Hecke Operators for Arithmetic Groups via Cell Complexes

Mark McConnell

Center for Communications Research, Princeton

Overview

- Cohomology of locally symmetric spaces for SL_n
- The conjectural connection between the cohomology and Galois representations
- Cell complexes that let us compute this cohomology

Joint work with Avner Ash (Boston College) and Paul Gunnells (U. Mass.)

Definitions

$G = \mathrm{GL}_n(\mathbf{R})$, the $n \times n$ matrices of non-zero determinant.

- $\mathrm{SL}_n(\mathbf{R})$ is the subgroup of G of determinant 1.

$K = \mathrm{O}_n(\mathbf{R})$, the $g \in G$ preserving the standard dot product on $\mathbf{R}^n$.

- $K \subset G$ is a maximal compact subgroup.

$\mathbf{R}_+ = \{\lambda I \in G \mid \lambda > 0\}$, the *homotheties*.

$X = G/K\mathbf{R}_+$ is the *symmetric space* for $\mathrm{SL}_n(\mathbf{R})$.

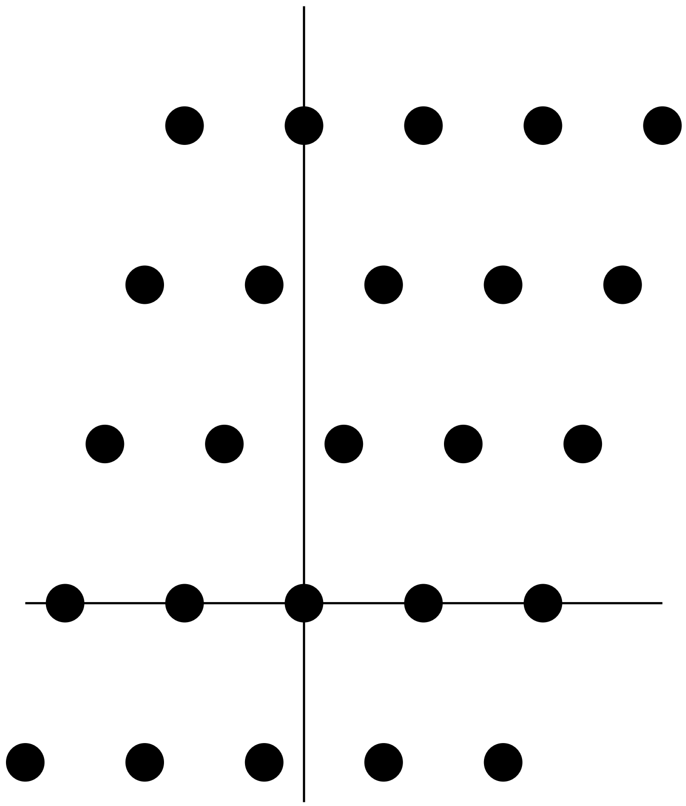
$\Gamma = \mathrm{SL}_n(\mathbf{Z})$, with integer entries and determinant 1.

$\Gamma \backslash X$ is a *locally symmetric space*.

Lattices

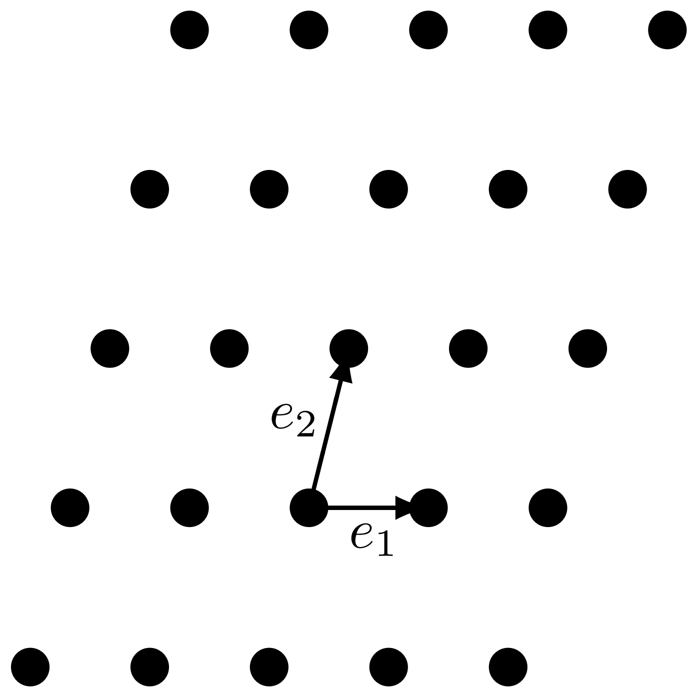
If $g \in G$, the rows of g form a basis $\{e_1, \ldots, e_n\}$ of $\mathbf{R}^n$.

