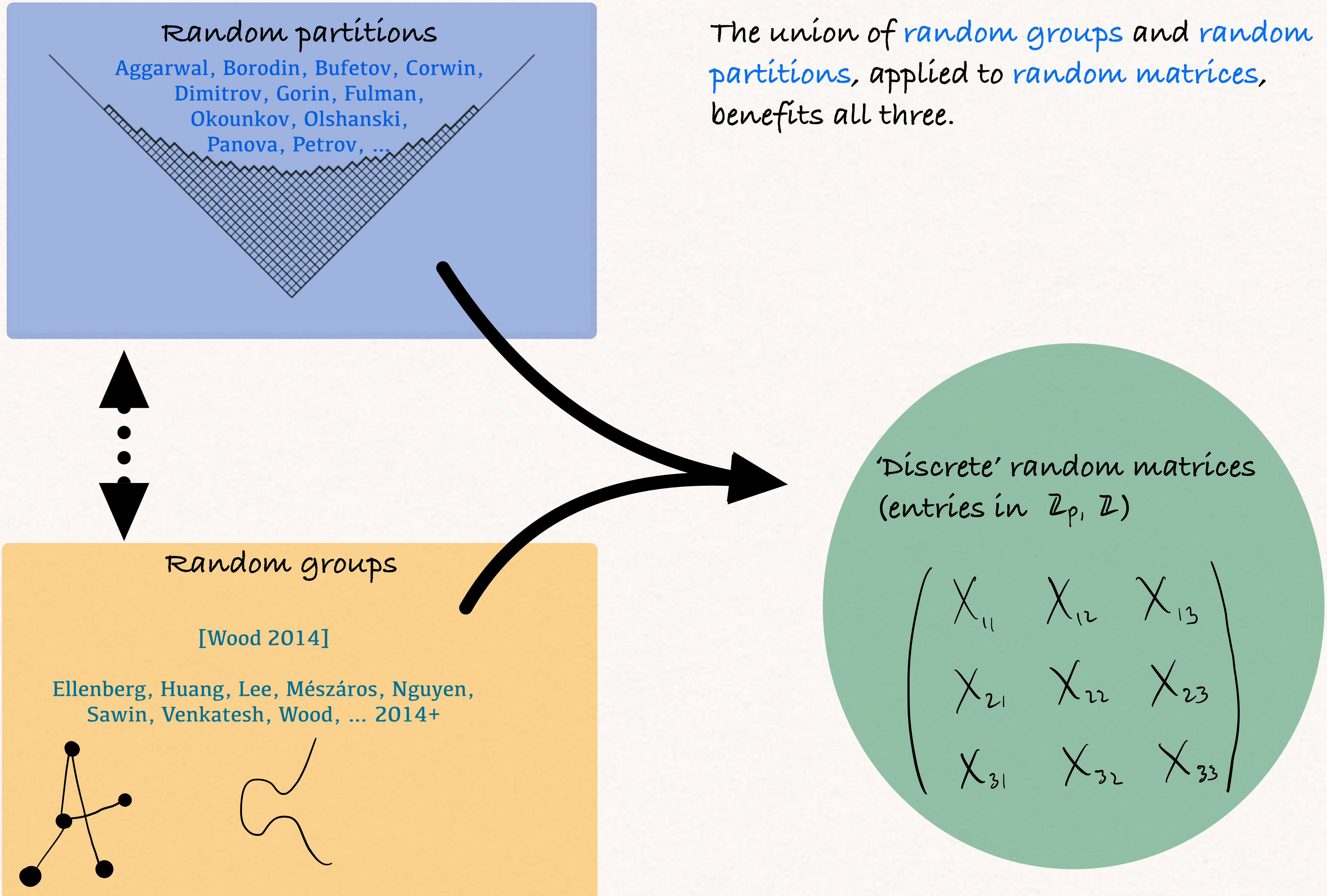
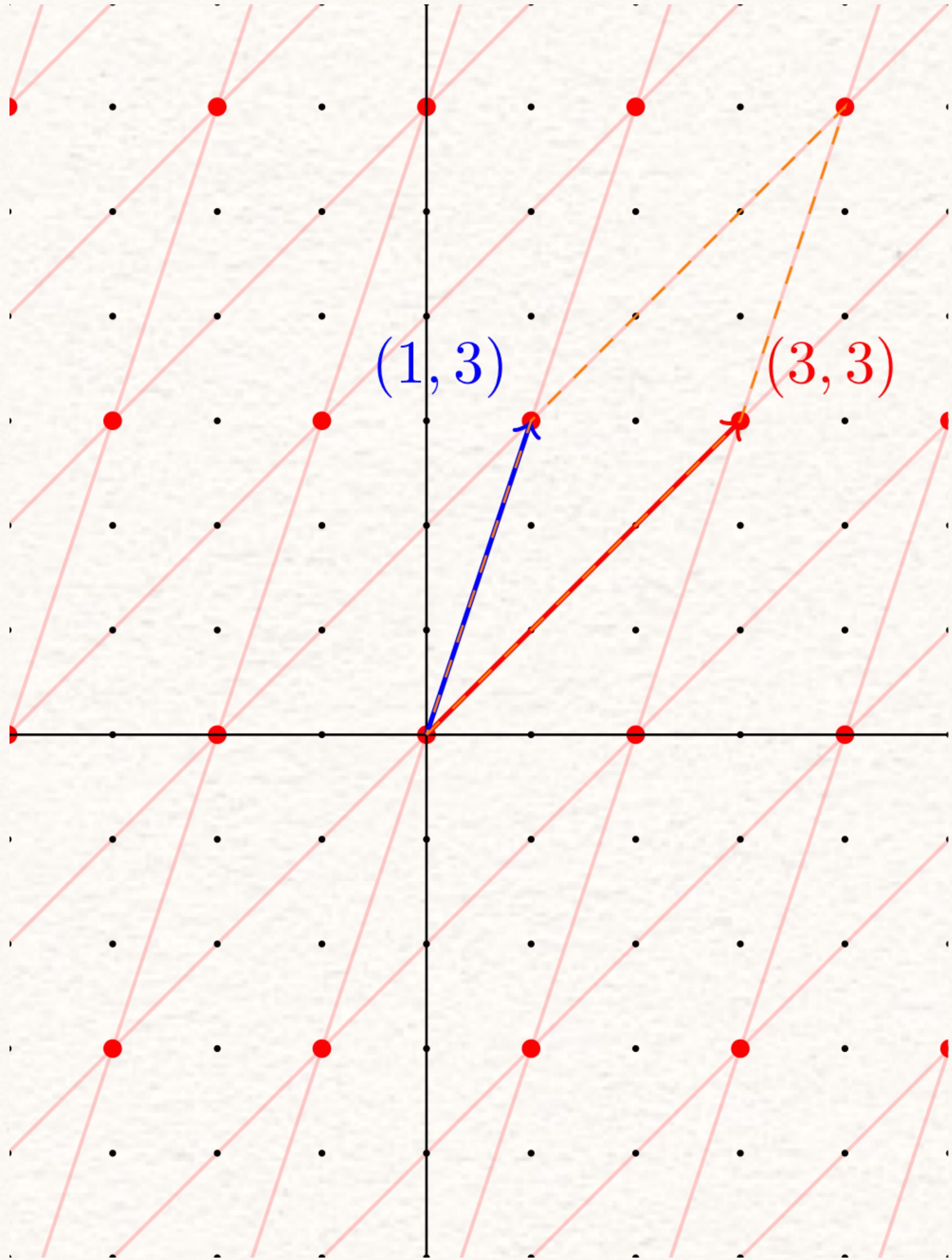
Random matrices, random partitions, and random groups

