Characteristic polynomials of random unitary matrices: theorems and conjectures

Ashkan Nikeghbali

University of Zurich

June 2010

The characteristic polynomial

- Our random matrix model: the space of unitary matrices of size n, $U(n)$, endowed with the Haar measure.
- Let $u_n \in U(n)$; the characteristic polynomial of u_n is given by

$$P_n(z) = \det(z\mathrm{Id}_n - u_n).$$

- The characteristic polynomial evaluated at 1, $\det(\mathrm{Id}_n - u_n)$, has received much attention (but (almost) nothing as a function of z). The main motivation is coming from number theory.

Questions

- Motivated by the existing conjectural link between random matrix theory and number theory, or simply by the wish to establish strong limit theorems (a.s. convergence, iterated logarithm law), one may ask the following natural question: is it possible to define on the same probability space random matrix models for all finite dimensions? Vaguely speaking, is there a natural induction or a natural way to couple all dimensions?
- How to understand a little more the conjectures between L-functions and random matrix theory?

The virtual permutations of Kerov, Olshanski and Vershik

- The space $\mathcal{S}^{\infty}$ of virtual permutation can be defined as follows. For $n \geqslant m \geqslant 1$, $\pi_{m,n}$ denotes the application from $\mathcal{S}_n$ to $\mathcal{S}_m$ such that for $\sigma \in \mathcal{S}_n$, $\pi_{m,n}(\sigma) \in \mathcal{S}_m$ is obtained from σ by deleting all the elements of $\{m+1,\dots,n\}$ from its cycle structure; then $\mathcal{S}^{\infty}$ is the projective limit of $(\mathcal{S}_n)_{n\geqslant 1}$, i.e. the set of sequences $(\sigma_n)_{n\geqslant 1}$ of permutations such that for $n \geqslant 1$, $\sigma_n \in \mathcal{S}_n$ and for $n \geqslant m \geqslant 1$, $\sigma_m = \pi_{m,n}(\sigma_n)$.
- A virtual permutation $(\sigma_n)_{n\geqslant 1}$ can naturally be constructed by the so-called *Chinese restaurant process* as follows:
  - σ_1 is the unique permutation in $\mathcal{S}_1$;
  - for $n \geqslant 1$, σ_{n+1} is obtained from σ_n either by adding $n+1$ as a fixed point, or by inserting $n+1$ inside a cycle of σ_n.

Generating random permutations

If the space $\mathcal{S}^{\infty}$ is endowed with the σ-algebra generated by the coordinates $(\sigma_n)_{n\geqslant 1}$, and if $\theta > 0$, then it is possible to define the so-called *Ewens measure of parameter* θ, as the unique measure under which for all $n \geqslant 1$, the coordinate σ_n follows Ewens measure of parameter θ on $\mathcal{S}_n$, i.e. for all $\sigma \in \mathcal{S}_n$,

$$\mathbb{P}[\sigma_n = \sigma] = \frac{\theta^{k_\sigma}}{\theta(\theta+1)\dots(\theta+n-1)},$$

where k_σ denotes the number of cycles of σ (in particular, for $\theta = 1$, σ_n follows uniform measure on $\mathcal{S}_n$). A random virtual permutation following Ewens measure of parameter θ can be constructed by the Chinese restaurant process, with the following assumption: conditionally on σ_n, $n+1$ is a fixed point of σ_{n+1} with probability $\theta/(\theta+n)$, otherwise, it is inserted inside the cycle structure of σ_n, each of the n possible places having the same probability $1/(\theta+n)$.

Strong convergence

Proposition [Tsilevich (1997)]

Let $\sigma = (\sigma_n)_{n \geqslant 1}$ be a virtual permutation following the Ewens measure of parameter $\theta > 0$, and for $n \geqslant 1$, $p \geqslant 1$, let $\ell_p(\sigma_n)$ be the length of the p-th longest cycle of the permutation $\sigma_n \in \mathcal{S}_n$ (for p larger than the number of cycles of σ_n, one defines $\ell_p(\sigma_n) := 0$). Then, almost surely, for all $p \geqslant 1$, the limit:

$$y_p(\sigma) := \lim_{n \to \infty} \frac{\ell_p(\sigma_n)}{n}$$

exists, and $(y_p(\sigma))_{p \geqslant 1}$ follows a Poisson-Dirichlet distribution of parameter θ.

This can be translated into an almost sure convergence result for random permutation matrices.

Proposition

Let $(u_n)_{n\geqslant 1}$ be a random virtual permutation consisting of the sequence of permutation matrices associated to a virtual permutation σ which follows the Ewens measure of parameter $\theta > 0$. Then, for all $n \geqslant 1$, zero is an eigenangle of u_n, and its multiplicity increases almost surely to infinity when n goes to infinity. Moreover, for $n \geqslant 1$, $k \geqslant 1$, let $\theta_k^{(n)}$ be the k-th smallest strictly positive eigenangle of u_n, and $\theta_{-k}^{(n)}$ the k-th largest strictly negative eigenangle of u_n. Then, almost surely, for all $n \geqslant 1$, $k \geqslant 1$, $\theta_{-k}^{(n)} = -\theta_k^{(n)}$, and for n going to infinity, $n\theta_k^{(n)}/2\pi$ converges to the k-th smallest element of the set which contains exactly all the strictly positive multiples of $1/y_p(\sigma)$ for all $p \geqslant 1$.

A natural extension of virtual permutations

This part is based on joint work with P. Bourgade and J. Najnudel. (based on earlier work with A. Rouault).

- Neretin (2001) has defined the virtual unitary group but it is not an extension of the virtual permutations;
- We propose a more natural definition for *virtual isometries*;
- Main ingredient: complex reflections, i.e. unitary transformations u such that the rank of $\mathrm{Id} - u$ is 0 or 1.

