

Hecke operators in algorithmic number theory

Habilitation à diriger des recherches

Aurel Page

03/06/25

Université de Bordeaux, Inria
Institut de Mathématiques de Bordeaux

Introduction

Academic career

Employment:

- 2017–present: Inria researcher, Université de Bordeaux
- 2014–2017: Research Fellow, University of Warwick
- 2014: PhD thesis

PhD supervision:

- starting in 2025: Rayane Bait (with N. Mascot), Alexander Wiesner (with B. Eick, K. Belabas and B. Allombert), Thibault Monneret (with B. Wesolowski)
- 2022–2025: Fabrice Étienne
- 2018–2021: Jean Kieffer (with D. Robert)

Research area

Algorithmic number theory:

- Number theory: questions about **integers** and **rational numbers**.
- Algorithmic: **algorithm** design and analysis, implementation, **computation**.

Focus on a tool: **Hecke operators**.

Ramanujan: 1916

$$\begin{aligned}\Delta &= q(1-q)^{24}(1-q^2)^{24}(1-q^3)^{24} \dots \\ &= q - 24q^2 + 252q^3 - 1472q^4 + \dots \\ &= \sum_{n \geq 1} \tau(n)q^n.\end{aligned}$$

From computing $\tau(1), \dots, \tau(30)$:

Conjecture (Ramanujan)

- $\tau(mn) = \tau(m)\tau(n)$ *whenever* $\gcd(m, n) = 1$
- $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$

Mordell: 1917

Proves Ramanujan's conjecture by using **modularity**:

$$\Delta(-1/z) = z^{12} \Delta(z)$$

where $q = \exp(2\pi iz)$ and $\operatorname{Re}(z) > 0$.

For each prime p , constructs a function φ by combining

$$\Delta(pz), \Delta(z/p), \Delta((z+1)/p), \dots, \Delta((z+p-1)/p),$$

proves that φ is again modular, and that this forces

$$\varphi = Q\Delta$$

for some constant Q .

Hecke: 1937

For each integer n , defines an **operator** T_n on modular forms of weight k :

$$T_n F(z) = n^{k-1} \sum_{\substack{a \cdot d = n \\ b \bmod d, d > 0}} F\left(\frac{az + b}{d}\right) d^{-k},$$

Derives many properties of these operators, and reproves Ramanujan's conjecture as a corollary of the identity:

$$T_n \Delta = \tau(n) \Delta \text{ for all } n.$$

Shimura: 1959

Revisits Hecke's operators: for certain groups $H \subset G$, defines a **ring** $\mathbb{Z}[H \backslash G / H]$ and **actions** of this ring on many structures:

- spaces of modular forms,
- cohomology groups,
- abelian varieties.

This is what we now call an **abstract Hecke ring**.

Hecke operators of finite groups

Notation for a set X : $\mathbb{Z}[X] = \bigoplus_{x \in X} \mathbb{Z}x$

Let G be a finite group: $\mathbb{Z}[G]$ is a ring.

A $\mathbb{Z}[G]$ -**module** is an abelian group W with an action of G by linear automorphisms.

Notation: the group of **fixed points** is

$$W^G = \{w \in W \mid gw = w \text{ for all } g \in G\}.$$

Hecke operators of finite groups

Let $H \subset G$ be a subgroup.

We have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], W) \cong W^H$$

given by $\varphi \mapsto \varphi(H)$.

This gives the **Hecke ring**

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G/H]) \cong \mathbb{Z}[G/H]^H \cong \mathbb{Z}[H \backslash G/H].$$

For every $T \in \mathbb{Z}[H \backslash G/H]$, we get a **Hecke operator**

$$T: W^H \longrightarrow W^H$$

by precomposition.

Hecke operators of arithmetic groups

Number theoretic versions: infinite groups.

- $G = \mathrm{GL}_r(\mathbb{Q}), H = \mathrm{GL}_r(\mathbb{Z}), T_n \leftrightarrow H \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} H;$
- $G = \mathrm{GL}_r(\mathbb{Q}_p), H = \mathrm{GL}_r(\mathbb{Z}_p);$
- $G = \mathrm{GL}_r(\mathbb{A}_f), H = \mathrm{GL}_r(\hat{\mathbb{Z}}).$

Hecke operators of arithmetic groups

Number theoretic versions: infinite groups.

