Random matrix theory motivated by number theory

Ashkan Nikeghbali
University of Zurich

References

- K. Maples, J. Najnudel, A.N., *Limit operators for circular ensembles*.
- P. Bourgade, J. Najnudel, A.N., *A unitary extension of virtual permutations*.
- R. Chhaibi, J. Najnudel, A.N., *A limiting random analytic function related to the CUE*.
- F. Delbaen, E. Kowalski, A.N., *mod-ϕ convergence*.

The random matrix model

- The unitary group with the Haar measure;
- Eigenvalues on the unit circle; $e^{i\theta_1}, \cdots, e^{i\theta_n}$.
- Weyl's integration formula: the joint density of the eigenangles $(\theta_1, \cdots, \theta_n) \in [0, 2\pi]^n$ is:

$$\frac{1}{(2\pi)^n n!} \prod_{j<k} |e^{i\theta_j} - e^{i\theta_k}|^2.$$

Determinantal structure

- If u_n is distributed according to Haar measure, then one can define, for $1 \leq p \leq n$, the p-point correlation function $\rho_p^{(n)}$ of the eigenangles, as follows: for any bounded, measurable function ϕ from $\mathbb{R}^p$ to $\mathbb{R}$,

$$\mathbb{E}\left[\sum_{1 \leq j_1 \neq \cdots \neq j_p \leq n} \phi(\theta_{j_1}^{(n)}, \ldots, \theta_{j_p}^{(n)})\right]$$
$$= \int_{[0,2\pi)^p} \rho_p^{(n)}(t_1, \ldots, t_p)\phi(t_1, \ldots, t_p) dt_1 \ldots dt_p.$$

- If the kernel $K^{(n)}$ is defined by

$$K^{(n)}(t) := \frac{\sin(nt/2)}{2\pi \sin(t/2)}$$

then the p-point correlation function is be given by

$$\rho_p^{(n)}(t_1, \ldots, t_n) = \det\left(K^{(n)}(t_j - t_k)\right)_{j,k=1}^{p}.$$

Proposition

Let E_n denote the set of eigenvalues taken in $(-\pi, \pi]$ and multiplied by $n/2\pi$. Let Define for $y \neq y^{'}$

$$K^{(\infty)}(y, y^{'}) = \frac{\sin[\pi(y^{'} - y)]}{\pi(y^{'} - y)}$$

and

$$K^{(\infty)}(y, y) = 1.$$

Then there exists a point process E_∞ such that for all $r \in \{1, \dots, n\}$, and for all measurable and bounded functions F with compact support from $\mathbb{R}^r$ to $\mathbb{R}$:

$$\mathbb{E}\left(\sum_{x_1 \neq \dots \neq x_r \in E_n} F(x_1, \dots, x_r)\right) \underset{n\to\infty}{\longrightarrow} \int_{\mathbb{R}^r} F(y_1, \dots, y_r)\rho_r^{(\infty)}(y_1, \dots, y_r) dy_1 \dots dy_r,$$

where

$$\rho_r^{(\infty)}(y_1, \dots, y_r) = \det((K^{(\infty)}(y_j, y_k))_{1 \leq j,k \leq r}).$$

Moreover the point process E_n converges to E_∞ in the following sense: for all Borel measurable bounded functions f with compact support from $\mathbb{R}$ to $\mathbb{R}$,

$$\sum_{x \in E_n} f(x) \underset{n \to \infty}{\longrightarrow} \sum_{x \in E_\infty} f(x),$$

where the convergence above holds in law.

Dyson (1962)

Pair Correlation

For suitable test functions f,

$$\lim_{n\to\infty}\frac{1}{n}\int_{U(n)}\sum_{j\neq k} f(\tilde{\theta}_j-\tilde{\theta}_k)dX=\int_{-\infty}^{\infty} f(v)\left(1-\left(\frac{\sin\pi v}{\pi v}\right)^2\right)dv$$

Distribution of zeros

The Riemann zeta function: for $\mathfrak{Re}(s) > 1$,

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \left(1 - p^{-s}\right)^{-1};$$

It can be analytically continued:

$$\xi(s) = \pi^{-s/2} s(s-1)\Gamma(s/2)\zeta(s) = \xi(1-s).$$

Riemann hypothesis: write a zero ρ_n as:

$$\rho_n = 1/2 + i\gamma_n, \quad \gamma_n > 0.$$

Montgomery

Conjecture

Write $\tilde{\gamma}_n = \frac{\gamma_n}{2\pi} \log(\gamma_n/2\pi)$; then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j\neq k\leq N} f(\tilde{\gamma}_j - \tilde{\gamma}_k) = \int_{-\infty}^{\infty} f(v) \left(1 - \left(\frac{\sin \pi v}{\pi v}\right)^2\right) dv$$

Why the unitary group?

- The sine kernel has some universal feature; so is there really something about zeta?
- Spectral interpretation: the conjectures are proved in the function field case by Katz and Sarnak;
- There are more striking connections to RMT through the approach by Keating and Snaith.

