Computational Challenges in Perfect form theory

Mathieu Dutour Sikirić

Rudjer Bošković Institute, Zagreb Croatia

April 24, 2018

I. Enumerating Perfect forms

Notations

- We define S^n the space of symmetric matrices, $S^n_{>0}$ the cone of positive definite matrices.
- For $A \in S^n_{>0}$ define $A[x] = xAx^T$,

  $\min(A) = \min_{x \in \mathbb{Z}^n - \{0\}} A[x]$ and $\mathrm{Min}(A) = \{x \in \mathbb{Z}^n \text{ s.t. } A[x] = \min(A)\}$

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

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

  implies $B = A$.
- If A is perfect, then its perfect domain is the polyhedral cone

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

- The Ryshkov polyhedron $\mathcal{R}_n$ is defined as

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

Known results on perfect form enumeration

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$9.200.000	Λ_9?

- The enumeration of perfect forms is done with the Voronoi algorithm.
- Blichfeldt used Korkine-Zolotarev reduction theory.
- Perfect form theory has applications in
  - Lattice theory for the lattice packing problem.
  - Computation of homology groups of $GL_n(\mathbb{Z})$.
  - Compactification of Abelian Varieties.

Perfect forms in dimension 9

- Finding the perfect forms in dimension 9 would solve the lattice packing problem.
- Several authors did partial enumeration of perfect forms in dimension 9:
  - Schürmann & Vallentin: ≥ 500000
  - Anzin: ≥ 524000
  - Andreanov & Scardicchio: ≥ 500000 (but actually 1.10^6)
  - van Woerden: $\geq 9.10^6$

  So, one does not necessarily expect an impossibly large number.
- Other reason why it may work:
  - Maximal kissing number is 136 (by Watson)
  - The number of complex cones (with number of rays greater than $n(n+1)/2+20$) is not too high.
  - Many cones have a pyramid decomposition: $C = C' + \mathbb{R}_+ v_1 + \cdots + \mathbb{R}_+ v_r$ with $dim\, C' = dim\, C - r$

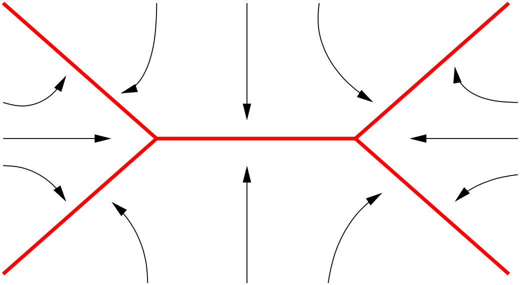
Needed tools: Canonical form

- The large number of perfect forms mean that we need special methods for isomorphism
- Two alternatives:
  - Use very fine invariants: $(\det(A), \min(A))$ is already quite powerful.
  - Use a canonical form.
- Minkowski reduction provides a canonical form but is hard to compute.
- Isomorphism and stabilizer computations can be done by ISOM/AUTOM but we risk being very slow if the invariant are not fine enough.
- Partition backtrack programs for graph isomorphism (nauty, bliss, saucy, traces, etc.) provides a canonical form for graphs.
- Using this we can:
  - Find a canonical form for edge weighted graphs.
  - Find a canonical ordering of the shortest vectors.
  - Find a canonical presentation of the shortest vectors.
  - Find a canonical representation of the form.

Needed tools: MPI parallelization and Dual description

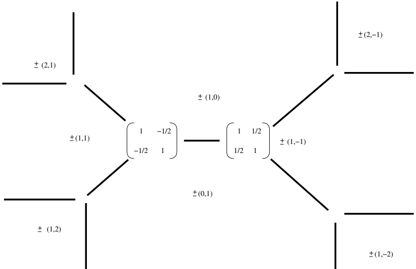
- There are two essential difficulties for the computation:
  - The very large number of perfect forms.
  - The difficult to compute perfect forms whose number of shortest vectors is very high.
- For the first problem, the solution is to use `MPI` (Message Passing Interface) formalism for parallel computation. This can scale to thousands of processors (work with Wessel van Woerden).
- The dual description problem is harder:
  - As mentioned, many cones are pyramid and thus their dual description is relativly easy.
  - But many cones, in particular the one of Λ_9, are not so simple but yet have symmetries.
  - We need to use symmetries for this computation. The methods exist.
  - The critical problem is that we need a permutation group library in `C++`.

