COMPOSITIO MATHEMATICA

Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field

Dmitry Faifman and Zeév Rudnick

Compositio Math. **146** (2010), 81–101.

doi:10.1112/S0010437X09004308

FOUNDATION
COMPOSITIO
MATHEMATICA

The London Mathematical Society

Compositio Math. 146 (2010) 81–101
doi:10.1112/S0010437X09004308

Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field

Dmitry Faifman and Zeév Rudnick

Abstract

We study the fluctuations in the distribution of zeros of zeta functions of a family of hyperelliptic curves defined over a fixed finite field, in the limit of large genus. According to the Riemann hypothesis for curves, the zeros all lie on a circle. Their angles are uniformly distributed, so for a curve of genus g a fixed interval $\mathcal{I}$ will contain asymptotically $2g|\mathcal{I}|$ angles as the genus grows. We show that for the variance of number of angles in $\mathcal{I}$ is asymptotically $(2/\pi^2)\log(2g|\mathcal{I}|)$ and prove a central limit theorem: the normalized fluctuations are Gaussian. These results continue to hold for shrinking intervals as long as the expected number of angles $2g|\mathcal{I}|$ tends to infinity.

1. Introduction

Let C be a smooth, projective, geometrically connected curve of genus $g \geqslant 1$ defined over a finite field $\mathbb{F}_q$ of cardinality q. The zeta function of the curve is defined as

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

where N_n is the number of points on C with coefficients in an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ of degree n. The zeta function 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 $P(0) = 1$, satisfies the functional equation

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

and has all its zeros on the circle $|u| = 1/\sqrt{q}$ (this is the Riemann hypothesis for curves [Wei48]). Moreover, there is a unitary symplectic matrix $\Theta_C \in \mathrm{USp}(2g)$, defined up to conjugacy, so that

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

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

Our goal is to study the statistics of the set of angles $\{\theta_{j,C}\}$ as we draw C at random from a family of hyperelliptic curves of genus g defined over $\mathbb{F}_q$ where q is assumed to be odd. The family, denoted by $\mathcal{H}_{2g+2,q}$, is that of curves having an affine equation of the form $y^2 = Q(x)$,

Received 13 May 2008, accepted in final form 22 April 2009, published online 11 December 2009.
2000 Mathematics Subject Classification 11G20 (primary), 14G10, 15A52 (seconadary).
Keywords: hyperelliptic curve, random matrix theory, central limit theorem, zeros of L-functions.
Supported by the Israel Science Foundation (grant No. 925/06).

with $Q \in \mathbb{F}_q[x]$ a monic, square-free polynomial of degree $2g+2$. The corresponding function field is called a real quadratic function field. The measure on $\mathcal{H}_{2g+2,q}$ is simply the uniform probability measure on the set of such polynomials Q.

A fundamental statistic is the counting function of the angles. Thus for an interval[1] $\mathcal{I} = [-\beta/2, \beta/2]$ (which may vary with the genus g or with q), let

$$N_{\mathcal{I}}(C) = \#\{j : \theta_{j,C} \in \mathcal{I}\}.$$

The angles are uniformly distributed as $g \to \infty$ (see Proposition 5.1): for fixed $\mathcal{I}$,

$$N_{\mathcal{I}}(C) \sim 2g|\mathcal{I}|\,.$$

We wish to study the fluctuations of $N_{\mathcal{I}}$ as we vary C in $\mathcal{H}_{2g+2,q}$. This is in analogy to the work of Selberg [Sel44, Sel46a, Sel46b], who studied the fluctuations in the number $N(t)$ of zeros of the Riemann zeta function $\zeta(s)$ up to height t. By the Riemann–von Mangoldt formula,

$$N(t) = \frac{t}{2\pi}\log\frac{t}{2\pi e} + \frac{7}{8} + S(t) + O\left(\frac{1}{t}\right)$$

with $S(t) = (1/\pi)\arg\zeta(1/2+it)$. Selberg showed that the variance of $S(t)$, for t picked uniformly in $[0,T]$, is $(1/2\pi^2)\log\log T$, and that the moments of $S(t)/\sqrt{(1/2\pi^2)\log\log t}$ are those of a standard Gaussian.

Katz and Sarnak [KS99a] showed that for fixed genus, the conjugacy classes $\{\Theta_C : C \in \mathcal{H}_{2g+2,q}\}$ become uniformly distributed in $\mathrm{USp}(2g)$ in the limit $q \to \infty$ of large constant field size. In particular the statistics of $N_{\mathcal{I}}$ are the same as those of the corresponding quantity for a random matrix in $\mathrm{USp}(2g)$. That is, if $U \in \mathrm{USp}(2g)$ is a unitary symplectic matrix, with eigenvalues $e^{2\pi i\theta_j(U)}$, $j = 1, \dots, 2g$, set

$$\widehat{N}_{\mathcal{I}}(U) = \#\{j : \theta_j(U) \in \mathcal{I}\}.$$

Then the work of Katz and Sarnak [KS99a] gives

$$\lim_{q\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+2,q}}(N_{\mathcal{I}}(C) = k) = \mathrm{Prob}_{\mathrm{USp}(2g)}(\widehat{N}_{\mathcal{I}}(U) = k). \tag{1.2}$$

In the limit of large matrix size, the statistics of $\widehat{N}_{\mathcal{I}}(U)$ and related quantities, such as the logarithm of the characteristic polynomial of U, have been found to have Gaussian fluctuations in various ensembles of random matrices [BF97, CL95, DE01, HKO01, Joh97, KS00, Pol89, Sos00, Wie02]. In particular, when averaged over $\mathrm{USp}(2g)$, the expected value of $\widehat{N}_I$ is $2g|\mathcal{I}|$, the variance is $(2/\pi^2)\log(2g|\mathcal{I}|)$ and the normalized random variable $(\widehat{N}_{\mathcal{I}} - 2g|\mathcal{I}|)/\sqrt{(2/\pi^2)\log(2g|\mathcal{I}|)}$ has a normal distribution as $g \to \infty$. Moreover this holds for shrinking intervals, that is if we take the length of the interval $|\mathcal{I}| \to 0$ as $g \to \infty$ as long as the expected number of angles tends to infinity,[2] that is as long as $2g|\mathcal{I}| \to \infty$. Thus (1.2) implies that for the iterated limit $\lim_{g\to\infty}(\lim_{q\to\infty})$ we get a Gaussian distribution:

$$\lim_{g\to\infty}\left(\lim_{q\to\infty}\mathrm{Prob}_{\mathcal{H}_{2g+2,q}}\left(a < \frac{N_{\mathcal{I}}(C) - 2g|\mathcal{I}|}{\sqrt{(2/\pi^2)\log(2g|\mathcal{I}|)}} < b\right)\right) = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-x^2/2}\,dx.$$

In this paper we will study these problems for a *fixed* constant field $\mathbb{F}_q$ in the limit of large genus $g \to \infty$, that is without first taking $q \to \infty$, which was crucial to the approach of Katz and Sarnak. We will show that as $g \to \infty$, for both the global regime ($|\mathcal{I}|$ fixed) and the

[1] Due to the functional equation, it suffices to restrict the discussion to symmetric intervals.
[2] This is sometime called the 'mesoscopic' regime.

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

mesoscopic regime ($|\mathcal{I}| \to 0$ while $2g|\mathcal{I}| \to \infty$), the expected value of $N_{\mathcal{I}}$ is $2g|\mathcal{I}|$, the variance is asymptotically $(2/\pi^2)\log(2g|\mathcal{I}|)$ and that the fluctuations are Gaussian, that is, for fixed $a < b$,

$$\lim_{g\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+2,q}}\left(a < \frac{N_{\mathcal{I}} - 2g|\mathcal{I}|}{\sqrt{(2/\pi^2)\log(2g|\mathcal{I}|)}} < b\right) = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-x^2/2}\,dx. \tag{1.3}$$

Our argument hinges upon the fact that $P_C(u)$ is the L-function attached to a quadratic character of $\mathbb{F}_q[x]$. Thus for Q monic, square free, of degree $2g+2$ the quadratic character χ_Q is defined in terms of the quadratic residue symbol as $\chi_Q(f) = Q/f$ (see § 2.2). The associated L-function is

$$\mathcal{L}(u, \chi_Q) = \prod_P (1 - \chi_Q(u)u^{\deg P})^{-1}$$

the product taken over all monic irreducible polynomials $P \in \mathbb{F}_q[x]$. Then

$$P_C(u) = (1-u)^{-1}\mathcal{L}(u, \chi_Q)$$

as was found in Artin's thesis [Art24]. Thus one may tackle the problem using Selberg's original arguments [Sel44] adapted to the function field setting;[3] this was carried out in the M.Sc. thesis of the first-named author [Fai08]. Instead we follow a quicker route, via the explicit formula, used in forthcoming work by Hughes, Ng and Soundararajan.

