Topological application of Perfect form theory

Mathieu Dutour Sikirić

Institute Rudjer Bošković, Zagreb Croatia

November 21, 2016

I. Lattices and Gram matrices

Lattice packings

- ▶ A lattice $L \subset \mathbb{R}^n$ is a set of the form $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ with (v_1, \ldots, v_n) independent.
- A packing is a family of balls B_n(x_i, r), i ∈ I of the same radius r and center x_i such that their interiors are disjoint.



- ▶ If *L* is a lattice, the lattice packing is the packing defined by taking the maximal value of $\alpha > 0$ such that $L + B_n(0, \alpha)$ is a packing.
- The maximum α is called λ(L) and the determinant of (v₁,..., v_n) is det L.

Gram matrix and lattices

- ▶ Denote by Sⁿ the vector space of real symmetric n × n matrices, Sⁿ_{>0} the convex cone of real symmetric positive definite n × n matrices and Sⁿ_{≥0} the convex cone of real symmetric positive semidefinite n × n matrices.
- ► Take a basis (v₁,..., v_n) of a lattice L and associate to it the Gram matrix G_v = (⟨v_i, v_j⟩)_{1≤i,j≤n} ∈ Sⁿ_{>0}.
- Example: take the hexagonal lattice generated by $v_1 = (1,0)$ and $v_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$



Isometric lattices

► Take a basis $(v_1, ..., v_n)$ of a lattice *L* with $v_i = (v_{i,1}, ..., v_{i,n}) \in \mathbb{R}^n$ and write the matrix

$$V = \left(\begin{array}{cccc} v_{1,1} & \dots & v_{n,1} \\ \vdots & \ddots & \vdots \\ v_{1,n} & \dots & v_{n,n} \end{array}\right)$$

and $G_{\mathbf{v}} = V^T V$. The matrix $G_{\mathbf{v}}$ is defined by $\frac{n(n+1)}{2}$ variables as opposed to n^2 for the basis V.

- If $M \in S_{>0}^n$, then there exists V such that $M = V^T V$ (Gram Schmidt orthonormalization)
- ▶ 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 **v** and *u* an isometry of \mathbb{R}^n , then $G_{\mathbf{v}} = G_{u(\mathbf{v})}$.

Arithmetic minimum

- For $A \in S^n$ and $x \in \mathbb{R}^n$ we write $A[x] = x^T A x$.
- The arithmetic minimum of $A \in S_{>0}^n$ is

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

• The minimal vector set of $A \in S_{>0}^n$ is

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

Both min(A) and 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

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

Changing basis

If v and v' are two basis of a lattice L then V' = VP with P ∈ GL_n(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 ∈ Sⁿ_{>0}, they are called arithmetically equivalent if there is at least one P ∈ GL_n(ℤ) such that

$$A = P^T B P$$

- ► Lattices up to isometric equivalence correspond to $S_{>0}^n$ up to arithmetic equivalence.
- In practice, Plesken/Souvignier wrote a program ISOM for testing arithmetic equivalence and a program AUTO for computing automorphism group of lattices.
 All such programs take Gram matrices as input.

II. Computational techniques

Dual description problem

- A vertex of a polytope P is a point v ∈ P, which cannot be expressed as v = λv¹ + (1 − λ)v² with 0 < λ < 1 and v¹ ≠ v² ∈ 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 ≥ 0, which cannot be expressed as

$$f(x) - b = \lambda(f_1(x) - b_1) + (1 - \lambda)(f_2(x) - b_2)$$
 with $f_i(x) - b_i \ge 0$ 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 P defined by linear inequalities.

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

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.

III. Perfect forms and domains

Perfect forms

- ► A form A is extreme if it is a local maximum of the packing density.
- A matrix A ∈ Sⁿ_{>0} is perfect (Korkine & Zolotarev) if the equation

$$B \in S^n$$
 and $B[x] = \min(A)$ for all $x \in Min(A)$

implies B = A.

- Theorem: (Korkine & Zolotarev) If a form is extreme then it is perfect.
- Up to a scalar multiple, perfect forms are rational.
- All root lattices are perfect, many other families are known.

