A random walk on the category of finite abelian p-groups

Quebec-Maine Number Theory Conference

Nikita Lvov

October 6, 2024

Introduction: Groups as Random Objects

Conjecture (Cohen-Lenstra, 1984)

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

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

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 $1/2$.

Cokernels of Corners

Example

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

Definition

Denote by $\mathcal{M}_{n,n}^{Haar}$ the top left $n \times n$ corner of a large (or infinite) matrix whose entries are independent, Haar random variables.

Hence,

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a random process on finite abelian p-groups.

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$\mathit{coker}(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$\mathit{coker}(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$coker(\mathcal{M}_{n,n}^{Haar})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Markov Chain

Theorem (Van Peski, L.)

$$\textit{coker}(\mathcal{M}_{n,n}^{\textit{Haar}})$$

is a Markov chain.

Example

$$\mathbb{Z}/2\mathbb{Z}$$

Theorem

$$\textit{coker}(\mathcal{M}_{n,n}^{\textit{Bernoulli}})$$

is "asymptotically" a Markov chain.

Definitions; Description of Markov Chain

Definition

- X_0 denotes the set of finite abelian p-groups G.

Definitions; Description of Markov Chain

Definition

- X_0 denotes the set of finite abelian p-groups G.
- X_1 denotes the set of abelian p-groups H such that $H \cong H_{tors} \times \mathbb{Z}_p$.

Definitions; Description of Markov Chain

Definition

- X_0 denotes the set of finite abelian p-groups G.
- X_1 denotes the set of abelian p-groups H such that $H \cong H_{tors} \times \mathbb{Z}_p$.

Two Random Operators

- $d : X_1 \to X_0$:

  take quotient by random element

Definitions; Description of Markov Chain

Definition

- X_0 denotes the set of finite abelian p-groups G.
- X_1 denotes the set of abelian p-groups H such that $H \cong H_{tors} \times \mathbb{Z}_p$.

Two Random Operators

- $d : X_1 \to X_0$:
  take quotient by random element
- $d^* : X_0 \to X_1$:
  pick random element of $Ext(\,\cdot\,, \mathbb{Z}_p)$[a]

[a] For G finite, $Ext(G, \mathbb{Z}_p)$ is dual to G.

Connection with Random Matrices

$$d\Big(coker(M_{n,n+1})\Big) = \left[\begin{array}{ccc} & M_{n,n+1} & \\ \hline * & \dots & * \end{array}\right]$$

(Quotient by a random element)

Connection with Random Matrices

$$d\left(coker(M_{n,n+1})\right) = \left[\begin{array}{ccc} & M_{n,n+1} & \\ \hline * & \dots & * \end{array}\right]$$

(Quotient by a random element)

$$d^*\left(coker(M_{n,n})\right) = \left[\begin{array}{c|c} & * \\ M_{n,n} & \vdots \\ & * \end{array}\right]$$

Connection with Random Matrices

$$d\left(coker(M_{n,n+1})\right) = \left[\begin{array}{ccc} & M_{n,n+1} & \\ \hline * & \cdots & * \end{array}\right]$$

(Quotient by a random element)

$$d^*\left(coker(M_{n,n})\right) = \left[\begin{array}{c|c} & * \\ M_{n,n} & \vdots \\ & * \end{array}\right]$$

(Random $\mathbb{Z}_p$-extension)

Connection with Random Matrices

$$d\left(coker(M_{n,n+1})\right) = \left[\begin{array}{ccc} & M_{n,n+1} & \\ \hline * & \cdots & * \end{array}\right]$$

(Quotient by a random element)

$$d^*\left(coker(M_{n,n})\right) = \left[\begin{array}{c|c} & * \\ M_{n,n} & \vdots \\ & * \end{array}\right]$$

(Random $\mathbb{Z}_p$-extension)

$$dd^*\left(coker(M_{n,n})\right) = \left[\begin{array}{ccc|c} & & & * \\ & M_{n,n} & & \vdots \\ & & & * \\ \hline * & \cdots & * & * \end{array}\right]$$

