Practical computation of Hecke operators

Mathieu Dutour Sikirić

Institute Rudjer Bošković, Croatia and
Universität Rostock

May 7, 2014

I. Computing with polytopes

Polytopes, definition

- A polytope $P \subset \mathbb{R}^n$ is defined alternatively as:
  - The convex hull of a finite number of points $v^1, \dots, v^m$:

$$P = \{v \in \mathbb{R}^n \mid v = \sum_i \lambda_i v^i \text{ with } \lambda_i \geq 0 \text{ and } \sum \lambda_i = 1\}$$

  - The following set of solutions:

$$P = \{x \in \mathbb{R}^n \mid f_j(x) \geq b_j \text{ with } f_j \text{ linear}\}$$

    with the condition that P is bounded.
- The cube is defined alternatively as
  - The convex hull of the 2^n vertices

$$\{(x_1, \dots, x_n) \text{ with } x_i = \pm 1\}$$

  - The set of points $x \in \mathbb{R}^n$ satisfying to

$$x_i \leq 1 \text{ and } x_i \geq -1$$

Facets and vertices

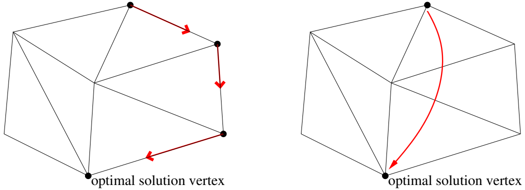
- A vertex of a polytope P is a point $v \in P$, which cannot be expressed as $v = \lambda v^1 + (1-\lambda)v^2$ with $0 < \lambda < 1$ and $v^1 \neq v^2 \in P$.
- A polytope is the convex hull of its vertices and this is the minimal set defining it.
- A facet of a polytope is an inequality $f(x) - b \geq 0$, which cannot be expressed as $f(x) - b = \lambda(f_1(x) - b_1) + (1-\lambda)(f_2(x) - b_2)$ with $f_i(x) - b_i \geq 0$ on P.
- A polytope is defined by its facet inequalities. and this is the minimal set of linear inequalities defining it.
- The dual-description problem is the problem of passing from one description to another.
- There are several programs CDD, LRS for computing dual-description computations.
- In case of large problems, we can use the symmetries for faster computation.

Linear programs

- A linear program is the problem of maximizing a linear function $f(x)$ over a set $\mathcal{P}$ defined by linear inequalities.

$$\mathcal{P} = \{x \in \mathbb{R}^d \quad \text{such that} \quad f_i(x) \geq b_i\}$$

  with f_i linear and $b_i \in \mathbb{R}$.
- The solution of linear programs is attained at vertices of $\mathcal{P}$.
- There are two classes of solution methods:



Simplex method   Interior point method

- Simplex methods use exact arithmetic but have bad theoretical complexity
- Interior point methods have good theoretical complexity but only gives an approximate vertex.

Face complex

- A face of a polytope P is a set defined by $f(x) = 0$ with f an affine function that is positive on P.
- Faces vary in dimension between 0 (vertices) and $n - 1$ (facets).
- The set of faces form a lattice under the inclusion relation, i.e. they are completely described by the set of vertices $S \subset \{1, \dots, p\}$.
- If F, F' are faces of dimenion k, $k + 2$ with $F \subset F'$ then there exist two faces F_1, F_2 with $F \subset F_i \subset F'$.
- There are essentially two techniques for computing the set of faces of a polytope P:
  - We know vertices and facets of P: Then given a subset S, find all the facets containing the vertices of S, check if the rank is correct (linear algebra)
  - We know only the vertices of P: Checking if a set defines a face can be done by linear programming.

The second approach is good if one wants the low dimensional faces and the facets cannot be computed.

Boundary operator I

Let us take a n-dimensional polytope P

- Given a face F we can define its differential (boundary) by

$$dF = \sum_{F' \subset F} \epsilon(F', F) F'$$

  With $\epsilon(F', F) = \pm 1$.
- Essentially all algorithm for computing face lattice also give the boundary operators.
- But the sign can be troublesome. Essentially there are two possible orientations on a face F and we have to make decisions.
- For an edge $e = \{v, v'\}$ we set $de = v' - v$ (arbitrary choice)
- We have the collapsing relation

$$d \circ d = 0$$

  By using it we can recursively compute the signs $\epsilon(F', F)$ up to a global sign for F.

Boundary operator II

- The recursive method works well, but it is painful to program and it requires the knowledge of all faces from dimension 0 to k.
- The recursive method does not use the polyhedral linear structure of $\mathbb{R}^n$ which is an advantage (generality) and an inconvenient (speed and complexity).
- For each face F we define a spanning set $s(F)$.
- The formula for ϵ is then:

  $$\epsilon(F', F) = \operatorname{sign} \det \operatorname{Mat}_{s(F)} s(F') \cup \operatorname{Cent}(F)$$

  with $\operatorname{Cent}(F)$ the center of the face F.
- The formula only requires that we know the $k-1$ dimensional and k-dimensional faces.

