left(\frac{q + 2}{q + 3}\right)^{\epsilon n} + O_q(q^{\epsilon n}),
\]
for all $\epsilon > 0$ and where, looking at the proof of the theorem and proceeding as in Proposition 4.3 in [BDFL09], we can exchange $O_q(q^{\epsilon n})$ by $O(q^{(\epsilon n + 1)})$.

**Corollary 4.6.** Let $0 \leq l \leq q$, let $x_1, \ldots, x_l$ be distinct elements of $\mathbb{F}_q$, and let $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{F}_q$ such that $a_1 = \ldots = a_{r_0} = b_1 = \ldots = b_{r_0} = 0$, $a_{r_0} = \ldots = a_{r_0 + r_1} = 0 = b_{r_0 + r_1 + 1} = \ldots = b_{r_0 + r_1 + r_2}$ and $b_{r_0 + 1}, \ldots, b_{r_0 + r_1}, a_{r_0 + r_1 + 1}, \ldots, a_{r_0 + r_1 + r_2}, a_j, b_j \neq 0$ if $j > r_0 + r_1 + r_2 = m$. Then for every $\epsilon > 0$, the number
\[
|\{(f, f_1, f_2) \in \mathcal{F}(n,n_1,n_2) : f(x_1) f_1(x_1) = a_i, f(x_i) f_2(x_i) = b_i, f_1(x_i) f_2(x_1) = c_i, 1 \leq i \leq l\}|,
\]
where $f(x_i)^2 c_i = a_i b_i$, is equal to
\[
q^{n_1 n_2} \left(\frac{1}{(q - 1)(q + 3)}\right)^m \left(\frac{q}{(q - 1)^2(q + 3)}\right)^l \left(1 + O(q^{-\epsilon min(n,n_1,n_2) + 1})\right).
\]

**Proof.** Let us write $f = (x - x_1) \ldots (x - x_{r_0}) f'$, $f_1 = (x - x_{r_0 + 1}) \ldots (x - x_{r_0 + r_1}) f'_1$, and $f_2 = (x - x_{r_0 + r_1 + 1}) \ldots (x - x_{r_0 + r_1 + r_2}) f'_2$. Now, apply Proposition 4.3 to the pairs $(f', f'_1, f'_2)$ and sum.

**Corollary 4.7.** With notation in Corollary 4.6, the number
\[
|\{(f, f_1, f_2) \in \mathcal{F}(n,n_1,n_2) : \chi(f(x_i) f_1(x_i)) = e_i^1, \chi(f(x_i) f_2(x_i)) = e_i^2, \chi(f_1(x_i) f_2(x_1)) = e_i, 1 \leq i \leq l\}|_{\mathcal{F}(n,n_1,n_2)}
\]
where $e_1^1, e_1^2$, $e_i \in \{-1, 0, 1\}$, $\chi(f(x_i)^2) e_i = e_i^1 e_i^2$, and exactly $2m$ of them are equal to zero, is equal to
\[
C_m^l = \left(\frac{q - 1}{2}\right)^m \left(\frac{q - 1}{2}\right)^{2l - m} \left(\frac{1}{(q - 1)(q + 3)}\right)^m \left(\frac{q}{(q - 1)^2(q + 3)}\right)^l \left(1 + O(q^{-\epsilon min(n,n_1,n_2) + 1})\right).
\]
where we use the notation $N$ agrees with Gaussian moments for all $k$ is also equal to the number

Corollary 4.8. Let $0 \leq l \leq q$, let $x_1, \ldots, x_l$ be distinct elements of $\mathbb{P}^1(\mathbb{F}_q)$, and let $e_1, e_2, e_3 \in \{-1, 0, 1\}$ be such that $\chi(f(x_1)^2)e_1 = e_1^2$, and exactly $2m$ of them are equal to zero. Then

\[
\left| \{(f, f_1, f_2) \in \hat{F}_{[n,n_1,n_2]} : \chi(f(x_i)f_1(x_i)) = e_1, \chi(f(x_i)f_2(x_i)) = e_2, \chi(f_1(x_i)f_2(x_i)) = e_3\} \right|
\]

is also equal to the number $C_{l}^q$ defined in Corollary 4.7.

