Math. Res. Lett. **19** (2012), *no.* 02, 255–272

STATISTICS OF THE JACOBIANS OF HYPERELLIPTIC CURVES OVER FINITE FIELDS

Maosheng Xiong and Alexandru Zaharescu

Abstract. Let C be a smooth projective curve of genus $g \geq 1$ over a finite field $\mathbb{F}_q$ of cardinality q. Denote by $\#\mathcal{J}_C$ the size of the Jacobian of C over $\mathbb{F}_q$. We first obtain an estimate on $\#\mathcal{J}_C$ when $\mathbb{F}_q(C)/\mathbb{F}_q(X)$ is a geometric Galois extension, which improves a general result of Shparlinski [19]. Then we study the behavior of the quantity $\#\mathcal{J}_C$ as C varies over a large family of hyperelliptic curves of genus g. When g is fixed and $q \to \infty$, its limiting distribution is given by the powerful theorem of Katz and Sarnak in terms of the trace of a random matrix. When q is fixed and the genus $g \to \infty$, we also find explicitly the limiting distribution and show that the result is consistent with that of Katz and Sarnak when both $q, g \to \infty$.

1. Introduction

Let C be a smooth projective curve of genus $g \geq 1$ over a finite field $\mathbb{F}_q$ of cardinality q. The Jacobian $\mathrm{Jac}(C)$ is a g-dimensional abelian variety. The set of the $\mathbb{F}_q$-rational points on $\mathrm{Jac}(C)$, denoted by $\mathcal{J}_C = \mathrm{Jac}(C)(\mathbb{F}_q)$, is a finite abelian group. The group $\mathcal{J}_C$ has been studied extensively, partly because of its importance in the theory of algebraic curves and its surprising applications in public-key cryptography and computational number theory. For example, such groups are extremely useful in primality testing [3] and integer factorization [12, 13]. Statistics of group structures of $\mathcal{J}_C$, for instance the analog of the Cohen–Lenstra conjecture over function fields remains an inspiring problem in number theory and provides insight for number fields case. Interested readers may refer to [1, 2, 22] for details and current development. The main purpose of this paper is to study $\#J_C$, the size of the Jacobian over $\mathbb{F}_q$. This quantity is also the class number of the function field $\mathbb{F}_q(C)$ [17, Theorem 5.9], a subject of study with a rich history.

The zeta function of $C/\mathbb{F}_q$ is a rational function of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)},$$

where $P_C(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$ with $P_C(0) = 1$, satisfying a functional equation and having all its zeros on the circle $|u| = 1/\sqrt{q}$ (the Riemann hypothesis for curves [23]). Moreover, there is a unitary symplectic matrix $\Theta_C \in \mathrm{USp}(2g)$, defined up to conjugacy, so that

$$P_C(u) = \det\left(I - u\sqrt{q}\Theta_C\right).$$

The eigenvalues of Θ_C are of the form $e\left(\theta_{C,j}\right), j = 1, \ldots, 2g$, where $e(\theta) = e^{2\pi i\theta}$.

Received by the editors xxx.

2000 *Mathematics Subject Classification.* 11G20, 11T55, 11M38.

Key words and phrases. zeta functions of curves, class number, Jacobian, Gaussian distribution.

It is known that $\#\mathcal{J}_C = P_C(1)$ (see [14, Corollary VIII.6.3]). From this we immediately derive that

$$(q^{1/2}-1)^{2g} \le \#\mathcal{J}_C \le (q^{1/2}+1)^{2g},$$

which is tight in the case $g = 1$ due to the classical result of Deuring [6]. Many improvements of this bound have been obtained in [15, 16, 19–21]. In particular in an interesting paper [19], Shparlinski proves that if C is a smooth absolutely irreducible curve of genus g over $\mathbb{F}_q$ with gonality d, then

$$\log \#\mathcal{J}_C = g\log q + O\left(g\log^{-1}(g/d)\right) \tag{1.1}$$

as $g \to \infty$, where the implied constant may depend on q. (The gonality of a curve C is the smallest integer d such that C admits a non-constant map of degree d to the projective line over the ground field $\mathbb{F}_q$. For example, a hyperelliptic curve is a curve given by an affine model $Y^2 = F(X)$ for some $F \in \mathbb{F}_q[X]$, so the gonality is $d = 2$.) This generalizes and improves similar results of Tsfasman [21].

In this paper, we first prove that if the function field $\mathbb{F}_q(C)$ is a geometric Galois extension of $\mathbb{F}_q(X)$, a sharper estimate can be obtained. Here "geometric" means that the constant field of $\mathbb{F}_q(C)$ is still $\mathbb{F}_q$.

Theorem 1.1. *Let C be a smooth projective curve of genus $g \ge 1$ over $\mathbb{F}_q$. Assume that the function field $\mathbb{F}_q(C)$ is a geometric Galois extension of the rational function field $\mathbb{F}_q(X)$ with $N = \#\mathrm{Gal}\left(\mathbb{F}_q(C)/F(X)\right)$. Then*

$$|\log \#\mathcal{J}_C - g\log q| \le (N-1)\left(\log\max\left\{1, \frac{\log(7g/(N-1))}{\log q}\right\} + 3\right). \tag{1.2}$$

We remark that under the condition of Theorem 1.1, the gonality of the curve clearly satisfies $d \le N$, and the quantity $|\log \#\mathcal{J}_C - g\log q|$ is essentially bounded by $O(\log\log g)$, which is significantly smaller than $O(g/\log g)$ implied from (1.1).

Next we will study how the value $(\log \#\mathcal{J}_C - g\log q)$ fluctuates when C varies inside a family. More precisely, assume that q is odd. For each positive integer $d \ge 3$, denote by $\mathcal{H}_{d,q}$ the family of hyperelliptic curves having an affine equation of the form $Y^2 = F(X)$, with $F \in \mathbb{F}_q[X]$ a monic square-free polynomials of degree d. The genus of a curve $C \in \mathcal{H}_{d,q}$ is given by

$$g = g(C) = \left[\frac{d-1}{2}\right],$$

where for $x \in \mathbb{R}$, $[x]$ denotes the largest integer not exceeding x. For any $C \in \mathcal{H}_{d,q}$, since $\mathbb{F}_q(C)/\mathbb{F}_q(X)$ is a geometric Galois extension with Galois group $\mathbb{Z}/2\mathbb{Z}$, Theorem 1.1 implies that

$$|\log \#\mathcal{J}_C - g\log q| \le \log\max\left\{1, \log\frac{\log(7g)}{\log q}\right\} + 3.$$

We study how the value $(\log \#\mathcal{J}_C - g\log q)$ is distributed as C varies over the family $\mathcal{H}_{d,q}$. The measure on $\mathcal{H}_{d,q}$ is simply the uniform probability measure on the set of such polynomials.