Roger Van Peski (Columbia University)

USC Department Colloquium
March 26, 2025

The union of random groups and random partitions, applied to random matrices, benefits all three.



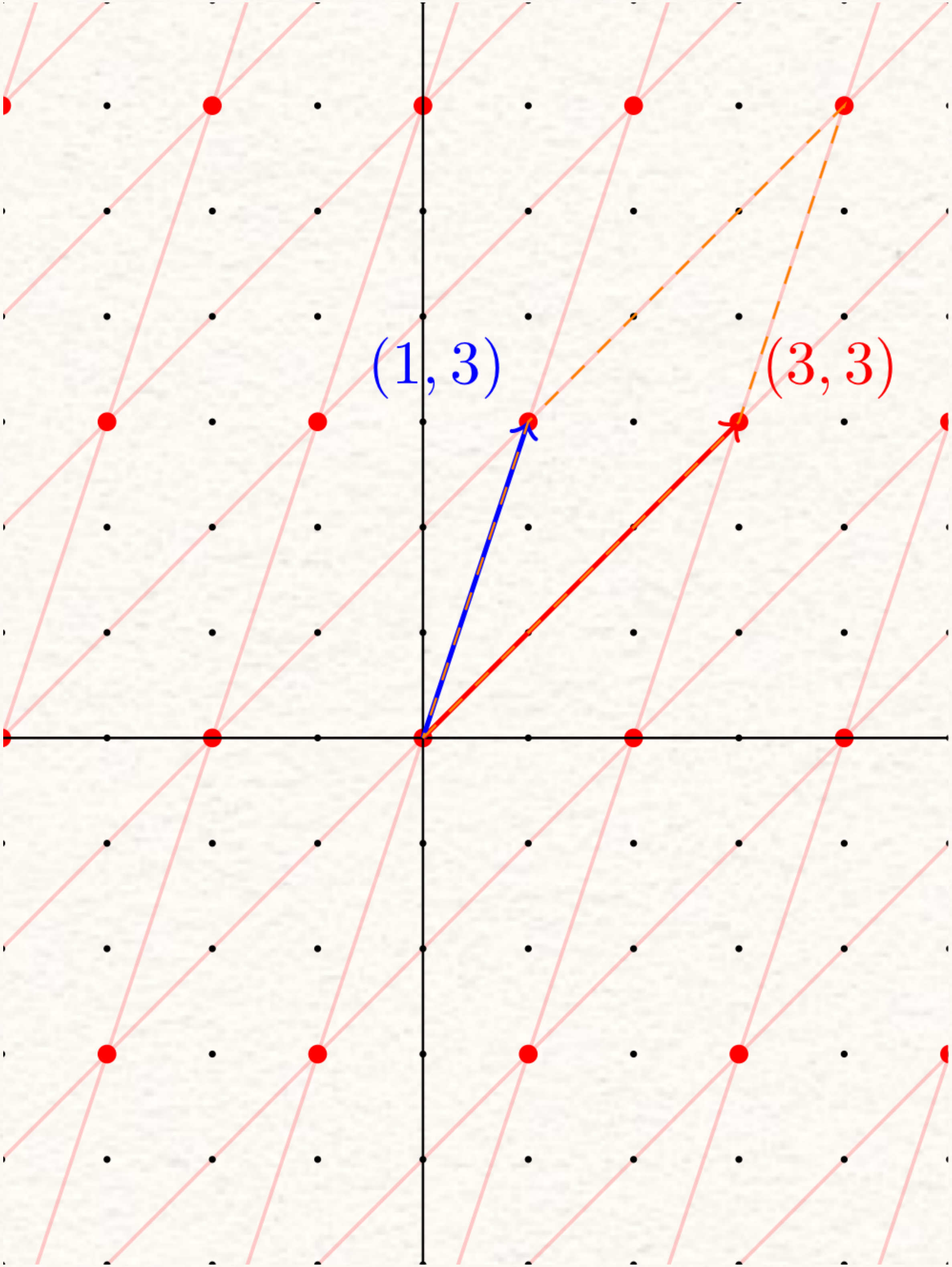


$$A = \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix}$$

$$A : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$

$$\mathrm{Cok}(A) := \mathbb{Z}^2 / A\mathbb{Z}^2$$
$$\cong \mathbb{Z}/6\mathbb{Z}$$