The $\mathbf{Z}$-span of $\{e_i\}$ is a *lattice*. It is an additive subgroup $\cong \mathbf{Z}^n$.



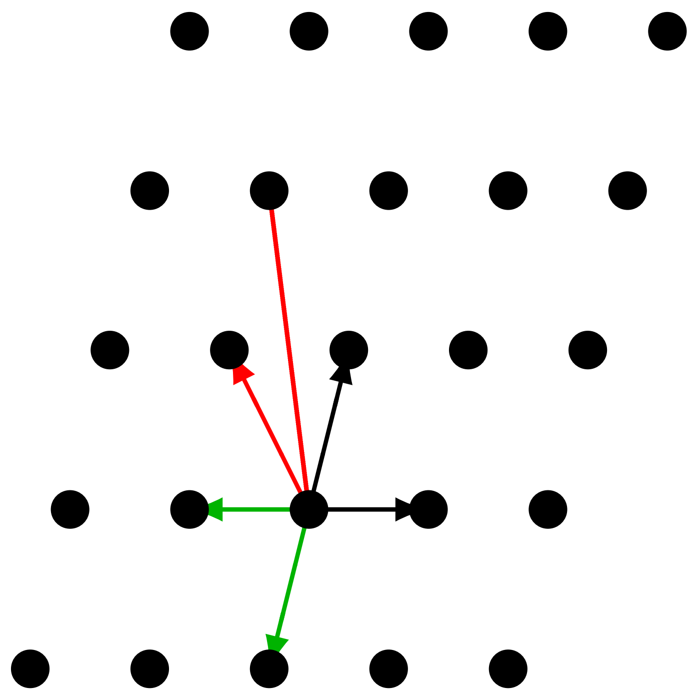
Marked Lattices

A *marked lattice* is a lattice together with a distinguished lattice basis.



Γ acts by preserving the underlying lattice, but changing the distinguished basis. All bases are equivalent mod Γ. Hence

$$\Gamma \backslash G = \{\text{lattices} \in \mathbf{R}^n\}.$$



K acts on a marked lattice by rotating/reflecting the whole picture.

$\mathbf{R}_+$ acts by rescaling the whole picture (homothety).

Hence the locally symmetric space

$$\Gamma\backslash X = \{\text{lattices} \in \mathbf{R}^n\} \text{ modulo rotations and homotheties.}$$

Smith Normal Form

If L is a lattice and $M \subseteq L$ a sublattice of finite index,

$$L/M \cong \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_n\mathbf{Z}$$

where $a_i \in \mathbf{Z}$, $a_i \geq 1$, and $a_1 \mid a_2 \mid \cdots \mid a_n$.

- The a_i are the *invariant factors* of (L, M).
- They are the diagonal entries in the *Smith normal form* (SNF) of a matrix giving a basis of M with respect to a basis of L.

Hecke Correspondences

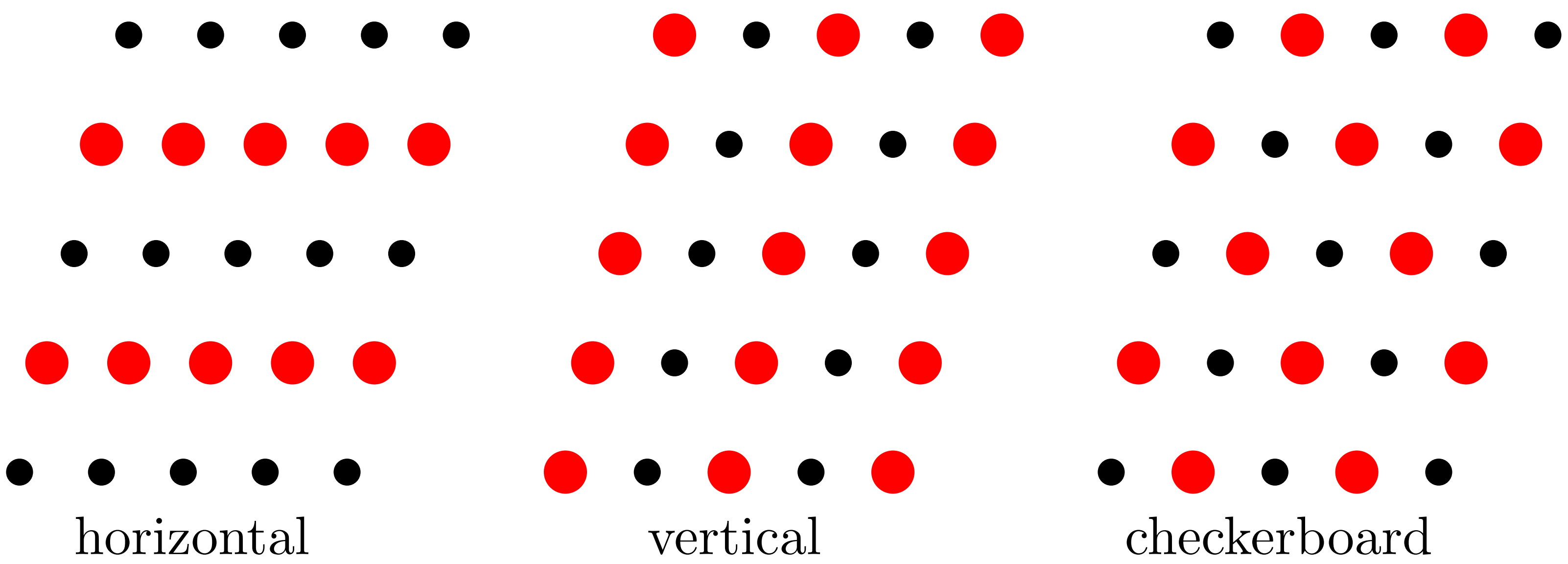
$$L/M \cong \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_n\mathbf{Z} \qquad (*)$$