An important challenge is to investigate the local regime, when the length of the interval is of order $1/2g$ as $g \to \infty$. Due to the central limit theorem for random matrices, we may rewrite (1.3) as

$$\begin{aligned}\lim_{g\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+2,q}}\left(a < \frac{N_{\mathcal{I}} - 2g|\mathcal{I}|}{\sqrt{(2/\pi^2)\log(2g|\mathcal{I}|)}} < b\right)\\ = \lim_{g\to\infty} \mathrm{Prob}_{\mathrm{USp}(2g)}\left(a < \frac{\widehat{N}_{\mathcal{I}} - 2g|\mathcal{I}|}{\sqrt{(2/\pi^2)\log(2g|\mathcal{I}|)}} < b\right)\end{aligned} \tag{1.4}$$

and ask if (1.4) remains valid also for shrinking intervals of the form $\mathcal{I} = (1/2g)\mathcal{J}$ where $\mathcal{J}$ is fixed, when the result is no longer a Gaussian. An equivalent form of (1.4) was conjectured in [KS99b].

2. Background on Dirichlet characters and L-functions

2.1 L-functions over the rational function field

We review some generalities about Dirichlet L-functions for the rational function field; see [Ros02] for details.

The norm of a nonzero polynomial $f \in \mathbb{F}_q[x]$ is defined as $\|f\| = q^{\deg f}$. The zeta function of the rational function field is

$$\zeta_q(s) := \prod_P (1 - \|P\|^{-s})^{-1}, \quad \Re(s) > 1$$

the product over all irreducible monic polynomials ('primes') in $\mathbb{F}_q[x]$. In terms of the more convenient variable

$$u = q^{-s}$$

[3] The paper [Sel44] is under the Riemann hypothesis; [Sel46a, Sel46b] are unconditional.

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

the zeta function becomes

$$Z(u) = \prod_P (1 - u^{\deg P})^{-1}, \quad |u| < 1/q.$$

By the fundamental theorem of arithmetic in $\mathbb{F}_q[x]$, $Z(u)$ can be expressed as a sum over all monic polynomials,

$$Z(u) = \sum_{f \text{ monic}} u^{\deg f},$$

and hence

$$Z(u) = \frac{1}{1 - qu}.$$

Given a monic polynomial $Q \in \mathbb{F}_q[x]$, a Dirichlet character modulo Q is a homomorphism

$$\chi : (\mathbb{F}_q[x]/Q\mathbb{F}_q[x])^\times \to \mathbb{C}^\times.$$

A character modulo Q is *primitive* if there is no proper divisor $\tilde{Q}$ of Q and some character $\tilde{\chi}$ mod $\tilde{Q}$ so that $\chi(n) = \tilde{\chi}(n)$ whenever $\gcd(n, Q) = 1$.

For a Dirichlet character χ modulo Q of $\mathbb{F}_q[x]$, we form the L-function

$$\mathcal{L}(u, \chi) = \prod_P (1 - \chi(P) u^{\deg P})^{-1} \tag{2.1}$$

(convergent for $|u| < 1/q$), where P runs over all monic irreducible polynomials. It can be expressed as a series

$$\mathcal{L}(u, \chi) = \sum_f \chi(f) u^{\deg f} \tag{2.2}$$

where the sum is over all monic polynomials. If χ is nontrivial, then it is easy to show that

$$\sum_{\deg f = n} \chi(f) = 0, \quad n \geqslant \deg Q$$

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

One needs to distinguish 'even' characters from the rest, where 'even' means $\chi(cH) = \chi(H)$, for all $c \in \mathbb{F}_q^\times$. The analogue for ordinary Dirichlet characters is $\chi(-1) = 1$. For even characters, the L-function has a trivial zero at $u = 1$.

We assume from now on that $\deg Q > 0$ and that χ is primitive. One then defines a 'completed' L-function

$$\mathcal{L}^*(u, \chi) = (1 - \lambda_\infty(\chi) u)^{-1} \mathcal{L}(u, \chi)$$

where $\lambda_\infty(\chi) = 1$ if χ is 'even', and is zero otherwise. The completed L-function $\mathcal{L}^*(u, \chi)$ is then a polynomial of degree

$$D = \deg Q - 1 - \lambda_\infty(\chi)$$

and satisfies the functional equation

$$\mathcal{L}^*(u, \chi) = \epsilon(\chi)(q^{1/2} u)^D \mathcal{L}^*\left(\frac{1}{qu}, \chi^{-1}\right)$$

with $|\epsilon(\chi)| = 1$. We express $\mathcal{L}^*(u, \chi)$ in term of its inverse zeros as

$$\mathcal{L}^*(u, \chi) = \prod_{j=1}^{D} (1 - \alpha_{j,\chi} u). \tag{2.3}$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

The Riemann hypothesis in this setting, proved by Weil [Wei48], is that all $|\alpha_{j,\chi}| = \sqrt{q}$. We may thus write

$$\alpha_{j,\chi} = \sqrt{q} e^{2\pi i \theta_{j,\chi}} \tag{2.4}$$

for suitable phases $\theta_{j,\chi} \in \mathbb{R}/\mathbb{Z}$. As a consequence, for any nontrivial character, not necessarily primitive, the inverse zeros of the L-function all have absolute value $\sqrt{q}$ or 1.

LEMMA 2.1. *Let χ be a nontrivial Dirichlet character modulo f. Then for $n < \deg f$,*

$$\left| \sum_{\deg B = n} \chi(B) \right| \leqslant \binom{\deg f - 1}{n} q^{n/2}$$

(the sum over all monic polynomials of degree n).

Proof. Indeed, all we need to do is compare the series expansion (2.2) of $\mathcal{L}(u, \chi)$, which is a polynomial of degree at most $\deg f - 1$, with the expression in terms of the inverse zeros:

$$\sum_{0 \leqslant n < \deg f} \left(\sum_{\deg B = n} \chi(B) \right) u^n = \prod_{j=1}^{\deg f - 1} (1 - \alpha_j u)$$

to get

$$\sum_{\deg B = n} \chi(B) = (-1)^n \sum_{\substack{S \subset \{1, \dots, \deg f - 1\} \\ \#S = n}} \prod_{j \in S} \alpha_j$$

and then use $|\alpha_j| \leqslant \sqrt{q}$. □

Note that for $n \geqslant \deg f$ the character sum vanishes.

2.2 Quadratic characters

We assume from now on that q is odd. Let $P(x) \in \mathbb{F}_q[x]$ be monic and irreducible. The quadratic residue symbol $(f/P) \in \{\pm 1\}$ is defined for f coprime to P by

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

For arbitrary monic Q, the Jacobi symbol f/Q is defined for f coprime to Q by writing $Q = \prod P_j$ as a product of monic irreducibles and setting

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

If f, Q are not coprime we set $(f/Q) = 0$. If $c \in \mathbb{F}_q^*$ is a scalar then

$$\left(\frac{c}{Q}\right) = c^{((q-1)/2) \deg Q}. \tag{2.5}$$

The law of quadratic reciprocity asserts that if $A, B \in \mathbb{F}_q[x]$ are monic and coprime then

$$\left(\frac{A}{B}\right) = \left(\frac{B}{A}\right) (-1)^{((q-1)/2) \deg A \deg B} = \left(\frac{B}{A}\right) (-1)^{((\|A\|-1)/2) \cdot ((\|B\|-1)/2)}. \tag{2.6}$$

This relation continues to hold if A and B are not coprime as both sides vanish.

Given a square-free $Q \in \mathbb{F}_q[x]$, we define the quadratic character χ_Q by

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

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

If $\deg Q$ is even, this is a primitive Dirichlet character modulo Q. Note that by virtue of (2.5), χ_Q is an even character (that is trivial on scalars) if and only if $\deg Q$ is even.

It is important for us that the numerator $P_C(u)$ of the zeta function (1.1) of the hyperelliptic curve $y^2 = Q(x)$ coincides with the completed Dirichlet L-function $\mathcal{L}^*(u, \chi_Q)$ associated with the quadratic character χ_Q.

