Artin-Schreier L-functions and Random Unitary Matrices

Alexei Entin

Raymond and Beverly Sackler School of Math. Sciences
Tel Aviv University
Tel Aviv 69978
E-mail: alfxeyen@post.tau.ac.il

May 11, 2014

Abstract

We give a new derivation of an identity due to Z. Rudnick and P. Sarnak about the \( n \)-level correlations of eigenvalues of random unitary matrices as well as a new proof of a formula due to M. Diaconis and P. Shahshahani expressing averages of trace products over the unitary matrix ensemble. Our method uses the zero statistics of Artin-Schreier L-functions and a deep equidistribution result due to N. Katz.

1 Introduction

In [8] Z. Rudnick and P. Sarnak computed the \( n \)-level correlation for the zeroes of the Riemann zeta function (and in fact for a much larger class of L-functions) for a restricted class of test functions and obtained a complicated combinatorial expression involving the Fourier transform of the test function (see Theorem 1 below). By a complicated and highly unstraightforward combinatorial argument they were able to show that this expression coincides with the \( n \)-correlation for the eigenvalues of random unitary matrices.

In the present paper we will give a new derivation of this fact using a different approach. The main advantage of our new approach is that it can be extended to cases to which the combinatorial approach has so far not been extended. The method has been applied in [5] to equate the \( n \)-level densities of quadratic L-functions and random unitary symplectic matrices for a class of test functions unattained previously. Another derivation of the \( n \)-correlation for random unitary matrices has been recently given in [1].

Assume the Riemann Hypothesis. Denote the nontrivial zeroes of the Riemann zeta-function by \( 1/2 + \gamma_j, j = \pm 1, \pm 2, \ldots \) so that

\[
\gamma_j \in \mathbb{R}, \, \gamma_{-j} = -\gamma_j, \, |\gamma_1| \leq |\gamma_2| \leq \ldots
\]
Denote by \( \tilde{\gamma}_j = \gamma_j \log |\gamma_j| / 2\pi \) the normalised zero ordinates, normalised so that the mean spacing between the \( \tilde{\gamma}_j \) is 1. To define the \( n \)-correlation for the Riemann zeroes we fix a smooth test function \( \phi : \mathbb{R}^n \to \mathbb{C} \) which is symmetric (i.e. unchanged by any permutation of the variables), satisfies \( \phi(x_1 + t, ..., x_n + t) = \phi(x_1, ..., x_n) \) for any \( t \in \mathbb{R} \) and is a Schwartz function on the hyperplane \( \sum x_i = 0 \), i.e. \( \phi \) and all its partial derivatives decay faster than any polynomial on this hyperplane. We define the \( n \)-correlation of the first \( T \) Riemann zeroes with test function \( \phi \) to be
\[
R_n(T, \phi) = \frac{1}{T} \sum_{1 \leq j_1, ..., j_n \leq T} \phi(\tilde{\gamma}_{j_1}, ..., \tilde{\gamma}_{j_n}).
\]
It is more convenient to consider the unrestricted sums
\[
C_n(T, \phi) = \frac{1}{T} \sum_{1 \leq j_1, ..., j_n \leq T} \phi(\tilde{\gamma}_{j_1}, ..., \tilde{\gamma}_{j_n}).
\]

The passage from unrestricted sums to restricted ones is made by a standard technique called combinatorial sieving (essentially inclusion-exclusion), which expresses the restricted sum as a combination of the unrestricted sums for all \( m \leq n \) (with auxiliary test functions obtained from \( \phi \) by identifying some of the variables). We omit the details as this passage is described in [8, §4] among other places. We concentrate on the asymptotics of \( C_n(T, \phi) \).

In [8] Z. Rudnick and P. Sarnak computed the limit of the \( n \)-correlation for the Riemann zeroes (and more general L-functions) as \( T \to \infty \) for a restricted class of test functions. Suppose that we can write
\[
\phi(x_1, ..., x_n) = \int_{\mathbb{R}^n} \Phi(\xi_1, ..., \xi_n) \delta(\xi_1 + ... + \xi_n) e^{2\pi i \sum_{j=1}^n \xi_j x_j} d\xi_1 ... d\xi_n,
\]
\[
(1)
\]
(here \( \delta \) is the Dirac delta function) for some Schwartz function \( \Phi \in \mathcal{S}(\mathbb{R}^n) \) which is supported on the set \( \sum |\xi_j| < 2 \). Note that the values of \( \Phi \) on the hyperplane \( \xi_1 + ... + \xi_n = 0 \) are determined by \( \phi \), it is essentially the Fourier transform of \( \phi \) restricted to \( \sum x_j = 0 \). Our restriction on \( \phi \) will be that \( \Phi \) is supported on the set \( \sum |\xi_j| < 2 \), which we assume from now on.