Writing

$$P_C(u) = \prod_{i=1}^{2g} \left(1 - \sqrt{q} e\left(\theta_{C,i}\right) u\right),$$

then

$$\log \#\mathcal{J}_C - g \log q = \sum_{i=1}^{2g} \log\left(1 - q^{-1/2} e(\theta_{C,i})\right).$$

Katz and Sarnak [10] showed that for fixed genus g, the conjugacy classes $\{\Theta_C\colon C \in \mathcal{H}_{d,q}\}$ become uniformly distributed in $\mathrm{USp}(2g)$ in the limit $q \to \infty$. In particular, since

$$\lim_{q\to\infty} \sqrt{q}\left(\log \#\mathcal{J}_C - g\log q\right) = -\sum_{i=1}^{2g} e(\theta_{C,i}),$$

it implies that

(i) When g is fixed and $q \to \infty$, the value $-\sqrt{q}\left(\log \#\mathcal{J}_C - g \log q\right)$ for $C \in \mathcal{H}_{d,q}$ is distributed asymptotically as the trace of a random matrix in $\mathrm{USp}(2g)$.

Furthermore, since the limiting distribution of traces of a random matrix in $\mathrm{USp}(2g)$, as $g \to \infty$, is a standard Gaussian by a theorem of Diaconis and Shahshahani [7], it also implies that

(ii) If $q \to \infty$ and then $g \to \infty$, the value $\sqrt{q}\left(\log \#\mathcal{J}_C - g \log q\right)$ is distributed as a standard Gaussian.

Katz and Sarnak's powerful theorem [10] provides an almost complete answer, except that in their argument, it is crucial to take the limit that $q \to \infty$. What happens if $g \to \infty$ instead? Complementary to (i) and (ii) above, we prove the following.

Theorem 1.2. *(1) If q is fixed and $g \to \infty$, then for $C \in \mathcal{H}_{d,q}$, the quantity $\log \#\mathcal{J}_C - g \log q + \delta_{d/2} \log\left(1 - q^{-1}\right)$ converges weakly to a random variable X, whose characteristic function $\phi(t) = \mathbb{E}\left(e^{itX}\right)$ is given by*

$$\phi(t) = 1 + \sum_{r=1}^{\infty} \frac{1}{r!} \sum_{\substack{P_1,\dots,P_r\\ \text{distinct}}} \prod_{j=1}^{r} \frac{\left(1 - |P_j|^{-1}\right)^{-it} + \left(1 + |P_j|^{-1}\right)^{-it} - 2}{2\left(1 + |P_j|^{-1}\right)}, \quad \forall t \in \mathbb{R},$$

where we denote

$$\delta_\gamma = \begin{cases} 1, & \gamma \in \mathbb{Z}, \\ 0, & \gamma \notin \mathbb{Z}, \end{cases}$$

and the sum on the right is over all distinct monic irreducible polynomials $P_1, \dots, P_r \in \mathbb{F}_q[X]$ and $|P_j| = q^{\deg P_j}$.

(2) If both $q, g \to \infty$, then for $C \in \mathcal{H}_{d,q}$, $\sqrt{q}\left(\log \#\mathcal{J}_C - g \log q\right)$ is distributed as a standard Gaussian, that is, for any $\gamma \in \mathbb{R}$, we have

$$\lim_{\substack{q\to\infty\\ g\to\infty}} \frac{1}{\#\mathcal{H}_{d,q}} \#\left\{C \in \mathcal{H}_{d,q} : \sqrt{q}\left(\log \#\mathcal{J}_C - g\log q\right) \le \gamma\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-\frac{t^2}{2}}\, dt.$$

Remark 1.1. (1) Kurlberg and Rudnick [11] and Faifman and Rudnick [8] initiated the investigation of such problems under the limit that q is fixed and $g \to \infty$. Bucur *et al.* [4, 5] made further important development. Theorem 1.2 is similar to their work. Theorem 1.2 can also be considered as a function field analog of the distribution of $L(1,\chi_d)$ (over $\mathbb{Q}$) investigated by Granville and Soundararajan in [9]. The proof of Theorem 1.2 borrows techniques developed by Rudnick [18] and Faifman and Rudnick [8].

(2) Statement (2) of Theorem 1.2 is more general than statement (ii) which could be derived from the theorem of Katz and Sarnak because there is no requirement that $q \to \infty$ first.

(3) Instead of averaging over $\mathcal{H}_{d,q}$, the proof can be easily adapted to the moduli space of hyperelliptic curves of a fixed genus. Interested readers may refer to [4, 5] for terminology and treatment.

(4) The authors are grateful to Alina Bucur for suggesting the following insightful heuristics: First notice $\#\mathcal{J}_C = P_C(1)$ and by the functional equation

$$P_C(1) = q^g P_C(1/q) = q^g \frac{Z_C(1/q)}{Z_{\mathbb{P}^1}(1/q)}.$$

The Euler product expansion of $Z_C(u)/Z_{\mathbb{P}^1}(u)$ converges absolutely at $u = 1/q$, so we can write $\#\mathcal{J}_C$ as q^g times a product over Euler factors corresponding to monic irreducible polynomials evaluated at $1/q$. Explicitly, for P a monic irreducible polynomial, the corresponding Euler factor evaluated at $1/q$ will be

$$\begin{cases} \left(1-|P|^{-1}\right)^{-1} & \text{if } C \text{ splits at } P, \\ \left(1+|P|^{-1}\right)^{-1} & \text{if } C \text{ is inert at } P, \\ 1 & \text{if } C \text{ ramifies at } P. \end{cases}$$

This suggests that the difference $\log \#\mathcal{J}_C - g \log q$ should be modeled by a sum of i.i.d. random variables, one for each monic irreducible polynomials. In this model, the probability that C ramifies the above some polynomial P is computed in the usual way: the residue field at P has $r = |P|$ elements, so that probability of ramification is $(r-1)/(r^2-1) = 1/(r+1) = (1+|P|)^{-1}$. This is counting the reductions modulo P^2 that are not zero, but are divisible by P of the defining polynomial of the curve. The split and inert cases occur with equal probability, namely $\frac{|P|}{2(1+|P|)}$. Thus the random variable corresponding to P has characteristic function

$$\phi_P(t) = \frac{1}{1+|P|} + \left(1-|P|^{-1}\right)^{-it} \frac{|P|}{2(1+|P|)} + \left(1+|P|^{-1}\right)^{-it} \frac{|P|}{2(1+|P|)}.$$

One can check that

$$\phi(t) = \prod_P \phi_P(t),$$

which confirms statement (1) of Theorem 1.2.

2. Preliminaries

In this section we collect several results which will be used later. Interested readers can refer to [17] for more details.

2.1. Zeta functions of function fields. Let $K = \mathbb{F}_q(X)$ be the rational function field over the finite field $\mathbb{F}_q$ and let L/K be a finite geometric Galois extension. Here "geometric" means that the constant field of L is still $\mathbb{F}_q$. We list several facts about such extensions L/K as follows (see [17, Chapter 9] for more details).

