Asymptotics, exact results, and analogies in p-adic random matrix theory

Roger Van Peski

PhD defense talk June 8, 2023

Aperitif

Let A_1, \ldots, A_{τ} be iid uniform in $Mat_N(\mathbb{Z}/p\mathbb{Z})$. What does the distribution of

$$\operatorname{rank}(A_{\tau}\cdots A_2A_1)$$

look like for large N and τ ?

Aperitif

Let A_1, \ldots, A_{τ} be iid uniform in $Mat_N(\mathbb{Z}/p\mathbb{Z})$. What does the distribution of

$$\operatorname{rank}(A_{\tau}\cdots A_2A_1)$$

look like for large N and τ ?



Aperitif

Let A_1, \ldots, A_τ be iid uniform in $Mat_N(\mathbb{Z}/p\mathbb{Z})$. What does the distribution of

$$\operatorname{rank}(A_{\tau}\cdots A_2A_1)$$

look like for large N and τ ?



Fact: $\operatorname{corank}(A_{\tau} \cdots A_{1}) \approx \log_{p} \tau$, finite limit fluctuations.

An intriguing random integer

Theorem (VP '23, special case)

For each $N \ge 1$ take A_1, A_2, \ldots iid uniform in $Mat_N(\mathbb{Z}/p\mathbb{Z})$. Then as $N \to \infty$,

$$\operatorname{corank}(A_{\tau_N}\cdots A_1) - \log_p \tau_N - \alpha \xrightarrow{d} \mathcal{L}_{1,p^{-\alpha}/(p-1)}$$

(an explicit \mathbb{Z} -valued random variable), for any sequence $\tau_N, N \ge 1$ s.t. $1 \ll \tau_N \ll p^N$ and $-\log_p \tau_N$ converges in \mathbb{R}/\mathbb{Z} to some $\alpha \in [0, 1)$.

An intriguing random integer

Theorem (VP '23, special case)

For each $N \ge 1$ take A_1, A_2, \ldots iid uniform in $Mat_N(\mathbb{Z}/p\mathbb{Z})$. Then as $N \to \infty$,

$$\operatorname{corank}(A_{\tau_N}\cdots A_1) - \log_p \tau_N - \alpha \xrightarrow{d} \mathcal{L}_{1,p^{-\alpha}/(p-1)}$$

(an explicit \mathbb{Z} -valued random variable), for any sequence $\tau_N, N \ge 1$ s.t. $1 \ll \tau_N \ll p^N$ and $-\log_p \tau_N$ converges in \mathbb{R}/\mathbb{Z} to some $\alpha \in [0, 1)$.

Here for any $\chi \in \mathbb{R}_{>0}$, $\mathcal{L}_{1,\chi}$ is the \mathbb{Z} -valued r.v. defined by

$$\Pr(\mathcal{L}_{1,\chi} = x) = \frac{1}{\prod_{i \ge 1} (1 - p^{-i})} \sum_{j \ge 0} e^{-\chi p^{j-x}} \frac{(-1)^j p^{-\binom{j}{2}}}{\prod_{i=1}^j (1 - p^{-i})}$$

for any $x \in \mathbb{Z}$.

Random matrices in physics and number theory

Perhaps I am now too courageous when I try to guess the distribution of the distances between successive levels (of energies of heavy nuclei). Theoretically, the situation is quite simple if one attacks the problem in a simpleminded fashion. The question is simply what are the distances of the characteristic values of a symmetric matrix with random coefficients.

Eugene Wigner on the Wigner surmise, 1956







Local spacings since proven **universal** for many different choices of matrix distribution (Erdos-Yau, Tao-Vu, Pastur-Scherbina...)

(From Bohigas-Giannoni, Chaotic motion and random matrix theories)

1983: Cohen and Lenstra consider class groups of number fields $\mathbb{Q}(\sqrt{-d})$ for many d, and conjecture¹ that their p-parts follow the *Cohen-Lenstra distribution* on finite abelian p-groups defined by

$$\Pr(G) = \frac{\prod_{i \ge 1} (1 - 1/p^i)}{|\operatorname{Aut}(G)|}.$$

¹Based on data from D. Buell, C. P. Schnorr, D. Shanks, and H. Williams.