Moments of the zeta function

It was conjectured by number theorists that the following should hold: for $\mathfrak{Re}(\lambda > -1/2)$,

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^{2\lambda} dt \sim a(\lambda)g(\lambda)(\log T)^{\lambda^2/2},$$

with

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

and g a rational function with $g(1)=1$, $g(2)=2$, $g(3)=\frac{42}{9!}$ and $g(4)=\frac{24024}{16!}$.

A random model for the value distribution of $\zeta(1/2+it)$

A remarkable random variable: for $u \in U(n)$,

$$P_n(z) = \det(zI - u)$$

and

$$\int_{U(n)} |P_n(1)|^{2\lambda} d\mu \sim \frac{G^2(1+\lambda)}{G(1+2\lambda)} n^{\lambda^2},$$

where G is the Barnes function defined by $G(z+1) = \Gamma(z)G(z)$ and $G(1) = 1$.

The missing factor

It is not hard to see that:

$$\frac{G^2(1+k)}{G(1+2k)} = \prod_{j=1}^{k-1} \frac{j!}{(j+k)!}.$$

For $k = 1, 2, 3, 4$, this $g(k)$.

Conjecture

$$g(\lambda) = \frac{G^2(1+\lambda)}{G(1+2\lambda)}.$$

A remarkable finite n computation

Keating and Snaith proved that for s, t complex numbers with $\mathfrak{Re}(t) > -1$,

$$\mathbb{E}[|P_n(1)|^t \exp(is \arg P_n(1))] = \prod_{k=1}^{n} \frac{\Gamma(k)\Gamma(k+t)}{\Gamma(k+(t+s)/2)\Gamma(k+(t-s)/2)}.$$

From this they were able to show that as $n \to \infty$

$$\frac{\log P_n(1)}{\sqrt{1/2 \log n}} \to \mathcal{N}_{\mathbb{C}}, \text{ in law }.$$

This is to be compared with Selberg's CLT:

$$\frac{\log \zeta(1/2 + iU_T)}{\sqrt{1/2 \log \log T}} \to \mathcal{N}_{\mathbb{C}} \quad \text{in law}$$

where

$$\mathcal{N}_{\mathbb{C}} = \mathcal{N}(0,1) + i\mathcal{N}'(0,1).$$

Questions

- This approach allows a dictionary where one tries to solve in the RMT world hard problems in NT;
- Problem by Katz and Sarnak: how to associate in a natural way to a given ensemble of random matrices an infinite dimensional operator with the good eigenvalues?
- Can one construct a limiting random analytic function from the characteristic polynomials?
- Take a typical problem about the value distribution of the zeta function, say Ramachandra's conjecture. Can one develop methods which would lead to theorems?
- Examples of problems which are proved in NT and whose RMT analogue would be meaningful.

Goals

- Give a meaning to strong convergence;
- Prove convergence of eigenvalues and eigenvectors;
- Set the framework for the construction of the operator;

Consider

$$\xi_n(z) = \frac{P_n(e^{2iz\pi/n})}{P_n(1)}.$$

Theorem (Chhaibi, Najnudel, N)

In the space of continuous functions from $\mathbb{C}$ to $\mathbb{C}$, endowed with the topology of uniform convergence on compact sets, the random entire function ξ_n converges in law to a limiting entire function ξ_∞. The zeros of ξ_∞ are all real and form a determinantal sine-kernel point process, i.e. for all $r \geq 1$, the r-point correlation function ρ_r corresponding to this point process is given, for all $x_1, \ldots, x_r \in \mathbb{R}$, by

$$\rho_r^{(\infty)}(x_1, \ldots, x_r) = \det\left(\frac{\sin[\pi(x_j - x_k)]}{\pi(x_j - x_k)}\right)_{1 \leq j,k \leq r}.$$

Virtual Permutations (Kerov, Olshanski, Vershik)

Proposition

For $n \in \mathbb{N}$, let $t(n) \in \{1, \dots, n\}$. Then any permutation σ_n can be uniquely written as

$$\sigma_n = \tau_{n,t(n)} \tau_{n-1,t(n-1)} \cdots \tau_{1,1}$$

where $\tau_{k,j} = 1$ if $j = k$ and otherwise is the transposition (j, k).

- If for each $k \geq 1$, $\mathbb{P}[t(k) = j] = 1/k$ for $1 \leq j \leq k$, and the $t(k)$ are independent, then σ_n is Haar distributed.
- A virtual permutation is a sequence $\{(\sigma_n), n \geq 1\}$ such that $\sigma_{n+1} = \tau_{n+1,t(n+1)} \sigma_n$.
- One goes from σ_{n+1} to σ_n by deleting $n + 1$ from the cycle structure of σ_{n+1}.
- With $(t(n))_{n \geq 1}$, independent and chosen as above, each σ_n is Haar distributed.
- Then there exists a projective limit of the Haar measure on the space of virtual permutations and it is w.r.to this measure that a.s. convergence can be established.