**Proof.** Distinguish the case in which some $x_j$ is the point at infinity or not. Generalize Corollary 4.7 for the sets $\hat{F}_{(n_1,n_2)}$ looking at the symmetry observed in Remark 2.7 and add for the different components of $\hat{F}_{[n,n_1,n_2]}$. □

Proof. (of Theorem 4.1) Apply Corollary 4.8 in order to compute

\[
\frac{\left| \{(f, f_1, f_2) \in \hat{F}_{[n,n_1,n_2]} : \hat{S}(f, f_1, f_2) = M \} \right|}{\left| \hat{F}_{[n,n_1,n_2]} \right|} = \sum_{(E_1, \ldots, E_{q+1}) \in \{-1, 1, 3\}, \sum E_i=M} \sum_{j=0}^{N_1} \binom{N_1}{j} 3^{N_1} C_{N_1+j} \frac{6}{4q+3} \frac{3q+2}{4q+3} \frac{1}{4q+3} \frac{q}{4q+3} (1 + O(q^{-\frac{l+1}{2} \min(n,n_1,n_2)+q}))
\]

\[= \text{Prob} \left\{ \sum_{i=1}^{q+1} X_i = M \right\} (1 + O(q^{-\frac{l+1}{2} \min(n,n_1,n_2)+q}))\],

where we use the notation $N_i$ for the number of elements equal to $i$ in the vectors $(E_1, \ldots, E_{q+1})$. □

## 5. Averages and moments sequences

We want to compute the moments of $\text{Tr}(\text{Frob}_C)/\sqrt{1+q}$. That is, the $k$th moments

\[M_k(q, g_1, g_2, g_3) = \frac{1}{|B(\mathbb{F}_q)|} \sum_{C \in B(\mathbb{F}_q)(\mathbb{F}_q)} \left( \frac{\text{Tr}(\text{Frob}_C)}{\sqrt{1+q}} \right)^k.
\]

**Theorem 5.1.** With notation in Theorem 4.1, we have

\[M_k(q, g_1, g_2, g_3) = \mathbb{E} \left( \left( \frac{1}{\sqrt{1+q}} \sum_{i=1}^{1+q} X_i \right)^k \right) + O(q^{-\frac{k+1}{2} \min(n,n_1,n_2)+k})
\]

**Corollary 5.2.** If $g_1, g_2, g_3$ and $q$ tend to infinity, then the moments of $\text{Tr}(\text{Frob}_C)/\sqrt{1+q}$, as $C$ runs over the irreducible component $B(\mathbb{F}_q)(\mathbb{F}_q)$ of the moduli space $B_3(\mathbb{F}_q)$, are asymptotically Gaussian with mean 0 and variance 1.

**Proof.** Since the moments of a sum of bounded i.i.d. random variables converge to the Gaussian moments (Bil95 Sec. 30), it follows that, as $q \to \infty$, $M_k(q, g_1, g_2, g_3)$ agrees with Gaussian moments for all $k$. Then, Theorem 30.2 in [Bil95] implies the corollary. □
Proof. (of Theorem 5.1) We can write the $k$th moment as
\[
M_k(q, g_1, g_2, g_3) = (-1)^k \frac{q(q^2 - 1)}{|F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]|} \sum_{(f_1, f_2, f_3) \in F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]} \left( \widetilde{S}(f_1, f_2, f_3) \right)^k =
\]
\[
= \frac{(-1)^k q(q^2 - 1)}{|F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]|} \sum_{(f_1, f_2, f_3) \in F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]} \sum_{x \in \mathbb{P}^1(F_q)} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x)))^k =
\]
\[
= (-1)^k q(q^2 - 1) \sum_{l=1}^k c(k, l) \sum_{(x, b) \in P_{k,l}} \frac{1}{|F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]|} \sum_{(f_1, f_2, f_3) \in F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]} B(x, b, f_1, f_2, f_3),
\]
where
\[
P_{k,l} = \left\{ (x, b) : x = (x_1, ..., x_l) \in \mathbb{P}^1(F_q)^l, x_i's \text{ distinct}, b = (b_1, ..., b_l) \in \mathbb{Z}_{>0}, l \sum b_i = k \right\}
\]

and $c(k, l)$ is a certain combinatorial factor. We do not need exact formulas for it, but as it was notice in [BDFL09]
\[
\sum_{l=1}^k c(k, l) \sum_{(x, b) \in P_{k,l}} 1 = (q + 1)^k. \tag{5.1}
\]