1983: Cohen and Lenstra consider class groups of number fields $\mathbb{Q}(\sqrt{-d})$ for many d, and conjecture¹ that their p-parts follow the *Cohen-Lenstra distribution* on finite abelian p-groups defined by

$$\Pr(G) = \frac{\prod_{i \ge 1} (1 - 1/p^i)}{|\operatorname{Aut}(G)|}.$$

4. Note. The data which form the output of the group computation currently exist online on the ' omputer Science Department's VAX computer. The author is willing to respond to limited requests from interested parties, or to provide copies of the data if supplied with a magnetic tape.

(from D. Buell, *Class Groups of Quadratic Fields. II*, 1987)

¹Based on data from D. Buell, C. P. Schnorr, D. Shanks, and H. Williams.

 $A \in \operatorname{Mat}_N(\mathbb{Z})$ is a linear map $A : \mathbb{Z}^N \to \mathbb{Z}^N$,

 $\operatorname{coker}(A) := \mathbb{Z}^N / A \mathbb{Z}^N.$

 $A \in \operatorname{Mat}_N(\mathbb{Z})$ is a linear map $A : \mathbb{Z}^N \to \mathbb{Z}^N$,

$$\operatorname{coker}(A) := \mathbb{Z}^N / A \mathbb{Z}^N.$$

For random A, coker(A) is a random abelian group.

 $A \in \operatorname{Mat}_N(\mathbb{Z})$ is a linear map $A : \mathbb{Z}^N \to \mathbb{Z}^N$,

$$\operatorname{coker}(A) := \mathbb{Z}^N / A \mathbb{Z}^N.$$

For random A, $\operatorname{coker}(A)$ is a random abelian group. Simpler: take $A \in \operatorname{Mat}_N(\mathbb{Z}_p)$ so $\operatorname{coker}(A)$ is an abelian *p*-group.

 $A \in \operatorname{Mat}_N(\mathbb{Z})$ is a linear map $A : \mathbb{Z}^N \to \mathbb{Z}^N$,

$$\operatorname{coker}(A) := \mathbb{Z}^N / A \mathbb{Z}^N.$$

For random A, $\operatorname{coker}(A)$ is a random abelian group. Simpler: take $A \in \operatorname{Mat}_N(\mathbb{Z}_p)$ so $\operatorname{coker}(A)$ is an abelian *p*-group.

Theorem (Friedman-Washington '87)

Let $A^{(N)} \in \operatorname{Mat}_N(\mathbb{Z}_p)$ be random with iid entries drawn from the additive Haar measure on \mathbb{Z}_p . Then as $N \to \infty$, $\operatorname{coker}(A^{(N)})$ limits to Cohen-Lenstra distribution $\Pr(G) = \prod_{i>1} (1-p^{-i})/|\operatorname{Aut}(G)|$.

 $A \in \operatorname{Mat}_N(\mathbb{Z})$ is a linear map $A : \mathbb{Z}^N \to \mathbb{Z}^N$,

$$\operatorname{coker}(A) := \mathbb{Z}^N / A \mathbb{Z}^N.$$

For random A, $\operatorname{coker}(A)$ is a random abelian group. Simpler: take $A \in \operatorname{Mat}_N(\mathbb{Z}_p)$ so $\operatorname{coker}(A)$ is an abelian *p*-group.

Theorem (Friedman-Washington '87)

Let $A^{(N)} \in \operatorname{Mat}_N(\mathbb{Z}_p)$ be random with iid entries drawn from the additive Haar measure on \mathbb{Z}_p . Then as $N \to \infty$, $\operatorname{coker}(A^{(N)})$ limits to Cohen-Lenstra distribution $\Pr(G) = \prod_{i>1} (1 - p^{-i})/|\operatorname{Aut}(G)|$.

Theorem (Wood '15)

Above limit also holds if $A^{(N)}$ have iid entries from any distribution that is nonconstant modulo p (universality).

Groups and singular numbers

Proposition (Smith normal form)

For nonsingular $A \in Mat_N(\mathbb{Q}_p)$, there are $U, V \in GL_N(\mathbb{Z}_p)$ for which

$$UAV = \operatorname{diag}(p^{\lambda_1}, \dots, p^{\lambda_N})$$

for singular numbers $\lambda_i \in \mathbb{Z}$ (unique).

(Like singular value decomposition, $\operatorname{GL}_N(\mathbb{Z}_p)$ replacing O(N), U(N)).

Groups and singular numbers

Proposition (Smith normal form)

For nonsingular $A \in Mat_N(\mathbb{Q}_p)$, there are $U, V \in GL_N(\mathbb{Z}_p)$ for which

$$UAV = \operatorname{diag}(p^{\lambda_1}, \dots, p^{\lambda_N})$$

for singular numbers $\lambda_i \in \mathbb{Z}$ (unique).

