Journal of Number Theory 132 (2012) 467–484

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Statistics for products of traces of high powers of the Frobenius class of hyperelliptic curves ☆

Edva Roditty-Gershon

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

ARTICLE INFO

Article history:
Received 29 May 2011
Revised 13 September 2011
Accepted 15 September 2011
Available online 20 December 2011
Communicated by K. Soundararajan

Keywords:
Hyperelliptic curve
Random matrix theory
n-level density
One-level density
Zeros of L-functions

ABSTRACT

We study the averages of products of traces of high powers of the Frobenius class of hyperelliptic curves of genus g over a fixed finite field. We show that for increasing genus g, the limiting expectation of these products equals to the expectation when the curve varies over the unitary symplectic group $USp(2g)$. We also consider the scaling limit of linear statistics for eigenphases of the Frobenius class of hyperelliptic curves, and show that their first few moments are Gaussian.

Contents

☆ Supported in part by the Israel Science Foundation (grant No. 1083/10).
E-mail address: roditty@post.tau.ac.il.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.09.008

1. Introduction

Let C be a nonsingular projective curve of genus g, defined over a finite field $\mathbb{F}_q$ of odd cardinality q. The zeta function of C is defined as

$$Z_C(u) = \exp \sum_{n=1}^{\infty} N_n(C) \frac{u^n}{n}, \quad |u| < \frac{1}{q} \tag{1.1}$$

where $N_n(C)$ is the number of points of C with coefficients in an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ of degree n. The zeta function is known to be a rational function of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} \tag{1.2}$$

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

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

By the Riemann hypothesis (proved by Weil [9]), we may interpret $P_C(u)$ as the characteristic polynomial of a $2g \times 2g$ unitary matrix Θ_C, where the eigenvalues $e^{i\theta_j}$ of Θ_C correspond to zeros $q^{-1/2}e^{-i\theta_j}$ of $Z_C(u)$:

$$P_C(u) = \det(I - u\sqrt{q}\Theta_C). \tag{1.3}$$

The conjugacy class of Θ_C is called the *unitarized Frobenius class* of C.

We consider the family $\mathcal{H}_{2g+1}$ of hyperelliptic curves of genus g given in affine form by an equation

$$C_Q\colon\ y^2 = Q(x)$$

where $Q(x) \in \mathbb{F}_q[x]$ is a square-free, monic polynomial of degree $2g+1$. We will study the expected value of products of traces of high powers of the Frobenius class of C as we vary the curve C over $\mathcal{H}_{2g+1}$, and show that these statistics determine the n-level density of the eigenvalues. Our work is in the limit of large genus and fixed constant field.

Consider $\mathcal{H}_{2g+1}$ as a probability space with the uniform probability measure, so that the expected value of any function F on $\mathcal{H}_{2g+1}$ is defined as

$$\langle F\rangle := \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{Q\in\mathcal{H}_{2g+1}} F(Q).$$

Katz and Sarnak [5] showed that for a fixed genus, the Frobenius classes Θ_Q become uniformly distributed in $USp(2g)$ in the limit $q\to\infty$ of large field size. That is, for any continuous function on the space of conjugacy classes of $USp(2g)$,

$$\lim_{q\to\infty}\big\langle F(\Theta_Q)\big\rangle = \int\limits_{USp(2g)} F(U)\,dU.$$

If we take the opposite limit, that of fixed constant field and large genus $g\to\infty$ (that is, without first taking $q\to\infty$, which was crucial to the approach of Katz and Sarnak), since the matrices Θ_Q now inhabit different spaces as g grows, it is not clear how to formulate an equidistribution problem. However, we can discuss the statistics of products of traces of powers of Θ_Q, that is, $\langle\prod_{j=1}^n(\operatorname{tr}U^{k_j})^{a_j}\rangle$. Rudnick [8] showed that for a fixed constant field and large genus $g\to\infty$, if $3\log_q g < n < 4g - 5\log_q g$ but $n\neq 2g$ then

$$\big\langle\operatorname{tr}U^n\big\rangle = \int\limits_{USp(2g)} \operatorname{tr}U^n\,dU + o\bigg(\frac{1}{g}\bigg).$$

In the case of fixed $k_1,\dots,k_n$, $a_1,\dots,a_n$ Bucur, David, Feigon and Lalín [1] studied the variation of the trace of the Frobenius endomorphism in the cyclic trigonal ensemble. They showed 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 [6] who considered the same limit for hyperelliptic curves.

In this paper (in continuation of Rudnick's work [8]), we study the general case of average of product of traces $\langle\prod_{j=1}^n(\operatorname{tr}U^{k_j})^{a_j}\rangle$, where $k_1,\dots,k_n$ are of order of the genus g, and $a_1,\dots,a_n$ are fixed.

1.1. Result

First we state a result [3,2,4] which expresses the mean value of products of traces of high powers when averaged over the unitary symplectic group $USp(2g)$ in terms of independent standard normal random variables.

Let Z_j be independent standard normal random variables, and let

$$\eta_{k_j} = \begin{cases} 1 & \text{if } k_j \text{ is even,}\\ 0 & \text{if } k_j \text{ is odd.}\end{cases}$$

If $k_j, a_j\in\{1,2,\dots\}$ for $1\leqslant j\leqslant n$ are such that $\sum_{j=1}^n a_jk_j\leqslant 2g+1$, k_j distinct, then

$$\int\limits_{USp(2g)}\prod_{j=1}^n\big(\operatorname{tr}U^{k_j}\big)^{a_j}\,dU = \mathbb{E}\bigg(\prod_{j=1}^n(\sqrt{k_j}Z_j-\eta_{k_j})^{a_j}\bigg)$$

where $\mathbb{E}$ denotes the expectation. For the proof see [3,2,4].