Complex Reflections

- We endow $\mathbb{C}^n$ with the scalar product: $\langle x, y\rangle = \sum_{k=1}^{n} x_k \bar{y}_k$.
- A reflection is a unitary transformation such that r such that it is the identity or the rank of $Id - r$ is 1.
- Every reflection can be represented as:

$$r(x) = x - (1-\alpha)\frac{\langle x, a\rangle}{\langle a, a\rangle}a,$$

  where a is some vector and α is an element of the unit circle.
- Given two distinct unit vectors e and m , there exists a unique complex reflection r such that $r(e) = m$ and it is given by

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

Constructing virtual isometries $(u_n)_{n\geq 1}$

The sequence $(u_n)_{n\geq 1}$ can be constructed in the following way:

1. One considers a sequence $(x_n)_{x\geq 1}$ of independent random vectors, x_n being uniform on the unit sphere of $\mathbb{C}^n$.
2. Almost surely, for all $n \geq 1$, x_n is different from the last basis vector e_n of $\mathbb{C}^n$, which implies that there exists a unique complex reflection $r_n \in U(n)$ such that $r_n(e_n) = x_n$ and $I_n - r_n$ has rank one.
3. We define $(u_n)_{n\geq 1}$ by induction as follows: $u_1 = x_1$ and for all $n \geq 2$,

$$u_n = r_n \begin{pmatrix} u_{n-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

Random virtual isometries

Theorem [Bourgade-Najnudel-N]

Let $(x_n)_{n\geq 1}$ be a sequence of random vectors, $x_n \in \mathbb{C}^n$ and $||x|| = 1$. Let $(u_n)_{n\geq 1}$ be the virtual isometry satisfying $u_n(e_n) = x_n$. Then for each n, the random matrix u_n follows the Haar measure on $U(n)$ iff the vectors (x_n) are independent and uniformly distributed on the corresponding spheres (i.e. x_n uniformly distributed on the unit sphere of $\mathbb{C}^n$).

Projective limit of the Haar measure

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

$$\{(u_n), u_k \in \mathcal{B}_k\}, \quad k \geq 1 \quad \text{and } B_k \in \mathcal{B}(U(k)).$$

There exists a unique probability measure μ_∞ on this space such that its image under projection on $U(n)$ is the Haar measure on $U(n)$.

The characteristic polynomial

Theorem [Bourgade-Najnudel-N]

Let $(u_n)_{n\geq 1}$ be the virtual isometry satisfying $u_n(e_n) = x_n$ and note $v_n = x_n - e_n$. Let $(f_k^{(n)})_{1\leq k\leq n}$ be an o.n. basis of $\mathbb{C}^n$ consisting of eigenvectors of u_n and let $(\lambda_k^{(n)})_{1\leq k\leq n}$ be the corresponding sequence of eigenvalues. Recall $P_n = \det(z - u_n)$. Let us also decompose x_{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 such that $x_{n+1} \neq e_{n+1}$, one has $\nu_n \neq 1$ and

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

Idea of the proof

- Let $x_n = u_n(e_n)$ and let r_n denote the unique reflection on $\mathbb{C}^n$ mapping e_n to x_n. Therefore, we have $u_{n+1} = r_{n+1} \circ (u_n \oplus 1)$.
- Write $r_{n+1} = I_{n+1} + \frac{1}{\bar{\nu}_n - 1} v_{n+1} \bar{v}_{n+1}^t$.
- Then note that

$$P_{n+1}(z) = (z-1) P_n(z) \det \left(I_{n+1} - \left(\frac{1}{\bar{\nu}_n - 1} (zI_{n+1} - u_n \oplus 1)^{-1} v_{n+1} \bar{v}_{n+1}^t (u_n \oplus$$

- Use $\det(1 + A) = 1 + \mathrm{Tr}(A)$ for a matrix of rank 1.

Theorem (Maple-Najnudel-N)

Almost surely the eigenvalues of u_{n+1} are the unique roots of the rational equation

$$\sum_{j=1}^{n} |\mu_j^{(n)}|^2 \frac{\lambda_j^{(n)}}{\lambda_j^{(n)} - z} + \frac{|1-\nu_n|^2}{1-z} = 1 - \overline{\nu}_n$$

on the unit circle. Furthermore, they interlace between 1 and the eigenvalues of u_n

$$0 < \theta_1^{(n+1)} < \theta_1^{(n)} < \theta_2^{(n+1)} < \cdots < \theta_n^{(n)} < \theta_{n+1}^{(n+1)} < 2\pi.$$

and the eigenvectors satisfy the relation

$$(h_k^{(n+1)})^{\frac{1}{2}} f_k^{(n+1)} = \sum_{j=1}^{n} \frac{\mu_j^{(n)}}{\lambda_j^{(n)} - \lambda_k^{(n+1)}} f_j^{(n)} + \frac{\nu_n - 1}{1 - \lambda_k^{(n+1)}} e_{n+1},$$

$$h_k^{(n+1)} = \sum_{j=1}^{n} \frac{|\mu_j^{(n)}|^2}{|\lambda_j^{(n)} - \lambda_k^{(n+1)}|^2} + \frac{|\nu_n - 1|^2}{|1 - \lambda_k^{(n+1)}|^2}$$

is the unique positive real which makes $f_k^{(n+1)}$ a unit vector.