Time-Reversible Markov Chains

Definition

Given a Markov Chain at equilibrium, time-reversal gives another Markov chain:

$$\mathbb{P}^*(A \to B) = \frac{\mathbb{P}(B)\mathbb{P}(B \to A)}{\mathbb{P}(A)}$$

Time-Reversible Markov Chains

Definition

Given a Markov Chain at equilibrium, time-reversal gives another Markov chain:

$$\mathbb{P}^*(A \to B) = \frac{\mathbb{P}(B)\mathbb{P}(B \to A)}{\mathbb{P}(A)}$$

Definition

A Markov chain is *time-reversible* if

$$\mathbb{P}(A)\mathbb{P}(A \to B) = \mathbb{P}(B)\mathbb{P}(B \to A) \tag{1.1}$$

Time-Reversible Markov Chains

Definition

Given a Markov Chain at equilibrium, time-reversal gives another Markov chain:

$$\mathbb{P}^*(A \to B) = \frac{\mathbb{P}(B)\mathbb{P}(B \to A)}{\mathbb{P}(A)}$$

Definition

A Markov chain is *time-reversible* if

$$\mathbb{P}(A)\mathbb{P}(A \to B) = \mathbb{P}(B)\mathbb{P}(B \to A) \tag{1.1}$$

Reminder

Any time-reversible Markov chain can be represented as a symmetric random walk on a weighted graph.

(d, d^*) is Time-Reversible

Observation

For any $GL_{n+1}(\mathbb{Z}_p)$-invariant measure $\mathcal{M}_{n,n+1}$,

$$\operatorname{coker}\left[\begin{array}{ccccc} & & \mathcal{M}_{n,n+1} & & \\ \hline 0 & 0 & \dots & 0 & 1 \end{array}\right] \approx \operatorname{coker}\left[\begin{array}{ccccc} & & \mathcal{M}_{n,n+1} & & \\ \hline * & * & \dots & * & * \end{array}\right]$$

(d, d^*) is Time-Reversible

Observation

For any $GL_{n+1}(\mathbb{Z}_p)$-invariant measure $\mathcal{M}_{n,n+1}$,

$$\text{coker}\left[\begin{array}{cccc} & \mathcal{M}_{n,n+1} & & \\ \hline 0 & 0 & \dots & 0 & 1 \end{array}\right] \approx \text{coker}\left[\begin{array}{cccc} & \mathcal{M}_{n,n+1} & & \\ \hline * & * & \dots & * & * \end{array}\right]$$

Corollary

(d^*, d) is a time-reversible Markov chain.

$$\left(\text{coker}(\mathcal{M}_{n,n}^{Haar}) \,\middle|\, \text{coker}(\mathcal{M}_{n,n+1}^{Haar}) = H\right) \approx$$

$$\left(\text{coker}(\mathcal{M}_{n+1,n+1}^{Haar}) \,\middle|\, \text{coker}(\mathcal{M}_{n,n+1}^{Haar}) = H\right)$$

Interpretation as a Random Walk

The weighted graph Γ

$$(d^*, d)$$

is a random walk on a bipartite weighted graph Γ with:

- Vertices labeled by G or H.

Interpretation as a Random Walk

The weighted graph Γ

$$(d^*, d)$$

is a random walk on a bipartite weighted graph Γ with:

- Vertices labeled by G or H.
- Edges:

$$0 \to \mathbb{Z}_p \to H \to G \to 0$$

Interpretation as a Random Walk

The weighted graph Γ

$$(d^*, d)$$

is a random walk on a bipartite weighted graph Γ with:

- Vertices labeled by G or H.
- Edges:

$$0 \to \mathbb{Z}_p \to H \to G \to 0$$

- Weights:

$$\frac{1}{|Aut(\mathbb{Z}_p \to H \to G)||G|}$$

Interpretation as a Random Walk

The weighted graph Γ

$$(d^*, d)$$

is a random walk on a bipartite weighted graph Γ with:

- Vertices labeled by G or H.
- Edges:

$$0 \to \mathbb{Z}_p \to H \to G \to 0$$

- Weights:

$$\frac{1}{|Aut(\mathbb{Z}_p \to H \to G)||G|}$$

We get dd^* by taking two random steps on this weighted graph.