$\mathbf{C}^n$ is equipped with the scalar product $\langle x, y\rangle = \sum \overline{x}_k y_k$. Let e and m be two vectors of norm 1. There exists a unique complex reflection r such that $r(e) = m$ and it is given by

$$r = \mathrm{Id} - \frac{1}{1 - \langle m, e\rangle} \langle m - e, .\rangle (m - e).$$

Natural projections

We now need to define an extension of the $\pi_{m,n}$ which is valid for the unitary group; it is indeed possible to construct a natural projection from the unitary group of a finite-dimensional Hilbert space E to a unitary group of a subspace of F.

Proposition

Let H be a complex Hilbert space, E a finite-dimensional subspace of H and F a subspace of E. Then, for any unitary operator u on H which fixes each element of $E^{\perp}$, there exists a unique unitary operator $\pi_{E,F}(u)$ on H which satisfies the two following conditions:

- $\pi_{E,F}(u)$ fixes each element of $F^{\perp}$;
- the image of H by $u - \pi_{E,F}(u)$ is included into the image of $F^{\perp}$ by $u - \mathrm{Id}$.

Moreover, if G is a subspace of F, $\pi_{F,G} \circ \pi_{E,F}(u)$ is well-defined and is equal to $\pi_{E,G}(u)$.

How this works on a simple example

Let us consider the simple case where $E = \mathrm{Vect}(F, e)$, where e is a unit vector, orthogonal to F. In this case, if u is a unitary operator fixing each element of $E^{\perp}$, then the operator $v := \pi_{E,F}(u)$ can be constructed explicitly as follows.

- If $u(e) = e$, then one takes $v = u$, which fixes $E^{\perp}$ and e, hence, it fixes $F^{\perp}$, and $(u - v)(H) = \{0\} = (u - \mathrm{Id})(F^{\perp})$.
- If $u(e) \neq e$, then for all $x \in H$, we define

$$v(x) := u(x) + \frac{\langle e - u(e), u(x) \rangle}{\langle e - u(e), u(e) \rangle} (e - u(e)). \tag{1}$$

Note that if $u \neq e(u)$, $u = r\pi_{E,F}(u)$, where r is the unique reflection such that $r(e) = u(e)$. Similarly, $u = \pi_{E,F}(u)r'$ which r' is the unique reflection such that $r'(u^{-1}(e)) = e$.

Projection

In fact $\pi_{E,F}$ is also a projection in the sense of the minimization of a distance:

Proposition

Let H be a complex Hilbert space, and let $U_0(H)$ be the space of the unitary operators on H which fix each element of the orthogonal of a finite-dimensional subspace of H. Then the map d from $U_0(H) \times U_0(H)$ to $\mathbb{N}$, given by $d(u,v) := \operatorname{rank}(u-v)$ defines a finite distance on $U_0(H)$. Moreover, if $F \subset E$ are two finite-dimensional subspaces of H, and if u is a unitary operator fixing each element of $E^{\perp}$, then $\pi_{E,F}(u)$ is the unique unitary operator fixing each element of $F^{\perp}$ and such that $d(u,\pi_{E,F}(u))$ is minimal. The image of H by $u-\pi_{E,F}(u)$ is equal to the image of $F^{\perp}$ by $u-\mathrm{Id}$, and one has:

$$d(u,\pi_{E,F}(u)) = \dim(E) - \dim(F) - \dim(\{x \in E \cap F^{\perp}, u(x) = x\}),$$

in particular, if one is not an eigenvalue of the restriction of u to $E \cap F^{\perp}$, then

$$d(u,\pi_{E,F}(u)) = \dim(E) - \dim(F)$$

Virtual isometries

The existence of the projective map described above implies the possibility to define the virtual isometries. Indeed, let $H := \ell^2(\mathbb{C})$, and let $(e_n)_{n \geqslant 1}$ be the canonical Hilbert basis of H. For all $n \geqslant 1$, the space of unitary operators fixing each element of the orthogonal of $\mathrm{Span}(e_1, \ldots, e_n)$ can be canonically identified with the unitary group $U(n)$. By this identification, for $n \geqslant m \geqslant 1$, the projection $\pi_{\mathrm{Span}(e_1,\ldots,e_n),\mathrm{Span}(e_1,\ldots,e_m)}$ defines a map $\pi_{n,m}$ from $U(n)$ to $U(m)$, and for $n \geqslant m \geqslant p \geqslant 1$, one has $\pi_{n,p} = \pi_{n,m}\pi_{m,p}$.

Definition

A *virtual isometry* is a sequence $(u_n)_{n \geqslant 1}$ of unitary matrices, such that for all $n \geqslant 1$, $u_n \in U(n)$ and $\pi_{n+1,n}(u_{n+1}) = u_n$. In this case, for all $n \geqslant m \geqslant 1$, $\pi_{n,m}(u_n) = u_m$. The space of virtual isometries will be denoted U^∞.

Proposition

Let $(\sigma_n)_{n\geqslant 1}$ be a sequence of permutations such that $\sigma_n \in \mathcal{S}_n$ for all $n \geqslant 1$, and let $(\Sigma_n)_{n\geqslant 1}$ be the corresponding sequence of permutation matrices. Then $(\Sigma_n)_{n\geqslant 1}$ is a virtual isometry if and only if $(\sigma_n)_{n\geqslant 1}$ is a virtual permutation.

Proposition

Let $(x_n)_{n\geqslant 1}$ be a sequence of vectors, x_n lying on the complex unit sphere of $\mathbb{C}^n$ for all $n\geqslant 1$. Then, there exists a unique virtual isometry $(u_n)_{n\geqslant 1}$ such that $u_n(e_n)=x_n$ for all $n\geqslant 1$, and u_n is given by

$$u_n = r_n r_{n-1}\dots r_1,$$

where for $j\in\{1,\dots,n\}$, $r_j=\mathrm{Id}$ if $x_j=e_j$, and otherwise, r_j is the unique reflection such that $r_j(e_n)=x_n$. Moreover, in the particular case where for all $n\geqslant 1$, $x_n=e_{i_n}$ for $i_n\in\{1,\dots,n\}$, then $(u_n)_{n\geqslant 1}$ is the sequence of matrices associated to a virtual permutation $(\sigma_n)_{n\geqslant 1}$ constructed by the Chinese restaurant process: for all $n\geqslant 1$,

$$\sigma_n=\tau_{n,i_n}\tau_{n-1,i_{n-1}}\dots\tau_{1,i_1},$$

where, for $j,k\in\{1,\dots,n\}$, $\tau_{j,k}=\mathrm{Id}$ if $j=k$ and $\tau_{j,k}$ is the transposition (j,k) if $j\neq k$.