Fix a vector $(x, b) \in P_{(k,l)}$. Then, the number
\[
\sum_{(f_1, f_2, f_3) \in F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]} \frac{B(x, b, f_1, f_2, f_3)}{|F[2g_1 + 2, 2g_2 + 2, 2g_3 + 2]|} = \sum_{(\epsilon_1, ..., \epsilon_l) \in (-1, 1, 3)^l} \left( \prod_{i=1}^l P_{\epsilon_i} \right) \left( \prod_{i=1}^l \epsilon_i^{b_i} \right) =
\]
\[
\sum_{(\epsilon_1, ..., \epsilon_l) \in (-1, 1, 3)^l} \left( \prod_{i=1}^l P_{\epsilon_i} \right) \left( \prod_{i=1}^l \epsilon_i^{b_i} \right) = \prod_{i=1}^l \left( 3^{b_i} q + 6 + (-1)^{b_i} 3(q + 2) \right) \frac{4(q + 3)}{4(q + 3)} (1 + O(q^{\frac{1}{2} \min(n, n_1, n_2) + l}))
\]

We obtain that
\[
M_k(q, g_1, g_2, g_3) = (-1)^k q(q^2 - 1) \sum_{l=1}^k c(k, l) \sum_{(x, b) \in P_{k,l}} \prod_{i=1}^l \left( 3^{b_i} q + 6 + (-1)^{b_i} 3(q + 2) \right) \frac{4(q + 3)}{4(q + 3)} (1 + O(q^{\frac{1}{2} \min(n, n_1, n_2) + k}))
\]
where the error term is estimated using 5.1.

On the other hand, the corresponding moment of the normalized sum of our random variables is
\[
\mathbb{E} \left( \left( \frac{1 - \sqrt{q}}{1 + q} \sum_{i=1}^{1+q} X_i \right)^k \right) = \frac{1}{(1 + q)^{k/2}} \sum_{l=1}^k \sum_{(i, b) \in A_{k,l}} \mathbb{E}(X_{i_1}^{b_1} ... X_{i_l}^{b_l}),
\]
where
\[
A_{k,l} = \left\{ (i, b) : i = (i_1, ..., i_l), 1 \leq i_j \leq q + 1, i_j's \text{ distinct}, b = (b_1, ..., b_l) \in \mathbb{Z}_{>0}, l \sum b_i = k \right\}
\]
is clearly isomorphic to $P_{k,l}$.
Since 
\[ \mathbb{E}(X_i^b) = \frac{3^b q + 6 + (-1)^b 3(q + 2)}{4(q + 3)} \]
and \( X_1, \ldots, X_{1+q} \) are independent, we get the equality in the statement of the theorem. \( \square \)

6. General case

Proposition 6.1. Let \( C/\mathbb{F}_q \) be a curve with a regular morphism \( \varphi : C \rightarrow \mathbb{P}^1_{\mathbb{F}_q} \) such that 

\[ \text{Gal}(\mathbb{F}_q(C)/\mathbb{F}_q(t)) \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}. \]

We call such a curve \( r \)-quadratic, and an affine model of \( C \) in \( \mathbb{A}^{r+1} \) is given by 

\[ C': \begin{cases} y_i^2 = h_i(t) \\ \vdots \\ y_r^2 = h_r(t) \end{cases} \]

where each \( h_i \) is different from \( \prod_{j \neq i} h_j \) for every non-empty subset \( \{i\} \neq J \subseteq \{1, \ldots, r\} \), and where we take \( h_i \) square-free.