2.3 The explicit formula

Lemma 2.2. *Let $h(\theta) = \sum_{|k|\leqslant K} \widehat{h}(k)e(k\theta)$ be a trigonometric polynomial, which we assume is real valued and even: $h(-\theta) = h(\theta) = \overline{h(\theta)}$. Then for a primitive character χ we have*

$$\sum_{j=1}^{D} h(\theta_{j,\chi}) = D\int_0^1 h(\theta)\,d\theta + \lambda_\infty(\chi)\frac{1}{\pi i}\int_0^1 h(\theta)\frac{d}{d\theta}\log\left(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}\right)d\theta$$
$$-\sum_f \widehat{h}(\deg f)\frac{\Lambda(f)}{\|f\|^{1/2}}(\chi(f)+\overline{\chi(f)}). \tag{2.7}$$

Proof. By computing the logarithmic derivative $u(\mathcal{L}'/\mathcal{L})$ in two different ways, either using the Euler product (2.1) or the zeros (2.3) we get an identity, for $n > 0$,

$$-\sum_{j=1}^{D}\alpha_{j,\chi}^n = \sum_{\deg f = n}\Lambda(f)\chi(f) + \lambda_\infty(\chi)$$

where $\Lambda(f) = \deg P$ if $f = P^k$ is a prime power, and $\Lambda(f) = 0$ otherwise. Therefore we get an explicit formula in terms of the phases $\theta_{j,\chi}$,

$$-\sum_{j=1}^{D} e^{2\pi i n\theta_{j,\chi}} = \frac{\lambda_\infty(\chi)}{q^{|n|/2}} + \sum_{\deg f=|n|}\frac{\Lambda(f)}{\|f\|^{1/2}}\begin{cases}\overline{\chi(f)} & n<0,\\ \chi(f) & n>0,\end{cases}$$

which is valid for n both positive and negative.

Now let $h(\theta) = \sum_{|k|\leqslant K}\widehat{h}(k)e(k\theta)$ be a trigonometric polynomial, which we assume is real valued and even: $h(-\theta) = h(\theta) = \overline{h(\theta)}$. Then the Fourier coefficients are also real and even: $\widehat{h}(-k) = \widehat{h}(k) = \overline{\widehat{h}(k)}$. Using the Fourier expansion of h we get

$$\sum_{j=1}^{D} h(\theta_j) = D\widehat{h}(0) + \sum_j\sum_{k=1}^{K}\widehat{h}(k)(e(k\theta_j)+e(-k\theta_j))$$
$$= D\int_0^1 h(\theta)\,d\theta - \sum_{k=1}^{K}\widehat{h}(k)\left(2\frac{\lambda_\infty(\chi)}{q^{k/2}} + \sum_{\deg f=k}\frac{\Lambda(f)}{\|f\|^{1/2}}(\chi(f)+\overline{\chi(f)})\right)$$
$$= D\int_0^1 h(\theta)\,d\theta - 2\lambda_\infty(\chi)\sum_{k=1}^{K}\frac{\widehat{h}(k)}{q^{k/2}} - \sum_f \widehat{h}(\deg f)\frac{\Lambda(f)}{\|f\|^{1/2}}(\chi(f)+\overline{\chi(f)}).$$

Note that since h is real valued,

$$\sum_{k=1}^{K}\frac{\widehat{h}(k)}{q^{k/2}} = \int_0^1 h(\theta)\frac{q^{-1/2}e^{2\pi i\theta}}{1-q^{-1/2}e^{2\pi i\theta}} = \frac{1}{2\pi i}\int_0^1 h(\theta)\frac{d}{d\theta}\log\frac{1}{1-(e^{2\pi i\theta}/\sqrt{q})}\,d\theta$$

which gives the claim. □

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

For the quadratic character χ_Q, with Q square-free of degree $2g+2$, we get $\lambda_\infty = 1$, $D = 2g$, and the explicit formula reads

$$\sum_{j=1}^{2g} h(\theta_{j,Q}) = 2g\int_0^1 h(\theta)\,d\theta + \frac{1}{\pi i}\int_0^1 h(\theta)\frac{d}{d\theta}\log\left(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}\right)d\theta$$
$$- 2\sum_f \widehat{h}(\deg f)\frac{\Lambda(f)}{\|f\|^{1/2}}\chi_Q(f). \tag{2.8}$$

3. Averaging over $\mathcal{H}_{2g+2,q}$

Let $\mathcal{H}_{d,q} \subset \mathbb{F}_q[x]$ be the set of all square-free monic polynomials of degree d. The cardinality of $\mathcal{H}_{d,q}$ is

$$\#\mathcal{H}_{d,q} = \begin{cases} \left(1-\dfrac{1}{q}\right)q^d & d \geqslant 2, \\ q & d = 1, \end{cases}$$

as may be seen by expressing the generating function $\sum_{d=0}^{\infty}\mathcal{H}_{d,q}u^d$ in terms of the zeta function $Z(u)$ of the rational function field:

$$Z(u) = Z(u^2)\sum_{d=0}^{\infty}\mathcal{H}_{d,q}u^d.$$

In particular we have

$$\#\mathcal{H}_{2g+2,q} = \left(1-\frac{1}{q}\right)q^{2g+2}. \tag{3.1}$$

We denote by $\langle\bullet\rangle$ the mean value of any quantity defined on $\mathcal{H}_{2g+2,q}$, that is

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

LEMMA 3.1. *If $f \in \mathbb{F}_q[x]$ is not a square then*

$$\langle\chi_Q(f)\rangle \leqslant \frac{2^{\deg f-1}}{(1-1/q)q^{g+1}}.$$

Proof. We use the Mobius function to pick out the square free monic polynomials via the formula

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

where we sum over all monic polynomials whose square divides Q. Thus the sum over all square-free polynomials is given by

$$\sum_{Q\in\mathcal{H}_{2g+2,q}}\chi_Q(f) = \sum_{\deg Q=2g+2}\sum_{A^2|Q}\mu(A)\left(\frac{Q}{f}\right)$$
$$= \sum_{\deg A\leqslant g+1}\mu(A)\left(\frac{A}{f}\right)^2\sum_{\deg B=2g+2-2\deg A}\left(\frac{B}{f}\right).$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

To deal with the inner sum, note that $(\bullet/f)$ is a nontrivial character since f is not a square, so we can use Lemma 2.1 to get

$$\left|\sum_{\deg B=2g+2-2\deg A}\left(\frac{B}{f}\right)\right| \leqslant \binom{\deg f-1}{2g+2-2\deg A} q^{g+1-\deg A} \tag{3.2}$$

if $2g+2-2\deg A<\deg f$, and the sum is zero otherwise. Hence we have

$$\begin{aligned}\left|\sum_{Q\in\mathcal{H}_{2g+2,q}}\chi_Q(f)\right| &\leqslant \sum_{\deg A\leqslant g+1}\left|\sum_{\deg B=2g+2-2\deg A}\left(\frac{B}{f}\right)\right| \\ &\leqslant \sum_{g+1-(\deg f/2)<\deg A\leqslant g+1}\binom{\deg f-1}{2g+2-2\deg A}q^{g+1-\deg A} \\ &= q^{g+1}\sum_{g+1-(\deg f/2)<j\leqslant g+1}\binom{\deg f-1}{2g+2-2j}\leqslant 2^{\deg f-1}q^{g+1}.\end{aligned}$$

Dividing by $\#\mathcal{H}_{2g+2,q}=q^{2g+2}(1-(1/q))$ proves the lemma. □

Lemma 3.2. *Let $P_1,\dots,P_k$ be prime polynomials. Then*

$$\left\langle \chi_Q\left(\prod_{j=1}^k P_j^2\right)\right\rangle = 1+O\left(\sum_{j=1}^k\frac{1}{\|P_j\|}\right).$$

Proof. We have $\chi_Q(\prod_{j=1}^k P_j^2)=1$ if $\gcd(\prod_{j=1}^k P_j,Q)=1$, and $\chi_Q(\prod_{j=1}^k P_j^2)=0$ otherwise. Since for primes $P_1,\dots,P_k$ the condition $\gcd(\prod_{j=1}^k P_j,Q)\neq 1$ is equivalent to P_j dividing Q for some j, we may write

$$\chi_Q\left(\prod_{j=1}^k P_j^2\right)=1-\begin{cases}1 & \text{there exists } P_j|Q,\\ 0 & \text{otherwise,}\end{cases}$$

and hence

$$\left\langle \chi_Q\left(\prod_{j=1}^k P_j^2\right)\right\rangle = 1-\frac{1}{\#\mathcal{H}_{2g+2,q}}\#\{Q\in\mathcal{H}_{2g+2,q}:\exists P_j|Q\}.$$

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

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

so that recalling $\mathcal{H}_{2g+2,q}=(1-(1/q))q^{2g+2}$, we have

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

Thus

$$\left\langle \chi_Q\left(\prod_{j=1}^k P_j^2\right)\right\rangle = 1+O\left(\sum_{j=1}^k\frac{1}{\|P_j\|}\right)$$

as claimed. □

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

For a polynomial $Q \in \mathbb{F}_q[x]$ of positive degree, set

$$\eta(Q) = \sum_{P|Q} \frac{1}{\|P\|}$$

the sum being over all monic irreducible (prime) polynomials dividing Q.