Perfect domains and arithmetic closure

- 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

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

- ▶ If A has m shortest vectors then Dom(A) has $\frac{m}{2}$ extreme rays.
- So actually, the perfect domains realize a tessellation not of Sⁿ_{≥0}, nor Sⁿ_{≥0} but of the rational closure Sⁿ_{rat,≥0}.
- The rational closure $S_{rat,>0}^n$ has a number of descriptions:

•
$$S_{rat,\geq 0}^n = \sum_{v\in\mathbb{Z}^n} \mathbb{R}_+ p(v)$$

- ▶ If $A \in S_{\geq 0}^n$ then $A \in S_{rat,\geq 0}^n$ if and only if *Ker A* is defined by rational equations.
- So, actually, the stabilizers of some faces of the polyhedral complex are infinite.

Finiteness

- Theorem:(Voronoi) Up to arithmetic equivalence there is only finitely many perfect forms.
- The group $GL_n(\mathbb{Z})$ acts on $S_{>0}^n$:

 $Q \mapsto P^t Q P$

and we have $Min(P^tQP) = P^{-1}Min(Q)$

- $\operatorname{Dom}(P^T Q P) = c(P)^T \operatorname{Dom}(Q) c(P)$ with $c(P) = (P^{-1})^T$
- 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 (<mark>DSV</mark>)	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 ≤ 7)
- Blichfeldt used Korkine-Zolotarev reduction theory.
- Cohn & Kumar used Fourier analysis and Linear programming.

IV. Ryshkov polyhedron and the Voronoi algorithm

The Ryshkov polyhedron

► The Ryshkov polyhedron R_n is defined as

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

- The cone is invariant under the action of $GL_n(\mathbb{Z})$.
- ▶ The cone 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

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

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 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 + αr.
- ► If A' is not equivalent to a form in L, then we insert it into 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

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

with





Flipping on an edge II

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

with

$$B = \left(\begin{array}{cc} 1 & 1/4 \\ 1/4 & 1 \end{array}\right) = A_{hex} + D/4$$





Flipping on an edge III

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

with

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





Flipping on an edge IV



The Ryshkov polyhedron R_2



Well rounded forms and retract

- A form Q is said to be well rounded if it admits vectors v₁, ..., v_n such that
 - (v_1, \ldots, v_n) form a \mathbb{R} -basis of \mathbb{R}^n (not necessarily a \mathbb{Z} -basis)
 - v_1, \ldots, 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 ℤ-basis of ℤⁿ for n ≥ 5.

Topological applications

- ► The fact that we have finite stabilizers for all faces means that we can compute rational homology/cohomology of GL_n(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 GL_n(R) with R a ring of algebraic integers.

V. Tessellations

Linear Reduction theories for $S_{rat,>0}^n$

Decompositions related to perfect forms:

- ► The perfect form theory (Voronoi I) for lattice packings (full face lattice known for n ≤ 7, perfect domains known for n ≤ 8)
- ► The central cone compactification (Igusa & Namikawa) (Known for n ≤ 6)

Decompositions related to Delaunay polytopes:

- ► The *L*-type reduction theory (Voronoi II) for Delaunay tessellations (Known for n ≤ 5)
- ► The C-type reduction theory (Ryshkov & Baranovski) for edges of Delaunay tessellations (Known for n ≤ 5)

Fundamental domain constructions:

- ► The Minkowski reduction theory (Minkowski) it uses the successive minima of a lattice to reduce it (Known for n ≤ 7) not face-to-face
- Venkov's reduction theory also known as Igusa's fundamental cone (finiteness proved by Venkov and Crisalli)

Self-dual cones

For an open cone C in \mathbb{R}^n the dual cone is

$$C^* = \{x \in \mathbb{R}^n \text{ s.t. } \langle x, y \rangle > 0 \text{ for } y \in C\}$$

- Such cones are classified by Euclidean Jordan algebras and the classification gives:
 - ► *Sⁿ*: The cone of positive definite real quadratic forms
 - H^n : The cone of positive definite Hermitian quadratic forms
 - Q^n : The cone of positive definite quaternionic quadratic forms
 - The cone of 3×3 positive definite octonion matrices.
 - ▶ The hyperbolic cone *H_n*

$$H_n = \left\{ (x_1, \dots, x_n) \text{ s.t. } x_1 > 0 \text{ and } x_1^2 - x_2^2 - \dots - x_n^2 > 0 \right\}$$