- $G = \mathrm{GL}_r(\mathbb{Q}), H = \mathrm{GL}_r(\mathbb{Z}), T_n \leftrightarrow H \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} H;$
- $G = \mathrm{GL}_r(\mathbb{Q}_p), H = \mathrm{GL}_r(\mathbb{Z}_p);$
- $G = \mathbb{G}(\mathbb{A}_f), H = \mathbb{G}(\hat{\mathbb{Z}}).$

Algorithmic applications

- 1 Computational algebraic number theory
- 2 Spectral geometry
- 3 Cryptography

Computational algebraic number theory

Number fields and algebraic integers

A **number field** is a field of finite dimension over $\mathbb{Q}$.

Example: $F = \mathbb{Q}(\sqrt{-5}) = \mathbb{Q} + \mathbb{Q}\sqrt{-5}$.

Every number field F has a **ring of integers** $\mathbb{Z}_F$.

Example: $\mathbb{Z}_F = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

Unique factorisation can fail in number fields.

Example: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Replacement: unique factorisation of **ideals**.

Example: $(6) = (2, 1 + \sqrt{-5})^2 \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$.

Class groups

Failure is measured by the **class group**

$$\text{Cl}(F) = \frac{\{\text{nonzero ideals of } F\}}{\{\text{ideals of the form } (\alpha) \text{ for } \alpha \in F^\times\}},$$

which is a finite abelian group.

Problem

Given a number field F and its ring of integers $\mathbb{Z}_F$, compute the class group $\text{Cl}(F)$.

Buchmann's algorithm

S -units $\mathbb{Z}_{F,S}^\times =$ elements $\alpha \in F^\times$ such that the ideal (α) is a product of the primes in S .

Algorithm

- 1 Choose S set of prime ideals generating $\text{Cl}(F)$ (GRH).
- 2 Find some set S -units $R \subset \mathbb{Z}_{F,S}^\times$.
- 3 Compute $C = \mathbb{Z}^S / v_S(\langle R \rangle)$ and $U = \ker(v_S: \langle R \rangle \rightarrow \mathbb{Z}^S)$.
- 4 Check if $\langle R \rangle = \mathbb{Z}_{F,S}^\times$ using class number formula (GRH).
- 5 Output C .

Running time:

- Heuristic: $\exp(\tilde{O}(\log \Delta_F)^\gamma)$ for some $1/3 \leq \gamma \leq 2/3$.
- Practice: impossible for $\dim_{\mathbb{Q}} F > 150$.

Galois theory and Hecke operators

For every F :

- its Galois group G acts on its Galois closure $\tilde{F}$, and
- there is a subgroup $H \subset G$ such that $F = \tilde{F}^H$.

If $U \subset G$ is a subgroup, **Hecke operators** T give morphisms

$$T: (\tilde{F}^U)^\times \longrightarrow (\tilde{F}^H)^\times = F^\times.$$

More precisely, morphisms of algebraic groups

$$T: \operatorname{Res}_{\tilde{F}^U/\mathbb{Q}} \mathbb{G}_m \longrightarrow \operatorname{Res}_{F/\mathbb{Q}} \mathbb{G}_m.$$

Norm relations and S-units

Definition

G a finite group, subgroups $H \subset G$ and $U_1, \dots, U_k \subset G$. Say that G admits a **norm relation** with respect to $(U_1, \dots, U_k; H)$ if there exists a surjective morphism of $\mathbb{Q}[G]$ -modules

$$\bigoplus_i \mathbb{Q}[G/U_i]^{n_i} \longrightarrow \mathbb{Q}[G/H].$$

Proposition

If there is such a norm relation, then the image under Hecke operators of

$$\mathbb{Z}_{L_1, S}^\times, \dots, \mathbb{Z}_{L_k, S}^\times$$

*has **finite index** in $\mathbb{Z}_{F, S}^\times$, where $L_i = \tilde{F}^{U_i}$.*

Algorithmic consequence

Theorem (Biasse–Fieker–Hofmann–P., Étienne)

Assume GRH. If there is a norm relation, then the computation of $\mathbb{Z}_{F,S}^\times$ reduces in polynomial time to the computation of $\mathbb{Z}_{L_1,S}^\times, \dots, \mathbb{Z}_{L_k,S}^\times$.