We denote by \( e_i \) the standard basis vector \((0, ..., 1, ..., 0) \in \mathbb{R}^n \) (1 in the \( i \)-th position) and \( e_{i,k} = e_i - e_k \). It is proved in [8] that under condition (1) (and for a fixed test function)
\[
\lim_{T \to \infty} C_n(T, \phi) = \Phi(0) + \sum_{m=1}^{[n/2]} \left\{ (\alpha_1, \beta_1), ..., (\alpha_m, \beta_m) \right\} \int_{\mathbb{R}^m} \Phi \left( \sum_{j=1}^n \xi_j e_{\alpha_j, \beta_j} \right) \prod_{j=1}^m |\xi_j| d\xi_j,
\]
\[
(2)
\]
the sum being over all disjoint sets of pairs \( \{(\alpha_1, \beta_1), ..., (\alpha_m, \beta_m)\} \) with \( 1 \leq \alpha_j < \beta_j \leq n \).
Next we define the $n$-correlation for unitary matrices. Let $N$ be a natural number, $\phi$ a test function as above. We define the associated periodic test function with scaling factor $N$ by

$$\tilde{\phi}(x_1, \ldots, x_n) = \sum_{u_1, \ldots, u_{n-1} \in \mathbb{Z}} \phi(N(x_1 + u_1), \ldots, N(x_{n-1} + u_{n-1}), N x_n),$$

($\mathbb{Z}$ denotes the set of integers). This function has period 1 in each variable. Let $U$ be a size $N$ unitary matrix with eigenvalues $e^{2\pi i \theta_j}$, $j = 1, \ldots, N$. The $\theta_j$ are real numbers defined up to order and addition of integers, so the quantity

$$R_n(U, \phi) = \frac{1}{N} \sum_{1 \leq j_1, \ldots, j_n \leq N} \tilde{\phi}(\theta_{j_1}, \ldots, \theta_{j_n})$$

is well-defined, and we call it the $n$-correlation of $U$ with test function $\phi$. Again it is simpler to consider the unrestricted sums

$$C_n(U, \phi) = \frac{1}{N} \sum_{1 \leq j_1, \ldots, j_n \leq N} \tilde{\phi}(\theta_{j_1}, \ldots, \theta_{j_n}).$$

By an ingenious combinatorial argument it was shown in [8] that

$$\lim_{N \to \infty} \int_{U(N)} C_n(U, \phi) dU$$

is also given by the RHS of (2), provided that the test function $\phi$ satisfies the condition (1). Here the integration is w.r.t. the normalised Haar measure on $U(N)$, the ensemble of $N \times N$ unitary matrices. Consequently the $n$-correlations of zeta-zeroes and random unitary matrix eigenvalues coincide for this class of test functions (it is conjectured that this is in fact true without any restriction on the test function).

Our goal is to give a new proof of the following result:

**Theorem 1.** Let $\phi$ be a test function as above satisfying the condition (1). Then

$$\int_{U(N)} C_n(U, \phi) dU = \Phi(0) + \sum_{m=1}^{\lfloor n/2 \rfloor} \Phi \left( \sum_{j=1}^{n} \xi_j e_{\alpha_j, \beta_j} \right) \prod_{j=1}^{m} |\xi_j| d\xi_j + O(1/N)$$

as $N \to \infty$, the sum being over all disjoint sets of pairs $\{(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m)\}$ with $1 \leq \alpha_j < \beta_j \leq n$. Here the implied constant in $O(1/N)$ may depend on $\phi$.

The main term appearing here is exactly the RHS of (2).
A closely related quantity to the \( n \)-level correlations of the eigenvalues of random unitary matrices is the average trace product, namely

\[
M(r_1, \ldots, r_n; N) = \int_{U(N)} \prod_{i=1}^{n} \text{tr} U^{r_i} dU,
\]

where \( r_1, \ldots, r_n \) are integers, \( U(N) \) denotes the ensemble of \( N \times N \) unitary matrices and integration is w.r.t. the normalised Haar measure on \( U(N) \). The following theorem is proved by P. Diaconis and M. Shahshahani in [3]. Our statement is taken from [2].

