Probabilistic aspects in random matrix theory and analytic number theory

Ashkan Nikeghbali
University of Zurich

The random matrix model

- The unitary group with the Haar measure;
- Eigenvalues on the unit circle;
- Weyl's integration formula

Dyson

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

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

Why the unitary group?

- The sine kernel has some universal feature; so is there really something about zeta?
- The results 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

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

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?
- 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;
- Set the framework for the construction of the operator;
- prove the following: for $u \in U(n)$ Haar distributed, we have the following identity in law

$$\det(I - u) = \prod_{k=1}^{n} \left(1 + e^{i\theta_k} \sqrt{\beta_{1,k-1}}\right)$$

where are random variables in sight are independent.

How does it work?

- How to generate inductively the Haar measure?
- How to generate the uniform distribution on the unit sphere?
- How does it work with permutations?

Complex Reflections

- We endow $\mathbb{C}^n$ with the scalar product: $x \cdot y = \sum_{k=1}^{n} x_k \bar{y}_k$.
- 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:

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

  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

$$r(x) = x - \frac{x \cdot (m-e)}{1 - e \cdot m}(m-e).$$

Virtual isometries

Theorem [Bourgade-Najnudel-N]

Let $(x_n)_{n\geq 1}$ be a sequence of vectors, $x_n \in \mathbb{C}^n$ and $||x|| = 1$. There exists a unique sequence of unitary transformations $(u_n)_{n\geq 1}$, with $u_n \in U(n)$, such that $u_n(e_n) = x_n$ and

$$u_n = r_n.r_{n-1}...r_1$$

where for $j \in \{1, ..., n\}$, $r_j = Id$ if $x_j = e_j$ and otherwise r_j is the unique reflection such that $r_j(e_j) = x_j$.
Such a sequence is called a virtual isometry and the space of all virtual isometries is noted U^∞.

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 $\mathbb{C}^n$).

Strong Convergence

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 polynomials

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

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

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,

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

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 $\frac{1}{\pi}\frac{dx}{1+x^2}$.

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

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

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