The Spectrum of Γ

Remark

The spectrum of Γ can be deduced from the spectrum of dd^*.

The Spectrum of Γ

Remark

The spectrum of Γ can be deduced from the spectrum of dd^*.

Theorem

The spectrum of dd^* is the closure of

$$\left\{ \frac{1}{|G|} \right\}$$

The Spectrum of Γ

Remark

The spectrum of Γ can be deduced from the spectrum of dd^*.

Theorem

The spectrum of dd^* is the closure of

$$\left\{ \frac{1}{|G|} \right\}$$

Theorem

There exists an explicit unitary operator $\mathcal{U}$ such that:

$$\mathcal{U}^{-1} dd^* \mathcal{U} = \frac{1}{|G|}$$

The Unitary Operator $\mathcal{U}$

Theorem (Van Peski, L.)

There exists a unitary operator $\mathcal{U}$ such that:

$$\mathcal{U}\left(\frac{|Sur(F,\cdot)|}{|Aut(\cdot)|}\right) = \sqrt{c_0}\left(\frac{|Sur(\cdot,F)|}{|Aut(\cdot)|}\right)$$

The Unitary Operator $\mathcal{U}$

Theorem (Van Peski, L.)

There exists a unitary operator $\mathcal{U}$ such that:

$$\mathcal{U}\left(\frac{|Sur(F,\cdot)|}{|Aut(\cdot)|}\right) = \sqrt{c_0}\left(\frac{|Sur(\cdot,F)|}{|Aut(\cdot)|}\right)$$

Caveat

$\mathcal{U}$ may not be surjective, but...

The Unitary Operator $\mathcal{U}$

Theorem (Van Peski, L.)

There exists a unitary operator $\mathcal{U}$ such that:

$$\mathcal{U}\left(\frac{|Sur(F,\cdot)|}{|Aut(\cdot)|}\right) = \sqrt{c_0}\left(\frac{|Sur(\cdot,F)|}{|Aut(\cdot)|}\right)$$

Caveat

$\mathcal{U}$ may not be surjective, but...

Theorem

$$im(\mathcal{U}) = \overline{im(dd^*)}$$

The Unitary Operator $\mathcal{U}$, cont'd

Theorem (Van Peski, L.)

$$c_0 \sum_G \frac{|Sur(G, F_1)||Sur(G, F_2)|}{|Aut(G)|} = \sum_G \frac{|Sur(F_1, G)||Sur(F_2, G)|}{|Aut(G)|} \quad \forall F_1, F_2$$

The Unitary Operator $\mathcal{U}$, cont'd

Theorem (Van Peski, L.)

$$c_0 \sum_G \frac{|Sur(G, F_1)||Sur(G, F_2)|}{|Aut(G)|} = \sum_G \frac{|Sur(F_1, G)||Sur(F_2, G)|}{|Aut(G)|} \quad \forall\, F_1, F_2$$

Example

Substituting $F_2 = 0$ yields the well-known identity:

$$c_0 \sum_G \frac{|Sur(G, F_1)|}{|Aut(G)|} = 1 \quad \forall\, F_1.$$

Thank you!