**Theorem 2.** Let \( r_1, \ldots, r_n, N \) be nonzero integers s.t. \( \sum |r_i| \leq 2N \). Let \( s_1, \ldots, s_m \) be the distinct values appearing in the list \( |r_i|, i = 1, \ldots, n \) and \( a_j, b_j, j = 1, \ldots, m \) be such that \( s_j \) appears \( a_j \) times in the list \( r_1, \ldots, r_n \) while \( -s_j \) appears \( b_j \) times. Then

\[
M(r_1, \ldots, r_n; N) = \begin{cases} \prod_{j=1}^{m} a_j! s_j^{a_j}, & a_j = b_j, j = 1, \ldots, m, \\ 0, & \text{otherwise.} \end{cases}
\]

We will derive Theorem 1 from Theorem 2 by a standard calculation which will be carried out in section 5. Our method for proving Theorem 2 proceeds by computing the average of \( \prod_{i=1}^{n} \text{tr} U^{r_i} \) over the set of Frobenius elements of a suitable family of Artin-Schreier L-functions and using the equidistribution result of N. Katz [6, Theorem 3.9.2] to relate this to the unitary matrix average. A similar approach was applied in [5] to the unitary symplectic ensemble using hyperelliptic curves. The method of [3] is completely different and is based on the representation theory of unitary matrices.

## 2 Artin-Schreier L-functions

In this section we summarise the properties of Artin-Schreier (A-S in short) L-functions that we will need. A more detailed survey and further references may be found in [4, §3,§7]. An exposition of the basic properties of A-S L-functions with full details may be found in [9] and of Dirichlet L-functions for the ring of polynomials (which will be needed shortly) in [7].

Let \( p \) be a prime number \( q \) its power, \( F_q \) the finite field with \( q \) elements. Let \( f \in F_q[x] \) be a polynomial of degree \( d \) prime to \( p \). For the rest of the paper we always assume \( (d, p) = 1 \). Fix an additive character \( \psi : F_p^\times \rightarrow \mathbb{C}^\times \). The Artin-Schreier (A-S) function with defining polynomial \( f \) is given by

\[
L_f(z) = \exp \left( \sum_{r=1}^\infty \sum_{\alpha \in F_q} \psi \left( \text{tr}_{F_{q^r}/F_p} f(\alpha) \right) \frac{z^r}{r} \right).
\]

It is known that \( L_f(z) \) is in fact a polynomial of degree \( d - 1 \) and in fact

\[
L_f(z) = \prod_{j=1}^{d-1} (1 - q^{1/2} e^{2\pi i \theta_j} z),
\]
where \( \theta_j = \theta_{f,j} \) are real numbers (well defined upto the addition of integers and reordering). This is an equivalent formulation of the Riemann Hypothesis for the curve \( y^p - y = f(x) \) over \( \mathbb{F}_q \). We denote by \( \Theta_f \) the conjugacy class of the matrix \( \text{diag}(e^{2\pi i \theta_1}, e^{2\pi i \theta_2}, ..., e^{2\pi i \theta_{d-1}}) \in \text{U}(d-1) \). It is called the Frobenius class of \( \Theta_f \).

Denote

\[
\mathcal{F}_d = \{ f \in \mathbb{F}_q[x] \mid \deg f = d, f(0) = 0 \}.
\]

The family of L-functions \( \{ L_f \}_{f \in \mathcal{F}_d} \) is independent of the choice of additive character \( \psi \), because replacing \( \psi \) with \( \psi^a \) (with \( (a, p) = 1 \)) has the same effect on the L-function as replacing \( f \) with \( af \) (by (5)). The following deep result due to N. Katz (special case of [6, Theorem 3.9.2]) is the main ingredient of the present work:

**Theorem 3.** Let \( d \) be fixed and assume \( p > 5 \). Then as \( q \to \infty \) the family \( \{ \Theta_f \}_{f \in \mathcal{F}_d} \) becomes equidistributed in the space of conjugacy classes of some Lie group \( \text{SU}(d-1) \subset G \subset \text{U}(d-1) \) with the measure induced from the Haar measure on \( G \).