Since Z_j are independent standard normal random variables, we have

$$\mathbb{E}\left(\prod_{j=1}^{n}(\sqrt{k_j}Z_j-\eta_{k_j})^{a_j}\right)=\prod_{j=1}^{n}\mathbb{E}\big((\sqrt{k_j}Z_j-\eta_{k_j})^{a_j}\big)=\prod_{j=1}^{n}\mathbb{E}\left(\sum_{i=0}^{a_j}\binom{a_j}{i}(\sqrt{k_j}Z_j)^i(-\eta_{k_j})^{a_j-i}\right)$$
$$=\prod_{j=1}^{n}\sum_{i=0}^{a_j}\binom{a_j}{i}(\sqrt{k_j})^i\mathbb{E}\big((Z_j)^i\big)(-\eta_{k_j})^{a_j-i}$$
$$=\prod_{j=1}^{n}\sum_{i=0}^{\lfloor\frac{a_j}{2}\rfloor}\binom{a_j}{2i}(k_j)^i\left(\frac{(2i)!}{2^i(i)!}\right)(-\eta_{k_j})^{a_j-2i}. \tag{1.4}$$

We will show

Theorem 1.1. *Assume $k_j\in\{1,2,\ldots\}$ for $1\leqslant j\leqslant n$ are such that $\sum_{j=1}^{n}a_jk_j\leqslant 2g-1$ for fixed integers a_j. Assume that k_j are distinct and $\log_q g\ll\min(k_1,\ldots,k_n)$, then*

$$\left\langle\prod_{j=1}^{n}\big(\operatorname{tr}U^{k_j}\big)^{a_j}\right\rangle=\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}(k_j)^{i_j}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}(i_j)!}(-\eta_{k_j})^{a_j-2i_j}+o(1). \tag{1.5}$$

Comparing (1.4) and (1.5) we find

Corollary 1.2. *If $\log_q g\ll\min(k_1,\ldots,k_n)$ and $\sum_{j=1}^{n}k_ja_j\leqslant 2g-1$, then*

$$\left\langle\prod_{j=1}^{n}\big(\operatorname{tr}U^{k_j}\big)^{a_j}\right\rangle=\int\limits_{USp(2g)}\prod_{j=1}^{n}\big(\operatorname{tr}U^{k_j}\big)^{a_j}\,dU+o(1). \tag{1.6}$$

To prove these results, we cannot use the same methods that were used for the fixed genus case by Katz and Sarnak [5]. Rather, we use a variant of the analytic methods similar to those used in [8].

1.2. Application: The n-level density

Denote by $\theta_1,\ldots,\theta_N$ the sequence of angles of U a unitary matrix of size $N\times N$. The traces of powers determine the number of sets of angles $\theta_{i_1},\ldots,\theta_{i_n}$ lying in a subinterval of $\mathbb{R}/2\pi\mathbb{Z}$, or the n-level density. For the case of $n=1$ or the one-level density see [8]. To define the n-level density, we start with an even test function f, in the Schwartz space $\mathcal{S}(\mathbb{R})$, and for any $N\geqslant 1$ set

$$F(\theta):=\sum_{k\in\mathbb{Z}}f\left(N\left(\frac{\theta}{2\pi}-k\right)\right),$$

which has a period of 2π and is localized in an interval of size $\approx 1/N$ in $\mathbb{R}/2\pi\mathbb{Z}$. For a unitary $N\times N$ matrix U with eigenvalues $e^{i\theta_j}$, $j=1,\ldots,N$, define

$$Z_f(U):=\sum_{j=1}^{N}F(\theta_j),$$

which counts the number of "low-lying" eigenphases θ_j in the smooth interval of length $\approx 1/N$ around the origin defined by f. The product Z_f^n counts the number of sets of angles $\theta_{i_1}, \ldots, \theta_{i_n}$ in the smooth interval of length $\approx 1/N$ around the origin defined by f. In order to study the n-level density, we need to compute the n-th moment of Z_f.

Katz and Sarnak [5] conjectured that for fixed q, the expected value of Z_f over $\mathcal{H}_{2g+1}$ will converge to $\int_{USp(2g)} Z_f(U)\,dU$ as $g \to \infty$ for any such test function f. Rudnick [8] proved this conjecture for a test function f such that the Fourier transform $\hat{f}$ supported in $(-2, 2)$. Corollary 1.2 implies:

Corollary 1.3. *If supp* $\hat{f} \subseteq (\frac{-1}{m}, \frac{1}{m})$ *then the first m moments of* $Z_f(U)$ *converge to the Gaussian moments with mean*

$$\hat{f}(0) - \int_0^1 \hat{f}(u)\,du$$

and variance

$$2\int_{-1/2}^{1/2} |u|\hat{f}(u)^2\,du.$$

This is called "Mock Gaussian" behavior in [4].

To show Corollary 1.3, one uses a Fourier expansion to see that (for $N = 2g$)

$$Z_f(U) = \int_{-\infty}^{\infty} f(x)\,dx + \frac{1}{N}\sum_{k\neq 0} \hat{f}\left(\frac{k}{N}\right) \operatorname{tr} U^k, \tag{1.7}$$

and then by Corollary 1.2 and [4], the above follows.

2. Background on Dirichlet characters and L-functions

In this section we review some known background on quadratic L-function. See [7] for details.

2.1. The zeta function

For a nonzero polynomial $f \in \mathbb{F}_q[x]$, we define the norm $|f| := q^{\deg f}$. A prime polynomial is a monic irreducible polynomial. For a monic polynomial f, the von Mangoldt function $\Lambda(f)$ is defined to be zero unless f is a prime power in which case $\Lambda(P^k) = \deg P$.

The analog of Riemann's zeta function is

$$\zeta_q(s) := \prod_{P \text{ prime}} \left(1 - |P|^{-s}\right)^{-1}, \quad \mathcal{R}(s) < 1. \tag{2.1}$$

As a result of expanding in additive form using unique factorization, we have

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}}. \tag{2.2}$$

The following identity is equivalent to (2.2):

$$\sum_{\substack{\deg f=n \\ f \text{ monic}}} \Lambda(f) = q^n. \tag{2.3}$$

Let $\pi_q(n)$ be the number of prime polynomials of degree n. The Prime Polynomial Theorem in $\mathbb{F}_q[x]$ asserts that

$$\pi_q(n) = \frac{q^n}{n} + O\left(q^{n/2}\right) \tag{2.4}$$

which follows from (2.3).

2.2. Quadratic characters

Let $P \in \mathbb{F}_q[x]$ (q odd) be a prime polynomial. The quadratic residue symbol $(\frac{f}{P}) \in \{\pm 1\}$ is defined for f coprime to P by

$$\left(\frac{f}{P}\right) \equiv f^{(\frac{|P|-1}{2})} \mod P.$$

For arbitrary monic $Q \in \mathbb{F}_q[x]$ and for f coprime to Q, the Jacobi symbol $(\frac{f}{Q})$ is defined by writing $Q = \prod P_j$ as a product of prime polynomials and setting

$$\left(\frac{f}{Q}\right) = \prod \left(\frac{f}{P_j}\right).$$

If f, Q are not coprime we set $(\frac{f}{Q}) = 0$.