For fixed L and fixed $a_1, \ldots, a_n$, only finitely many $M \subseteq L$ satisfy $(*)$.

The *Hecke correspondence* $T(a_1, \ldots, a_n)$ is the one-to-many map $\Gamma \backslash X \to \Gamma \backslash X$ given by

$$L \mapsto \{M \text{ satisfying } (*)\}.$$

Example. The Hecke correspondence $T(1,2)$ is generically a 1-to-3 map. It carries the L in our pictures to the following three lattices of red points.



Can take formal **Z**-linear combinations of Hecke correspondences. Can compose them. This makes them a ring.

Fact. The Hecke correspondences for Γ form a commutative ring that is isomorphic to the polynomial ring on the generators

$$T(p,k) = T(1,\ldots,1,p,\ldots,p) \qquad \text{for } p \text{ prime, } k = 1,\ldots,n.$$

with k copies of p and $n-k$ copies of 1. (Let $T(p,0) = \mathrm{id}$.)

Equivalent Definition of Hecke Correspondences

Let $\alpha = \mathrm{diag}(a_1, \ldots, a_n)$. Let $\tilde{\Gamma} = \Gamma \cap (\alpha^{-1}\Gamma\alpha)$. This is a subgroup of Γ of finite index. There are two maps

$$\begin{array}{c} \tilde{\Gamma}\backslash X \\ c_1 \downarrow \quad \downarrow c_2 \\ \Gamma\backslash X \end{array}$$

with $c_1 : \tilde{\Gamma}x \mapsto \Gamma x$ and $c_2 : \tilde{\Gamma}x \mapsto \Gamma\alpha x$.

The Hecke correspondence $T(a_1, \ldots, a_n)$ is:

- lift $x \in \Gamma\backslash X$ by c_1, which gives finitely many points, and push these points back down by c_2.

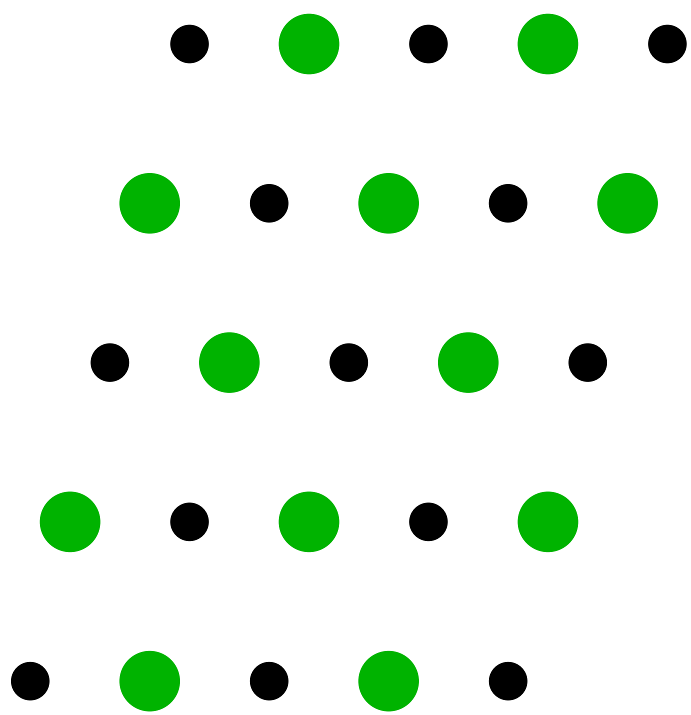
Example. For $\alpha = \mathrm{diag}(1, \ldots, 1, N)$, the group $\tilde{\Gamma}$ is

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_n(\mathbf{Z}) \;\middle|\; \gamma \equiv \begin{pmatrix} * & \cdots & * & 0 \\ \vdots & \ddots & \vdots & 0 \\ * & \cdots & * & 0 \\ * & \cdots & * & * \end{pmatrix} \mod N \right\}.$$

$\Gamma_0(N)\backslash X$ is a space of lattices with extra structure.

$$\Gamma_0(N)\backslash X = \{(L, L') \mid L' \subseteq L,\ L/L' \cong \mathbf{Z}/N\mathbf{Z}\}/(\text{rot.}, \text{homoth.})$$

Example. This pair is a point in $\Gamma_0(2)\backslash X$ for $n = 2$. The two maps $\Gamma_0(2)\backslash X \to \Gamma\backslash X$ are $c_1 : (\text{pair}) \mapsto$ black, $c_2 : (\text{pair}) \mapsto$ green.



