Optimization for lattices, packings, and coverings

Lecture 2

Frank Vallentin (Universität zu Köln)

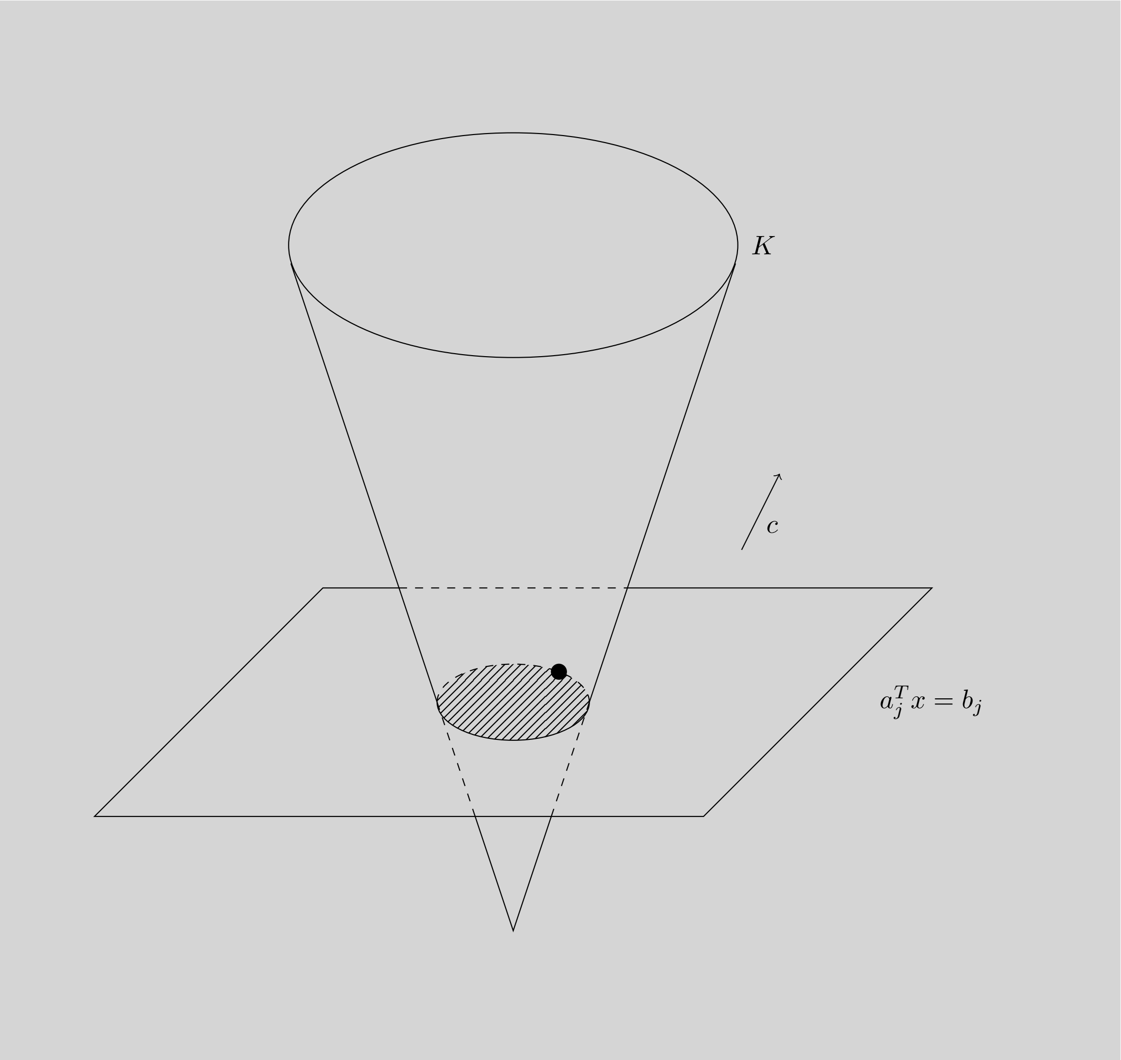
Online summer school on optimization, interpolation and modular forms
August 24 to 28, 2020
EPF Lausanne

1. Introduction to conic optimization

Recap from yesterday: Conic optimization

E finite-dimensional Euclidean space with inner product $\langle x, y \rangle$

$K \subseteq E$ proper convex cone



primal standard form of conic program

$$p^* = \sup \left\{ \langle c, x \rangle : x \in E,\, x \succeq_K 0,\, \langle a_j, x \rangle = b_j \; (j \in [m]) \right\}$$