LEMMA 3.3. *The mean values of η and η^2 are uniformly bounded as $g \to \infty$:*

$$\langle \eta \rangle \leqslant 1, \quad \langle \eta^2 \rangle \leqslant \frac{1}{(1-(1/q))^3}.$$

Proof. We consider the first moment: we have

$$\begin{aligned}\langle \eta(Q) \rangle &= \frac{1}{\#\mathcal{H}_{2g+2,q}} \sum_{Q \in \mathcal{H}_{2g+2,q}} \sum_{P|Q} \frac{1}{\|P\|} \\ &= \frac{1}{\#\mathcal{H}_{2g+2,q}} \sum_{\deg P \leqslant 2g+2} \frac{1}{\|P\|} \#\{Q \in \mathcal{H}_{2g+2,q} : P|Q\}.\end{aligned}$$

We bound the number of square-free Q divisible by P by the number of all Q of degree $2g+2$ divisible by P, which is $q^{2g+2}/\|P\|$, to find

$$\begin{aligned}\langle \eta(Q) \rangle &\leqslant \frac{1}{(1-(1/q))q^{2g+2}} \sum_{\deg P \leqslant 2g+2} \frac{1}{\|P\|} \#\{\deg Q = 2g+2 : P|Q\} \\ &\leqslant \frac{1}{(1-(1/q))q^{2g+2}} \sum_{\deg P \leqslant 2g+2} \frac{q^{2g+2}}{\|P\|^2} \leqslant \frac{1}{1-q^{-1}} \sum_f \frac{1}{\|f\|^2} = 1\end{aligned}$$

(the last sum is over all monic polynomials) proving that $\langle \eta(Q) \rangle$ is uniformly bounded.

For the second moment of η, we have

$$\begin{aligned}\langle \eta^2 \rangle &= \frac{1}{\#\mathcal{H}_{2g+2,q}} \sum_{Q \in \mathcal{H}_{2g+2,q}} \left(\sum_{P|Q} \frac{1}{\|P\|} \right)^2 \\ &= \frac{1}{\#\mathcal{H}_{2g+2,q}} \sum_{\deg P_1, \deg P_2 \leqslant 2g+2} \frac{1}{\|P_1\| \cdot \|P_2\|} \#\{Q \in \mathcal{H}_{2g+2,q} : P_1|Q, P_2|Q\}.\end{aligned}$$

For square-free Q, if two primes $P_1|Q$ and $P_2|Q$ then necessarily $P_1 \neq P_2$ and then Q is divisible by both if and only it is divisible by their product, hence

$$\begin{aligned}\#\{Q \in \mathcal{H}_{2g+2,q} : P_1|Q, P_2|Q\} &= \#\{Q \in \mathcal{H}_{2g+2,q} : P_1P_2|Q\} \\ &\leqslant \#\{Q : \deg Q = 2g+2, P_1P_2 \mid Q\} \\ &= \begin{cases} \dfrac{q^{2g+2}}{\|P_1P_2\|} & \deg(P_1P_2) \leqslant 2g+2, \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

and hence the contribution of such pairs is bounded by

$$\frac{1}{(1-(1/q))q^{2g+2}} \sum_{P_1} \sum_{P_2} \frac{q^{2g+2}}{\|P_1\|^2\|P_2\|^2} \leqslant \frac{1}{(1-(1/q))} \left(\sum_f \frac{1}{\|f\|^2} \right)^2 = \frac{1}{(1-(1/q))^3}.$$

Thus we see $\langle \eta^2 \rangle \leqslant (1-(1/q))^{-3}$ which is again uniformly bounded. □

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

4. Beurling–Selberg functions

Let $\mathcal{I} = [-\beta/2, \beta/2]$ be an interval, symmetric about the origin, of length $0 < \beta < 1$, and $K \geqslant 1$ an integer. Beurling–Selberg polynomials $I_K^{\pm}$ are trigonometric polynomials approximating the indicator function $\mathbf{1}_{\mathcal{I}}$ satisfying (see the beautiful exposition in [Mon94, ch. 1.2]):

- $I_K^{\pm}$ are trigonometric polynomials of degree $\leqslant K$;
- monotonicity,
$$I_K^- \leqslant \mathbf{1}_{\mathcal{I}} \leqslant I_K^+; \tag{4.1}$$
- the integral of $I_K^{\pm}$ is close to the length of the interval,
$$\int_0^1 I_K^{\pm}(x)\, dx = \int_0^1 \mathbf{1}_{\mathcal{I}}(x)\, dx \pm \frac{1}{K+1}; \tag{4.2}$$
- $I_K^{\pm}(x)$ are even.[4]

As a consequence of (4.2), the non-zero Fourier coefficients of $I_K^{\pm}$ satisfy

$$|\widehat{I}_K^{\pm}(k) - \widehat{\mathbf{1}}_{\mathcal{I}}(k)| \leqslant \frac{1}{K+1} \tag{4.3}$$

and in particular

$$|\widehat{I}_K^{\pm}(k)| \leqslant \frac{1}{K+1} + \min\left(\beta, \frac{\pi}{|k|}\right), \quad 0 < |k| \leqslant K. \tag{4.4}$$

Proposition 4.1. *Let $\mathcal{I} = [-\beta/2, \beta/2]$ be an interval and $K \geqslant 1$ an integer so that $K\beta > 1$. Then*

$$\sum_{n \geqslant 1} \widehat{I}_K^{\pm}(2n) = O(1) \tag{4.5}$$

$$\sum_{n \geqslant 1} n \widehat{I}_K^{\pm}(n)^2 = \frac{1}{2\pi^2} \log K\beta + O(1) \tag{4.6}$$

where the implied constants are independent of K and β.

Proof. To bound the sum (4.5), we may use (4.3) to write

$$\widehat{I}_K^{\pm}(2n) = \frac{\sin 2\pi n\beta}{2\pi n} + O\left(\frac{1}{K}\right)$$

and hence

$$\sum_{n \geqslant 1} \widehat{I}_K^{\pm}(2n) = \sum_{1 \leqslant n \leqslant K/2} \frac{\sin 2\pi n\beta}{2\pi n} + O(1).$$

We treat separately the range $n < 1/\beta$ and $1/\beta < n < K$. To bound the sum over $n < 1/\beta$, use $\sin 2\pi n\beta \ll n\beta$ and hence

$$\sum_{1 \leqslant n < 1/\beta} \frac{\sin 2\pi n\beta}{2\pi n} \ll \sum_{1 \leqslant n < 1/\beta} \frac{n\beta}{n} = O(1).$$

[4] This is because we take the interval $\mathcal{I} = [-\beta/2, \beta/2]$ which is symmetric about the origin.

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

For the sum on $n > 1/\beta$, we apply summation by parts. The partial sums of $\sin 2\pi n\beta$ are

$$\sum_{n=1}^{N} \sin 2\pi n\beta = \frac{\cos \pi\beta - \cos(2N+1)\pi\beta}{2 \sin \pi\beta} = O\left(\frac{1}{\beta}\right). \tag{4.7}$$

Therefore

$$\sum_{1/\beta<n<K/2} \frac{\sin 2\pi n\beta}{2\pi n} \ll \frac{1}{\beta K} + 1 + \frac{1}{\beta}\int_{1/\beta}^{K} \frac{1}{t^2}\, dt = O(1)$$

and hence $\sum_{n\geqslant 1} \widehat{I}_K^{\pm}(2n) = O(1)$.