Idea of Proof

- Let f be an eigenvector of u_{n+1} with corresponding eigenvalue z. Then we write
$$f = \sum_{j=1}^{n} a_j f_j^{(n)} + b e_{n+1}$$
where $a_1, \ldots, a_n, b$ are (as yet unknown) complex numbers, not all zero. Our goal is to write these coefficients in terms of x_{n+1} and the eigenvalues of u_n.
- We write $zf = u_{n+1} f$ and use $u_{n+1} = r_{n+1} \circ (u_n \oplus 1)$.
- This leads to the system $Qf = 0$ where
$$Q = I_{n+1} + wv^t,$$
and
$$w = \begin{pmatrix} \frac{\mu_1^{(n)}}{\lambda_1^{(n)} - z} \\ \vdots \\ \frac{\mu_n^{(n)}}{\lambda_n^{(n)} - z} \\ \frac{\nu_n - 1}{1 - z} \end{pmatrix}; \text{ and } \quad v^t = \left(\lambda_1^{(n)} \frac{\overline{\mu_1^{(n)}}}{\overline{\nu_n} - 1}, \quad \ldots \quad \lambda_n^{(n)} \frac{\overline{\mu_n^{(n)}}}{\overline{\nu_n} - 1}, \quad 1 \right).$$

- The one can show that
$$v^t w = -1,$$
and this gives the recurrence relations.
- The interlacing property is obtained after a careful study of the rational function $\Phi : S^1 \to \mathbb{C} \cup \{\infty\}$ by
$$\Phi(z) = \sum_{j=1}^{n} \frac{\lambda_j^{(n)} |\mu_j^{(n)}|^2}{\lambda_j^{(n)} - z} + \frac{|\nu_n - 1|^2}{1 - z} - (1 - \overline{\nu_n}).$$

Some fundamental a priori estimates

Let us fix $\epsilon > 0$, and let us define the following events:

$$E_0 = \{\theta_0^{(1)} \neq 0\} \cap \{\forall n \geq 1, \nu_n \neq 0\} \cap \{\forall n \geq 1, 1 \leq k \leq n, \mu_k^{(n)} \neq 0\}$$
$$E_1 = \{\exists n_0 \geq 1, \forall n \geq n_0, |\nu_n| \leq n^{-\frac{1}{2}+\epsilon}\}$$
$$E_2 = \{\exists n_0 \geq 1, \forall n \geq n_0, 1 \leq k \leq n, |\mu_k^{(n)}| \leq n^{-\frac{1}{2}+\epsilon}\}$$
$$E_3 = \{\exists n_0 \geq 1, \forall n \geq n_0, k \geq 1, n^{-\frac{5}{3}-\epsilon} \leq \theta_{k+1}^{(n)} - \theta_k^{(n)} \leq n^{-1+\epsilon}\}.$$

We then let $E := E_0 \cap E_1 \cap E_2 \cap E_3$. Then E is a set of full measure.

Convergence of eigenangles

Theorem (Bourgade, Najnudel, N/ Maples, Najnudel, N)

There is a sine-kernel point process $(y_k)_{k\in\mathbb{Z}}$ such that almost surely,

$$\frac{n}{2\pi}\theta_k^{(n)} = y_k + O((1+k^2)n^{-\frac{1}{3}+\epsilon}),$$

for all $n \geq 1$, $|k| \leq n^{1/4}$ and $\epsilon > 0$, where the implied constant may depend on $(u_m)_{m\geq 1}$ and ϵ, but not on n and k.

Some filtrations

Lemma (Maples, Najnudel, N)

For $n \geq 1$, we define the σ-algebra $\mathcal{A}_n = \sigma\{\lambda_j^{(m)} \mid 1 \leq m \leq n, 1 \leq j \leq m\}$ and its limit $\mathcal{A} = \vee_{n=1}^{\infty} \mathcal{A}_n$. For all $n \geq 1$, the σ-algebra $\mathcal{A}_n$ is equal, up to completion, to the σ-algebra generated by u_1 the variables $|\mu_j^{(m)}|$ and ν_m for $1 \leq m \leq n-1$ and $1 \leq j \leq m$.

Lemma (Maples, Najnudel, N)

For $1 \leq j \leq n$, we define the phase $\phi_j^{(n)}$ by $\mu_j^{(n)} = \phi_j^{(n)} |\mu_j^{(n)}|$, and the σ-algebras $\mathcal{B}_n = \mathcal{A} \vee \sigma\{\phi_j^{(m)} \mid 1 \leq m \leq n-1, 1 \leq j \leq m\}$ and $\mathcal{B} = \vee_{n=1}^{\infty} \mathcal{B}_n$. Then the σ-algebra $\mathcal{B}_n$ is equal, up to completion, to the σ-algebra generated by $\mathcal{A}$ and the eigenvectors $f_j^{(m)}$ for $1 \leq j \leq m$ and $1 \leq m \leq n$.