Semidefinite programming (SDP)

$$E = \mathbb{S}^n, \quad \langle X, Y \rangle = \mathrm{Tr}\, XY, \quad K = \mathbb{S}^n_+$$

Determinant maximization (MAXDET)

$$E = \mathbb{S}^n \times \mathbb{R}, \quad \langle (X,s),(Y,t) \rangle = \mathrm{Tr}\, XY + st, \quad K = \mathscr{D}^{n+1} = \{(X,s) : X \in \mathbb{S}^n_+, s \geq 0, (\det X)^{1/n} \geq s\}$$

Polynomial optimization (POP)

$$E = \mathbb{R}[x_1, \ldots, x_n]_d, \quad \langle f, g \rangle = \frac{1}{d!} f(\nabla) g, \quad K = P_{n,d} = \{f : f(x) \geq 0 \text{ for all } x \in \mathbb{R}^n\}, \quad d \text{ even}$$

Algorithms and complexity - bad news -

Conic programs can be difficult - NP-hard - to solve.

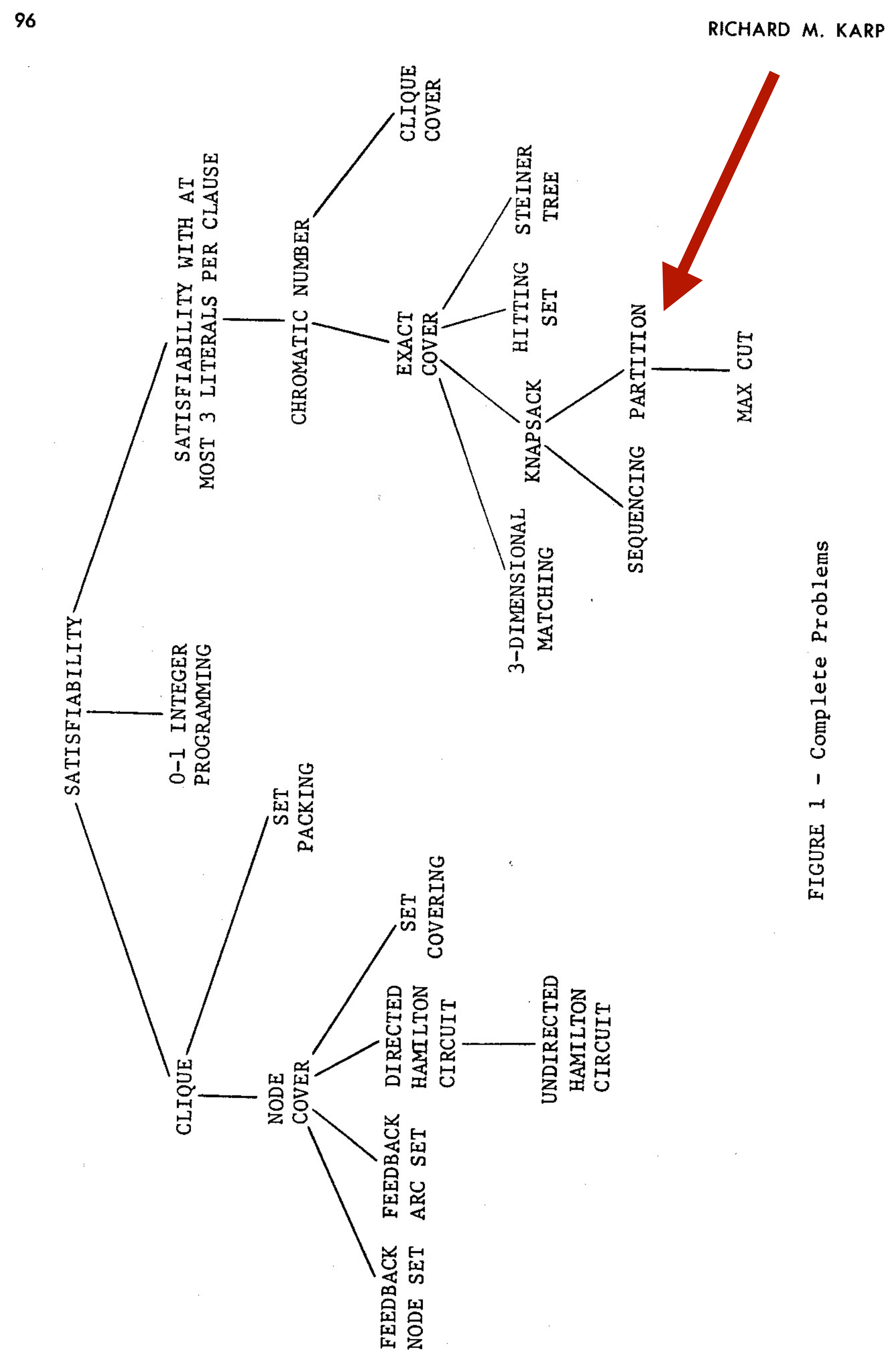
Polynomial time reduction from NP-complete PARTITION problem