For every non-empty \( J \subseteq \{1, \ldots, r\} \), the affine equation 

\[ y^2 = \prod_{j \in J} h_j(t) \]

defines a quadratic subextension of \( \mathbb{F}_q(C)/k \) and every quadratic subextension of \( \mathbb{F}_q(C)/k \) is obtained in this way, so there are \( 2^r - 1 \) of them.

Write \( C_J \) for the hyperelliptic curve given by the affine equation \( y^2 = \prod_{j \in J} h_j(t) \). Then 

\[ g(C) = \sum_{J \subseteq \{1, \ldots, r\}} g(C_J). \]

Theorem 6.2. There exists a one-to-one correspondence between the set of \( r \)-quadratic extensions of \( k \) and the set of unordered \( 2^r - 1 \)-tuples of square-free and pairwise coprime polynomials.

Proof. Let \( K = k(\sqrt{h_1}, \ldots, \sqrt{h_r}) \) be an \( r \)-quadratic extension. We associate to such an extension, a \( 2^r - 1 \)-tuple \( (f_1, \ldots, f_{2^r-1}) \) of square-free and pairwise coprime polynomials in the following way: for every \( i \in \{1, \ldots, 2^r-1\} \), we write \( x_1^i \ldots x_r^i \) for the representation of the integer \( i \) in base 2 (so \( x_i \in \{1,0\} \) for every \( i \)) and we define \( m_i \) to be the greatest common divisor of all polynomials \( h_j \) such that the \( x_j = 1 \).

We then define the polynomials \( f_i \) as the maximum factor in the decomposition of \( m_i \) which is coprime with all the \( h_j \) such that \( x_j^i = 0 \). Notice that, in particular, \( f_{2^r-1} = (h_1, \ldots, h_r) \).

Viceversa, given a tuple \( (f_1, \ldots, f_{2^r-1}) \) of square-free and pairwise coprime polynomials, we define the \( r \)-quadratic extension \( k(\sqrt{h_1}, \ldots, \sqrt{h_r}) \), where \( h_i \) is defined to be the product of the \( f_j \) such that the \( i \)-th digit of \( j \) in base 2 is 1, i.e. \( x_i^j = 1 \). \( \square \)

Remark 6.3. Notice that, with notations of Theorem 6.2, we have that \( f_{2^r-1} = (h_1, \ldots, h_r) \), and every \( h_i \) can be written as \( h_i = f_{2^r-1} h'_i \) where \( h'_i \) is coprime with \( f_{2^r-1} \) (which is a product of some of the remaining polynomials \( f_1, \ldots, f_{2^r-2} \)). We sometimes denote the polynomial \( f_{2^r-1} \) by \( f \).
After Theorem [6.2], we are led to define the following sets:
\[ \mathcal{F}_{(n_1, \ldots, n_{2r-1})} := \{ (f_1, \ldots, f_{2r-1}) \in \mathcal{F}_{n_1} \times \cdots \times \mathcal{F}_{n_{2r-1}} : (f_i, f_j) = 1, \ i, j = 1, \ldots, 2r-1, i \neq j \}, \]
\[ \tilde{\mathcal{F}}_{(n_1, \ldots, n_{2r-1})} := \{ (f_1, \ldots, f_{2r-1}) \in \tilde{\mathcal{F}}_{n_1} \times \cdots \times \tilde{\mathcal{F}}_{n_{2r-1}} : (f_i, f_j) = 1, \ i, j = 1, \ldots, 2r-1, i \neq j \}, \]

It is easy to prove that if \( C \) is an \( r \)-quadratic curve whose affine model is given by equations \( y_i^2 = h_i(t), \ i = 1, \ldots, r \), then
\[
\#C(\mathbb{F}_q) = \sum_{x \in \mathbb{F}_q^r} \prod_{i=1}^r (1 + \chi(h_i(x))).
\]

Now, we express this formula in terms of the polynomials \( f_1, \ldots, f_{2r-1} \) defined in the proof of Theorem [6.2].