II. Homology

Polytopal complex

- A polytopal complex $\mathcal{PC}$ is a family of cells:
  - It contains $\emptyset$ and P such that for every face F one has $\emptyset \subset F \subset P$.
  - If F is a face and

$$\emptyset = F_0 \subset F_1 \subset \cdots \subset F_p = F$$

    is a chain, which cannot be further refined, then $\dim\ F = p$.
  - We set $dim\ \mathcal{PC} = dim\ P - 1$
  - If F_{p-1} and F_{p+1} are two cells of dimension $p-1$ and $p+1$ then there exist exactly two cells G, G' such that

$$F_{p-1} \subset G, G' \subset F_{p+1}$$

  - The faces F are equivalent to polytopes.
- Example:
  - Any plane graph, any map on a surface.
  - Any polyhedral subdivision
  - Any polytope.

Homology from the tesselation

Let $\mathcal{PC}$ be a polytopal complex.

- For any $0 \leq p \leq dim\, \mathcal{PC}$ denote by $C_p(\mathcal{PC}, \mathbb{Z})$ the $\mathbb{Z}$-module, whose basis is the p-dimensional faces of $\mathcal{PC}$.
- We denote by d_p the boundary operator:

$$d_p : C_p(\mathcal{PC}, \mathbb{Z}) \rightarrow C_{p-1}(\mathcal{PC}, \mathbb{Z})$$

  Note that $d_0 : C_0 \rightarrow \{0\}$.
- We define

$$B_p(\mathcal{PC}, \mathbb{Z}) = \mathrm{Im}\, d_{p+1} \text{ and } Z_p(\mathcal{PC}, \mathbb{Z}) = \text{Ker } d_p$$

- From the relation $d_p d_{p-1} = 0$ we have $B_p \subset Z_p$ and we define

$$H_p(\mathcal{PC}, \mathbb{Z}) = Z_p / B_p$$

- H_i is a sum of $\mathbb{Z}$ (rational) and $\mathbb{Z}/a\mathbb{Z}$ groups (torsion).

Topological invariance

- If $\mathcal{M}$ is a manifold and $\mathcal{PC}_1$ and $\mathcal{PC}_2$ are two polytopal subdivision modelled on it, then

$$H_p(\mathcal{PC}_1, \mathbb{Z}) = H_p(\mathcal{PC}_2, \mathbb{Z}) \text{ for } 0 \leq p \leq dim(\mathcal{M})x$$

- $H_0(\mathcal{PC}) = \mathbb{Z}^m$ with m the number of connected components.
- A space X is called contractible if it can be continuously deformed to a point x. For a contractible space, one has

$$H_0(X) = \mathbb{Z} \text{ and } H_p(X) = \{0\} \text{ for } p > 0$$

- For a n-dimensional polytope P we have

$$H_i(P) = \begin{cases} \mathbb{Z} & \text{if } i = 0 \text{ or } i = n-1 \\ 0 & \text{otherwise} \end{cases}$$

  The reason is that a n-dimensional polytope is essentially a $n-1$ dimensional sphere.

III. Resolutions and G-modules

G-modules

- We use the GAP notation for group action, on the right.
- A G-module M is a $\mathbb{Z}$-module with an action

$$\begin{array}{rcl} M \times G & \to & M \\ (m, g) & \mapsto & m.g \end{array}$$

- The group ring $\mathbb{Z}G$ formed by all finite sums

$$\sum_{g \in G} \alpha_g g \text{ with } \alpha_g \in \mathbb{Z}$$

  is a G-module.
- If the orbit of a point v under a group G is $\{v_1, \dots, v_m\}$, then the set of sums

$$\sum_{i=1}^{m} \alpha_i v_i \text{ with } \alpha_i \in \mathbb{Z}$$

  is a G-module.
- We can define the notion of generating set, free set, basis of a G-module. But not every finitely generated G-module admits a basis.

Polyhedral complex and G-module

Let us take P a n-dimensional polytopes and a group G acting on it.