PARTITION: Given $c \in \mathbb{N}^n$, does there exist $x \in \{-1, +1\}^n$ so that $c^{\mathsf{T}}x = 0$?

PARTITION has a positive answer exactly when

$$\sup \left\{ t : (c^{\mathsf{T}}x)^4 + n \sum_{i=1}^{n} x_i^4 - \left(\sum_{i=1}^{n} x_i^2 \right)^2 - t \in P_{n,4} \right\}$$

has $t = 0$ as optimal solution.



Algorithms and complexity
- good news -

LP, SOCP, SDP, MAXDET can be solved in polynomial time (under mild technical assumptions)

Theorem. Consider the primal semidefinite program

$$p^* = \sup\{\langle C, X\rangle : X \in \mathbb{S}^n_+, \langle A_1, X\rangle = b_1, \ldots, \langle A_m, X\rangle = b_m\}.$$

with rational input C, $A_1, \ldots, A_m$, and $b_1, \ldots, b_m$. Suppose we know a rational point $X_0 \in \mathcal{F}$ and positive rational numbers r, R so that

$$B(X_0, r) \subseteq \mathcal{F} \subseteq B(X_0, R),$$

where $B(X_0, r)$ is the ball of radius r, centered at X_0, in the affine subspace

$$\mathcal{F} = \{X \in \mathbb{S}^n : \langle A_j, X\rangle = b_j \text{ for } j = 1, \ldots, m\}.$$

For every positive rational number $\epsilon > 0$ one can find in polynomial time a rational matrix $X^* \in \mathcal{F}$ such that

$$\langle C, X^*\rangle - p^* \leq \epsilon,$$

where the polynomial is in n, m, $\log_2 \frac{R}{r}$, $\log_2(1/\epsilon)$, and the bit size of the data X_0, C, $A_1, \ldots, A_m$, and $b_1, \ldots, b_m$.

Proof using ellipsoid method (Grötschel, Lovász, Schrijver, 1981)

Proof using interior point method (de Klerk, Vallentin, 2016) based on (Nesterov, Nemirovski, 1994)

technical assumptions needed: $\operatorname{diag}\left(\begin{pmatrix} 1 & x_{i-1} \\ x_{i-1} & x_i \end{pmatrix},\ i = 1,\ldots,n\right) \in \mathbb{S}^{2n}_+,\ x_0 = 2 \Longrightarrow x_i \geq 2^{2^i}$

A first SDP application
- eigenvalue optimization -

$X \in \mathcal{S}^n$ symmetric matrix with (real) eigenvalues

$$\lambda_1(X) \geq \lambda_2(X) \geq \ldots \geq \lambda_n(X)$$

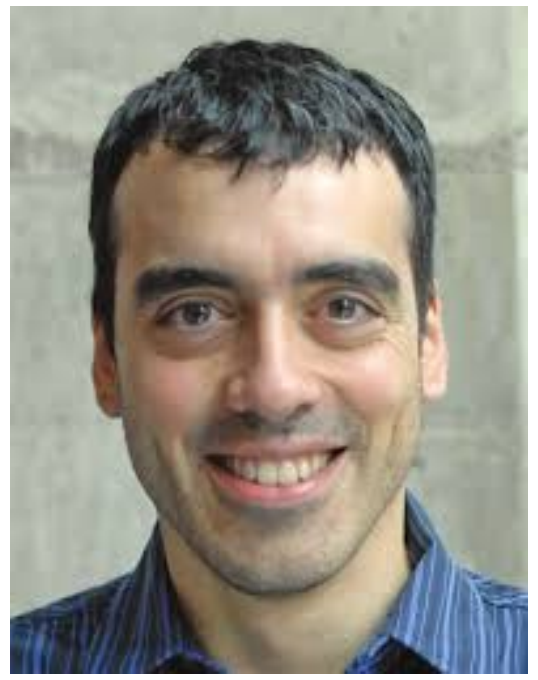
Finding the **sum of the largest k eigenvalues** is an SDP