Congruence Subgroups

Let $\Gamma(N) = \{\gamma \in \mathrm{SL}_n(\mathbf{Z}) \mid \gamma \equiv I \bmod N\}$.

Say Γ' is a *congruence subgroup of level* N if there is an N such that $\Gamma(N) \subseteq \Gamma' \subseteq \Gamma$. (Example: $\Gamma_0(N)$.) All congruence subgroups are of finite index in Γ. The locally symmetric space $\Gamma' \backslash X$ has an interpretation as a space of lattices with extra structure. Hecke correspondences are defined as before:

$$\begin{array}{c} (\Gamma' \cap \alpha^{-1}\Gamma'\alpha)\backslash X \\ c_1 \downarrow \quad \downarrow c_2 \\ \Gamma \backslash X \end{array}$$

The Hecke correspondences generate a polynomial algebra. (Must modify the generators slightly when $p \mid N$.)

Connections with Automorphic Forms

Let V be a Γ'-module. In this talk, V will be defined over $\mathbf{R}$ or $\mathbf{C}$. Often $V = \mathbf{C}$ with trivial Γ'-action ("constant coefficients").

Let $\omega \in H^i(\Gamma' \backslash X; V)$. A Hecke correspondence acts on cohomology by $\omega \mapsto c_{2*}c_1^*\omega$. We say the Hecke correspondences descend to a ring of *Hecke operators* on cohomology.

Cuspidal Cohomology

We always use $\omega \in H^i(\Gamma'\backslash X; V)$ to denote a cuspidal cohomology class.

- A *cuspidal differential form* is a differential form with coefficients in V satisfying certain vanishing conditions as you go out to infinity (toward the *cusps*) in $\Gamma'\backslash X$. It is rapidly decreasing, and appropriate integrals vanish over the parabolic subgroup associated to each cusp.
- A cohomology class is *cuspidal* if it is supported on a cuspidal differential form.

The cuspidal cohomology is one building block of $H^*(\Gamma'\backslash X; V)$. The rest of H^i is not cuspidal, but comes from the cuspidal cohomology of other groups. Often Eisenstein classes connect the cohomology of the big space with the cuspidal part of lower-rank subgroups of G.

The Hecke polynomial

Also, we always assume $\omega \in H^i(\Gamma' \backslash X; V)$ is an *eigenclass* for the Hecke operators.

Let $a(p,k)$ be the eigenvalue for $T(p,k)$. Define the *Hecke polynomial* by

$$P(\omega, p) = \sum_{k=0}^{n} (-1)^k p^{k(k-1)/2} a(p,k) T^k.$$

Frobenius

For any finite Galois extension $\mathbf{Q}(\beta)/\mathbf{Q}$, if p is unramified in $\mathbf{Q}(\beta)$, there is an element $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbf{Q}(\beta)/\mathbf{Q})$, well-defined up to conjugacy, called the *Frobenius element.* Characterized by saying it pushes forward to the generator of the Galois extension $\mathbf{F}_p(\bar{\beta})/\mathbf{F}_p$ given by $x \mapsto x^p$.

Let $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. The algebraic closure $\bar{\mathbf{Q}}/\mathbf{Q}$ is an inverse limit of finite Galois extensions, compact in the natural topology. $\exists\, \mathrm{Frob}_p \in \mathrm{Gal}(\mathbf{Q}(\beta)/\mathbf{Q})$, the limit of the finite ones, defined up to conjugacy.

We now come to the main point of the talk, the conjecture we want to test.

Conjecture. *Let $\omega \in H^i(\Gamma'\backslash X; V)$ be a cuspidal Hecke eigenclass. Then there is a number field F with ring of integers B, such that for any prime l and prime λ of B lying over l, there is a continuous semi-simple Galois representation*

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_n(B_\lambda),$$

unramified outside lN, and such that, for any prime $p \nmid lN$, the characteristic polynomial of $\rho(\mathrm{Frob}_p^{-1})$ is the Hecke polynomial $P(\omega, p)$.

- Relates topology (ω) with number theory ($\rho(\mathrm{Frob}_p^{-1})$).
- We say that ρ, if it exists, is *attached* to ω.

Source of the conjecture

Comes from the world of motives and the Langlands program.

