Introduction to Reduction Theory

Maxwell Forst

March 2026

The primary reference for this presentation is *Computational Geometry of Positive Definite Quadratic Forms* by Achill Schürmann

Lattice definition

A lattice Λ is a discrete, co-compact subgroup of a Euclidean vector space V.

- **Euclidean:** Λ is equipped with an Euclidean norm $\|\cdot\|$.
- **discrete:** for any $\boldsymbol{a}, \boldsymbol{b} \in \Lambda$ with $\boldsymbol{x} \neq \boldsymbol{y}$ then $\|\boldsymbol{x} - \boldsymbol{y}\| \geq c$ for some $c > 0$.
- **co-compact:** for any $\boldsymbol{x} \in V$ there exists $\boldsymbol{a} \in \Lambda$ such that $\|\boldsymbol{x} - \boldsymbol{a}\| \leq C$ for some $C > 0$.

In more practical terms

$$\Lambda = \text{span}\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d\} = A\mathbb{Z}^d,$$

where $d = \dim(V)$ and $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d$ is linearly independent and $A = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d]$.
In this presentation we will only deal with full rank lattices.

Successive Minima

Let $\|\cdot\|$ be a norm on $\mathbb{R}^n$

- Let $\lambda_i(L)$ be the the smallest value of r such that set $\{\boldsymbol{x} \in L : \|\boldsymbol{x}\| \leq r\}$ contains a set i linearly independent lattice points. We call $\lambda_i(L)$ the ith **successive minima** of L.
- Define the set $S_i(L) = \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = \lambda_i(L)\}$.
- Clearly $\lambda_1(L) \leq \ldots \leq \lambda_n(L)$.
- When $\lambda_1(L) = \ldots = \lambda_n(L)$ we say that the lattice is well rounded.

Similarity classes of lattices

A basis for a lattice Λ is not unique. If A is a basis matrix for lambda then B is a basis matrix for Λ if and only if $A = BU$ where $U \in \mathrm{GL}_d(\mathbb{Z})$

Two lattices $\Lambda = A\mathbb{Z}^d$ and $\Omega = E\mathbb{Z}^d$ are said to be **similar** if there exists a real number r and a real orthogonal matrix O so that

$$\Lambda = rO\Omega.$$

As such similarity classes of lattices can be identified with the triple quotient

$$\mathbb{R}\backslash \mathrm{O}_d(\mathbb{R})\backslash \mathrm{GL}_d(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}).$$

Reduction domains

The goal of reduction theory is to find a canonical representation for each similarity class of lattice.

Reduction Domain

A reduction domain is a set coset representative for element of

$$\mathbb{R}\backslash \mathrm{O}_d(\mathbb{R})\backslash \mathrm{GL}_d(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}).$$

The Gram matrix of a lattice

In the triple quotient

$$\mathbb{R}\backslash \mathrm{O}_d(\mathbb{R})\backslash \mathrm{GL}_d(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}).$$

- The action of $\mathbb{R}$ is trivial to work with. We can eliminate $\mathbb{R}$ by normalizing one of the geometric invariants of the lattice. Set each Λ to has $\det(\Lambda) = 1$ or set each Λ to have $\lambda_1(\Lambda) = 1$ etc.
- We can remove the action of $\mathrm{O}_d(\mathbb{Z})$ by considering the Gram matrix $G = A^T A$ where A is a basis matrix for Λ since $R^T R = I$ if $R \in \mathrm{O}_d(\mathbb{R})$.

The Gram matrix G is always a positive definite symmetric matrix. Thus we are considering the action of $\mathrm{GL}_d(\mathbb{Z})$ on the set of positive definite symmetric matrices where $U \in \mathrm{GL}_d(\mathbb{Z})$

$$U : G \to U^T G U.$$

Quadratic forms

Let S^d denote the space of $d \times d$ real symmetric matrices. S^d is a $\binom{d+1}{2}$ dimensional real vector space.
We define an inner product on S^d by

$$\langle G, H \rangle = \text{trace}(GH)$$

for $G, H \in S^d$
A quadratic form is a function $q : \mathbb{R}^d \to \mathbb{R}$ of the form

$$f(\boldsymbol{x}) = \boldsymbol{x}^T G \boldsymbol{x}$$

where $G \in S^d$.
With the inner product on S^d, $f(\boldsymbol{x}) = \left\langle G, \boldsymbol{x}\boldsymbol{x}^T \right\rangle$ so we will consider S^d to be the space of quadratic forms.

