Equivariant L-type and coverings

Mathieu Dutour Sikiric

Institut Rudjer Boskovic, Zagreb

Achill Schuermann

Magdeburg University

Frank Vallentin

TU Munich and CWI Amsterdam

I. Lattices

and

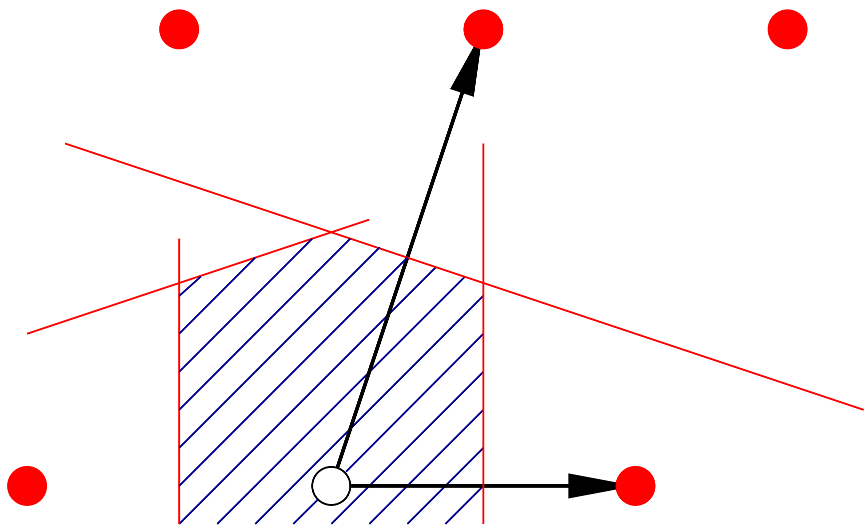
Delaunay polytopes

The Voronoi polytope of a lattice

- A lattice L is a rank n subgroup of $\mathbb{R}^n$, i.e.

$$L = v_1\mathbb{Z} + \cdots + v_n\mathbb{Z} .$$

- The Voronoi cell $\mathcal{V}$ of L is defined by inequalities $\langle x, v\rangle \leq \frac{1}{2}||v||^2$ for $v \in L$.
- $\mathcal{V}$ is a polytope, i.e. it has a finite number of vertices (of dimension 0), faces and facets (of dimension $n-1$).



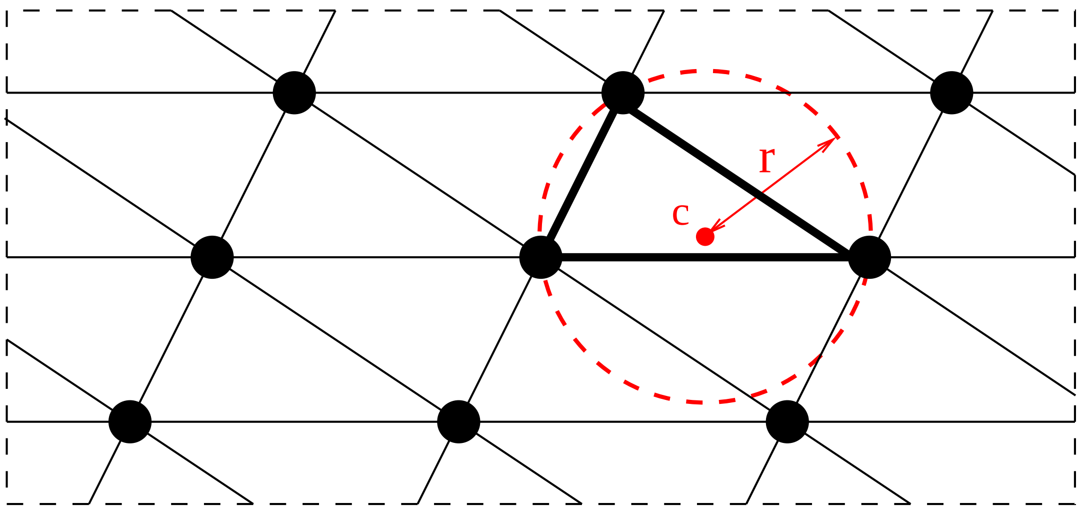
Empty sphere and Delaunay polytopes

A sphere $S(c,r)$ of center c and radius r in an n-dimensional lattice L is said to be an empty sphere if:

(i) $\|v-c\| \geq r$ for all $v \in L$,

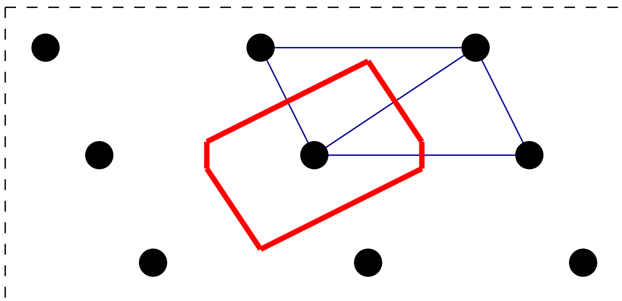
(ii) the set $S(c,r) \cap L$ contains $n+1$ affinely independent points.

A Delaunay polytope P in a lattice L is a polytope, whose vertex-set is $L \cap S(c,r)$.



Voronoi and Delaunay in lattices

- Vertices of Voronoi polytope are center of empty spheres which defines Delaunay polytopes.
- Voronoi and Delaunay polytopes define dual tesselations of the space $\mathbb{R}^n$ by polytopes.
- Every k-dimensional face of a Delaunay polytope is orthogonal to a $(n-k)$-dimensional face of a Voronoi polytope.



- Given a lattice L, it has a finite number of orbits of Delaunay polytopes under translation.

Lattices with two Delaunay polytopes

- Take $L = \mathbb{Z}^n$; Delaunay:

Name	Center	Nr. vertices	Radius
Cube	$(\frac{1}{2})^n$	2^n	$\frac{1}{2}\sqrt{n}$

- Take $D_n = \{x \in \mathbb{Z}^n \mid \sum_{i=1}^n x_i$ is even$\}$; Delaunay:

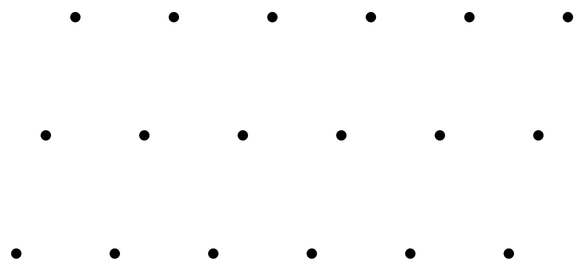
Name	Center	Nr. vertices	Radius
Half-Cube	$(\frac{1}{2})^n$	$\frac{1}{2}2^n$	$\frac{1}{2}\sqrt{n}$
Cross-polytope	$(1, 0^{n-1})$	$2n$	1

- Take $E_8 = D_8 \cup (\frac{1}{2}^8) + D_8$; Delaunay:

Name	Center	Nr. vertices	Radius
Simplex	$(\frac{5}{6}, \frac{1}{6}^7)$	9	$\sqrt{\frac{8}{9}}$
Cross-polytope	$(1, 0^7)$	16	1

Lattice packings

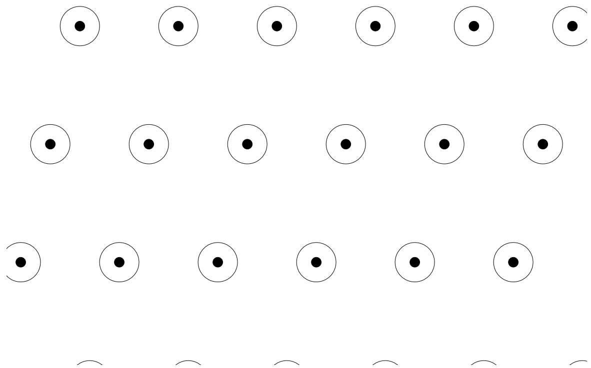
- A lattice L is a subgroup of $\mathbb{R}^d$ of the form $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_d$.