Eigenfunctions

Corollary

- *To every $F \in X_0$, we can associate an eigenfunction of dd^*:*

$$E_F \stackrel{\text{def}}{=\!=} \mathcal{U}(1_F)$$

Eigenfunctions

Corollary

- *To every $F \in X_0$, we can associate an eigenfunction of dd^*:*

$$E_F \stackrel{\text{def}}{=\!=} \mathcal{U}(1_F)$$

- *The eigenvalue of E_F is $|F|^{-1}$.*

Eigenfunctions

Corollary

- *To every $F \in X_0$, we can associate an eigenfunction of dd^*:*

$$E_F \overset{\text{def}}{=\!=} \mathcal{U}(1_F)$$

- *The eigenvalue of E_F is $|F|^{-1}$.*
- *We can calculate E_F explicitly.*

Eigenfunctions

Corollary

- *To every $F \in X_0$, we can associate an eigenfunction of dd^*:*

$$E_F \overset{\text{def}}{=\!=} \mathcal{U}(1_F)$$

- *The eigenvalue of E_F is $|F|^{-1}$.*
- *We can calculate E_F explicitly.*
- *The E_F are independent and they span a dense subset of*

$$ker(dd^*)^{\perp} = \overline{im(dd^*)}.$$

Proofs

Proof of First Main Theorem

Definition

$$M(F) \stackrel{\text{def}}{=\!=} \mu_0(\,\cdot\,)|Sur(\,\cdot\,,F)| = c_0 \frac{|Sur(\,\cdot\,,F)|}{|Aut(\,\cdot\,)|}$$

Proof of First Main Theorem

Definition

$$M(F) \stackrel{\text{def}}{=\!=} \mu_0(\,\cdot\,)|Sur(\,\cdot\,,F)| = c_0\frac{|Sur(\,\cdot\,,F)|}{|Aut(\,\cdot\,)|}$$

Lemma (Main Lemma)

$$dd^*\Big(M(F)\Big) = \frac{1}{|F|}\sum_{Hom(\,\mathbb{Z}_p\,,\,F\,)} M\Big(coker(\mathbb{Z}_p \to F)\Big)$$

Proof of First Main Theorem (cont'd)

Corollary

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F)$$

Proof of First Main Theorem (cont'd)

Corollary

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F)$$

Proof.

$$dd^*M(F) = \frac{1}{|F|}M(F) + \textit{lower order terms} \ldots$$

with respect to the partial ordering, where $F' \leq F$ iff F' is a quotient of F.

Proof of First Main Theorem (cont'd)

Corollary

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F)$$

Proof.

$$dd^*M(F) = \frac{1}{|F|}M(F) + \textit{lower order terms} \ldots$$

$$\Rightarrow$$

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F) + \textit{lower order terms} \ldots$$

Proof of First Main Theorem (cont'd)

Corollary

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F)$$

Proof.

$$dd^*M(F) = \frac{1}{|F|}M(F) + \textit{lower order terms ...}$$

$$\Rightarrow$$

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F) + \textit{lower order terms ...}$$

$$\Rightarrow$$

$$dd^*\mathcal{U}(1_F) = \frac{1}{|F|}\mathcal{U}(1_F)$$

Proof of Second Main Theorem

Theorem

The orthogonal complement of the E_F *in* $L^2(X_0, \mu_0)$ *is* $ker(dd^*) \cap L^2(X_0, \mu_0)$.

Proof of Second Main Theorem

Theorem

The orthogonal complement of the E_F in $L^2(X_0, \mu_0)$ is $ker(dd^*) \cap L^2(X_0, \mu_0)$.

Proof.

We compute the asymptotics of $(dd^*)^N(\nu)$ where ν is finitely supported. □

Proof of Second Main Theorem

Theorem

The orthogonal complement of the E_F in $L^2(X_0, \mu_0)$ is $ker(dd^*) \cap L^2(X_0, \mu_0)$.

Proof.

We compute the asymptotics of $(dd^*)^N(\nu)$ where ν is finitely supported. □

Lemma

The dominant term of $(dd^*)^N(\nu)$ is a linear combination of the $M(F)$'s.

"Application"

For all G,

$$\frac{|Aut(G \times \mathbb{Z}/p\mathbb{Z})|}{|Aut(G)|} =$$

"Application"

For all G,

$$\frac{|Aut(G \times \mathbb{Z}/p\mathbb{Z})|}{|Aut(G)|} =$$

$$= \frac{1}{p}\Big(|Hom(G \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})| - |Hom(G \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z})|\Big)$$

Thank you!