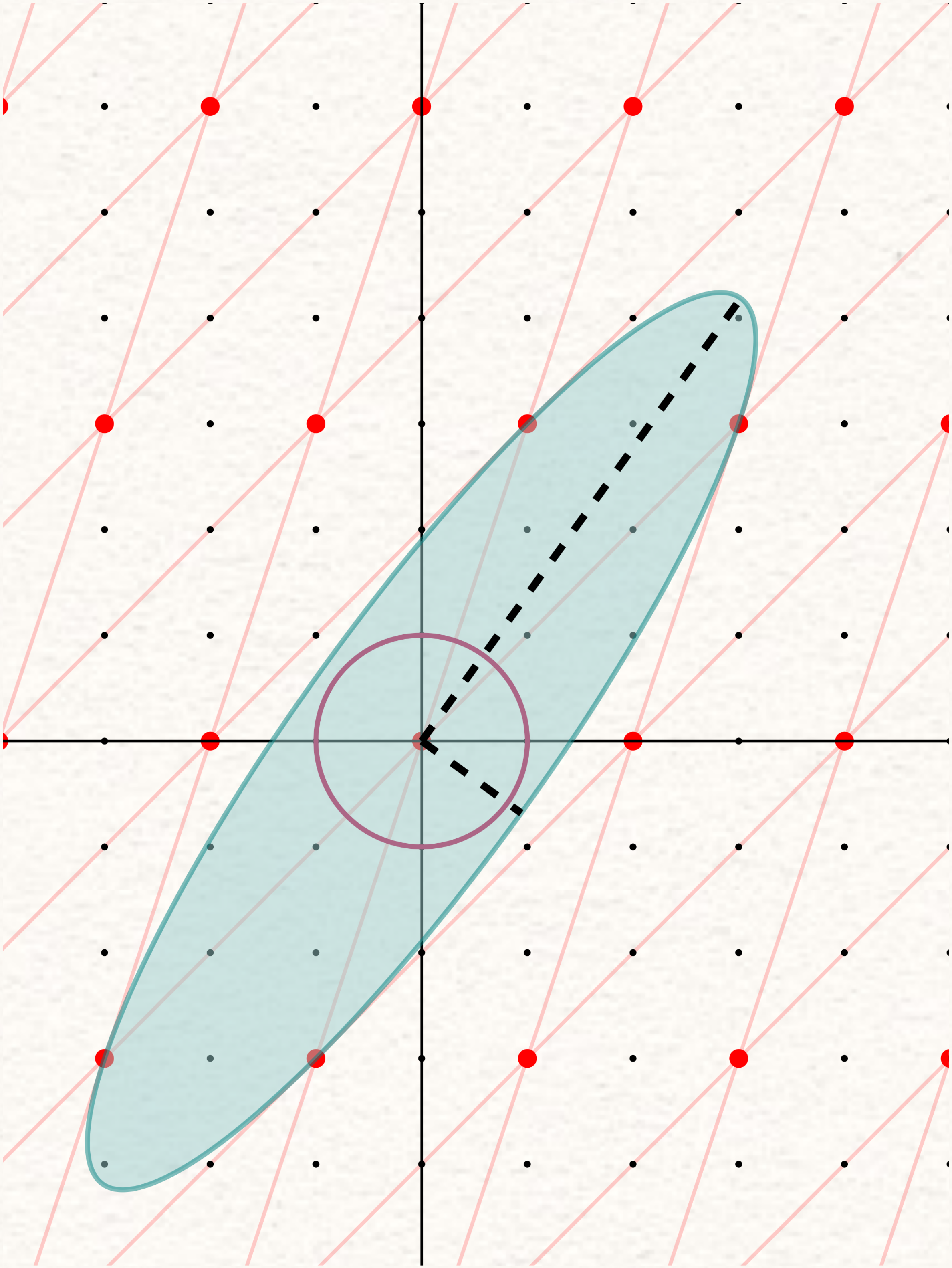
$$\#\mathrm{Cok}(A) = |\det A|$$



$A \in \mathrm{Mat}_N(\mathbb{Z})$

Question: how does cokernel look

- if A is random?
- if $A = A_T \cdots A_2 A_1$, $A_1, A_2, \ldots$ random?
- if $N \to \infty$?



Singular values: real

$$\sigma_1 \geq \sigma_2 \geq 0$$

given by

$$A = U \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix} V,$$

U, V unitary.

Singular values of

$$A_T \cdots A_2 A_1 ?$$

Ergodic theory [Bellman 1954], Furstenberg-Kesten 1960]...
Statistical physics [Akemann-Burda-Kieburg, 2010+]
Neural networks

Q: Which probability measures on abelian p-groups ($\#G = p^n$) describe those occurring 'in nature'?

Cohen and Lenstra (1983): $\mathbb{P}(G) \propto \frac{1}{\#\mathrm{Aut}(G)}$

(distributions of class groups)

"Our point is that the most naive assumption on the distribution ... leads directly to the Cohen-Lenstra principle that groups should carry a weight inversely proportional to the order of its automorphism group" -Friedman and Washington, 1987

Naive model random group: <u>cokernel</u> of random matrix

Fix a prime p.