- If L is a lattice, the lattice packing is the packing defined by taking the maximal value of $\alpha > 0$ such that $L + B(0, \alpha)$ is a packing.

Lattice packings

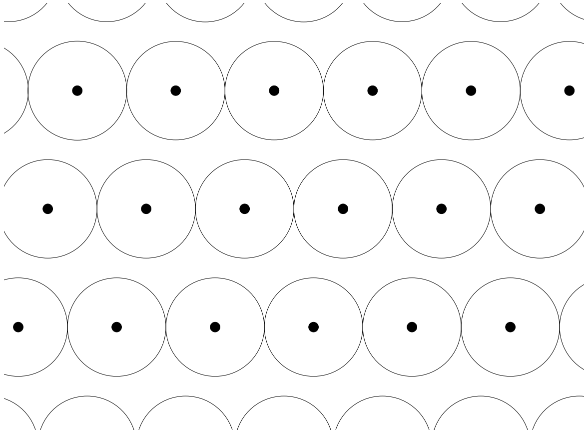
- A lattice L is a subgroup of $\mathbb{R}^d$ of the form $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_d$.



- If L is a lattice, the lattice packing is the packing defined by taking the maximal value of $\alpha > 0$ such that $L + B(0, \alpha)$ is a packing.

Lattice packings

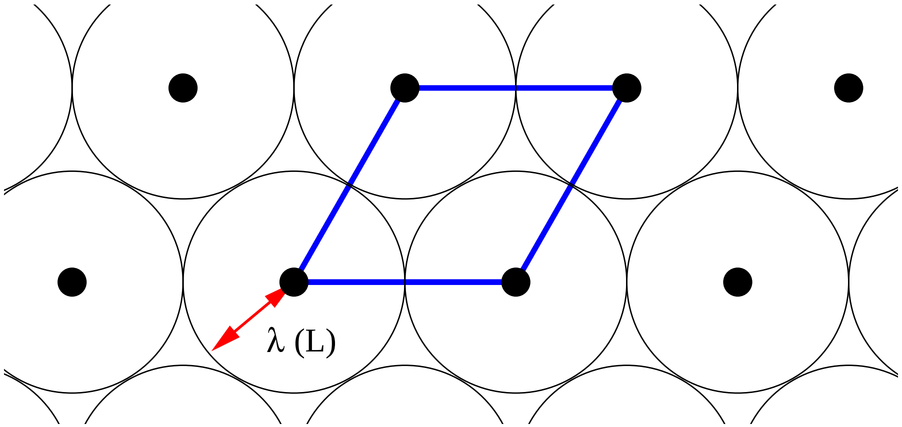
- A lattice L is a subgroup of $\mathbb{R}^d$ of the form $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_d$.



- If L is a lattice, the lattice packing is the packing defined by taking the maximal value of $\alpha > 0$ such that $L + B(0, \alpha)$ is a packing.

Density of lattice packing

- The lattice packing defined by a lattice L:



- The packing density has the expression

$$\alpha(L) = \frac{\lambda(L)^n \kappa_n}{det\ L} \quad \text{with} \quad \lambda(L) = \frac{1}{2} \min_{v \in L - \{0\}} ||v||,$$

κ_n the volume of the unit ball $B(0,1)$ and $det\ L$ the volume of an unit cell.

Lattice covering

- We consider covering of $\mathbb{R}^n$ by n-dimensional balls of the same radius, whose center belong to a lattice L.

- The covering density has the expression

$$\Theta(L) = \frac{\mu(L)^n \kappa_n}{det(L)} \geq 1$$

with $\mu(L)$ being the largest radius of Delaunay polytopes and κ_n the volume of the unit ball B^n.

- Objective is to minimize $\Theta(L)$. Solution for $n \leq 5$: A_n^*.

Lattice packing-covering

L is a n-dimensional lattice.

- We want a lattice, such that the sphere packing (resp, covering) obtained by taking spheres centered in L with maximal (resp, minimal) radius are both good.
- The quantity of interest is

$$\frac{\Theta(L)}{\alpha(L)} = \{\frac{\mu(L)}{\lambda(L)}\}^n \geq 1$$

- Lattice packing-covering problem: minimize $\frac{\Theta(L)}{\alpha(L)}$.

Dim.	Solution	Dim.	Solution
2	A_2^*	4	H_4 (Horvath lattice)
3	A_3^*	5	H_5 (Horvath lattice)

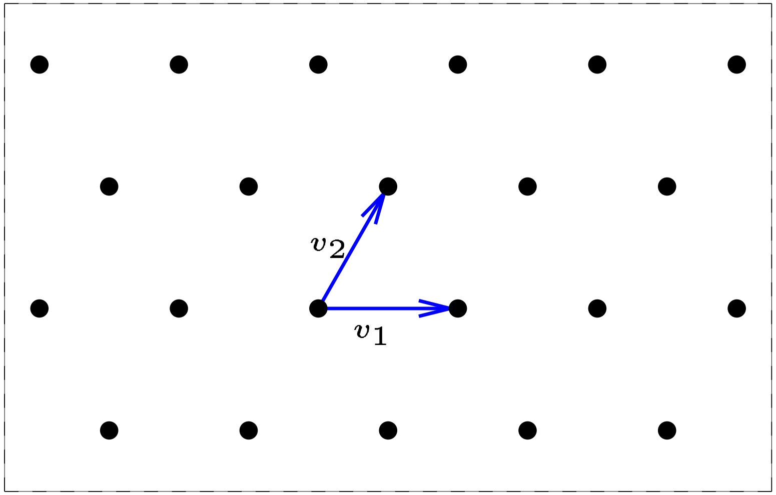
II. Gram matrices

and

computational methods

Gram matrix and lattices

- Denote by S^n the vector space of real symmetric $n \times n$ matrices and $S^n_{>0}$ the convex cone of real symmetric positive definite $n \times n$ matrices.
- Take a lattice $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ and associate to it the Gram matrix $G_{\mathbf{v}} = (\langle v_i, v_j \rangle)_{1 \le i,j \le n} \in S^n_{>0}$.
- Example: take the hexagonal lattice generated by $v_1 = (1, 0)$ and $v_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$



$$G_{\mathbf{v}} = \frac{1}{2} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

Isometric lattices

- Take a lattice $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ with $v_i = (v_{i,1}, \ldots, v_{i,n}) \in \mathbb{R}^n$ and write the matrix

$$V = \begin{pmatrix} v_{1,1} & \ldots & v_{n,1} \\ \vdots & \ddots & \vdots \\ v_{1,n} & \ldots & v_{n,n} \end{pmatrix}$$

  and $G_{\mathbf{v}} = V^T\,V$
- If $M \in S^n_{>0}$, then there exists V such that $M = V^T\,V$
- If $M = V_1^T\,V_1 = V_2^T\,V_2$, then $V_1 = OV_2$ with $O^T\,O = I_n$ (i.e. O corresponds to an isometry of $\mathbb{R}^n$).
- Also if L is a lattice of $\mathbb{R}^n$ with basis $\mathbf{v}$ and u an isometry of $\mathbb{R}^n$, then $G_{\mathbf{v}} = G_{u(\mathbf{v})}$.