For SL_2, the conjecture is known. (Hecke, Weil, Eichler, Shimura, Deligne.) $X = \mathfrak{h}$, the upper half-plane. $\Gamma'\backslash\mathfrak{h}$ is a modular curve. ω comes from a cusp form of weight 2 on the modular curve. The Hecke correspondences cut out an abelian subvariety $A \subseteq \mathrm{Jac}(\Gamma'\backslash\mathfrak{h})$. The points of order l^m (as $m \to \infty$) on $A(\bar{\mathbf{Q}})$ are $\cong B_\lambda \times B_\lambda$. Galois acts on this product, giving a 2-dimensional ρ. The *motive* is A, or really $H_1(A)$.

Both sides of the conjecture are independent of l. The motive is the "l-adic cohomology without the l."

For $n > 2$ there is no obvious candidate for a motive. The locally symmetric space $\Gamma'\backslash X$ is no longer an algebraic variety.

Nevertheless, standard conjectures would attach a motive to each cuspidal automorphic representation Π of GL_n over a number field, as long as the infinity type of Π is algebraic. One knows that if Π arises from a cuspidal ω where V is a rational representation, then Π satisfies this algebraicity condition. There would be a Galois representation ρ coming from the motive, giving the conjecture as stated that relates the Hecke eigenvalues of ω to $\rho(\mathrm{Frob}_p^{-1})$.

Computational Topology

We are able to

- compute $H^i(\Gamma' \backslash X; V)$ explicitly by machine;
- compute the action of the Hecke operators;
- check the conjecture computationally.

The Well-Rounded Retract

Recall X is the space of marked lattices L in $\mathbf{R}^n$. Let

$$m(L) = \min\{\|\mathbf{v}\| \mid \mathbf{v} \in L, \mathbf{v} \neq 0\}.$$

The *minimal vectors of* L are

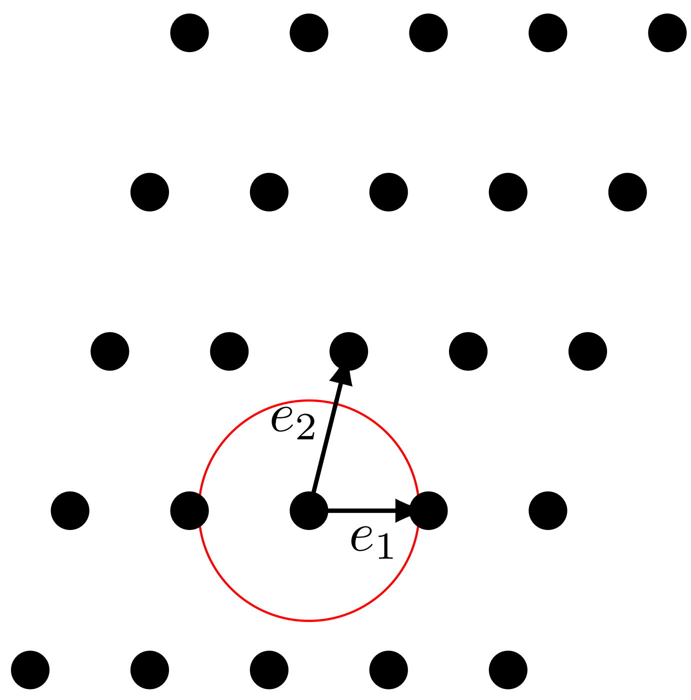
$$M(L) = \{\mathbf{v} \in L \mid \|\mathbf{v}\| = m(L)\}.$$

Say L is *well-rounded* if $M(L)$ spans $\mathbf{R}^n$.