II. Well rounded retract and homology



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.
- Such vector configurations correspond to bounded faces of $\mathcal{R}_n$.
- Every form in $\mathcal{R}_n$ can be continuously deformed to a well rounded form and this defines a contractible polyhedral complex $\mathcal{WR}_n$ of dimension $\frac{n(n-1)}{2}$.
- Every face of $\mathcal{WR}_n$ has finite stabilizer.
- $\mathcal{WR}_n$ is essentially optimal (Pettet, Souto, 2008).

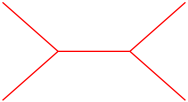


Topological applications

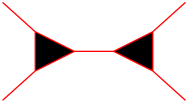
- The fact that $\mathcal{WR}_n$ is contractible, has finite stabilizers, and is acted on by $\mathrm{GL}_n(\mathbb{Z})$ means that we can compute rational homology of $\mathrm{GL}_n(\mathbb{Z})$.
- This has been done for $n \leq 7$ (Elbaz-Vincent, Gangl, Soulé, 2013).
- We can get $K_8(\mathbb{Z})$ (DS, Elbaz-Vincent, Martinet, in preparation).
- By using perfect domains, we can compute the action of Hecke operators on the cohomology.
- This has been done for $n \leq 4$ (Gunnells, 2000).
- Using T-space theory this can be extended to the case of $\mathrm{GL}_n(R)$ with R a ring of algebraic integers:
    - For Eisenstein and Gaussian integers, this means using matrices invariant under a group.
    - For other number fields with r real embeddings and s complex embeddings this gives a space of dimension

$$r\frac{n(n+1)}{2} + sn^2$$

III. Tesselations: Central cone compactification



or



?

Linear Reduction theories in $S^n_{\geq 0}$

Decompositions related to perfect forms:

- 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 $n \leq 6$)

Decompositions related to Delaunay polytopes:

- 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 $n \leq 5$)

Fundamental domain constructions:

- 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 Venkov and Crisalli)

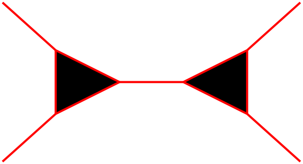
Central cone compactification

- We consider the space of integral valued quadratic forms:

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

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

dim.	Centrally perfect forms
2	A_2 (Igusa, 1967)
3	A_3 (Igusa, 1967)
4	A_4, D_4 (Igusa, 1967)
5	A_5, D_5 (Namikawa, 1976)
6	A_6, D_6, E_6 (DS)



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

Enumeration of centrally perfect forms

- Suppose that we have a conjecturally correct list of centrally perfect forms $A_1, \ldots, A_m$. Suppose further that for each form A_i we have a conjectural list of neighbors $N(A_i)$.
- We form the cone

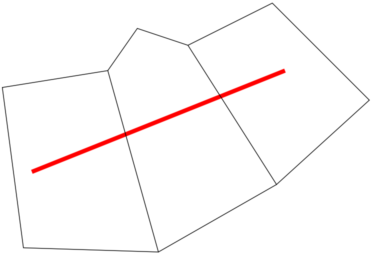
$$C(A_i) = \{X - A_i \text{ for } X \in N(A_i)\}$$

  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:

$$f_{opt} = \min_{X \in \mathcal{I}_n} f(X)$$

  It is solved iteratively (using **glpk**) since $\mathcal{I}_n$ 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.

IV. Perfect coverings



Problem setting and algorithm

We have a d dimensional cone $\mathcal{C}$ embedded into $S^n_{>0}$ and we want to find a set of perfect matrix $A_1, \ldots, A_m$ such that

$$\mathcal{C} \subset Dom(A_1) \cup \cdots \cup Dom(A_m)$$

We want the cones having an intersection that is full dimensional in $\mathcal{C}$ (this is for application in Algebraic Geometry).
We take a cone $\mathcal{C}$ in $S^n_{>0}$ of symmetry group G.

- We start by taking a matrix A in the interior of $\mathcal{C}$.
- We compute a perfect form B such that $A \in Dom(B)$ and insert B into the list of orbit
- We iterate the following:
  - For each untreated orbit of perfect domain in $\mathcal{O}$ compute the facets.
  - For each facet do the flipping and keep if the intersection with $\mathcal{C}$ is full dimensional in $\mathcal{C}$.
  - Insert the obtained perfect domains if they are not equivalent to a known one.