Changing basis

- If $\mathbf{v}$ and $\mathbf{v}'$ are two basis of a lattice L then $V' = VP$ with $P \in GL_n(\mathbb{Z})$. This implies

$$G_{\mathbf{v}'} = V'^T V' = (VP)^T VP = P^T \{V^T V\} P = P^T G_{\mathbf{v}} P$$

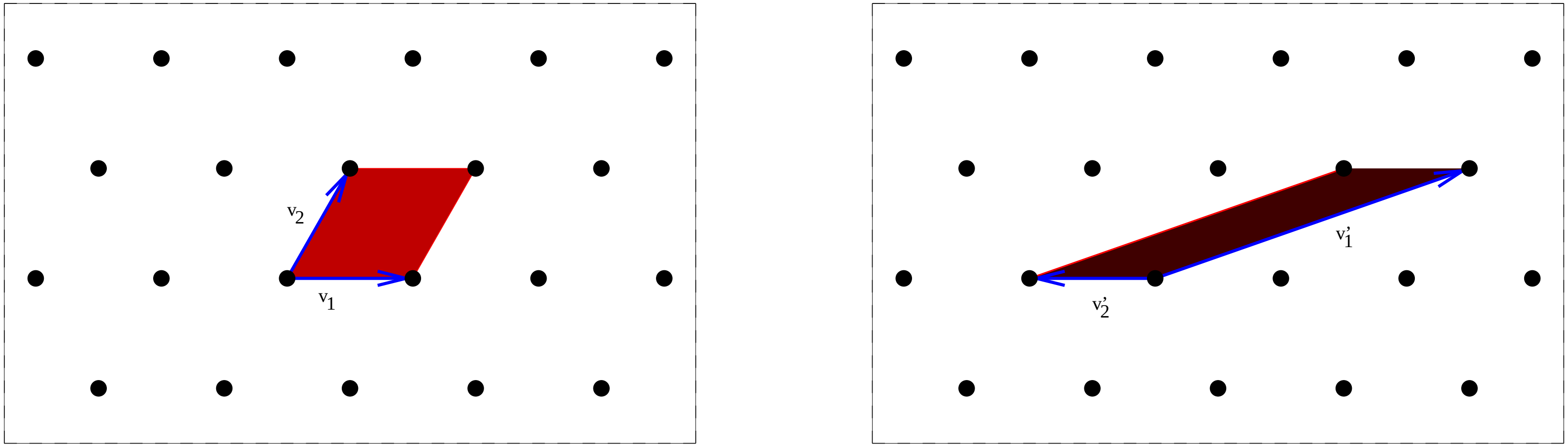
- If $A, B \in S^n_{>0}$, they are called arithmetically equivalent if there is at least one $P \in GL_n(\mathbb{Z})$ such that

$$A = P^T BP$$

- Lattices up to isometric equivalence correspond to $S^n_{>0}$ up to arithmetic equivalence.
- In practice, Plesken wrote a program isom for testing arithmetic equivalence.

An example

- Take the hexagonal lattice and two basis in it.



$v_1 = (1,0)$ and $v_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ $\quad v'_1 = (\frac{5}{2}, \frac{\sqrt{3}}{2})$ and $v'_2 = (-1,0)$

- One has $v'_1 = 2v_1 + v_2$, $v'_2 = -v_1$ and $P = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$

$$G_{\mathbf{v}} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \text{ and } G_{\mathbf{v}'} = \begin{pmatrix} 7 & -\frac{5}{2} \\ -\frac{5}{2} & 1 \end{pmatrix} = P^T G_{\mathbf{v}} P$$

The enumeration problem

- Given a matrix $M \in S^n_{>0}$, we want to compute the Delaunay polytopes of a lattice corresponding to M.
- There is a finite number of Delaunay up to translation but still on the order of $(n+1)!$.
- If $A \in S^n_{>0}$, then the symmetry group

$$Aut(A) = \{P \in GL_n(\mathbb{Z}) \mid A = P^T A P\}$$

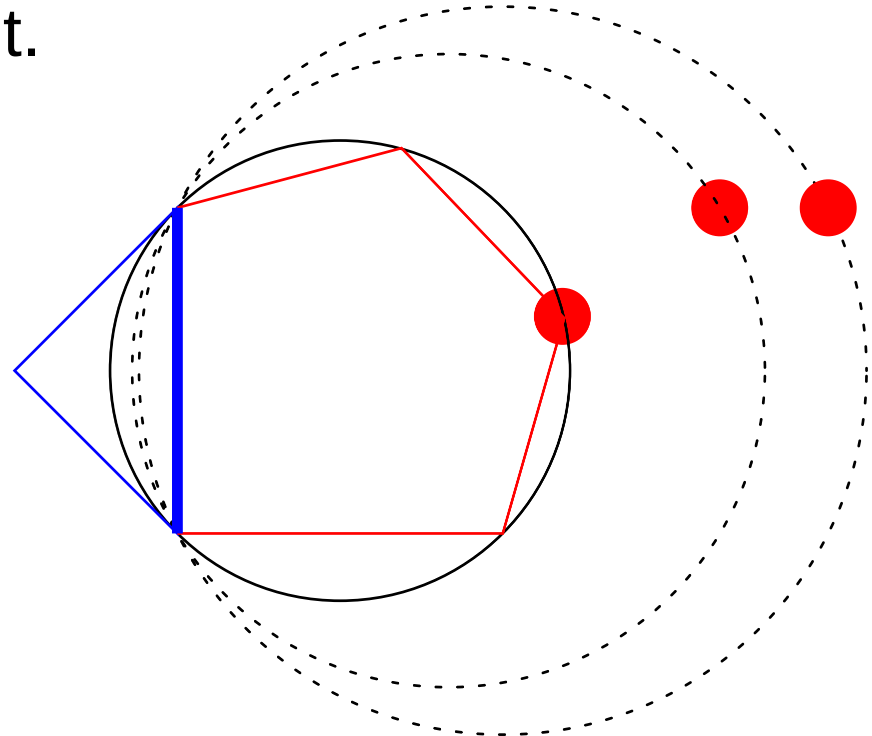
is finite.
- $Aut(A)$ corresponds to isometries of the corresponding lattice. We want to use those symmetries to accelerate the computation.