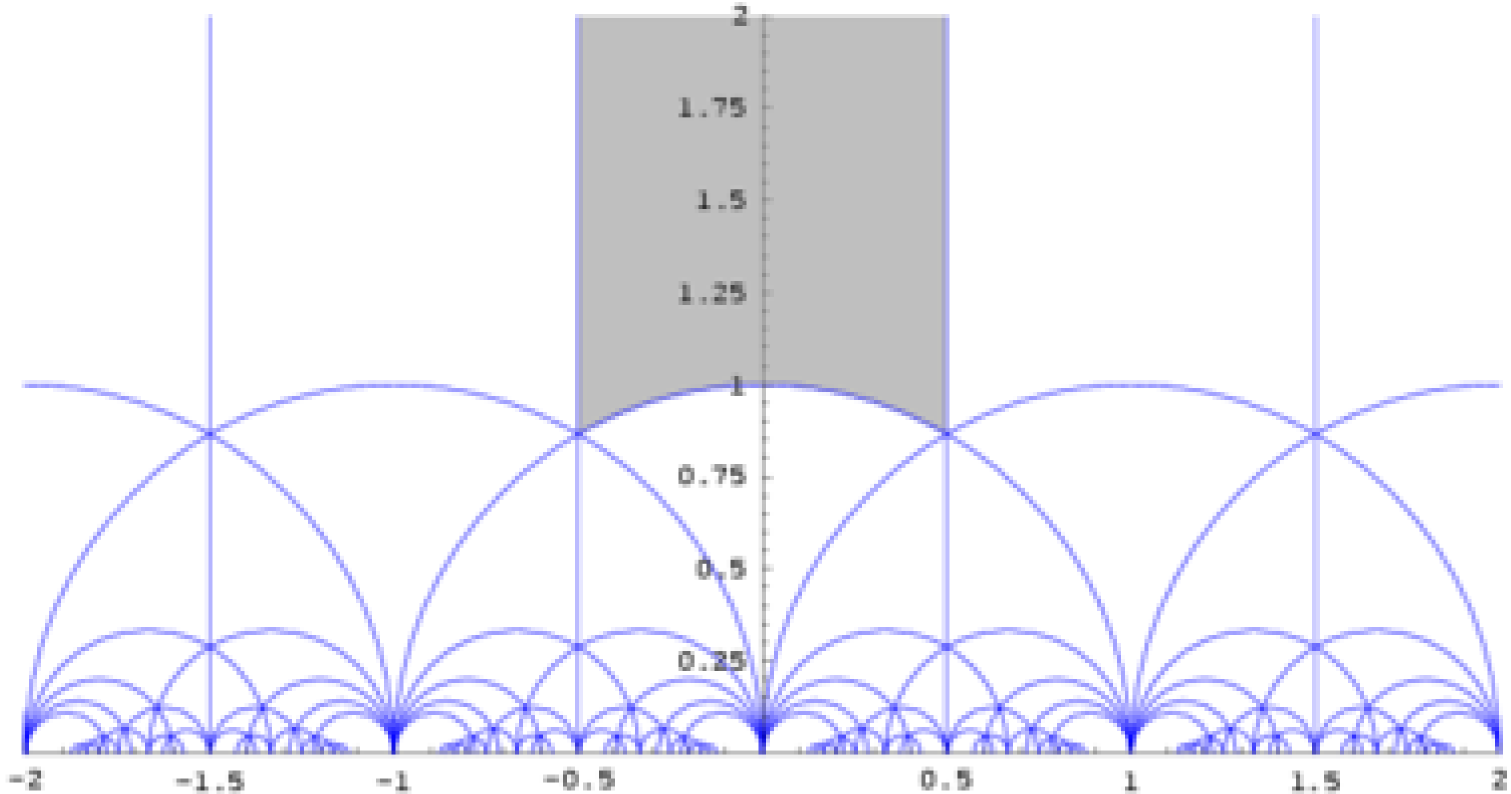
Definition. The *well-rounded retract* W is the set of all well-rounded lattices in X.