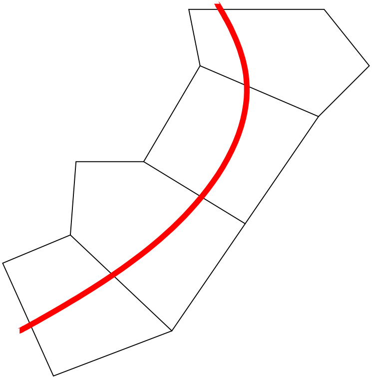
The space intersection problem

- Given a family of vectors $(v_i)_{1 \leq i \leq M}$ spanning a cone $\mathcal{C} \in \mathbb{R}^n$ and a d-dimensional vector space $\mathcal{S}$ we want to compute the intersection

$$\mathcal{C} \cap \mathcal{S}$$

  that is facets and/or extreme rays description.
- In the case considered we have d small.
- Tools:
  - We can compute the group of transformations preserving $\mathcal{C}$ and $\mathcal{S}$.
  - We can check if a point in $\mathcal{S}$ belongs to $\mathcal{C} \cap \mathcal{S}$ by linear programming.
  - We can test if a linear inequality $f(x) \geq 0$ defines a facet of $\mathcal{C} \cap \mathcal{S}$ by linear programming.
- Algorithm:
  - Compute an initial set of extreme rays by linear programming.
  - Compute the dual description using the symmetries.
  - For each facet found, check if they are really facet. If not add the missed extreme rays and iterate.

V. Perfect domains for symplectic group



The invariant manifold

- We are interested in the group $G = \mathrm{Sp}(2n, \mathbb{Z})$ defined as

$$G = \left\{ M \in \mathrm{GL}_{2n}(\mathbb{Z}) \text{ s.t. } MJM^T = J \right\} \text{ with } J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

- We want something similar to $\mathrm{GL}_n(\mathbb{Z})$.
- The idea is to introduce the manifold

$$M_G = \left\{ MM^T \text{ for } M \in \mathrm{Sp}(2n, \mathbb{Z}) \right\} = \left\{ A \in S^n_{>0} \text{ s.t. } AJA^T = J \right\}$$

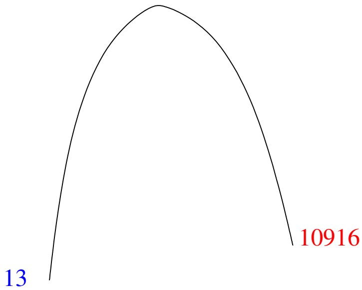
- We have $M_G \subset S^n_{>0}$, G acts on it and it is contractible.
- We can consider the perfect domains $Dom(A)$ that intersects M_G in their interior.
- The number of orbits of such perfect domains under $\mathrm{Sp}(2n, \mathbb{Z})$ ought to be finite.
- Maybe the method also applies to other groups $G \subset \mathrm{GL}_n(\mathbb{Z})$?

Results for $n = 2$ and $n = 3$

- In MacPherson & M. McConnell, 1993 a reduction theory for $\mathrm{Sp}(4, \mathbb{Z})$ is given:
  - It describe a cell complex on which G acts.
  - Number of orbits in the decomposition are 1(vector), 1(Lagrangian space), 2, 3, 3, 2, 2(A_4 or D_4).
  - The rank in the decomposition does not correspond to the linear algebra rank.
- We can effectively compute the homology and Hecke operators for $n = 2$ (Joint work with P. Gunnells). So far we have
  - Computed 4 Hecke operators
  - Computed for the Siegel subgroups of $\mathrm{Sp}(4, \mathbb{Z})$ up to $p = 19$.

  Need more optimization and computational power.
- For $n = 3$ likely there is a similar decomposition. We took at random points in the manifold and computed the corresponding perfect domain and obtained 22 orbits so far.

VI. Perfect form complex



Perfect form complex

- Each orbit of face corresponds to a vector configuration.
- The rank $rk(\mathcal{V})$ of a vector configuration $\mathcal{V} = \{v_1, \dots, v_m\}$ is the rank of the matrix family $\{p(v_i) = v_i^T v_i\}$.
- The complex is fully known for $n \leq 7$. Number of orbits by rank (Elbaz-Vincent, Gangl, Soulé, 2013):
  - $n = 4$: 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
- It is out of question to enumerate the whole perfect form complex in dimension 8.
- Instead the idea is to try to enumerate the cells in lowest rank and go upward in rank.