First, the zeta function $\zeta_L(s)$ of L is defined by

$$\zeta_L(s) = \prod_{P\in\mathcal{S}_L} \left(1 - |P|^{-s}\right)^{-1},$$

where the product is over $\mathcal{S}_L$, the set of all primes of L, and for each $P \in \mathcal{S}_L$, $|P|$ is the cardinality of the residue field of L at P. For the rational function field K, the zeta function $\zeta_K(s)$ turns out to be

$$\zeta_K(s) = \left(1 - q^{-s}\right)^{-1} \left(1 - q^{1-s}\right)^{-1}.$$

If C is a smooth projective curve of genus $g \geq 1$ over $\mathbb{F}_q$ with function field $\mathbb{F}_q(C) = L$, then $Z_C\left(q^{-s}\right) = \zeta_L(s)$, i.e., the zeta function of the curve C coincides with the zeta function of the function field $\mathbb{F}_q(C)$ (see [17, p. 57, Chapter 5] for details).

Let $G = \mathrm{Gal}(L/K)$ be the Galois group of L/K and $\rho : G \to \mathrm{Aut}_{\mathbb{C}}(V)$ a representation of G, where V is a finite-dimensional vector space over the complex numbers $\mathbb{C}$ of dimension m. One defines the Artin L-series associated to the representation ρ as follows.

If P is a prime of K which is unramified in L and $\mathcal{B}$ is a prime of L lying above P, one defines the local factor $L_P(s, \rho)$ as

$$L_P(s,\rho) = \det\left(I - \rho((\mathcal{B}, L/K))|P|^{-s}\right)^{-1}, \tag{2.1}$$

where I is the identity automorphism on V and $(\mathcal{B}, L/K) \in G$ is the Frobenius automorphism at $\mathcal{B}$. Since L/K is Galois, this definition does not depend on the choice of $\mathcal{B}$ over P.

Let $\{\alpha_1(P), \alpha_2(P), \ldots, \alpha_m(P)\}$ be the eigenvalues of $\rho((\mathcal{B}, L/K))$. In terms of these eigenvalues, we get another useful expression for $L_P(s,\rho)$:

$$L_P(s,\rho)^{-1} = \left(1 - \alpha_1(P)|P|^{-s}\right)\left(1 - \alpha_2(P)|P|^{-s}\right)\cdots\left(1 - \alpha_m(P)|P|^{-s}\right).$$

We note that these eigenvalues $\alpha_i(P)$ are all roots of unity because $(\mathcal{B}, L/K)$ has finite order.

At a prime P of K which is ramified in L, the local factor $L_P(s,\rho)$ can also be defined. The definition is similar to (2.1), except that the action $\rho((\mathcal{B}, L/K))$ is restricted to a subspace of V which is fixed by the inertial group $I(\mathcal{B}/P)$. We are contended with the fact that there are only finitely many primes P which are ramified in L and in either case we can write $L_P(s,\rho)$ as

$$L_P(s,\rho)^{-1} = \left(1 - \alpha_1(P)|P|^{-s}\right)\left(1 - \alpha_2(P)|P|^{-s}\right)\cdots\left(1 - \alpha_m(P)|P|^{-s}\right),$$

where the values $\alpha_i(P)$'s are either roots of unity or zero. The Artin L-series $L(s,\rho)$ is defined by the infinite product

$$L(s,\rho) = \prod_{P\in\mathcal{S}_K} L_P(s,\rho),$$

where $\mathcal{S}_K$ is the set of all primes in $K = \mathbb{F}_q(X)$.

It is known that if $\rho = \rho_0$, the trivial representation, then $L(s, \rho_0) = \zeta_K(s)$, and if $\rho = \rho_{\mathrm{reg}}$, the regular representation, then $L(s, \rho_{\mathrm{reg}}) = \zeta_L(s)$. It is also known that $L(s,\rho)$ depends only on the character χ of ρ, so we can write it as $L(s,\chi)$.

Finally, let L/K be a finite, geometric and Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Let $\{\chi_1, \chi_2, \dots, \chi_h\}$ be the set of irreducible characters of G. We set $\chi_1 = \chi_0$, the trivial character. Denote by d_i the degree of χ_i, i.e., $d_i = \chi_i(e)$ is the dimension of the representation space corresponding to χ_i. Then using results about group characters and formal properties of Artin L-series, one derives that

$$\zeta_L(s) = \zeta_K(s) \prod_{i=2}^{h} L(s, \chi_i)^{d_i}. \tag{2.2}$$

2.2. Averaging over $\mathcal{H}_{d,q}$. Let $\mathcal{H}_{d,q} \subset \mathbb{F}_q[X]$ be the set of all monic square-free polynomials of degree $d \geq 3$.

Lemma 2.1. *For any Dirichlet character $\chi : \mathbb{F}_q[X] \to \mathbb{C}$ modulo $f \in \mathbb{F}_q[X]$, we have*

$$\frac{1}{\#\mathcal{H}_{d,q}} \sum_{F \in \mathcal{H}_{d,q}} \chi(F) \leq \frac{2^{\deg f - 1}}{(1 - q^{-1})\, q^{d/2}}.$$

Proof. This is [8, Lemma 3.1], which proves the case when $\chi = \left(\frac{f}{\cdot}\right)$ is a quadratic character. For the general case, the proof follows exactly the same line of argument, so we omit the details here. □

Lemma 2.2. *Let $h \in \mathbb{F}_q[X]$ be a monic square-free polynomial. Then*

$$\frac{1}{\#\mathcal{H}_{d,q}} \sum_{\substack{F \in \mathcal{H}_{d,q} \\ \gcd(F,h)=1}} 1 = \prod_{P|h} \left(1 + |P|^{-1}\right)^{-1} + O\left(q^{-d/2}\sigma(h)\right),$$

where $\sigma(h) = \sum_{D|h} 1$.

Proof. This is essentially [18, Lemma 5], which treats the case that $h = P$ is a monic irreducible polynomial. In fact in this case Rudnick [18, Lemma 5] yields a much stronger error term $O(q^{-d})$. The extra saving is obtained by carefully analyzing the functional equation of the zeta function. To obtain the error term $O(q^{-d/2}\sigma(h))$, the proof follows a standard procedure which is included [18, Lemma 5]. We also omit details here. □

3. Proof of Theorem 1.1

Let C be a smooth projective curve of genus $g \geq 1$ over $\mathbb{F}_q$. The zeta function $Z_C(u)$ is of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)},$$

where $P_C(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$ with $P_C(0) = 1$, satisfying the functional equation

$$P_C(u) = \left(qu^2\right)^g P_C\left(\frac{1}{qu}\right),$$

and having all its zeros on the circle $|u| = 1/\sqrt{q}$. We may write $P_C(u)$ as

$$P_C(u) = \prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)u\right),$$

where these $\theta_i \in [0,1)$ and $e(\alpha)$ stand for $e^{2\pi i\alpha}$ for any $\alpha \in \mathbb{R}$.