Quick proof

One has $u_1(e_1) = x_1$ if and only if $u_1 = x_1$, which is equal to r_1. For all $n \geqslant 1$, two cases are possible:

- if $x_{n+1} = e_{n+1}$, then $\pi_{n+1,n}(u_{n+1}) = u_n$ and $u_{n+1}(e_{n+1}) = e_{n+1}$ if and only if $u_{n+1} = (u_n) \oplus 1$, where the symbol $\oplus$ denotes diagonal blocks of matrices;
- if $x_{n+1} \neq e_{n+1}$, using the explicit formulas $\pi_{n+1,n}(u_{n+1}) = u_n$ and $u_{n+1}(e_{n+1}) = x_{n+1}$ if and only if $u_{n+1} = r_{n+1}\,(u_n \oplus 1)$.

The Haar measure

Is there an analogue of the Haar measure on U^∞?

Proposition

Let $(x_n)_{n\geqslant 1}$ be a random sequence of vectors, x_n lying on the complex unit sphere of $\mathbb{C}^n$ for all $n \geqslant 1$, and let $(u_n)_{n\geqslant 1}$ be the unique virtual isometry such that $u_n(e_n) = x_n$ for all $n \geqslant 1$. Then, for each n, the matrix u_n follows Haar measure on $U(n)$ if and only if $x_1, \dots, x_n$ are independent and for all $j \in [1, n]$, x_j follows uniform measure on the complex unit sphere of $\mathbb{C}^j$.

Proposition

For all $n \geqslant m \geqslant 1$, the image of the Haar measure on $U(n)$ by the projection $\pi_{n,m}$ is equal to the Haar measure on $U(m)$.

Extension result

Now we need an extension theorem:

Proposition

Let $\mathcal{U}$ be the σ-algebra on U^{∞}, generated by the sets:

$$\{(u_n)_{n\geqslant 1}, u_k \in B_k\},$$

for all $k \geqslant 1$ and for all Borel sets B_k in $U(k)$. Let $(\mu_n)_{n\geqslant 1}$ be a family of probability measures, μ_n defined on the space $U(n)$ (endowed with its Borel σ-algebra), and such that the image of μ_{n+1} by $\pi_{n+1,n}$ is equal to μ_n for all $n \geqslant 1$. Then, there exists a unique probability measure on $(U^{\infty}, \mathcal{U})$ such that its image by the n-th coordinate is equal to μ_n for all $n \geqslant 1$.

Proposition

There exists a unique probability measure μ_0 on the space $(U^\infty, \mathcal{U})$ such that its image by all the coordinate maps are equal to Haar measure on the corresponding unitary group. This measure can be described as follows. Let $(x_n)_{n\geqslant 1}$ be a random sequence of vectors, x_n lying on the complex unit sphere of $\mathbb{C}^n$ for all $n \geqslant 1$, and let $(u_n)_{n\geqslant 1}$ be the unique virtual isometry such that $u_n(e_n) = x_n$ for all $n \geqslant 1$. Then, the distribution of $(u_n)_{n\geqslant 1}$ is equal to μ_0 if and only if $(x_n)_{n\geqslant 1}$ are independent, and for all $n \geqslant 1$, x_n follows uniform measure on the complex unit sphere of $\mathbb{C}^n$.

From now, the measure μ_0 will be called *Haar measure on virtual isometries*. This is the analog of the uniform measure on virtual permutations, which can be obtained in the setting of the above Proposition, by taking $(x_n)_{n\geqslant 1}$ independent, x_n uniform on the finite set $\{e_1, \ldots, e_n\}$.

Theorem

Let $(u_n)_{n\geqslant 1}$ be a random virtual isometry, following Haar measure. For $n \geqslant 1$, $k \geqslant 1$, let $\theta_k^{(n)}$ be the k-th smallest strictly positive eigenangle of u_n, and let $\theta_{1-k}^{(n)}$ be the k-th largest nonnegative eigenangle of u_n. Then almost surely, for all $k \in \mathbb{Z}$, $n\theta_k^{(n)}/2\pi$ converges to a limit x_k when n goes to infinity. Moreover, the point process $(x_k)_{k\in\mathbb{Z}}$ is a determinantal process and its kernel K is the *sine kernel*, i.e it is given by:

$$K(x,y) = \frac{\sin(\pi(x-y))}{\pi(x-y)}.$$

This result is obtained as a consequence (after lengthy computations) of the following recursive decomposition of the characteristic polynomial:

Proposition

Let $(u_n)_{n \geqslant 1}$ be a virtual isometry, and for $n \geqslant 1$, let $x_n := u_n(e_n)$, $v_n := x_n - e_n$, let $(f_k^{(n)})_{1 \leqslant k \leqslant n}$ be an orthonormal basis of $\mathbb{C}^n$, consisting of eigenvectors of u_n, let $(\lambda_k^{(n)})_{1 \leqslant k \leqslant n}$ be the corresponding sequence of eigenvalues, let P_n be the characteristic polynomial of u_n, given by

$$P_n(z) := \det(z\mathrm{Id}_n - u_n),$$

and let us decompose the vector $x_{n+1} \in \mathbb{C}^{n+1}$ as follows:

$$x_{n+1} = \sum_{k=1}^{n} \mu_k^{(n)} f_k^{(n)} + \nu_n e_{n+1},$$

Then for all $n \geqslant 1$ such that $x_{n+1} \neq e_{n+1}$, one has $\nu_n \neq 1$, and the polynomials P_n and P_{n+1} satisfy the relation:

$$P_{n+1}(z) = \frac{P_n(z)}{\overline{\nu_n} - 1} \left[(z - \nu_n)(\overline{\nu_n} - 1) - (z - 1) \sum_{k=1}^{n} |\mu_k^{(n)}|^2 \frac{\lambda_k^{(n)}}{z - \lambda_k^{(n)}} \right],$$