The law of quadratic reciprocity asserts that for $A, B \in \mathbb{F}_q[x]$ monic polynomials

$$\left(\frac{B}{A}\right) = (-1)^{(\frac{q-1}{2})\deg A \deg B} \left(\frac{A}{B}\right). \tag{2.5}$$

For $D \in \mathbb{F}_q[x]$ a monic polynomial of positive degree which is not a perfect square, we define the quadratic character χ_D by

$$\chi_D = \left(\frac{D}{f}\right). \tag{2.6}$$

2.3. L-functions

For the quadratic character χ_D, the corresponding L-function is defined by

$$\mathcal{L}(u, \chi_D) := \prod_{P \text{ prime}} \left(1 - \chi_D(P) u^{\deg P}\right)^{-1}, \quad |u| < \frac{1}{q}.$$

Expanding in additive form using unique factorization, we write

$$\mathcal{L}(u, \chi_D) = \sum_{\beta \geqslant 0} A_D(\beta) u^{\beta}$$

with

$$A_D(\beta) := \sum_{\substack{\deg B=\beta \\ B \text{ monic}}} \chi_D(B).$$

If D is nonsquare of positive degree, then $A_D(\beta) = 0$ for $\beta \geqslant \deg D$ and hence the L-function is in fact a polynomial of degree at most $\deg D - 1$.

Now, assume that D is also square-free. Then $\mathcal{L}(u, \chi_D)$ has a trivial zero at $u = 1$ if and only if $\deg D$ is even. Thus

$$\mathcal{L}(u, \chi_D) = (1-u)^{\lambda} \mathcal{L}^*(u, \chi_D), \quad \lambda = \begin{cases} 1, & \deg D \text{ even}, \\ 0, & \deg D \text{ odd} \end{cases}$$

where $\mathcal{L}^*(u, \chi_D)$ is a polynomial of even degree

$$2\delta = \deg D - 1 - \lambda$$

satisfying the functional equation

$$\mathcal{L}^*(u, \chi_D) = \left(qu^2\right)^{\delta} \mathcal{L}^*\left(\frac{1}{qu}, \chi_D\right).$$

We write

$$\mathcal{L}^*(u, \chi_D) = \sum_{\beta=0}^{2\delta} A_D^*(\beta) u^{\beta},$$

where $A_D^*(0) = 1$, and the coefficients $A_D^*(\beta)$ satisfy

$$A_D^*(\beta) = q^{\beta-\delta} A_D^*(2\delta - \beta). \tag{2.7}$$

In particular, the leading coefficient is $A_D^*(2\delta) = q^{\delta}$.

2.4. The explicit formula

For D monic, square-free, and of positive degree, the zeta function (1.2) of the hyperelliptic curve $y^2 = D(x)$ is

$$Z_D(u) = \frac{\mathcal{L}^*(u, \chi_D)}{(1-u)(1-qu)}.$$

By the Riemann Hypothesis (proved by Weil [9]) all the zeros of $Z_D(u)$, hence of $\mathcal{L}^*(u, \chi_D)$, lie on the circle $|u| = 1/q$. Thus we may write

$$\mathcal{L}^*(u, \chi_D) = \det(I - u\sqrt{q}\Theta_D)$$

for a unitary $2g \times 2g$ matrix Θ_D.

By taking a logarithmic derivative of the identity

$$\det(I - u\sqrt{q}\Theta_D) = (1-u)^{-\lambda} \prod_P \left(1 - \chi_D(P)u^{\deg P}\right)^{-1},$$

we find

$$-\operatorname{tr}\Theta_D^n = \frac{\lambda}{q^{n/2}} + \frac{1}{q^{n/2}} \sum_{\deg f = n} \Lambda(f)\chi_D(f). \tag{2.8}$$

2.5. The Weil bound

Assume that B is monic of positive degree and not a perfect square. Then we have a bound for the character sum over primes:

$$\left| \sum_{\substack{\deg P = n \\ P \text{ prime}}} \left(\frac{B}{P}\right) \right| \ll \frac{\deg B}{n} q^{n/2}. \tag{2.9}$$

This is deduced from the explicit formula (2.8) when writing $B = DC^2$ with D square-free of positive degree, and from the unitarity of Θ_D.

3. The hyperelliptic ensemble $\mathcal{H}_{2g+1}$

3.1. Averaging over $\mathcal{H}_{2g+1}$

We denote by $\mathcal{H}_d$ the set of square-free monic polynomials of degree d in $\mathbb{F}_q[x]$. By using (2.1) and writing

$$\sum_{d \geqslant 0} \frac{\#\mathcal{H}_d}{q^{ds}} = \sum_f |f|^{-s} = \frac{\zeta_q(s)}{\zeta_q(2s)}$$

where the sum is over monic and square-free polynomials. We have

$$\#\mathcal{H}_d = \begin{cases} (1-1/q)q^d, & d \geqslant 2, \\ q, & d = 1. \end{cases}$$

In particular, for $g \geqslant 1$,

$$\#\mathcal{H}_{2g+1} = (q-1)q^{2g}.$$

We consider $\mathcal{H}_{2g+1}$ as a probability space with the uniform probability measure, so that the expected value of any function F on $\mathcal{H}_{2g+1}$ is defined as

$$\langle F \rangle := \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{Q \in \mathcal{H}_{2g+1}} F(Q). \tag{3.1}$$

We can pick out square-free polynomials by using the Möbius function μ of $\mathbb{F}_q[x]$

$$\sum_{A^2|Q} \mu(A) = \begin{cases} 1, & Q \text{ is square-free,} \\ 0, & \text{otherwise.} \end{cases}$$

Thus we may write the expected value as

$$\langle F(Q)\rangle = \frac{1}{(q-1)q^{2g}} \sum_{2\alpha+\beta=2g+1} \sum_{\deg B=\beta} \sum_{\deg A=\alpha} \mu(A) F\left(A^2 B\right) \tag{3.2}$$

the sum is over all monic A, B.

3.2. Averaging quadratic characters

For a given polynomial $f \in \mathbb{F}_q[x]$ apply (3.2) to the quadratic character $\chi_Q(f)$. Then

$$\chi_{A^2B}(f) = \left(\frac{B}{f}\right)\left(\frac{A}{f}\right)^2 = \begin{cases} \left(\frac{B}{f}\right), & \gcd(A, f) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Hence

$$\langle \chi_Q(f)\rangle = \frac{1}{(q-1)q^{2g}} \sum_{2\alpha+\beta=2g+1} \sum_{\substack{\deg A=\alpha \\ \gcd(A,f)=1}} \mu(A) \sum_{\deg B=\beta} \left(\frac{B}{f}\right). \tag{3.3}$$

3.3. A sum of Möbius values

Define

$$\sigma(f,\alpha) := \sum_{\substack{\deg A=\alpha \\ \gcd(A,f)=1}} \mu(A). \tag{3.4}$$

Note that $\sigma(f,\alpha)$ depends only on the degrees of the primes dividing f, hence we can write for $p_1,\dots,p_n$ distinct primes of degrees $k_1,\dots,k_n$ respectively: $\sigma(\prod_{i=1}^n p_i, \alpha) = \sigma(k_1,\dots,k_n;\alpha)$.