Base p expansions: $1984 \text{ (base 10)} = 3 + 3\cdot 7 + 5\cdot 7^2 + 5\cdot 7^3$

$$\mathbb{Z}_p = \{a_0 + a_1 p + a_2 p^2 + \dots : a_i \in \{0,\dots,p-1\} \text{ for } i=1,2,\dots\}$$

Example: $-1 = 6 + 6\cdot 7 + 6\cdot 7^2 + \dots \in \mathbb{Z}_7$

An $N \times N$ matrix $A \in \mathrm{Mat}_N(\mathbb{Z}_p)$ gives linear map $A: \mathbb{Z}_p^N \to \mathbb{Z}_p^N$ with <u>cokernel</u>

$$\mathrm{Cok}(A) := \mathbb{Z}_p^N / A\mathbb{Z}_p^N$$

(Additive) Haar probability measure on $\mathbb{Z}_p$: Pick $a_i \in \{0,\dots,p-1\}$ uniformly random, independent.

Let $A \in \mathrm{Mat}_N(\mathbb{Z}_p)$ have independent Haar entries. Then for any abelian p-group G,

$$\lim_{N\to\infty} \mathbb{P}(\mathrm{Cok}(A) \cong G) = \frac{\prod_{i\geq 1}(1-p^{-i})}{\#\mathrm{Aut}(G)}$$

[Friedman-Washington 1987]

Let $A \in \mathrm{Mat}_N(\mathbb{Z}_p)$ have entries sampled independently from any probability distribution which is not constant modulo p. Then for any abelian p-group G,

$$\lim_{N\to\infty} \mathbb{P}(\mathrm{Cok}(A) \cong G) = \frac{\prod_{i\geq 1}(1-p^{-i})}{\#\mathrm{Aut}(G)}$$

[Wood 2015]

Also holds for <u>integer</u> matrices (different primes become independent).

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Basic progression:

1. Probe limit by exact computations with algebraically nice models (e.g. additive Haar matrices)
2. Prove universality, same limits shared by different prelimit matrix distributions (moment method)

How to describe limits of a big random group?

$\mathrm{Cok}(A)$ converges in distribution as $N \to \infty$, but

$\mathrm{Cok}(A_T \cdots A_2 A_1)$ gets bigger as $T \to \infty$ (no convergence).

Can still study e.g. its rank.

How to describe limits of a BIG random group?

$\mathrm{Cok}(A)$ converges in distribution as $N \to \infty$, but

$\mathrm{Cok}(A_T \cdots A_2 A_1)$ gets bigger as $T \to \infty$ (no convergence).

Can still study e.g. its rank.

Theorem [VP 2023, special case]
For independent $N \times N$ Haar matrices, as $N, T \to \infty$,

$$\mathrm{rank}(\mathrm{Cok}(A_T \cdots A_2 A_1)) - \log_p(T) \xrightarrow{*} \mathcal{L}^{(1)}$$

for a new explicit, $\mathbb{Z}$-valued random variable $\mathcal{L}^{(1)}$.

$$\mathbb{P}(\mathcal{L}^{(1)} = x) = \frac{1}{\prod_{i \geq 1}(1-p^{-i})} \sum_{j \geq 0} e^{-\alpha p^{j-x}} \frac{(-1)^j p^{-\binom{j}{2}}}{\prod_{i=1}^{j}(1-p^{-i})} \qquad (x \text{ integer})$$

"DISCRETE SINGULAR VALUES"

$A \in \mathrm{Mat}_N(\mathbb{Z}_p)$ has decomposition

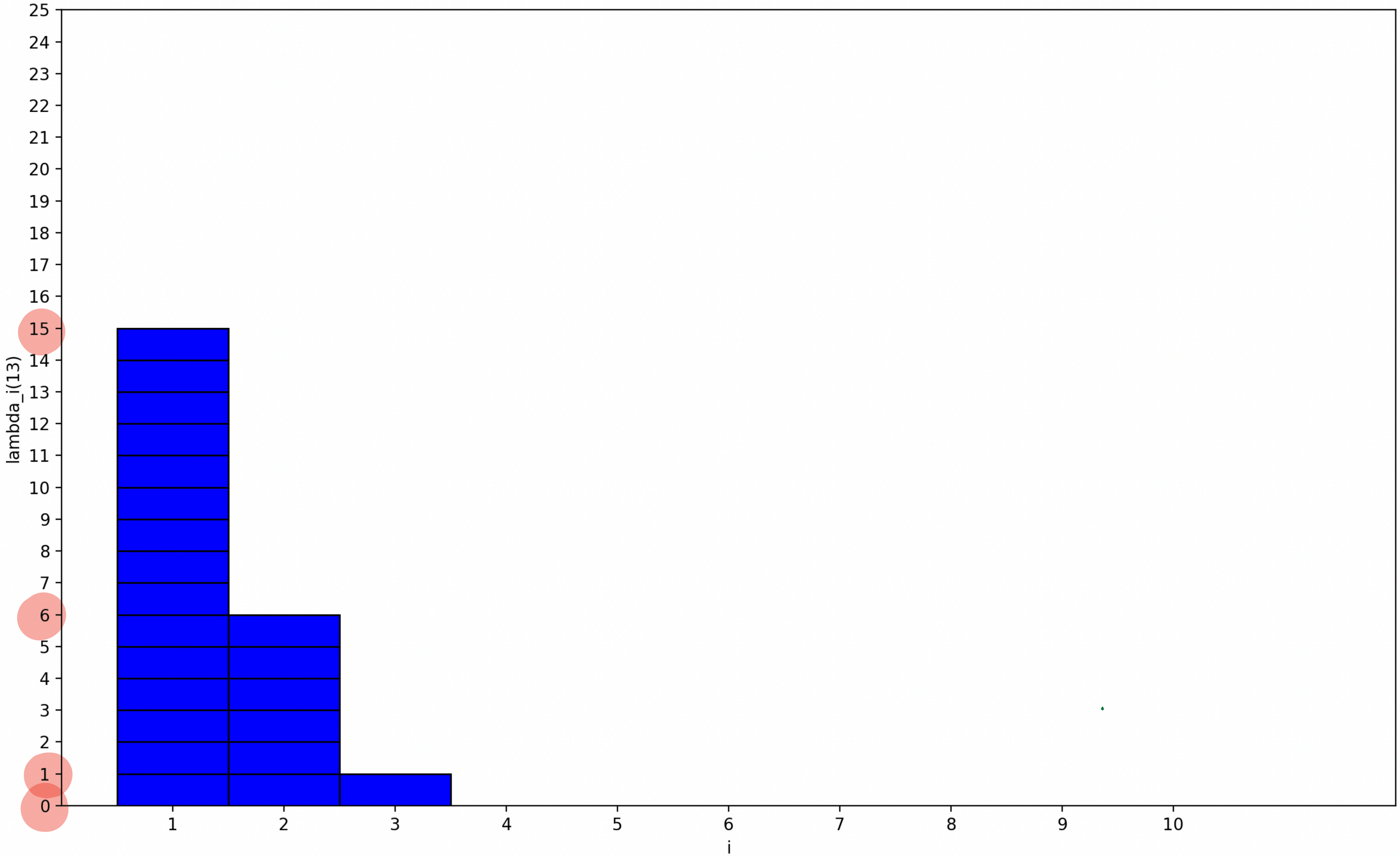
$A = U \,\mathrm{Diag}(p^{\lambda_1}, \ldots, p^{\lambda_N})\, V, \qquad U, V \in GL_N(\mathbb{Z}_p)$