$$\lambda_1(X) + \cdots + \lambda_k(X) = \max_{Y \in \mathcal{E}_k} \langle X, Y \rangle$$

$$\mathcal{E}_k = \{Y \in \mathcal{S}^n : I_n \succeq Y \succeq 0, \langle I_n, Y \rangle = k\}.$$

This gadget can be used to show that optimizing convex functions which only depend on the eigenvalues over given affine spaces of symmetric matrices is (usually) SDP representable.

A second SDP application
- polynomial optimization and sum of squares -

Lasserre (2001) Parrilo (2003)

$$
\begin{aligned}
p_{min} = \text{minimize} \quad & p(x) \\
& x \in K, \\
& K = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\},
\end{aligned}
$$

where $p, g_1, \ldots, g_m \in \mathbb{R}[x]$.

Clearly,

$$p_{min} = \sup\{t : p - t \in \mathcal{P}(K)\}$$

where

$$\mathcal{P}(K) = \{f \in \mathbb{R}[x] : f(x) \geq 0 \; \forall x \in K\}$$

Sum of squares relaxation

$$p_{sos} = \sup\{t : p - t \in \Sigma + g_1\Sigma + \cdots + g_m\Sigma\},$$

where

$$\Sigma = \{h_1^2 + \cdots + h_r^2 : r \in \mathbb{N}, h_i \in \mathbb{R}[x]\}$$

cone of sum of squares polynomials.

Sum of squares and SDP

$p \in \mathbb{R}[x]_{\leq d} \cap \Sigma$ if and only if $\exists Q \in \mathcal{S}_{\succeq 0}^{\binom{n+d}{d}}$:

$$p = [x]_d^\top Q [x]_d, \quad \text{i.e.} \quad \sum_{\substack{\beta,\gamma \in \mathbb{N}_d^n \\ \beta+\gamma=\alpha}} Q_{\beta,\gamma} = p_\alpha \ \ \forall \alpha \in \mathbb{N}_{2d}^n$$

Clearly

$$p_{min} = \sup\{t : p - t \in \mathcal{P}(K)\} \leq p_{sos} = \sup\{t : p - t \in \Sigma + g_1\Sigma + \cdots + g_m\Sigma\}$$

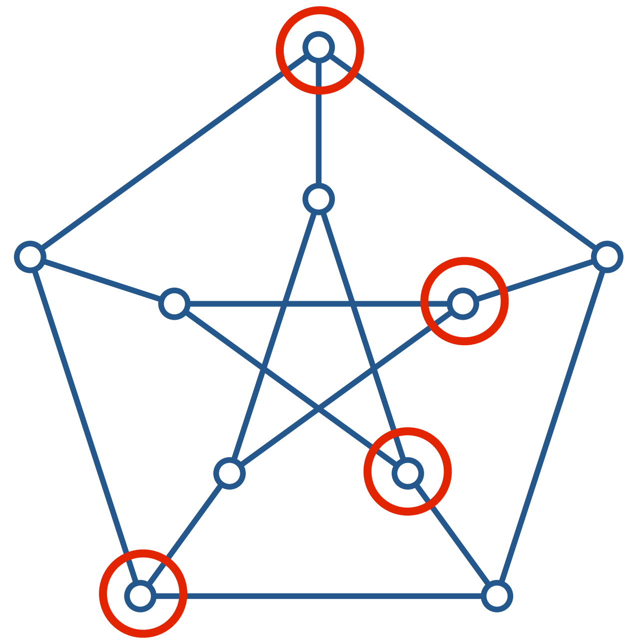
and generally $p_{min} \neq p_{sos}$.

