ACTA ARITHMETICA
143.1 (2010)

Traces of high powers of the Frobenius class in the hyperelliptic ensemble

by

Zeév Rudnick (Tel Aviv and Princeton, NJ)

1. Introduction. Fix a finite field $\mathbb{F}_q$ of odd cardinality, and let C be a nonsingular projective curve defined over $\mathbb{F}_q$. For each extension field of degree n of $\mathbb{F}_q$, denote by $N_n(C)$ the number of points of C in $\mathbb{F}_{q^n}$. The zeta function associated to C is defined as

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

and is known to be a rational function of u of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} \tag{1.1}$$

where $P_C(u)$ is a polynomial of degree $2g$ with integer coefficients, satisfying a functional equation

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

The Riemann Hypothesis, proved by Weil [19], is that the zeros of $P(u)$ all lie on the circle $|u| = 1/\sqrt{q}$. Thus one may give a spectral interpretation of $P_C(u)$ as the characteristic polynomial of a $2g \times 2g$ unitary matrix Θ_C:

$$P_C(u) = \det(I - u\sqrt{q}\,\Theta_C)$$

so that the eigenvalues $e^{i\theta_j}$ of Θ_C correspond to zeros $q^{-1/2}e^{-i\theta_j}$ of $Z_C(u)$. The matrix (or rather the conjugacy class) Θ_C is called the *unitarized Frobenius class* of C.

We would like to study how the Frobenius classes Θ_C change as we vary the curve over a family of hyperelliptic curves of genus g, in the limit of

2010 *Mathematics Subject Classification*: Primary 11G20.
Key words and phrases: hyperelliptic curve, random matrix theory, zeros of L-functions, one-level density.

DOI: 10.4064/aa143-1-5

large genus and fixed constant field. The particular family $\mathcal{H}_{2g+1}$ we choose is the family of all curves given in affine form by an equation

$$C_Q : y^2 = Q(x)$$

where

$$Q(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0 \in \mathbb{F}_q[x]$$

is a square-free, monic polynomial of degree $2g+1$. The curve C_Q is thus nonsingular and of genus g.

We consider $\mathcal{H}_{2g+1}$ as a probability space (ensemble) 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 [11] showed that as $q \to \infty$, the Frobenius classes Θ_Q become equidistributed in the unitary symplectic group $\mathrm{USp}(2g)$ (in genus one this is due to Birch [2] for q prime, and to Deligne [3]). That is, for any continuous function on the space of conjugacy classes of $\mathrm{USp}(2g)$,

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

This implies that various statistics of the eigenvalues can, in this limit, be computed by integrating the corresponding quantities over $\mathrm{USp}(2g)$.

Our goal is to explore the opposite limit, that of fixed constant field and large genus (q fixed, $g \to \infty$; cf. [13, 6]). Since the matrices Θ_Q now inhabit different spaces as g grows, it is not clear how to formulate an equidistribution problem. However, one can still meaningfully discuss various statistics, the most fundamental being various products of traces of powers of Θ_Q, that is, $\langle \prod_{j=1}^r \operatorname{tr} \Theta_Q^{n_j} \rangle$. Here we study the basic case of the expected values $\langle \operatorname{tr} \Theta_Q^n \rangle$, where n is of order of the genus g.

The mean value of traces of powers when averaged over the unitary symplectic group $\mathrm{USp}(2g)$ is easily seen [5] to be

$$\int\limits_{\mathrm{USp}(2g)} \operatorname{tr} U^n\, dU = \begin{cases} 2g, & n = 0, \\ -\eta_n, & 1 \le |n| \le 2g, \\ 0, & |n| > 2g, \end{cases} \tag{1.2}$$

where

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

We will show:

THEOREM 1. *For all $n > 0$ we have*

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \left\{ \begin{array}{ll} -\eta_n, & 0 < n < 2g, \\ -1 - 1/(q-1), & n = 2g, \\ 0, & n > 2g \end{array} \right\} + \eta_n \frac{1}{q^{n/2}} \sum_{\substack{\deg P | (n/2) \\ P \text{ prime}}} \frac{\deg P}{|P|+1} + O_q(nq^{n/2-2g} + gq^{-g}),$$

the sum over all irreducible monic polynomials P, and where $|P| := q^{\deg P}$.

In particular, we have

COROLLARY 2. *If $3 \log_q g < n < 4g - 5 \log_q g$ but $n \neq 2g$ then*

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \int_{\mathrm{USp}(2g)} \operatorname{tr} U^n \, dU + o\left(\frac{1}{g}\right).$$

We do however get deviations from the Random Matrix Theory results (1.2) for small values of n, for instance

$$\langle \operatorname{tr} \Theta_Q^2 \rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^2 \, dU + \frac{1}{q+1},$$

and for $n = 2g$ where we have

$$\langle \operatorname{tr} \Theta_Q^{2g} \rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^{2g} \, dU - \frac{1}{q-1}.$$

Analogous results can be derived for mean values of products, e.g. for $\langle \operatorname{tr} \Theta_Q^m \operatorname{tr} \Theta_Q^n \rangle$, when $m + n < 4g$; see §6.

To prove these results, we cannot use the powerful equidistribution theorem of Deligne [3], as was done for the fixed genus case in [11]. Rather, we use a variant of the analytic methods developed to deal with such problems in the number field setting [15, 10, 18]. Extending the range of our results to cover $n > 4g$ is a challenge.

