What can automorphic forms tell us about algorithmic problems?

Aurel Page
Inria / IMB Bordeaux

07/07/2026
ANTS XVII – Groningen

Funded by
the European Union

Plan

Automorphic forms

Automorphic forms, in textbooks

$\mathbb{G}/\mathbb{Q}$ reductive group, $\mathbb{A} = \prod'_v \mathbb{Q}_v$ ring of adèles.

Definition:
A function $\varphi\colon \mathbb{G}(\mathbb{Q})\backslash\mathbb{G}(\mathbb{A}) \to \mathbb{C}$ is an **automorphic form** if:

- φ is smooth of moderate growth,
- φ is K-finite,
- φ is $Z(\mathfrak{g})$-finite (satisfies some differential equations).

Automorphic forms, in textbooks

$\mathbb{G}/\mathbb{Q}$ reductive group, $\mathbb{A} = \prod'_v \mathbb{Q}_v$ ring of adèles.

Definition:
A function $\varphi\colon \mathbb{G}(\mathbb{Q})\backslash\mathbb{G}(\mathbb{A}) \to \mathbb{C}$ is an **automorphic form** if:

- φ is smooth of moderate growth,
- φ is K-finite,
- φ is $Z(\mathfrak{g})$-finite (satisfies some differential equations).

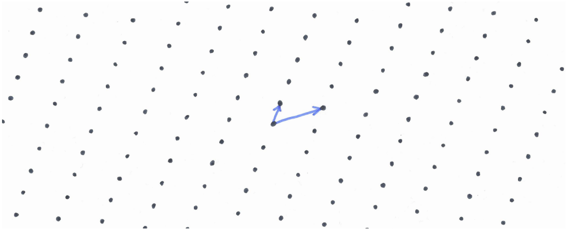
This definition looks very far from the computable world!

Euclidean lattices

Definition: A **Euclidean lattice** of rank n is an

$$L = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$$

where $b_1, \ldots, b_n$ is a basis of $\mathbb{R}^n$.



Two lattices L, L' are **similar** if $L \rightsquigarrow L'$ by Euclidean isometry and scaling.

The space of lattices

Guiding principle

Make a space of the objects you study, and study that space.

Definition: The **space X_n of lattices** of rank n is

$$X_n = \mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{GL}_n(\mathbb{R}) / \mathrm{O}_n(\mathbb{R})\mathbb{R}_{>0}.$$

The space of lattices

Guiding principle

Make a space of the objects you study, and study that space.

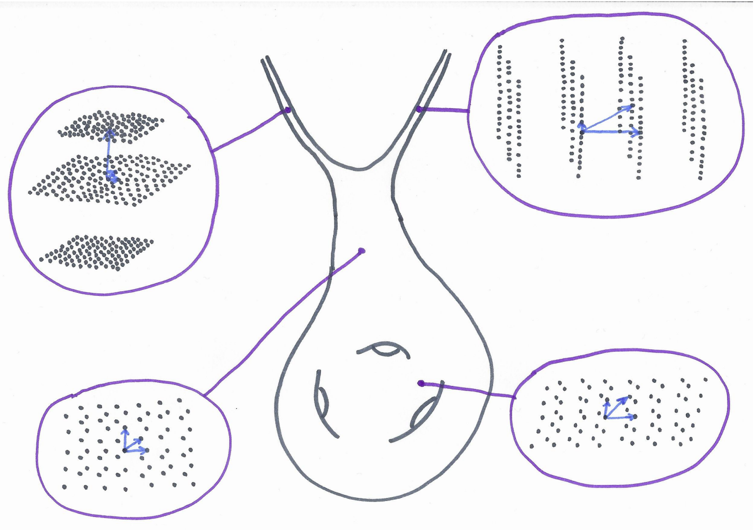
Definition: The **space X_n of lattices** of rank n is

$$X_n = \mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{GL}_n(\mathbb{R}) / \mathrm{O}_n(\mathbb{R})\mathbb{R}_{>0}.$$

Structure:

- manifold, finite dimension, noncompact;
- Haar measure μ, finite $\mu(X_n)$;
- decomposition according to lattice balancedness.