(Like singular value decomposition, $\operatorname{GL}_N(\mathbb{Z}_p)$ replacing O(N), U(N)).

If $A \in \operatorname{Mat}_N(\mathbb{Z}_p)$, then $\lambda_i \ge 0$ and

$$\operatorname{coker}(A) \cong \bigoplus_{i} \mathbb{Z}/p^{\lambda_{i}}\mathbb{Z}$$

Groups and singular numbers

Proposition (Smith normal form)

For nonsingular $A \in Mat_N(\mathbb{Q}_p)$, there are $U, V \in GL_N(\mathbb{Z}_p)$ for which

$$UAV = \operatorname{diag}(p^{\lambda_1}, \dots, p^{\lambda_N})$$

for singular numbers $\lambda_i \in \mathbb{Z}$ (unique).

(Like singular value decomposition, $\operatorname{GL}_N(\mathbb{Z}_p)$ replacing O(N), U(N)).

If $A \in \operatorname{Mat}_N(\mathbb{Z}_p)$, then $\lambda_i \ge 0$ and

$$\operatorname{coker}(A) \cong \bigoplus_{i} \mathbb{Z}/p^{\lambda_{i}}\mathbb{Z}$$

Write $SN(A) = (SN(A)_1, \dots, SN(A)_N) := (\lambda_1, \dots, \lambda_N)$ above.

At a probabilistic level things look quite different



Histogram of singular values of a single $10^3 \times 10^4$ Ginibre (iid Gaussian) matrix

Histogram of singular numbers of a single 100×100 iid additive Haar matrix

Can study singular values of $A_{\tau}A_{\tau-1}\cdots A_1$ for A_i random real/complex matrices, $\tau = 1, 2, \ldots$

Can study singular values of $A_{\tau}A_{\tau-1}\cdots A_1$ for A_i random real/complex matrices, $\tau = 1, 2, \ldots$

Interest from ergodic theory (Furstenberg-Kesten 1960 onward), statistical physics (Akemann, Burda, Forrester, Ipsen, Kieburg, Liu, Wang, Wei, and others, 2010s onward), integrable probability (Ahn, Gorin, Strahov, Sun and others, also 2010s onward). Can study singular values of $A_{\tau}A_{\tau-1}\cdots A_1$ for A_i random real/complex matrices, $\tau = 1, 2, \ldots$

Interest from ergodic theory (Furstenberg-Kesten 1960 onward), statistical physics (Akemann, Burda, Forrester, Ipsen, Kieburg, Liu, Wang, Wei, and others, 2010s onward), integrable probability (Ahn, Gorin, Strahov, Sun and others, also 2010s onward).

Question

How do singular numbers of *p*-adic matrix products behave?

Dynamical local limits?



Question

For $r \in (0,1)$, does joint evolution of bulk singular numbers $\lambda_{\lfloor rN \rfloor + i}(\tau), i \in \{\dots, -1, 0, 1, \dots\}$ converge as matrix size $N \to \infty$ to some Markov process on

$$\operatorname{Sig}_{2\infty} := \{ \mu = (\dots, \mu_{-1}, \mu_0, \mu_1, \dots) \in \mathbb{Z}_{\geq 0}^{\mathbb{Z}} : \mu_{i+1} \leq \mu_i \}$$
?



Definition (VP 2023)



Definition (VP 2023)



Definition (VP 2023)



Definition (VP 2023)



Definition (VP 2023)

Universal bulk limit



Theorem (VP 2023, informal version)

The discrete-time evolution of singular numbers of $n \times n$ matrix products $A_{\tau}^{(n)} \cdots A_{1}^{(n)}$ in the bulk limits to the reflecting Poisson sea (with t = 1/p), for any generic $\operatorname{GL}_{n}(\mathbb{Z}_{p})$ -invariant matrix distributions, provided $\operatorname{corank}(A_{i}^{(n)} \pmod{p})$ is not too large.

Remark: at the right edge, have limit to half-infinite version of reflecting Poisson sea.