1.1. Application: The one-level density. The traces of powers determine all *linear* statistics, such as the number of angles θ_j lying in a subinterval of $\mathbb{R}/2\pi\mathbb{Z}$, or the one-level density, a smooth linear statistic. To define the one-level density, we start with an even test function f, say in the Schwartz space $\mathcal{S}(\mathbb{R})$, and for any $N \geq 1$ set

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

which has period 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 $e^{i\theta_j}$, $j = 1, \dots, N$, 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.

Katz and Sarnak [9] conjectured that for fixed q, the expected value of Z_f over $\mathcal{H}_{2g+1}$ will converge to $\int_{\mathrm{USp}(2g)} Z_f(U)\, dU$ as $g \to \infty$ for *any* such test function f. Theorem 1 implies:

COROLLARY 3. *If $f \in \mathcal{S}(\mathbb{R})$ is even, with Fourier transform $\widehat{f}$ supported in $(-2, 2)$, then*

$$\langle Z_f \rangle = \int_{\mathrm{USp}(2g)} Z_f(U)\, dU + \frac{\mathrm{dev}(f)}{g} + o\left(\frac{1}{g}\right)$$

where

$$\mathrm{dev}(f) = \widehat{f}(0) \sum_{P\ prime} \frac{\deg P}{|P|^2 - 1} - \widehat{f}(1)\, \frac{1}{q-1},$$

the sum over all irreducible monic polynomials P.

To show Corollary 3, one uses a Fourier expansion to see that

$$Z_f(U) = \int_{-\infty}^{\infty} f(x)\, dx + \frac{1}{N} \sum_{n \neq 0} \widehat{f}\left(\frac{n}{N}\right) \mathrm{tr}\, U^n. \tag{1.3}$$

Averaging $Z_f(U)$ over the symplectic group $\mathrm{USp}(2g)$, using (1.2), and assuming f is even, gives ([1])

$$\int_{\mathrm{USp}(2g)} Z_f(U)\, dU = \widehat{f}(0) - \frac{1}{g} \sum_{1 \leq m \leq g} \widehat{f}\left(\frac{m}{g}\right)$$

and then we use Theorem 1 to deduce Corollary 3.

Corollary 3 is completely analogous to what is known in the number field setting for the corresponding case of zeta functions of quadratic fields, except for the lower order term which is different: While the coefficient of $\widehat{f}(0)$ is as in the number field setting [14], the coefficient of $\widehat{f}(1)$ is special to our function field setting.

2. Quadratic L-functions. In this section we give some known background on the zeta function of hyperelliptic curves. The theory was initiated by E. Artin [1]. We use Rosen [16] as a general reference.

([1]) Note that as $g \to \infty$, $\int_{\mathrm{USp}(2g)} Z_f(U)\, dU \sim \int_{-\infty}^{\infty} f(x) \left(1 - \frac{\sin 2\pi x}{2\pi x}\right) dx$.

2.1. 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 $f = P^k$ is a prime power in which case $\Lambda(P^k) = \deg P$.

The analogue of Riemann's zeta function is

$$\zeta_q(s) := \prod_{P \text{ prime}} (1 - |P|^{-s})^{-1},$$

which is shown to equal

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}}. \tag{2.1}$$

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

$$\pi_q(n) = \frac{q^n}{n} + O(q^{n/2}),$$

which follows from the identity (equivalent to (2.1))

$$\sum_{\deg f = n} \Lambda(f) = q^n, \tag{2.2}$$

the sum over all monic polynomials of degree n.

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

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

and the corresponding L-function

$$\mathcal{L}(u, \chi_D) := \prod_P (1 - \chi_D(P) u^{\deg P})^{-1}, \qquad |u| < \frac{1}{q},$$

the product over all monic irreducible (prime) polynomials P. Expanding in additive form using unique factorization, we write

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

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 $\beta \geq \deg D$ and hence the L-function is in fact a polynomial of degree at most $\deg D - 1$.

2.3. To proceed further, assume that D is square-free (and monic of positive degree). Then $\mathcal{L}(u,\chi_D)$ has a "trivial" zero at $u=1$ if and only if $\deg D$ is even. Thus

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

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

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

satisfying the functional equation

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

In fact, $\mathcal{L}^*(u,\chi_D)$ is the Artin L-function associated to the unique nontrivial quadratic character of $\mathbb{F}_q(x)(\sqrt{D(x)})$ (see [16, Propositions 17.7 and 14.6]). 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

$$A_D^*(\beta)=q^{\beta-\delta}A_D^*(2\delta-\beta). \tag{2.3}$$

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

2.4. For D monic, square-free, and of positive degree, the zeta function (1.1) of the hyperelliptic curve $y^2=D(x)$ is

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

The Riemann Hypothesis, proved by Weil [19], asserts that all zeros of $Z_C(u)$, hence of $\mathcal{L}^*(u,\chi_D)$, lie on the circle $|u|=1/\sqrt{q}$. Thus we may write

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

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

2.5. By taking a logarithmic derivative of the identity

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

which comes from writing $\mathcal{L}^*(u,\chi_D)=(1-u)^{-\lambda}\mathcal{L}(u,\chi_D)$, we find

$$-\operatorname{tr}\Theta_D^n=\frac{\lambda}{q^{n/2}}+\frac{1}{q^{n/2}}\sum_{\deg f=n}\Lambda(f)\chi_D(f). \tag{2.4}$$

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

$$\left|\sum_{\substack{\deg P=n\\ P\,\text{prime}}}\left(\frac{B}{P}\right)\right| \ll \frac{\deg B}{n}\, q^{n/2}. \tag{2.5}$$

This is deduced by writing $B = DC^2$ with D square-free, of positive degree, and then using the explicit formula (2.4) and the unitarity of Θ_D (which is the Riemann Hypothesis).