The space of lattices



Variants

Generalise to **lattices with extra data** $(L, \alpha_1, \dots, \alpha_k)$:

- α_i bilinear form or ring structure compatible with Euclidean structure;
- isomorphisms should preserve the α_i ($\rightsquigarrow \mathbb{G}$).

Example:

$X(\mathcal{O})$: finite set of right $\mathcal{O}$-ideals up to $B^\times$-multiplication, where $\mathcal{O}$ order in definite quaternion algebra B.

$X(\mathcal{O}) =$ space of (L, α) where $\alpha \colon \mathcal{O} \to \mathrm{End}(L)$ compatible: adjoint = quaternionic involution.

Automorphic forms, more concretely

"Definition": an **automorphic form** is a "nice" function on a space X of lattices.

Examples:

- Constant functions are automorphic.
- $\dim X = 0$: every function is automorphic.
- X compact: automorphic forms are dense in $L^2(X)$.
- $X_2 = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$: hyperbolic Laplace operator

$$\Delta = -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right);$$

  bounded eigenfunctions of Δ are automorphic;
  eigenfunction y^s with eigenvalue $s(1-s)$ for $s \in \mathbb{C}$,
  average to make $\mathrm{SL}_2(\mathbb{Z})$-invariant $\rightsquigarrow E_s$ (Eisenstein series).

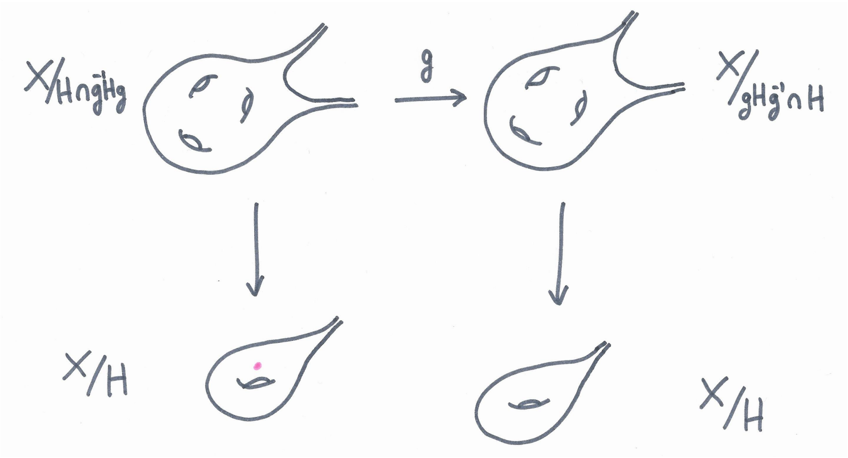
Hecke operators, theoretically

Group theory:
Group G acting on set X (resp. module M), subgroup $H \subset G$.

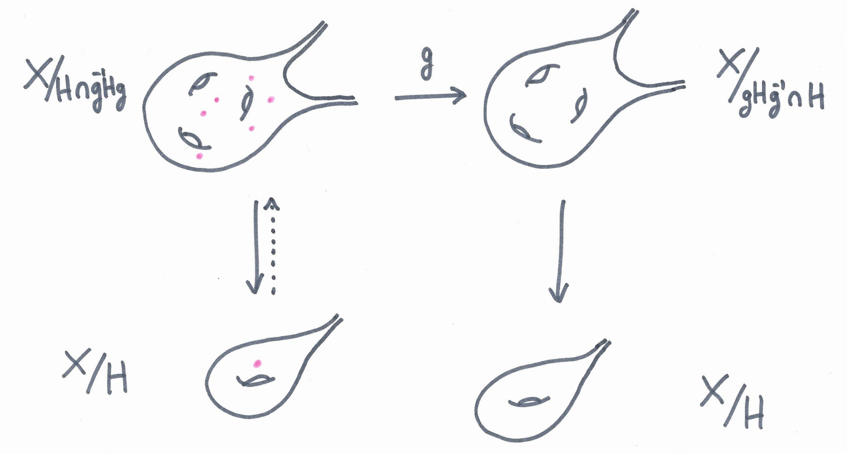
Hecke operators are what remains of the G-action on X/H (resp. on fixed points M^H).

Our context: prime p, group $G = \mathbb{G}(\mathbb{Q}_p)$, compact open H.
$\rightsquigarrow$ Hecke operators T_p at p.