Equality guaranteed for example by **Putinar's theorem**: If $\exists N \in \mathbb{N}$ such that $N - \sum_{i=1}^n x_i^2 \in \Sigma + g_1\Sigma + \cdots + g_m\Sigma$. Then

$$\forall x \in K : p(x) > 0 \Longrightarrow p \in \Sigma + g_1\Sigma + \cdots + g_m\Sigma$$

1. Extremely general and powerful result
2. Degree of Σ can be very high
3. Even for small degree: numerical instability
4. Right choice of polynomial basis poorly understood

A third SDP application
- approximating α and χ -



$\alpha(G) = 4$

$G = (V, E)$ finite graph with weight function $w : V \to \mathbb{R}_{\geq 0}$

$I \subseteq V$ is **independent** if $\{x, y\} \notin E$ or all $x, y \in I$

$$\alpha_w(G) = \max \left\{ \sum_{x \in I} w(x) : I \text{ independent} \right\}$$

weighted independence number of G.

$$\chi(G) = \min \left\{ k : \exists C_1, \ldots, C_k \text{ independent} : V = \bigcup_{i=1}^{k} C_i \right\}$$

chromatic number of G.

Finding α_w and χ is NP-hard.

Lovász' ϑ-number is an SDP relaxation for α_w

$$\alpha_w(G) \leq \vartheta'_w(G)$$

$$\begin{aligned} \vartheta'_w(G) = \min \quad & M \\ & K - (w^{1/2})(w^{1/2})^{\mathsf{T}} \text{ is positive semidefinite,} \\ & K(x,x) \leq M \quad \text{for all } x \in V, \\ & K(x,y) \leq 0 \quad \text{for all } \{x,y\} \notin E \text{ where } x \neq y, \\ & M \in \mathbb{R},\ K \in \mathcal{S}^V \end{aligned}$$

and for χ

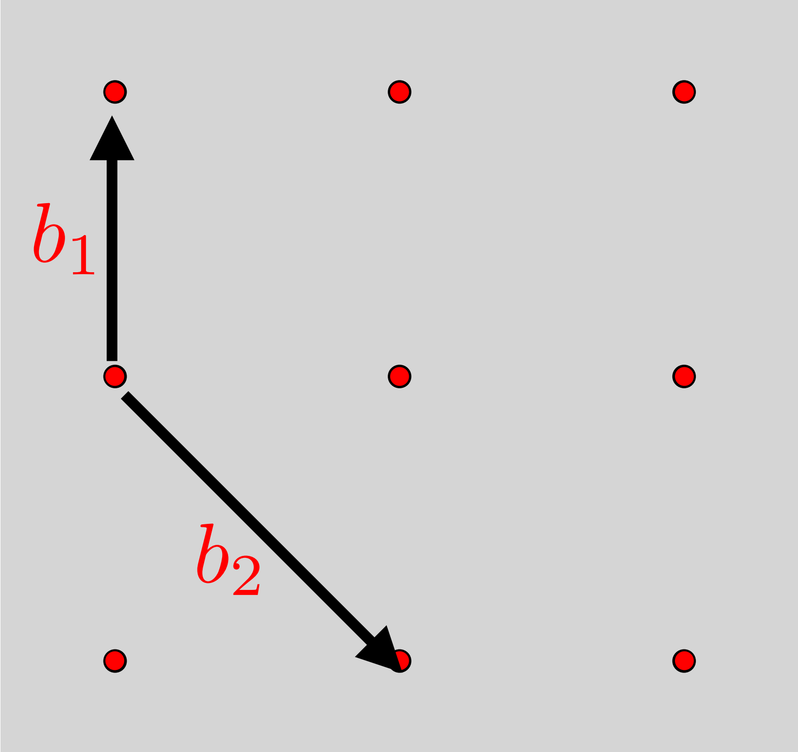
$$\chi(G) \geq \vartheta'_1(\overline{G}) = \max \left\{ \frac{\lambda_n(A) - \lambda_1(A)}{\lambda_n(A)} : A \in \mathcal{S}^V, A_{xy} \geq 0, A_{xy} = 0 \text{ for } \{x,y\} \notin E \right\}.$$

G.F. Voronoi (1868–1908)

2. Voronoi’s lattice reduction theory

Parameter space of lattices

Lattice $L = \mathbb{Z}b_1 + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_n \subseteq \mathbb{R}^n$



$$\overbrace{O(n) \setminus GL_n(\mathbb{R})}^{\mathbb{S}^n_{++}} \, / \, GL_n(\mathbb{Z})$$

orthogonal transformation
AB with $A \in O(n)$
leaves distances invariant

lattice basis
$B = (b_1, \ldots, b_n)$

lattice basis transformation
BT with $T \in GL_n(\mathbb{Z})$

Reduction theory of lattices

$\tilde{\mathbb{S}}^n_+ = \text{cone}\{xx^\mathsf{T} : x \in \mathbb{Z}^n\} \subset \mathbb{S}^n_+$ rational closure of $\mathbb{S}^n_{++}$