To prove (4.6), we use (4.3) to write

$$\sum_{n>0} n\widehat{I}_K^{\pm}(n)^2 = \frac{1}{\pi^2} \sum_{n\leqslant K} \frac{(\sin \pi n\beta)^2}{n} + O(1).$$

We split the sum into two parts: the sum over $1 \leqslant n \leqslant 1/\beta$, where we use $|\sin \pi n\beta| \ll n\beta$ to see that it gives a bounded contribution, and the sum over $1/\beta < n \leqslant K$, where we use $\sin(y)^2 = (1/2)(1 - \cos(2y))$ to get

$$\begin{aligned}\sum_{n>0} n\widehat{I}_K^{\pm}(n)^2 &= \frac{1}{2\pi^2} \sum_{1/\beta<n\leqslant K} \frac{1}{n} - \frac{1}{2\pi^2} \sum_{1/\beta<n\leqslant K} \frac{\cos 2\pi n\beta}{n} + O(1) \\ &= \frac{1}{2\pi^2} \log K\beta - \frac{1}{2\pi^2} \sum_{1/\beta<n\leqslant K} \frac{\cos 2\pi n\beta}{n} + O(1).\end{aligned}$$

To bound $\sum_{1/\beta<n\leqslant K}(\cos 2\pi n\beta/n)$, apply summation by parts using

$$\sum_{1\leqslant n\leqslant N} \cos 2\pi n\beta = \frac{\sin(2N+1)\pi\beta - \sin \pi\beta}{2 \sin \pi\beta} \ll \frac{1}{\beta}, \quad 0 < \beta < 1$$

to find that it gives a bounded contribution. Hence

$$\sum_{n>0} n\widehat{I}_K^{\pm}(n)^2 = \frac{1}{2\pi^2} \log K\beta + O(1)$$

as claimed. □

5. Counting functions

Let χ be a primitive Dirichlet character. We denote by $N_{\mathcal{I}}(\chi)$ the number of angles $\theta_{j,\chi}$ of the L-function $\mathcal{L}^*(u,\chi)$ (see (2.4)) in the interval $\mathcal{I} = [-\beta/2, \beta/2]$. Define $S_{\mathcal{I}}(\chi)$ by

$$N_{\mathcal{I}}(\chi) = 2g|\mathcal{I}| + \frac{2}{\pi} \arg\left(1 - \frac{e^{i\pi|\mathcal{I}|}}{\sqrt{q}}\right) + S_{\mathcal{I}}(\chi).$$

Set

$$N_K^{\pm}(\chi) = \sum_{j=1}^{D} I_K^{\pm}(\theta_{j,\chi}).$$

Here K will depend on $\deg Q$. This will be our approximation to the counting function $N_{\mathcal{I}}(\chi)$. Then by virtue of (4.1),

$$N_K^{-}(\chi) \leqslant N_{\mathcal{I}}(\chi) \leqslant N_K^{+}(\chi). \tag{5.1}$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

Using the explicit formula (2.7), we find

$$N_K^{\pm}(\chi) =: D\left(\beta \pm \frac{1}{K+1}\right) + \lambda_\infty(\chi)\frac{1}{\pi i}\int_0^1 I_K^{\pm}(\theta)\frac{d}{d\theta}\log\left(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}\right)d\theta + S_K^{\pm}(\chi) \tag{5.2}$$

where $S_K^{\pm}(\chi)$ is

$$S_K^{\pm}(\chi) := -\sum_{\deg f\leqslant K}\widehat{I}_K^{\pm}(\deg f)\frac{\Lambda(f)}{\|f\|^{1/2}}\{\chi(f)+\overline{\chi(f)}\} \tag{5.3}$$

the sum taken over all prime powers $f\in\mathbb{F}_q[x]$ (of degree $\leqslant K$).

Note that since $\|\mathbf{1}_{\mathcal{I}} - I_K^{\pm}\|_{L^1} = 1/(K+1)$, we have

$$\begin{aligned}\frac{1}{\pi i}\int_0^1 I_K^{\pm}(\theta)\frac{d}{d\theta}\log\left(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}\right)d\theta &= \frac{1}{\pi i}\int_{-\beta/2}^{\beta/2}\frac{d}{d\theta}\log\left(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}\right)d\theta + O\left(\frac{1}{K}\right)\\ &= \frac{2}{\pi}\arg\left(1-\frac{e^{i\pi\beta}}{\sqrt{q}}\right)+O\left(\frac{1}{K}\right).\end{aligned} \tag{5.4}$$

5.1 Quadratic characters

For the case at hand, of quadratic characters, we write $N_{\mathcal{I}}(Q)$ for $N_{\mathcal{I}}(\chi_Q)$, with similar meaning for $S_{\mathcal{I}}(Q)$, $N_K^{\pm}(Q)$ and $S_K^{\pm}(Q)$. We have

$$S_K^{\pm}(Q) := S_K^{\pm}(\chi_Q) = -2\sum_{\deg f\leqslant K}\widehat{I}_K^{\pm}(\deg f)\frac{\Lambda(f)}{\|f\|^{1/2}}\chi_Q(f). \tag{5.5}$$

We may now deduce that the zeros are uniformly distributed.

Proposition 5.1. *Every fixed (symmetric) interval $\mathcal{I}=[-\beta/2,\beta/2]$ contains asymptotically $2g|\mathcal{I}|$ angles $\theta_{j,Q}$, in fact*

$$N_{\mathcal{I}}(Q) = 2g|\mathcal{I}| + O\left(\frac{g}{\log g}\right).$$

Proof. Indeed from (5.1) it suffices to show that for the smooth counting functions $N_K^{\pm}(\chi_Q)$ we have

$$N_K^{\pm}(\chi_Q) = 2g|\mathcal{I}| + O\left(\frac{g}{\log g}\right).$$

Now from (5.2), (5.4) it follows that

$$N_K^{\pm}(\chi_Q) = 2g|\mathcal{I}| + O\left(\frac{g}{K}\right) + O(1) + |S_K^{\pm}(Q)|.$$

To bound $S_K^{\pm}(Q)$, use (5.5) and (4.4) in the form $\widehat{I}_K^{\pm}(\deg f)\Lambda(f) = O(1)$ to deduce that

$$S_K^{\pm}(Q) \ll \sum_{\deg f\leqslant K}\frac{1}{\sqrt{\|f\|}} \ll q^{K/2}$$

and hence

$$|N_K^{\pm}(\chi_Q) - 2g|\mathcal{I}|| \ll \frac{g}{K} + q^{K/2}.$$

Taking $K\approx \log_q g - \log_q\log g$ gives the result. □

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

6. Expected value

We first bound the expected value of $S_{\mathcal{I}}$.

PROPOSITION 6.1. *Assume that either the interval $\mathcal{I} = [-\beta/2, \beta/2]$ is fixed or that it shrinks to zero with $g \to \infty$ in such a way that $g\beta \to \infty$. Then*

$$\langle S_{\mathcal{I}} \rangle = O(1).$$

Proof. Using (5.1), (5.2) and (5.4), we find that for any K,

$$\langle S_K^- \rangle \leqslant \langle S \rangle + O\left(\frac{g}{K}\right) \leqslant \langle S_K^+ \rangle.$$

Taking $K \approx g/100$ gives the remainder term above is bounded. So it remains to bound the expected value of $S_K^{\pm}$ for such K.

Recall that $S_K^{\pm}$ is a sum over prime powers. We separate out the contribution of even powers, which is not oscillatory, from that of the odd powers:

$$S_K^{\pm} = \text{even} + \text{odd}.$$

We claim that the even powers give

$$\text{even} = -2 \sum_{n \geqslant 1} \widehat{I}_K^{\pm}(2n) + O(\eta(Q)) \tag{6.1}$$

where

$$\eta(Q) = \sum_{P|Q} \frac{1}{\|P\|},$$

the sum over prime divisors of Q.

To see (6.1), note that for an even power of a prime, say $f = g^2$, we have $\chi_Q(f) = 1$ if $\gcd(g, Q) = 1$ and 0 otherwise. Writing the even powers of a prime as $f = g^2$, and noting that $\Lambda(f) = \Lambda(g)$, we have

$$\begin{aligned} \text{even} &= -2 \sum_{\gcd(g,Q)=1} \frac{\widehat{I}_K^{\pm}(2 \deg g)\Lambda(g)}{\|g\|} \\ &= -2 \sum_{n \geqslant 1} \frac{\widehat{I}_K^{\pm}(2n)}{q^n} \sum_{\deg g = n} \Lambda(g) + O\left(\sum_{P|Q} \frac{1}{\|P\|}\right) \end{aligned}$$

where the remainder term is a sum over all prime divisors of Q. By the prime number theorem, $\sum_{\deg g = n} \Lambda(g) = q^n$ and hence

$$-2 \sum_{\gcd(g,Q)=1} \frac{\widehat{I}_K^{\pm}(2 \deg g)\Lambda(g)}{\|g\|} = -2 \sum_{n \geqslant 1} \widehat{I}_K^{\pm}(2n), \tag{6.2}$$

proving (6.1).

It now follows that expected value of the even powers is bounded: indeed, the sum $\sum_{n \geqslant 1} \widehat{I}_K^{\pm}(2n)$ is bounded by Proposition 4.1 (note that our choice $K \approx g/100$ and the condition $g\beta \to \infty$ guarantees $K\beta \to \infty$, hence Proposition 4.1 is applicable). As for the term $\eta(Q) = \sum_{P|Q} 1/\|P\|$, it is not bounded individually, but its mean is bounded by Lemma 3.3.