- Denote n_k the number of orbits of faces of dimension k.
- For each dimension k we need to select a number of orbit representatives $G_1^k, \dots, G_{n_k}^k$.
- The differentials of a k-dimensional face F is

$$\begin{array}{rcl} d_k F & = & \sum_{i=1}^{N} \alpha_i F_i \ \ \text{(no group action)} \\ & = & \sum_{i=1}^{N} \alpha_i G_{p(i)}^{k-1} g_i \ \ \ g_i \in \Gamma \\ & = & \sum_{i=1}^{n_{k-1}} G_i^{k-1} \left\{ \sum_{j=1}^{n_i} \alpha_{i,j} g_{i,j} \right\} \ \ \text{(grouping terms)} \end{array}$$

- So, we can express the differencial d_k as a G-module $n_k \times n_{k-1}$ matrix.
- The terms g_i are not defined uniquely because the stabilizer may not be trivial.
- If we choose an orientation on F then we have as well defined an orientation on $F.g$ by the G-linearity.

Free G-modules

- A G-module is free if it admits a basis $e_1, \ldots, e_k$.
- For free G-modules, we can work in much the same way as for vector space, i.e., with matrices.
- Let $\phi : M \to M'$ be a G-linear homomorphism between two free G-modules and (e_i), (e'_i) two basis of M, M'.
- We can write $\phi(e_i) = \sum_j f_j a_{ij}$ with $a_{ij} \in \mathbb{Z}G$
- but then we have with $g_i \in \mathbb{Z}G$

$$\begin{array}{rcl} \phi(\sum_i e_i g_i) & = & \sum_i \phi(e_i g_i) \\ & = & \sum_i \phi(e_i) g_i \\ & = & \sum_j f_j (\sum_i a_{ij} g_i) \end{array}$$

- More generally the "right" matrix product is $AB = C$ with $c_{ij} = \sum_k b_{kj} a_{ik}$.

Resolutions

Take G a group.

- A resolution of a group G is a sequence of G-modules $(M_i)_{i\geq 0}$:
$$\mathbb{Z} \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \leftarrow \dots$$
together with a collection of G-linear operators $d_i : M_i \to M_{i-1}$ such that $\text{Ker } d_i = \operatorname{Im} d_{i-1}$
- What is useful to homology computations are free resolutions with all M_i being free G-modules.
- In general if a group G acts on a polytope P then some faces have non-trivial stabilizer. So, the resolution that comes from the cell-complex is not free in general.
- In terms of homology if an element s stabilizes a face F then we have
$$F.s = \epsilon_F(s)F \text{ with } \epsilon_F(s) = \pm 1$$
whether s preserves the orientation of F or not. The sign can be computed by the same technique as for $\epsilon(F', F)$.

IV. Group homology

Covering space

- If X, Y are two topological spaces, then a mapping $\phi : X \to Y$ is called a covering map if
  - For any $y \in Y$, there exist a neighborhood N_y of y
  - such that for any $x \in \phi^{-1}(y)$ there exist a neighborhood N_x with
    - $N_y \subset \phi(N_x)$,
    - $N_x \cap N_{x'} = \emptyset$ if $x \neq x'$,
    - $\phi : N_x \to \phi(N_x)$ is bijective.
- As a consequence $|\phi^{-1}(y)|$ is independent of y and ϕ is surjective.
- There exist a group G of homeomorphisms of X such that for any $x, x' \in X$, there is a $g \in G$ such that $g(x) = x$.
- We then write $X/_G = Y$.
- An example is $X = \mathbb{R}$, $Y = S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and $\phi(x) = e^{ix}$

Group homology

- Take G a group, suppose that:
  - X is a contractible space.
  - G acts fixed point free on X.

  Then we define $H_p(G) = H_p(X/G)$.
- The space X is then a classifying space.
- Every group has a classifying space but finding them can be difficult.
- For example if $G = \mathbb{Z}^2$, then $X = \mathbb{R}^2$, $Y = X/G$ is a 2-dimensional torus and one has
  - $H_0(G) = \mathbb{Z}$,
  - $H_1(G) = \mathbb{Z}^2$,
  - $H_2(G) = \mathbb{Z}$,
  - $H_i(G) = 0$ for $i > 2$.

Using resolutions for homology

- The constructon of abstract spaces is relatively complicated.
- The method is to take a free-resolution of a group G.
- The homology is then obtained by killing off the G-action of a free resolution, i.e replacing the G-modules $(\mathbb{Z}G)^k$ by $\mathbb{Z}^k$, replacing accordingly the d_i by $\tilde{d}_i$ and getting

$$H_i(G, \mathbb{Z}) = \text{Ker } \tilde{d}_i / \mathrm{Im}\, \tilde{d}_{i-1}$$

- The big problem is to get free resolutions. It is not an easy task.
- Two alternatives:
  - Compute free resolutions for the stabilizers and put it all together with the CTC Wall lemma. KeyWord: Spectral sequence
  - Compute a resolution with only finite stabilizers: Kill the faces with orientation reversing stabilizers. Kill the G-action. Then compute the quotient. It is the homology modulo the torsion.

