(Number Theory Days, Basel, 10/11/23)

FIXED-POINT STATISTICS FROM SPECTRAL MEASURES

(joint with A. Frey & E. Kowalski)

① Two theorems

Theorem 1 ("The problem of coincidences", Montmort 1713)

For each integer $k \geq 0$,

$$\lim_{n\to\infty} \frac{|\{\sigma \in S_n \mid |\mathrm{Fix}(\sigma)| = k\}|}{n!} = \frac{1}{e}\cdot\frac{1}{k!}.$$

Theorem 2 ("Deligne's equidistribution theorem", 1980)

Consider the family of elliptic curves

$$E_t : y^2 = x^3 + x + t$$

For a finite field F, $|E_t(F)| = |F| - a(t)$ with $|a(t)| \leq 2\sqrt{|F|}$ (Hasse-Weil). For $-2 \leq \alpha < \beta \leq 2$,

$$\lim_{n\to\infty} \frac{\left|\left\{t \in \mathbb{F}_{p^n} \;\middle|\; \frac{a(t)}{p^n} \in [\alpha,\beta]\right\}\right|}{p^n} = \int_\alpha^\beta \mu_{ST},$$

where μ_{ST} is the measure on $[-2,2]$ given by the direct image of the Haar measure on $SU(2)$ by the trace $Tr : SU(2) \to [-2,2]$. Explicitly,

$$\mu_{ST}(x) = \frac{1}{2\pi}\sqrt{4-x^2}\,dx.$$

- The proof of Theorem 1 is very easy: D_n for "derangement"

$$\left|\{\sigma \in S_n \mid |\mathrm{Fix}(\sigma)| = k\}\right| = \binom{n}{k} \cdot D_{n-k}$$

where $D_m = \{\sigma \in S_m \mid \mathrm{Fix}(\sigma) = \emptyset\}$. This we is computed by inclusion-exclusion as

$$D_m = m! \sum_{j=0}^{m} \frac{(-1)^j}{j!}$$

S_i fixes i

$$D_m = m! - |S_1 \cup \cdots \cup S_m| = m! - \sum_i |S_i| + \sum_{i<j} |S_i \cap S_j| - \cdots$$

So the quotity we want is

$$\frac{1}{n!} \frac{n!}{k!\,(n-k)!} (n-k)! \sum_{j=0}^{} \frac{(-1)^j}{j!}$$

which has limit $\frac{1}{k!}\frac{1}{e}$ as $n \to \infty$ $= m! - \binom{m}{1}(m-1)! + \binom{m}{2}(m-2)! - \cdots$

- The proof of Theorem 2 is less easy. It has two parts:

(1) "Abstract": here the measure μ_{ST} appears

(2) Riemann hypothesis over finite fields

A key point in the abstract part is to control the top degree cohology with compact support

$$H_c^{2d}(X_{\bar{F}}, \mathcal{L})$$

of an ℓ-adic local system $\mathcal{L}$ on a variety over a finite field $\rho : \pi_1(X_{\bar{F}}) \to GL(V)$ ↑ vector space over $\bar{\mathbb{Q}}_\ell$

$$\dim_{\bar{\mathbb{Q}}_\ell} H_c^{2d}(X_{\bar{F}}, \mathcal{L}) = \dim_{\bar{\mathbb{Q}}_\ell} (\rho_{\pi_1(X_{\bar{F}})})^{\pi_1} \geq 0$$

Σ coinvts

If ρ is semi-simple

$$\downarrow$$

$$= \dim_{\bar{\mathbb{Q}}_\ell}\left(\rho^{\pi_1(X_{\bar{F}})}\right) \quad \text{invariants}$$

$$= \dim_{\bar{\mathbb{Q}}_\ell}\left(V^{G}\right) \qquad G = \text{Zariski closure of } \rho(\pi_1(X_{\bar{F}}))$$

$$= \dim_{\mathbb{C}}\left(V_{\mathbb{C}}^{K}\right) \qquad K \subset G(\mathbb{C}) \text{ maximal compact}$$

unitary trick →

$$= \int_K \mathrm{Tr}(\rho(g))\, d\mu_{\mathrm{Haar}}.$$

$$= \int_{\mathbb{C}} \mathrm{Tr}_* \mu_{\mathrm{Haar}}.$$

More generally, setting $i(M) = \dim H_c^{2d}(X_{\bar{F}}, M)$

we get the formula

$$i\left(M^{\otimes a} \otimes (M^\vee)^{\otimes b}\right) = \int_{\mathbb{C}} z^a \bar{z}^b \, \mathrm{Tr}_* \mu_{\mathrm{Haar}}$$

for all integers $a, b \geq 0$.