Lemma 3.1. *Assume* $\min(k_1,\dots,k_n) \geqslant 2$, *then*

$$\sigma(k_1,\dots,k_n;\alpha) = \begin{cases} 1, & \alpha = 0, \\ -q, & \alpha = 1, \\ 0, & 2 \leqslant \alpha < \min(k_1,\dots,k_n). \end{cases}$$

Proof. By definition

$$\sigma(k_1,\dots,k_n;\alpha) = \sum_{\substack{\deg A=\alpha \\ \gcd(A,p_1\cdots p_n)=1}} \mu(A).$$

Now if $\deg A < \min(k_1,\dots,k_n)$ then A is automatically coprime to $p_1,\dots,p_n$ hence in this case the sum is over all A with degree α. Therefore

$$\sigma(k_1,\dots,k_n;\alpha)=\sum_{\deg A=\alpha}\mu(A)$$

which vanishes if $\alpha\geqslant 2$, equals 1 for $\alpha=0$ and $-q$ for $\alpha=1$. □

3.4. The probability that $f\nmid Q$

Lemma 3.2. *Let $f=p_1p_2\cdots p_k$ with $p_1,\dots,p_n$ prime polynomials. Then*

$$\left\langle\chi_Q\left(f^2\right)\right\rangle=1+O\left(\sum_{p\mid f}\frac{1}{\|p\|}\right). \tag{3.5}$$

Proof. We may write

$$\chi_Q\left(p_1^2\cdots p_k^2\right)=1-\delta(Q,p_1\cdots p_l),\quad \delta(Q,p_1\cdots p_l)=\begin{cases}1, & \gcd(Q,p_1^2\cdots p_l^2)\neq 1,\\ 0, & \gcd(Q,p_1^2\cdots p_l^2)=1,\end{cases}$$

and hence

$$\left\langle\chi_Q\left(p_1^2\cdots p_n^2\right)\right\rangle=1-\frac{\#\{Q\in\mathcal{H}_{2g+1}\colon \exists p_j\mid Q\}}{\#\mathcal{H}_{2g+1}}.$$

Replacing the set of square-free Q by arbitrary monic Q of degree $2g+1$ gives

$$\#\{Q\in\mathcal{H}_{2g+1}\colon \exists p_j\mid Q\}\leqslant\#\{\deg Q=2g+1=:\exists p_j\mid Q\}\leqslant\sum_{j=1}^{k}\frac{q^{2g+1}}{|p_j|},$$

so that recalling $\#H_{2g+1}=(q-1)q^{2g}$ we have

$$1-\frac{1}{(1-1/q)}\sum_{j=1}^{k}\frac{1}{|p_j|}\leqslant\left\langle\chi_Q\left(p_1^2\cdots p_n^2\right)\right\rangle\leqslant 1.$$

Thus

$$\left\langle\chi_Q\left(p_1^2\cdots p_n^2\right)\right\rangle=1+O\left(\sum_{j=1}^{k}\frac{1}{|p_j|}\right),$$

as claimed. □

4. Multiple character sums

Define

$$S(\beta;k_1,\dots,k_n):=\sum_{\deg p_1=k_1}\sum_{\deg p_2=k_2}\cdots\sum_{\deg p_n=k_n}\sum_{\deg B=\beta}\left(\frac{B}{p_1p_2\cdots p_n}\right) \tag{4.1}$$

the sum over distinct primes $p_1,\dots,p_n$ and arbitrary monic B.

Let F be a square-free polynomial and

$$\mathcal{L}(u,\chi_F)=\sum_{\beta=0}^{\infty}A_F(\beta)u^{\beta},\quad A_F(\beta):=\sum_{\deg B=\beta}\chi_F(B).$$

By quadratic reciprocity (see (2.5))

$$S(\beta;k_1,\dots,k_n)=(-1)^{\frac{q-1}{2}\beta(\sum_{i=1}^n p_i)}\sum_{\deg p_1=k_1}\sum_{\deg p_2=k_2}\cdots\sum_{\deg p_n=k_n}A_{\prod_{i=1}^n p_i}(\beta)$$

the sum over distinct primes $p_1,\dots,p_n$.

Since the L-function $\mathcal{L}(u,\chi_F)$ is a polynomial of degree $\deg F-1$, we have

Lemma 4.1. *If $\beta\geqslant\sum_{i=1}^n k_i$ then $S(\beta;k_1,\dots,k_n)=0$.*

5. Averaging $\prod_{i=1}^{n}(\operatorname{tr}U^{k_i})^{a_i}$

5.1. Reducing to prime powers

By using the explicit formula (2.8), we can write

$$\operatorname{tr}U^k=\frac{-1}{q^{\frac{k}{2}}}\sum_{\deg f=k}\Lambda(f)\chi_Q(f).$$

We separate out the contributions of primes $\mathcal{P}_k$, squares of primes $\square_k$ (appears only in case k is even), and higher prime powers $\mathbb{H}_k$ to $\operatorname{tr}U^k$:

$$\left(-\operatorname{tr}U^k\right)^a=(\mathcal{P}_k+\eta_k\square_k+\mathbb{H}_k)^a=\sum_{i_1+i_2+i_3=a}\binom{a}{i_1,i_2,i_3}(\mathcal{P}_k)^{i_1}(\eta_k\square_k)^{i_2}(\mathbb{H}_k)^{i_3}$$

where $\binom{a}{i_1,i_2,i_3}=\frac{a!}{i_1!i_2!i_3!}$. Denote

$$\square(m,k_j)=\frac{(-\frac{k_j}{2})^m}{q^{\frac{mk_j}{2}}}\sum_{\substack{\deg p_1,\dots,\deg p_m=\frac{k_j}{2}\\ p_1,\dots,p_m\text{ distinct}}}\chi_Q\left((p_1)^2\cdots(p_m)^2\right),\tag{5.1}$$

$$\Delta(2m,k_j)=\frac{(k_j)^{2m}}{q^{mk_j}}\sum_{\substack{\deg p_1,\dots,\deg p_m=k_j\\ p_1,\dots,p_m\text{ distinct}}}\chi_Q\left((p_1)^2\cdots(p_m)^2\right),\tag{5.2}$$

$$\mathcal{P}(m,k_j)=\frac{(k_j)^m}{q^{\frac{mk_j}{2}}}\sum_{\substack{\deg p_1,\dots,\deg p_m=k_j\\ p_1,\dots,p_m\text{ distinct}}}\chi_Q(p_1\cdots p_m).\tag{5.3}$$

Hence the product $\prod_{j=1}^n(\operatorname{tr}U^{k_j})^{a_j}$ gives various terms

(1) Squares: $\prod_{j=1}^n\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}(a_j-2i_j)!(\eta_{k_j})^{a_j-2i_j}\Delta(2i_j,k_j)\square(a_j-2i_j,k_j)$.
(2) Distinct primes: $\prod_{j=1}^n\mathcal{P}(a_j,k_j)$.

