Universality Results for Random Matrices over Local Rings

Maine-Quebec Number Theory Conference

Nikita Lvov

October 5, 2025

Introduction: Groups as Random Objects

Conjecture (Cohen-Lenstra, 1984)

As K ranges through imaginary quadratic fields, ordered by discriminant,

$$\mathbb{P}(Cl_K[p^\infty] \cong G) \propto \frac{1}{|Aut(G)|}$$

Example

$\mathbb{Z}/p^2\mathbb{Z}$ occurs more frequently than $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Random Abelian Groups from Random Matrices

Theorem (Friedman-Washington, 1989)

Suppose the coefficients of $\mathcal{M}_{n,n}$ are independent Haar distributed random variables in $\mathbb{Z}_p$. As $n \to \infty$, we get a limiting probability distribution on finite abelian p-groups that satisfies

$$\mathbb{P}(G) \propto \frac{1}{|Aut(G)|}$$

Random Abelian Groups from Random Matrices

Theorem (Friedman-Washington, 1989)

Suppose the coefficients of $\mathcal{M}_{n,n}$ are independent Haar distributed random variables in $\mathbb{Z}_p$. As $n \to \infty$, we get a limiting probability distribution on finite abelian p-groups that satisfies

$$\mathbb{P}(G) \propto \frac{1}{|Aut(G)|}$$

Theorem (Maples, 2013; Wood, 2015)

Suppose the coefficients of $\mathcal{M}_{n,n}$ are non-degenerate identically distributed random variables [a]. Then the same conclusion holds.

[a] Degenerate: constant modulo p

Illustration

Example (A Bernoulli random matrix - ”White Noise”)

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

Entries are 0 or 1 with probability $1/2$.

Group Theoretic Point of View

Observation

The cokernel map is $GL_n(\mathbb{Z}_p) \times GL_n(\mathbb{Z}_p)$ invariant. We will use this action. In fact, we will only need the right action of SL_n.

Remark

From now on, replace $\mathbb{Z}_p$ with $\mathbb{Z}/p^r\mathbb{Z}$ for some $r >> 1$.

Main Lemma

A column vector of $\mathcal{M}_{n,n}$ is approximately uniformly distributed modulo the other column vectors of $\mathcal{M}_{n,n}$.

Column Replacement Estimate (Lindeberg, Tao-Vu)

Theorem

The total variation distance between

$$\left[\begin{array}{c|c} \mathcal{M}_{n,n-1} & \begin{matrix} m_{1,n} \\ \vdots \\ m_{n,n} \end{matrix} \end{array}\right] \Big/ SL_n \quad \text{and} \quad \left[\begin{array}{c|c} \mathcal{M}_{n,n-1} & \begin{matrix} h_{1,n} \\ \vdots \\ h_{n,n} \end{matrix} \end{array}\right] \Big/ SL_n$$

is at most $O_r(e^{-cn})$.

Corollary

$$d_{TV}\left(F\left[\quad \mathcal{M}_{n,n} \quad\right], F\left[\quad \mathcal{H}aar_{n,n} \quad\right]\right) \leq O_r(e^{-Cn}).$$

F can be the cokernel, the determinant, the span.

Other Local Rings (e.g. quotients of power series rings, extensions of $\mathbb{Z}_p$)

Motivation for considering random matrices over other local rings:

- Random models for class groups of fields with a Galois action.
- Random models for Iwasawa invariants (Ellenberg-Jain-Venkatesh).
- To understand $det(A - Ix)$ for random matrices.

Observation

Universality fails if every entry belongs to the maximal ideal, or if every entry lies in a sub-ring of R.

Theorem

Universality holds for i.i.d. random matrices over any finite local ring R, assuming that the support is not contained in the translate of a sub-ring, or the translate of an ideal of R.

Ergodic Averages

$$\begin{pmatrix} h_{11} & h_{12} & h_{13} & h_{14} & h_{15} & \\ h_{21} & h_{22} & h_{23} & h_{24} & h_{25} & \\ h_{31} & h_{32} & h_{33} & h_{34} & h_{35} & \cdots \\ h_{41} & h_{42} & h_{43} & h_{44} & h_{45} & \\ h_{51} & h_{52} & h_{53} & h_{54} & h_{55} & \\ & & \vdots & & & \end{pmatrix}$$

Theorem ("Ergodic Friedman-Washington")

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{(coker(\mathcal{H}aar_{i,i}) \cong G)} \propto \frac{1}{\#Aut(G)}$$

Remark

An analogous statement holds for the determinant. An analogous statement holds over general finite local rings R.

Ergodic Universality

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} & m_{15} & \\ m_{21} & m_{22} & m_{23} & m_{24} & m_{25} & \\ m_{31} & m_{32} & m_{33} & m_{34} & m_{35} & \cdots \\ m_{41} & m_{42} & m_{43} & m_{44} & m_{45} & \\ m_{51} & m_{52} & m_{53} & m_{54} & m_{55} & \\ & & \vdots & & & \end{pmatrix}$$

Theorem ("Ergodic Universality")

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{(coker(\mathcal{M}_{i,i}) \cong G)} \propto \frac{1}{\#Aut(G)}$$

Remark

Analogous statement holds with the cokernel replaced by the determinant, and with $\mathbb{Z}_p$ replaced by any finite local ring.

Thank you!