- References
 - A. Ash, D. Mumford, M. Rapoport, Y. Tai Smooth compactifications of locally symmetric varieties, Cambridge University Press
 - M. Koecher, Beiträge zu einer Reduktionstheorie in Positivtätsbereichan I/II, Math. Annalen 141, 384–432, 144, 175–182

T-space theory

- A *T*-space *F* is a vector space in *Sⁿ* with *F*_{>0} = *F* ∩ *Sⁿ*_{>0} being non-empty.
- All above reduction theories apply to that case.
- But some dead ends exist to the polyhedral tessellations.
- ▶ Relevant group is Aut(\mathcal{F}) = { $g \in GL_n(\mathbb{Z})$ s.t. $g\mathcal{F}g^T = \mathcal{F}$ }.
- For a finite group $G \subset GL_n(\mathbb{Z})$ of space

$$\mathcal{F}(\mathcal{G}) = \left\{ A \in \mathcal{S}^n ext{ s.t. } gAg^{\mathcal{T}} = A ext{ for } g \in \mathcal{G}
ight\}$$

we have Aut($\mathcal{F}(G)$) = Norm(G, GL_n(\mathbb{Z})) (Zassenhaus) and a finite number of \mathcal{F} -perfect forms.

- There exist some *T*-spaces having a rational basis and an infinity of perfect forms.
- ► Another finiteness case is for spaces obtained from GL_n(R) with R number ring.

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 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 SL(n, Z[1/p]), Duke Mathematical Journal 47-4 (1980) 803-818.

VI. Central cone compactification

Central cone compactification

• We consider the space of integral valued quadratic forms:

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

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 $A[x] \ge 1$. So, $I_n \subset R_n$
- Any root lattice gives a vertex both of R_n and conv I_n .
- The centrally perfect forms are known for $n \leq 6$:



► By taking the dual we get tessellations of Sⁿ_{rat,>0}.

Enumeration of centrally perfect forms

- Suppose that we have a conjecturally correct list of centrally perfect forms A₁, ..., A_m. Suppose further that for each form A_i we have a conjectural list of neighbors N(A_i).
- We form the cone

$$C(A_i) = \{X - A_i \text{ for } X \in N(A_i)\}$$

and we compute the orbits of facets of $C(A_i)$.

For each orbit of facet of representative f we form the corresponding linear form f and solve the Integer Linear Problem

$$f_{opt} = \min_{X \in I_n} f(X)$$

We have to use GLPK program for that. It is done iteratively since I_n is defined by an infinity of inequalities.

If f_{opt} = f(A_i) always then the list is correct. If not then the X realizing f(X) < f(A_i) need to be added to the full list.

VII. Perfect form complex

Known number of orbits of faces for $n \leq 9$

- Each orbit of face corresponds to a vector configuration.
- ► The rank rk(V) of a vector configuration V = {v₁,..., v_m} is the rank of the matrix family {p(v_i) = v_i^Tv_i}.
- ► The complex is fully known for n ≤ 7. Number of orbits by rank:
 - n = 4: 1, 3, 4, 4, 2, 2, 2.
 - ▶ *n* = 5: 2, 5, 10, 16, 23, 25, 23, 16, 9, 4, 3.
 - *n* = 6: 3, 10, 28, 71, 162, 329, 589, 874, 1066, 1039, 775, 425, 181, 57, 18, 7
 - *n* = 7: 6, 28, 115, 467, 1882, 7375, 26885, 87400, 244029, 569568, 1089356, 1683368, 2075982, 2017914, 1523376, 876385, 374826, 115411, 24623, 3518, 352, 33
- For n = 8 the following is known:
 - Number of perfect forms is 10916
 - Number of orbits of low rank faces is: 13 (Zahareva & Martinet), 106, 783, 6167, 50645
- For n = 9 the following is known:
 - Number of orbits of low rank faces is: 44 (Keller, Martinet & Schürmann), 759, 13437

Testing realizability of vector families

- ► Problem: Suppose we have a configuration of vector V. Does there exist a matrix A ∈ Sⁿ_{>0} such that Min(A) = V?
- Consider the linear program

$$egin{aligned} & \lambda \ & ext{with} \quad \lambda = \mathcal{A}[v] ext{ for } v \in \mathcal{V} \ & \mathcal{A}[v] \geq 1 ext{ for } v \in \mathbb{Z}^n - \{0\} - \mathcal{V} \end{aligned}$$

If $\lambda_{opt} < 1$ then \mathcal{V} is realizable, otherwise no.