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

The expected value of the odd powers is

$$\langle \text{odd} \rangle = -2 \sum_{\deg f \text{ odd}} \frac{\widehat{I}_K^{\pm}(\deg f)\Lambda(f)}{\sqrt{\|f\|}} \langle \chi_Q(f) \rangle.$$

To estimate the expected value of the odd powers, we use Lemma 3.1 and (4.4) in the form $\widehat{I}_K^{\pm}(\deg f)\Lambda(f) = O(1)$ to find

$$\langle \text{odd} \rangle \ll \sum_{\deg f \leqslant K} \frac{1}{\sqrt{\|f\|}} \frac{2^{\deg f}}{q^{g+1}} \ll \frac{(2\sqrt{q})^K}{q^{g+1}},$$

which for $K \approx g/100$ is bounded. □

Hence we see that

$$\left\langle \frac{S_{\mathcal{I}}}{\sqrt{(2/\pi^2)\log(g\beta)}} \right\rangle \to 0, \quad g \to \infty. \tag{6.3}$$

7. A sum over primes

Consider the sum over primes

$$T_K^{\pm}(Q) := -2 \sum_P \frac{\widehat{I}_K^{\pm}(\deg P) \deg P}{\sqrt{\|P\|}} \chi_Q(P).$$

This will be our approximation to $S_{\mathcal{I}}$. From now on assume that

$$K \approx \frac{g}{\log\log(g\beta)}$$

which will guarantee $\log K\beta \sim \log g\beta$ and $K = o(g)$.

Theorem 7.1. *Assume that $g \to \infty$ and either $0 < \beta < 1$ is fixed or $\beta \to 0$ while $\beta g \to \infty$. Take $K \approx g/\log\log(g\beta)$. Then:*

(i) $$\langle |T_K^{\pm}|^2 \rangle \sim \frac{2}{\pi^2} \log \beta g;$$

(ii) $$\langle |T_K^{+} - T_K^{-}|^2 \rangle = O(1); \tag{7.1}$$

(iii) $$\langle |S_K^{\pm} - T_K^{\pm}|^2 \rangle = O(1). \tag{7.2}$$

The rest of this section is devoted to the proof of Theorem 7.1.

7.1 Computing $\langle (T_K^{\pm})^2 \rangle$

We have

$$\langle (T_K^{\pm})^2 \rangle = 4 \sum_{P_1, P_2} \widehat{I}_K^{\pm}(\deg P_1)\widehat{I}_K^{\pm}(\deg P_2) \frac{\deg P_1 \deg P_2}{\sqrt{\|P_1\|\|P_2\|}} \langle \chi_Q(P_1P_2) \rangle.$$

The sum is over $\deg P_1, \deg P_2 \leqslant K < g$. Consider the contribution of pairs such that P_1P_2 is not a perfect square (the 'off-diagonal pairs'). We may use Lemma 3.1 to bound their contribution by

$$\ll \frac{1}{q^{g+1}} \left(\sum_{\deg P \leqslant K} \frac{|\widehat{I}_K^{\pm}(\deg P)| \deg P \, 2^{\deg P}}{\sqrt{|P|}} \right)^2.$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

Using (4.4) in the form $|\widehat{I}_K^{\pm}(k)| \ll 1/|k|$ gives that the inner sum is bounded by

$$\ll \sum_{\deg P \leqslant K} \frac{2^{\deg P}}{\sqrt{|P|}} \frac{\deg P}{\deg P} \ll (2\sqrt{q})^K.$$

Hence the off-diagonal contribution is bounded by

$$\ll \frac{(4q)^K}{q^{g+1}},$$

which is negligible since we take $K = o(g)$.

Consider the contribution of pairs such that $P_1 \cdot P_2$ is a square. Since P_1 and P_2 are primes, this forces $P_1 = P_2$. These contribute

$$\begin{aligned} &4 \sum_P \frac{(\deg P)^2}{\|P\|} \widehat{I}_K^{\pm}(\deg P)^2 \langle \chi_Q(P)^2 \rangle \\ &= 4 \sum_P \frac{(\deg P)^2}{\|P\|} \widehat{I}_K^{\pm}(\deg P)^2 + O\Big(\sum_P \frac{(\deg P)^2}{\|P\|^2} \widehat{I}_K^{\pm}(\deg P)^2 \Big) \end{aligned} \tag{7.3}$$

by Lemma 3.2.

Using the prime number theorem $\#\{P : \deg P = n\} = q^n/n + O(q^{n/2})$ gives

$$\begin{aligned} 4 \sum_P \frac{(\deg P)^2}{\|P\|} \widehat{I}_K^{\pm}(\deg P)^2 &= 4 \sum_{1 \leqslant n \leqslant K} \Big(n + O\Big(\frac{n^2}{q^{n/2}} \Big) \Big) \widehat{I}_K^{\pm}(n)^2 + O(1) \\ &= 4 \sum_{1 \leqslant n \leqslant K} n \widehat{I}_K^{\pm}(n)^2 + O(1). \end{aligned}$$

By Proposition 4.1 we find

$$4 \sum_P \frac{(\deg P)^2}{\|P\|} \widehat{I}_K^{\pm}(\deg P)^2 = \frac{2}{\pi^2} \log K\beta + O(1) \tag{7.4}$$

(note that if $g\beta \to \infty$ then $K\beta \approx g\beta/\log\log(g\beta) \to \infty$). To bound the remainder term in (7.3) use (4.4) in the form $\widehat{I}_K^{\pm}(\deg P) \deg P = O(1)$ to find that the sum is at most $\sum_P 1/\|P\|^2 = O(1)$. Therefore we find

$$\langle (T_K^{\pm})^2 \rangle = \frac{2}{\pi^2} \log(K\beta) + O(1).$$

7.2 Bounding $\langle |T_K^+ - T_K^-|^2 \rangle$

Next we compute the variance of the difference $\langle |T_K^+ - T_K^-|^2 \rangle$. Arguing as above, one sees that the only terms which may significantly contribute to the average are again the diagonal terms

$$\langle |T_K^+ - T_K^-|^2 \rangle = 4 \sum_{\deg P \leqslant K} \frac{(\deg P)^2}{\|P\|} (\widehat{I}_K^+(\deg P) - \widehat{I}_K^-(\deg P))^2 \langle \chi_Q(P)^2 \rangle + o(1).$$

Since by (4.3)

$$|\widehat{I}_K^+(n) - \widehat{I}_K^-(n)| \leqslant \frac{2}{K+1}$$

we get

$$\langle |T_K^+ - T_K^-|^2 \rangle \ll \frac{1}{K^2} \sum_{\deg P \leqslant K} \frac{(\deg P)^2}{\|P\|}.$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

Using the prime number theorem, this is easily seen to be $O(1)$. Hence we find

$$\langle |T_K^+ - T_K^-|^2 \rangle = O(1).$$

7.3 Bounding $\langle |S_K^\pm - T_K^\pm|^2 \rangle$

Next we show that $\langle |S_K^\pm - T_K^\pm|^2 \rangle = O(1)$. We have

$$\begin{aligned} S_K^\pm - T_K^\pm &= -2 \sum_{f=P^j, j\geqslant 2} \widehat{I}_K^\pm(\deg f) \frac{\Lambda(f)}{\|f\|^{1/2}} \chi_Q(f) \\ &= \text{even} + \text{odd} \end{aligned} \tag{7.5}$$

where the term 'even' is a sum over the even powers of primes, and 'odd' is the sum over odd powers of primes where the exponent is at least 3. We will show that the second moments of both the odd and even terms are bounded.

We first argue that the second moment of the even powers contribute a bounded amount. As we saw in the proof of Proposition 6.1, see (6.1), we have

$$\text{even} \ll 1 + \sum_{P|Q} \frac{1}{\|P\|}$$

the sum being over all prime divisors of Q. This is not bounded individually, but its second moment is bounded by Lemma 3.3.

It remains to bound the contribution of the odd powers. We have

$$\langle |\text{odd}|^2 \rangle = 4 \sum_{f_1, f_2} \widehat{I}_K^\pm(\deg f_1) \widehat{I}_K^\pm(\deg f_2) \frac{\Lambda(f_1)\Lambda(f_2)}{\|f_1 f_2\|^{1/2}} \langle \chi_Q(f_1 f_2) \rangle$$

where the sum is over odd higher prime powers, that is over $f = P^j$ with $j \geqslant 3$ and odd.