V. Perfect forms and domains

Arithmetic minimum of positive definite matrices

- Denote by S^n the vector space of real symmetric $n \times n$ matrices, $S^n_{>0}$ the convex cone of real symmetric positive definite $n \times n$ matrices and $S^n_{\geq 0}$ the convex cone of real symmetric positive semidefinite $n \times n$ matrices.
- The arithmetic minimum of $A \in S^n_{>0}$ is

$$\min(A) = \min_{x \in \mathbb{Z}^n - \{0\}} A[x] \text{ with } A[x] = x^T A x$$

- The minimal vector set of $A \in S^n_{>0}$ is

$$\mathrm{Min}(A) = \{x \in \mathbb{Z}^n \mid A[x] = \min(A)\}$$

- Both $\min(A)$ and $\mathrm{Min}(A)$ can be computed using some programs (for example SV by Vallentin)
- The matrix $A_{hex} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ has

$$\mathrm{Min}(A_{hex}) = \{\pm(1,0), \pm(0,1), \pm(1,-1)\}.$$

Equivalence and Stabilizer

- If $A, B \in S^n_{>0}$, they are called arithmetically equivalent if there is at least one $P \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$A = P^T B P$$

- The arithmetic automorphism group of $A \in S^n_{>0}$ is defined as the set of $P \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$A = P^T A P$$

- In practice, Plesken/Souvignier wrote a program ISOM for testing arithmetic equivalence and a program AUTO for computing automorphism groups.
- Those program requires to find a set of short vectors and use partition backtrack.
- They are a-priori exponential in time but in practice more than ok in dimension less than 10.

Perfect forms and domains

- A matrix $A \in S^n_{>0}$ is perfect (Korkine & Zolotarev) if the equation

$$B \in S^n \text{ and } x^T Bx = \min(A) \text{ for all } x \in \mathrm{Min}(A)$$

  implies $B = A$.
- Theorem: (Korkine & Zolotarev) If a form is extreme then it is perfect.
- Up to a scalar multiple, perfect forms are rational.
- If $v \in \mathbb{Z}^n$ then the corresponding rank 1 form is $p(v) = vv^T$.
- If A is a perfect form, its perfect domain is

$$\mathrm{Dom}(A) = \sum_{v \in \mathrm{Min}(A)} \mathbb{R}_+ p(v)$$

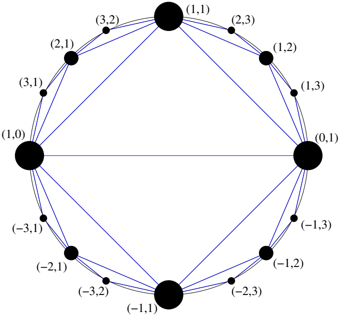
- If A has m shortest vectors then $\mathrm{Dom}(A)$ has $\frac{m}{2}$ extreme rays.
- So actually, the perfect domains realize a tessellation not of $S^n_{>0}$, nor $S^n_{\geq 0}$ but of the rational closure $S^n_{rat,\geq 0}$.

Finiteness

- Theorem:(Voronoi) Up to arithmetic equivalence there is only finitely many perfect forms.
- The group $\mathrm{GL}_n(\mathbb{Z})$ acts on $S^n_{>0}$:

$$Q \mapsto P^t Q P$$

  and we have $\mathrm{Min}(P^t Q P) = P^{-1}\,\mathrm{Min}(Q)$
- $\mathrm{Dom}(P^T Q P) = c(P)^T\,\mathrm{Dom}(Q) c(P)$ with $c(P) = \left(P^{-1}\right)^T$
- For $n = 2$, we get the classical picture:



Known results on lattice packing density maximization

dim.	Nr. of perfect forms	Best lattice packing
2	1 (Lagrange)	A_2
3	1 (Gauss)	A_3
4	2 (Korkine & Zolotarev)	D_4
5	3 (Korkine & Zolotarev)	D_5
6	7 (Barnes)	E_6 (Blichfeldt & Watson)
7	33 (Jaquet)	E_7 (Blichfeldt & Watson)
8	10916 (DSV)	E_8 (Blichfeldt & Watson)
9	$\geq$500000	Λ_9?
24	?	Leech (Cohn & Kumar)

- The enumeration of perfect forms is done with the Voronoi algorithm.
- The number of orbits of faces of the perfect domain tessellation is much higher but finite (Known for $n \leq 7$)
- Blichfeldt used Korkine-Zolotarev reduction theory.
- Cohn & Kumar used Fourier analysis and Linear programming.