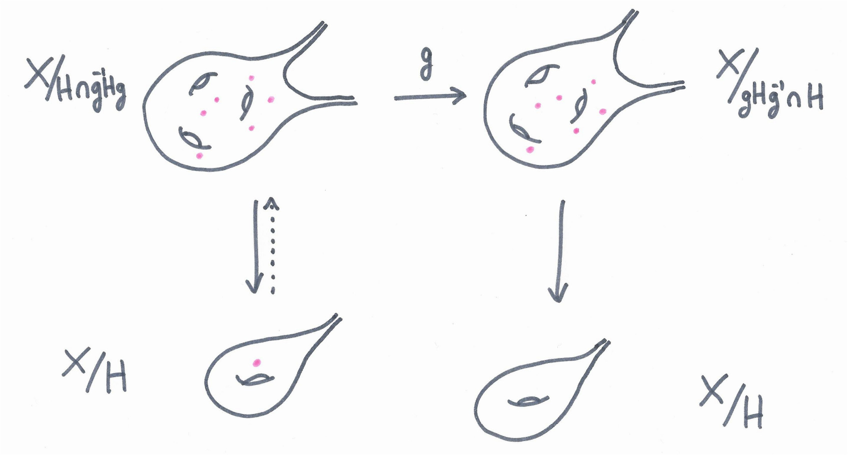
Hecke operators, geometrically



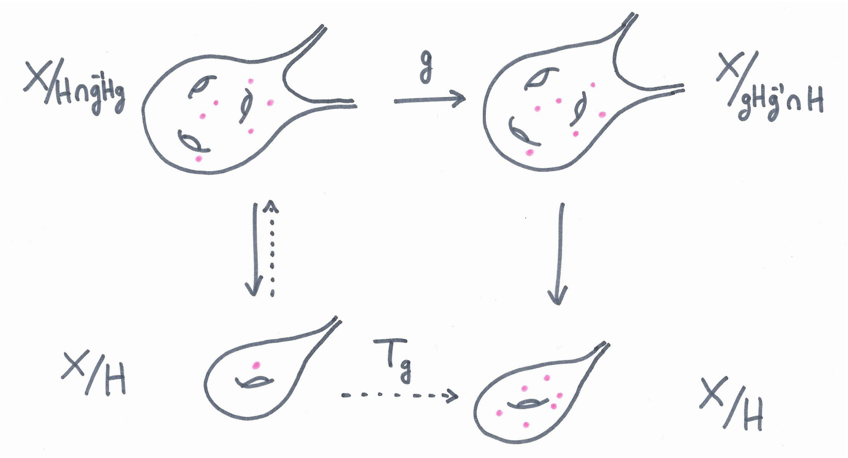
Hecke operators, geometrically



Hecke operators, geometrically



Hecke operators, geometrically



Hecke operators, concretely

Hecke operators have **concrete and natural incarnations**:

- Kneser-type **neighbours.**

  Example for X_n:
  $T_p \colon L \mapsto$ all sublattices $L' \subset L$ of index p.
- If abelian varieties connection, **isogenies.**

  Example for $X(B_{p,\infty})$:
  $T_\ell \colon E \mapsto$ all E' with $E \to E'$ an ℓ-isogeny.

Can often **transfer solutions** of algorithmic problems.

Spectral decomposition

Hecke spectrum on $L^2(X)$ in terms of automorphic forms.

Recall **Fourier theory**:

- $L^2(\mathbb{R}/\mathbb{Z}) = \hat{\bigoplus}_m \mathbb{C}(x \mapsto e^{2\pi i m x})$ discrete spectrum.
- $L^2(\mathbb{R}) \rightsquigarrow (x \mapsto e^{ix\xi}) \notin L^2(\mathbb{R})$, $\xi \in \mathbb{R}$ continuous spectrum.