Arithmetic equivalence

Two quadratic forms $G, H \in S^d$ are said to be arithmetically equivalent if $G = U^T H U$ for some $U \in \mathrm{GL}_d(\mathbb{Z})$.

Let

$$S^d_{>0} = \{Q \in S^d : \left\langle Q, \boldsymbol{x}\boldsymbol{x}^T \right\rangle > 0, \forall \boldsymbol{x} \in \mathbb{R}^n_{\neq 0}\}$$

and

$$S^d_{\geq 0} = \{Q \in S^d : \left\langle Q, \boldsymbol{x}\boldsymbol{x}^T \right\rangle \geq 0, \forall \boldsymbol{x} \in \mathbb{R}^n_{\neq 0}\}$$

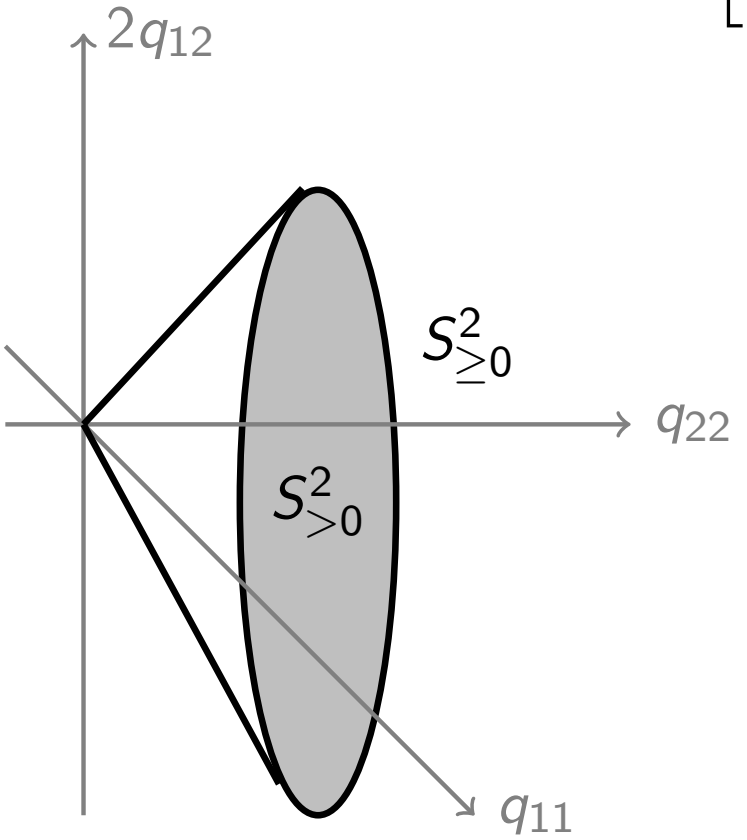
Similarity classes of lattices are in one-to-one correspondence to arithmetic equivalence classes of quadratic forms (with normalized determinant).