Let us fix \((f_1, \ldots, f_{2r-1}) \in \tilde{\mathcal{F}}_{(n_1, \ldots, n_{2r-1})}\). For every \( i \in \{1, \ldots, 2r-1\} \), we define the polynomial \( p_i \) as the product of the polynomials \( f_j \) such that the relation between the representations in base 2 of \( i \) and \( j \) is the following: \( x_k^i = 1 \Rightarrow x_k^j = 1 \). It is immediate to see that, inside the correspondence of Theorem [6.2], the polynomials \( p_1, \ldots, p_{2r-1} \) define all the quadratic subextensions of the \( r \)-quadratic extension defined by \((f_1, \ldots, f_{2r-1})\).

Then we define:
\[
\tilde{S}(f_1, \ldots, f_{2r-1}) := \sum_{x \in \mathbb{F}_q^r} \sum_{i \in \{1, \ldots, 2r-1\}} \chi(p_i(x))
\]
and we can rewrite
\[
\#C(\mathbb{F}_q) = \sum_{x \in \mathbb{F}_q^r} \prod_{i=1}^{2r-1} (1 + \chi(p_i(x))) = q + 1 + \tilde{S}(f_1, \ldots, f_{2r-1}).
\]

**Lemma 6.4.** Let \( n_1, \ldots, n_\beta \) be positive integers.

For \( 0 \leq l \leq q \) let \( x_1, \ldots, x_l \) be distinct elements of \( \mathbb{F}_q \). Let \( U \in \mathbb{F}_q[X] \) be such that \( U(x_i) \neq 0 \) for \( i = 0, \ldots, l \). Let \( a_1^1, \ldots, a_l^1, \ldots, a_1^\beta, \ldots, a_l^\beta \in \mathbb{F}_q^* \). The number of elements in the set
\[
\{(f_1, \ldots, f_\beta) \in \mathcal{F}_{n_1} \times \cdots \times \mathcal{F}_{n_\beta} : (f_j, U) = 1, \ f_1(x_i) = a_1^i, \ldots, f_\beta(x_i) = a_\beta^i, \ 1 \leq i \leq l, 1 \leq j \leq \beta \}
\]
is the number
\[
R_{n_1, \ldots, n_\beta}(l) = \frac{q^{n_1+\cdots+n_\beta-\beta l}L}{c_q^\beta(2)(1-q^{-2})^{\beta l}} \sum_{P \mid U} \left( \frac{1}{(1+|P|^{-1})^\beta - |P|^{-\beta}} \right) \left( 1 + O\left( q^{l-\min(n_1, \ldots, n_\beta)} \right) \right)
\]
where \( L : = \prod_{P \text{ prime}} \left( 1 - \frac{|P|^{-\beta}}{(1+|P|^{-1})^\beta} \right) \).

**Proof.** By inclusion-exclusion (see [GGL95, Theorem 13.5]), with
\[
f(D) = |\{(f_1, \ldots, f_\beta) \in \mathcal{F}_{n_1} \times \cdots \times \mathcal{F}_{n_\beta} : (f_j, U) = 1, D \mid (f_1, \ldots, f_\beta), D \mid (f_j, f_k), f_j(x_i) = a_j^i, i = 1, \ldots, l, j, k = 1, \ldots, \beta, j \neq k \}|,
\]
\[
g(D) = |\{(f_1, \ldots, f_\beta) \in \mathcal{F}_{n_1} \times \cdots \times \mathcal{F}_{n_\beta} : (f_j, U) = 1, D = (f_1, \ldots, f_\beta) = (f_j, f_k), f_j(x_i) = a_j^i, i = 1, \ldots, l, j, k = 1, \ldots, \beta, j \neq k \}|,
\]
we have
\[
R_{n_1, \ldots, n_\beta}(l) = g(1) = \sum_{D, D(x_i) = 0, (D, U) = 1} \mu(D) f(D).
\]
First observe that if $D \mid (f_1, \ldots, f_\beta)$ then $D \mid (f_i, f_j)$ so it is clear that when $(D, U) = 1$