Langlands decomposition:

$$\begin{aligned} L^2(X) &= L^2_{\mathrm{disc}}(X) \oplus L^2_{\mathrm{cont}}(X) \\ &= L^2_{\mathrm{res}}(X) \oplus L^2_{\mathrm{cusp}}(X) \oplus L^2_{\mathrm{cont}}(X). \end{aligned}$$

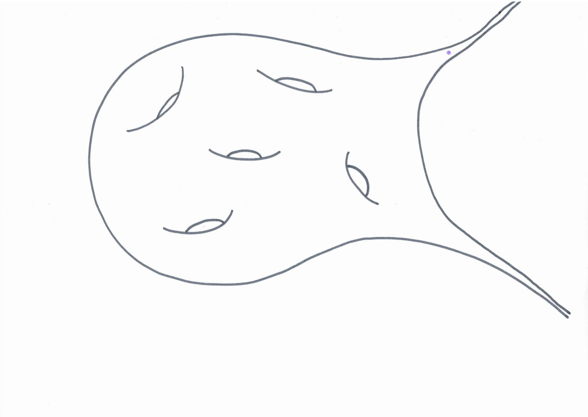
- $\mathbf{1} \in L^2_{\mathrm{res}}(X)$.
- Eisenstein series contribute to $L^2_{\mathrm{res}}(X)$ and $L^2_{\mathrm{cont}}(X)$.
- $L^2_{\mathrm{cusp}}(X)$ is nice (Ramanujan conjecture).

Equidistribution

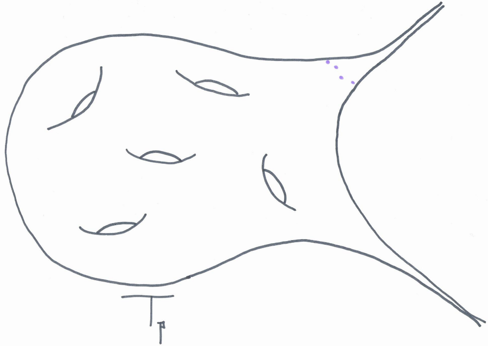
Let $x \in X$.
The **Hecke orbit** $T_p \cdot x \subset X$ **equidistributes** as $p \to \infty$.

(under mild hypotheses)

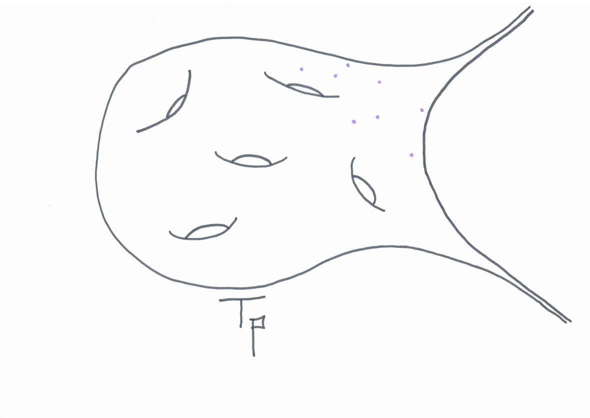
Equidistribution



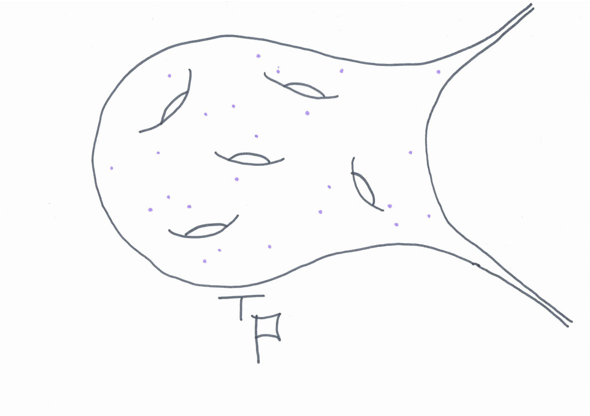
Equidistribution



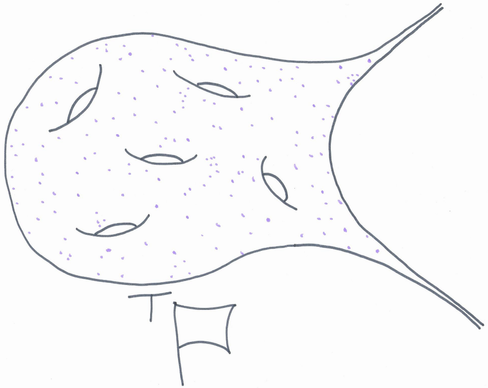
Equidistribution



Equidistribution



Equidistribution



Equidistribution

Spectral analysis:

$$L^2(X) = \mathbb{C}\mathbf{1} \oplus L^2_0(X) \text{ orthogonal decomposition.}$$