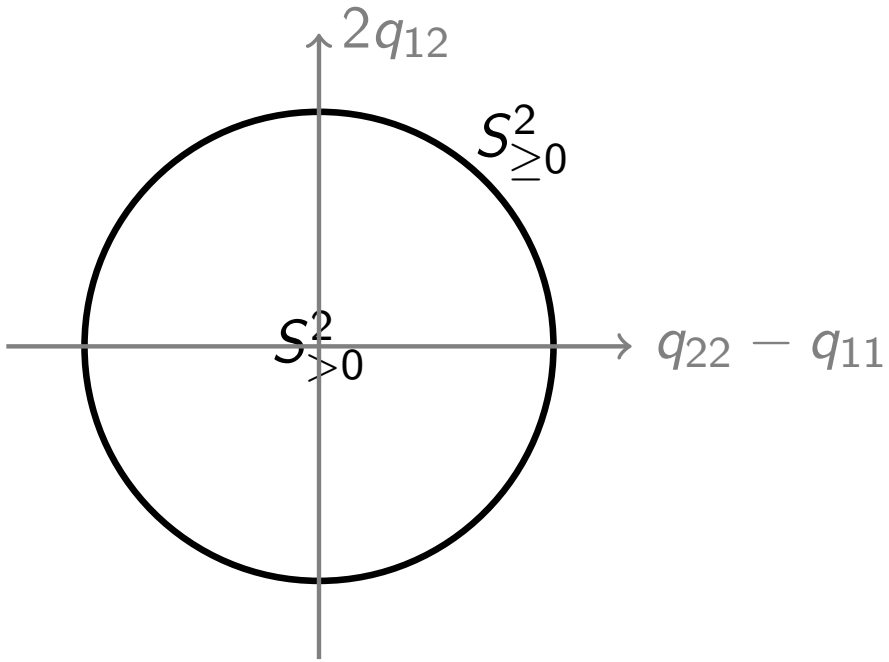
The cone of PDQFs

Clearly $S^d_{>0} \subset S^d_{\geq 0}$. It is not hard to show that both $S^d_{>0}$ and $S^d_{\geq 0}$ are cones in S^d meaning that for any $G, H \in S^d_{\geq 0}$ then $aG + bH \in S^d_{\geq 0}$ for any $a, b > 0$

S^d, $S^d_{>0}$ and $S^d_{\geq 0}$ in dimension 2

$$Q = \begin{bmatrix} q_{11} & q_{12} \\ q_{12} & q_{22} \end{bmatrix}$$





Reduction algorithms

In this talk we will examine 3 reduction algorithms

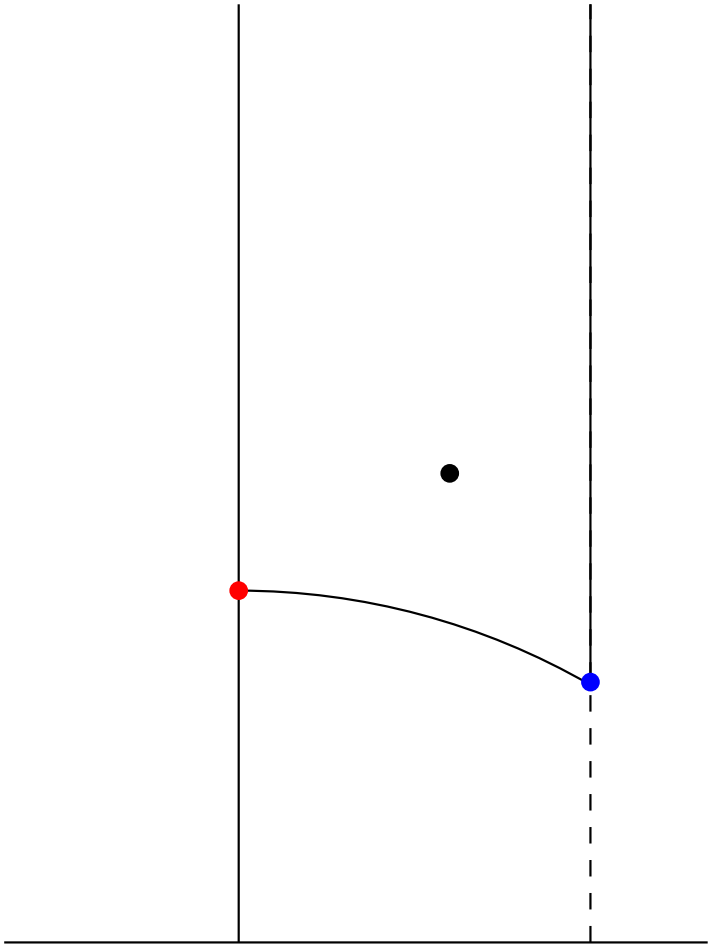
- the Minkowski reduction,
- the HKZ (Hermite-Korkine-Zolotarev) reduction,
- Voronoi's first reduction.

Minkowski reduction

A basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d$ for a lattice $\Lambda = A\mathbb{Z}^d$ is Minkowski reduced if

- **(1):** $\boldsymbol{a}_i$ is the shortest vector such that $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i\}$ can be extended to a basis for the lattice for each $1 \leq i \leq d$.
- **(2):** $\boldsymbol{a}_i \cdot \boldsymbol{a}_{i-1} \geq 0$ for each $2 \leq i \leq d$.
- **(3):** $\boldsymbol{a}_i \in \text{span}_{\mathbb{R}}\{e_1, \ldots, e_i\}$ and $\boldsymbol{a}_i \cdot e_i \geq 0$ for each $1 \leq i \leq d$.