We will also make use of the connection between A-S L-functions and Dirichlet L-functions. If \( Q(x) \in \mathbb{F}_q[x] \) is a monic polynomial and \( \chi \) is a Dirichlet character modulo \( Q = x^{d+1} \) we define its L-function

\[
L_{\chi}(z) = \sum_{u \in \mathbb{F}_q[x]} \chi(u) z^{\deg u} = \prod_{P \in \mathbb{F}_q[x] \text{ prime}} (1 - \chi(P) z^{\deg P})^{-1}.
\]

A Dirichlet character \( \chi \) is called even if it is trivial on \( \mathbb{F}_q \). It is called primitive if it is not induced from a character of smaller modulus.

A basic fact we will use is the following (see [4, §7] for a proof):

**Proposition 2.1.** To each \( f \in \mathcal{F}_d \) we can assign a primitive even Dirichlet character \( \chi_f \) modulo \( Q = x^{d+1} \) s.t. \( L_f(z) = (1-z)^{-1} L_{\chi_f}(z) \). If \( p > d \) then this gives a bijection between \( \mathcal{F}_d \) and the set of even primitive Dirichlet characters \( \chi \) modulo \( Q \).

We will also make use of the explicit formula (a proof can be found in [4, §7] as well):

\[
\text{tr} \Theta_f^r = -q^{-r/2} - q^{-r/2} \sum_{\substack{u \text{ monic} \\ \deg u = r}} \Lambda(u) \chi_f(u). \tag{6}
\]

Here \( r \) is any natural number and

\[
\Lambda(u) = \begin{cases} \deg P, & u = P^k \text{ for some prime } P; \\ 0, & \text{otherwise} \end{cases}
\]

is the von Mangoldt function.
A final fact that we will need is the orthogonality relation for characters. Let \( Q = x^{d+1} \) be our modulus, \( u \in \mathbb{F}_q[x] \) nonconstant and prime to \( x \). Then

\[
\langle \chi(u) \rangle_{\chi} = \begin{cases} 
1, & u \equiv a \pmod{x^{d+1}} \text{ for some } a \in \mathbb{F}_q^\times, \\
-1/(q-1), & u \equiv a + bx^d \pmod{x^{d+1}} \text{ for some } a, b \in \mathbb{F}_q^\times, \\
0, & \text{otherwise},
\end{cases}
\]

where \( \langle \cdot \rangle_{\chi} \) denotes the average taken over all even primitive characters modulo \( Q \).

3 Average trace products for Artin-Schreier \( L \)-functions

We keep the notation of the previous section. In particular \( q \) is a power of a prime \( p \) and \( d \) is a natural number prime to \( p \). We also assume \( p > d \) for this section. In the present section we will compute an estimate for the quantity

\[
\langle \prod_{i=1}^{k} \text{tr } \Theta_f^{r_i} \prod_{j=1}^{l} \text{tr } \Theta_f^{-t_j} \rangle_{f \in \mathcal{F}_d},
\]

where \( r_1, ..., r_k, t_1, ..., t_l \) are natural numbers satisfying \( \sum r_i = \sum t_j < d \). We will see that the case \( \sum r_i = \sum t_j \) is really all we need. In the following section we will combine this estimate with Theorem 3 to obtain Theorem 2.

For the rest of this section the asymptotic big-\( O \) notation will always have an implicit constant which may depend on \( k, l, d \) (which we assume are fixed), but not on \( p, q \). We begin by applying (6). Take some \( f \in \mathcal{F}_d \). We have

\[
\prod_{i=1}^{k} \text{tr } \Theta_f^{r_i} \prod_{j=1}^{l} \text{tr } \Theta_f^{-t_j} = \prod_{i=1}^{k} \text{tr } \Theta_f^{r_i} \prod_{j=1}^{l} \text{tr } \Theta_f^{-t_j} = (-1)^{k+l} q^{-\sum r_i} \sum_{u_1, \ldots, v_k, v_1, \ldots, v_l \text{monic}} \prod_{i=1}^{k} \Lambda(u_i) \chi_f(u_i) \prod_{j=1}^{l} \Lambda(v_j) \chi_f(v_j) + O(q^{-1/2})
\]

(the error term comes from the term \( q^{-r/2} \) in (6) and the fact that \( \text{tr } \Theta_f = O(1) \)).