Write $T_p^0 =$ restriction of T_p to $L^2_0(X)$:

$$T_p\mathbf{1} = (\deg T_p)\mathbf{1} \qquad \text{and} \qquad \frac{T_p^0}{\deg T_p} \xrightarrow[p\to\infty]{} 0.$$

$f \in L^2(X, \mathbb{R})$ probability density: $\langle f, \mathbf{1} \rangle = 1$

$$\Longrightarrow \left\| \frac{T_p}{\deg T_p} f - \mathbf{1} \right\|_2 = \left\| \frac{T_p^0}{\deg T_p}(f - \mathbf{1}) \right\|_2 \xrightarrow[p\to\infty]{} 0.$$

Algorithmic problems

Motivation

For cryptography, we need algorithmic problems that are **hard.**

Motivation

For cryptography, we need algorithmic problems that are **hard** for a **random instance.**

There exist NP-hard problems that are easy on average (SAT).

Worst-case complexity $\rightsquigarrow$ **average complexity.**

Setup

Consider:

- a set X of instances,
- an algorithmic problem $\mathcal{P}$,
- a **probability distribution** μ on X.

Question: can $\mathcal{P}$ be solved **efficiently on average** on X?

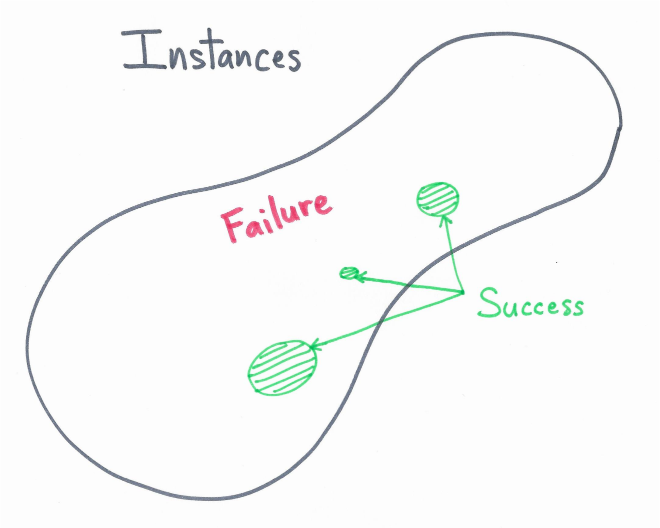
Efficiency on average

Definition:
An algorithm is **efficient on average** if

- it runs in polynomial time, and
- it solves $\mathcal{P}$ on a set of measure $\geq 1/\mathrm{poly}(\mathrm{size})$.

The algorithm does not know whether the instance it receives has been drawn at random or not!

Efficiency on average



How to prove that a problem is hard?

Very difficult!

- Consider the best algorithms you have.
- Identify some weak instances.
- **Compare problems**: prove reductions.

How to prove that a problem is hard?

Very difficult!

- Consider the best algorithms you have.
- Identify some weak instances.
- **Compare problems**: prove reductions.

To prove $\mathcal{P}_1$ easier than $\mathcal{P}_2$:

- assume access to an **oracle** $\mathbf{O}_{\mathcal{P}_2}$ that solves $\mathcal{P}_2$;
- use it in an efficient algorithm that solves $\mathcal{P}_1$.

We allow calling $\mathbf{O}_{\mathcal{P}_2}$ many times, with computations in between.

Close distributions

What happens if the distribution f of inputs is not exactly the correct distribution g?

The **statistical distance** $\|f - g\|_1$ bounds the change of probability of any subset of X.

Automorphic forms as a toolbox

Study **algorithmic problems** on X:

- relate instances using **Hecke operators**,
- use **equidistribution** or other properties,
- and add more work! No magic wand.
- $\|\cdot\|_1 \leq \|\cdot\|_2$ by Cauchy–Schwartz.

Applications

Isogeny problems:
$\mathcal{P}_1$ = EndRing: given $E/\mathbb{F}_{p^2}$ supersingular, compute $\mathrm{End}(E)$.
$\mathcal{P}_2$ = OneEnd: given E, compute some $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

Theorem (P.–Wesolowski 2024)

$\mathcal{P}_1$ and $\mathcal{P}_2$ are equivalent.