(3) Mixed terms – distinct primes and squares and some high powers:
$\prod_{j=1}^{n}\sum_{i_{j_1}+i_{j_2}=a_j}(\sum_{m=1}^{i_{j_1}}\mathcal{P}(m,k_j)\Delta(i_{j_1}-m,k_j))\square(i_{j_2},k_j)$. We can examine a specific term such as $\prod_{j=1}^{n}\mathcal{P}(m_j,k_j)\Delta(i_{j_1}-m_j,k_j)\square(i_{j_2},k_j)$ since the mixed terms are a finite sum of this kind of terms.

(4) Higher powers:
$\prod_{i=1}^{n}\frac{k_i/d_{i_1}\cdots k_i/d_{i_{m_i}}}{q^{\frac{k_i m_i}{2}}}\sum_{\deg p_{i_j}=k_i}\chi_Q\left(p_{i_1}^{d_{i_1}}\cdots p_{i_{m_i}}^{d_{i_{m_i}}}\right)$ where there is $1\leqslant i\leqslant n$; $1\leqslant j\leqslant m_i$ (at least one index) such that $d_{i_j}\geqslant 3$.

Our findings are, assuming $\sum_{j=1}^{n}a_jk_j\leqslant 2g-1$ and $\log_q g\ll\min(k_1a_1,\ldots,k_na_n)$:

$$\left\langle\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}(a_j-2i_j)!(\eta_{k_j})^{a_j-2i_j}\Delta(2i_j,k_j)\square(a_j-2i_j,k_j)\right\rangle$$
$$=\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}(k_j)^{i_j}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}(i_j)!}(-\eta_{k_j})^{a_j-2i_j}+O\left(\frac{1}{q^g}\right).$$

All the other terms contribute $o(1)$ under these terms.

5.2. Squares

Consider the term

$$\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}(a_j-2i_j)!(\eta_{k_j})^{a_j-2i_j}\Delta(2i_j,k_j)\square(a_j-2i_j,k_j)\tag{5.4}$$

which equals to

$$\sum_{i_1=0}^{\lfloor\frac{a_1}{2}\rfloor}\cdots\sum_{i_n=0}^{\lfloor\frac{a_n}{2}\rfloor}\prod_{j=1}^{n}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}(a_j-2i_j)!(\eta_{k_j})^{a_j-2i_j}\Delta(2i_j,k_j)\square(a_j-2i_j,k_j).$$

Hence it is enough to compute the expected value of the term $\prod_{j=1}^{n}\Delta(2i_j,k_j)\square(a_j-2i_j,k_j)$. This contributes to the product $\prod_{j=1}^{n}(\operatorname{tr}U^{k_j})^{a_j}$

$$\prod_{j=1}^{n}\frac{(k_j)^{2i_j}(\frac{-k_j}{2})^{a_j-2i_j}}{q^{\frac{k_j}{2}a_j}}\sum_{\substack{\deg p_{l,i_j}=k_j,\,1\leqslant l\leqslant i_j\\ \deg p_{l,i_j}=\frac{k_j}{2},\,2i_j\leqslant l\leqslant a_j}}\chi_Q\left(\prod_{j=1}^{n}\left(p_{1,j}^2\cdots p_{i_j,j}^2\right)\left(p_{2i_j,j}^2\cdots p_{a_j,j}^2\right)\right)$$

the sum is over different primes. To average we use Lemma 3.2

$$\left\langle\chi_Q\left(f^2\right)\right\rangle=1+O\left(\sum_{P\mid f}\frac{1}{\|P\|}\right).$$

Hence the average of $\prod_{j=1}^{n}\Delta(2i_j,k_j)\square(a_j-2i_j,k_j)$ is

$$\prod_{j=1}^{n}\frac{(k_j)^{2i_j}(\frac{-k_j}{2})^{a_j-2i_j}}{q^{\frac{k_j}{2}a_j}}\binom{\pi(k_j)}{i_j}\binom{\pi(\frac{k_j}{2})}{a_j-2i_j}\left(1+O\left(\frac{1}{q^{\min(k_1,\ldots,k_n)}}\right)\right).$$

The contribution of squares to the product $\prod_{j=1}^{n}(\operatorname{tr}U^{k_j})^{a_j}$ is

$$\begin{aligned}
&\sum_{i_1=0}^{\lfloor\frac{a_1}{2}\rfloor}\cdots\sum_{i_n=0}^{\lfloor\frac{a_n}{2}\rfloor}\prod_{j=1}^{n}\frac{(k_j)^{2i_j}(\frac{-k_j}{2})^{a_j-2i_j}}{q^{\frac{k_j}{2}a_j}}(\eta_{k_j})^{a_j-2i_j}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}(a_j-2i_j)!\binom{\pi(k_j)}{i_j}\binom{\pi(\frac{k_j}{2})}{a_j-2i_j}\\
&\quad\times\left(1+O\left(\frac{1}{q^{\min(k_1,\ldots,k_n)}}\right)\right)\\
&=\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}\frac{(k_j)^{2i_j}(\frac{-k_j}{2})^{a_j-2i_j}}{q^{\frac{k_j}{2}a_j}}(\eta_{k_j})^{a_j-2i_j}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}(a_j-2i_j)!\binom{\pi(k_j)}{i_j}\binom{\pi(\frac{k_j}{2})}{a_j-2i_j}\\
&\quad\times\left(1+O\left(\frac{1}{q^{\min(k_1,\ldots,k_n)}}\right)\right)\\
&=\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}\frac{(k_j)^{2i_j}(\frac{k_j}{2})^{a_j-2i_j}}{q^{\frac{k_j}{2}a_j}}(-\eta_{k_j})^{a_j-2i_j}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}}\frac{\pi(k_j)!\pi(\frac{k_j}{2})!}{(i_j)!(\pi(k_j)-i_j)!(\pi(\frac{k_j}{2})-a_j+2i_j)!}\\
&\quad\times\left(1+O\left(\frac{1}{q^{\min(k_1,\ldots,k_n)}}\right)\right)\\
&=\prod_{j=1}^{n}\sum_{i_j=0}^{\lfloor\frac{a_j}{2}\rfloor}(k_j)^{i_j}\binom{a_j}{2i_j}\frac{(2i_j)!}{2^{i_j}(i_j)!}(-\eta_{k_j})^{a_j-2i_j}+o(1).
\end{aligned}\tag{5.5}$$