Testing realizability of vector families I

- Problem: Suppose we have a configuration of vector $\mathcal{V}$. Does there exist a matrix $A \in S^n_{>0}$ such that $\mathrm{Min}(A) = \mathcal{V}$?
- Consider the linear program

$$\begin{array}{rl} \text{minimize} & \lambda \\ \text{with} & \lambda = A[v] \text{ for } v \in \mathcal{V} \\ & A[v] \geq 1 \text{ for } v \in \mathbb{Z}^n - \{0\} - \mathcal{V} \end{array}$$

  If $\lambda_{opt} < 1$ then $\mathcal{V}$ is realizable, otherwise no.
- In practice one replaces $\mathbb{Z}^n$ by a finite set $\mathcal{Z}$ and iteratively increases it until a conclusion is reached.
- A related problem is to find the smallest configuration $\mathcal{W}$ such that there exist a $A \in S^n_{>0}$ with $\mathcal{V} \subseteq \mathcal{W} = \mathrm{Min}(A)$ and possibly $rk(\mathcal{V}) = rk(\mathcal{W})$.
- The major problem is to limit the number of iterations.

Testing realizability of vector families II

- A vector configuration can be simplified by applying LLL reduction to the positive definite quadratic form $\sum_i v_i v_i^T$. This diminishes the coefficient size
- We can use the $\mathrm{GL}_n(\mathbb{Z})$-symmetries of $\mathcal{V}$ to diminish the size of the problem.
- The linear programs occurring are potentially very complex. We need exact solution fast technique for them. The idea is to use double precision and **glpk**. From this we search for a primal/dual solution. If failing we use the simplex method in rational arithmetic with **cdd**.
- According to the optimal solution A_0:
  - If A_0 is positive definite but there is a v such that $A_0[v] < 1$ then insert it into $\mathcal{Z}$.
  - If $Ker(A_0) \neq 0$ we take a v with $A_0 v = 0$ and insert it into $\mathcal{Z}$.
  - If A_0 is not positive semidefinite, we take an eigenvector of negative eigenvalue and search for rational approximation v.

Simpliciality results

- The perfect form complex provides a compactification of the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties, which is a canonical model in the sense of the minimal model program (Shepherd-Barron, 2006).
- For a cone in the perfect form complex, we can consider if it is simplicial or if it is basic, i.e. if its generators can be extended to a $\mathbb{Z}$-basis of $\mathrm{Sym}^2(\mathbb{Z}^n)$.
  This describes the corresponding singularities of the compactification.
- Theorem: If $\mathcal{V} = \{v_1, \dots, v_m\}$ is a configuration of shortest vectors in dimension n such that $rk(\mathcal{V}) = r$ with $r \in \{n, n+1, n+2\}$. Then $m = r$.
- The proof of this is relatively elementary and use simple combinatorial arguments (DS., Hukek, Schürmann, 2015).
- Conjecture: The equality $m = r$ also holds if $r \in \{n+3, n+4\}$.
- No extension to T-spaces.

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 $\mathcal{V} = \{v_1, \dots, v_n\}$ be a short vector configuration with n vectors.
- We search for the vectors v such that $\mathcal{W} = \mathcal{V} \cup \{v\}$ is a vector configuration.
- We can assume that $\mathcal{V}$ has maximum determinant in the $n+1$ subvector configurations with n vectors of $\mathcal{W}$. Thus

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

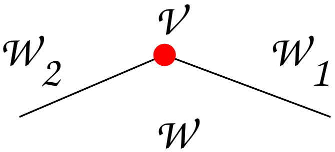
  for $1 \leq i \leq n$.
- The above inequalities determine a n-dim. polytope.
- We enumerate all the integer points by exhaustive enumeration.
- We then check for realizability of the vector families.

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 $(\mathcal{V}, \mathcal{W})$ with $\mathcal{V} \subset \mathcal{W}$, $rk(\mathcal{V}) = r-2$ and $rk(\mathcal{W}) = r-1$.
- If we have a configuration of rank r, then it contains a configuration $\mathcal{V}$ of rank $r-2$ and dimension n which is contained in two configurations $\mathcal{W}_1$ and $\mathcal{W}_2$ of rank $r-2$ such that $\mathcal{V} \subset \mathcal{W}_1$ and $\mathcal{V} \subset \mathcal{W}_2$.
- 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 $\mathcal{W}$ such that $\mathcal{W}_1 \cup \mathcal{W}_2 \subset \mathcal{W}$ and $rk(\mathcal{W}) = r$.