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 $\mathbb{F}_q[x]$. The cardinality of $\mathcal{H}_d$ is

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

as is seen by writing

$$\sum_{d\geq 0}\frac{\#\mathcal{H}_d}{q^{ds}} = \sum_{f\,\text{monic square-free}} |f|^{-s} = \frac{\zeta_q(s)}{\zeta_q(2s)}$$

and using (2.1). In particular, for $g \geq 1$,

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

We consider $\mathcal{H}_{2g+1}$ as a probability space (ensemble) 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 $\mathbb{F}_q[x]$ (as is done over the integers) via

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

Thus we may write expected values as

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

the sums over all monic A, B.

3.2. Averaging quadratic characters. Suppose now that we are given a polynomial $f \in \mathbb{F}_q[x]$ and apply (3.2) to the quadratic character $\chi_Q(f) = \left(\frac{Q}{f}\right)$. 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

$$\langle \chi_Q(f) \rangle = \frac{1}{(q-1)q^{2g}} \sum_{2\alpha+\beta=2g+1} \sigma(f;\alpha) \sum_{\deg B=\beta} \left(\frac{B}{f}\right),$$

where

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

3.3. A sum of Möbius values. Suppose P is a prime of degree n, and $k \geq 1$ and $\alpha \geq 0$. Set

$$\sigma_n(\alpha) := \sigma(P^k;\alpha) = \sum_{\substack{\deg A=\alpha \\ \gcd(A,P^k)=1}} \mu(A).$$

Since the conditions $\gcd(A,P^k)=1$ and $\gcd(A,P)=1$ are equivalent for a prime P and any $k \geq 1$, this quantity is independent of k; the notation anticipates that it depends only on the degree n of P, as is shown in:

Lemma 4.

(i) *For $n=1$,*

$$\sigma_1(0) = 1, \qquad \sigma_1(\alpha) = 1-q \quad \textit{for all } \alpha \geq 1.$$

(ii) *If $n \geq 2$ then*

$$\sigma_n(\alpha) = \begin{cases} 1, & \alpha = 0 \bmod n, \\ -q, & \alpha = 1 \bmod n, \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. Since P is prime,

$$\sigma_n(\alpha) = \sum_{\deg A=\alpha} \mu(A) - \sum_{\substack{\deg A=\alpha \\ P|A}} \mu(A) = \sum_{\deg A=\alpha} \mu(A) - \sum_{\deg A_1=\alpha-n} \mu(PA_1).$$

Now $\mu(PA_1) \neq 0$ only when A_1 is coprime to P, in which case $\mu(PA_1) = \mu(P)\mu(A_1) = -\mu(A_1)$. Hence

$$\sigma_n(\alpha) = \sum_{\deg A=\alpha} \mu(A) + \sum_{\substack{\deg A_1=\alpha-n \\ (P,A_1)=1}} \mu(A_1),$$

that is,

$$\sigma_n(\alpha) - \sigma_n(\alpha - n) = \sum_{\deg A = \alpha} \mu(A) = \begin{cases} 1, & \alpha = 0, \\ -q, & \alpha = 1, \\ 0, & \alpha \geq 2, \end{cases}$$

on using

$$\sum_{A \text{ monic}} \frac{\mu(A)}{|A|^s} = \frac{1}{\zeta_q(s)} = 1 - q^{1-s}$$

and (2.1). For $n \geq 2$ we get (ii), while for $n = 1$ we find that $\sigma_1(0) = 1$ and for $\alpha \geq 1$,

$$\sigma_1(\alpha) = \sigma_1(\alpha - 1) = \cdots = \sigma_1(1) = -q,$$

giving (i). ∎

3.4. The probability that $P \nmid Q$

LEMMA 5. *Let P be a prime. Then*

$$\langle \chi_Q(P^2) \rangle = \frac{|P|}{|P| + 1} + O(q^{-2g}).$$

Proof. Since P is prime, $\chi_Q(P^2) = 1$ unless P divides Q, that is, setting

$$\iota_P(f) := \begin{cases} 1, & P \nmid f, \\ 0, & P \mid f, \end{cases}$$

we have $\chi_Q(P^2) = \iota_P(Q)$ and thus, by (3.2),

$$\langle \chi_Q(P^2) \rangle = \langle \iota_P \rangle = \frac{1}{(q-1)q^{2g}} \sum_{\deg A^2 B = 2g+1} \mu(A) \iota_P(A^2 B).$$

Since P is prime, $P \nmid A^2 B$ if and only if $P \nmid A$ and $P \nmid B$. Hence

$$\langle \chi_Q(P^2) \rangle = \frac{1}{(q-1)q^{2g}} \sum_{0 \leq \alpha \leq g} \sum_{\deg A = \alpha,\, P \nmid A} \mu(A) \sum_{\deg B = 2g+1-2\alpha,\, P \nmid B} 1.$$