Example

- $F = \mathbb{Q}(\zeta_{6552})$
- $\dim_{\mathbb{Q}} F = 1728$
- $\Delta_F = 2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$
- $(\log \Delta_F)^2 \approx 10^8$

$\text{Cl}(F)$ computed in 4.2 hours on a laptop.

- $\text{rk}_2 \text{Cl}(F) = 112$
- $\text{rk}_3 \text{Cl}(F) = 101$
- $h_{6552}^+ = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13 \approx 7 \cdot 10^{13}$

Spectral geometry

Can you hear the shape of a drum?

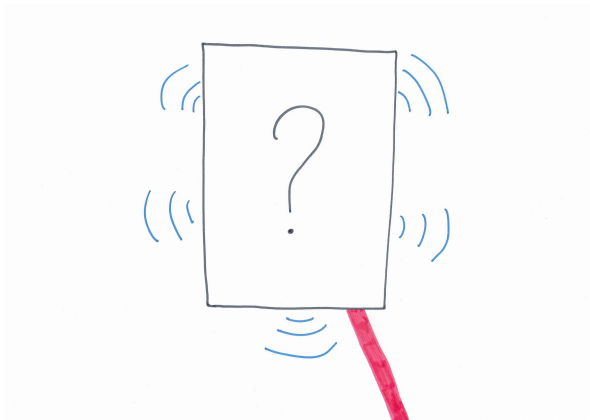
Can you hear the shape of a drum?



Can you hear the shape of a drum?



Can you hear the shape of a drum?



Can you hear the shape of a drum?

Vibrating frequencies are determined by the eigenvalues of the
Laplace operator

$$\Delta = \frac{\partial^2}{\partial^2 x} + \frac{\partial^2}{\partial^2 y}.$$

Isospectral manifolds

Today: manifold M = closed connected orientable Riemannian manifold.

$\rightsquigarrow$ **Laplace operator** Δ acting on space $\Omega^i(M)$ of i -forms, with discrete spectrum.

Definition

Two manifolds M and N are **isospectral** if for all i , the spectra of Δ on $\Omega^i(M)$ and $\Omega^i(N)$ agree with multiplicity.

Question: isospectral $\implies$ isometric?

Answer: no in all dimensions ≥ 2 (Vignéras 1980).

Isospectral manifolds

Today: manifold M = closed connected orientable Riemannian orbifold.

$\rightsquigarrow$ **Laplace operator** Δ acting on space $\Omega^i(M)$ of i -forms, with discrete spectrum.

Definition

Two manifolds M and N are **isospectral** if for all i , the spectra of Δ on $\Omega^i(M)$ and $\Omega^i(N)$ agree with multiplicity.

Question: isospectral $\implies$ isometric?

Answer: no in all dimensions ≥ 2 (Vignéras 1980).

Spectral geometry

Question: Can we say more in special classes of manifolds?

Question: Which invariants of Riemannian manifolds are isospectral invariants?

- dimension $\dim M$: yes
- volume $\text{Vol}(M)$: yes
- Betti numbers $\text{rk } H_i(M)$: yes
- ring $H^\bullet(M)$: no (Lauret–Miatello–Rossetti 2013)
- torsion homology $\#H_i(M)[p^\infty]$: no $\forall p$ (Bartel–P. 2016).

Vignéras's construction

B quaternion algebra: $\mathbb{R} \otimes B \cong M_2(\mathbb{R})^s \times M_2(\mathbb{C})^c \times \mathbb{H}^r$.

$\mathcal{O} \subset B$ order: $SL_1(\mathcal{O}) \subset SL_2(\mathbb{R})^s \times SL_2(\mathbb{C})^c$.

Define **arithmetic manifold** $M(\mathcal{O}) = SL_1(\mathcal{O}) \backslash (\mathcal{H}^2)^s \times (\mathcal{H}^3)^c$.

Theorem (Vignéras)

*If $\mathcal{O}_1$ and $\mathcal{O}_2$ are maximal orders **and extra conditions hold**, then $M(\mathcal{O}_1)$ and $M(\mathcal{O}_2)$ are isospectral.*

Representation equivalence

The proof uses the **trace formula**, and proves a stronger statement, namely that $SL_1(\mathcal{O}_1)$ and $SL_1(\mathcal{O}_2)$ are **representation equivalent**: writing $G = SL_2(\mathbb{R})^s \times SL_2(\mathbb{C})^c$,

$$L^2(SL_1(\mathcal{O}_1) \backslash G) \cong L^2(SL_1(\mathcal{O}_2) \backslash G)$$

as unitary representations of G .