5.3. Primes

In this section we focus on the contribution of different primes: Notice that the case of different primes is equivalent to the case of $a_j=1, 1\leqslant j\leqslant n$ and all the k_j's are different. Hence we consider the case of $\prod_{i=1}^{n}\mathcal{P}_{k_i}$. Assume (for the convenience of writing) $k_1=\min(k_1,\ldots,k_n)$. We use (3.3) and the explicit formula of (2.8) for the mean value of $\prod_{i=1}^{n}\mathcal{P}_{k_i}$:

$$\begin{aligned}
\left\langle\prod_{i=1}^{n}\mathcal{P}_{k_i}\right\rangle&=\frac{(-1)^n(\prod_{i=1}^{n}k_i)}{q^{\frac{\sum_{i=1}^{n}k_i}{2}+2g}(q-1)}\sum_{\deg P_i=k_i}\sum_{2\alpha+\beta=2g+1}\sum_{\substack{\deg A=\alpha\\ \gcd(A,P_i)=1}}\mu(A)\sum_{\deg B=\beta}\left(\frac{B}{\prod_{i=1}^{n}P_i}\right)\\
&=\frac{(-1)^n(\prod_{i=1}^{n}k_i)}{q^{\frac{\sum_{i=1}^{n}k_i}{2}+2g}(q-1)}\sum_{0\leqslant\alpha\leqslant g}\sigma(k_1,\ldots,k_n;\alpha)S(2g+1-2\alpha;k_1,\ldots,k_n).
\end{aligned}\tag{5.6}$$

If $\sum_{i=1}^{n}k_i<2g$, then for $\alpha=0$ and for $\alpha=1$ we have, by Lemma 4.1, $S(2g+1-2\alpha;k_1,\ldots,k_n)=0$. Now $\sigma(k_1,\ldots,k_n;\alpha)=0$ for $2\leqslant\alpha\leqslant k_1$ by Lemma 3.1. Thus it suffices to take $k_1\leqslant\alpha$ and $2g+1-2\alpha<\sum_{i=1}^{n}k_i$.

For this we use the Weil bound

$$S(2g+1-2\alpha;k_1,\dots,k_n) \ll \frac{(2g+1-2\alpha)^n}{k_1k_2\cdots k_n} q^{2g+1-2\alpha+\frac{\sum_{i=1}^n k_i}{2}} \tag{5.7}$$

to get

$$\begin{aligned}\left\langle \prod_{i=1}^n \mathcal{P}_{k_i} \right\rangle &= \frac{(\prod_{i=1}^n k_i)}{q^{\frac{\sum_{i=1}^n k_i}{2}+2g}(q-1)} \sum_{k_1 \leqslant \alpha \leqslant g} \sigma(k_1,\dots,k_n;\alpha) S(2g+1-2\alpha;k_1,\dots,k_n) \\ &\ll \frac{q(-1)^n}{(q-1)} \sum_{\max(k_1, g-\frac{\sum_{i=1}^n k_i-1}{2}) \leqslant \alpha \leqslant g} \sigma(k_1,\dots,k_n;\alpha) q^{-2\alpha}(2g+1-2\alpha)^n. \end{aligned} \tag{5.8}$$

Notice that $\sigma(k_1,\dots,k_n;\alpha) \ll q^{\alpha}$, hence the above term is bounded by

$$\frac{g^{n+1}}{q^{\max(k_1, g-\frac{\sum_{i=1}^n k_i-1}{2})-1}},$$

provided $(n+2)\log_q g < k_1$ this is $o(1)$.

5.4. Mixed terms: Primes and squares

Define $\prod_{j=1}^n \mathcal{P}(i_j-2m_j,k_j)\Delta(2m_j,k_j)\square(a_j-i_j,k_j)$ to be the contribution of primes, squares and some higher powers, to $\prod_{j=1}^n (\operatorname{tr} U^{k_j})^{a_j}$. In this case $i_j - 2m_j \neq 0$ for at least one of the j's, and for j such that k_j is odd we have $i_j = a_j$. For the convenience of writing we will bound the expected value of the term $\mathcal{P}(i-2m,k)\Delta(2m,k)\square(a-i,k)$. The expected value of the product will be bounded exactly in the same methods. We start by writing

$$\chi_Q\left(p_1^2\cdots p_l^2\right) = 1-\delta(Q,p_1\cdots p_l), \quad \delta(Q,p_1\cdots p_l) = \begin{cases} 1, & \gcd(Q,p_1^2\cdots p_l^2) \neq 1, \\ 0, & \gcd(Q,p_1^2\cdots p_l^2) = 1. \end{cases}$$

Define

$$\omega_Q^l(k_j) := \sum_{\substack{\deg p_1\cdots \deg p_l = k \\ p_1\dots p_l \text{ distinct}}} \delta(Q,p_1\cdots p_l) \tag{5.9}$$

the sum is over prime factors. This satisfies

$$\omega_Q^l(k_j) \leqslant \frac{2g+1}{k_j}\pi(k_j)^{l-1},$$

$$\square(a-i,k) = \frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}} \sum_{\substack{\deg p_1,\dots,\deg p_{a-i}=\frac{k}{2} \\ p_1,\dots,p_{a-i} \text{ distinct}}} \chi_Q\left((p_1)^2\cdots(p_{a-i})^2\right) = \frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}}\left(\binom{\pi(\frac{k}{2})}{a-i} - \omega_Q^{a-i}\left(\frac{k}{2}\right)\right),$$

$$\Delta(2m,k) = \frac{k^{2m}}{q^{mk}} \sum_{\substack{\deg p_1,\dots,\deg p_m=k \\ p_1,\dots,p_m \text{ distinct}}} \chi_Q\left((p_1)^2\cdots(p_m)^2\right) = \frac{k^{2m}}{q^{mk}}\left(\binom{\pi(k)}{m} - \omega_Q^m(k)\right).$$