Proof

Since $(u_n)_{n \geqslant 1}$ is a virtual isometry and $x_{n+1} \neq e_{n+1}$, one has $u_{n+1} = r_{n+1}(u_n \oplus 1)$, where r_{n+1} is the unique reflection such that $r_{n+1}(e_{n+1}) = x_{n+1}$. One can check that the matrix r_{n+1} is given by:

$$r_{n+1} = \mathrm{Id}_{n+1} + \frac{1}{\overline{\nu_n} - 1} v_{n+1} \overline{v_{n+1}}^t,$$

which implies, for $z \notin \{\lambda_1^{(n)}, \dots \lambda_n^{(n)}, 1\}$,

$$\begin{aligned} P_{n+1}(z) &= \det(z\mathrm{Id}_{n+1} - u_n \oplus 1) \det \left[\mathrm{Id}_{n+1} - \left(\frac{1}{\overline{\nu_n} - 1} (z\mathrm{Id}_{n+1} - u_n \oplus 1)^{-1} v_{n+1} \overline{v_{n+1}}^t \right. \right. \\ &= (z-1) P_n(z) \left[1 - \frac{1}{\overline{\nu_n} - 1} \operatorname{Tr} \left((z\mathrm{Id}_{n+1} - u_n \oplus 1)^{-1} v_{n+1} \overline{v_{n+1}}^t (u_n \oplus 1) \right) \right], \end{aligned}$$

since $\det(\mathrm{Id} + A) = 1 + \operatorname{Tr}(A)$ for any matrix A with rank one. One deduces, by writing the matrices in the basis $(e_{n+1}, f_1^{(n)}, \dots, f_n^{(n)})$:

$$P_{n+1}(z) = (z-1) P_n(z) \left[1 - \frac{1}{\overline{\nu_n} - 1} \left(\frac{|\nu_n - 1|^2}{z - 1} + \sum^{n} |\mu_k^{(n)}|^2 \frac{\lambda_k^{(n)}}{z - \lambda^{(n)}} \right) \right]$$

The moments of the characteristic polynomial

Take z on the unit circle in the recursive formula for the characteristic polynomial to obtain the following decomposition:

Proposition

Let $u_N \in U(N)$ be distributed with the Haar measure $\mu_{U(N)}$. Then for all $\theta \in \mathbf{R}$

$$\det(\mathrm{Id}_N - e^{i\theta} u_N) \overset{\text{law}}{=} \prod_{k=1}^{N} \left(1 + e^{i\theta_k} \sqrt{\beta_{1,k-1}}\right),$$

with $\theta_1, \dots, \theta_n, \beta_{1,0}, \dots, \beta_{1,n-1}$ independent random variables, the θ_k's uniformly distributed on $[0, 2\pi]$ and the $\beta_{1,j}$'s ($0 \leqslant j \leqslant N-1$) being beta distributed with parameters 1 and j (by convention, $\beta_{1,0}$ is the Dirac distribution on 1).

Let $Y_N = \det(\mathrm{Id}_N - u_N)$. For all t and s with $\mathfrak{Re}(t \pm s) > -1$,

$$\mathbf{E}\left(|Y_N|^t e^{is \arg Y_N}\right) = \prod_{k=1}^{N} \frac{\Gamma(k)\,\Gamma(k+t)}{\Gamma\left(k+\frac{t+s}{2}\right)\Gamma\left(k+\frac{t-s}{2}\right)}. \tag{2}$$

$$\frac{\log Y_N}{\sqrt{\frac{1}{2}\log N}} \overset{\text{law}}{\Rightarrow} \mathcal{N}_1 + i\mathcal{N}_2,$$

where $\mathcal{N}_1$ and $\mathcal{N}_2$ are two independent standard Gaussian random variables.

The moments conjecture

Keating-Snaith, *CMP*, 2000.

For $\mathrm{Re}(\lambda) > -1$, we should have

$$\lim_{T\to\infty} \frac{1}{(\log T)^{\lambda^2}} \frac{1}{T} \int_0^T \left|\zeta\left(\frac{1}{2}+it\right)\right|^{2\lambda} dt = \mathcal{G}(\lambda) A(\lambda) \qquad (3)$$

where $\mathcal{G}(\lambda)$ is the so-called *random matrix factor* that we would rather call the *group factor*,

$$\mathcal{G}(\lambda) = \frac{(G(1+\lambda))^2}{G(1+2\lambda)} \qquad (4)$$

while $A(\lambda)$ is the *arithmetic factor* defined by the Euler product

$$A(\lambda) = \prod_p \left(1-\frac{1}{p}\right)^{\lambda^2} \left(\sum_{m=0}^{\infty} \left(\frac{\Gamma(\lambda+m)}{m!\Gamma(\lambda)}\right)^2 p^{-m}\right). \qquad (5)$$

- There have been many conjectures made in number theory, based on computations made in the RMT world.
- Most conjectures can be made theorems in function fields.
- we want to propose a framework which unifies both the number field and function field cases.

How to understand the moments conjecture?

This part is based on joint works with E. Kowalski.
In probability theory, one typically looks at re-scaled sums of random variables. What happens if one looks at re-scaled characteristic functions, as suggested by the results of Keating and Snaith?
We are interested in sequences of random variables $(Z_n)_{n\geqslant 0}$ which do not converge in distribution, but which have the remarkable feature that the "decay" of their characteristic functions $\varphi_{Z_n}(u) = \mathbf{E}[\exp(iuX_n)]$, when $n \to \infty$, is precisely given by that of characteristic functions in some family of standard probability distributions.