VI. Ryshkov polyhedron and the Voronoi algorithm

The Ryshkov polyhedron

- The Ryshkov polyhedron R_n is defined as

$$R_n = \{A \in S^n \text{ s.t. } A[x] \geq 1 \text{ for all } x \in \mathbb{Z}^n - \{0\}\}$$

- R_n is invariant under the action of $\mathrm{GL}_n(\mathbb{Z})$.
- R_n is locally polyhedral, i.e. for a given $A \in R_n$

$$\{x \in \mathbb{Z}^n \text{ s.t. } A[x] = 1\}$$

  is finite
- Vertices of R_n correspond to perfect forms.
- For a form $A \in R_n$ we define the local cone

$$Loc(A) = \{Q \in S^n \text{ s.t. } Q[x] \geq 0 \text{ if } A[x] = 1\}$$

The Voronoi algorithm

- Find a perfect form (say A_n), insert it to the list $\mathcal{L}$ as undone.
- Iterate
  - For every undone perfect form A in $\mathcal{L}$, compute the local cone $Loc(A)$ and then its extreme rays.
  - For every extreme ray r of $Loc(A)$ realize the flipping, i.e. compute the adjacent perfect form $A' = A + \alpha r$.
  - If A' is not equivalent to a form in $\mathcal{L}$, then we insert it into $\mathcal{L}$ as undone.
- Finish when all perfect forms have been treated.

The sub-algorithms are:

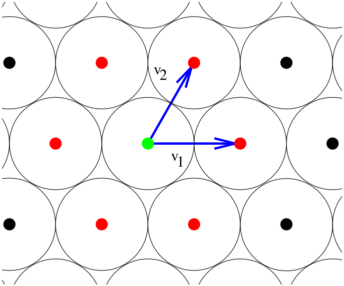
- Find the extreme rays of the local cone $Loc(A)$ (use CDD or LRS or any other program)
- For any extreme ray r of $Loc(A)$ find the adjacent perfect form A' in the Ryshkov polyhedron R_n
- Test equivalence of perfect forms using ISOM

Flipping on an edge I

$$\mathrm{Min}(A_{hex}) = \{\pm(1,0), \pm(0,1), \pm(1,-1)\}$$

with

$$A_{hex} = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} \text{ and } D = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