Question (Pesce 1995):

isospectrality $\implies$ representation equivalence?

- Pesce 1995: yes with "strong isospectrality" instead.
- Doyle–Rossetti 2011: yes in dimension 2.

Refined criteria: theorem template

Theorem $\langle * \rangle$ (Bartel–P.)

At least one of the following two statements is true:

- ① *there exists a number field L in an a-priori finite list and a certain Hecke character of L ;*
- ② *$M(\mathcal{O}_1)$ and $M(\mathcal{O}_2)$ are $*\text{-isospectral}$.*

For each instance of $*$, existence can be checked using PARI/GP's new Hecke characters package (developped with Pascal Molin).

Refined criteria: theorem template

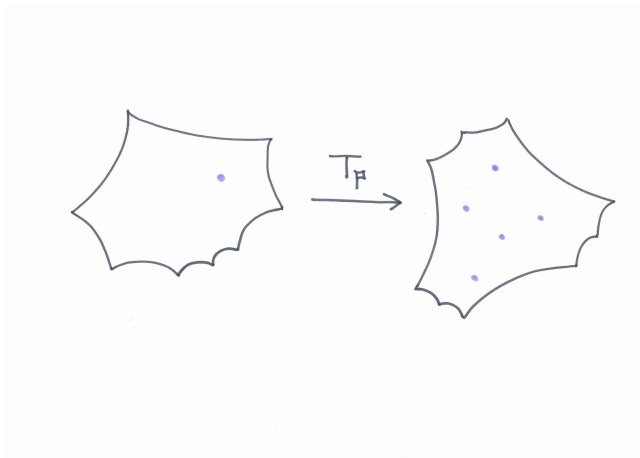
Theorem $\langle * \rangle$ (Bartel–P.)

At least one of the following two statements is true:

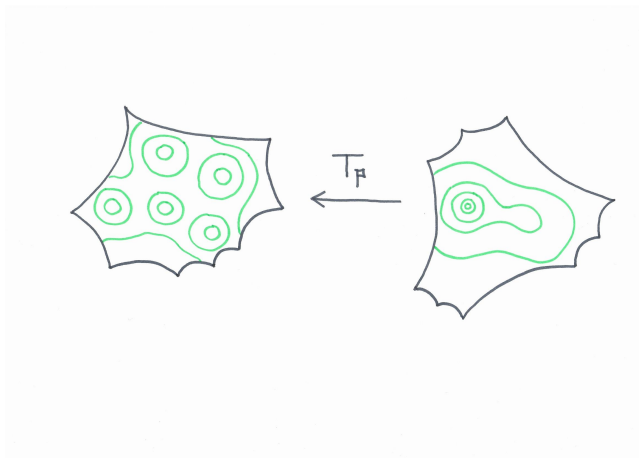
- ① *there exists a number field L in an a-priori finite list and a $*\text{-shady character}$ of L ;*
- ② *$M(\mathcal{O}_1)$ and $M(\mathcal{O}_2)$ are $*\text{-isospectral}$.*

For each instance of $*$, existence can be checked using PARI/GP's new Hecke characters package (developped with Pascal Molin).

Hecke operators, geometrically



Hecke operators, geometrically



Hecke operators and isospectrality

We obtain a large supply of Hecke operators:

$$T: \Omega^i(M(\mathcal{O}_1))_{\Delta=\lambda} \longrightarrow \Omega^i(M(\mathcal{O}_2))_{\Delta=\lambda}.$$

We are able to prove, under our conditions, that there exists an **invertible** one.

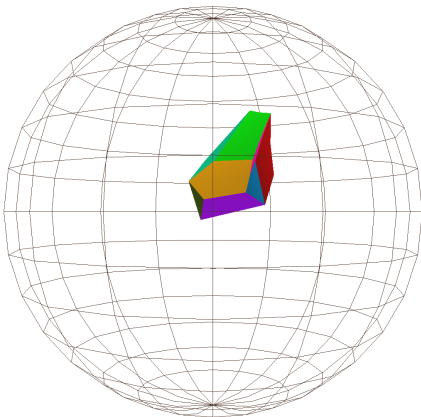
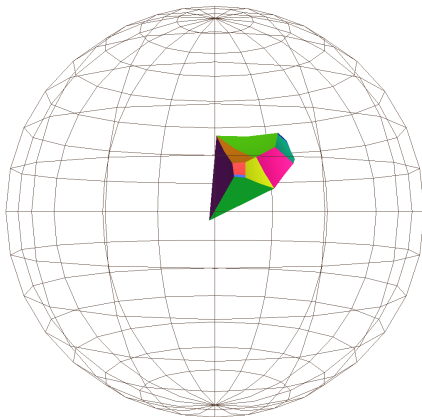
Dimension 3: an exotic pair