Since $\#\mathcal{J}_C = P_C(1)$, we have

$$\#\mathcal{J}_C = \prod_{i=1}^{2g} (1 - \sqrt{q}e(\theta_i)) = q^g \prod_{i=1}^{2g} \left(1 - q^{-1/2}e(\theta_i)\right).$$

Taking logarithms on both sides and using the expansion

$$-\log(1-z) = \sum_{n\geq 1} \frac{z^n}{n}, \quad |z| < 1, \tag{3.1}$$

we obtain the equation

$$\log \#\mathcal{J}_C - g\log q = \sum_{n\geq 1} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e(n\theta_i). \tag{3.2}$$

Denote $L = \mathbb{F}_q(C)$ and $K = \mathbb{F}_q(X)$. The zeta functions of L and K can be written as

$$\zeta_L(s) = (1-q^{-s})^{-1}(1-q^{1-s})^{-1} \prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)q^{-s}\right),$$

and

$$\zeta_K(s) = (1-q^{-s})^{-1}(1-q^{1-s})^{-1}.$$

Since L/K is a geometric Galois extension with $G = \mathrm{Gal}(L/K)$ and $\#G = N$, let $\{\chi_1, \chi_2, \ldots, \chi_h\}$ be the set of irreducible characters of G with $\chi_1 = \chi_0$, the trivial character and denote by d_i the degree of χ_i. From (2.2) we find that

$$\prod_{i=2}^{h} L(s,\chi_i)^{d_i} = \prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)q^{-s}\right), \tag{3.3}$$

where for each i with $2 \leq i \leq h$, the Artin L-series associated to χ_i can be written as

$$L(s,\chi_i)^{-1} = \prod_{P} \left(1 - \alpha_{i,1}(P)|P|^{-s}\right)\left(1 - \alpha_{i,2}(P)|P|^{-s}\right)\cdots\left(1 - \alpha_{i,d_i}(P)|P|^{-s}\right).$$

Here the product is over all monic irreducible polynomials $P \in \mathbb{F}_q(X)$ and $P = \infty$ with $|P| = q^{\deg P}$ ($\deg\infty = 1$ hence $|\infty| = q$) and these $\alpha_{i,j}(P)$'s are either roots of unity or zero.

Taking logarithms on both sides of (3.3), using the expansion (3.1) again and equating the coefficients, we obtain for any positive integer n the identity

$$q^{n/2} \sum_{j=1}^{2g} -e(n\theta_i) = \sum_{\deg f = n} \Lambda(f) \sum_{i=2}^{h} d_i \sum_{j=1}^{d_i} \alpha_{i,j}(f), \tag{3.4}$$

where the sum on the right side over $\deg f = n$ is over all monic polynomials $f \in \mathbb{F}_q[X]$ with $\deg f = n$, $\Lambda(f) = \deg P$ if $f = P^k$ is a prime power, and $\Lambda(f) = 0$ otherwise.

Let Z be a positive integer which will be chosen later. Denote

$$\epsilon_{1,Z} = \sum_{n\leq Z} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e(n\theta_i)$$

and

$$\epsilon_{2,Z} = \sum_{n>Z} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e(n\theta_i).$$

From (3.2) we can write

$$\log \#\mathcal{J}_C - g \log q = \epsilon_{1,Z} + \epsilon_{2,Z}.$$

If $Z \geq 2$ we have

$$|\epsilon_{2,Z}| \leq \sum_{n \geq Z+1} q^{-n/2} n^{-1} 2g \leq \frac{2g}{Z+1} q^{-(Z+1)/2} \left(1 - q^{-1/2}\right)^{-1}, \tag{3.5}$$

and if $Z = 1$ we have

$$|\epsilon_{2,Z}| \leq 2g \left(-\log\left(1 - q^{-1/2}\right) - q^{-1/2}\right) \leq \frac{2g}{q - \sqrt{q}}. \tag{3.6}$$

For $\epsilon_{1,Z}$, we use the identity (3.4). Since $|\alpha_{i,j}| \leq 1$ for all i, j, we obtain the inequality

$$|\epsilon_{1,Z}| \leq \sum_{n \leq Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f) \sum_{i=2}^{h} d_i^2.$$

It is known that

$$1 + \sum_{i=2}^{h} d_i^2 = N = \#G$$

and

$$\sum_{\deg f = n} \Lambda(f) = q^n + 1.$$

Here the extra "1" on the right side in the above equation accounts for $f = \infty^n$. Hence

$$|\epsilon_{1,Z}| \leq (N-1) \left(\sum_{n \leq Z} \frac{1}{n} + \sum_{n \leq Z} \frac{1}{nq^n} \right).$$

If $Z = 1$, this is

$$|\epsilon_{1,Z}| \leq (N-1)\left(1 + q^{-1}\right), \tag{3.7}$$

and if $Z \geq 2$, we use

$$\sum_{n \leq Z} \frac{1}{n} \leq 1.5 + \log Z - \log 2$$

and

$$\sum_{n \leq Z} \frac{1}{nq^n} \leq -\log\left(1 - q^{-1}\right) \leq \frac{1}{q-1}$$

to obtain

$$|\epsilon_{1,Z}| \leq (N-1) \left(1.5 - \log 2 + \frac{1}{q-1} + \log Z\right), \quad Z \geq 2. \tag{3.8}$$

Case 1: If $2\left(1-q^{-1/2}\right)^{-1} g \geq (N-1)q$, we choose

$$Z = \left[\frac{2\log \frac{2\left(1-q^{-1/2}\right)^{-1} g}{N-1}}{\log q}\right] \geq 2.$$

We find from (3.8) that

$$|\epsilon_{1,Z}| \leq (N-1)\left\{1.5 + \frac{1}{q-1} + \log\left(\frac{\log \frac{2\left(1-q^{-1/2}\right)^{-1} g}{N-1}}{\log q}\right)\right\}$$

and from (3.5) that

$$|\epsilon_{2,Z}| \leq \frac{N-1}{2}.$$

In this case noticing that $q \geq 2$, we obtain

$$|\log \#\mathcal{J}_C - g\log q| \leq (N-1)\left(\log\left(\frac{\log \frac{7g}{N-1}}{\log q}\right) + 3\right).$$

Case 2: If $2\left(1-q^{-1/2}\right)^{-1} g < (N-1)q$, we choose $Z = 1$, and from (3.7) and (3.6) we obtain that

$$|\log \#\mathcal{J}_C - g\log q| \leq (N-1)\left(2 + q^{-1}\right) < 3(N-1).$$

In either case we conclude that

$$|\log \#\mathcal{J}_C - g\log q| \leq (N-1)\left(\log\max\left\{1, \frac{\log(7g/(N-1))}{\log q}\right\} + 3\right).$$