Comparison to dynamical local limits over $\mathbb C$

Bulk local limits of log singular values of complex matrix products: Brownian motions with drift conditioned never to intersect (highly nonlocal) [Akemann-Burda-Kieburg '20], [Ahn '22]



...while p-adic local limits feature only local interactions at collisions



Explicit fixed-time bulk limit

Hope for $(SN(A_{\tau_N}\cdots A_1)'_i - \log_p \tau_N - \alpha)_{1 \le i \le k}$ to converge to random el't of

$$\operatorname{Sig}_k := \{(\lambda_1, \dots, \lambda_k) \in \mathbb{Z}^k : \lambda_1 \ge \dots \ge \lambda_k\}$$

Explicit fixed-time bulk limit

Hope for $(SN(A_{\tau_N}\cdots A_1)'_i - \log_p \tau_N - \alpha)_{1 \le i \le k}$ to converge to random el't of

$$\operatorname{Sig}_k := \{(\lambda_1, \dots, \lambda_k) \in \mathbb{Z}^k : \lambda_1 \ge \dots \ge \lambda_k\}$$

Theorem (VP '23)

If $\tau_N, N \ge 1$ are such that $1 \ll \tau_N \ll p^N$ and $-\log_p \tau_N$ converges in \mathbb{R}/\mathbb{Z} to some $\alpha \in [0, 1)$, and A_1, \ldots, A_{τ_N} in $\operatorname{Mat}_N(\mathbb{Z}_p)$ iid with additive Haar entries, then as $N \to \infty$

$$(\operatorname{SN}(A_{\tau_N}\cdots A_1)'_i - \log_p \tau_N - \alpha)_{1 \le i \le k} \xrightarrow{d} \mathcal{L}_{k,p^{-\alpha}/(p-1)},$$

an explicit Sig_k -valued random variable.

Explicit fixed-time bulk limit

Hope for $(SN(A_{\tau_N}\cdots A_1)'_i - \log_p \tau_N - \alpha)_{1 \le i \le k}$ to converge to random el't of

$$\operatorname{Sig}_k := \{(\lambda_1, \dots, \lambda_k) \in \mathbb{Z}^k : \lambda_1 \ge \dots \ge \lambda_k\}$$

Theorem (VP '23)

If $\tau_N, N \ge 1$ are such that $1 \ll \tau_N \ll p^N$ and $-\log_p \tau_N$ converges in \mathbb{R}/\mathbb{Z} to some $\alpha \in [0, 1)$, and A_1, \ldots, A_{τ_N} in $\operatorname{Mat}_N(\mathbb{Z}_p)$ iid with additive Haar entries, then as $N \to \infty$

$$(\operatorname{SN}(A_{\tau_N}\cdots A_1)'_i - \log_p \tau_N - \alpha)_{1 \le i \le k} \xrightarrow{d} \mathcal{L}_{k,p^{-\alpha}/(p-1)},$$

an explicit Sig_k -valued random variable.

Holds also for other 'nice' examples, universality likely but harder.

What is $\mathcal{L}_{k,\chi}$?

Example

When k=2 (taking t=1/p), $\chi\in\mathbb{R}_{>0}$, $(L+x,L)\in\mathrm{Sig}_2$,

$$\Pr(\mathcal{L}_{2,\chi} = (L+x,L)) = \frac{t^{\binom{x}{2}}}{(t;t)_{\infty}} \sum_{m \ge 0} e^{-t^{L-m}\chi} \times (-1)^m t^{m^2 + (x-1)m} \sum_{i=0}^x \frac{(-1)^{x-i}}{(t;t)_{x-i}} {m+i \brack i}_t \times \left(\frac{(t^{L-m}\chi)^{i+m}}{(i+m)!} + \frac{(t^{L-m}\chi)^{i+m-1}\mathbb{1}(i+m\ge 1)}{(i+m-1)!}\right)$$

where

$$(a;t)_n := (1-a)(1-ta)\cdots(1-t^{n-1}a) \text{ and } \begin{bmatrix} a\\b \end{bmatrix}_t := \frac{(t;t)_a}{(t;t)_b(t;t)_{a-b}}$$

But really, what is $\mathcal{L}_{k,\chi}$?