Enumerating the configurations of rank $r = n$

- This is in general a very hard problem with no satisfying solution.
- 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 (Keller, Martinet & Schürmann, 2012) is

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

  with γ_n the Hermite constant in dimension n.
- This bound is tight up to dimension 8.
- For dimension 9 and 10 the bound combined with known upper bound on γ_n gives 30 and 59 as upper bound.
- Any improvement, especially not using γ_n, would be very useful.

The case of prime cyclic lattices

- For a prime $p \in \mathbb{N}$ we consider a lattice L spanned by $e_1 = (1, 0, \dots, 0)$, ..., $e_n = (0, \dots, 0, 1)$ and

$$e_{n+1} = \frac{1}{p}(a_1, \dots, a_n), a_i \in \mathbb{Z}$$

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

- By standard reductions, we can assume that
  - $a_1 \leq a_2 \leq \cdots \leq a_n$.
  - $1 \leq a_i \leq \lfloor p/2 \rfloor$.
  - $(a_1, \dots, a_n)$ is lexicographically minimal for the action of $(\mathbb{Z}_p)^*$.
- With above restrictions, the families of vectors can be enumerated via a tree search.

Enumeration up to fixed index

- We want to enumerate the configurations of shortest vectors of index N.
- For a prime index we do the enumeration of all possibilities and check for each of them.
- For an index $N = p_1 \times p_2 \times \cdots \times p_m$ we do following:
  - First the enumeration for $N_2 = p_1 \times \cdots \times p_{m-1}$.
  - For each realizable configuration of index N_2 we compute the stabilizer.
  - Then we enumerate the overlattices up to the stabilizer action.
  - And we check realizability for each of them.
- So for $n = 10$ we have to consider up to index 59.
  - This gives 17 prime numbers to consider with a maximal number of cases 16301164 for $p = 59$.
  - One very complicated case of $49 = 7^2$.
  - It would have helped so much to have better bounds on γ_{10}!

Enumeration results for $n \leq 11$

- Known number of orbits of cones in the perfect cone decomposition for rank $r \leq 12$ and dimension at most 11.

$d \backslash r$	4	5	6	7	8	9	10	11	12
4	1	3	4	4	2	2	2	-	-
5		2	5	10	16	23	25	23	16
6			3	10	28	71	162	329	589
7				6	28	115	467	1882	7375
8					13[a]	106	783	6167	50645
9						44[b]	759	13437	?
10							283	16062	?
11								6674[c]	?

a: Zahareva & Martinet, *b*: Keller, Martinet & Schürmann.
others: Grushevsky, Hulek, Tommasi, DS, 2017.
c: Partial enumeration, done only up to index 44 with highest realizable index of 32.

Known enumeration results for $n = 12$

- In dimension 12 the combinatorial explosion for configuration of shortest vectors really takes place.
- Up to index 30 we found:

1	1	2	8	3	6
4	56	5	22	6	109
7	62	8	501	9	199
10	685	11	397	12	2372
13	876	14	3012	15	2340
16	8973	17	3173	18	11840
19	5369	20	23072	21	11811
22	23096	23	12393	24	63397
25	19843	26	42627	27	30120
28	77019	29	23629	30	87568

Total: 454576 configurations so far .

Consequences

- Thm: With the exception of the cone of the root lattice D_4, every cone in the perfect cone decomposition of dimension at most 10 is basic.
- Starting from dimension 11 there are configurations of shortest vectors which are orientable in the sense of homology.
- In dimension 12 there is a configuration of shortest vectors whose orbit under $GL_{12}(\mathbb{Z})$ splits in two orbits under $SL_{12}(\mathbb{Z})$.
- Conj. The maximum index in dimension $n \geq 8$ is 2^{n-5}.
- Conj. A configuration of shortest vectors of rank $r = n$ can be extended to a $\mathbb{Z}$-basis of $\mathrm{Sym}^2(\mathbb{Z}^n)$.
- Conj. There is a configuration of shortest vectors of a n-dimensional lattice of rank $r = n$ with trivial stabilizer (smallest known size is 4).

THANK YOU