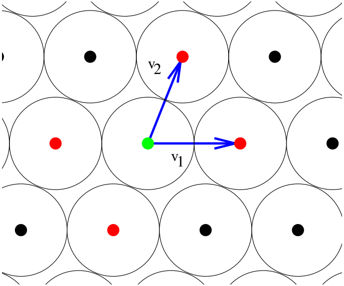


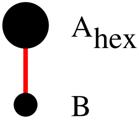
Flipping on an edge II

$$\mathrm{Min}(B) = \{\pm(1,0), \pm(0,1)\}$$

with

$$B = \begin{pmatrix} 1 & 1/4 \\ 1/4 & 1 \end{pmatrix} = A_{hex} + D/4$$



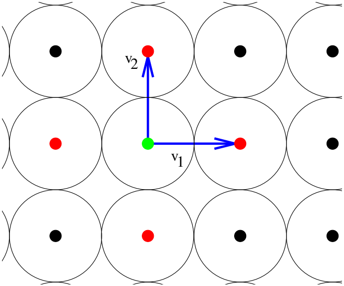


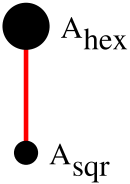
Flipping on an edge III

$$\mathrm{Min}(A_{sqr}) = \{\pm(1,0), \pm(0,1)\}$$

with

$$A_{sqr} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A_{hex} + D/2$$



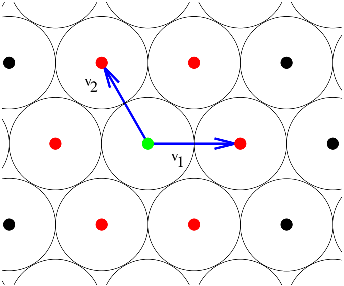


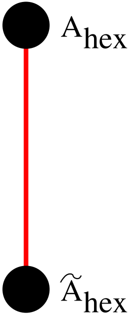
Flipping on an edge IV

$$\mathrm{Min}(\tilde{A}_{hex}) = \{\pm(1,0), \pm(0,1), \pm(1,1)\}$$

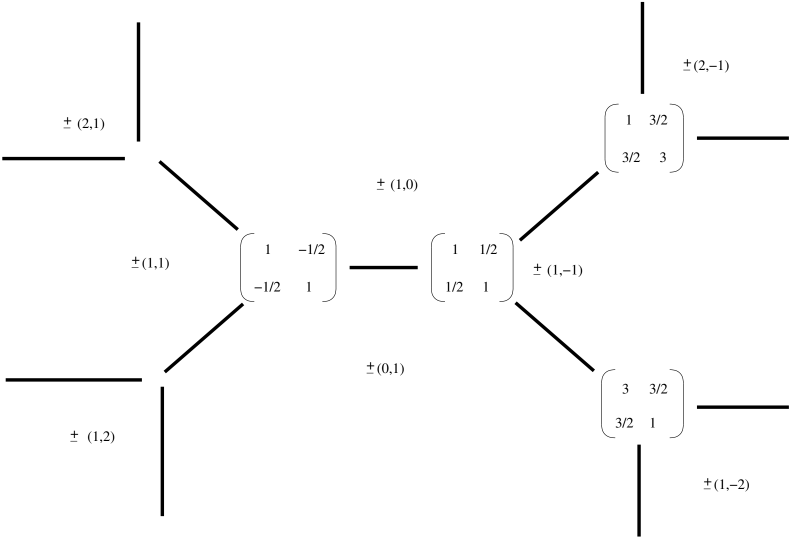
with

$$\tilde{A}_{hex} = \begin{pmatrix} 1 & -1/2 \\ -1/2 & 1 \end{pmatrix} = A_{hex} + D$$





The Ryshkov polyhedron R_2



Well rounded forms and retract

- A form Q is said to be well rounded if it admits vectors v_1, ..., v_n such that
  - $(v_1, \dots, v_n)$ form a $\mathbb{R}$-basis of $\mathbb{R}^n$ (not necessarily a $\mathbb{Z}$-basis)
  - $v_1, \dots, v_n$ are shortest vectors of Q.
- Well rounded forms correspond to bounded faces of R_n.
- Every form can be continuously deformed to a well rounded form and this defines a retracting homotopy of R_n onto a polyhedral complex WR_n of dimension $\frac{n(n-1)}{2}$.
- Every face of WR_n has finite stabilizer.
- Actually, in term of dimension, we cannot do better:
  - A. Pettet and J. Souto, *Minimality of the well rounded retract*, Geometry and Topology, **12** (2008), 1543-1556.
- We also cannot reduce ourselves to lattices whose shortest vectors define a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

Topological applications

- The fact that we have finite stabilizers for all faces means that we can compute rational homology/cohomology of $\mathrm{GL}_n(\mathbb{Z})$ efficiently.
- This has been done for $n \leq 7$
  - P. Elbaz-Vincent, H. Gangl, C. Soulé, *Perfect forms, K-theory and the cohomology of modular groups*, Adv. Math 245 (2013) 587–624.
- As an application, we can compute $K_n(\mathbb{Z})$ for $n \leq 8$.
- By using perfect domains, we can compute the action of Hecke operators on the cohomology.
- This has been done for $n \leq 4$:
  - P.E. Gunnells, *Computing Hecke Eigenvalues Below the Cohomological Dimension*, Experimental Mathematics 9-3 (2000) 351–367.
- The above can, in principle, be extended to the case of $\mathrm{GL}_n(R)$ with R a ring of algebraic integers.

VII. Tessellations

Linear Reduction theories for S^n

Some $\mathrm{GL}_n(\mathbb{Z})$ invariant tessellations of $S^n_{rat,\geq 0}$:

- The perfect form theory (Voronoi I) for lattice packings (full face lattice known for $n \leq 7$, perfect domains known for $n \leq 8$)
- The central cone compactification (Igusa & Namikawa) (Known for $n \leq 6$)
- The L-type reduction theory (Voronoi II) for Delaunay tessellations (Known for $n \leq 5$)
- The C-type reduction theory (Ryshkov & Baranovski) for edges of Delaunay tessellations (Known for $n \leq 5$)
- The Minkowski reduction theory (Minkowski) it uses the successive minima of a lattice to reduce it (Known for $n \leq 7$) not face-to-face
- Venkov's reduction theory also known as Igusa's fundamental cone (finiteness proved by Crisalli and Venkov)

Central cone compactification

- We consider the space of integral valued quadratic forms:

$$I_n = \{A \in S^n_{>0} \text{ s.t. } A[x] \in \mathbb{Z} \text{ for all } x \in \mathbb{Z}^n\}$$

  All the forms in I_n have integral coefficients on the diagonal and half integral outside of it.
- The centrally perfect forms are the elements of I_n that are vertices of conv I_n.
- For $A \in I_n$ we have $A[x] \geq 1$. So, $I_n \subset R_n$
- Any root lattice is a vertex both of R_n and conv I_n.
- The centrally perfect forms are known for $n \leq 6$:

dim.	Centrally perfect forms
2	A_2 (Igusa)
3	A_3 (Igusa)
4	A_4, D_4 (Igusa)
5	A_5, D_5 (Namikawa)
6	A_6, D_6, E_6 (Dutour Sikirić)

- By taking the dual we get tessellations of $S^n_{rat,\geq 0}$.