Definition (VP 2023) For $(L_1, \ldots, L_k) \in \operatorname{Sig}_k$, $\Pr(\mathcal{L}_{k,\chi} = (L_1, \dots, L_k)) := \sum_{d \le L_k} \frac{e^{-\chi t^d} t^{\sum_{i=1}^k {\binom{L_i - d}{2}}}}{(t; t)_{L_k - d} \prod_{i=1}^{k-1} (t; t)_{L_i - L_{i+1}}}$ $\times \frac{1}{(t;t)_{\infty}} \sum_{\mu \in \operatorname{Sig}_{k-1}} (-1)^{\sum_{i=1}^{k} L_i - \sum_{i=1}^{k-1} \mu_i - d} \prod_{i=1}^{k-1} \begin{bmatrix} L_i - L_{i+1} \\ L_i - \mu_i \end{bmatrix}_{t}$ $L_1 > \mu_1 > L_2 > \mu_2 > \dots$ $\times Q_{(\mu_1 - d, \dots, \mu_{k-1} - d)'}(\gamma(\chi(1 - t)t^d), \alpha(1); 0, t)$

where again t = 1/p and last term is a Hall-Littlewood polynomial specialized with α and Plancherel parameters 1 and $\chi(1-t)t^d$.

Macdonald processes [Borodin-Corwin '11]

Macdonald polynomials $P_{\lambda}(x_1, \ldots, x_n; q, t)$ indexed by integer partitions $\lambda = (\lambda_1 \ge \ldots \ge \lambda_n \ge 0)$ are symmetric polynomials in x_1, \ldots, x_n with two parameters q, t.

Macdonald processes [Borodin-Corwin '11]

Macdonald polynomials $P_{\lambda}(x_1, \ldots, x_n; q, t)$ indexed by integer partitions $\lambda = (\lambda_1 \ge \ldots \ge \lambda_n \ge 0)$ are symmetric polynomials in x_1, \ldots, x_n with two parameters q, t.



(Figure credits: A. Borodin)

The $\mathbb{Z}_p \leftrightarrow \mathbb{C}$ analogy is actually extremely close



The $\mathbb{Z}_p \leftrightarrow \mathbb{C}$ analogy is actually extremely close



Macdonald processes are also a key tool in our proofs.

Conclusion

We've seen structural analogies between random matrices over \mathbb{Z}_p and \mathbb{R}, \mathbb{C} through Macdonald processes, which belie serious probabilistic differences.

Conclusion

We've seen structural analogies between random matrices over \mathbb{Z}_p and \mathbb{R}, \mathbb{C} through Macdonald processes, which belie serious probabilistic differences.

Basic asymptotic questions inspired by real/complex random matrix theory yield new universal objects in p-adic random matrix theory.

Conclusion

We've seen structural analogies between random matrices over \mathbb{Z}_p and \mathbb{R}, \mathbb{C} through Macdonald processes, which belie serious probabilistic differences.

Basic asymptotic questions inspired by real/complex random matrix theory yield new universal objects in *p*-adic random matrix theory.

The end. Thank you all!

Bonus 1: An infinite amount of ringing



Infinitely many clocks ring on any time interval—nontrivial even to formally define reflecting Poisson sea! [VP 2023]

Bonus 1: An infinite amount of ringing



Infinitely many clocks ring on any time interval—nontrivial even to formally define reflecting Poisson sea! [VP 2023]

However, for 'nice initial conditions' $\mu(0)$ with $\lim_{i\to-\infty} \mu_i(0) = \infty$ as in above picture, projections suffice.

Bonus 2: more formal statement of bulk limit

Theorem (VP 2023)

Let $r \in (0,1)$, μ a 'nice initial condition', and for each $n \ge 1$, let

- $A_i^{(n)}, i \ge 1$ iid $n \times n$ matrices with distribution invariant under $\operatorname{GL}_n(\mathbb{Z}_p)$,
- B⁽ⁿ⁾ ∈ Mat_n(ℤ_p) fixed 'initial condition matrix' with singular numbers SN(B⁽ⁿ⁾)_{[rn]+i} → µ_i for all i.

•
$$\lambda^{(n)}(\tau) = SN(A_{\tau}^{(n)} \cdots A_{1}^{(n)} B^{(n)}).$$

Then $L_i^{(n)}(T) := \lambda_{\lfloor rn \rfloor + i}(\lfloor c_n^{-1}T \rfloor), i \in \mathbb{Z}, T \ge 0$ converges to reflecting Poisson sea $(\mu_i(T))_{i\in\mathbb{Z}}$ with $\mu(0) = \mu$, for $c_n = c(r, Law(SN(A_i^{(n)})))$ explicit, provided that **1** SN $(A_i^{(n)})$ is not identically $(0, \dots, 0)$, and **2** $X_n := \operatorname{corank}(A_i^{(n)} \pmod{p}) \ll rn \text{ w.h.p.}$ (formally, $\lim_{n\to\infty} \Pr(X_n > rn - j | X_n > 0) = 0$ for any $j \in \mathbb{N}$).