Now using the orthogonality relation (7) and the fact that for \( p > d \) the characters \( \chi_f \) for \( f \in \mathcal{F}_d \) are precisely all the even primitive characters modulo \( x^{d+1} \) we conclude that:
\[
\langle \prod_{i=1}^{k} \langle \sum_{j=1}^{l} \langle \Theta_{f_i} \rangle \rangle \rangle_{f \in F_d} =
\]

\[
= (-1)^{k+l} q^{-\sum r_i} \sum_{u \in F_q^*} \sum_{\text{monic}}^{u_1 \ldots v_k v_1 \ldots v_j} \prod_{i=1}^{k} \Lambda(u_i) \prod_{j=1}^{l} \Lambda(v_j) -
\]

\[
- (-1)^{k+l} q^{-\sum r_i} \sum_{a,b \in F_q^*}^{a \neq 1 \text{ or } a \neq b}^{\deg u_i = r_i, \deg v_j = t_j} + O(q^{-1/2}).
\]

Now since \(\sum r_i = \sum t_j < d\), for \(u_i, v_j\) monic and prime to \(x\) with \(\deg u_i = r_i, \deg v_j = t_j\) we can only have

\[
\prod_{u \in F_q^*} u_i \equiv (a + bx^d) \prod_{v_j} v_j \quad (\text{mod } x^{d+1})
\]

for \(a \in F_q^*, b \in F_q\) if \(a = 1, b = 0\) and \(\prod u_i = \prod v_j\). Therefore we have

\[
\langle \prod_{i=1}^{k} \langle \sum_{j=1}^{l} \langle \Theta_{f_i} \rangle \rangle \rangle_{f \in F_d} =
\]

\[
= (-1)^{k+l} q^{-\sum r_i} \sum_{\text{monic}}^{u_1 \ldots v_k v_1 \ldots v_j} \prod_{i=1}^{k} \Lambda(u_i) \prod_{j=1}^{l} \Lambda(v_j) + O(q^{-1/2}). \quad (8)
\]

Now the contribution to (8) of \(u_i, v_j\) some of which are proper prime powers or such that two of the \(u_i\) or two of the \(v_j\) coincide is easily seen to be \(O(q^{-1})\). For example suppose that \(u_1\) is a power (higher than 1) of some polynomial. Then there are at most \(q^{r-1}\) possibilities for \(u_1\) and at most \(q^{r_1}\) possibilities for every other \(u_i\). Once the \(u_i\) are determined there are at most \(d^{n_k} = O(1)\) ways to factor the product \(\prod u_i\) into \(l\) factors \(v_j\) (because each \(v_j\) is composed of a subset of the prime factors of \(\prod u_i\) of which there are at most \(d\)). After multiplying by \(q^{-\sum r_i}\) and using \(\Lambda(u_i), \Lambda(v_j) \leq d\) we get a total contribution of at most \(O(q^{-1})\). Coincidences of the form \(u_1 = u_2\) also contribute at most \(O(q^{-1})\) and this is seen similarly.

The main contribution is thus from sets of primes \(u_1, \ldots, u_k, v_1, \ldots, v_l\) s.t. the \(u_i\) are distinct and the \(v_j\) are distinct. When such \(u_i\) are chosen the \(v_j\) are the same as the \(u_i\) up to a change of order (in particular we get this contribution
only if \( k = l \) and the \( r_i \) and \( t_j \) coincide up to order). The number of tuples of distinct primes \( u_1, \ldots, u_k \) with \( \deg u_i = r_i \) is \( q^{\sum r_i} / \prod r_i + O(q^{\sum r_i - 1}) \) (this follows from the fact that the number of prime polynomials of degree \( r \) is \( q^r / r + O(q^{r/2}/r) \)). Now as in the statement of Theorem 2 let \( s_1, \ldots, s_m \) be the distinct values appearing in the list \( r_1, \ldots, r_k \), each appearing \( a_i \) times. If \( k = l \) and the \( r_i = t_i \) then for each choice of \( u_i \) we have \( \prod_{\nu=1}^m a_\nu \) ways to order the \( v_j \) (so that \( \deg v_j = t_j \)), so taking everything together we conclude that

\[
\left( \prod_{i=1}^k |\text{tr} \Theta_j^i|^2 \right)_{f \in \mathcal{F}_d} = \prod_{j=1}^m a_j! \prod_{i=1}^k t_i + O(q^{-1/2}).
\]