Definitions

Definition

Let (X_N) be a sequence of $\mathbf{R}^m$-valued random variables defined on a probability space $(\Omega, \Sigma, \mathbf{P})$. Let

$$Q_N(t) = Q_N(t_1, t_2, \dots, t_m)$$

be a sequence of non-negative quadratic forms on $\mathbf{R}^m$. The sequence (X_N) is then said to be convergent in the mod-Gaussian sense with covariance Q_N and limiting function Φ if

$$\lim_{N \to +\infty} \exp(Q_N(t)/2) \mathbf{E}(e^{it \cdot X_N}) = \Phi(t) \qquad (6)$$

locally uniformly for $t \in \mathbf{R}^m$.
Let $0 \leqslant \delta_{1,N} \leqslant \delta_{2,N} \leqslant \cdots \leqslant \delta_{m,N}$ be the eigenvalues of Q_N; we will assume in fact that for some fixed $\mu > 0$, we have

$$\delta_{\ ,N} \leqslant \delta^{\mu} \qquad \delta_{\ ,N} \to +\infty \qquad (7)$$

Definition

We say that a sequence of random variables (Z_N) converges in the mod-Poisson sense with parameters λ_N if the following limit

$$\lim_{N\to+\infty} \exp(\lambda_N(1-e^{iu}))\,\mathbf{E}(e^{iuZ_N}) = \Phi(u)$$

exists for every $u \in \mathbf{R}$, and the convergence is locally uniform.

Examples

If we take $\lambda = iu$, with $u \in \mathbf{R}$ in the result by Keating and Snaith, then one obtains for $Z_N = \log |Y_N|^2$:

$$\lim_{N\to\infty} e^{u^2 \log N}\mathbf{E}[e^{iuZ_N}] = \lim_{N\to\infty} e^{u^2 \log N}\mathbf{E}[e^{iu \log |Y_N|^2}] = \frac{(G(1+iu))^2}{G(1+2iu)}. \qquad (8)$$

Consequently the sequence (Z_n) converges in the mod-Gaussian sense with parameters $(0, 2\log N)$ and limiting function $\frac{(G(1+iu))^2}{G(1+2iu)}$ which is not a characteristic function.

Taking $\lambda = iu$, for $u \in \mathbf{R}$ in the moments conjecture, the r.v. $\log |\zeta(1/2 + iU_T)|^2$, where U_T is a r.v. uniformly distributed on $(0, T)$, converges, when $T \to \infty$, in the mod-Gaussian sense with parameters $(0, 2 \log\log T)$ and limiting function $\mathcal{G}(iu) A(iu)$.
According to the calculations by Keating-Snaith, the group factor $\mathcal{G}$ is occurring as a limiting function for the mod-Gaussian convergence of the characteristic polynomial on the unitary group. This extra factor predicted by random matrix theory should be considered as a correction factor to account for the fact that the prime numbers do not behave independently of each other. At this point, one should also note that mod-Gaussian convergence is obviously a stronger mode of convergence than the classical central limit theorem which is obtained after re-normalisation: the normalisation has the effect of ”erasing” the dependence structure. Indeed, to prove Selberg's central limit theorem for the zeta function, one does not need to take into account the dependence between the prime numbers.

The arithmetic factor

How about the arithmetic factor? One can prove that

$$A(iu) = \lim_{N \to +\infty} e^{u^2(\log(e^{\gamma} \log N))} \mathbf{E}\left(e^{iuL_N}\right)$$

where

$$L_N = \sum_{p \leqslant N} \log \left| 1 - \frac{e^{i\theta_p}}{\sqrt{p}} \right|^2 ,$$

for any sequence $(\theta_p)_{p \leqslant N}$ of independent random variables, uniformly distributed on $[0, 1]$ and with γ the Euler constant.

Structure of the moments

A classical result of Erdős and Kác states that the arithmetic function $\omega(n)$, the number of (distinct) prime divisors of a positive integer $n \geqslant 1$, behaves for large n like a Gaussian random variable with mean $\log\log n$ and variance $\log\log n$, in the sense that

$$\lim_{N\to+\infty} \frac{1}{N} \left|\left\{n \leqslant N \mid a < \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} < b\right\}\right| = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt \qquad (9)$$

for any real numbers $a < b$.
It seems slightly more appropriate to consider

$$\omega'(n) = \omega(n) - 1 \qquad (10)$$

for $n \geqslant 2$, because Poisson random variables takes all integral values $\geqslant 0$,

Proposition

For $u \in \mathbf{R}$, let

$$\Phi_1(u) = \frac{1}{\Gamma(e^{iu}+1)} \tag{11}$$

and let

$$\Phi_2(u) = \prod_p \left(1 - \frac{1}{p}\right)^{e^{iu}} \left(1 + \frac{e^{iu}}{p-1}\right). \tag{12}$$

Then for any $u \in \mathbf{R}$, we have

$$\lim_{N \to +\infty} \frac{(\log N)^{(1-e^{iu})}}{N} \sum_{2 \leqslant n \leqslant N} e^{iu\omega'(n)} = \Phi_1(u)\Phi_2(u), \tag{13}$$

and the convergence is locally uniform.

Remark

We shall see that the Euler product Φ_2 (like A) corresponds to mod-Poisson convergence for a natural asymptotic probabilistic model of primes, and that

A small calculation shows that

$$\Phi_2(u) = \lim_{y\to+\infty} \exp((1-e^{iu})\lambda_y) \prod_{p\leqslant y} \left(1 - \frac{1}{p} + \frac{1}{p} e^{iu}\right)$$
$$= \lim_{y\to+\infty} \mathbf{E}(e^{iuP_{\lambda_y}})^{-1}\, \mathbf{E}(e^{iuZ'_y})$$

where

$$\lambda_y = \sum_{p\leqslant y} \log\left(\frac{1}{1-p^{-1}}\right) = \sum_{\substack{p\leqslant y\\ k\geqslant 1}} \frac{1}{kp^k} = \log\log y + \kappa + o(1),$$

as $y \to +\infty$, for some real constant κ and

$$Z'_y = \sum_{p\leqslant y} B'_p \tag{14}$$

is a sum of independent Bernoulli random variables with parameter $1/p$:

$$\mathbf{P}(B'_p = 1) = \frac{1}{p}, \qquad \mathbf{P}(B'_p = 0) = 1 - \frac{1}{p}.$$

Remark

We note that, as expected, the parameters of these Bernoulli laws correspond exactly to the “intuitive” probability that an integer n be divisible by p.