Lattice problems: next section.

Average hardness of lattice problems

joint with K. de Boer, R. Toma and B. Wesolowski

Lattice problems

L lattice.

$$\det(L) = \mathrm{Vol}(\mathbb{R}^n/L)$$

$$\lambda_i(L) = \inf\{r : \dim \mathrm{Span}_{\mathbb{R}}(L \cap B(r)) \geq i\}.$$

Theorem (Minkowski)

$\lambda_1(L) \leq \sqrt{n}\det(L)^{\frac{1}{n}}$.

Problem (Shortest Vector Problem: SVP)

Given L, find a nonzero $v \in L$ with $\|v\| \leq \lambda_1(L)$.

Lattice problems

L lattice.

$$\det(L) = \mathrm{Vol}(\mathbb{R}^n/L)$$

$$\lambda_i(L) = \inf\{r : \dim \mathrm{Span}_{\mathbb{R}}(L \cap B(r)) \geq i\}.$$

Theorem (Minkowski)

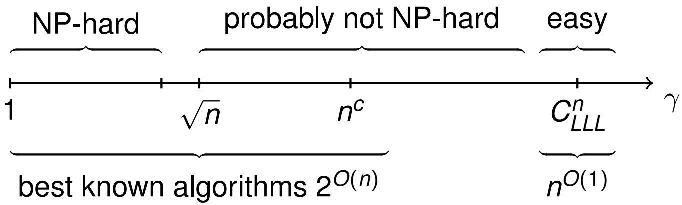
$\lambda_1(L) \leq \sqrt{n}\det(L)^{\frac{1}{n}}$.

Problem (Shortest Vector Problem: γ-SVP)

Given L, find a nonzero $v \in L$ with $\|v\| \leq \gamma\lambda_1(L)$.

Hardness of lattice problems

Depending on the approximation factor γ:



Average hardness of lattice problems

Easy instances:
If $\lambda_1(L) < \lambda_2(L)/C_{LLL}^n$ then LLL solves SVP in polynomial time.

Reductions:

- First average-case hardness: Ajtai 1996.
  Ad hoc distribution, not dimension preserving.
- Ideal lattices: dBDPMW 2020.
  Haar measure distribution, dimension preserving.

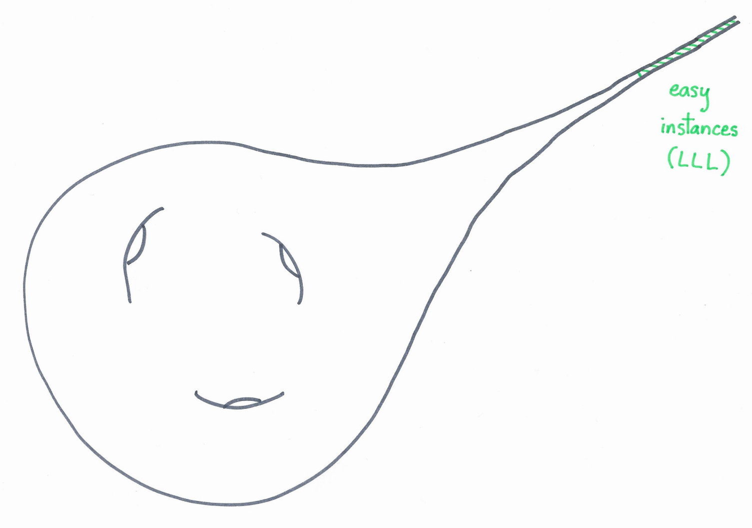
Haar measure distribution

Goal: prove hardness for the Haar measure distribution.

Properties of the Haar measure:

- $\lambda_i(L) \approx \sqrt{n}\,\det(L)^{\frac{1}{n}}$ with proba ≈ 1.
- identified easy instances are **rare**: proba $\leq 2^{-cn}$.

Haar measure distribution



Strategy

Goal: prove $\mathrm{SVP} \leq \mathrm{avgSVP}$.

Assume oracle $\mathbf{O}_{\mathrm{avgSVP}}$ solves γ-SVP efficiently **on average**.

Algorithm:

- Input: lattice L.
- Output: $v \in L$.

