Computing Orbital Integrals as Local Densities

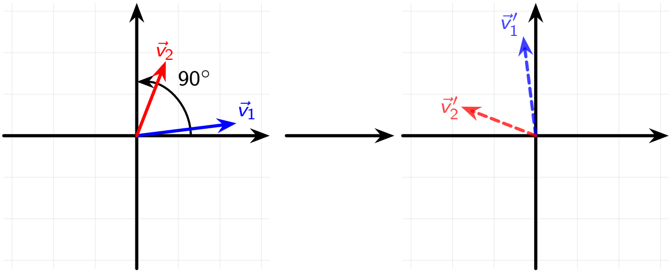
Michael Middlezong, Lucas Qi
Mentor: Thomas Rüd

MIT PRIMES Conference 2025

October 18, 2025

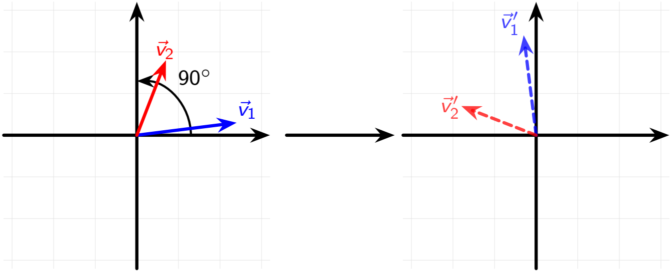
Introducing the problem

Consider this linear transformation on $\mathbb{R}^2$:



Introducing the problem

Consider this linear transformation on $\mathbb{R}^2$:



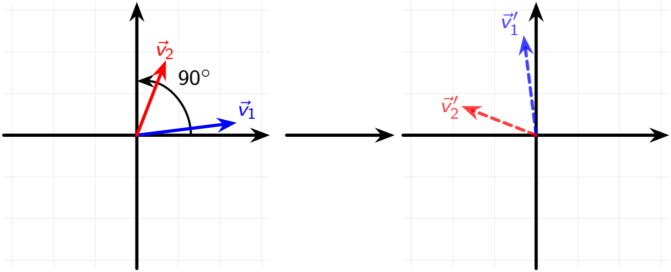
Good basis: $\{(1,0),(0,1)\}$

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

All coefficients are integers.

Introducing the problem

Consider this linear transformation on $\mathbb{R}^2$:



Good basis: $\{(1,0),(0,1)\}$

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

All coefficients are integers.

Bad basis: $\{(2,0),(0,1)\}$

$$\begin{pmatrix} 0 & \boxed{-1/2} \\ 2 & 0 \end{pmatrix}$$

Not an integer!

Introducing the problem

Question

Given a linear transformation, what is the probability that a random basis is "good" (associated matrix has integer coefficients)?

Introducing the problem

Question

Given a linear transformation, what is the probability that a random basis is "good" (associated matrix has integer coefficients)?

Probability $\implies$ need a measure on the set of bases.
However, in $\mathbb{R}$, the probability will always be 0. The problem is more interesting in $\mathbb{Q}_p$.

p-adic integers

Definition

The set of p-adic integers, denoted $\mathbb{Z}_p$, is the ring of infinite power series

$$\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} a_i p^i \right\}$$

with $0 \leq a_i < p$ for each i.

p-adic integers

Definition

The set of p-adic integers, denoted $\mathbb{Z}_p$, is the ring of infinite power series

$$\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} a_i p^i \right\}$$

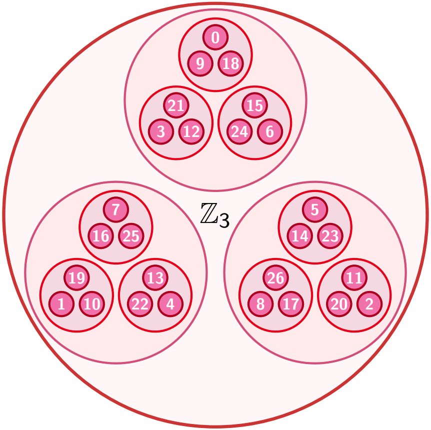
with $0 \leq a_i < p$ for each i.