Lagrange Reduction



- A (a, b) point in the reduction domain corresponds to the equivalence class of lattices given by

$$\begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix} \mathbb{Z}^2.$$

- The red dot is the lattice $\mathbb{Z}^n$ and the blue dot is the lattice

$$\begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix} \mathbb{Z}^2.$$

Minkowski reduction

A quadratic form $Q = \{q_{ij}\}$ is Minkowski reduced if

- **(1):** $\left\langle Q, \boldsymbol{x}\boldsymbol{x}^T \right\rangle \geq q_{ii}$ for all $\boldsymbol{x} \in \mathbb{Z}^n$ such that $\{e_1, \ldots, e_{i-1}, \boldsymbol{x}\}$ is extendable to a basis for $\mathbb{Z}^d$ for each $1 \leq i \leq d$.
- **(2):** $q_{ii+1} \geq 0$ for each $1 \leq i \leq d-1$.

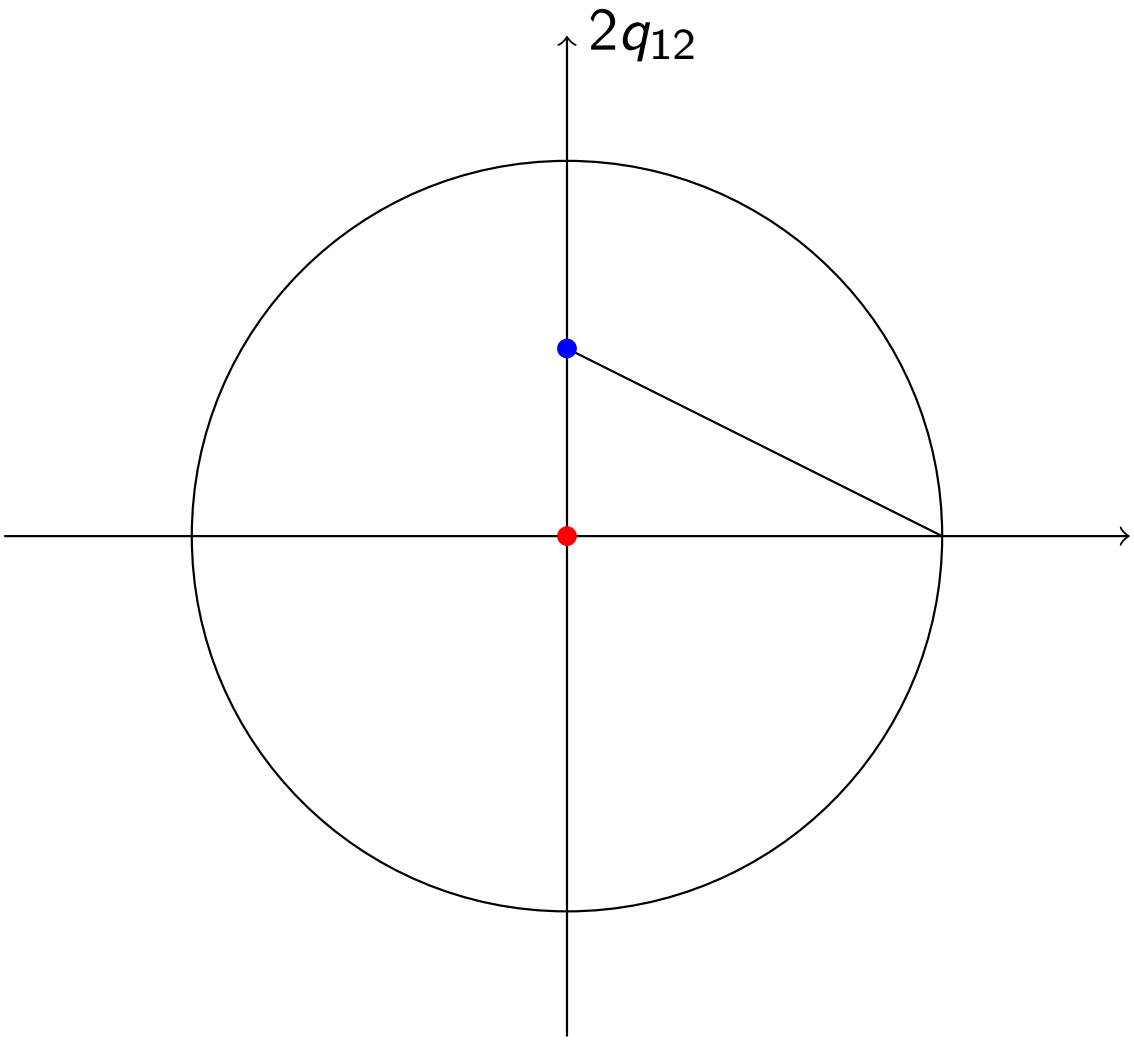
Let

$$M_d = \{Q \in S^d_{>0} : Q \text{ satisfies (1)}\}$$

and

$$M_d^+ = \{Q \in M_d : Q \text{ satisfies (2)}\}$$

Lagrange Reduction



Here a point (a, b) represents the symmetric matrix

$$\begin{bmatrix} q_{11} & q_{12} \\ q_{12} & q_2 2 \end{bmatrix}$$

Minkowski reduction

The non-linear inequalities in the Legrange domain become linear inequalities in the space of quadratic forms.

- This is true in general for the Minkowski reduction, M_d and M_d^+ are polyhedral cones in S^d.
- M_d has a larger number of facets then M_d^+ but due to symmetries can be easier to work with.

Finding the best lattice packing

Theorem (Minkowski)

M_d and M_d^+ are polyhedral cones and $M_d^+ \cap S^d_{>0}$ is a reduction domain in S^d

Theorem (Minkowski)

The quadratic form corresponding the best lattice packing is a vertex of M_d^+

Complexity of M_d and M_d^+

d	# of facets M_d	# of facets M_d^+	# of rays M_d	# of rays M_d^+
2	3	3	3	3
3	12	19	9	11
4	39	323	26	109
5	200	15971	117	4105
6	1675		1086	
7	65684			

The (Hermite)-Korkin-Zolotarev Reduction

A basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ for the lattice L is KZ-reduced if