1. Pick prime p.
2. $L' \leftarrow$ random sublattice of index p in L.
3. $v \leftarrow \mathbf{O}_{\mathrm{avgSVP}}(L')$
4. Output v.

Analysis: approximation factor

Question: How good is the output vector?

Measure of imbalancedness:

$$\alpha = \frac{\sqrt{n}\det(L)^{\frac{1}{n}}}{\lambda_1(L)} \geq 1.$$

Assume O$_{\mathrm{avgSVP}}$ successful on L' and the L' are Haar random:

$$\begin{aligned} \|v\| &\leq \gamma\lambda_1(L') \\ &\approx \gamma\sqrt{n}\det(L')^{\frac{1}{n}} \\ &= \gamma\sqrt{n}p^{\frac{1}{n}}\det(L)^{\frac{1}{n}} \\ &= \gamma\alpha p^{\frac{1}{n}}\lambda_1(L). \end{aligned}$$

Analysis: distribution

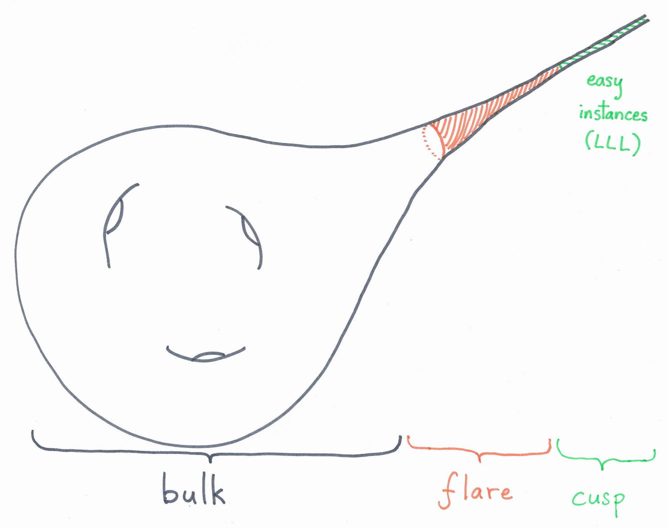
For distribution of L' close to Haar random:

- **Initial distribution** $f \in L^2(X)$ concentrated around L;
- estimate $\|f\|_2$;
- apply known bounds on Hecke eigenvalues.

Complications

- Bounds not good enough:
  ~~unstructured lattices~~ $\rightarrow$ **module lattices** of fixed rank.
- Imbalanced lattices:
  - ~~SVP~~ $\rightarrow$ **SIVP**;
  - **trichotomy**: bulk / flare / cusp.
- Discretisation.

Complications



Main result

Number field K: degree d, discriminant Δ_K.

Theorem (de Boer–Toma–P.–Wesolowski 2026)

Let $r \geq 1$. Assume GRH. Given an oracle **O** *for average γ-SIVP on module lattices of rank r, we can solve γ'-SIVP in the worst case for*

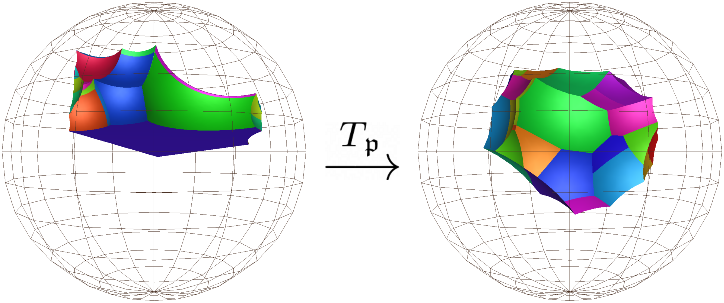
$$\gamma' = \mathrm{poly}_r(|\Delta_K|^{\frac{1}{d}}, n) \cdot \gamma,$$

using at most $\mathrm{poly}_r(\log|\Delta_K|)$ calls to **O***.*

- Side result: balancedness of random module lattices.
- Unexpected application: isomorphism between central simple algebras over $\mathbb{Q}$ of fixed dimension, given orders with factored discriminants.

Conclusion

I love Hecke operators!
Do you?



Thank you!

Remember:

- Automorphic form = nice function on a **space of lattices.**
- **Hecke operators** orbits **equidistribute.**
- $\to$ **prove reductions** between algorithmic problems.