(9)

On the other hand if the \( r_i \) and the \( t_j \) do not coincide up to order (e.g. if \( k \neq l \)) then

\[
\left( \prod_{i=1}^k |\text{tr} \Theta_j^i| \prod_{j=1}^l |\text{tr} \Theta_j^{-t_j}| \right)_{f \in \mathcal{F}_d} = O(q^{-1/2}).
\]

(10)

## 4 Proof of Theorem 2

We are now ready to prove Theorem 2. We keep the notation of the previous two sections and assume \( p > d \). We fix natural numbers \( n, d, r_1, \ldots, r_k \) with \( \sum r_i < d \) and take the limit \( q \to \infty \). Then by Theorem 3 we have

\[
\left( \prod_{i=1}^n |\text{tr} \Theta_j^i|^2 \right)_{f \in \mathcal{F}_d} \to \int_{U(d-1)} \prod_{i=1}^n |\text{tr} U^r_i|^2 = M(r_1, \ldots, r_k; -r_1, \ldots, -r_k; d-1)
\]

as \( q \to \infty \) (using the notation of section 1 and the integral being as usual w.r.t. the normalised Haar measure). We may integrate over \( U(d-1) \) and not some smaller Lie group \( SU(d-1) \subset G \subset U(d-1) \) as stated in Theorem 3 because unitary scalars make no difference to the absolute value of the traces. Using the estimate (9) we obtain

\[
M(r_1, \ldots, r_k; -r_1, \ldots, -r_k; d-1) = \prod_{j=1}^m a_j! \prod_{i=1}^k r_i,
\]

where the \( s_j, a_j \) are determined from \( r_i \) as in the end of the previous section. This settles Theorem 2 for \( r_i \) that can be ordered so that \( r_{k+i} = -r_i, 1 \leq i \leq k \) and \( n = 2k \) is even, where we take \( d = N-1 \). Similarly using (10) and Theorem 3 we obtain (for natural numbers \( r_i, t_j \)). \( M(r_1, \ldots, r_k, -t_1, \ldots, -t_l; N) = 0 \) if \( \sum r_i = \sum t_j \) but the \( t_j \) are not a reordering of the \( r_i \).

The only remaining case to consider is \( M(r_1, \ldots, r_k, -t_1, \ldots, -t_l; N) \) (again the \( r_i, t_j \) are natural numbers) where \( \sum r_i \neq \sum t_j \). But the map \( U \to e^{i\alpha}U \) (with \( \alpha \in \mathbf{R} \)) preserves the Haar measure on \( U(N) \) and multiplies the trace product \( \prod_{j=1}^l \text{tr} U^{-t_j} \prod_{i=1}^l \text{tr} U^r_i \) by \( e^{i\alpha(\sum r_i - \sum t_j)} \) and so

\[
M(r_1, \ldots, r_k, -t_1, \ldots, -t_l; N) = e^{i\alpha(\sum r_i - \sum t_j)} M(r_1, \ldots, r_k, -t_1, \ldots, -t_l; N)
\]
for every \( \alpha \in \mathbb{R} \). It follows that \( M(r_1, \ldots, r_k, -t_1, \ldots, -t_l; N) = 0 \) if \( \sum r_i \neq \sum t_j \).

Note that the condition \( \sum r_i + \sum t_j \leq 2N \) is not required in this case.

5 \( n \)-correlations

In the present section we derive Theorem 1 from Theorem 2. We do this by a standard calculation involving Fourier series. For the rest of the section we fix a natural number \( n \) and a test function \( \phi \) satisfying the assumptions made in the introduction. That is \( \phi : \mathbb{R}^n \to \mathbb{R} \) is symmetric (unchanged by any permutation of the variables), translation invariant in the sense that 
\[
\phi(x_1, \ldots, x_n) = \phi(x_1 + t, \ldots, x_n + t)
\]
for all \( t \in \mathbb{R} \) and can be expressed as
\[
\phi(x_1, \ldots, x_n) = \int_{\mathbb{R}^n} \Phi(\xi_1, \ldots, \xi_n) e^{2\pi i \sum_{j=1}^n \xi_j x_j} d\xi_1 \ldots d\xi_n
\]
(\( \delta \) denotes the Dirac delta function, the values of \( \Phi \) on the hyperplane \( \sum \xi_j = 0 \) are determined by \( \phi \)) where \( \Phi \) is a Schwartz function supported on \( \sum |\xi_j| < 2 \).