Closest Vector Problem

- Given a lattice L, a vector c, find all vectors $v \in L$ such that
$$||v - c|| \text{ is minimal}$$
or in other term, if $M \in S^n_{>0}$ and $c \in \mathbb{R}^n$, find all $v \in \mathbb{Z}^n$ such that
$${}^t(v-c)M(v-c) \text{ is minimal}$$
- CVP is conjecturally a NP problem.
- Only way is to do an exhaustive search in a set of possible solutions, two programs:
  - Lattice-CVP (Dutour) use a hypercube, performing well up to dimension 10.
  - Voro (Vallentin) use an ellipsoid, performing well up to dimension, say 40.

Finding Delaunays

- Given a Delaunay polytope and a facet of it, there exist a unique adjacent Delaunay polytope.
- We use an iterative procedure:
  - Select a point outside the facet.
  - Create the sphere around it.
  - If there is no interior point finish, otherwise rerun with this point.



Finding Delaunay decomposition

- Find the isometry group of the lattice (program autom by Plesken & Souvignier).
- Find an initial Delaunay polytope (program finddel) by Vallentin and insert into list of orbits as undone.
- Iterate
  - Find the orbit of facets of undone Delaunay polytopes (GAP + lrs by Avis + Recursive Adjacency Decomposition method by Dutour).
  - For every facet, find the adjacent Delaunay polytope.
  - For every Delaunay test if they are isomorphic to existing ones. If not insert them to the list as undone.
  - Finish when every orbit is done.

Computing dual description

- cdd and lrs are general purpose programs for finding dual descriptions, which does not work for some polytopes.
- For symmetric convex cones, it suffices to compute orbits of facets
- The key idea of the Adjacency Decomposition Method is:
  - compute some initial facet (by linear programming) and insert the orbit into the list of orbits.
  - compute the adjacent facets to this facet (this is a dual description computation) and insert them into the list of orbits if they are new.
  - the algorithm finish when all orbits are finished.

Computing dual description

- The algorithm provides an improvement over a straightforward application of cdd and lrs
- Technically, we represent the group as permutation group on the extreme rays. Then, we use two following functions

  Stabilizer(GroupExt, ListInc, OnSets);

  RepresentativeAction(GroupExt, ListInc1, ListInc2, OnSets);

  The important thing is to use the action OnSets, which is extremely efficient and uses backtrack search, i.e. in practice we never build the full orbit.

Further strategies

- Using the Adjacency Decomposition method we can usually find a conjecturally complete list of facets. However in many cases, there remain a few orbits of facets that are particularly difficult to compute.
- If the number of untreated orbits is lower than $n-1$, then we can use following theorem and conclude. Balinski theorem The skeleton of a n-dimensional polytope is n-connected, i.e. the removal of any set of $n-1$ vertices leaves it connected.
- Otherwise, we can apply the Adjacency decomposition method to the remaining orbits of facets. This strategy is Recursive Adjacency Decomposition method

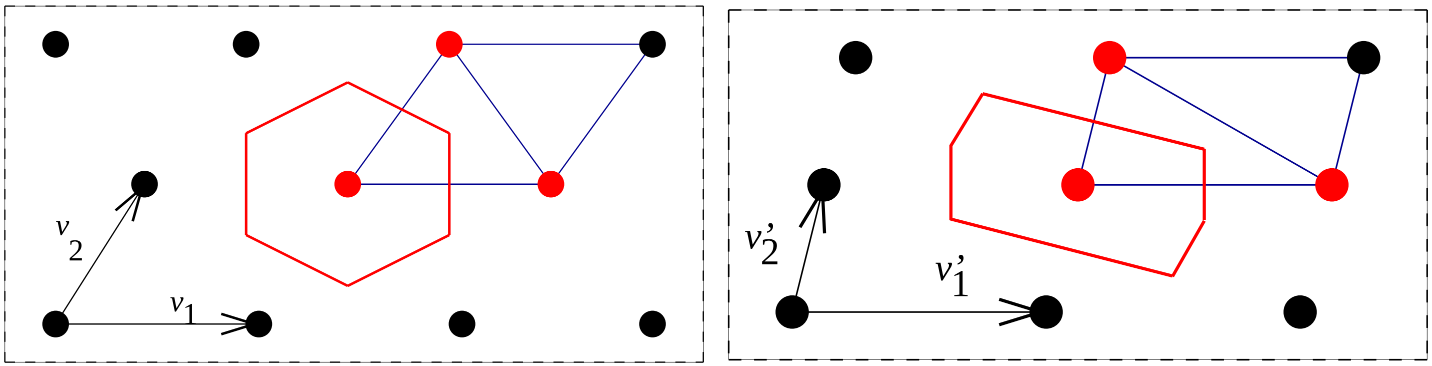
Banking methods

- When one applies the Adjacency decomposition method, recursively, we can met some identical facets several times.
- The idea is to store the dual description of facets in a bank and when a computation happen to make call to that bank to see if it already done.
- So, one wants to compute dual description of some faces of a polyhedral cone. The key point is that this computation is intrisic, i.e. independent over what polytope the face belong to.

III. L-type domain

L-type domains

- Take a lattice L and select a basis $v_1, \dots, v_n$.
- We want to assign the Delaunay polytopes of a lattice. Geometrically, this means that



are part of the same L-type domain.

- A L-type domain is the assignment of Delaunay polytopes, so it is also the assignment of the Voronoi polytope of the lattice.

Equalities and inequalities

- Take $M = G_v$ with $v = (v_1, \dots, v_n)$ a basis of lattice L.
- If $V = (w_1, \dots, w_N)$ with $w_i \in \mathbb{Z}^n$ are the vertices of a Delaunay polytope of empty sphere $S(c, r)$ then:

$$||w_i - c|| = r \text{ i.e. } w_i^T M w_i - 2w_i^T M c + c^T M c = r^2$$

- Substracting one obtains

$$\{w_i^T M w_i - w_j^T M w_j\} - 2\{w_i^T - w_j^T\} M c = 0$$

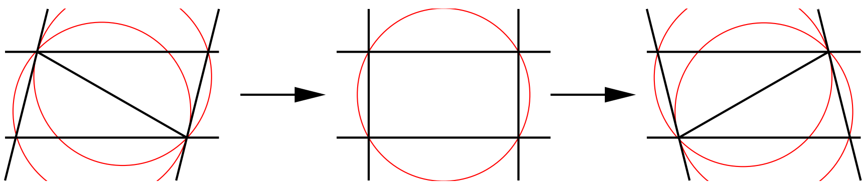
- Inverting matrices, one obtains $Mc = \psi(M)$ with ψ linear and so one gets linear equalities on M.
- Similarly $||w - c|| \geq r$ translates into linear inequalities on M.

Defining inequalities

- If one takes a generic matrix M in $S^n_{>0}$, then all its Delaunay are simplices and so no linear equality are implied on M.
- Hence the corresponding L-type is of dimension $\frac{n(n+1)}{2}$, they are called primitive
- A L/type is primitive if and only if all Delaunay are simplices.
- A primitive L-type domain is essentially the data of all its defining simplices.