This completes the proof of Theorem 1.1. □

4. Proof of Theorem 1.2

4.1. Preparation. Let $\mathbb{F}_q$ be a finite field of cardinality q with q odd. Denote

$$\mathcal{H}_{d,q} = \left\{F \in \mathbb{F}_q[X] : F \text{ is monic, square-free and} \deg F = d\right\}.$$

For any $F \in \mathcal{H}_{d,q}$, the hyperelliptic curve C_F is given by the affine model

$$C_F : Y^2 = F(X).$$

It has genus

$$g = g_F = \left[\frac{d-1}{2}\right].$$

Suppose that the zeta function $Z_{C_F}(u)$ is of the form

$$Z_{C_F}(u) = \frac{\prod_{i=1}^{2g}\left(1-\sqrt{q}e\left(\theta_{i,F}\right)u\right)}{(1-u)(1-qu)},$$

where the $\theta_{i,F}$'s are real numbers. Then

$$\#\mathcal{J}_{C_F} = \prod_{i=1}^{2g}\left(1-\sqrt{q}e\left(\theta_{i,F}\right)\right) = q^g \prod_{i=1}^{2g}\left(1-q^{-1/2}e\left(\theta_{i,F}\right)\right).$$

Taking logarithms on both sides we obtain the equation

$$\log \#\mathcal{J}_{C_F} - g\log q = \sum_{n\geq 1} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right).$$

As $d \to \infty$ or $d, q \to \infty$, the genus $g = \left[\frac{d-1}{2}\right] \to \infty$. Choose

$$Z = \left[\frac{d}{(\log d)^2}\right]. \tag{4.1}$$

We write

$$\log \#\mathcal{J}_{C_F} - g\log q = \sum_{n\leq Z} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right) + \epsilon_{1,Z}(F), \tag{4.2}$$

where

$$\epsilon_{1,Z}(F) = \sum_{n> Z} q^{-n/2} n^{-1} \sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right).$$

It is easy to see that

$$|\epsilon_{1,Z}(F)| \leq \sum_{n>Z} q^{-n/2} n^{-1} 2g \leq \frac{9g}{Z}\, q^{-Z/2}.$$

Denote $L = \mathbb{F}_q(C_F)$ and $K = \mathbb{F}_q(X)$. Since L/K is a geometric quadratic extension and the Legendre symbol $\chi := \left(\frac{F}{\cdot}\right)$ generates the Galois group $\mathrm{Gal}(L/K)$, from (2.2) we have

$$L\left(s,\chi\right) = \prod_{i=1}^{2g}\left(1-\sqrt{q}e\left(\theta_{i,F}\right)q^{-s}\right), \tag{4.3}$$

and by definition

$$L(s,\chi) = \prod_{P}\left(1-\left(\frac{F}{P}\right)|P|^{-s}\right)^{-1}. \tag{4.4}$$

Here the product is over all monic irreducible polynomials $P \in \mathbb{F}_q(X)$ and $P = \infty$ with $|P| = q^{\deg P}$ ($\deg\infty = 1$ hence $|\infty| = q$).

Computing $\frac{\mathrm{d}}{\mathrm{d}s}L(s,\chi)$ in two different ways using (4.3) and (4.4) and equating the coefficients we obtain for each positive integer n the identity

$$\sum_{i=1}^{2g} -e\left(n\theta_{i,F}\right) = q^{-n/2} \sum_{\deg f = n} \Lambda(f)\left(\frac{F}{f}\right) + q^{-n/2}\delta_{d/2}, \tag{4.5}$$

where the sum over $\deg f = n$ on the right side is over all monic polynomials $f \in \mathbb{F}_q[X]$ with $\deg f = n$, and for any $\gamma \in \mathbb{R}$, $\delta_\gamma = 1$ if $\gamma \in \mathbb{Z}$, and $\delta_\gamma = 0$ if $\gamma \notin \mathbb{Z}$. The extra term $q^{-n/2}\delta_{n/2}$ comes from $f = \infty^n$, noting the fact that $F \in \mathcal{H}_{d,q}$ is monic and

$$\left(\frac{F}{\infty}\right) = \begin{cases} 1, & \deg F \equiv 0 \,(\mathrm{mod}\ 2), \\ 0, & \deg F \equiv 1 (\mathrm{mod}\ 2). \end{cases}$$

Using the identity (4.5) in (4.2) and denoting

$$N_F = \log \# \mathcal{J}_{C_F} - g \log q + \delta_{d/2} \log\left(1 - q^{-1}\right),$$

we find that

$$N_F = \triangle_Z(F) + \epsilon_Z(F),$$

where

$$\triangle_Z(F) = \sum_{n \le Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f) \left(\frac{F}{f}\right) \tag{4.6}$$

and

$$|\epsilon_Z(F)| \le \frac{10g}{Z}\, q^{-Z/2}. \tag{4.7}$$

An upper bound for $\triangle_Z(F)$ is given by

$$|\triangle_Z(F)| \le \sum_{n \le Z} q^{-n} n^{-1} \sum_{\deg f = n} \Lambda(f) \le 1 + \log Z.$$

4.2. The rth moment $\triangle_Z$. For any function $\chi : \mathcal{H}_d \to \mathbb{C}$, we denote by $\langle \chi \rangle$ the mean value of χ on $\mathcal{H}_{d,q}$, that is,

$$\langle \chi \rangle := \frac{1}{\# \mathcal{H}_{d,q}} \sum_{F \in \mathcal{H}_{d,q}} \chi(F).$$

For any positive integer r, we find

$$\triangle_Z(F)^r = \sum_{n_1, \ldots, n_r \le Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \le i \le r}} \Lambda(f_1) \cdots \Lambda(f_r) \left(\frac{F}{f_1 \cdots f_r}\right),$$

hence

$$\langle (\triangle_Z)^r \rangle = \sum_{n_1, \ldots, n_r \le Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \le i \le r}} \Lambda(f_1) \cdots \Lambda(f_r) \left\langle \left(\frac{\cdot}{f_1 \cdots f_r}\right) \right\rangle.$$

If $f_1 \cdots f_r$ is not a square in $\mathbb{F}_q[X]$, then $\left(\frac{\cdot}{f_1 \cdots f_r}\right) : \mathbb{F}_q[X] \to \mathbb{C}$ is a non-trivial Dirichlet character modulo h with $\deg h \le \sum_{i=1}^{r} \deg f_i$, by Lemma 2.1 we find that

$$\left\langle \left(\frac{\cdot}{f_1 \cdots f_r}\right) \right\rangle \le \frac{2^{n_1 + \cdots + n_r - 1}}{\left(1 - q^{-1}\right) q^{d/2}}.$$

The total contribution to $\langle (\triangle_Z)^r \rangle$ from this case is bounded by

$$T_1 \le \sum_{n_1, \ldots, n_r \le Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \le i \le r}} \Lambda(f_1) \cdots \Lambda(f_r) \frac{2^{n_1 + \cdots + n_r - 1}}{\left(1 - q^{-1}\right) q^{d/2}}.$$