② Spectral measures

$\mathcal{C}$ a category, $\otimes$, $D: \mathcal{C} \to \mathcal{C}$

$i: \mathrm{Ob}(\mathcal{C}) \to \mathbb{C}$ "invariant"

Inspired by notion in factorization algebras

Definition: Let M be an object of $\mathcal{C}$. A positive measure μ on $\mathbb{C}$ is called a spectral measure of M relative to i if

$$i\left(M^{\otimes a} \otimes (M^\vee)^{\otimes b}\right) = \int_{\mathbb{C}} z^a \bar{z}^b \mu \quad \text{for all } a, b \geq 0$$

This may or not exist, may or not be unique: classical question whether a measure is determined by its moments.

Lemma: If $i(M \otimes D(N)) + i(D(M) \otimes N) \leq i(M \otimes D(M)) + i(N \otimes D(N))$ (*)

and $\sum_{n \geq 1} i\left(\left(M \otimes D(M)\right)^{\otimes n}\right)^{-1/2n} = +\infty$

then μ exists and is unique. ← Carleman criterion

(*) holds e.g. if $\mathcal{C}$ is semi-simple with unit object $\mathbb{1}$, κ-linear and $i(M) = \dim_\kappa \mathrm{Hom}(\mathbb{1}, M)$.

③ A new proof of Theorem 1

Statement: $(X_n)_{n \geq 0}$ sequence of random variables uniformly distributed on S_n

$$|\mathrm{Fix}(X_n)| \xrightarrow[\text{law}]{n \to \infty} P_1$$ ← Poisson distribution with parameter 1

$$\nu_1(\{k\}) = \frac{1}{e} \cdot \frac{1}{k!}$$

- We use the method of moments, which says that it suffices to prove: for each $k \geq 0$ (stated in non-negative integers)

$$\frac{1}{n!} \sum_{\sigma \in S_n} |\mathrm{Fix}(\sigma)|^k \longrightarrow \mathbb{E}(P_1^k)$$

$$\frac{1}{e} \sum_{l=0}^{\infty} \frac{l^k}{l!}$$

From representation theory of finite groups:

$$\frac{1}{n!}\sum_{\sigma\in S_n}|\mathrm{Fix}(\sigma)|^k = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathrm{Rep}(S_n)}(\mathbb{1}_S, \mathrm{Std}^{\otimes k})$$

where Std is the "standard" representation of S_n on $\mathbb{C}^n$, e.g. σ acts by permutation matrices.

- Now, Deligne–Knop have defined a category

$\underline{\mathrm{Rep}(S_t)}$ for t a complex number

which is semisimple if $t \notin \mathbb{Z}_{\geq 0}$ and for $t = n$ satisfies:

$$\mathrm{Rep}(S_t)/\mathcal{N} \xrightarrow{\sim} \mathrm{Rep}(S_n)$$
$$[X] \longmapsto \{1,\dots,n\}^{\times} \circlearrowright S_n$$

Basic objects: $[X]$ for X a finite set

$$\mathrm{Hom}_{\mathbb{C}}([X],[Y]) = \mathbb{C}\cdot[\text{partitions of } X \amalg Y]$$

unit object: $\mathbb{1}_t = [\emptyset]$

standard representation: $\mathrm{Std}_t = [\{1\}]$

$\otimes$-product: $\mathrm{Std}_t^{\otimes k} = [\{1,\dots,k\}]$

Define $\quad i(M) = \dim_{\mathbb{C}} \mathrm{Hom}_{\underline{\mathrm{Rep}(S_t)}}(\mathbb{1}_t, M)$

Then

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\underline{\mathrm{Rep}}(S_t)}(\mathbb{1}_t, \mathrm{std}_t^{\otimes k})$$

$$= \text{number of partitions of the set } \{1,\dots,k\} \quad \leq k^k \quad \text{(Bell number)}$$

Some recurrence relation: $a_{k+1} = \sum_{j=0}^{k} \binom{k}{j} a_j$

$$= \mathbb{E}(p_1^k) \quad \text{Carleman} \geq \sum \frac{1}{(2k)^{2k/2k}} = +\infty .$$

Dolinski's formula

so std_t has spectral measure the Poisson distribution

- To conclude, we prove that:

$$\dim \mathrm{Hom}_{\mathrm{Rep}(S_n)}(\mathbb{1}_n, \mathrm{std}^{\otimes k}) \leq \dim \mathrm{Hom}_{\underline{\mathrm{Rep}}(S_t)}(\mathbb{1}_t, \mathrm{std}_t^{\otimes k})$$

with equality if and only if $k \leq n$.