As in the case of the Riemann zeta function, we also note that the independent model fails to capture the truth on the distribution of $\omega(n)$, the extent of this failure being measured, in some sense, by the factor $\Phi_1(u)$. Because

$$\frac{Z'_y - \log\log y}{\sqrt{\log\log y}} \overset{\text{law}}{\Rightarrow} \mathcal{N}(0,1),$$

this discrepancy between the independent model and the arithmetic truth is invisible at the level of the normalized convergence in distribution (as it is for $\log|\zeta(1/2+it)|$, by Selberg’s Central Limit Theorem, hiding the Random Matrix Model).

Moments of function fields zeta functions

We give an example of mod-Gaussian convergence in the setting of families of L-functions, as developed by Katz and Sarnak. We restrict our attention to the family of hyperelliptic curves.

Let p be an odd prime number and let $q = p^n$, $n \geqslant 1$, be a power of p. We denote by $\mathbf{F}_q$ a field with q elements, in particular $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Recall from the theory of finite fields that if we fix an algebraic closure $\bar{\mathbf{F}}_q$ of $\mathbf{F}_q$, then for every $n \geqslant 1$ there exists a unique subfield $\mathbf{F}_{q^n}$ of $\bar{\mathbf{F}}_q$ which has order q^n (i.e., it is a field extension of degree n of $\mathbf{F}_q$), which is characterized as the set of $x \in \bar{\mathbf{F}}_q$ such that $x^{q^n} = x$.

Let $g \geqslant 1$ be an integer, and let $f \in \mathbf{F}_q[T]$ be a monic polynomial of degree $2g+1$ with no repeated roots (in an algebraic closure $\bar{\mathbf{F}}_q$ of $\mathbf{F}_q$). Then the set C_f of solutions, in $\bar{\mathbf{F}}_q^2$, of the polynomial equation

$$C_f \,:\, y^2 = f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1 x + a_0,$$

is called an *affine hyperelliptic curve of genus g*. Taking the associated homogeneous equation in projective coordinates $[x : y : z]$, one gets the projective curve

$$\tilde{C}_f \,:\, y^2 z^{2g-1} = f(xz^{-1})z^{2g+1} = x^{2g+1} + a_{2g}zx^{2g} + \cdots + a_1 z^{2g} x + a_0 z^{2g+1},$$

which corresponds to C_f with an added point at infinity with projective coordinates $[0 : 1 : 0]$.

For every $n \geqslant 1$, denote by $\tilde{C}_f(\mathbf{F}_{q^n})$ the set of points in $\tilde{C}_f$ which have coordinates in the subfield $\mathbf{F}_{q^n}$ of $\bar{\mathbf{F}}_q$. The L-function $P_f(T)$ of $\tilde{C}_f$ (sometimes called the L-function of C_f instead) is then defined as the numerator of the zeta function $Z(\tilde{C}_f)$ defined by the formal power series expansion

$$Z(\tilde{C}_f) = \exp\Big(\sum_{n\geqslant 1} \frac{|\tilde{C}_f(\mathbf{F}_{q^n})|}{n} T^n\Big) = \exp\Big(\sum_{n\geqslant 1} \frac{|C_f(\mathbf{F}_{q^n})|+1}{n} T^n\Big),$$

which is known to represent a rational function of the form

$$Z(\tilde{C}_f) = \frac{P_f(T)}{(1-T)(1-qT)},$$

which determines uniquely the L-function P_f.

(A. Weil on the Riemann Hypothesis for curves over finite fields)
– P_f is a polynomial with integer coefficients of degree $2g$, with $P_f(0) = 1$.
– [Functional equation] We have the polynomial identity

$$q^g T^{2g} P_f\left(\frac{1}{qT}\right) = P_f(T).$$

– [Riemann Hypothesis] If we write

$$P_f(T) = \prod_{1 \leqslant j \leqslant 2g} (1 - \alpha_{f,j} T), \qquad \alpha_{f,j} \in \mathbf{C}, \tag{15}$$

then all the inverse roots $\alpha_{f,j}$ satisfy $|\alpha_{f,j}| = \sqrt{q}$.
– [Spectral interpretation] There exists a well-defined conjugacy class F_f in the set $USp(2g, \mathbf{C})^\sharp$ of conjugacy classes in the compact unitary group $USp(2g, \mathbf{C})$ such that

$$P_f(T) = \det(1 - q^{1/2} T F_f). \tag{16}$$

We now state a particular case of Deligne's equidistribution theorem:

Theorem, Katz-Sarnak

Fix an integer $g \geqslant 1$. For every power q of an odd prime p, let $\mathcal{H}_{g,q}$ be the set of monic polynomials in $\mathbf{F}_q[T]$ of degree $2g+1$ which have no multiple roots. Let $H_{g,q}$ be random variables with values in $USp(2g, \mathbf{C})^\sharp$ and with distributions given by

$$\mathbf{P}(H_{g,q} = C) = \frac{1}{|\mathcal{H}_{g,q}|} |\{f \in \mathcal{H}_{g,q} \mid F_f = C\}| \tag{17}$$

for any conjugacy class $C \in USp(2g, \mathbf{C})^\sharp$.
Then, as $q \to +\infty$, among odd powers of primes, the random variables $H_{g,q}$ converge in law to a random variable H_g distributed according to

$$\mathbf{P}(H_g \in A) = \mu_g(A), \tag{18}$$

for any conjugacy-invariant measurable set A in $USp(2g, \mathbf{C})$, where μ_g is the probability Haar measure on $USp(2g, \mathbf{C})$.