Remark

We can see p-adic integers as having a base-p representation that extends infinitely to the left:

$$\ldots \overline{a_2 a_1 a_0} = a_0 + a_1 p + a_2 p^2 + \ldots$$

Illustration of p-adic integers



p-adic numbers

Definition

The field of p-adic numbers, denoted $\mathbb{Q}_p$, is the field of fractions of $\mathbb{Z}_p$. Consequently, every element of $\mathbb{Q}_p$ can be represented as follows:

$$\mathbb{Q}_p = \left\{ \sum_{i=m}^{\infty} a_i p^i \right\}$$

where $m \in \mathbb{Z}$ (notably, m can be negative) and $0 \leq a_i < p$.

p-adic measures

When a topological group (like $\mathbb{Q}_p$) satisfies certain conditions (locally compact and Hausdorff), it admits a translation-invariant measure known as a **Haar measure** which is unique up to scaling.

Definition

Let μ be the Haar measure of $\mathbb{Q}_p$ normalized so that $\mu(\mathbb{Z}_p) = 1$. This is the **canonical measure** on $\mathbb{Q}_p$.

Returning back to our illustration...

Returning to the problem

Question

Given a linear transformation, what is the probability that a random basis is "good" (associated matrix has integer coefficients)?

Returning to the problem

Question

Given a linear transformation, what is the probability that a random basis is "good" (associated matrix has integer coefficients)?

- Fix a linear transformation.
- Each basis gives rise to a matrix.
- How do we know which matrices can arise?

Returning to the problem

Question

Given a linear transformation, what is the probability that a random basis is "good" (associated matrix has integer coefficients)?

- Fix a linear transformation.
- Each basis gives rise to a matrix.
- How do we know which matrices can arise?

Definition

Given a matrix $\gamma \in \mathrm{GL}_n(\mathbb{Q}_p)$, the set of matrices that you can get by using different bases is called the **orbit** of γ, denoted by $\mathrm{Orb}(\gamma)$.

Returning to the problem

Question

Given a linear transformation, what is the probability that a random basis is "good" (associated matrix has integer coefficients)?

- Fix a linear transformation.
- Each basis gives rise to a matrix.
- How do we know which matrices can arise?

Definition

Given a matrix $\gamma \in \mathrm{GL}_n(\mathbb{Q}_p)$, the set of matrices that you can get by using different bases is called the **orbit** of γ, denoted by $\mathrm{Orb}(\gamma)$.

Goal: define a measure on $\mathrm{Orb}(\gamma)$.

Characteristic polynomials

A matrix's **characteristic polynomial** is invariant under basis change.

Characteristic polynomials

A matrix's **characteristic polynomial** is invariant under basis change.

Example

In GL_2, characteristic polynomials are determined by trace and determinant:

$$\chi_\gamma(x) = x^2 - \mathrm{tr}(\gamma)x + \det(\gamma).$$

Characteristic polynomials

A matrix's **characteristic polynomial** is invariant under basis change.

Example

In GL_2, characteristic polynomials are determined by trace and determinant:

$$\chi_\gamma(x) = x^2 - \mathrm{tr}(\gamma)x + \det(\gamma).$$

Proposition

For *almost all* matrices, the orbit of a matrix is *precisely* the set of matrices with the same characteristic polynomial.

Quotient measure

$$\frac{\text{measure on } \mathrm{GL}_n}{\text{measure on } \underbrace{\text{set of char polys}}_{\mathbb{A}_{\mathrm{GL}_n}}} = \text{measure on } \mathrm{Orb}(\gamma)$$

Quotient measure

$$\frac{\text{measure on } \mathsf{GL}_n}{\text{measure on } \underbrace{\text{set of char polys}}_{\mathbb{A}_{\mathsf{GL}_n}}} = \text{measure on } \mathrm{Orb}(\gamma)$$

This way of defining a measure leads to the **geometric measure**, denoted by μ^{geom}.