1. $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ is a basis.
2. $\boldsymbol{x}_1$ is a shortest vector of L.
3. $\boldsymbol{x}_i$ minimizes $\|\text{proj}_{\text{span}\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{i-1}\}}\boldsymbol{x}_i\|$ among all possible choices of $\boldsymbol{x}_i$.

- If there are multiple possible choices of $\boldsymbol{x}_i$ at any step choose the one with the smallest norm. It there are multiple shortest choices one can be chosen at random [2].

Minkowski reduction vs HKZ

- Like the Minkowski reduction, the HKZ reduction gives a reduction domain (up to a finite set of sign changes).
- Also, like the Minkowski reduction the HKZ reduction defines a polyhedral cone in the space of quadratic forms and thus can also be used to find the best lattice packing in a given dimension.
- For a lattice Λ with HKZ reduced basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$

$$\frac{4}{i+3}\lambda_i(\Lambda) \leq \|\boldsymbol{b}_i\| \leq \frac{i+3}{4}\lambda_i(\Lambda)$$

  for each $1 \leq i \leq d$.
- There exists a lattice Λ with Minkowski reduced basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d$ and HkZ reduced basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ such that $\|\boldsymbol{a}_d\| \geq \|\boldsymbol{b}_d\|$ [2].

The LLL Reduction

Another advantage that the HKZ reduction has over the Minkowski reduction is the LLL (Lenstra-Lenstra-Lovász) algorithm

- LLL is not a true reduction, rather it is an approximation of the HKZ reduction.
- Unlike, the Minkowski reduction and the HKZ reduction which involve finding the shortest vector and thus solving an NP-hard problem LLL can run in polynomial time.

The Ryshkov polyhedron

Let

$$P = \{Q \in S^d_{>0} : \lambda_1(Q) \geq 1\} = \{Q \in S^d_{>0} : \left\langle Q\boldsymbol{x}\boldsymbol{x}^T \right\rangle \geq 1, \forall \boldsymbol{x} \in \mathbb{Z}^d_{\neq 0}\}.$$

We call P the Ryshkov polyhedron.