Equivalence and enumeration

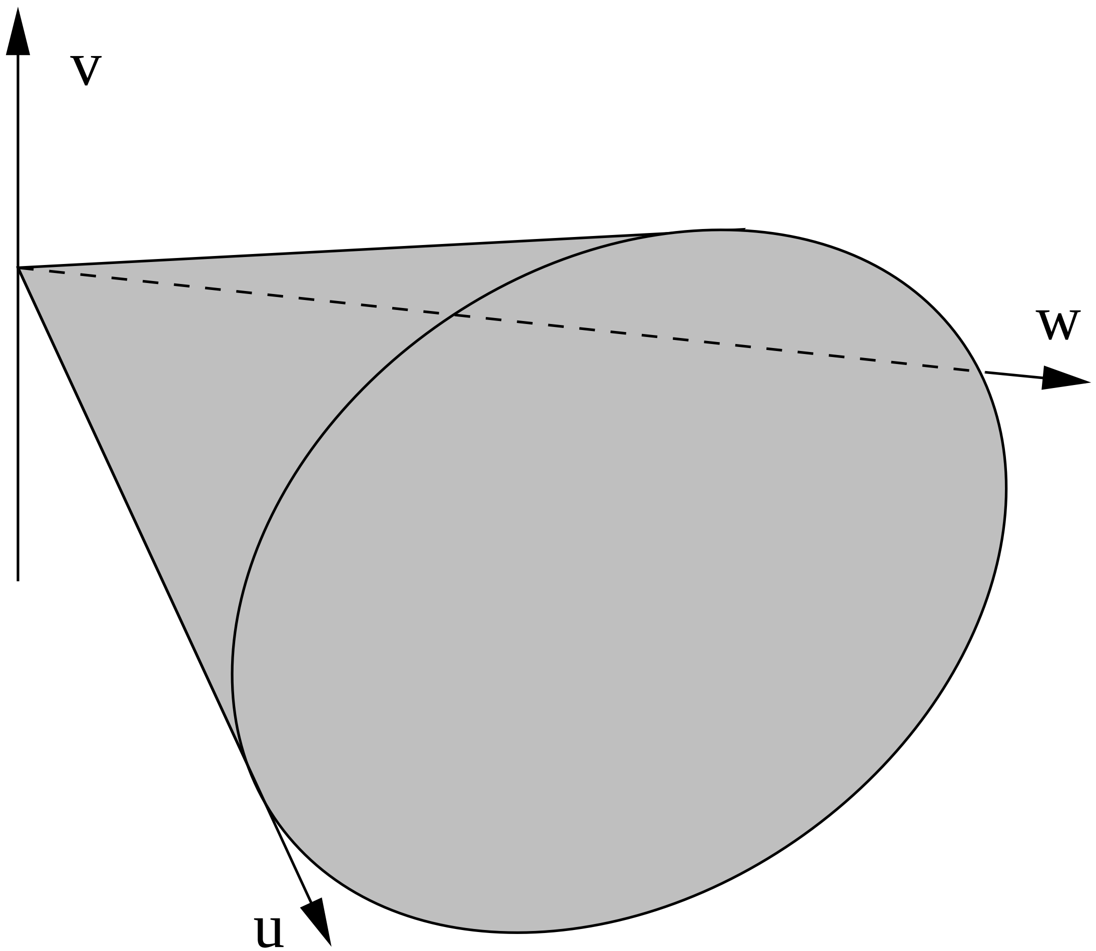
- Voronoi's theorem The inequalities obtained by taking adjacent simplices suffice to describe all inequalities.
- The group $GL_n(\mathbb{Z})$ acts on $S^n_{>0}$ by arithmetic equivalence and preserve the primitive L-type domains.
- Voronoi proved that after this action, there is a finite number of primitive L-type domains.
- Bistellar flipping creates new triangulation. In dim. 2:



- Enumerating primitive L-types is done classicaly:
  - Find one primitive L-type domain.
  - Find the adjacent ones and reduce by arithmetic equivalence.

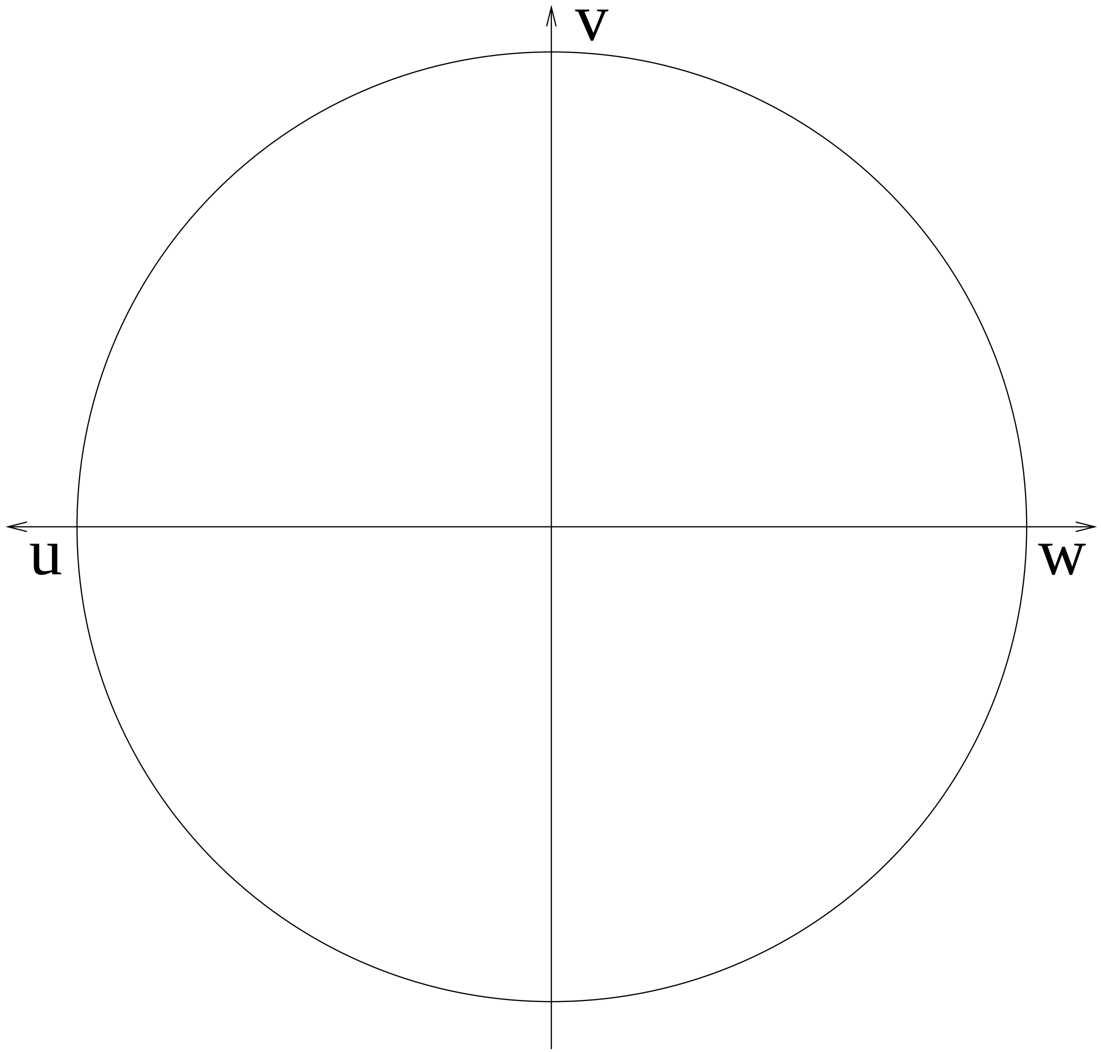
The partition of $S^2_{>0} \subset \mathbb{R}^3$

$\begin{pmatrix} \mathrm{u} & \mathrm{v} \\ \mathrm{v} & \mathrm{w} \end{pmatrix} \in S^2_{>0}$ if and only if $\mathrm{v}^2 < \mathrm{uw}$ and $\mathrm{u} > 0$.