Proposition

Let $g \geqslant 1$ be an integer. Let $H_{g,q}$ be random variables as in the Theorem. For any $\lambda \in \mathbf{C}$ with $\mathrm{Re}(\lambda) > 0$, we have

$$\lim_{g \to +\infty} \lim_{q \to +\infty} \frac{1}{g^{(\lambda^2+\lambda)/2}} \mathbf{E}(\det(1 - H_{g,q})^{\lambda}) = M_{Sp}(\lambda),$$

where

$$M_{Sp}(\lambda) = 2^{-\lambda^2/2} \left(\frac{\pi}{2}\right)^{\lambda/2} \frac{G(3/2)}{G(3/2+\lambda)}$$

In particular, for any integer $k \geqslant 1$, we have

$$\lim_{g \to +\infty} \lim_{q \to +\infty} \frac{1}{g^{(k^2+k)/2}} \mathbf{E}(\det(1 - H_{g,q})^{k}) = \prod_{j=1}^{k} \frac{1}{(2j-1)!!}.$$

Remark

It remains a major problem to obtain results of this type without the inner limit over q, which already transforms the arithmetic to a pure “random matrix” problem by the magic of Deligne’s equidistribution theorem.
Our approach allows us to produce conjectures in this situation.

The number of irreducible factors

Let $\mathbf{F}_q$ be a finite field with $q = p^n$ elements, with $n \geqslant 1$ and p prime. For a polynomial $f \in \mathbf{F}_q[X]$, let

$$\omega(f) = \omega_q(f) = \left|\{\pi \in \mathbf{F}_q[X] \mid \pi \text{ is irreducible monic and divides } f\}\right|$$

be the analogue of the number of prime factors of an integer (we will usually drop the subscript q).
We consider the statistic behavior of this function under two types of limits:
(i) either q is replaced by q^m, $m \to +\infty$, and f is assumed to range over monic polynomials of fixed degree $d \geqslant 1$ in $\mathbf{F}_{q^m}[X]$; or
(ii) q is fixed, and f is assumed to range over monic polynomials of degree $d \to +\infty$ in $\mathbf{F}_q[X]$.

The first case is not ”too difficult” and corresponds to the Katz-Sarnak regime: let us assume first that $f \in \mathbf{F}_q[X]$ is squarefree. Let K_f denote the splitting field of f, i.e., the extension field of $\mathbf{F}_q$ generated by the d roots of f, and let F_f denote the Frobenius automorphism $x \mapsto x^q$ of K_f. This automorphism permutes the roots of f, which all lie in K_f, and after enumerating them, leads to an element of $\mathfrak{S}_d$, denoted F_f. This depends on the enumeration of the roots, but the conjugacy class $F_f^\sharp \in \mathfrak{S}_d^\sharp$ is well-defined.
Now, by the very definition, we have

$$\omega(f) = \varpi(F_f^\sharp), \tag{19}$$

which can be seen as the analogue of the spectral interpretation of an L-function as a characteristic polynomial.

Fact. In the limit of fixed d and $m \to +\infty$, for f uniformly chosen among monic squarefree polynomials of degree d in $\mathbf{F}_{q^m}[X]$, the conjugacy classes $F_f^\sharp$ become uniformly distributed in $\mathfrak{S}_d^\sharp$ for the natural (Haar) measure. Hence, we obtain

$$\omega(f) \overset{\text{law}}{\Rightarrow} \varpi(\sigma_d),$$

as $m \to +\infty$, where f is distributed uniformly among monic polynomials of degree d in $\mathbf{F}_{q^m}[X]$, and σ_d is distributed uniformly among $\mathfrak{S}_d$.

The second limit, where the base field $\mathbf{F}_q$ is fixed and the degree d grows, is analogue of the problematic situation of families of curves of increasing genus over a fixed finite field.

Theorem

Let $q \neq 1$ be a power of a prime p, and let $\omega(f)$ denote as before the number of monic irreducible polynomials dividing $f \in \mathbf{F}_q[X]$. Write $|g| = q^{\deg(g)} = |\mathbf{F}_q[X]/(g)|$ for any non-zero $g \in \mathbf{F}_q[X]$.
For any $u \in \mathbf{R}$, we have

$$\lim_{d \to +\infty} \frac{\exp((1 - e^{iu}) \log d)}{q^d} \sum_{\deg(f)=d} e^{iu(\omega(f)-1)} = \tilde{\Phi}_1(u)\tilde{\Phi}_2(u), \tag{20}$$

where

$$\tilde{\Phi}_1(u) = \frac{1}{\Gamma(e^{iu}+1)} \tag{21}$$

and

$$\tilde{\Phi}_2(u) = \prod_{\pi} \left(1 - \frac{1}{|\pi|}\right)^{e^{iu}} \left(1 + \frac{e^{iu}}{|\pi| - 1}\right), \tag{22}$$

the product running over all monic irreducible polynomials $\pi \in \mathbf{F}_q[X]$ and the sum over all monic polynomials $f \in \mathbf{F}_q[X]$ with degree $\deg(f) = d$. Moreover, the convergence is uniform.

The idea from the proof we want to highlight – the source of the splitting of the limiting function in two parts of distinct probabilistic origin – is to first separate the irreducible factors of “small” degree and those of “large” degree, and then observe that an equidistribution theorem allows us to perform a transfer of the contribution of large factors to the corresponding average over random permutations, conditioned to not have small cycle lengths. This will explain the factor $\tilde{\Phi}_1$ corresponding to the cycle length of random permutations.

Values distribution

Problem

It is a hard (and open) problem to prove that

$$\overline{\{\zeta(1/2+it), t \in \mathbf{R}\}} = \mathbf{C}.$$

How about the similar problem for the characteristic polynomial:

$$\mathbf{P}[(\det(\mathrm{Id}_n - u_n)) \in U]?$$

for some open set U?