Writing $m := \deg P$, we get

$$\#\{B : \deg B = \beta,\, P \nmid B\} = q^\beta \times \begin{cases} 1 & \text{if } m > \beta, \\ 1 - 1/|P| & \text{if } m \leq \beta, \end{cases}$$

and

$$\sum_{\deg A = \alpha,\, P \nmid A} \mu(A) = \sigma_m(\alpha)$$

is computed in Lemma 4. Hence

$$\begin{aligned}\langle \chi_Q(P^2)\rangle &= \frac{1}{(q-1)q^{2g}} \sum_{0\le\alpha\le g} \sigma_m(\alpha) q^{2g+1-2\alpha} \\ &\quad \times \begin{cases} 1-1/|P|, & 0\le\alpha\le g-(m-1)/2, \\ 1, & g-(m-1)/2<\alpha\le g \end{cases} \\ &= \left(1-\frac{1}{|P|}\right)\frac{1}{1-1/q}\left(\sum_{\alpha=0}^{\infty}\frac{\sigma_m(\alpha)}{q^{2\alpha}} + O(q^{-2g})\right).\end{aligned}$$

Moreover, inserting the values of $\sigma_m(\alpha)$ given by Lemma 4 gives

$$\sum_{\alpha=0}^{\infty}\frac{\sigma_m(\alpha)}{q^{2\alpha}} = \frac{1-1/q}{1-1/|P|^2}$$

(this is valid for both $m=1$ and $m\ge 2$!) and hence

$$\begin{aligned}\langle \chi_Q(P^2)\rangle &= \left(1-\frac{1}{|P|}\right)\frac{1}{1-1/q}\,\frac{1-1/q}{1-1/|P|^2} + O(q^{-2g}) \\ &= \frac{|P|}{|P|+1} + O(q^{-2g})\end{aligned}$$

as claimed. ∎

4. Double character sums. We consider the double character sum

$$S(\beta;n) := \sum_{\substack{\deg P=n\\ P\text{ prime}}}\ \sum_{\substack{\deg B=\beta\\ B\text{ monic}}} \left(\frac{B}{P}\right).$$

We may express $S(\beta;n)$ in terms of the coefficients $A_P(\beta)=\sum_{\deg B=\beta}\chi_P(B)$ of the L-function $\mathcal{L}(u,\chi_P)=\sum_\beta A_P(\beta)u^\beta$:

$$S(\beta;n) = (-1)^{((q-1)/2)\beta n}\sum_{\deg P=n} A_P(\beta),$$

which follows from the law of quadratic reciprocity [16]: If A, B are monic then

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

Since $A_P(\beta)=0$ for $\beta\ge\deg P$, we find:

LEMMA 6. *For $n\le\beta$ we have*

$$S(\beta;n)=0.$$

4.1. Duality

PROPOSITION 7.

(i) *If n is odd and $0 \le \beta \le n-1$ then*

$$S(\beta;n) = q^{\beta-(n-1)/2} S(n-1-\beta;n), \tag{4.1}$$

$$S(n-1;n) = \pi_q(n) q^{(n-1)/2}. \tag{4.2}$$

(ii) *If n is even and $1 \le \beta \le n-2$ then*

$$S(\beta;n) = q^{\beta-n/2}\Big(-S(n-1-\beta;n) + (q-1)\sum_{j=0}^{n-\beta-2} S(j;n)\Big), \tag{4.3}$$

$$S(n-1;n) = -\pi_q(n) q^{(n-2)/2}. \tag{4.4}$$

Proof. Assume that $n = \deg P$ is odd. Then $\mathcal{L}(u,\chi_P) = \mathcal{L}^*(u,\chi_P)$, and so the coefficients $A_P(\beta) = A_P^*(\beta)$ coincide. Therefore the functional equation in the form (2.3) implies

$$A_P(\beta) = A_P(n-1-\beta) q^{\beta-(n-1)/2}, \quad n \text{ odd}, \ 0 \le \beta \le n-1.$$

Consequently, for n odd,

$$S(\beta;n) = q^{\beta-(n-1)/2} S(n-1-\beta;n), \quad n \text{ odd}, \ 0 \le \beta \le n-1.$$

In particular,

$$S(n-1;n) = q^{(n-1)/2} S(0,n) = q^{(n-1)/2}\pi_q(n), \quad n \text{ odd}.$$

Next, assume that $n = \deg P$ is even. Then $\mathcal{L}(u,\chi_P) = (1-u)\mathcal{L}^*(u,\chi_P)$, which implies that the coefficients of $\mathcal{L}(u,\chi_P)$ and $\mathcal{L}^*(u,\chi_P)$ satisfy

$$A_P(\beta) = A_P^*(\beta) - A_P^*(\beta-1), \quad \beta \ge 1,$$

and

$$A_P^*(\beta) = A_P(\beta) + A_P(\beta-1) + \cdots + A_P(0)\ . \tag{4.5}$$

Moreover,

$$A_P(0) = A_P^*(0), \quad A_P(n-1) = -A_P^*(n-2).$$

In particular, since

$$A_P^*(0) = 1, \quad A_P^*(n-2) = q^{(n-2)/2}$$

(see (2.3)), we get

$$A_P(n-1) = -A_P^*(n-2) = -q^{(n-2)/2}, \quad n \text{ even},$$

so that

$$S(n-1;n) = -\pi_q(n) q^{(n-2)/2}, \quad n \text{ even}.$$

The functional equation (2.3) implies

$$A_P^*(\beta) = A_P^*(n-2-\beta) q^{\beta-(n-2)/2}, \quad 0 \le \beta \le n-2,$$