Quotient measure

$$\frac{\text{measure on } \mathsf{GL}_n}{\text{measure on } \underbrace{\text{set of char polys}}_{\mathbb{A}_{\mathsf{GL}_n}}} = \text{measure on Orb}(\gamma)$$

This way of defining a measure leads to the **geometric measure**, denoted by μ^{geom}.

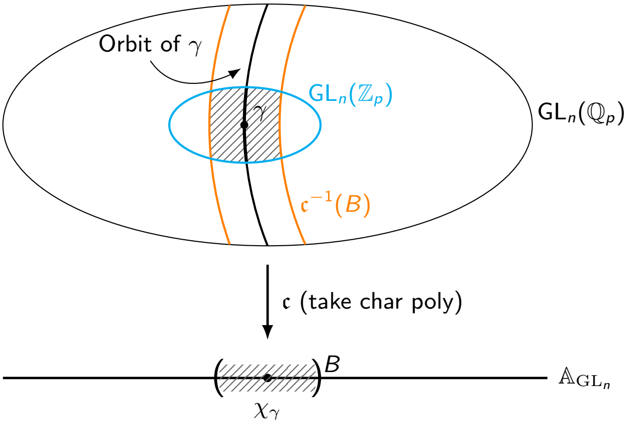
Problem

Compute

$$\int_{\mathrm{Orb}(\gamma)} \mathbb{1}_{\mathsf{GL}_n(\mathbb{Z}_p)}\, d\mu^{\mathrm{geom}}.$$

Illustration of the geometric measure

$$\int_{\mathrm{Orb}(\gamma)} \mathbb{1}_{\mathrm{GL}_n(\mathbb{Z}_p)}\, d\mu^{\mathrm{geom}} = \lim_{B \to \{\chi_\gamma\}} \frac{\mathrm{vol}_{\mathrm{GL}_n(\mathbb{Q}_p)}(\mathfrak{c}^{-1}(B) \cap \mathrm{GL}_n(\mathbb{Z}_p))}{\mathrm{vol}_{\mathbb{A}_{\mathrm{GL}_n}}(B)}$$



Local ratios

Let $\gamma \in \mathrm{GL}_n(\mathbb{Z}_p)$. Define

$$\nu_k(\gamma) = \frac{\#\{h \in \mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z}) \colon \chi_h \equiv \chi_\gamma \bmod p^k\}}{\underbrace{\#\,\mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})/\#\mathbb{A}_{\mathrm{GL}_n}(\mathbb{Z}/p^k\mathbb{Z})}_{\text{normalizing factor}}}.$$

Local ratios

Let $\gamma \in \mathrm{GL}_n(\mathbb{Z}_p)$. Define

$$\nu_k(\gamma) = \frac{\#\{h \in \mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})\colon \chi_h \equiv \chi_\gamma \bmod p^k\}}{\underbrace{\#\,\mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})/\#\mathbb{A}_{\mathrm{GL}_n}(\mathbb{Z}/p^k\mathbb{Z})}_{\text{normalizing factor}}}.$$

Theorem (Achter–Gordon, 2017)

In GL_2, the ratios converge to the orbital integral (up to a constant):

$$\lim_{k\to\infty} \nu_k(\gamma) = (*) \cdot \int_{\mathrm{Orb}(\gamma)} \mathbb{1}_{\mathrm{GL}_2(\mathbb{Z}_p)}\, d\mu^{\mathrm{geom}}.$$

Research questions

- Can local ratios be used to compute orbital integrals in GL_n and SL_n?
- Can we compute orbital integrals where the test function $\mathbb{1}_{\mathrm{GL}_n(\mathbb{Z}_p)}$ is different?