A.s. weak convergence of eigenvectors

We introduce the following eigenvectors, for $n \geq k$:

$$g_k^{(n)} := D_k^{(n)} f_k^{(n)},$$

where $D_k^{(n)} \in \mathbb{C}$ is the random variable

$$D_k^{(n)} = \prod_{s=k}^{n-1} (h_k^{(s+1)})^{\frac{1}{2}} \frac{\lambda_k^{(s)} - \lambda_k^{(s+1)}}{\mu_k^{(s)}}.$$

Theorem (Maples, Najnudel, N)

For each $k \geq 1$ and $\ell \geq 1$, the sequence $\{\langle g_k^{(n)}, e_\ell \rangle\}_{n \geq k \vee \ell}$ is a martingale with respect to the filtration $(\mathcal{B}_n)_{n \geq k \vee \ell}$, and the conditional expectation of $|\langle g_k^{(n)}, e_\ell \rangle|^2$, given $\mathcal{A}$, is almost surely bounded when n varies.

A.s. weak convergence of eigenvectors

Because this martingale is bounded in L^2, we have the following immediate corollary.

Corollary (Maples, Najnudel, N)

Almost surely, for all $k \in \mathbb{Z}$ and $\ell \geq 1$, the scalar product $\langle g_k^{(n)}, e_\ell \rangle$ converges to a limit $g_{k,\ell}$ when n goes to infinity.

- For each $k \in \mathbb{Z}$, the infinite sequence $g_k := (g_{k,\ell})_{\ell \geq 1} \in \mathbb{C}^\infty$ can be considered as the weak limit of the eigenvector $g_k^{(n)}$ of u_n, when n goes to infinity.

A.s. weak convergence of eigenvectors

Theorem (Maples, Najnudel, N)

Let $(u_n)_{n\geq 1}$ be a virtual rotation, following the Haar measure. For $k \in \mathbb{Z}$ and $n \geq 1$, let $v_k^{(n)}$ be a unit eigenvector corresponding to the kth smallest nonnegative eigenangle of u_n for $k \geq 1$, and the $(1-k)$th largest strictly negative eigenangle of u_n for $k \leq 0$. Then for all $k \in \mathbb{Z}$, there almost surely exist some complex numbers $(\psi_k^{(n)})_{n\geq 1}$ of modulus 1, and a sequence $(t_{k,\ell})_{\ell\geq 1}$, such that for all $\ell \geq 1$,

$$\sqrt{n}\,\langle \psi_k^{(n)} v_k^{(n)}, e_\ell \rangle \underset{n\to\infty}{\longrightarrow} t_{k,\ell}.$$

Almost surely, for all $k \in \mathbb{Z}$, the sequence $(t_{k,\ell})_{\ell\geq 1}$ depends, up to a multiplicative factor of modulus one, only on the virtual rotation $(u_n)_{n\geq 1}$. Moreover, if $(\psi_k)_{k\in\mathbb{Z}}$ is a sequence of iid, uniform variables on $\mathbb{U}$, independent of $(t_{k,\ell})_{\ell\geq 1}$, then $(\psi_k t_{k,\ell})_{k\in\mathbb{Z},\ell\geq 1}$ is an iid family of standard complex gaussian variables ($\mathbb{E}[|\psi_k t_{k,\ell}|^2] = 1$).

A flow of operators on a random space

- For each $\alpha \in \mathbb{R}$, let $(\alpha_n)_{n\geq 1}$ be a sequence such that α_n is equivalent to αn when n goes to infinity. For $n \geq 1$, $k \in \mathbb{Z}$, we have

$$u_n^{\alpha_n} f_k^{(n)} = e^{i\theta_k^{(n)}\alpha_n} f_k^{(n)}.$$

- Now, $e^{i\theta_k^{(n)}\alpha_n}$ tends to $e^{2i\pi\alpha y_k}$ and after normalization, the coordinates of $f_k^{(n)}$ tend to the corresponding coordinates of the sequence $(t_{k,\ell})_{\ell\geq 1}$. It is then natural to expect that, in a sense which needs to be made precise, $u_n^{\alpha_n}$ tends to some operator U, acting on some infinite sequences, such that

$$U((t_{k,\ell})_{\ell\geq 1}) = e^{2i\pi\alpha y_k}(t_{k,\ell})_{\ell\geq 1}.$$

Definition of the random space

Definition

The space $\mathcal{E}$ is the random vector subspace of $\mathbb{C}^\infty$, generated by the sequences $(t_{k,\ell})_{\ell\geq 1}$, or equivalently, $(g_{k,\ell})_{\ell\geq 1}$, for $k \in \mathbb{Z}$. For $\alpha \in \mathbb{R}$, the operator U^α is the unique linear application from $\mathcal{E}$ to $\mathcal{E}$ such that for all $k \in \mathbb{Z}$,

$$U^\alpha((t_{k,\ell})_{\ell\geq 1}) = e^{2i\pi\alpha y_k}(t_{k,\ell})_{\ell\geq 1},$$

or equivalently,

$$U^\alpha((g_{k,\ell})_{\ell\geq 1}) = e^{2i\pi\alpha y_k}(g_{k,\ell})_{\ell\geq 1}.$$