$$f(D) = | \{(f_1, \ldots, f_\beta) \in \mathcal{F}_{n_1 - \deg(D)} \times \cdots \times \mathcal{F}_{n_\beta - \deg(D)} : (f_j, U D) = 1, f_j(x_i) = a_i^j, 1 \leq i \leq l, 1 \leq j \leq \beta \}|$$

hence Lemma 4.2 implies

$$f(D) = \prod_{j=1}^{\beta} S_{n_j - \deg(D)}^U(l)$$

$$= \frac{q^{n_1 + \cdots + n_\beta - \beta l - \beta \deg(D)}}{\zeta_q^\beta(2)(1 - q^{-2})^\beta} \prod_{P \mid U} (1 + |P|^{-1})^{-\beta} \left( 1 + O(q^{\frac{\deg(D)}{2} - \min(n_1, \ldots, n_\beta)}) \right).$$

So, one has

$$R_{n_1, \ldots, n_\beta}^U(l) = \sum_{D : D(x_i) = 0, (D, U) = 1} \mu(D) g(D) =$$

$$= \frac{q^{n_1 + \cdots + n_\beta - \beta l}}{\zeta_q^\beta(2)(1 - q^{-2})^\beta} \prod_{P \mid U} (1 + |P|^{-1})^{-\beta} \sum_{D(x_i) = 0, (D, U) = 1} \mu(D) |D|^{-\beta} \prod_{P \mid D} (1 + |P|^{-1})^{-\beta} \left( 1 + O(q^{\frac{\deg(D)}{2} - \min(n_1, \ldots, n_\beta)}) \right).$$

Now we observe that

$$\sum_{D(x_i) = 0, (D, U) = 1} \mu(D) |D|^{-\beta} \prod_{P \mid D} (1 + |P|^{-1})^{-\beta} =$$

$$= \sum_{D, D(x_i) = 0, (D, U) = 1} \mu(D) |D|^{-\beta} \prod_{P \mid D} (1 + |P|^{-1})^{-\beta} + O(q^{-\beta \min(n_1, \ldots, n_\beta)}),$$

where we have that

$$\sum_{D, D(x_i) = 0, (D, U) = 1} \mu(D) |D|^{-\beta} \prod_{P \mid D} (1 + |P|^{-1})^{-\beta} =$$

$$= \left( \frac{(1 + q^{-1})^\beta - q^{-\beta}}{(1 + q^{-1})^\beta} \right)^{-l} \prod_{P \mid U} \left( \frac{(1 + |P|^{-1})^\beta - |P|^{-\beta}}{(1 + |P|^{-1})^\beta} \right)^{-1} \prod_{P \text{ prime}} \left( 1 - \frac{|P|^{-\beta}}{(1 + |P|^{-1})^\beta} \right) =$$

$$= \left( \frac{(1 + q^{-1})^\beta - q^{-\beta}}{(1 + q^{-1})^\beta} \right)^{-l} \prod_{P \mid U} \left( \frac{(1 + |P|^{-1})^\beta - |P|^{-\beta}}{(1 + |P|^{-1})^\beta} \right)^{-1} L.$$
Proposition 6.5. Let $0 \leq l \leq q$, let $x_1, \ldots, x_l$ be distinct elements of $\mathbb{F}_q$, and $a^1_1, \ldots, a^1_l, \ldots, a^r_1, \ldots, a^r_l \in \mathbb{F}_q^*$. Then for any $1 > \epsilon > 0$, we have

$$\left|\{(f_1, \ldots, f_{2^r-1}) \in \mathcal{F}(n_1, \ldots, n_{2^r-1}) : f_{2^r-1}(x_i)h'_j(x_i) = a^j_i, i = 1, \ldots, l, j = 1, \ldots, r\}\right| =$$

$$= \frac{q^{n_1+\cdots+n_r-n_{2^r-1}-sl}L}{\zeta_q(2)^s(1-q^{-2})^s} \sum_{U \in \mathcal{F}_{n_{2^r-1}}} \frac{1}{(1+q^{-1})^s-q^{-s}} \prod_{U(x_i) \neq 0} \frac{1}{P(U)(1+P^{-1})^{s-1}+O(q^{n_1+\cdots+n_r-n_{2^r-1}+s})},$$

where $K := \prod_{P} \left|\frac{|P|}{|P|+1}\right|^s$ and $s := 2^r - 2$.