We also define the periodic test function associated with \( \phi \) with scaling factor \( N \) by
\[
\tilde{\phi}(x_1, \ldots, x_n) = \sum_{u_1, \ldots, u_{n-1} \in \mathbb{Z}} \phi(N(x_1 + u_1), \ldots, N(x_{n-1} + u_{n-1}), N x_n).
\]

The Fourier series expansion of \( \tilde{\phi} \) is the following:
\[
\hat{\phi}(x_1, \ldots, x_n) = \frac{1}{N^{n-1}} \sum_{\sum r_j = 0} \Phi\left(\frac{r_1}{N}, \ldots, \frac{r_n}{N}\right) e^{2\pi i \sum_{j=1}^n r_j x_j}.
\]

Combined with (3) we get
\[
C_n(U, \phi) = \frac{1}{N^n} \sum_{\sum r_j = 0} \Phi\left(\frac{r_1}{N}, \ldots, \frac{r_n}{N}\right) \prod_{j=1}^n \text{tr}(U r_j).
\]

Averaging and using (4) we get
\[
\int_{U(N)} C_n(U, \phi) dU = \frac{1}{N^n} \sum_{r_1, \ldots, r_n \in \mathbb{Z}} \hat{\phi}\left(\frac{r_1}{N}, \ldots, \frac{r_n}{N}\right) M(r_1, \ldots, r_n; N) \tag{11}
\]
(we omitted the condition \( \sum r_j = 0 \) because otherwise we have \( M(r_1, \ldots, r_n; N) = 0 \) by Theorem 2).

At this point we use the assumption that \( \Phi(\xi_1, \ldots, \xi_n) \) is supported on the set \( \sum_{i=1}^n |\xi_i| < 2 \). Thus the sum in (11) is only over \( r_1, \ldots, r_n \) satisfying \( \sum |r_j| < 2N \) (and \( \sum r_j = 0 \)). As in the statement of Theorem 2, for each tuple \( r_1, \ldots, r_n \) of integers we consider the distinct nonzero values \( s_1, \ldots, s_m \) appearing among the \( r_i \) (note that some \( r_i \) may be zero). If \( s_j \) appears \( a_j \) times among the \( r_i \) and
−s_j appears b_j times then \( \sum a_j + \sum b_j \leq n \) and nonzero contribution comes only from the case \( a_j = b_j \) in which case

\[
M(r_1, \ldots, r_n; N) = N^{n-2} \sum_{j=1}^{n} a_j! s_j^{a_j} \prod_{j=1}^{n} \xi_j^{s_j} \tag{12}
\]

(we used the fact that tr \( U^0 = N \)).

We make the convention that the asymptotic big-O notation has an implicit constant which may depend on \( n \) and \( \phi \) but not on \( N \) (note the difference from the convention adopted in the previous section, where \( N \) was also assumed fixed!). First we observe that the case in which \( a_j = b_j > 1 \) for some \( j \) contributes only \( O(1/N) \) to (11). Indeed for any choice of \( a_1, \ldots, a_m \) (and \( b_j = a_j \)) we have \( O(N^m) \) choices for the \( s_j \) (satisfying \( s_j \leq N \) and each contributes \( O(1) \) by (12) and due to the factor \( N^{n-2} \) appearing in (11)), so we only get a significant contribution from those tuples with \( \sum a_j = 1 \), i.e. \( a_j = b_j = 1 \), while the rest contribute \( O(1/N) \).