- The notation U^α is motivated by the immediate fact that $(U^\alpha)_{\alpha\in\mathbb{R}}$ is a flow of operators on $\mathcal{E}$, i.e. $U^0 = I_{\mathcal{E}}$ and $U^{\alpha+\beta} = U^\alpha U^\beta$ for all $\alpha, \beta \in \mathbb{R}$.

Theorem (Maples, Najnudel, N)

Almost surely, for any sequence $(s_\ell)_{\ell\geq 1}$ in $\mathcal{E}$ and for all integers $m \geq 1$,

$$[u_n^{\alpha_n}((s_\ell)_{1\leq\ell\leq n})]_m \underset{n\to\infty}{\longrightarrow} [U^{\alpha}((s_\ell)_{\ell\geq 1})]_m \,,$$

where $[\cdot]_m$ denotes the mth coordinate of a vector or a sequence.

Theorem

Let $\epsilon > 0$. Almost surely, for all $k \in \mathbb{Z}$, we have the following.

1. The euclidian norm $\|g_k[n]\|$ is equivalent to a strictly positive random variable times $\sqrt{n}$, when n goes to infinity.
2. $\|g_k[n] - g_k^{(n)}\| = O_\epsilon(n^{\frac{1}{3}+\epsilon})$.
3. For any $T > 0$ and $\delta \in (0, 1/6)$,

$$\sup_{\alpha \in [-T,T]} \sup_{\alpha_n \in [n(\alpha - n^{-\delta}), n(\alpha + n^{-\delta})]} \|u_n^{\alpha_n} g_k[n] - e^{2\pi i \alpha y_k} g_k[n]\| = O(n^{\frac{1}{2}-\delta}).$$

Theorem

Almost surely, for all $k \in \mathbb{Z}$, $\ell \geq 1$, $\alpha, \gamma \in \mathbb{R}$, and for all sequences $(\alpha_n)_{n\geq 1}$ and $(\gamma_n)_{n\geq 1}$ such that $\alpha_n/n = \alpha + o(n^{-\delta})$ and $\gamma_n/n = \gamma + o(n^{-\delta})$ for some $\delta \in [0, 1/6)$,

$$\langle u_n^{\alpha_n}(g_k[n]) - e^{2\pi i \alpha y_k} g_k[n], u_n^{\gamma_n}(e_\ell)\rangle = o(n^{-\delta}),$$

when n goes to infinity. Moreover, for $\delta \in (0, 1/6)$, we get the uniform estimate:

$$\sup_{\substack{\alpha_n \in [n(\alpha - n^{-\delta}), n(\alpha + n^{-\delta})] \\ \gamma_n \in [n(\gamma - n^{-\delta}), n(\gamma + n^{-\delta})]}} \langle u_n^{\alpha_n}(g_k[n]) - e^{2\pi i \alpha y_k} g_k[n], u_n^{\gamma_n}(e_\ell)\rangle = O(n^{-\delta}).$$

- We can naturally define an inner product $\langle \cdot, \cdot \rangle$ on $\mathcal{E}$, by saying that the vectors $(t_{k,\ell})_{\ell \geq 1}$, $k \in \mathbb{Z}$ have norm 1 and are pairwise orthogonal. Note that this construction does not depend on the phase of $(t_{k,\ell})_{\ell \geq 1}$ for $k \in \mathbb{Z}$, so it is almost surely well-defined. From this point on, we assume that the phases are chosen in such a way that $(t_{k,\ell})_{\ell \geq 1, k \in \mathbb{Z}}$ are iid, complex gaussian. Then, the scalar product on $\mathcal{E}$ can almost surely be written as a function of the coordinates of the sequences:

Proposition

Let $(w_\ell)_{\ell \geq 1}$ and $(w'_\ell)_{\ell \geq 1}$ be two vectors in $\mathcal{E}$. Then

$$\langle w, w' \rangle = \lim_{n \to \infty} \frac{1}{n} \sum_{\ell=1}^{n} w_\ell \overline{w'_\ell} = \lim_{s \to 1, s < 1} (1 - s) \sum_{\ell=1}^{\infty} s^{\ell-1} w_\ell \overline{w'_\ell}.$$