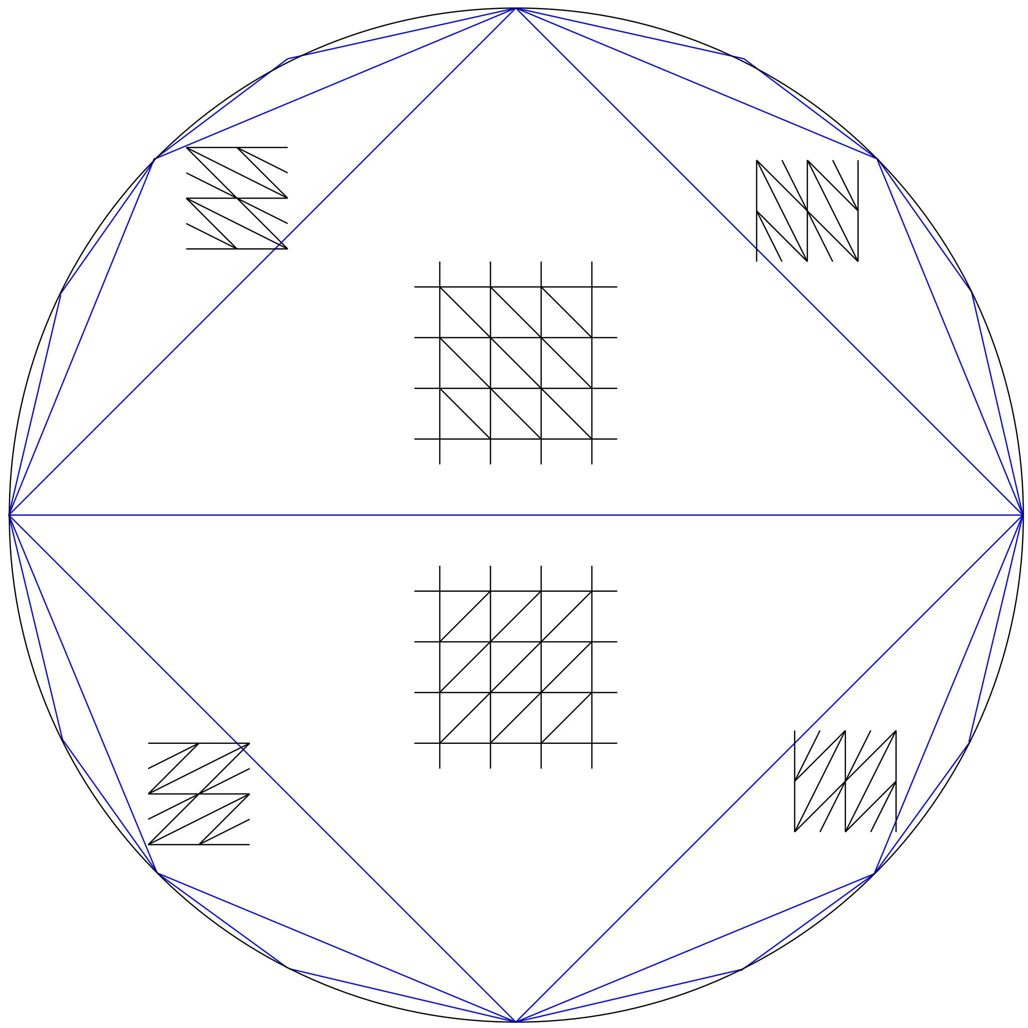
The partition of $S^2_{>0} \subset \mathbb{R}^3$

We cut by the plane $\mathrm{u} + \mathrm{w} = 1$ and get a circle representation.

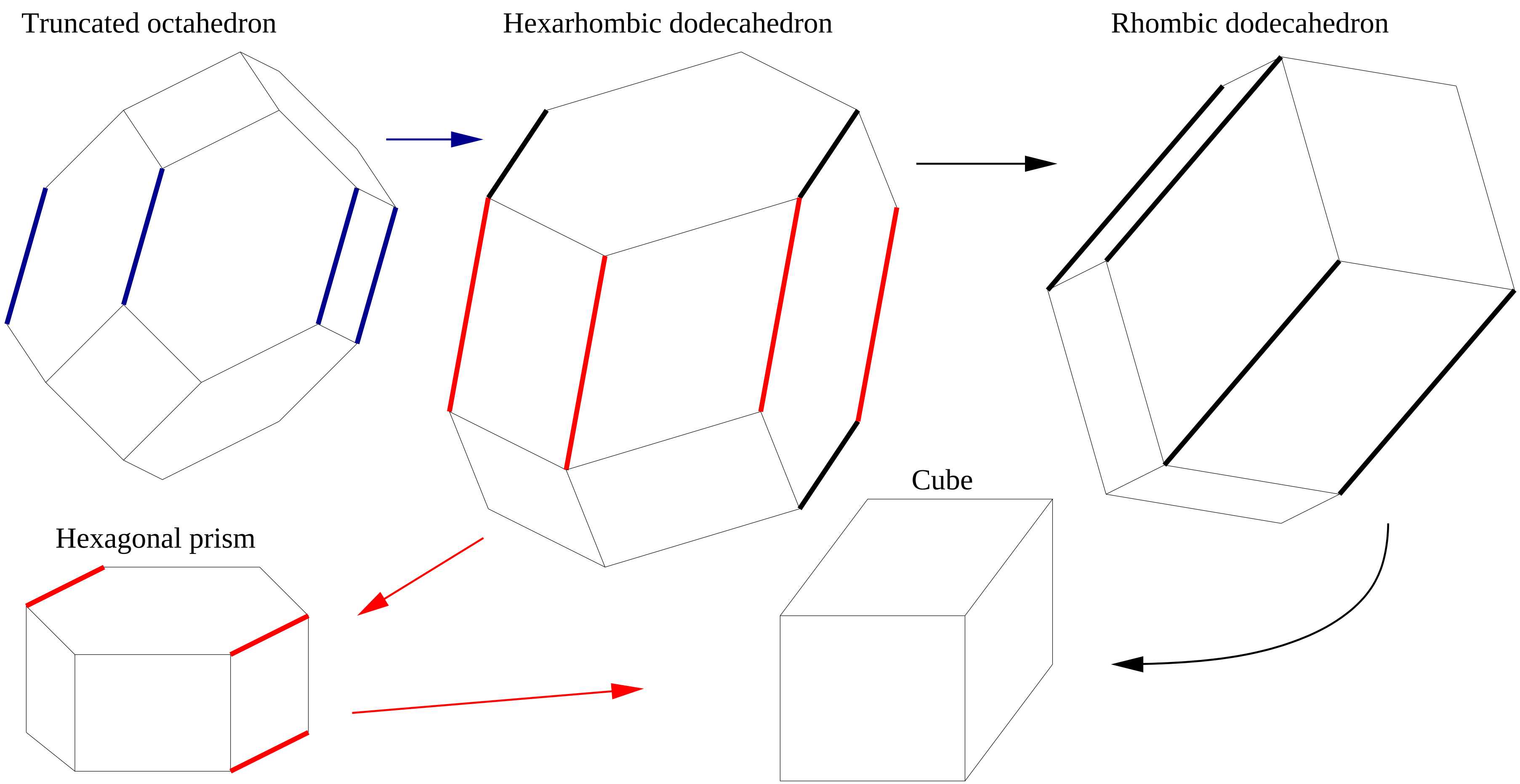


The partition of $S^2_{>0} \subset \mathbb{R}^3$

Primitive L-types in $S^2_{>0}$:



3-dimensional Voronoi polytopes



Enumeration of L-types

Dimension	Nr. L-type	Nr. primitive
1	1	1
2	2	1
3	5 Fedorov	1 Fedorov
4	52 DeSh	3 Voronoi
5	179377 Engel	222 BaRy, Engel & Gr
6	?	$\geq 2.5.10^6$ Engel, Va
7	?	?

Optimization problem

We want to find the best lattice packing, covering, packing-covering.

- The lattice packing problem is solved by the theory of perfect forms and perfect domain. See “premier mémoire” by Voronoi (1908) and book by Martinet for the search of optimal lattice packings.
- Thm. Given a L-type domain LT, there exist a unique lattice, which minimize the covering density over LT.
- Thm. Given a L-type domain LT, there exist a lattice (possibly several), which minimize the packing-covering density over LT.
- See “*Semidefinite programming approaches to lattice packing and covering problems*” by Schürmann & Vallentin

Radius of Delaunay polytope

- Fix a primitive L-type domain, i.e. a collection of simplexes as Delaunay polytopes $D_1, \dots, D_m$.
- Thm. For every $D_i = Conv(0, v_1, \dots, v_n)$, the radius of the Delaunay polytope is at most 1 if and only if

$$\begin{pmatrix} 4 & \langle v_1, v_1\rangle & \langle v_2, v_2\rangle & \dots & \langle v_n, v_n\rangle \\ \langle v_1, v_1\rangle & \langle v_1, v_1\rangle & \langle v_1, v_2\rangle & \dots & \langle v_1, v_n\rangle \\ \langle v_2, v_2\rangle & \langle v_2, v_1\rangle & \langle v_2, v_2\rangle & \dots & \langle v_2, v_n\rangle \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \langle v_n, v_n\rangle & \langle v_n, v_1\rangle & \langle v_n, v_2\rangle & \dots & \langle v_n, v_n\rangle \end{pmatrix} \in S^{n+1}_{\geq 0}$$

by Delone, Dolbilin, Ryshkov and Shtogrin.
- The condition is a semidefinite condition.

Covering problem

- Fix a primitive L-type domain, i.e. a collection of simplexes as Delaunay polytopes $D_1, \ldots, D_m$.
- Minkowski The function $-\log\det(M)$ is strictly convex on $S^n_{>0}$.
- Solve the problem
  - M in the L-type (linear condition),
  - the Delaunay D_i have radius at most 1 (semidefinite condition),
  - minimize $-\log\det(M)$ (strictly convex).
- The above problem is solved by the interior point methods implemented in MAXDET by Vandenberghe, Boyd & Wu. Unicity comes from the strict convexity of the objective function.

Packing covering problem

- We fix a primitive L-type domain.
- A shortest vector is an edge of a Delaunay. So, from the Delaunay decomposition, we know which vectors $v_1, \dots,$ v_p can be shortest.
- We consider the problem on $(M, m) \in S^n_{>0} \times \mathbb{R}$
  - M belong to the L-type domain (linear constraint)
  - all Delaunay have radius at most 1 (semidefinite condition)
  - $m \leq ||v_j||^2 = v_j^t M v_j$ for all i (linear constraint)
  - maximize m.
- The maximal value of m gives the maximal length of shortest vector and so the best packing-covering over a specific primitive L-type domain. A priori no unicity.

V. L-types

of

$S^n_{>0}$-spaces

$S^n_{>0}$-spaces

- A $S^n_{>0}$-space is a vector space $\mathcal{SP}$ of S^n, which intersect $S^n_{>0}$.
- We want to describe the Delaunay decomposition of matrices $M \in S^n_{>0} \cap \mathcal{SP}$.
- Motivations:
  - The enumeration of L-types is done up to dimension 5, perhaps possible for dimension 6 but certainly not for higher dimension.
  - We hope to find some good covering, and packing-covering by selecting judicious $\mathcal{SP}$. This is a search for best but unproven to be optimal coverings.
- A L-type in $\mathcal{SP}$ is an open convex polyhedral set included in $S^n_{>0} \cap \mathcal{SP}$, for which every element has the same Delaunay decomposition.

Rigidity and primitivity

- $(\mathcal{SP}, L)$-types form a polyhedral tessellation of the space $\mathcal{SP} \cap S^n_{>0}$.
- If $M \in \mathcal{SP} \cap S^n_{>0}$, then the rigidity degree of M is the dimension of the smallest L-type containing M, it is computed using the Delaunay decomposition of M.
- A $(\mathcal{SP}, L)$-type is primitive if it is full-dimensional in $\mathcal{SP}$.
- A $(\mathcal{SP}, L)$-type is rigid if it is one dimensional.
- Algorithm for finding a primitive $(\mathcal{SP}, L)$-type domain
  - Generate a random element in $S^n_{>0} \cap \mathcal{SP}$.
  - Compute its Delaunay decomposition.
  - Finish when the dimension of the $(\mathcal{SP}, L)$-type is maximal.

Flipping of primitive L-type

- A generic Delaunay decomposition for a matrix in $\mathcal{SP} \cap S^n_{>0}$ corresponds to a primitive L-type domain. It is not necessarily simplicial.
- Flipping from a primitive L-type domain on a facet is switching from one Delaunay decomposition to another Delaunay decomposition.
- Since we know the adjacencies, we are able to find which Delaunay in the Decomposition disappear.
- The computation is based on a repartitioning polytopes. It is a dual-description computation and it generalizes the bistellar flipping to non-simplicial case.

Enumeration technique

- Find a primitive $(\mathcal{SP}, L)$-type domain, insert it to the list as undone.
- Iterate
  - For every undone primitive $(\mathcal{SP}, L)$-type domain, compute the facets.
  - Eliminate redundant inequalities.
  - For every non-redundant inequality realize the flipping, i.e. compute the adjacent primitive $(\mathcal{SP}, L)$-type domain. If it is new, then add to the list as undone.