Conjugacy is different in SL_n

Example (SL_2 conjugacy is stricter)

The $\mathrm{SL}_2(\mathbb{R})$ matrices $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ have the same trace and determinant, but are not conjugate by an element of $\mathrm{SL}_2(\mathbb{R})$.

Proof. Suppose $M \in \mathrm{SL}_2(\mathbb{C})$ satisfies

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = M^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} M.$$

Rearranging, we have

$$M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} M.$$

Conjugacy is different in SL_n

Now, setting $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and multiplying yields

$$\begin{pmatrix} -b & a \\ -d & c \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix},$$

so $a = -d$ and $b = c$. Since M has determinant 1, we have

$$ad - bc = -a^2 - b^2 = 1 \implies a^2 + b^2 = -1.$$

Therefore, M cannot have all real entries. $\square$

Summary of our results

- We showed local ratios converge to orbital integrals in GL_n (up to a constant).

Theorem (Middlezong–Qi–Rüd, 2025)

In $\mathrm{GL}_n(\mathbb{Q}_p)$, the local densities converge as follows:

$$\lim_{k\to\infty} \nu_k(\gamma) = \frac{p^{n^2-1}}{\#\,\mathrm{SL}_n(\mathbb{F}_p)} \cdot \int_{\mathrm{Orb}(\gamma)} \mathbb{1}_{\mathrm{GL}_n(\mathbb{Z}_p)}\, d\mu^{\mathrm{geom}}.$$

Summary of our results

- We extended the method from integer test functions to bi-$\mathrm{GL}_n(\mathbb{Z}_p)$-invariant test functions.

Theorem (Middlezong–Qi–Rüd, 2025)

Let γ be an element of $S = \mathrm{GL}_n(\mathbb{Z}_p)\,\mathrm{diag}(p^{\lambda_1}, \ldots, p^{\lambda_n})\,\mathrm{GL}_n(\mathbb{Z}_p)$, where $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$. Then,

$$\lim_{k\to\infty} \nu_k(\gamma) = p^{-(n-1)(\lambda_1+\cdots+\lambda_n)} \cdot \frac{p^{n^2-1}}{\#\,\mathrm{SL}_n(\mathbb{F}_p)} \int_{\mathrm{Orb}(\gamma)} \mathbb{1}_S \, d\mu^{\mathrm{geom}}.$$

Summary of our results

- We defined a local ratio for SL_n using an additional conjugacy criterion. In SL_2, we showed that this ratio converges to the orbital integral, and we also provide the explicit factor needed to convert to the orbital integral using the canonical measure.

Theorem (Middlezong–Qi–Rüd, 2025)

The SL_2 ratios are related to the canonical measure orbital integral $O^{\mathrm{can}}(\gamma)$ by the following:

$$\lim_{k\to\infty} \nu_k^{\mathrm{SL}_2}(\gamma) = p^{-\delta} \cdot O^{\mathrm{can}}(\gamma) \cdot \begin{cases} \frac{p}{p-1}, & \chi = 1 \quad \text{(hyperbolic)}, \\ 1, & \chi = 0 \quad \text{(ramified elliptic)}, \\ \frac{p}{p+1}, & \chi = -1 \quad \text{(unramified elliptic)}. \end{cases}$$

Here, δ and χ are values that depend on γ.

Acknowledgments

We would like to thank:

- Dr. Thomas Rüd for his mentorship and guidance throughout the project.
- Dr. Eran Assaf for his valuable feedback on our presentation.
- The MIT PRIMES-USA program for making this project possible and hosting the PRIMES Conference.

References

Jeffrey D. Achter and Julia Gordon, *Elliptic curves, random matrices and orbital integrals*, Pacific J. Math. **286** (2017), no. 1, 1–24, With an appendix by S. Ali Altuğ. MR 3582398