(This is because in the semi-simplification we quotient morphisms by $N([x],[y]) = \{f : [x] \to [y] \mid \mathrm{Tr}(fg) = 0 \text{ for all } g : [y] \to [x]\}$ — "tensor radical" —

and we know when it is empty)

$$\mathrm{Tr} : \mathbb{1} \to [x] \otimes [x]^\vee \xrightarrow{\beta \otimes \mathrm{id}} [x] \otimes [x]^\vee \simeq [x]^\vee \otimes [x] \to \mathbb{1} \in \mathrm{End}(\mathbb{1})$$

Hence: $\lim_{n\to\infty} \dim \mathrm{Hom}_{\mathrm{Rep}(S_n)}(\mathbb{1}_n, \mathrm{std}^{\otimes k}) = \mathbb{E}(p_1^k)$. □

Remark:

This can be generalize to $\underline{\mathrm{Rep}}(GL_t(\mathbb{F}_q))$,

$\underline{\mathrm{Rep}}(\mathrm{Aff}_t(\mathbb{F}_q))$, ... or to other objects of

$\underline{\mathrm{Rep}}(S_t)$ to obtain new fixed-point statistics results.

Also, $\mathrm{Tr}^u_{\mathrm{Haar}, SU_n} \xrightarrow[n\to\infty]{*}$ complex Gaussian

(4) A Chebotarev theorem for pseudo-polynomials

Let $f \in \mathbb{Z}[T]$ be a polynomial of degree n with Galois group S_n. For each prime p, let

$$\rho_f(p) = \text{number of roots of } f \bmod p \text{ in } \mathbb{F}_p$$

It follows from Chebotarev's theorem that:

$$\lim_{X \to \infty} \frac{|\{p \le X \mid \rho_f(p) = k\}|}{\pi(X)} = \mathbb{P}(|\mathrm{Fix}(X_n)| = k)$$

Kronecker 1880

(Reason: $z \mapsto z^p$ permutes the set of roots of f in $\overline{\mathbb{F}_p}$ and Chebotarev says that $(\sigma_p)_{p \le X} \to \sigma$ uniformly distributed as $X \to +\infty$.)

- Is there something similar for $\mathrm{Rep}(S_t)$?

Definition. A pseudo-polynomial is a sequence $(a_n)_{n \ge 0}$ of integers such that $m - n \mid a_m - a_n$ for all $m > n \ge 0$.

e.g. $a_n = P(n)$ for $P \in \mathbb{Z}[T]$

$a_n = \lfloor e\, n! \rfloor = n! \sum_{m=0}^{n} \frac{1}{m!}$ is a pseudo-polynomial that doesn't come from a polynomial (exponential growth).

- The function $\mathbb{Z} \to \overline{\mathbb{Z}}$, $n \mapsto a_n$ has a well-defined reduction modulo p, so we can speak of the zeros mod p of a pseudopolynomial.

Conjecture (Knuth–Sundaram)

$F(n) = \lfloor e\, n! \rfloor$

$$\lim_{X \to \infty} \frac{\left| \{ p \le X \mid \rho_F(p) = \kappa \} \right|}{\pi(X)} = \frac{1}{e}\,\frac{1}{\kappa!}$$

Q: Does F have "Galois group" S_t? (t an indeterminate)

- Exponential sums

$f \in \mathbb{Z}[T]$ of $\deg_{\mathbb{Q}} f \ge 6$, f' Galois group S_{n-1}

$$W_f(a;p) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \exp\left(\frac{2\pi i}{p}\, a f(x) \right)$$

Deligne–Katz: $(W_f(a;p))_{a \in \mathbb{F}_p^\times}$ equidistributed for $\mathrm{Tr}_*\mu_{\mathrm{Haar},K}$ as $p \to \infty$, $SU_n \subset K \subset U_n$.

Conjecture:

(Len!) as before: $(W_F(a;p))_{a \in \mathbb{F}_p^\times}$ equidistributed like a complex gaussian: $\lim_{p \to \infty} \frac{1}{p-1} \sum_{a \in \mathbb{F}_p^\times} \varphi(W_F(a;p)) = \frac{1}{\pi} \int_{\mathbb{C}} \varphi(z)\, e^{-|z|^2}\, dz$ for all bounded continuous $\varphi : \mathbb{C} \to \mathbb{C}$.