Theorem (Bartel–P.–PARI/GP)

*There exists a pair of isospectral hyperbolic 3-manifolds with volume 0.251 . . . that are **isospectral**, but **not representation-equivalent**.*

Vignéras's construction with $F = \mathbb{Q}(\sqrt{-10 - 14\sqrt{5}})$, the unique A ramified exactly at the real places, and maximal orders.

Smallest possible volume? Previous record was 2.83 . . . (Linowitz–Voight 2014) and Sunada's construction cannot produce smaller ones.



Cryptography

Hard problems

Public-key cryptography relies on **hard algorithmic problems**, often of mathematical origin.

Obstacle: it is difficult to prove that a problem cannot be solved efficiently.

Instead, prove **reductions** to understand the relative difficulty of problems.

Method: construct an efficient algorithm that solves Problem A by making calls to an **oracle** solving Problem B.

Isogeny problems

Problem (ℓ -ISOGENY)

Given supersingular E, E' , compute an ℓ^k -isogeny $E \rightarrow E'$.

Problem (ENDRING)

Given a supersingular E , compute a basis $\beta_1, \dots, \beta_4$ of $\text{End}(E)$.

Theorem (Wesolowski, under GRH)

The ℓ -ISOGENY and ENDRING problems are equivalent.

Problem (ONEEND)

Given a supersingular E , compute some $\alpha \in \text{End}(E) \setminus \mathbb{Z}$.

Isogeny problems: theorem

Theorem (P.–Wesolowski)

The ONEEND and ENDRING problems are equivalent.

Corollary

ENDRING can be solved in time $\tilde{O}(\sqrt{p})$.

Corollary

If ENDRING is hard, then

- *the CGL hash function is collision-resistant, and*
- *the SQISIGN identification protocol is sound.*

Lattice problems

L lattice; $\lambda_i(L) = \min\{t : \dim\langle B(t) \cap L \rangle_{\mathbb{R}} \geq i\}$.

Problem (γ -SVP)

Given a lattice L , compute $v \neq 0 \in L$ such that $\|v\| \leq \gamma \lambda_1(L)$.

Problem (γ -SIVP)

Given a lattice L of rank n , compute independent $v_1, \dots, v_n \in L$ such that $\|v_i\| \leq \gamma \lambda_n(L)$.

Average versions of the problems: solve with non-negligible probability when the input is drawn from a specified distribution.

Lattice problems: theorem

Theorem (de Boer–P.–Toma–Wesolowski)

When restricted to module lattices of fixed rank, $n^{O(1)}\gamma$ -SIVP reduces to γ -AVGSIVP.

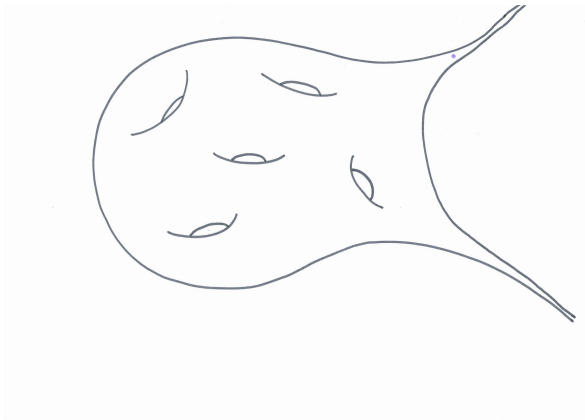
Interpretation: there is no module lattice that is much harder than a randomly chosen one.