Theorem

P is locally finite polyhedron, i.e. for any convex polytope T, $P \cap T$ is a convex polytope.

This means that locally P behaves like a polytope and thus we can talk about the facets and vertices of P.
Each facet of P lies on the affine plane $\{Q \in S^d : \left\langle Q, \boldsymbol{x}\boldsymbol{x}^T \right\rangle\}$ for some integer vector $\boldsymbol{x}$.

Perfect lattices

If $Q \in S^d_{>0}$ is a vertex of P, then Q lies at the intersection of $\binom{n+1}{2}$ linearly independent affine planes.

In other words, let $\Lambda = A\mathbb{Z}^d$ be a lattice with Gram matrix $Q = A^T A$. Then $S(\Lambda) = \{\pm A\boldsymbol{x}_1, \ldots, \pm A\boldsymbol{x}_k\}$, is a set of vector such that $\boldsymbol{x}_1\boldsymbol{x}_1^T, \ldots, \boldsymbol{x}_k\boldsymbol{x}_k^T$ is a spanning set for S^d.

Lattices with this property are called **perfect**

Voronoi's algorithm

Theorem(Voronoi)

Up to arithmetic equivalence there are only finitely many perfect lattices in a given dimension.

Theorem(Voronoi/Minkowski)

The best lattice packing must be a perfect lattice.

Voronoi's algorithm

We can find all perfect forms in dimension d in the following way

- **(1):** Add a known perfect form to the list of perfect lattices. This can always be done as the root lattice A_d is perfect in every dimension.
- **(2):** For each known perfect form Q find the edges of the Ryshkov polyhedron that connect to Q.
- **(3):** follow each edge connected to Q until a vertex of the Ryshkov polyhedron is found. This is a perfect form Q'.
- **(4):** compare Q' to the list of known perfect forms. If Q' is new form add it to the list of perfect forms.
- **(5):** repeat 2-4 until no new perfect forms are found.

Notes about Voronoi's algorithm

- We find the edges of the Ryshkov polyhedron connected to perfect form Q by examining the secondary cone $P(Q)$. This is polyhedral cone that is determined by $\min(Q) = \{\boldsymbol{x} \in \mathbb{Z}^d_{\neq 0} : \langle Q, \boldsymbol{x}\boldsymbol{x}^T \rangle = 1\}$.
- For each perfect form we need to compute the shortest vectors.
- Part of the difficulty of running Voronoi's algorithm is that number of perfect forms grows at least exponentially with the dimension. [1, 4]
- Additionally there exist lattices that have a large number of shortest vectors (particularly E_8) and as such have extremely complicated secondary cones.

Number of Perfect Forms

n	# of PF	date	Authors
2	1	1773	Lagrange
3	1	1840	Gauss
4	2	1877	Korkin, Zolotarev
5	3	1877	Korkin, Zolotarev
6	7	1957	Barnes
7	33	1993	Jaquet-Chiffelle
8	10916	2005	Sikirić, Schürmann, Vallentin
9	2.237.251040	2026	Sikirić, van Woerden[3]

Voronoi domains of perfect cones

For a perfect lattice Q define

$$V(Q) = \text{cone}\{\min(Q)\} \cap S^d_{>0}.$$

Theorem(Voronoi)

$$S^d_{>0} = \bigcup_{Q \text{ is perfect}} V(Q),$$

and $V(Q) \cap V(Q')$ is a common face of $V(Q)$ and $V(Q')$ for $Q \neq Q'$.

Since there are only finitely many perfect forms up to equivalence we can select a representative set of perfect forms at take a union of their Voronoi domains. Like with M_d each Voronoi domain will contain a finite number copies of the same equivalence class of lattices which is a result of some finite group acting on the Voronoi domain.

References

- Roland Bacher. On the number of perfect lattices. Journal de théorie des nombres de Bordeaux, 30:917–945, 2018.
- Shvo Regavim. Minkowski bases, korkin-zolotarev bases and successive minima. 06 2021.
- Mathieu Dutour Sikiri´c and Wessel van Woerden. The lattice packing problem in dimension 9 by voronoi's algorithm. arXiv preprint arXiv:2508.20719, 2025.
- Wessel van Woerden. An upper bound on the number of perfect quadratic forms. Advances in Mathematics, 365:107031, 2020.