and hence, for $1 \le \beta \le n-2$,

$$\begin{aligned} A_P(\beta) &= A_P^*(\beta) - A_P^*(\beta-1) \\ &= A_P^*(n-2-\beta)q^{\beta-(n-2)/2} - A_P^*(n-1-\beta)q^{\beta-n/2} \end{aligned}$$

and inserting (4.5) gives

$$A_P(\beta) = q^{\beta-n/2}\Big(-A_P(n-1-\beta) + (q-1)\sum_{j=0}^{n-\beta-2} A_P(j)\Big).$$

Summing over all primes P of degree n gives

$$S(\beta;n) = q^{\beta-n/2}\Big(-S(n-1-\beta;n) + (q-1)\sum_{j=0}^{n-\beta-2} S(j;n)\Big)$$

as claimed. ∎

4.2. An estimate for $S(\beta;n)$

LEMMA 8. *Suppose $\beta < n$. Then*

$$S(\beta;n) = \eta_\beta \pi_q(n) q^{\beta/2} + O\Big(\frac{\beta}{n}\, q^{n/2+\beta}\Big), \tag{4.6}$$

where $\eta_\beta = 1$ for β even, and $\eta_\beta = 0$ for β odd.

Proof. We write

$$S(\beta;n) = \sum_{\substack{B=\square \\ \deg B=\beta}} \sum_{\deg P=n} \Big(\frac{B}{P}\Big) + \sum_{\substack{B\neq\square \\ \deg B=\beta}} \sum_{\deg P=n} \Big(\frac{B}{P}\Big),$$

where the squares only occur when β is even.

For B not a perfect square, we use the Riemann Hypothesis for curves in the form (2.5):

$$\sum_{\deg P=n} \Big(\frac{B}{P}\Big) \ll \frac{\deg B}{n}\, q^{n/2}.$$

Hence summing over all nonsquare B of degree β, of which there are at most q^β, gives

$$\sum_{\substack{B\neq\square \\ \deg B=\beta}} \sum_{\deg P=n} \Big(\frac{B}{P}\Big) \ll \frac{\beta}{n}\, q^{\beta+n/2}.$$

Assume now that β is even. For $B = C^2$, we find that P and B are coprime since $\deg C = \beta/2 < n = \deg P$, and hence $\big(\frac{B}{P}\big) = \big(\frac{C^2}{P}\big) = +1$ and so the squares, of which there are $q^{\beta/2}$, contribute $\pi_q(n)q^{\beta/2}$. This proves (4.6). ∎

By using duality, (4.6) can be bootstrapped into an improved estimate when β is odd:

PROPOSITION 9. *If β is odd and $\beta < n$ then*

$$S(\beta;n) = -\eta_n \pi_q(n) q^{\beta-n/2} + O(q^n). \tag{4.7}$$

Proof. Assume n odd with $\beta < n$. Then by (4.1) for odd n,

$$S(\beta;n) = q^{\beta-(n-1)/2} S(n-1-\beta;n)$$

and inserting (4.6) with β replaced by $n-1-\beta$ (which is odd in this case) we get

$$S(n-1-\beta;n) \ll q^{n/2+n-1-\beta},$$

hence

$$S(\beta;n) \ll q^{\beta-(n-1)/2} q^{n/2+n-1-\beta} \ll q^n$$

as claimed.

Assume n even, with $\beta < n$. Using (4.3) and the bound (4.6) gives

$$\begin{aligned} S(\beta;n) &= q^{\beta-n/2}\Big(-S(n-1-\beta;n) + (q-1)\sum_{j=0}^{n-\beta-2} S(j;n)\Big) \\ &= q^{\beta-n/2}\Big(-\eta_{n-1-\beta}\pi_q(n) q^{(n-1-\beta)/2} + (q-1)\sum_{j=0}^{n-\beta-2} \eta_j \pi_q(n) q^{j/2}\Big) \\ &\quad + O\Big(q^{\beta-n/2}\sum_{j=0}^{n-1-\beta} \frac{j}{n}\, q^{n/2+j}\Big). \end{aligned}$$

The remainder term is $O(q^n)$. For the main term, we note that $n-1-\beta = 2L$ is even since β is odd and n is even, and then we can write the sum as

$$q^{\beta-n/2}\pi_q(n)\Big(-q^L + (q-1)\sum_{l=0}^{L-1} q^l\Big) = -q^{\beta-n/2}\pi_q(n),$$

which is our claim. ∎

5. Proof of Theorem 1. The explicit formula (2.4) says that for $n > 0$,

$$\operatorname{tr} \Theta_Q^n = -\frac{1}{q^{n/2}} \sum_{\deg f = n} \Lambda(f)\chi_Q(f),$$

the sum over all monic prime powers. We will separately treat the contributions $\mathcal{P}_n$ of primes, $\square_n$ of squares and $\mathbb{H}_n$ of higher odd powers of primes:

$$\operatorname{tr} \Theta_Q^n = \mathcal{P}_n + \square_n + \mathbb{H}_n\,. \tag{5.1}$$