The pairs where $f_1 \cdot f_2$ is not a square contribute $o(1)$ by the same argument as above. Consider the contribution of pairs such that $f_1 \cdot f_2$ is a square. If f_1 and f_2 are *odd* higher prime powers but $f_1 \cdot f_2$ is a square, then necessarily $f_1 = P^r$, $f_2 = P^s$ with P prime, $r, s \geqslant 2$, (and $r = s \mod 2$). Necessarily then $r + s \geqslant 4$. The contribution of such pairs can be bounded, using (4.4) in the form $\widehat{I}_K^\pm(\deg f)\Lambda(f) = O(1)$, by

$$\sum_P \sum_{r+s\geqslant 4} \frac{1}{\|P\|^{(r+s)/2}} \ll \sum_P \sum_{j\geqslant 4} \frac{j}{\|P\|^{j/2}} \ll \sum_P \frac{1}{\|P\|^2} = O(1).$$

Hence $\langle |\text{odd}|^2 \rangle = O(1)$ and therefore

$$\langle |S_K^\pm - T_K^\pm|^2 \rangle = O(1).$$

8. Higher moments of $T_K^\pm$

In this section we show that all moments of $T_K^\pm$ are Gaussian.

Theorem 8.1. *Assume the setting of Theorem 7.1 and let $r \geqslant 2$. Then*

$$|\langle (T_K^\pm)^{2r-1} \rangle| = o(1)$$

and

$$\langle (T_K^\pm)^{2r} \rangle = \frac{(2r)!}{r!\pi^{2r}} \log^r(\beta K) + O(\log^{r-1}(\beta K)).$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

Proof. For the odd moments, we have

$$\langle (T_K^{\pm})^{2r-1}\rangle = -2^{2r-1}\sum_{P_1,\dots,P_{2r-1}} \frac{\prod \widehat{I}_K^{\pm}(\deg P_j)\deg P_j}{\sqrt{\|\prod P_j\|}}\left\langle \chi_Q\Big(\prod P_j\Big)\right\rangle.$$

Since $\prod_j P_j$ cannot be a perfect square, we may apply Lemma 3.1 and obtain the bound

$$|\langle (T_K^{\pm})^{2r-1}\rangle| \ll \frac{1}{q^{g+1}}\Bigg(\sum_{\deg P\leqslant K}\frac{|\widehat{I}_K^{\pm}(\deg P)|\deg P\, 2^{\deg P}}{\sqrt{|P|}}\Bigg)^{2r-1}.$$

As was already calculated in § 7.1, the inner sum is bounded by

$$\ll \sum_{\deg P\leqslant K}\frac{2^{\deg P}}{\sqrt{|P|}}\frac{\deg P}{\deg P} \ll (2\sqrt{q})^K.$$

Hence

$$|\langle (T_K^{\pm})^{2r-1}\rangle| \ll \frac{(2\sqrt{q})^{(2r-1)K}}{q^{g+1}}$$

which vanishes assuming $K \approx g/\log\log(g\beta)$.

To compute the even moments, write

$$\langle (T_K^{\pm})^{2r}\rangle = 2^{2r}(T_{sq}^{2r}+T_{nsq}^{2r})$$

where both T_{sq}^{2r} and T_{nsq}^{2r} have the form

$$\sum_{P_1,\dots,P_{2r}}\frac{\prod \widehat{I}_K^{\pm}(\deg P_j)\deg P_j}{\sqrt{\|\prod P_j\|}}\left\langle \prod \chi_Q(P_j)\right\rangle$$

where T_{sq}^{2r} is the sum over prime $2r$-tuples $\{P_j\}$ for which $\prod_{j=1}^{2r} P_j$ is a perfect square, and T_{nsq}^{2r} contains the remaining (off-diagonal) terms.

The term T_{nsq}^{2r} can be bounded as was done for the odd moments:

$$T_{nsq}^{2r} \ll \frac{1}{q^{g+1}}\Bigg(\sum_{\deg P\leqslant K}\frac{|\widehat{I}_K^{\pm}(\deg P)|\deg P\, 2^{\deg P}}{\sqrt{|P|}}\Bigg)^{2r} \ll \frac{(2\sqrt{q})^{2rK}}{q^{g+1}}.$$

Now

$$T_{sq}^{2r} = \sum_{P_1\cdots P_{2r}=\square}\frac{\prod \widehat{I}_K^{\pm}(\deg P_j)\deg P_j}{\sqrt{\|\prod P_j\|}}\left\langle \prod \chi_Q(P_j)\right\rangle,$$

the sum taken over only those primes for which $\prod P_j$ is a square, which implies all P_j appear in equal pairs in each summand. Note that in particular all summands are positive. By Lemma 3.2 we may replace $\langle \prod \chi_Q(P_j)\rangle$ with 1 by introducing an error of $O(\sum_j 1/\|P_j\|)$.

The total error produced by this substitution is, keeping in mind that the primes $P_1,\dots,P_{2r}$ must come in identical pairs, bounded by

$$\sum_{j=1}^{r}\sum_{P_1,\dots,P_r}\frac{\prod_{k=1}^{r}\widehat{I}_K^{\pm}(\deg P_k)^2(\deg P_k)^2}{\|P_j\|^2\prod_{k\neq j}\|P_k\|}$$
$$\ll \sum_{P_2,\dots,P_r}\frac{\prod_{k=2}^{r}\widehat{I}_K^{\pm}(\deg P_k)^2(\deg P_k)^2}{\prod_{k=2}^{r}\|P_k\|}\sum_{P_1}\frac{\widehat{I}_K^{\pm}(\deg P_1)^2(\deg P_1)^2}{\|P_1\|^2}.$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

The inner sum is bounded, and hence the total error introduced is

$$\ll \sum_{P_2,\dots,P_r} \frac{\prod_{k=2}^r \widehat{I}_K^{\pm}(\deg P_k)^2 (\deg P_k)^2}{\prod_{k=2}^r \|P_k\|} \ll (\log(\beta K))^{r-1}$$

by (7.4).

So far we showed that

$$T_{sq}^{2r} = \sum_{P_1 \cdot \dots \cdot P_{2r} = \square} \frac{\prod \widehat{I}_K^{\pm}(\deg P_j) \deg P_j}{\sqrt{\|\prod P_j\|}} + O(\log^{r-1}(\beta K)).$$

Now we show that pairs of equal P_j in

$$\sum_{P_1 \cdot \dots \cdot P_{2r} = \square} \frac{\prod \widehat{I}_K^{\pm}(\deg P_j) \deg P_j}{\sqrt{\|\prod P_j\|}}$$

can be taken all distinct, for the remaining terms are bounded by very much less than

$$\sum_{P_1 = P_2 = P_3 = P_4} \frac{\widehat{I}_K^{\pm}(\deg P_1)^4 \deg^4 P_1}{\|P_1\|^2} \sum_{\prod_{j=5}^{2r} P_j = \square} \frac{\prod \widehat{I}_K^{\pm}(\deg P_j) \deg P_j}{\sqrt{\|\prod P_j\|}}$$

$$\ll \sum_{j=0}^{\infty} \frac{q^j}{j} \frac{j^4}{q^{2j}} \log^{r-2}(\beta K) \ll \log^{r-2}(\beta K).$$

Finally, the sum over distinct pairs is

$$\frac{(2r)!}{r! 2^r} \sum_{P_1,\dots,P_r \text{ distinct}} \frac{\prod \widehat{I}_K^{\pm}(\deg P_j)^2 \deg^2 P_j}{\|\prod P_j\|}.$$

Now we remove the restriction that $P_1, \dots, P_r$ are distinct, introducing (again) an error of $O(\log^{r-2}(\beta K))$, and obtain

$$T_{sq}^{2r} = \frac{(2r)!}{r! 2^r} \left(\sum_P \frac{\widehat{I}_K^{\pm}(\deg P)^2 \deg^2 P}{\|P\|} \right)^r + O(\log^{r-1}(\beta K)).$$

Summarizing all said above, and using (7.4) yields

$$T_{sq}^{2r} = \frac{(2r)!}{r! \pi^{2r} 2^{2r}} \log^r(\beta K) + O(\log^{r-1}(\beta K))$$

and

$$\langle (T_K^{\pm})^{2r} \rangle = \frac{(2r)!}{r! \pi^{2r}} \log^r(\beta K) + O(\log^{r-1}(\beta K))$$

as claimed. □

COROLLARY 8.2. *Under the assumption of Theorem 7.1, $T_K^{\pm}/\sqrt{(2/\pi^2)\log g\beta}$ has a standard Gaussian limiting distribution.*

Indeed, the main-term expressions for the moments of $T_K^{\pm}$ imply all moments of $T_K^{\pm}/\sqrt{(2/\pi^2)\log g\beta}$ are asymptotic to standard Gaussian moments, where the odd moments vanish and the even moments are

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x^{2r} e^{-x^2/2}\, dx = 1 \cdot 3 \cdot \dots \cdot (2r-1) = \frac{(2r)!}{2^r r!}.$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

9. Conclusion

In this section we prove the claim (1.3) in our introduction. Recall that we wrote

$$N_{\mathcal{I}}(Q) = 2g|\mathcal{I}| + \frac{2}{\pi}\arg\left(1 - \frac{e^{i\pi|\mathcal{I}|}}{\sqrt{q}}\right) + S_{\mathcal{I}}(Q)$$

and thus (1.3) is equivalent to the following theorem.