The Well-Rounded Retract for SL_2

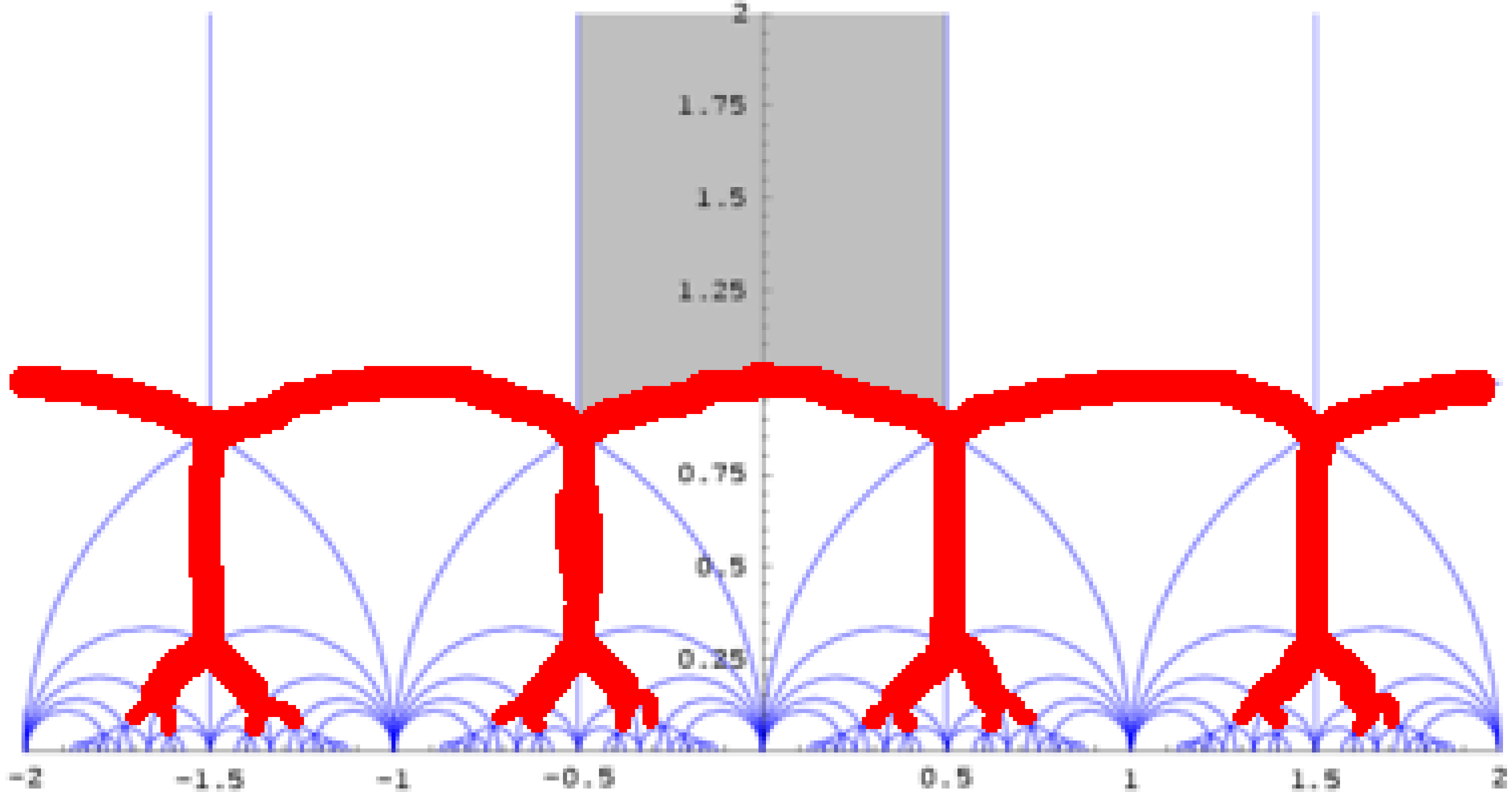
The short vectors $M(L) = \{\pm e_1\}$ are on the circle. Keep x fixed, and shrink y vertically, till $\pm e_2$ also touches the circle. Then $M(L) = \{\pm e_1, \pm e_2\}$ will span $\mathbf{R}^2$, and L will be well-rounded.



Classical Fundamental Domain for $\mathrm{SL}_2(\mathbf{Z})$

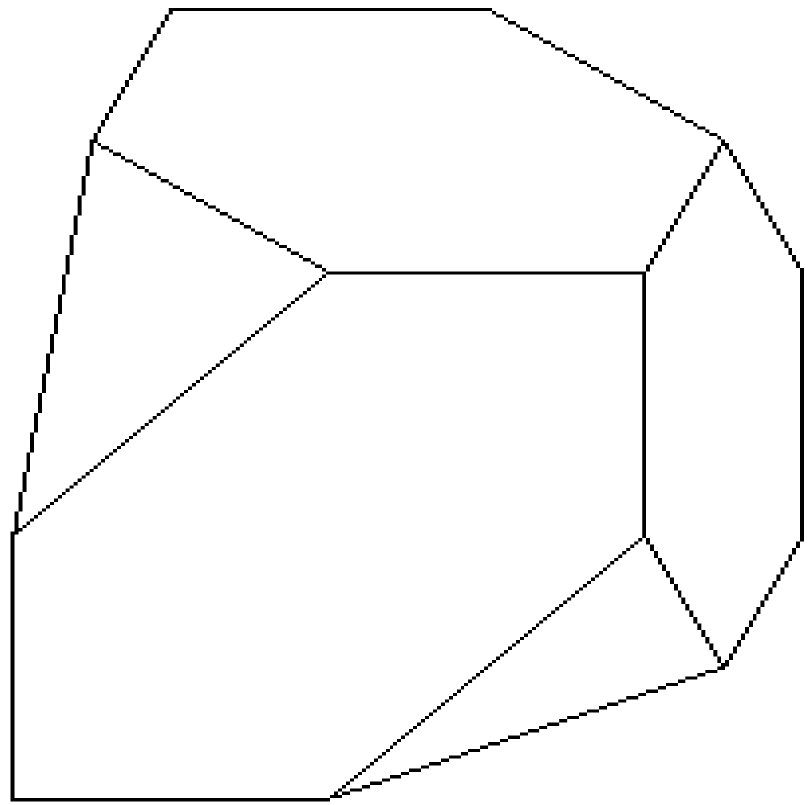


The Well-Rounded Retract for $\mathrm{SL}_2(\mathbf{Z})$



(For all n, W is dual to the Voronoï decomposition of X.)

Top Cell for $\mathrm{SL}_3(\mathbf{Z})$ (The Soulé Cube)



Four cubes meet at each triangle. Three meet at each hexagon.