- For $\delta > 0$, let $\mathcal{E}_\delta$ be given by combinations (λ_k) such that

$$\sum_{k\in\mathbb{Z}}(1+|k|^{1+\delta})|\lambda_k|^2 < \infty.$$

Indeed, under this assumption, for all $\ell \geq 1$, by Cauchy-Schwarz

$$\sum_{k\in\mathbb{Z}}|\lambda_k t_{k,\ell}| \leq \left(\sum_{k\in\mathbb{Z}}(1+|k|^{1+\delta})|\lambda_k|^2\right)^{1/2}\left(\sum_{k\in\mathbb{Z}}\frac{|t_{k,\ell}|^2}{1+|k|^{1+\delta}}\right)^{1/2}. \quad (1)$$

The first factor is finite from the definition of $\mathcal{E}_\delta$ and the second factor is almost surely finite, since

$$\mathbb{E}\left[\sum_{k\in\mathbb{Z}}\frac{|t_{k,\ell}|^2}{1+|k|^{1+\delta}}\right] = \sum_{k\in\mathbb{Z}}\frac{1}{1+|k|^{1+\delta}} < \infty.$$

Proposition

Let w and w' be two sequences in $\mathcal{E}_\delta$, such that

$$w_\ell = \sum_{k \in \mathbb{Z}} \lambda_k t_{k,\ell}, \; w'_\ell = \sum_{k \in \mathbb{Z}} \lambda'_k t_{k,\ell},$$

where

$$\sum_{k \in \mathbb{Z}} (1 + |k|^{1+\delta})(|\lambda_k|^2 + |\lambda'_k|^2) < \infty \tag{2}$$

Then, for

$$\langle w, w' \rangle := \sum_{k \in \mathbb{Z}} \lambda_k \overline{\lambda'_k},$$

the conclusion of the previous Proposition holds.

Proposition (Chhaibi, Najnudel, N)

Almost surely:

$$y_k^{(n)} \equiv \frac{n}{2\pi}\theta_k^{(n)} = k + O\left(\log(2+|k|)\right)$$

This comes from the fact (plus all information about the characteristic polynomial) that if $k \in \mathbb{Z}$, and if $\varepsilon > 0$ is small enough so that there are no eigenangles of U_n in $[0, \varepsilon]$ and $(\theta_k^{(n)}, \theta_k^{(n)} + \varepsilon]$, then:

$$k = y_k^{(n)} - \frac{1}{\pi}\mathfrak{Im}\left(\log\left(Z_n(e^{i(\theta_k^{(n)}+\varepsilon)})\right) - \log\left(Z_n(e^{i\varepsilon})\right)\right)$$

Theorem (Chhaibi, Najnudel, N)

Almost surely and uniformly on compact subsets of $\mathbb{C}$, we have the convergence:

$$\xi_n(z) \overset{n\to\infty}{\longrightarrow} \xi_\infty(z) := e^{i\pi z} \prod_{k\in\mathbb{Z}} \left(1 - \frac{z}{y_k}\right)$$

Here, the infinite product is not absolutely convergent. It has to be understood as the limit of the following product, obtained by regrouping the factors two by two:

$$\left(1 - \frac{z}{y_0}\right) \prod_{k\geq 1} \left[\left(1 - \frac{z}{y_k}\right)\left(1 - \frac{z}{y_{-k}}\right)\right],$$

which is absolutely convergent.

Proposition (Chhaibi, Najnudel, N)

Almost surely, ξ_∞ is of order 1. More precisely, the exists a.s. a random $C > 0$, such that for all $z \in \mathbb{C}$.

$$|\xi_\infty(z)| \leq e^{C|z|\log(2+|z|)}.$$

On the other hand, there exists a.s. a random $c > 0$ such that for all $x \in \mathbb{R}$,

$$|\xi_\infty(ix)| \geq ce^{c|x|}.$$

From Central to local limit theorems

Theorem

Let $(X_k)_{k\geq 1}$ be symmetric i.i.d. random variables which are non-lattice. Assume that there exists a sequence $(b_n)_{n\geq 1}$ such that $b_n \to \infty$ and as $n \to \infty$

$$\frac{X_1 + \cdots + X_n}{b_n} \to \mu \quad \text{in law}$$

where μ is a probability distribution whose c.f. is given by $\exp(-|t|^p)$ for some $0 < p \leq 2$. Then for every Borel bounded set B whose boundary has Lebesgue measure 0 we have

$$\lim_{n\to\infty} b_n \mathbb{P}(X_1 + \cdots X_n \in B) = c_p \lambda(B)$$

where λ is the Lebesgue measure and $c_p = \frac{1}{2\pi} \int \exp(-|t|^p) dt$.