This can be estimated as

$$T_1 \le \frac{q^{-d/2} 2^{(Z+1)r}}{2\left(1 - q^{-1}\right)} \le q^{-d/2} 2^{(Z+1)r} \ll q^{-d/3}. \tag{4.8}$$

If $f_1 \cdots f_r$ is a square in $\mathbb{F}_q[X]$, denote $f_1 \cdots f_r = h^2$ and $\widetilde{h} = \prod_{P|h} P$, then $\left(\frac{\cdot}{h^2}\right)$ is a trivial character, by Lemma 2.2 we find that

$$\left\langle \left(\frac{\cdot}{h^2}\right) \right\rangle = \frac{1}{\#\mathcal{H}_{d,q}} \sum_{\substack{F \in \mathcal{H}_{d,q} \\ \gcd(F,\widetilde{h})=1}} 1 = \prod_{P|\widetilde{h}} \left(1+|P|^{-1}\right)^{-1} + O\left(q^{-d/2}\sigma(\widetilde{h})\right).$$

Since f_i's are always prime powers, $\sigma(\widetilde{h}) \leq 2^r$. The total contribution to $\langle (\triangle_Z)^r \rangle$ from the error term $O\left(q^{-d/2}\sigma(\widetilde{h})\right)$ is bounded by

$$T_2 \leq \sum_{n_1,\ldots,n_r \leq Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \leq i \leq r}} \Lambda(f_1) \cdots \Lambda(f_r) q^{-d/2} 2^r.$$

This can be estimated as

$$T_2 \leq q^{-d/2} 2^r (1+\log Z)^r \ll q^{-d/3}. \tag{4.9}$$

The total contribution from the main term $\prod_{P|\widetilde{h}} \left(1+|P|^{-1}\right)^{-1}$ is

$$\sum_{n_1,\ldots,n_r \leq Z} \prod_{i=1}^{r} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \leq i \leq r \\ f_1 \cdots f_r = h^2}} \Lambda(f_1) \cdots \Lambda(f_r) \prod_{P|h} \left(1+|P|^{-1}\right)^{-1}.$$

Removing the restriction that $\deg f_1, \ldots, \deg f_r \leq Z$ results in an error bounded by

$$\sum_{\substack{h \\ \deg h > Z/2}} \prod_{P|h} \left(1+|P|^{-1}\right)^{-1} |h|^{-2} \sum_{\substack{f_1,\ldots,f_r \\ f_1 \cdots f_r = h^2}} \frac{\Lambda(f_1) \cdots \Lambda(f_r)}{(\deg f_1) \cdots (\deg f_r)}.$$

Noticing that $\frac{\Lambda(f_i)}{\deg f_i} \leq 1$ and f_i's are all prime powers, the sum over h is actually over all monic polynomials $h \in F[X]$ with $\omega(h) \leq r$ and $\deg h > Z/2$, where $\omega(h)$ is the function counting the number of distinct prime factors of h. If such an h is chosen, the number of choices for each f_i dividing h which is a prime power is less than $2r \deg h$. Hence the error by removing the restriction that $\deg f_1, \ldots, \deg f_r \leq Z$ is bounded by

$$T_3 \leq \sum_{\deg h > Z/2} |h|^{-2} (2r \deg h)^r = \sum_{n > Z/2} q^{-n} (2rn)^r \ll q^{-Z/4}.$$

Combining these estimates together we obtain

$$\langle (\triangle_Z)^r \rangle = H(r) + T,$$

where $T \ll q^{-Z/4}$ and

$$H(s) = \sum_{n_1,\ldots,n_s \geq 1} \prod_{i=1}^{s} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \leq i \leq s \\ f_1 \cdots f_s = h^2}} \Lambda(f_1) \cdots \Lambda(f_s) \prod_{P|h} \left(1+|P|^{-1}\right)^{-1}.$$

We write

$$\langle (N_F)^r \rangle = \langle (\triangle_Z)^r \rangle + E_{Z,r},$$

where

$$E_{Z,r} = \sum_{l=1}^{r} \binom{r}{l} \left\langle (\epsilon_Z)^l (\triangle_Z)^{r-l} \right\rangle \ll q^{-Z/4}.$$

Using (4.1) and the above we find that

$$\langle (N_F)^r \rangle = H(r) + O\left(q^{-Z/4}\right). \tag{4.10}$$

If q is fixed and $d \to \infty$, then for each fixed r,

$$\lim_{d\to\infty} \langle (N_F)^r \rangle = H(r).$$

Now suppose that X is a random variable with

$$\mathbb{E}(X^r) = H(r), \quad \forall r \in \mathbb{N}. \tag{4.11}$$

For any $t \in \mathbb{R}$, we can compute the characteristic function $\phi(t) = \mathbb{E}\left(e^{itX}\right)$ of X. Expanding e^{itX} by using the identity

$$e^x = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}, \tag{4.12}$$

using (4.11) and the expression of $H(r)$ from Proposition 5.1 which we will prove in the last section, we find that

$$\phi(t) = 1 + \sum_{n=1}^{\infty} \frac{(it)^n}{n!} \sum_{r=1}^{\infty} \frac{n!}{2^r r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=n \\ \lambda_i \geq 1}} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{j=1}^{r} \frac{u_{P_j}^{\lambda_j} + (-1)^{\lambda_j} v_{P_j}^{\lambda_j}}{\lambda_j!\,(1+|P_j|^{-1})},$$

where for any $P \in \mathbb{F}_q[X]$,

$$u_P = -\log\left(1 - |P_j|^{-1}\right), \quad v_P = \log\left(1 + |P_j|^{-1}\right).$$

Changing the order of summation again we obtain

$$\phi(t) = 1 + \sum_{r=1}^{\infty} \frac{1}{2^r r!} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{j=1}^{r} \left(\sum_{\lambda_j=1}^{\infty} \frac{(it)^{\lambda_j} \left(u_{P_j}^{\lambda_j} + (-1)^{\lambda_j} v_{P_j}^{\lambda_j}\right)}{\lambda_j!\,(1+|P_j|^{-1})} \right).$$

This implies

$$\phi(t) = 1 + \sum_{r=1}^{\infty} \frac{1}{2^r r!} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{j=1}^{r} \left(\frac{\left(1-|P_j|^{-1}\right)^{-it} + \left(1+|P_j|^{-1}\right)^{-it} - 2}{(1+|P_j|^{-1})} \right).$$

This completes the proof of (1) of Theorem 1.2.