The Well-Rounded Retract in general

- W is a locally finite cell complex.
- Γ acts on W, preserving the cells.
- There are only finitely many types of cells mod Γ'.
- W is a Γ-invariant deformation retract of X.
- The deformation retraction is a sequence of geodesic flows on X [Ash-M., 1996].
- $\Gamma' \backslash W$ is a finite cell complex and is a deformation retract of $\Gamma' \backslash X$.
- $H^i(\Gamma' \backslash W; V) = H^i(\Gamma' \backslash X; V)$, and we can find the groups for $\Gamma' \backslash W$ by computer.

Computing Hecke Operators

Trouble: W is not carried into itself by Hecke operators. The deformation retraction $T(p,k)(W) \to W$ is many-to-many and complicated.

For $\mathrm{SL}_2(\mathbf{Z})$, use the modular symbol algorithm (Manin).

Ash-Rudolph have an algorithm for all SL_n, generalizing continued fractions. It only works for $H^d(\Gamma' \backslash X; V)$, where d is the v.c.d. (top degree).

Gunnells has an algorithm based on the detailed structure of W and the Voronoï decomposition. It works for H^i for some $i < d$.

AGM III

Rest of the talk is on [Ash, Gunnells, M. 2009], the first computational work of this type for GL_4.

From now on, $n = 4$, $\Gamma' = \Gamma_0(N)$, and $V = \mathbf{C}$ (constant coefficients).

For GL_4, cuspidal cohomology lies only in H^4 and H^5, and these are dual to each other. Look at H^5. The v.c.d. is 6, and Gunnells' Hecke algorithm works on H^5 (codimension 1).

We decompose H^5 into Hecke eigenspaces for $T(p,k)$ for p as large as we can. On each eigenspace, we compute the Hecke polynomials and factor them, which says how Frob_p^{-1} acts on the eigenspace.

Say ρ *seems to be attached to* ω if the conjecture is satisfied at all the p you can compute before your machine runs out of memory.

Often just the $T(2,k)$ are enough to suggest how ρ decomposes.

Example. If a Hecke polynomial (degree 4) factors as (linear)(linear)(quadratic), it strongly suggests this is not a cuspidal eigenspace. Rather, it comes from an SL_2 symmetric space out at one of the cusps. The quadratic terms will be the Hecke polynomial for some newform of weight 2 or 4. The two linear terms are twists by a power of the cyclotomic character.

Results for GL_4

We computed $H^5(\Gamma_0(N); \mathbf{C})$ for all N up into the mid-50s, and for all prime $N \leq 211$.

We found Eisensteinian cohomology coming from the cusps for SL_2 as expected. Also for SL_3 [Ash, Grayson, Green 1984].

We found that the cuspidal part consists of functorial lifts of Siegel modular forms from paramodular subgroups of $\mathrm{Sp}_4(\mathbf{Q})$ that are not Gritsenko lifts. These correspond to selfdual automorphic representations on $\mathrm{GL}(4)/\mathbf{Q}$.

Autochthonous Forms?

We were hoping to find non-lifted cuspidal cohomology classes, which would corresponded to non-selfdual automorphic representations. These would be *autochthonous*, not coming from any lower-rank group. Need higher N?

Linear Algebra Issues

For GL_4, the cochain complex computing $H^5(\Gamma_0(N)\backslash W)$ has matrices d^5 and d^4 with $d^5 d^4 = 0$. The matrices have size

$$d^5 = N^3/96 \times N^3/10 \qquad d^4 = N^3/10 \times N^3/3$$

For $N = 211$, d^4 is $944,046 \times 3,277,686$.

The matrices are very sparse: only up to 6 entries per column, and 26 per row, independent of N.

We find the Smith normal form of the matrices, e.g., $d^4 = P_4 D_4 Q_4$, where P_4 and Q_4 have det ± 1, and D_4 is diagonal in SNF.

We prefer to work over $\mathbf{Z}$ (arbitrary precision). That gives the torsion in the cohomology over $\mathbf{Z}$, as well as the rank over $\mathbf{C}$. We do this for N up to the 30s. Thereafter, to avoid integer explosion, we work over a fixed finite field (set $\mathbf{C} = \mathbf{F}_{12379}$).

To find Hecke, we must compute and store the change of basis matrices P and Q. This rules out some of the leading linear algebra techniques:

- reduce d^4 mod p for many 16-bit p, compute the D_4 for each p, and reassemble the SNF over **Z** by Chinese remaindering. (Dumas et al.) It is unknown how do to this while remembering P and Q.
- Iterative methods (Krylov subspaces, Wiedemann, Lanczos). E.g., these solve $Ax = b$ linear algebra problems without reducing A.
- Essentially no low-valence rows and columns.

Instead, M. has developed *Sheafhom*. It uses classical methods like Gaussian elimination, but orders the steps differently and uses special data structures. It solved $N = 211$ on a 4G Linux laptop.