$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_N \geq 0$ "singular numbers" (integer partition)

$$\begin{tikzcd}[column sep=small]
& \begin{array}{c}\text{Random matrix}\\ A\end{array} \arrow[dl, "\text{singular numbers}"'] \arrow[dr, "\text{cokernel}"] & \\
\begin{array}{c}\text{Random partition}\\ \lambda=(\lambda_1,\lambda_2,\ldots,\lambda_N)\end{array} \arrow[rr, leftrightarrow, dotted, "\text{isomorphism type}"'] & & \begin{array}{c}\text{Random group}\\ \mathrm{Cok}(A)\cong\bigoplus_{i=1}^{N}\mathbb{Z}/p^{\lambda_i}\mathbb{Z}\end{array}
\end{tikzcd}$$

How does a 'big' random (abelian p-) group look?

$$\mathrm{Cok}(A_{13}\cdots A_2A_1) \cong \mathbb{Z}/p^{15}\mathbb{Z} \oplus \mathbb{Z}/p^{6}\mathbb{Z} \oplus \mathbb{Z}/p^{1}\mathbb{Z} \oplus \underbrace{\mathbb{Z}/p^{0}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{0}\mathbb{Z}}_{\text{(trivial)}}$$

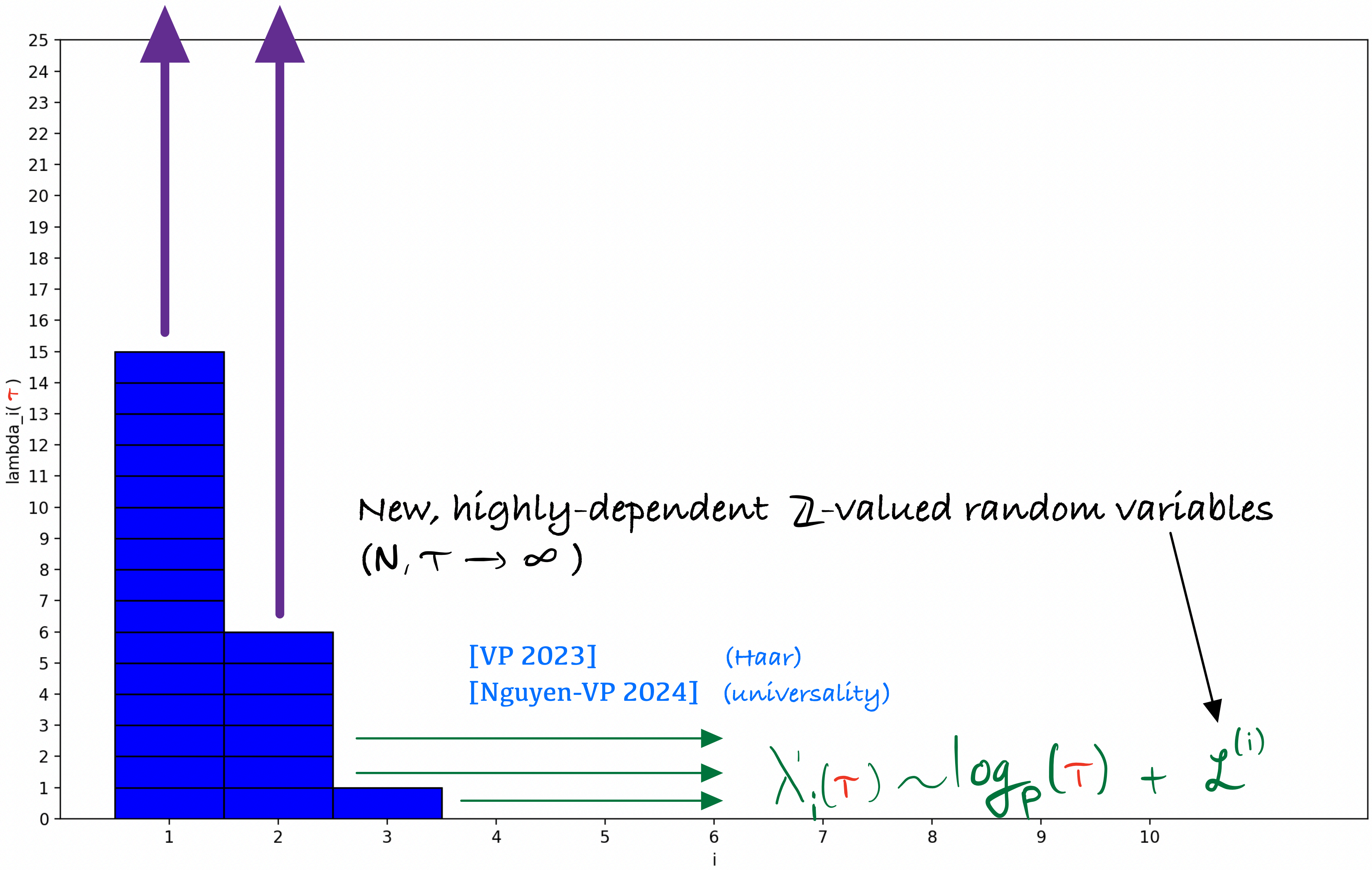


How does a 'big' random (abelian p-) group look?

Independent Gaussians

$\lambda_i(\tau) \sim C_i \cdot \tau + \sigma_i \sqrt{\tau}\, Z_i$ as $\tau \to \infty$

[VP 2020], [Shen 2024]
(Haar) (universality)



Theorem [VP 2020]
For independent $N \times N$ Haar matrices, as $T \to \infty$,

$$\frac{\lambda_i(T) - c_i T}{\sigma_i \sqrt{T}} \to \mathcal{N}(0,1) \quad \text{in joint distribution.}$$

Theorem [VP 2023a]
For independent $N \times N$ Haar matrices, as $N, T \to \infty$,

$$\lambda'_i(T) - \log_p(T) \xrightarrow{*} \mathcal{L}^{(i)} \quad \text{in joint distribution.}$$

Theorem [VP 2023b]
Construct multi-time limit of $\lambda'_i(T) - \log_p(T)$ (reflecting Poisson sea), which has $(\mathcal{L}^{(1)}, \mathcal{L}^{(2)}, \ldots)$ as stationary distribution.

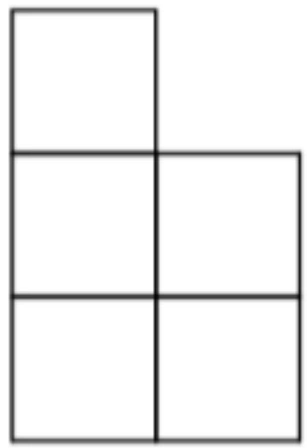
Theorem [Nguyen-VP 2024]
$\mathcal{L}^{(i)}$ are universal: any matrix distribution (nonconstant mod p) yields same asymptotics. Also holds for integer entries.

Where else does this limit appear?

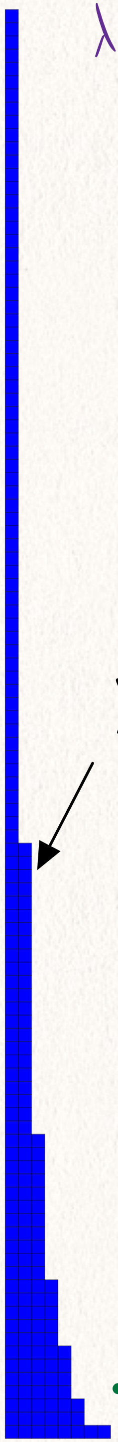
Cokernels of block-triangular matrices [Mészáros 2024]

A. A. Kirillov, 1990s: How does Jordan type of uniformly random upper-triangular matrix look?

$$\begin{pmatrix} 0 & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \mapsto \left(\begin{array}{ccc|cc} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \mapsto$$