Non-polyhedral reduction theories

- Some works with non-polyhedral, but still manifold domains:
  - R. MacPherson and M. McConnel, *Explicit reduction theory for Siegel modular threefolds*, Invent. Math. **111** (1993) 575–625.
  - D. Yasaki, *An explicit spine for the Picard modular group over the Gaussian integers*, Journal of Number Theory, **128** (2008) 207–234.
- Other works in complex hyperbolic space using Poincaré polyhedron theorem:
  - M. Deraux, *Deforming the* $\mathbb{R}$*-fuchsian* $(4,4,4)$*-lattice group into a lattice*.
  - E. Falbel and P.-V. Koseleff, *Flexibility of ideal triangle groups in complex hyperbolic geometry*, Topology **39** (2000) 1209–1223.
- Other works for non-manifold setting would be:
  - T. Brady, *The integral cohomology of* $Out_{+}(F_3)$, Journal of Pure and Applied Algebra **87** (1993) 123–167.
  - K.N. Moss, *Cohomology of* $\mathrm{SL}(n, \mathbb{Z}[1/p])$, Duke Mathematical Journa **47-4** (1980) 803–818.

VIII. Modular forms

Modular forms for $\mathrm{SL}(2, \mathbb{Z})$

- We call $\mathbb{H} = \{z \in \mathbb{C} \text{ s.t. } Im(z) > 0\}$ the upper half-plane.
- A function $f : \mathbb{H} \to \mathbb{C}$ is called a modular form of weight k for $\mathrm{SL}(2, \mathbb{Z})$ if:
  - f is holomorphic
  - For any matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

  - f is holomorphic at the cusps.
- Modular forms are of primary importance in number theory.
- Let us call M_k the space of modular forms of weight k. We have the Shimura-Eichler isomorphism:

$$M_k \simeq H_1(\mathrm{SL}_2(\mathbb{Z}), R_{k-2})$$

  with R_k the space of homogeneous polynomials of degree 2.
- Note that the space $\mathbb{H}$ can be mapped onto $S^2_{>0}$.

The general case and Hecke operators

- We want to find modular forms for some finite index subgroups Γ of $\mathrm{SL}(n, \mathbb{Z})$ with $n > 2$ (and other groups as well).
- What is known is that the spaces of modular forms are isomorphic to the space

$$H_k(\Gamma, \mathbb{Q})$$

- But in order to understand the operators we need more than just the dimensio and the solution to that is to consider the Hecke operators.
- This is the only way we know of extracting the arithmetic informations.

IX. Hecke operators on homology

Definitions

We take Γ a finite index subgoup of $\mathrm{SL}(n, \mathbb{Z})$.

- We consider elements $g \in \mathrm{GL}(n, \mathbb{Q})$ such that $\Gamma \cap g^{-1}\Gamma g$ has finite index in Γ.
- We want to consider the action of g on the homology classes. The problem is that the homology are obtained after killing the Γ action, so we need to consider something else than just g.
- The idea is to split the double coset

$$\Gamma g \Gamma = g_1 \Gamma \cup g_2 \Gamma \cup \cdots \cup g_m \Gamma$$

  into right cosets.
- The splitting can be done by a very simple iterative algorithm if we have:
  - A generating set for Γ.
  - An oracle function ϕ for testing membership in Γ

Actions on the perfect form complex

- A k-dimensional face F of the perfect form complex is defined as a family of vectors $v_1, \ldots, v_m$ with $v_i \in \mathbb{Z}^n$.
- The image $F.g$ is defined by the vectors $v_1 g, \ldots, v_m g$.
- In dimension $k = 1$ all is ok:
  - They are spanned by just one vector. So the image $F.g$ is spanned by $v_1 g$.
  - $v_1 g$ is not necessarily integral, but it is a multiple of an integral vector.
  - So, we can define the action in dimension 1.
- For higher dimensions we want to do recursively. That is if:

$$d_k F = \sum_i \alpha_i F_i h_i \text{ with } h_i \in \Gamma$$

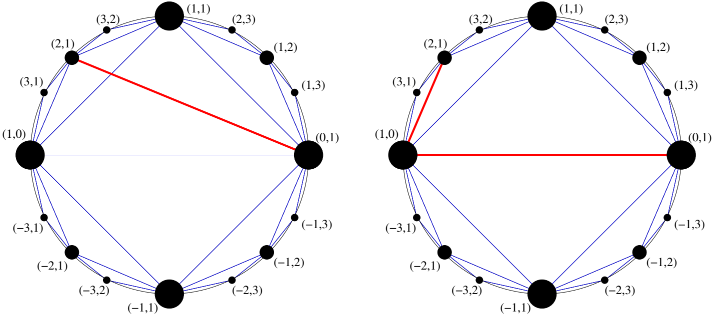
then

$$\begin{aligned} d_k(F.g) = b &= \textstyle\sum_i \alpha_i F_i h_i g \\ &= \textstyle\sum_i \alpha_i F_i g_i k_i \text{ with } k_i \in \Gamma \end{aligned}$$

So, we need to compute on all cosets. We must have $d_{k-1} b = 0$.