5.1. The contribution of squares. When n is even, we have a contribution to $\operatorname{tr}\Theta_Q^n$ coming from squares of prime powers (for odd n this term does not appear), which give

$$\square_n = -\frac{1}{q^{n/2}} \sum_{\deg h = n/2} \Lambda(h)\chi_Q(h^2).$$

Since $\chi_Q(h^2) = 0$ or 1, we clearly have $\square_n \le 0$ and

$$\square_n \ge -\frac{1}{q^{n/2}} \sum_{\deg h = n/2} \Lambda(h) = -1$$

by (2.2). Hence the contribution of squares is certainly bounded.

Now for $h = P^k$ a prime power,

$$\langle \chi_Q(h^2)\rangle = \langle \chi_Q(P^2)\rangle = 1 - \frac{1}{|P|+1} + O(q^{-2g}) \tag{5.2}$$

by Lemma 5. Thus, recalling that $\sum_{\deg h = m} \Lambda(h) = q^m$ from (2.2), we deduce that the contribution of squares to the average is

$$\begin{aligned}\langle \square_n\rangle &= -1 + \frac{1}{q^{n/2}} \sum_{\deg P | (n/2)} \left((\deg P)\, \frac{1}{|P|+1} + O(q^{-2g}) \right) \\ &= -1 + \frac{1}{q^{n/2}} \sum_{\deg P | (n/2)} \frac{\deg P}{|P|+1} + O(q^{-2g}).\end{aligned} \tag{5.3}$$

In particular, we find that the contribution of squares to the average is

$$\langle \square_n\rangle = -1 + O\left(\frac{n}{q^{n/2}}\right) + O(q^{-2g})$$

and thus if $n \gg 3\log_q g$ we get

$$\langle \square_n\rangle = -\eta_n\left(1 + o\left(\frac{1}{g}\right)\right).$$

5.2. The contributions of primes. The contribution to $\operatorname{tr}\Theta_Q^n$ of primes is

$$\mathcal{P}_n = -\frac{n}{q^{n/2}} \sum_{\deg P = n} \chi_Q(P).$$

Proposition 10.

$$\langle \mathcal{P}_n\rangle = -\frac{n}{(q-1)q^{2g+n/2}} \sum_{\substack{\beta+2\alpha = 2g+1 \\ \alpha,\beta \ge 0}} \sigma_n(\alpha) S(\beta; n). \tag{5.4}$$

Moreover, if $n > g$ then

$$\langle \mathcal{P}_n\rangle = -\frac{n}{(q-1)q^{2g+n/2}} \left(S(2g+1; n) - qS(2g-1; n)\right). \tag{5.5}$$

Proof. Using (3.2) we have

$$\begin{aligned}\langle \mathcal{P}_n\rangle &= -\frac{n}{(q-1)q^{2g+n/2}} \sum_{\deg P=n} \sum_{\substack{\beta+2\alpha=2g+1\\ \alpha,\beta\ge 0}} \sigma_n(\alpha) \sum_{\deg B=\beta} \left(\frac{B}{P}\right)\\ &= -\frac{n}{(q-1)q^{2g+n/2}} \sum_{\substack{\beta+2\alpha=2g+1\\ \alpha,\beta\ge 0}} \sigma_n(\alpha) S(\beta;n),\end{aligned}$$

which gives (5.4).

Now assume that $n > g$. Then $\sigma_n(\alpha) \ne 0$ forces $\alpha = 0, 1 \bmod n$ by Lemma 4(ii) and together with $\alpha \le g < n$ we must have $\alpha = 0, 1$. Hence in (5.4) the only nonzero terms are those with $\alpha = 0, 1$, which gives (5.5). ∎

5.3. Bounding the contribution of primes. Assume first that $n \le g$. In (5.4), if $S(\beta;n) \ne 0$ then $\beta < n$ by Lemma 6. For those, we use the bound $|S(\beta;n)| \ll (\beta/n)q^{\beta+n/2}$ of Lemma 8 and hence

$$\langle \mathcal{P}_n\rangle \ll \frac{n}{q^{2g+n/2}} \sum_{\beta<n} \frac{\beta}{n}\, q^{n/2+\beta} \ll nq^{n-2g} \le gq^{-g} \tag{5.6}$$

(since $n \le g$), which vanishes as $g \to \infty$.

For $g < n < 2g$, use (5.5), and note that $S(2g \pm 1; n) = 0$ by Lemma 6. Hence

$$\langle \mathcal{P}_n\rangle = 0, \quad g < n < 2g.$$

5.3.1. *The case $n = 2g$.* We have $S(2g+1; 2g) = 0$ by Lemma 6, and $S(2g-1; 2g) = -\pi_q(2g)q^{(2g-2)/2}$ by (4.4). Hence

$$\begin{aligned}\langle \mathcal{P}_n\rangle &= -\frac{2g}{(q-1)q^{2g+g}} \left(S(2g+1, 2g) - qS(2g-1, 2g)\right)\\ &= -\frac{2g}{(q-1)q^{2g+g}}\, q\pi_q(2g)q^{(2g-2)/2} = -\frac{1}{q-1} + O(gq^{-g}).\end{aligned}$$