$$= (3,2) = \lambda$$



$\lambda_i(N) \sim c_i \cdot N + \sigma_i \sqrt{N}\, Z_i$

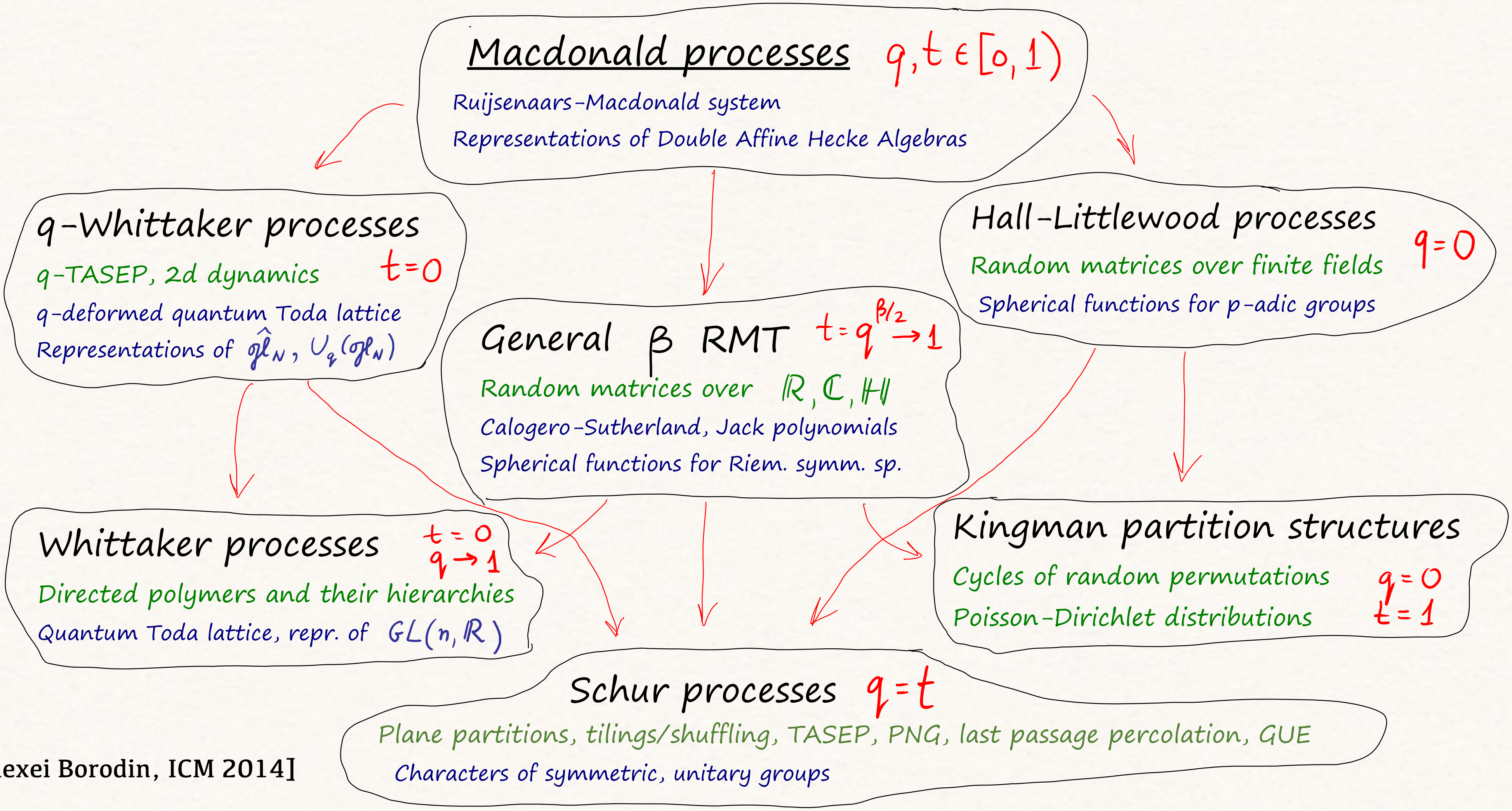
<u>dependent</u> Gaussians