For the proof of (2) of Theorem 1.2, it is enough to show that as $q \to \infty$, $\widetilde{\phi}(t) = \phi(t\sqrt{q}) \to e^{-t^2/2}$, the characteristic function of a standard Gaussian distribution. Notice that

$$\widetilde{\phi}(t) = \prod_{P} \left(1 + \frac{(1-|P|^{-1})^{-it\sqrt{q}} + (1+|P|^{-1})^{-it\sqrt{q}} - 2}{2(1+|P|^{-1})} \right),$$

where the product is over monic irreducible polynomials $P \in \mathbb{F}_q[X]$. It is easy to verify that as $q \to \infty$,

$$\log \widetilde{\phi}(t) = -t^2/2 + O(q^{-1/2}).$$

This completes the proof of (2) of Theorem 1.2. □

5. Analysis of $H(s)$

5.1. Proposition 1. Let $\mathbb{F}_q$ be a finite field of cardinality q. For any positive integer s, denote

$$H(s) = \sum_{n_1,\ldots,n_s \geq 1} \prod_{i=1}^{s} q^{-n_i} n_i^{-1} \sum_{\substack{\deg f_i = n_i \\ 1 \leq i \leq s \\ f_1 \cdots f_s = h^2}} \Lambda(f_1) \cdots \Lambda(f_s) \prod_{P \mid h} \left(1 + |P|^{-1}\right)^{-1}.$$

In this section wet derive another representation of $H(s)$ which has been used in the proof of Theorems 1.2.

Proposition 5.1. *For any positive integer $s \geq 1$ we have*

$$H(s) = \sum_{r=1}^{s} \frac{s!}{2^r r!} \sum_{\substack{\lambda_1 + \cdots + \lambda_r = s \\ \lambda_i \geq 1}} \sum_{\substack{P_1,\ldots,P_r \\ distinct}} \prod_{i=1}^{r} \frac{u_{P_i}^{\lambda_i} + (-1)^{\lambda_i} v_{P_i}^{\lambda_i}}{\lambda_i! \left(1 + |P_i|^{-1}\right)},$$

where the sum on the right side is over all positive integers $\lambda_1, \ldots, \lambda_r$ such that $\lambda_1 + \cdots + \lambda_r = s$ and over all distinct monic irreducible polynomials $P_1, \ldots, P_r \in \mathbb{F}_q[X]$, and

$$u_P = -\log\left(1 - |P|^{-1}\right), \quad v_P = \log\left(1 + |P|^{-1}\right), \quad \forall P \in \mathbb{F}_q[X]. \tag{5.1}$$

Proof. We rewrite $H(s)$ as

$$H(s) = \sum_{h} \prod_{P \mid h} \left(1 + |P|^{-1}\right)^{-1} |h|^{-2} \sum_{\substack{f_1,\ldots,f_s \\ f_1 \cdots f_s = h^2}} \frac{\Lambda(f_1) \cdots \Lambda(f_s)}{(\deg f_1) \cdots (\deg f_s)}.$$

Since f_i's are prime powers, the sum over h is actually over all monic polynomials $h \in \mathbb{F}_q[X]$ with $\omega(h) \leq r$, where $\omega(h)$ is the number of distinct prime factors of h. Hence

$$H(s) = \sum_{r=1}^{s} H(s,r), \tag{5.2}$$

where

$$H(s,r) = \sum_{\substack{h \\ \omega(h) = r}} \prod_{P \mid h} \left(1 + |P|^{-1}\right)^{-1} |h|^{-2} \sum_{\substack{f_1,\ldots,f_s \\ f_1 \cdots f_s = h^2}} \frac{\Lambda(f_1) \cdots \Lambda(f_s)}{(\deg f_1) \cdots (\deg f_s)}.$$

If $\omega(h) = r$, write explicitly $h = P_1^{a_1} \cdots P_r^{a_r}$ for some distinct primes $P_1, \ldots, P_r$ and exponents $a_1, \ldots, a_r \geq 1$, then

$$H(s,r) = \frac{1}{r!} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \sum_{\substack{a_1,\ldots,a_r \geq 1 \\ h=P_1^{a_1}\cdots P_r^{a_r}}} \prod_{i=1}^{r} \left(1 + |P_i|^{-1}\right)^{-1} |P_i|^{-2a_i}$$
$$\times \sum_{\substack{f_1,\ldots,f_s \\ f_1\cdots f_s = h^2}} \frac{\Lambda(f_1)\cdots\Lambda(f_s)}{(\deg f_1)\cdots(\deg f_s)}.$$

Since each f_i is a prime power and $f_1 \cdots f_s = P_1^{2a_1} \cdots P_r^{2a_r}$, there are finitely many ways to assign prime powers to each f_i, according to which we will break $H(s,r)$ into many subsums. With that in mind, for each partition of the set of indexes

$$\{1, 2, \ldots, s\} = \bigcup_{i=1}^{r} A_i, \quad \#A_i = \lambda_i \geq 1, \forall i,$$

it satisfies the property that

$$\sum_{i=1}^{r} \lambda_i = s.$$

We say $(A_1, \ldots, A_r)$ is the type of $(f_1, \ldots, f_r)$ with $f_1 \cdots f_r = h^2$, namely whenever $j \in A_i$, then f_j is a power of P_i. Suppose that $f_i = Q_i^{e_i}$ for some prime $Q_i \in \{P_1, \ldots, P_r\}$ and exponent $e_i \geq 1$, and the type of $(f_1, \ldots, f_r)$ is $(A_1, \ldots, A_r)$, since $f_1 \cdots f_s = P_1^{2a_1} \cdots P_r^{2a_r}$, comparing the exponents of P_j on both sides we find that

$$\sum_{i \in A_j} e_i = 2a_j \quad \forall 1 \leq j \leq r, \tag{5.3}$$

and

$$\frac{\Lambda(f_1)\cdots\Lambda(f_s)}{(\deg f_1)\cdots(\deg f_s)} = \frac{1}{e_1 \cdots e_s}.$$

Instead of summing over all integers $a_1, \ldots, a_r$, we sum over all positive integers $e_1, \ldots, e_s$ which satisfy the conditions (5.3). Noting that the value only depends on the vector of integers $(\lambda_1, \ldots, \lambda_r)$ such that

$$\sum_{i=1}^{r} \lambda_i = s,$$

hence we can write $H(s,r)$ as

$$H(s,r) = \frac{s!}{r!} \sum_{\substack{\lambda_1+\cdots+\lambda_r=s \\ \lambda_i \geq 1}} \sum_{\substack{P_1,\ldots,P_r \\ \text{distinct}}} \prod_{i=1}^{r}$$
$$\times \left(\frac{\left(1+|P_i|^{-1}\right)^{-1}}{\lambda_i!} \sum_{\substack{a_1+\cdots+a_{\lambda_i} \equiv 0 \pmod 2 \\ a_j \geq 1}} \frac{|P_i|^{-a_1-\cdots-a_{\lambda_i}}}{a_1 \cdots a_{\lambda_i}} \right).$$

For each prime P and positive integer λ, denote

$$\eta(\lambda)=\eta_P(\lambda):=\sum_{\substack{a_1+\cdots+a_\lambda\equiv 0 \pmod 2\\ a_i\geq 1}}\frac{|P|^{-a_1-\cdots-a_\lambda}}{a_1\cdots a_\lambda}$$

and

$$\tau(\lambda)=\tau_P(\lambda):=\sum_{\substack{a_1+\cdots+a_\lambda\equiv 1 \pmod 2\\ a_i\geq 1}}\frac{|P|^{-a_1-\cdots-a_\lambda}}{a_1\cdots a_\lambda}.$$