How about the analogue for function fields, i.e. is the discrete set

$$\{L_f(1/2),\ f \in \mathcal{F}\}$$

dense in $\mathbf{C}$?

Theorem

Let $m \geqslant 1$ be fixed and let (X_N) be a sequence of $\mathbf{R}^m$-valued random variables defined on $(\Omega, \Sigma, \mathbf{P})$, such that (X_N) converges in the mod-Gaussian sense with covariance (Q_N), and that the convergence is μ-balanced with $\mu > 0$, with $\sigma_N \geqslant 1$ for all N. Let (G_N) be Gaussian random variables with covariance matrices given by (Q_N), so that

$$\exp(-Q_N(t)/2) = \mathbf{E}(e^{it \cdot G_N}).$$

Assume moreover the following three conditions:
(1) There exist constants $a > 0$, $\alpha > 0$ and $C > 0$ such that, for any $N \geqslant 1$ and $t \in \mathbf{R}^m$ such that $\|t\| \leqslant \sigma_N^a$, we have

$$\mathbf{E}(e^{it \cdot X_N}) = \Phi(t) \exp(-Q_N(t)/2) \left\{ 1 + O\left(\frac{1}{\exp(\alpha \sigma_N^C)} \right) \right\}. \tag{23}$$

(2) The function Φ is of class C^1 on $\{\|t\| < 2\}$.
(3) For some $A \geqslant 1$ and $\beta \geqslant 0$, we have $|\Phi(t)| \ll \exp(\beta \|t\|^A)$, for $t \in \mathbf{R}^m$.

Let $D > 0$ be any number such that $D > 2(m+1+\max\{a^{-1}, A/C, 3m(m+1)\mu A\})$. Then, for any fixed non-empty open box

$$U = \{x \in \mathbf{R}^m \mid \|x - x_0\|_\infty < \varepsilon\} \subset \mathbf{R}^m,$$

$$\mathbf{P}(X_N \in U) = \mathbf{P}(G_N \in U) + O\Big(\frac{1}{\sigma_N^{1/2+1/D}} + \frac{\varepsilon^{-m}}{\sigma_N}\Big), \tag{24}$$

for $N \geqslant 1$, where the implied constant depends only on (m, Φ, a, α, C) and the implied constant in *(23)*.
In particular, for any fixed non-empty open set $U \subset \mathbf{R}^m$, we have

$$\mathbf{P}(X_N \in U) \gg \frac{1}{\sqrt{\sigma_N}}$$

provided $N \geqslant N_0$, where N_0 and the implied constant depend on U and the same data as above.

Consequences

Theorem

Let $z_0 \in \mathbf{C}^\times$ be arbitrary, $\varepsilon > 0$ such that $\varepsilon \leqslant |z_0|$. There exists $N_0(z_0, \varepsilon)$, which can be bounded explicitly, such that

$$\mu_N(\{g \in U(N) \mid |\det(1-g) - z_0| < \varepsilon\}) \gg \left(\frac{\varepsilon}{|z_0|}\right)^2 \frac{1}{\log N} \tag{25}$$

provided $N \geqslant N_0$, where μ_N denotes probability Haar measure on the unitary group $U(N) \subset GL(N, \mathbf{C})$, and the implied constant is absolute.

Theorem

Define

$$P_N(t) = \prod_{p \leqslant N} (1 - p^{-1/2 - it})^{-1} \tag{26}$$

for $N \geqslant 1$ and $t \in \mathbf{R}$. Let $z_0 \in \mathbf{C}^{\times}$ be arbitrary, $\varepsilon > 0$ such that $\varepsilon \leqslant |z_0|$. There exists $N_0(z_0, \varepsilon)$, explicitly bounded, such that

$$\liminf_{T \to +\infty} \frac{1}{T} \lambda(\{t \leqslant T \mid P_N(t) \in V\}) \gg \left(\frac{\varepsilon}{|z_0|}\right)^2 \frac{1}{\log\log N},$$

for all $N \geqslant N_0$, where λ is the Lebesgue measure and the implied constant is absolute.

Theorem

The set of central values of the L-functions attached to non-trivial primitive Dirichlet characters of $\mathbf{F}_p[X]$, where p ranges over primes, is dense in $\mathbf{C}$.

The zeta function

Keating and Snaith conjecture that:

Conjecture

Define $\log \zeta(1/2+iu)$, when $u \in \mathbf{R}$ is not the ordinate of a non-trivial zero of $\zeta(s)$, by continuation along the horizontal line $\mathrm{Im}(s) = u$, with limit 0 when $\mathrm{Re}(s) \to +\infty$.
For any $t = (t_1, t_2) \in \mathbf{R}^2$, we have

$$\frac{1}{T}\int_0^T e^{it\cdot\log\zeta(1/2+iu)}du = A(t)\mathcal{G}(t)\exp\left(-\frac{t^2}{2}(\log\log T)\right)(1+o(1))$$

as $T \to +\infty$.

Corollary

Assume there exist $\alpha > 0$, $\delta > 0$ and $\theta > 0$ such that the Keating-Snaith Conjecture holds with the error term $o(1)$ replaced by

$$\exp(-\alpha(\log\log T)^{\delta})$$

uniformly for $\|t\| \leqslant (\log\log 6T)^{\theta}$. Then the set of values $\zeta(1/2+it)$ is dense in the complex plane. In fact, there exists $C > 0$, $D \geqslant 0$, such that, for any $z_0 \in \mathbf{C}^{\times}$ and $\varepsilon \leqslant |z_0|$, there exists t with

$$0 \leqslant t \ll \max\left\{\exp\left(\exp\left((\log|z_0|)^2\right)\right), \exp\left(\exp\left(C\left(\frac{\varepsilon}{2|z_0|}\right)^{-D}\right)\right)\right\},$$

such that

$$|\zeta(\tfrac{1}{2}+it) - z_0| < \varepsilon.$$