Now let \( m \leq \lfloor n/2 \rfloor \) be a natural number and let \( \sigma = \{ (\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m) \} \) be a set of disjoint distinct pairs of indices \( 1 \leq \alpha_j, \beta_j \leq n \). For each such \( \sigma \) consider the contribution to (11) of the tuples \( r_1, \ldots, r_n \) of integers s.t. \( r_{\alpha_j} = -r_{\beta_j} > 0 \) and \( r_i = 0 \) if \( i \) is not among the \( \alpha_j, \beta_j \). We denote by \( e_i \) the standard basis vector \((0, \ldots, 1, \ldots, 0)\) (1 in the \( i \)-th position) and \( e_{i,k} = e_i - e_k \). The contribution to (11) from the considered tuples is (by (12))

\[
\frac{1}{N^{2m}} \sum_{s_1, \ldots, s_m \in \mathbb{N}} \Phi \left( \frac{1}{N} \sum_{j=1}^{n} s_j e_{\alpha_j, \beta_j} \right) \prod_{j=1}^{m} s_j \tag{13}
\]

(\( \mathbb{N} \) denotes the set of natural numbers). This is a Riemann sum (with step \( 1/N \)) approximating up to \( O(1/N) \) the integral

\[
\int_{\mathbb{R}^m} \Phi \left( \sum_{j=1}^{n} \xi_j e_{\alpha_j, \beta_j} \right) \prod_{j=1}^{m} \xi_j d\xi_j.
\]

We conclude that

\[
\langle C_n(U, \phi) \rangle_{U \in \mathbf{U}(N)} = \Phi(0) + \sum_{m=1}^{\lfloor n/2 \rfloor} \sum_{\{ (\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m) \}} \int_{\mathbb{R}^m} \Phi \left( \sum_{j=1}^{n} \xi_j e_{\alpha_j, \beta_j} \right) \prod_{j=1}^{m} \xi_j d\xi_j + O(1/N),
\]

where the sum is over all the disjoint sets of distinct pairs \( \{ (\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m) \} \). The term \( \Phi(0) \) is the contribution of \( r_1 = \ldots = r_n = 0 \) to (11).

If we use the symmetry (invariance under permutation of variables) of \( \phi \)
(implying the symmetry of Φ restricted to \( \sum \xi_i = 0 \)) we can rewrite this as

\[
\langle C_n(U, \phi) \rangle_{U \in U(N)} =
\]

\[
= \Phi(0) + \sum_{m=1}^{\lfloor n/2 \rfloor} \sum_{\{(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m)\}} \int_{\mathbb{R}^m} \Phi \left( \sum_{j=1}^{n} \xi_j e_{\alpha_j, \beta_j} \right) \prod_{j=1}^{m} |\xi_j| d\xi_j + O(1/N),
\]

the sum now being over disjoint sets \( \{ (\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m) \} \) with \( \alpha_j < \beta_j \). This concludes the proof of Theorem 1.

**Acknowledgment.** The author would like to thank Zeév Rudnick for suggesting this line of research and for many valuable discussions and suggestions in the course of research and writing the paper. The present work is part of the author’s Ph.D. studies in Tel-Aviv University under his supervision. The author would also like to thank Chantal David for pointing out some minor errors in previous versions of the paper.

The research leading to these results has received funding from the European Research Council under the European Unions Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no. 320755.

**References**

[1] B. Conrey, N. Snaith, *n*-correlation with restricted support, preprint at arXiv:1212.5537v1 [math.NT].

[2] P. Diaconis, S. N. Evans, *Linear functionals of eigenvalues of random matrices*, Transactions of the American Mathematical Society, Vol. 353, No. 7. (Jul., 2001), pp. 2615-2633.

[3] P. Diaconis, M. Shahshahani, *On the eigenvalues of random matrices*, Journal of Applied Probability, Vol. 31, Studies in Applied Probability. (1994), pp. 49-62.

[4] A. Entin, *On the distribution of zeroes of Artin-Schreier L-functions*, Springer J. of Geometric and Functional Analysis, vol. 22 (2012) no. 5, pp. 1322-1360.

[5] A. Entin, E. Roditty-Gershon, Z. Rudnick, *Low-lying zeros of quadratic Dirichlet L-functions, hyper-elliptic curves and random matrix theory*, Springer J. of Geometric and Functional Analysis vol. 23 no. 4 (2013).

[6] N. M. Katz, *Moments, monodromy and perversity: a diophantine perspective*, Annals of Math. Studies, 159/2005, Princeton University Press.

[7] M. Rosen, *Number theory in function fields*, Springer GTM 210.

[8] Z. Rudnick, P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Mathematical Journal vol. 81/1996 no. 2 pp. 269-322.
[9] S. A. Stepanov, *Arithmetic of Algebraic Curves*, Springer Monographs in Contemporary Mathematics 1995.