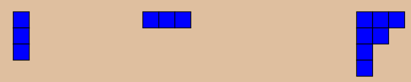
A random walk on finite abelian p-groups

Nikita Lvov

Background: Random p-groups from Random Matrices

Finite abelian p-groups can be represented as partitions:

$$\mathbb{Z}/p^3\mathbb{Z}, \quad \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}, \quad \mathbb{Z}/p^4\mathbb{Z}\times\mathbb{Z}/p^2\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$$

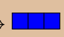


How to model a random p-group?

Take N generators and N random relations. Take the finite p-part.

Example. ($p = 2$) 4 generators and 4 relations:

$$\begin{array}{ccccccccc} 8x_1 & + & 7x_2 & + & 4x_3 & + & 9x_4 & = & 0 \\ 2x_1 & + & 1x_2 & + & 6x_3 & + & 3x_4 & = & 0 \\ 8x_1 & + & 4x_2 & + & 0x_3 & + & 2x_4 & = & 0 \\ 6x_1 & + & 7x_2 & + & 4x_3 & + & 1x_4 & = & 0 \end{array} \xrightarrow[\text{by the relations}]{\text{quotient of generators}} \mathbb{Z}/167\mathbb{Z}\times(\mathbb{Z}/2\mathbb{Z})^3 \xrightarrow{\text{2-part}}$$



This is a ***random matrix*** model for random abelian p-groups.

Theorem 1 (Cohen-Lenstra, Friedman-Washington, Maples, Wood). *[CL84] [FW89] [Map13] [Woo19] Suppose the coefficients are non-degenerate iid rv's [a]. As $N \to \infty$, we get a limiting probability distribution on finite abelian p-groups that satisfies*

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

Motivation. Modelling class groups of quadratic fields.

[a] Degenerate: constant modulo p

The Markov Chain

Motivation. Understanding Theorem 1. Why does limiting behaviour not depend on distribution of entries?

Idea. Get more insight by studying groups associated to submatrices of random matrices.

Infinite random matrix

↓

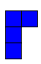
Random process valued in p-groups

Example. (See example on the right) The group in the $(3,3)$ entry is generated by the relations:

$$\begin{array}{ccccccc} 8x_1 & + & 7x_2 & + & 4x_3 & = & 0 \\ 2x_1 & + & 1x_2 & + & 6x_3 & = & 0 \\ 8x_1 & + & 4x_2 & + & 0x_3 & = & 0 \end{array}$$

It is the group:

$$\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \to$$



We restrict to the diagonal and the off-diagonal, as shown by the arrows in the diagram of the example on the right:

Theorem 2. *The diagonal/off-diagonal process converges to a Markov chain when entries are non-degenerate iid rv's.*

Explicitly, this Markov chain is given as follows:

- Vertical arrow: mod out by a uniformly random element.
- Horizontal arrow: cross with $\mathbb{Z}/p^k\mathbb{Z}$, then mod out by a uniformly random element. Take limit as $k \to \infty$.

* * *

[CL84] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. In Hendrik Jager, editor, *Number Theory Noordwijkerhout 1983*, pages 33–62, Berlin, Heidelberg, 1984. Springer Berlin Heidelberg.

[FW89] Eduardo Friedman and Lawrence C. Washington. On the distribution of divisor class groups of curves over a finite field. 1989.

[Map13] Kenneth Maples. Cokernels of random matrices satisfy the Cohen-Lenstra heuristics. *arXiv*, math.CO/1301.1239, 2013.

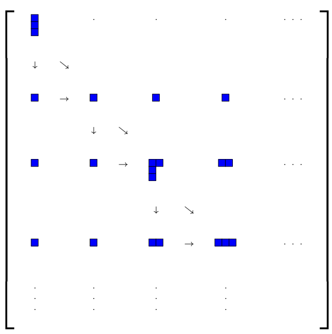
[Woo19] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. *American Journal of Mathematics*, 141(2):383–398, 2019.

Example

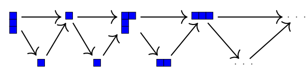
$$\begin{bmatrix} 8 & 7 & 4 & 9 & \dots \\ 2 & 1 & 6 & 3 & \dots \\ 8 & 4 & 0 & 2 & \dots \\ 6 & 7 & 4 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

($p = 2$)

↓



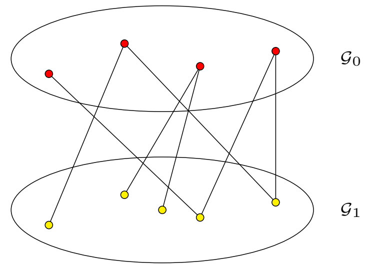
Sample path:



The Weighted Graph Γ

The Markov chain in Theorem 2 can be represented by a random walk on a weighted graph.

A Bipartite Graph



- Vertices: finite abelian p-groups (2 copies.)
- Edges:

$$0 \to G_1 \to G_0 \xrightarrow{\phi} \mathbb{Q}/\mathbb{Z}$$

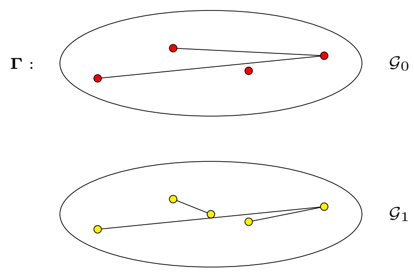
(Edge between G_1 and G_0)

- Weights:

$$\frac{1}{\left|G_1\right|\left|\#Aut\left(G_0 \xrightarrow{\phi} \mathbb{Q}/\mathbb{Z}\right)\right|}$$

Graph Γ:

Definition. Take the square of the bipartite graph above. This gives two connected weighted graphs:



Define Γ to be the $\mathcal{G}_0$ component.

Spectrum of Γ

Γ has nice properties, which allow us to determine its spectrum. Consider the Hilbert space $L^2(\Gamma)$ of real-valued functions on Γ, together with the natural inner product.

Example. This Hilbert space contains the following functions:

- Finitely supported functions.
- $G \mapsto 1$.
- $G \mapsto \#Sur(G, F)$, the number of surjective homomorphisms to F, for any finite abelian group F.

Theorem. (Theorem-definition) There exists a unitary operator $\mathcal{U}$ on the Hilbert space $L^2(\Gamma)$ and a constant C such that

$$\mathcal{U}\Big[\#Sur(F, \cdot)\Big] = C\#Sur(\cdot, F)$$

Definition. $\mathbf{\Delta_\Gamma} \stackrel{\text{def}}{=\!=}$ Laplacian of $\mathbf{\Gamma}$

Theorem. .

$$\mathcal{U}^{-1}\Delta_\Gamma\,\mathcal{U} \text{ is diagonal}$$

Furthermore, the diagonal entries are $\frac{1}{|G|} - 1$.