5.3.2. *The case $2g < n$.* Here we use (4.7) to find

$$\begin{aligned}\langle \mathcal{P}_n\rangle &= -\frac{n}{(q-1)q^{2g+n/2}} \left(S(2g+1; n) - qS(2g-1; n)\right)\\ &= -\frac{n}{(q-1)q^{2g+n/2}} \left(-\eta_n\pi_q(n)q^{2g+1-n/2} + q\eta_n\pi_q(n)q^{2g-1-n/2}\right)\\ &\quad + O\left(\frac{n}{q^{2g+n/2}}\, q^n\right)\\ &= \eta_n \frac{n\pi_q(n)}{q^n} + O(nq^{n/2-2g}) = \eta_n(1 + O(gq^{-g})) + O(nq^{n/2-2g}).\end{aligned}$$

The main term is asymptotic to η_n, and the remainder is $o(1/g)$ provided

$$2g < n < 4g - 5\log_q g.$$

5.4. The contribution of higher prime powers. The contribution of odd powers of primes P^d, $d>1$ odd, $\deg P^d = n$, is

$$\mathbb{H}_n = -\frac{1}{q^{n/2}} \sum_{\substack{d|n\\ 3\le d \text{ odd}}} \sum_{\deg P = n/d} \frac{n}{d}\, \chi_Q(P^d).$$

Since $\chi_Q(P^d) = \chi_Q(P)$ for d odd, the average is

$$\begin{aligned}\langle \mathbb{H}_n\rangle &= -\frac{1}{(q-1)q^{2g+n/2}} \sum_{\substack{d|n\\ 3\le d \text{ odd}}} \frac{n}{d} \sum_{\deg P = n/d} \sum_{2\alpha+\beta = 2g+1} \sigma_{n/d}(\alpha) \sum_{\deg B=\beta} \left(\frac{B}{P}\right)\\ &= -\frac{1}{(q-1)q^{2g+n/2}} \sum_{\substack{d|n\\ 3\le d \text{ odd}}} \frac{n}{d} \sum_{2\alpha+\beta = 2g+1} \sigma_{n/d}(\alpha) S\left(\beta; \frac{n}{d}\right).\end{aligned}$$

In order that $S(\beta; n/d) \neq 0$ we need $\beta < n/d$. Thus using the bound $S(\beta; n/d) \ll q^{\beta + n/2d}$ of (4.6) (recall that $\beta \le 2g+1$ is odd here) gives

$$\begin{aligned}\langle \mathbb{H}_n\rangle &\ll \frac{1}{q^{2g+n/2}} \sum_{\substack{d|n\\ 3\le d \text{ odd}}} \frac{n}{d} \sum_{\beta \le \min(n/d, 2g+1)} q^{n/2d+\beta}\\ &\ll \frac{n}{q^{2g+n/2}} \sum_{\substack{d|n\\ 3\le d \text{ odd}}} q^{n/2d + \min(2g, n/d)}.\end{aligned}$$

Treating separately the cases $n/3 < 2g$ and $n/3 \ge 2g$ we see that we have in either case

$$\langle \mathbb{H}_n\rangle \ll g q^{-2g}. \tag{5.7}$$

5.5. Conclusion of the proof. We saw that

$$\langle \operatorname{tr} \Theta_Q^n\rangle = \langle \mathcal{P}_n\rangle + \langle \square_n\rangle + \langle \mathbb{H}_n\rangle$$

with the individual terms giving

$$\begin{aligned}\langle \mathcal{P}_n\rangle &= \begin{cases} O(gq^{-g}), & 0<n<2g,\\ -1/(q-1) + O(gq^{-g}), & n=2g,\\ \eta_n + O(nq^{n/2-2g}), & 2g<n,\end{cases}\\ \langle \square_n\rangle &= -\eta_n + \eta_n \frac{1}{q^{n/2}} \sum_{\deg P | (n/2)} \frac{\deg P}{|P|+1} + O(q^{-2g}),\\ \langle \mathbb{H}_n\rangle &= O(gq^{-2g}).\end{aligned}$$

Putting these together gives Theorem 1. In particular,

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \left\{ \begin{array}{ll} -\eta_n, & 3\log_q g < n < 2g, \\ -1 - 1/(q-1), & n = 2g, \\ 0, & 2g < n < 4g - 8\log_q g \end{array} \right\} + o\Big(\frac{1}{g}\Big).$$

6. The product of two traces. Using the methods of this paper, one can also compute mean values of products of traces. For the product of two traces, the results can be stated as follows:

Assume $\min(m,n) \gg \log g$ and $m + n \le 4g - 100\log_q g$. Then

(i) If $m = n$ then

$$\langle |\operatorname{tr} \Theta_Q^n|^2 \rangle \sim \begin{cases} n + \eta_n, & n < g, \\ n + \eta_n + \frac{1}{q-1}, & n = g, \\ n - 1 + \eta_n, & g < n < 2g - 50\log_q g. \end{cases} \tag{6.1}$$