Two dimensional example

- Let us take the face $F = \{(1,0),(0,1)\}$ and $g = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$.
- We then have



- So we set

$$F.g = F.\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} + F$$

Computing on the perfect form complex: Groups

- We need to compute stabilizers of cells (possibly infinite) and checking equivalence.
- What we can do is for a face $F = \{v_1, \dots, v_m\}$ with $\text{rank}\{v_1, \dots, v_m\} = k < n$ is to:
  - Find a subspace $W \subset \mathbb{Z}^n$ of rank k with $v_i \in F$ and $W = (W \otimes \mathbb{R}) \cap \mathbb{Z}^n$.
  - Compute the finite group of automorphism of F in W by using AUTO.
  - Determine directly the group preserving W pointwise.

  This requires doing the number theory which is ok for $\mathbb{Z}^n$ but harder in other cases.
- An alternative is for a face F to consider all full dimensional cells G with $F \subset G$. We then:
  - have a finite set of such pairs (F, G) up to equivalence.
  - We can enumerate all of them by using the full-dimensional cells.

  This is harder computationally but much simpler and general.

Computing on the perfect form complex: Equations I

- In order to build the Hecke operators, we need to be able to solve
$$d_k x = b$$
for x a k-dimensional chain and b a $k-1$ dimensional chain.
- A necessary and sufficient condition for x to exist is $d_{k-1} b = 0$.
- In other words we have an infinite integral linear system.
- The chosen solution is to take a family $C_1, \dots C_r$ of top-dimensional cells such that
  - Any face occuring in b is contained in at least one C_i.
  - The graph defined by all C_i with adjacency relation is connected.
- If the system has no solution then we iterate by adding all cells neighboring to the C_i.

Computing on the perfect form complex: Equations II

- We are thus led to trying to find solutions of equations

$$Ax = b$$

  with A a very large matrix.
- We want to find sparse solutions because they are expected to be the nicest and simplest (compressed sensing).
- When searching for sparse solutions, a good heuristic is to svole the linear program

$$\min \|x\|_1 \text{ with } Ax = b$$

- We found good results with `GLPK` and bad ones with `LP_SOLVE` and `cdd`.
- Further improvement depend critically on improvements to the solver.

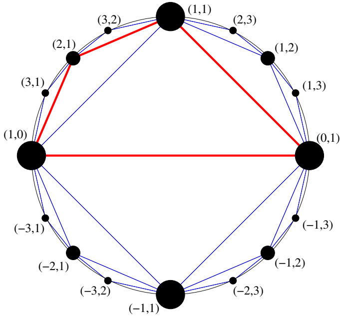
The invariance problem I

We set $F.g = \sum_i \alpha_i F_i g_i$.

- In order for the operator to be consistent we need that for every s stabilizing F we have
$$F.sg = F.g\epsilon_F(s)$$
- If $sg = g'v$ with $g'\Gamma \neq g\Gamma$ then we simply write
$$F.g' = (F.g)v^{-1}\epsilon_F(s)$$
- However if $sg = gv$ with $v \in \Gamma$ then we face a consistency problem because the solution of our system is not necessarily integral.
- Let us call $\Gamma(F, g)$ the corresponding stabilizer (maybe infinite).
- Let us call $O(x)$ the orbit of the solution x under $\Gamma(F, g)$.
- The following is invariant:
$$\frac{1}{|O(x)|}\sum_{u\in O(x), u.g=x} u\epsilon_F(g)$$

The invariance problem II

- For our example this gives



- In order to have $O(x)$ finite we impose that the solution x has the same singularities as $F.g$.
- If the solutions are not consistent then we cannot solve the system.
- By taking the average we forfeit the integral solution and so we can only compute the action on rational homology.

The action on homology

- Say, the group $H_k(\Gamma, \mathbb{Q})$ has dimension p.
- It has a basis of cycles

$$c_i = \sum_{j=1}^{n_k} \alpha_{i,j} F_i$$

  with $\alpha_{i,j} \in \mathbb{Z}$ and F_i representatives of orbits of k-dimensional faces of the cell-complex.
- The Hecke operator on a cycle c is defined as

$$T_g(c) = \sum_i c g_i$$

- Theorem: The operator T_g preserves H_k.
- The characteristic polynomial of T_g is the important arithmetic information.

THANK

YOU