Proof. We observe that

$$\left|\{(f_1, \ldots, f_{2^r-1}) \in \mathcal{F}(n_1, \ldots, n_{2^r-1}) : f_{2^r-1}(x_i)h'_j(x_i) = a^j_i\}\right| =$$

$$= \sum_{f_{2^r-1} \in \mathcal{F}_{n_{2^r-1}} \setminus \{(f_1, \ldots, f_{2^r-1}) \in \mathcal{F}_{n_1} \times \cdots \times \mathcal{F}_{n_r} : f \in \mathcal{F}_{n_{2^r-1}}, f(x_i) \neq 0\}} \sum_{h'_j(x_i) = a^j_i} 1 = \sum_{f \in \mathcal{F}_{n_{2^r-1}} : f(x_i) \neq 0} R_{f_{2^r-1}}^f(l).$$

Using Lemma 6.4, we have that

$$\left|\{(f_1, \ldots, f_{2^r-1}) \in \mathcal{F}(n_1, \ldots, n_{2^r-1}) : f_{2^r-1}(x_i)h'_j(x_i) = a^j_i\}\right| =$$

$$= \frac{q^{n_1+\cdots+n_r-s}L}{\zeta_q(2)^s(1-q^{-2})^s} \sum_{U \in \mathcal{F}_{n_{2^r-1}}} \frac{1}{(1+q^{-1})^s-q^{-s}} \prod_{U(x_i) \neq 0} \frac{1}{P(U)(1+P^{-1})^{s-1}+O(q^{n_1+\cdots+n_r-n_{2^r-1}+s})},$$

where for any polynomial $U$,

$$c(U) = \begin{cases} \mu^2(U) \prod_{P \mid U} \frac{1}{(1+P^{-1})^{s-1}} & U(x_i) \neq 0 \\ 0 & \text{otherwise}. \end{cases}$$

To evaluate $\sum_{\deg(U)=n_{2^r-1}} c(U)$, we consider the Dirichlet series

$$G(w) := \sum_{U \mid \deg(U)=n_{2^r-1}} c(U) = \prod_{P, P(x_i) \neq 0} \left(1 + \frac{1}{|P|^s} \cdot \frac{|P|^s}{(|P|+1)^s-1}\right) =$$

$$= \frac{\zeta_q(w)}{\zeta_q(2w)} H(w) \left(1 + \frac{1}{q^w(1+q^{-1})^s-q^{-w-s}}\right)^{-l},$$

where

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

We can see that $G(w)$ has simple pole at $w = 1$ with residue

$$\frac{H(1)\operatorname{Res}_{w=1} \zeta_q(w)}{\zeta_q(2)} \left(1 + \frac{1}{q^s} \cdot \frac{q^s}{(q+1)^s-1}\right)^{-l} = \frac{K}{\zeta_q(2) \log q} \left(1 + \frac{1}{q} \cdot \frac{q^s}{(q+1)^s-1}\right)^{-l}.$$
Using [Ros02, Theorem 17.1] we have that
\[ \sum_{\text{deg}(U) = n_{2r-1}} c(U) = \frac{K}{\zeta(2)} \left( \frac{q^\epsilon}{q(q+1)^{s} - 1} \right)^{-l} q^{n_{2r-1}} + O_q(q^{\epsilon n_{2r-1}}), \]
for all \( \epsilon \geq 0 \) and where, looking at the proof of the theorem and proceeding as in Proposition 4.3 in [BDFL09], we can exchange \( O_q(q^{\epsilon n_{2r-1}}) \) by \( O(q^{\epsilon n_{2r-1} + l}) \).

Finally, applying Proposition 6.5 as we did in Section 4, we obtain the following generalization of Theorem 4.1.