Hecke operators and probability distributions

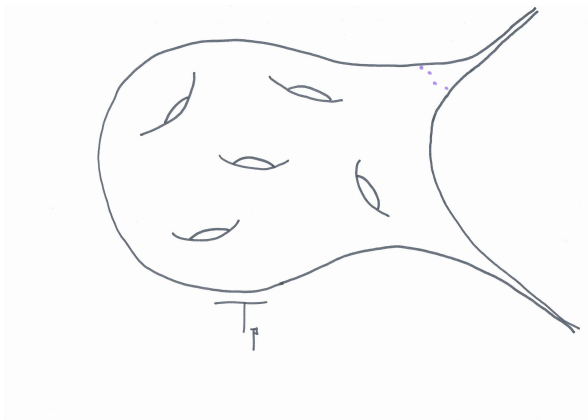
Common idea in both cases:

- ① the set X of instances of the problem has the structure of an arithmetic manifold:
 - set X of supersingular curves
 - space X of module lattices.
- ② **Hecke operators** act on probability distributions on X , with a natural interpretation:
 - $T_\ell \leftrightarrow$ random ℓ -isogeny from $E \in X$.
 - $T_p \leftrightarrow$ random sublattice $L' \subset L \in X$ with $L/L' \cong \mathbb{Z}_F/p$.

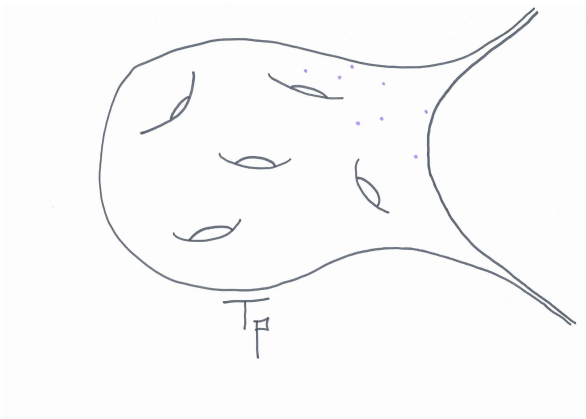
Hecke operators and equidistribution



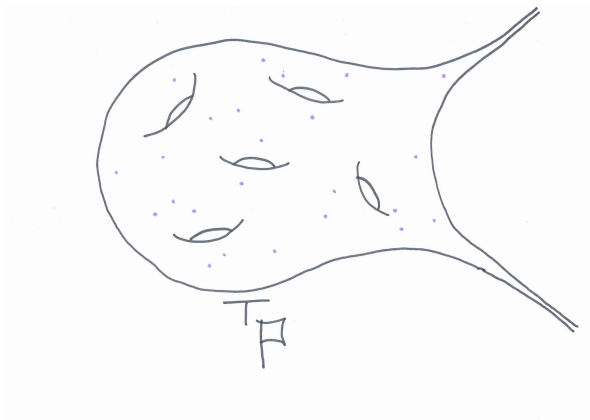
Hecke operators and equidistribution



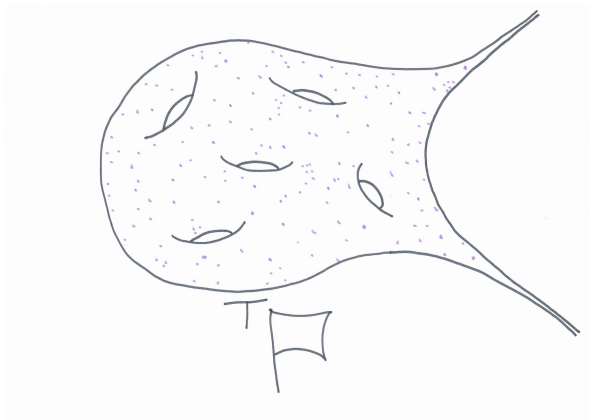
Hecke operators and equidistribution



Hecke operators and equidistribution

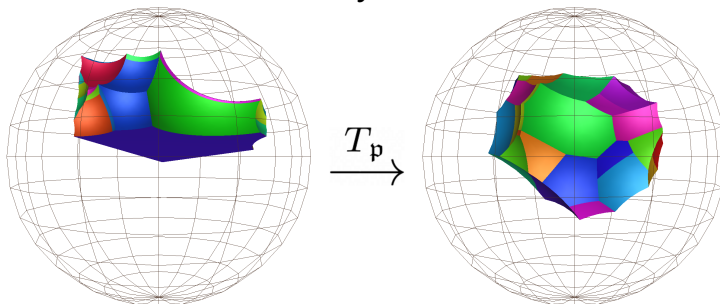


Hecke operators and equidistribution



Conclusion

I love Hecke operators!
Do you?



Thank you!