THEOREM 9.1. *Assume either that the interval $\mathcal{I} = [-\beta/2, \beta/2]$ is fixed, or that its length β shrinks to zero while $g\beta \to \infty$. Then*

$$\langle |S_{\mathcal{I}}|^2 \rangle \sim \frac{2}{\pi^2}\log g\beta$$

and $S_{\mathcal{I}}/\sqrt{(2/\pi^2)\log \beta g}$ has a standard Gaussian distribution.

To prove this, it suffices to show that the second moment of the difference $S_{\mathcal{I}} - T_K^{\pm}$ is negligible relative to $\log(g\beta)$.

PROPOSITION 9.2. *Assume that $K \approx g/\log\log g\beta$, and that either β is fixed or $\beta \to 0$ while $g\beta \to \infty$. Then*

$$\left\langle \left| \frac{S_{\mathcal{I}} - T_K^{\pm}}{\sqrt{(2/\pi^2)\log g\beta}} \right|^2 \right\rangle \to 0. \tag{9.1}$$

Indeed, due to Proposition 9.2, the second moment of $S_{\mathcal{I}}$ is close to that of $T_K^{\pm}$ and the distribution of $S_{\mathcal{I}}/\sqrt{(2/\pi^2)\log \beta g}$ coincides with that of $T_K^{\pm}/\sqrt{(2/\pi^2)\log(g\beta)}$, that is by Corollary 8.2 we find that $S_{\mathcal{I}}/\sqrt{(2/\pi^2)\log \beta g}$ has a standard Gaussian distribution. Thus we will have proved Theorem 9.1 once we establish Proposition 9.2.

9.1 Proof of Proposition 9.2

Assume that $K \approx g/\log\log(g\beta)$. Then it suffices to show

$$\langle |S_{\mathcal{I}} - T_K^{\pm}|^2 \rangle \ll \left(\frac{g}{K}\right)^2. \tag{9.2}$$

We first show

$$\langle |S_{\mathcal{I}} - S_K^{\pm}|^2 \rangle \ll \left(\frac{g}{K}\right)^2. \tag{9.3}$$

By (5.1), we have

$$S_K^- \leqslant S_{\mathcal{I}} + O\left(\frac{g}{K}\right) \leqslant S_K^+.$$

Hence

$$0 \leqslant S_{\mathcal{I}} - S_K^- + O\left(\frac{g}{K}\right) \leqslant S_K^+ - S_K^-.$$

Since we are dealing now with positive quantities, we may take absolute values and get

$$\left| S_{\mathcal{I}} - S_K^- + O\left(\frac{g}{K}\right) \right| \leqslant |S_K^+ - S_K^-|$$

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

and applying the triangle inequality gives

$$|S_{\mathcal{I}} - S_K^-| \leqslant |S_K^+ - S_K^-| + O\left(\frac{g}{K}\right),$$

hence

$$|S_{\mathcal{I}} - S_K^-|^2 \leqslant 2|S_K^+ - S_K^-|^2 + O\left(\left(\frac{g}{K}\right)^2\right).$$

Taking expected values we get

$$\langle |S_{\mathcal{I}} - S_K^-|^2 \rangle \leqslant 2\langle |S_K^+ - S_K^-|^2 \rangle + O\left(\left(\frac{g}{K}\right)^2\right). \tag{9.4}$$

To bound $\langle |S_K^+ - S_K^-|^2 \rangle$, use the triangle inequality to get

$$|S_K^+ - S_K^-| \leqslant |S_K^+ - T_K^+| + |T_K^+ - T_K^-| + |T_K^- - S_K^-|$$

and hence

$$|S_K^+ - S_K^-|^2 \leqslant 3(|S_K^+ - T_K^+|^2 + |T_K^+ - T_K^-|^2 + |T_K^- - S_K^-|^2).$$

Applying (7.1) and (7.2) we find

$$\langle |S_K^+ - S_K^-|^2 \rangle = O(1). \tag{9.5}$$

Inserting (9.5) into (9.4) gives

$$\langle |S_{\mathcal{I}} - S_K^-|^2 \rangle \ll \left(\frac{g}{K}\right)^2$$

and together with (9.5) we get

$$\langle |S_{\mathcal{I}} - S_K^+|^2 \rangle \ll \left(\frac{g}{K}\right)^2$$

proving (9.3).

To show (9.2), we use the triangle inequality to get

$$|S_{\mathcal{I}} - T_K^\pm| \leqslant |S_{\mathcal{I}} - S_K^\pm| + |S_K^\pm - T_K^\pm|$$

hence

$$\langle |S_{\mathcal{I}} - T_K^\pm|^2 \rangle \leqslant 2\langle |S_{\mathcal{I}} - S_K^\pm|^2 \rangle + 2\langle |S_K^\pm - T_K^\pm|^2 \rangle$$

which is $O((g/K)^2)$ by (9.3) and (7.2). □

Acknowledgement

We thank Chris Hughes, Jon Keating, Emmanuel Kowalski and Igor Shparlinski for discussions and comments on earlier versions of the paper.

References

Art24 E. Artin, *Quadratische Körper in Geibiet der Höheren Kongruzzen I and II*, Math. Z. **19** (1924), 153–296.

BF97 T. H. Baker and P. J. Forrester, *Finite N fluctuation formulas for random matrices*, J. Stat. Phys. **88** (1997), 1371–1385.

CL95 O. Costin and J. Lebowitz, *Gaussian fluctuation in random matrices*, Phys. Rev. Lett. **75** (1995), 69–72.

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press

DE01 P. Diaconis and S. Evans, *Linear functionals of eigenvalues of random matrices*, Trans. Amer. Math. Soc. **353** (2001), 2615–2633.

Fai08 D. Faifman, *Counting zeros of L-functions over the rational function field*, MSc thesis, Tel Aviv University (2008).

HKO01 C. P. Hughes, J. P. Keating and N. O'Connell, *On the characteristic polynomial of a random unitary matrix*, Comm. Math. Phys. **220** (2001), 429–451.

Joh97 K. Johansson, *On random matrices from classical compact groups*, Ann. of Math. (2) **145** (1997), 519–545.

KS99a N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45 (American Mathematical Society, Providence, RI, 1999).

KS99b N. M. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) **36** (1999), 1–26.

KS00 J. P. Keating and N. Snaith, *Random matrix theory and* $\zeta(1/2+it)$, Comm. Math. Phys. **214** (2000), 57–89.

Mon94 H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84 (American Mathematical Society, Providence, RI, 1994).

Pol89 H. D. Politzer, *Random-matrix description of the distribution of mesoscopic conductance*, Phys. Rev. B **40** (1989), 11917–11919.

Ros02 M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210 (Springer, New York, 2002).

Sel44 A. Selberg, *On the remainder in the formula for* $N(T)$*, the number of zeros of* $\zeta(s)$ *in the strip* $0 < t < T$, Avh. Nor. Vidensk. -Akad. Oslo I **1944** (1944), 1–27.

Sel46a A. Selberg, *Contributions to the theory of Dirichlet's L-functions*, Skr. Nor. Vidensk. -Akad. Oslo I **1946** (1946), 1–62.

Sel46b A. Selberg, *Contributions to the theory of the Riemann zeta-function*, Arch. Math. Naturvid. **48** (1946), 89–155.

Sos00 A. Soshnikov, *The central limit theorem for local linear statistics in classical compact groups and related combinatorial identities*, Ann. Probab. **28** (2000), 1353–1370.

Wei48 A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent* (Hermann, Paris, 1948).

Wie02 K. Wieand, *Eigenvalue distributions of random unitary matrices*, Probab. Theory Related Fields **123** (2002), 202–224.

Dmitry Faifman faifmand@post.tau.ac.il
Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University,
Tel Aviv 69978, Israel

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

https://doi.org/10.1112/S0010437X09004308 Published online by Cambridge University Press