VI. Applications

Subgroups of $GL_n(\mathbb{Z})$

- A finite subgroup G of $GL_n(\mathbb{Z})$ is contained into a maximal finite subgroup of $GL_n(\mathbb{Z})$.
- For every n, there is a finite number of maximal finite subgroup of $GL_n(\mathbb{Z})$ up to conjugacy.
- The actual enumeration of groups is done up to dimension 31 (Zassenhaus, Plesken, Pohst, Nebe).
- Denote by $\mathcal{SP}(G)$ the space of invariant form by a finite matrix group G of $GL_n(\mathbb{Z})$.
- Given a $S^n_{>0}$-space $\mathcal{SP}$, denote by $Aut(\mathcal{SP})$ the group of matrices leaving invariant $\mathcal{SP}$ under arithmetic action.
- A Bravais group G is a group satisfying to $Aut(\mathcal{SP}(G)) = G$. They are the “geometric groups” acting on $\mathbb{Z}^n$ and are enumerated up to dimension 6.

Equivariant L-type domains

- Thm. (Zassenhaus) For G a subgroup of $GL_n(\mathbb{Z})$, one has:

$$\{g \in GL_n(\mathbb{Z}) \mid g^T \mathcal{SP}(G) g = \mathcal{SP}(G)\} = N_{GL_n(\mathbb{Z})}(G) \ .$$

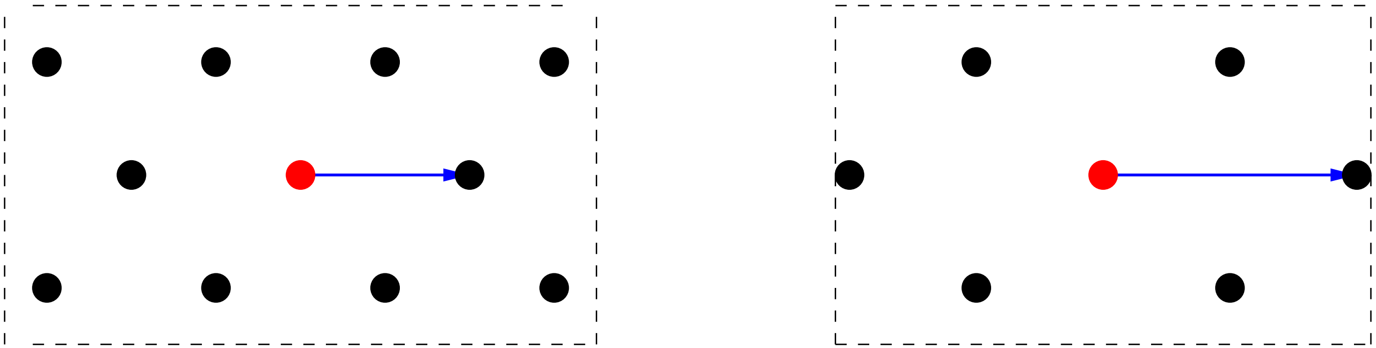
  Equivariant L-type domains are L-types of a $S^n_{>0}$-space $\mathcal{SP}(G)$ for G Bravais.

- Thm. For a given finite group $G \in GL_n(\mathbb{Z})$, there are a finite number of equivariant L-types under the action of $N_{GL_n(\mathbb{Z})}(G)$.

- $\mathcal{SP}(G)$ is defined by rational equations. If a $S^n_{>0}$-space $\mathcal{SP}$ is defined by rational equations, does it have a finite number of classes of L-types under $Aut(\mathcal{SP})$?

Extension of Coxeter lattices

- Anzin & Baranovski computed the Delaunay decompositions of the lattices A_9^5, A_{11}^4, A_{13}^7, A_{14}^5, A_{15}^8 and found them to be better coverings than A_n^*.
- We do extension along short vectors

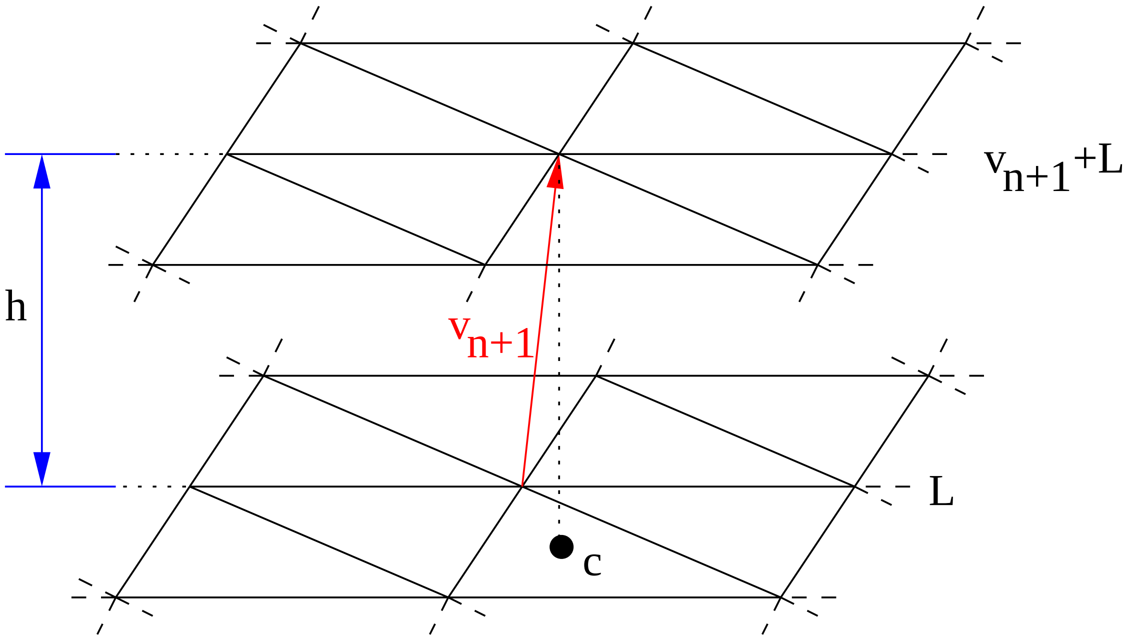


or compute in the $S^n_{>0}$-space $\mathcal{SP}(G)$ with G the stabilizer of a short vector.

- We manage to find record coverings in dimension 9, 11, 13, 14 and 15.

Lamination

- Given a n-dim. lattice L, create a $n+1$-dim. lattice L':



- c is the fixed orthogonal projection of v_{n+1} on L. We vary h and get a $S^{n+1}_{>0}$-space.
- Doing lamination over A_9^5 and A_{11}^4 one gets record coverings in dimension 10 and 12.

Best known lattice coverings

d	lattice	covering density Θ			
1	$\mathbb{Z}^1$	1	13	L_{13}^{c}	7.762108
2	A_2^*	1.209199	14	L_{14}^{c}	8.825210
3	A_3^*	1.463505	15	L_{15}^{c}	11.004951
4	A_4^*	1.765529	16	A_{16}^*	15.310927
5	A_5^*	2.124286	17	A_{17}^{9}	12.357468
6	L_6^c	2.464801	18	A_{18}^*	21.840949
7	L_7^c	2.900024	19	A_{19}^{10}	21.229200
8	L_8^c	3.142202	20	A_{20}^{7}	20.366828
9	L_9^c	4.268575	21	A_{21}^{11}	27.773140
10	L_{10}^c	5.154463	22	Λ_{22}^*	≤ 27.8839
11	L_{11}^c	5.505591	23	Λ_{23}^*	≤ 15.3218
12	L_{12}^c	7.465518	24	*Leech*	7.903536

THANK

YOU