Hence

$$\begin{aligned}&\mathcal{P}(i-2m,k)\Delta(2m,k)\square(a-i,k)\\&=\mathcal{P}(i-2m,k)\frac{k^{2m}}{q^{mk}}\left(\binom{\pi(k)}{m}-\omega_{\mathrm{Q}}^{m}(k)\right)\frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}}\left(\binom{\pi(\frac{k}{2})}{a-i}-\omega_{\mathrm{Q}}^{a-i}\left(\frac{k}{2}\right)\right).\end{aligned}$$

Notice that

$$\frac{k^{2m}}{q^{mk}}\binom{\pi(k)}{m}=\frac{k^m}{m!}+O\left(\sum_{l=1}^{m-1}\frac{k^{m+l}}{q^{lk}}\right) \tag{5.10}$$

$$\frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}}\binom{\pi(\frac{k}{2})}{a-i}=\frac{1}{(a-i)!}+O\left(\sum_{l=1}^{a-i-1}\frac{\frac{k}{2}^{l}}{q^{l\frac{k}{2}}}\right). \tag{5.11}$$

By (5.10), (5.11) and the prime section we have

$$\begin{aligned}&\left\langle\mathcal{P}(i-2m,k)\frac{k^{2m}}{q^{mk}}\binom{\pi(k)}{m}\frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}}\binom{\pi(\frac{k}{2})}{a-i}\right\rangle\sim\frac{k^m}{m!(a-i)!}\left\langle\mathcal{P}(i-2m,k)\right\rangle\\&\ll\frac{k^m}{m!(a-i)!}\frac{g^{i-2m+1}}{q^{\max(k,g-(i-2m)\frac{k}{2})}}\end{aligned}$$

which is $o(1)$ provided $k>a\log_q g$.

It is enough to compute the expected value of

$$\left\langle\mathcal{P}(i-2m,k)\frac{k^{2m}}{q^{mk}}\omega_{\mathrm{Q}}^{m}(k)\frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}}\omega_{\mathrm{Q}}^{a-i}\left(\frac{k}{2}\right)\right\rangle.$$

By the Cauchy–Schwartz inequality

$$\left\langle\mathcal{P}(i-2m,k)\frac{k^{2m}}{q^{mk}}\omega_{\mathrm{Q}}^{m}(k)\frac{(\frac{k}{2})^{a-i}}{q^{(a-i)\frac{k}{2}}}\omega_{\mathrm{Q}}^{a-i}\left(\frac{k}{2}\right)\right\rangle\leqslant\left\langle\left(\mathcal{P}(i-2m,k)\right)^2\right\rangle\frac{(2g+1)^2k^m}{q^{\frac{3k}{2}}}. \tag{5.12}$$

Next we show that $\langle(\mathcal{P}(i-2m,k))^2\rangle$ is polynomial in g. It follow that for $\log_q g\ll k$ the above is $o(1)$.

$$\begin{aligned}\left\langle\left(\mathcal{P}(i-2m,k)\right)^2\right\rangle&=\left\langle\left((\mathcal{P}_k)^{(i-2m)}-\Delta(2,k)(\mathcal{P}_k)^{(i-2m-2)}\right)^2\right\rangle\\&=\left\langle\left((\mathcal{P}_k)^{(2i-4m)}-2\Delta(2,k)(\mathcal{P}_k)^{2i-4m-2}+\left(\Delta(2,k)\right)^2(\mathcal{P}_k)^{2(i-2m-2)}\right)\right\rangle.\end{aligned}$$

We use on this term the same methods as before to have

$$\left\langle(\mathcal{P}_k)^{(2i-4m)}\right\rangle-2\left\langle\left(\frac{k^2}{q^k}\left(\pi(k)-\omega_{\mathrm{Q}}^{1}(k)\right)\right)(\mathcal{P}_k)^{2i-4m-2}\right\rangle+\left\langle\left(\left(\frac{k^2}{q^k}\left(\pi(k)-\omega_{\mathrm{Q}}^{1}(k)\right)\right)^2(\mathcal{P}_k)^{2(i-2m-2)}\right)\right\rangle$$

This comes down to bounding the general term $\langle(\mathcal{P}_k)^{2l}\rangle$, since

$$\left\langle\frac{k^2}{q^k}\pi(k)(\mathcal{P}_k)^{2i-4m-2}\right\rangle\sim k\left\langle(\mathcal{P}_k)^{2i-4m-2}\right\rangle;\quad\left\langle\left(\left(\frac{k^2}{q^k}\pi(k)\right)^2(\mathcal{P}_k)^{2(i-2m-2)}\right)\right\rangle\sim k^2\left\langle(\mathcal{P}_k)^{2(i-2m-2)}\right\rangle,$$

and for terms with $\omega_Q^1(k)$ we use the Cauchy–Schwartz inequality. For example

$$\left\langle \frac{k^2}{q^k}\omega_Q^1(k)(\mathcal{P}_k)^{2i-4m-2}\right\rangle \leqslant \frac{(2g+1)k}{q^k}\left\langle (\mathcal{P}_k)^{4i-8m-4}\right\rangle^{\frac{1}{2}}.$$

Lemma 5.1. *For $2g > k > 2l\log_q g$*

$$\left\langle (\mathcal{P}_k)^{2l}\right\rangle = O\left(g^l\right). \tag{5.13}$$

Proof. We will prove the lemma by induction.

For $\boldsymbol{l=1}$ we have

$$\left\langle (\mathcal{P}_k)^2\right\rangle = \left\langle \mathcal{P}(2,k)\right\rangle + \left\langle \Delta(2,k)\right\rangle.$$

By Section 5.3 (the prime section) we have $\langle \mathcal{P}(2,k)\rangle = o(1)$ For the second term we use (3.5)

$$\left\langle \Delta(2,k)\right\rangle = \frac{k^2}{q^k}\pi(k)\left(1+O\left(\frac{1}{q^k}\right)\right) = k + O\left(\frac{k}{q^k}\right).$$

In conclusion, for $2g > k > 2\log_q g$ we have

$$\left\langle (\mathcal{P}_k)^2\right\rangle = O(g).$$

For $\boldsymbol{l=2}$

$$\left\langle (\mathcal{P}_k)^4\right\rangle = \left\langle \mathcal{P}(4,k)\right\rangle + \left\langle \Delta(2,k)(\mathcal{P}_k)^2\right\rangle.$$