[Borodin 1995]

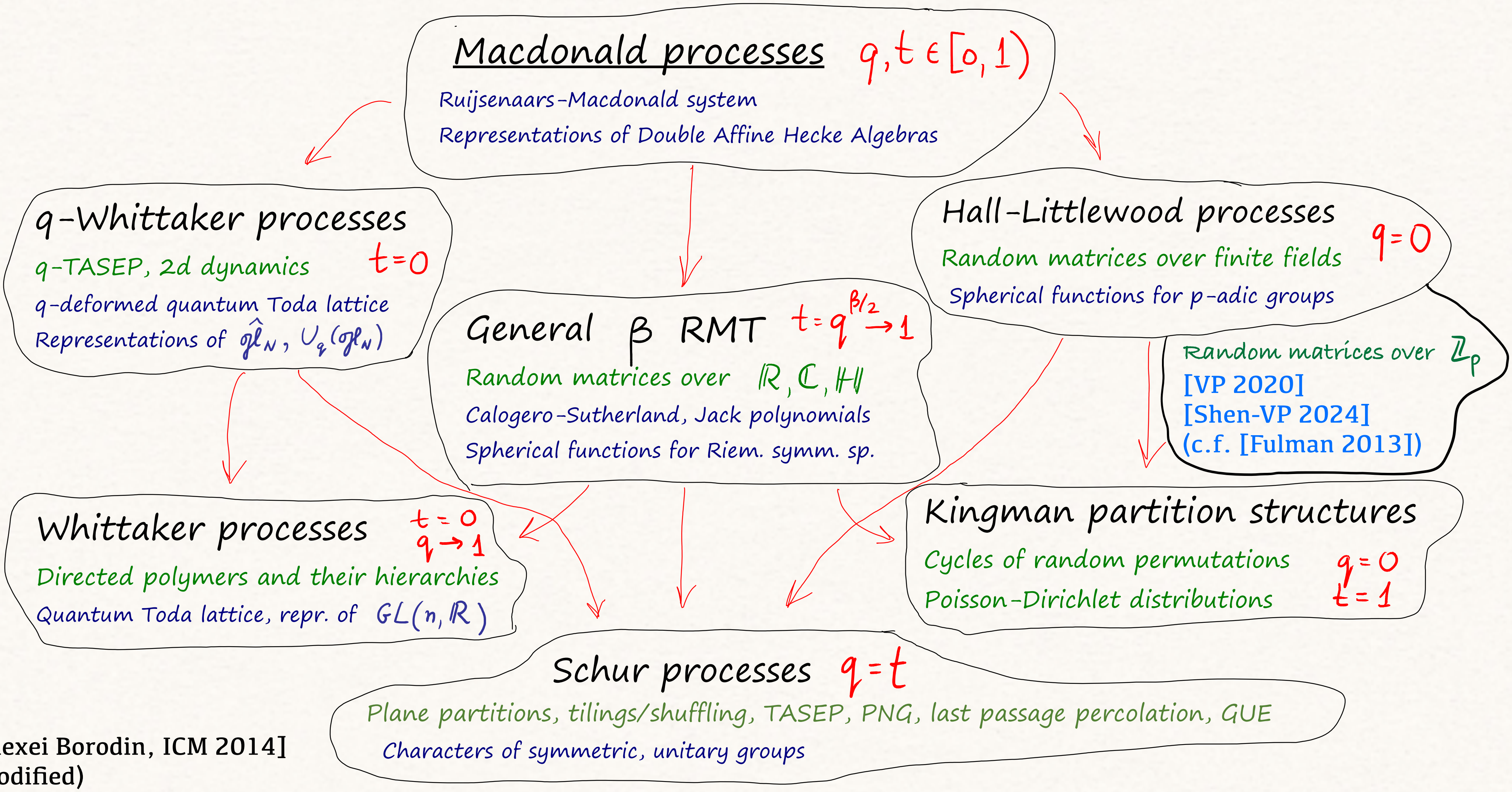
$\lambda(200) = (108, 45, 23, 12, 7, 3, 1, 1)$ from 200 x 200 matrix over $\mathbb{F}_2$