- ► In practice one replaces Zⁿ by a finite set and iteratively increases it until a conclusion is reached.
- The number of iterations can unfortunately be very high.
- We use integral symmetries of the configuration of vectors in order to make the linear program simpler.
- A related problem is to find the smallest configuration \mathcal{W} such that there exist a $A \in S_{>0}^n$ with $\mathcal{V} \subseteq \mathcal{W} = Min(A)$ and $rk(\mathcal{V}) = rk(\mathcal{W})$.

Simpliciality results

- ► Theorem: If V = {v₁,..., v_m} is a configuration of shortest vectors in dimension n such that rk(V) = r with r ∈ {n, n + 1, n + 2}. Then m = r.
- The proof of this is relatively elementary and use simple matrix arguments. See:
 - M. Dutour Sikirić, K. Hulek, A. Schürmann, Smoothness and singularities of the perfect form compactification of Ag, Algebraic Geometry 2(5) (2015) 642-653.
- Conjecture: The equality m = r also holds if r ∈ {n+3, n+4}. It is true for n ≤ 8.
- For Eisenstein or Gaussian integers similar results hold only for r = n.

Enumeration of vector configurations for r = n + 1, r = n + 2

Suppose we know the configuration of shortest vectors in dimension n of rank r = n.

- Let V = {v₁,..., v_n} be a short vector configuration with n vectors.
- We search for the vectors v such that W = V ∪ {v} is a vector configuration.
- ▶ We can assume that V has maximum determinant in the n+1 subvector configurations with n vectors of W. Thus

$$|\det(v_1,\ldots,v_{i-1},v_{i+1},\ldots,v_n,v)| \leq |\det(v_1,\ldots,v_n)|$$

for $1 \leq i \leq n$.

- ▶ The above inequalities determine a *n*-dim. polytope.
- We enumerate all the integer points by exhaustive enumeration.
- We then check for realizability of the vector families.

For rank r = n + 2, we proceed similarly.

Enumeration of vector configurations for r > n + 2

We assume that we know all the realizable vector configurations of rank r - 1 and r - 2.

- We enumerate all pairs (V, W) with V ⊂ W, rk(V) = r − 2 and rk(W) = r − 1.
- If we have a configuration of rank r, then it contains a configuration V of rank r − 2 and dimension n which is contained in two configurations W₁ and W₂ of rank r − 2 such that V ⊂ W₁ and V ⊂ W₂.
- \blacktriangleright So, we combine previous enumeration and obtain a set of configurations $\mathcal{W}_1\cup\mathcal{W}_2$
- We check for each of them if there exist a realizable vector configuration W such that W₁ ∪ W₂ ⊂ W and rk(W) = r.

Enumerating the configurations of rank r = n

- This is in general a very hard problem with no satisfying solution.
- One would expect that the number of realizable vector configurations in dimension 10, 11 and 12 not be too high.
- It does not seem possible to use the polyhedral structure in order to enumerate them.
- The only known upper bound on the possible determinant of realizable configurations V is

$$|\det(V)| \leq \left\lfloor \gamma_n^{n/2} \right\rfloor$$

- For dimension 9 and 10 the bound combined with known upper bound on γ_n gives 30 and 59 as upper bound.
- Those are quite large bounds.

The case of cyclic lattices

▶ For an index $d \in \mathbb{N}$ we consider a lattice *L* spanned by $e_1 = (1, 0, ..., 0), ..., e_n = (0, ..., 0, 1)$ and

$$e_{n+1}=rac{1}{d}(a_1,\ldots,a_n),a_i\in\mathbb{Z}$$

such that (e_1, \ldots, e_n) is the configuration of shortest vectors of a lattice.

By standard reductions, we can assume that

•
$$a_1 \leq a_2 \leq \cdots \leq a_n$$
.

► $1 \le a_i \le \lfloor d/2 \rfloor$.

For n = 10 at present one can only state $d \le 59$ and d prime.

- This case is important for two reasons:
 - It exemplifies the difficulty of the problem.
 - It shows up when enumerating the minimal configuration of shortest vectors.
- For n = 9, the largest feasible prime d is 7.

THANK YOU