By Section 5.3 (the prime section) we have $\langle \mathcal{P}(4,k)\rangle = o(1)$. For the second term we use Cauchy–Schwartz inequality

$$\begin{aligned}\left\langle \Delta(2,k)(\mathcal{P}_k)^2\right\rangle &= \left\langle \frac{k^2}{q^k}\left(\pi(k)-\omega_Q^1(k)\right)(\mathcal{P}_k)^2\right\rangle \sim k\left\langle (\mathcal{P}_k)^2\right\rangle - \left\langle \frac{k^2}{q^k}\omega_Q^1(k)(\mathcal{P}_k)^2\right\rangle \\ &\leqslant k\left\langle (\mathcal{P}_k)^2\right\rangle + \frac{k(2g+1)}{q^k}\left\langle (\mathcal{P}_k)^2\right\rangle^{\frac{1}{2}}.\end{aligned}$$

By the case of $\boldsymbol{l=1}$ we have

$$\left\langle \mathcal{P}(4,k)\right\rangle = O\left(g^2\right).$$

For the case of *general* l:

$$\left\langle (\mathcal{P}_k)^{2l}\right\rangle = \left\langle \mathcal{P}(2l,k)\right\rangle + \left\langle \Delta(2,k)(\mathcal{P}_k)^{2l-2}\right\rangle.$$

By Section 5.3 (the prime section) we have $\langle \mathcal{P}(2l,k)\rangle = o(1)$. For the second term we use the same method as before to get

$$\left\langle \Delta(2,k)(\mathcal{P}_k)^{2l-2}\right\rangle \leqslant k\left\langle (\mathcal{P}_k)^{2l-2}\right\rangle + \frac{k(2g+1)}{q^k}\left\langle (\mathcal{P}_k)^{2l-2}\right\rangle.$$

By the induction

$$\left\langle (\mathcal{P}_k)^{2l-2} \right\rangle = O\left(g^{l-1}\right).$$

Hence, provided $2l \log_q g < k < 2g$ we have

$$\left\langle (\mathcal{P}_k)^{2l} \right\rangle = O\left(g^{l}\right).$$

This concludes the lemma. □

Going back we get $\langle (\mathcal{P}(i-2m,k))^2 \rangle$ is polynomial in g. It follows that the contribution of mixed terms of primes and squares to the expected value of the product of traces is $o(1)$.

5.5. Higher powers

We now consider the contribution of higher powers to the product of traces. These arise from terms with $\mathbb{H}_{k_j}$ or from the remaining terms which were not considered before (notice that some of the cases involving higher powers were considered in the previous section). These terms coincide up to division by factors such as $q^{\frac{k_j}{2}(1-\frac{1}{d})}$ (d is some finite integer), with the contribution of one of the previous types. Since the mean value of these previous terms is in all cases bounded by $g^{\sum_{i=1}^n a_i}$, after the division we get a negligible term (provided $\log_q g \ll \min(k_1, \ldots, k_n)$).

5.6. Conclusion of the proof

We saw that $\langle \prod_{j=1}^n (\operatorname{tr} U^{k_j})^{a_j} \rangle$ is the sum of the expected values of the Frobenius class of hyperelliptic curves of genus g over the field $\mathbb{F}_q$ of various terms:

(1) Squares: $\prod_{j=1}^n \sum_{i_j=0}^{\lfloor \frac{a_j}{2} \rfloor} \binom{a_j}{2i_j} \frac{(2i_j)!}{2^{i_j}} (a_j - 2i_j)! \Delta(2i_j, k_j) \square (a_j - 2i_j, k_j)$.
(2) Distinct primes: $\prod_{j=1}^n \mathcal{P}(a_j, k_j)$.
(3) Mixed terms – distinct primes and squares and some high powers:
$\prod_{j=1}^n \sum_{i_{j_1}+i_{j_2}=a_j} (\sum_{m=1}^{i_{j_1}} \mathcal{P}(m, k_j) \Delta(i_{j_1} - m, k_j)) \square (i_{j_2}, k_j)$.
(4) $\mathbb{H}_{k_1,\ldots,k_n}$ higher powers.

We saw that under the following condition: $k_j \in \{1, 2, \ldots\}$ for $1 \leqslant j \leqslant n$ are such that $\sum_{j=1}^n a_j k_j \leqslant 2g - 1$ for fixed integers a_j, and $\log_q g \ll \min(k_1, \ldots, k_n)$, the expected value of all the above terms is negligible – $o(1)$, except from the first term, the squares. This gives

$$\left\langle \prod_{j=1}^n \sum_{i_j=0}^{\lfloor \frac{a_j}{2} \rfloor} \binom{a_j}{2i_j} \frac{(2i_j)!}{2^{i_j}} (a_j - 2i_j)! \Delta(2i_j, k_j) \square (a_j - 2i_j, k_j) \right\rangle$$

$$= \prod_{j=1}^n \sum_{i_j=0}^{\lfloor \frac{a_j}{2} \rfloor} (k_j)^{i_j} \binom{a_j}{2i_j} \frac{(2i_j)!}{2^{i_j} (i_j)!} (-\eta_{k_j})^{a_j - 2i_j} + O\left(\frac{1}{q^g}\right).$$

Putting this together gives Theorem 1.1.

Acknowledgment

I would like to thank Professor Zeev Rudnick for his cooperative guidance and for many valuable comments during the creation of this paper.

References

[1] A. Bucur, C. David, B. Feigon, M. Lalín, Statistics for traces of cyclic trigonal curves over finite fields, Int. Math. Res. Not. IMRN 2010 (5) (2010) 932–967.
[2] P. Diaconis, S.N. Evans, Linear functionals of eigenvalues of random matrices, Trans. Amer. Math. Soc. 353 (2001) 2615–2633.
[3] P. Diaconis, M. Shahshahani, On the eigenvalues of random matrices, Studies in Applied Probability, J. Appl. Probab. 31A (1994) 49–62.
[4] C.P. Hughes, Z. Rudnick, Mock–Gaussian behavior for linear statistics of classical compact groups, J. Phys. A 36 (2003) 2919–2932.
[5] N.M. Katz, P. Sarnak, Random Matrices, Frobenius Eigenvalues, and Monodromy, Amer. Math. Soc. Colloq. Publ., vol. 45, Amer. Math. Soc., Providence, RI, 1999.
[6] P. Kurlberg, Z. Rudnick, The fluctuations in the number of points on a hyperelliptic curve over a finite field, J. Number Theory 129 (2009) 580–587.
[7] M. Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 210, Springer, New York, 2002.
[8] Z. Rudnick, Traces of high powers of the Frobenius class in the hyperelliptic ensemble, Acta Arith. 143 (2010) 81–99.
[9] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.