Modϕ Convergence

Let μ be a probability measure on $\mathbb{R}^d$ with c.f. ϕ. Let X_n be random vector with values in $\mathbb{R}^d$ with c.f. φ_n. We say that there is mod-ϕ convergence if there exists $A_n \in GL_d(\mathbb{R})$ such that:

- (H1) ϕ is integrable;
- (H2) Denoting $\Sigma_n = A_n^{-1}$, we have $\Sigma_n \to 0$ and the vectors $Y_n = \Sigma_n X_n$ converge in law to μ.
- (H3) For all $k \geq 0$, we have

$$\sup_{n\geq 1} \int_{|t|\geq a} |\varphi_n(\Sigma_n^* t)| \mathbf{1}_{|\Sigma_n^* t| \leq k} dt \to 0 \quad \text{as } a \to \infty.$$

Theorem (Delbaen, Kowalski, N)

Suppose that mod-ϕ convergence holds for (X_n). Then for all continuous functions with compact support, we have:

$$\det(A_n)\mathbb{E}[f(X_n)] \to \frac{d\mu}{d\lambda}(0)\int f d\lambda.$$

Consequently for all relatively compact Borel set B with boundary of Lebesgue measure 0,

$$\det(A_n)\mathbb{P}(X_n \in B) \to \frac{d\mu}{d\lambda}(0)\lambda(B).$$

Link with mod-Gaussian Convergence

Proposition

If (H1) holds and if there exists a continuous function $\psi : \mathbb{R}^d \to \mathbb{C}$ such that

$$\varphi_n(t) = \psi(t)\phi(A_n^* t)(1 + o(1))$$

uniformly for $|\Sigma_n^* t| \leq k$ for $k > 0$, then we have mod-ϕ convergence.

Useful Lemma

Lemma

Suppose $f : \mathbb{R}^d \to \mathbb{R}$ is a continuous function with compact support. Then for each $\eta > 0$ we can find two integrable functions g_1, g_2 such that

(i) $\hat{g}_1$ and $\hat{g}_2$ have compact support;

(ii) $g_2 \leq f \leq g_1$,

(iii) $\int_{\mathbb{R}^d} (g_1 - g_2)(t) dt \leq \eta$.

Sketch of the proof of the Theorem

We can assume that f is continuous, integrable with $\hat{f}$ having compact support. We write

$$\mathbb{E}[f(X_n)] = \int_{\mathbb{R}^d} f(x) d\mu_n(x) = \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} \varphi_n(t)\hat{f}(-t)dt.$$

Change of variables:

$$\mathbb{E}[f(X_n)] = (2\pi)^{-d} |\det \Sigma_n| \int_{|\Sigma_n^* s| \leq k} \varphi_n(\Sigma_n^* s)\hat{f}(-\Sigma_n^* s)dt.$$

The integrand converges piecewise to $\varphi(s)\hat{f}(0)$.

The Winding Number of the Complex Brownian Motion

Let $(W_t)_{t\geq 0}$ be a complex BM starting at 1. Let $(\theta_t)_{t\geq 0}$ be the argument of W, starting at 0 and defined by continuity. Spitzer theorem asserts that

$$\frac{2\theta_t}{\log t} \to \mathcal{C}$$

where the convergence is in law and where $\mathcal{C}$ stands for a random variable with the Cauchy distribution with density $\dfrac{1}{\pi}\dfrac{dx}{1+x^2}$.

Theorem

We have the following local limit theorem for the winding number:

$$\frac{\log t}{2}\mathbb{P}(\theta_t \in (a, b)) \to \frac{b-a}{\pi}.$$

This is a situation where we are in the stronger mod-Cauchy convergence situation with an explicitly computable limiting function involving Bessel functions.

Random Matrices

Theorem

For B a suitable Borel set of $\mathbb{C}$,

$$\mathbb{P}(P_n \in B) \sim \frac{1}{\pi \log n}\lambda(B).$$

Conjecture for the Riemann zeta function

Conjecture

For any suitable Borel subset of $\mathbb{C}$, we have:

$$\lim_{T\to\infty} \frac{1/2\log\log T}{T}\lambda\{t\in[0,T] \mid \log\zeta(1/2+it)\in B\} = \frac{\lambda(B)}{2\pi}.$$

This conjecture is true if for instance one can show that for all $k>0$, there exists $C_k>0$ such that

$$\left|\frac{1}{T}\int_0^T \exp\left(it.\log\zeta(1/2+iu)\right)du\right| \leq \frac{C_k}{1+|t|^4(\log\log T)^2}$$

for all $T\geq 1$ and $|t|\leq k$.

Theorem [Kowalski-N]

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

For L-functions of hyper elliptic curves we have:

Theorem [Kowalski-N]

Let $\mathcal{H}_g(\mathbb{F}_q)$ be the set of square free, monic, polynomials of degree $2g+1$ in $\mathbb{F}_q[X]$. Fix a non-empty open interval $(\alpha, \beta) \subset (0, \infty)$. For all g large enough we have

$$\liminf_{q \to \infty} \frac{1}{|\mathcal{H}_g(\mathbb{F}_q)|} \left| \left\{ f \in \mathcal{H}_g(\mathbb{F}_q), \frac{L(C_f, 1/2)}{\sqrt{\pi g/2}} \in (\alpha, \beta) \right\} \right| >> \frac{1}{\sqrt{\log g}}.$$