$\sim \log_p(N) + \mathcal{L}^{(i)}, \quad i = 1, 2, \dots$

[VP 2024]



[Alexei Borodin, ICM 2014]

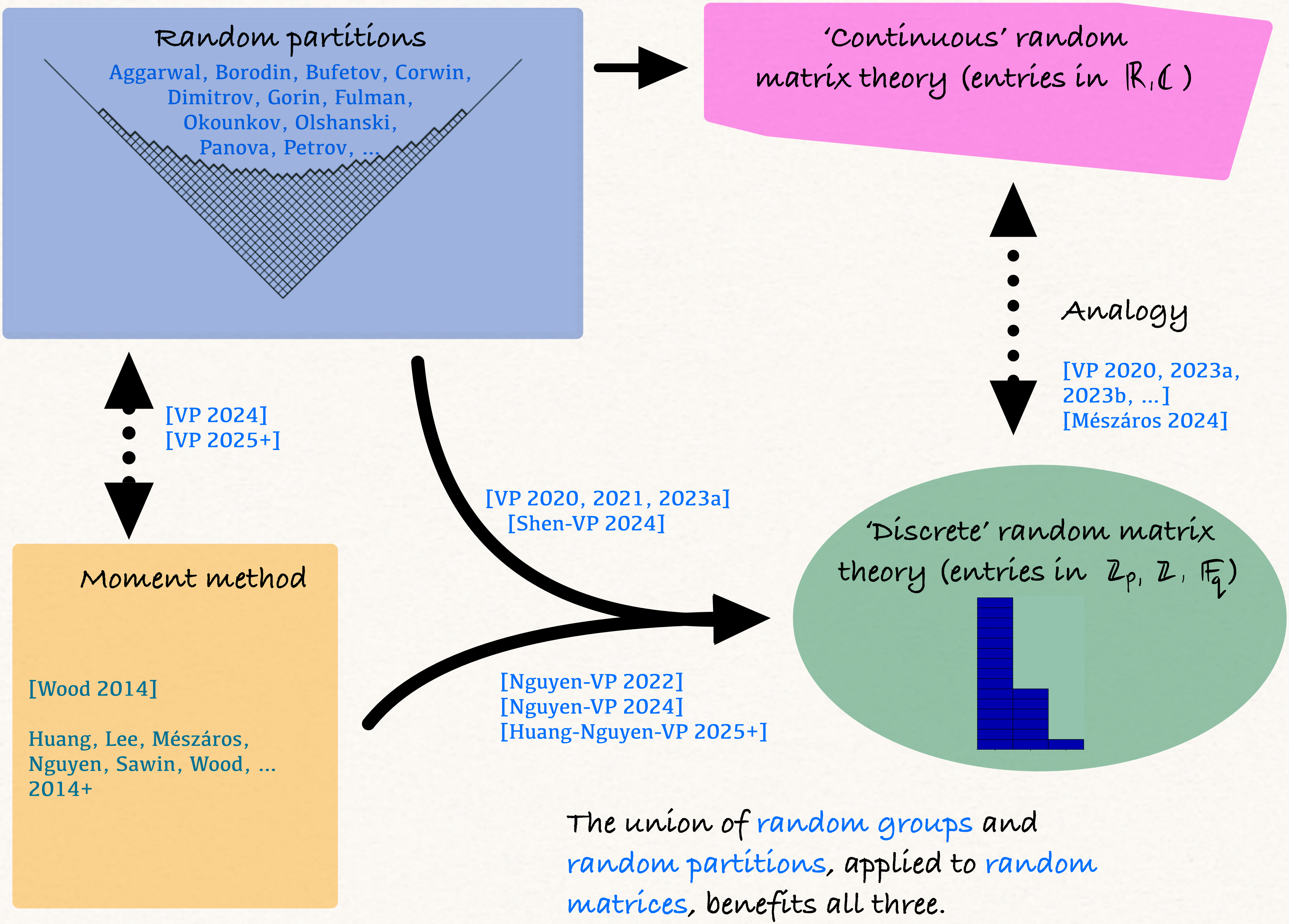


[Alexei Borodin, ICM 2014]
(modified)

Moment method

Real random variable X has moments $\mathbb{E}[X^k]$, $k = 1, 2, \ldots$

Random group G has moments $\mathbb{E}[\#\mathrm{Sur}(G \to H)]$


Random partitions
Aggarwal, Borodin, Bufetov, Corwin, Dimitrov, Gorin, Fulman, Okounkov, Olshanski, Panova, Petrov, ...
'Continuous' random matrix theory (entries in $\mathbb{R}, \mathbb{C}$)
Analogy
[VP 2020, 2023a, 2023b, ...]
[Mészáros 2024]
[VP 2024]
[VP 2025+]
[VP 2020, 2021, 2023a]
[Shen-VP 2024]
'Discrete' random matrix theory (entries in $\mathbb{Z}_p$, $\mathbb{Z}$, $\mathbb{F}_q$)
Moment method
[Wood 2014]
Huang, Lee, Mészáros, Nguyen, Sawin, Wood, ... 2014+
[Nguyen-VP 2022]
[Nguyen-VP 2024]
[Huang-Nguyen-VP 2025+]
The union of random groups and random partitions, applied to random matrices, benefits all three.