Since

$$-\log(1-x)=\sum_{n\geq 1}\frac{x^n}{n},\quad |x|<1,$$

we find

$$\eta(1)=-\tfrac{1}{2}\log\left(1-|P|^{-2}\right), \tag{5.4}$$

and

$$\eta(\lambda)+\tau(\lambda)=\sum_{a_1,\cdots a_\lambda\geq 1}\frac{|P|^{-a_1-\cdots-a_\lambda}}{a_1\cdots a_\lambda}=(-1)^\lambda\log^\lambda\left(1-|P|^{-1}\right). \tag{5.5}$$

Combining (5.4) and (5.5) we have

$$\tau(1)=-\log\left(1-|P|^{-1}\right)+\tfrac{1}{2}\log\left(1-|P|^{-2}\right).$$

For $\lambda\geq 2$, we can write

$$\eta(\lambda)=\sum_{\substack{a_2+\cdots+a_\lambda\equiv 0 \pmod 2\\ a_i\geq 1}}\left(\prod_{i=1}^{\lambda}\frac{|P|^{-a_i}}{a_i}\right)\eta(1)+\sum_{\substack{a_2+\cdots+a_\lambda\equiv 1 \pmod 2\\ a_i\geq 1}}\left(\prod_{i=1}^{\lambda}\frac{|P|^{-a_i}}{a_i}\right)\tau(1).$$

This shows that

$$\eta(\lambda)=\eta(1)\eta(\lambda-1)+\tau(1)\tau(\lambda-1). \tag{5.6}$$

Similarly for $\lambda\geq 2$,

$$\tau(\lambda)=\eta(1)\tau(\lambda-1)+\tau(1)\eta(\lambda-1). \tag{5.7}$$

We can assign the initial values

$$\eta(0)=1,\quad \tau(0)=0,$$

so that the recursive relations (5.6) and (5.7) hold for any $\lambda\geq 1$. Subtracting these two recursive relations we obtain

$$\eta(\lambda)-\tau(\lambda)=\left(\eta(1)-\tau(1)\right)\left(\eta(\lambda-1)-\tau(\lambda-1)\right).$$

Applying this relation recursively and using (5.5) we conclude that

$$\eta(\lambda)=\tfrac{1}{2}\left(u_P^\lambda+(-1)^\lambda v_P^\lambda\right),$$

where

$$u_P=-\log\left(1-|P|^{-1}\right),\quad v_P=\log\left(1+|P|^{-1}\right).$$

Therefore $H(s,r)$ can be written as

$$H(s,r)=\frac{s!}{2^r r!}\sum_{\substack{\lambda_1+\cdots+\lambda_r=s\\ \lambda_i\geq 1}}\ \sum_{\substack{P_1,\ldots,P_r\\ \text{distinct}}}\prod_{i=1}^{r}\frac{u_{P_i}^{\lambda_i}+(-1)^{\lambda_i}v_{P_i}^{\lambda_i}}{\lambda_i!\,(1+|P_i|^{-1})}.$$

Returning to (5.2) completes the proof of Proposition 5.1. □

Acknowledgments

The authors are grateful to the anonymous referee for many valuable suggestions. Maosheng Xiong is supported by RGC grant number 606211 and DAG11SC02 from Hong Kong. Alexandru Zaharescu is supported by NSF grant number DMS-0901621.

References

[1] J.D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra **204**(2) (2006), 316–333.
[2] J.D. Achter, *Results of Cohen–Lenstra type for quadratic function fields*, Computational Arithmetic Geometry, 1–7, Contemp. Math., **463**, Amer. Math. Soc., Providence, RI, 2008.
[3] L.M. Adleman, M.A. Huang, Primality testing and abelian varieties over finite fields, Lecture Notes in Mathematics **1512** (1992), Springer-Verlag, Berlin.
[4] A. Bucur, C. David, B. Feigon, M. Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, International Math. Research Notices, 2010, 932–967.
[5] A. Bucur, C. David, B. Feigon, 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.
[6] M. Deuring. *Die Typen der Multiplikatorenringe elliptischer Funktionenkö per*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
[7] P. Diaconis, S. Evans, *Linear functionals of eigenvalues of random matrices*, Trans. Amer. Math. Soc. **353**(7) (2001), 2615–2633.
[8] D. Faifman, Z. Rudnick, Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field, Compos. Math., **146** (2010), 81–101.
[9] A. Granville, Soundararajan, *The distribution of Values of $L(1,\chi_d)$*, Geom. Funct. Anal. **13**(5) (2003), 992–1028.
[10] N.M. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc. Colloq. Publ., **45**, American Mathematical Society, Providence, RI, 1999.
[11] P. Kurlberg, Z. Rudnick, *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory **3**(129) (2009), 580–587.
[12] H.W. Lenstra, Jr., J. Pila, C. Pomerance, *A hyperelliptic smoothness test. I*, Philos. Trans. Roy. Soc. London Ser. A **345**(1676) (1993), 397–408.
[13] H.W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126**(3) (1987), 649–673.
[14] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Math., **9**, American Mathematical Society, Providence, RI, 1996.
[15] H.G. Quebbemann. *Estimates of regulators and class numbers in function fields*, J. Reine Angew. Math. **419** (1991), 79–87.
[16] M.Y. Rosenbloom, M.A. Tsfasman, *Multiplicative lattices in global fields*, Invent. Math. **101** (1990), 687–696.
[17] M. Rosen, *Number theory in function fields*, Graduate Texts in Math., **210**, Springer-Verlag, New York, 2002.
[18] Z. Rudnick, *Traces of high powers of the Frobenius class in the hyperelliptic ensemble*, Acta Arith. **143** (2010), 81–99.
[19] I. Shparlinski, *On the size of the Jacobians of curves over finite fields*, Bull. Braz. Math. Soc. (N.S.) **39**(4) (2008), 587–595.

[20] A. Stein, E. Teske. *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, Math. Comp., **71** (2002), 837–861.
[21] M. Tsfasman, *Some remarks on the asymptotic number of points*, 'Coding theory and algebraic geometry (Luminy, 1991)', 178–192, Lect. Notes in Math., **1518**, Springer, Berlin, 1992.
[22] A. Venkatesh, S. Ellenberg, *Statistics of number fields and function fields*, Proceedings of the International Congress of Mathematicians, Hyderabad, India, 2010.
[23] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Publ. Inst. Math. Univ. Strasbourg, **7** (1945), Hermann et Cie., Paris, 1948.

Department of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, People's Republic of China
E-mail address: `mamsxiong@ust.hk`

Institute of Mathematics of the Romanian Academy, PO Box 1–764, 70700 Bucharest, Romania, and Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, IL 61801, USA
E-mail address: `zaharesc@math.uiuc.edu`