(ii) If $m < n$ then for "generic" values of (m,n) we have

$$\langle \operatorname{tr} \Theta_Q^m \operatorname{tr} \Theta_Q^n \rangle \sim \begin{cases} \eta_m\eta_n, & m + n < 2g, \\ \eta_m\eta_n - \eta_{m+n}, & n < 2g,\ m + n > 2g, \\ -\eta_{m+n}, & n > 2g,\ n - m < 2g, \\ 0, & n - m > 2g, \end{cases} \tag{6.2}$$

while on "exceptional" lines we have

$$\langle \operatorname{tr} \Theta_Q^m \operatorname{tr} \Theta_Q^n \rangle \sim \begin{cases} \eta_m\eta_n + \frac{1}{q-1}, & m + n = 2g, \\ \eta_m\eta_n - \eta_{m+n} + \eta_m\frac{1}{q-1}, & n = 2g, \\ -\frac{q}{q-1}\eta_{m+n}, & n - m = 2g. \end{cases} \tag{6.3}$$

The expected values for the symplectic group are (cf. [5, 4, 8, 12]):

(i) If $m = n$ then

$$\int\limits_{\mathrm{USp}(2g)} |\operatorname{tr} U^n|^2\, dU = \begin{cases} n + \eta_n, & 1 \le n \le g, \\ n - 1 + \eta_n, & g + 1 \le n \le 2g, \\ 2g, & n > 2g. \end{cases} \tag{6.4}$$

(ii) If $1 \le m < n$ then

$$\int\limits_{\mathrm{USp}(2g)} \operatorname{tr} U^m \operatorname{tr} U^n\, dU = \begin{cases} \eta_m\eta_n, & m + n \le 2g, \\ \eta_m\eta_n - \eta_{m+n}, & m < n \le 2g,\ m + n > 2g, \\ -\eta_{m+n}, & n > 2g,\ n - m \le 2g, \\ 0, & n - m > 2g. \end{cases} \tag{6.5}$$

Comparing (6.4), (6.5) with (6.2), (6.3) we find that if $m = \min(m,n) \gg \log_q g$ and $m + n < 4g - 100\log_q g$ then for "generic" values of (m,n), that

is, if $n, m \neq 2g$ and $|n \pm m| \neq 2g$, we have

$$\langle \operatorname{tr} \Theta_Q^m \operatorname{tr} \Theta_Q^n \rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^m \operatorname{tr} U^n \, dU, \tag{6.6}$$

while on the lines $n, m = 2g$, $|n \pm m| = 2g$ the difference between the averages over $\mathcal{H}_{2g+1}$ and $\mathrm{USp}(2g)$ is bounded by

$$\left| \langle \operatorname{tr} \Theta_Q^m \operatorname{tr} \Theta_Q^n \rangle - \int_{\mathrm{USp}(2g)} \operatorname{tr} U^m \operatorname{tr} U^n \, dU \right| \leq \frac{1}{q-1} + o(1), \quad g \to \infty.$$

These results can be used to study the two-level density (cf. [17, 7]).

Acknowledgments. We thank Pär Kurlberg and Nicolas Templier for their comments.

This research was supported by the Israel Science Foundation (grant No. 925/06) and by the Oswald Veblen Fund at the Institute for Advanced Study, Princeton.

References

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*, Math. Z. 19 (1924), 153–246.

[2] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. 43 (1968), 57–60.

[3] P. Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. 52 (1980), 137–252.

[4] P. Diaconis and S. N. Evans, *Linear functionals of eigenvalues of random matrices*, Trans. Amer. Math. Soc. 353 (2001), 2615–2633.

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

[6] D. Faifman and Z. Rudnick, *Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field*, preprint, 2008, arXiv:0803.3534.

[7] P. Gao, *n-level density of the low-lying zeros of quadratic Dirichlet L-functions*, preprint, 2008, arXiv:0806.4830v1.

[8] C. P. Hughes and Z. Rudnick, *Mock-Gaussian behaviour for linear statistics of classical compact groups*, J. Phys. A 36 (2003), 2919–2932.

[9] N. M. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) 36 (1999), 1–26.

[10] —, —, Appendix to [9], unpublished.

[11] —, —, *Random Matrices, Frobenius Eigenvalues, and Monodromy*, Amer. Math. Soc. Colloq. Publ. 45, Amer. Math. Soc., Providence, RI, 1999.

[12] J. P. Keating and B. E. Odgers, *Symmetry transitions in random matrix theory & L-functions*, Comm. Math. Phys. 281 (2008), 499–528.

[13] P. Kurlberg and Z. Rudnick, *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory 129 (2009), 580–587.

[14] S. J. Miller, *A symplectic test of the L-functions ratios conjecture*, Int. Math. Res. Notices 2008, no. 3.

[15] A. E. Özlük and C. Snyder, *Small zeros of quadratic L-functions*, Bull. Austral. Math. Soc. 47 (1993), 307–319.
[16] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, New York, 2002.
[17] M. Rubinstein, *Low-lying zeros of L-functions and random matrix theory*, Duke Math. J. 109 (2001), 147–181.
[18] K. Soundararajan, *Nonvanishing of quadratic Dirichlet L-functions at $s = 1/2$*, Ann. of Math. (2) 152 (2000), 447–488.
[19] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

Zeév Rudnick
Raymond and Beverly Sackler School
of Mathematical Sciences
Tel Aviv University
Tel Aviv 69978, Israel
E-mail: rudnick@post.tau.ac.il

School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540, U.S.A.

Received on 7.4.2009
and in revised form on 2.9.2009 (5995)