**Theorem 6.6.** In the limit when the degrees \( n_1, \ldots, n_{2r-1} \) go to infinity
\[
\frac{|\{(f_1, \ldots, f_{2r-1}) \in \hat{F}(n_1, \ldots, n_{2r-1}) : \hat{S}(f_1, \ldots, f_{2r-1}) = M\}|}{|\hat{F}(n_1, \ldots, n_{2r-1})|} = \text{Prob} \left( \sum_{j=1}^{q+1} X_j = M \right)
\]
where the \( X_j \) are i.i.d. random variables such that
\[
X_i = \begin{cases} 
-1 & \text{with probability } \frac{2^{r-1} q^{2r-1} P}{2^r} \\
2^{r-1} - 1 & \text{with probability } \frac{2^{r-1} P}{2^r} \\
2^r - 1 & \text{with probability } \frac{1 - 2^{r-1} P}{2^r}
\end{cases}
\]
where we define
\[
P := \frac{2^{r-1} (q - 1) 2^{r-1} q^{2r-2}}{(q^2 - 1)^{2r-1} - \sum_{j=2}^{2r-1} \binom{2r-1}{j} (q - 1)^{2r-1} q^{2r-1-j}}.
\]

Observe that Theorem 6.6 specializes to Theorem 1.1 of [BDFL09] when \( r = 1 \) and to Theorem 4.1 of the present paper when \( r = 2 \).

**References**

[BDFL09] A. Bucur, C. David, B. Feigon, and M. Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, Int. Math. Res. Not. (2009).

[BDFL11] A. Bucur, C. David, B. Feigon, and M. Lalín, *Biased statistics for traces of cyclic \( p \)-fold covers over finite fields*, WIN – Women in Number, Fields Institute Communications, American Mathematical Society, (2011).

[BDF+15] A. Bucur, C. David, B. Feigon, N. Kaplan, M. Lalín, E. Ozman, and M. Wood, *The distribution of points on cyclic covers of genus \( g \)*, (submitted) (2015).

[Bil95] P. Billingsley, *Probability and measure*, Wiley Series in Probability and Mathematical Statistics, New York: John Wiley, 1995.

[DS94] P. Diaconis and M. Shahshahani, *On the eigenvalues of random matrices*, J. Appl. Probab. 31A (1994), 49–62.

[GGL95] R. L. Graham, M. Grotschel, and L. Lovasz, *Handbook of combinatorics*, volume 2, 1995.

[Har77] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.
[KR09] P. Kurlberg and Z. Rudnick, *The fluctuation in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory 129 (2009), no. 3, 580–587.

[KS99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[LS96] H. W. Lenstra and P. Stevenhagen, *Chebotarëv and his density theorem*, The Mathematical Intelligencer 18 (1996), 26–37.

[PG05a] R. Pries and D. Glass, *Hyperelliptic curves with prescribed p-torsion*, Manuscripta 117 (2005), no. 3, 299–317.

[PG05b] R. Pries and D. Glass, *On the moduli space of Klein four covers of the projective line*, Computational Aspects of Algebraic Curves, Lecture Notes Series in Computing 13 (2005).

[Ros02] M. Rosen, *Number theory in function fields*, XI, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

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

[Xio10] M. Xiong, *The fluctuations in the number of points on a family of curves over a finite field*, Journal de Théorie de Nombres de Bordeaux 3 (2010), 755–769.

**Universiteit Leiden, Mathematisch Instituut, Niels Bohrweg 1, 2333 CA Leiden (The Netherlands)**

E-mail address: e.lorenzo.garcia@math.leidenuniv.nl

**Università degli Studi “Roma Tre”, Dipartimento di Matematica e Fisica, Largo San Leonardo Murialdo 1, 00146 Roma (Italy)**

E-mail address: meleleo@mat.uniroma3.it

**Universitat de Barcelona, Departament d’Àlgebra i Geometria, Gran Via de les Corts Catalanes 585, 08005 Barcelona (Spain)**

E-mail address: pmilione@ub.edu