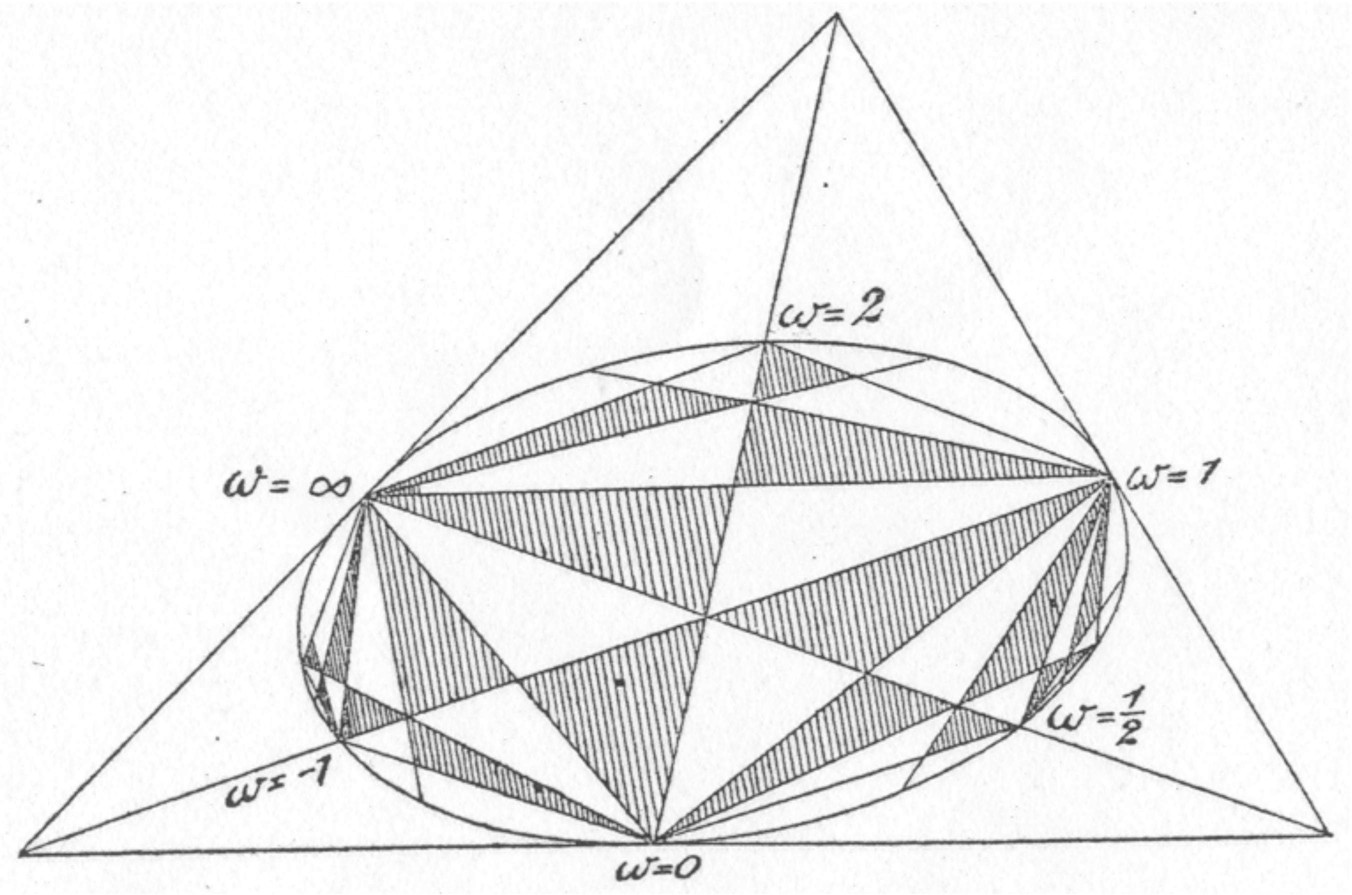
$GL_n(\mathbb{Z})$ acts on $\tilde{\mathbb{S}}^n_+$ by $(g, Q) \mapsto g^\mathsf{T} Q g$

reduction theory of lattices = find „nice“ fundamental domain for $\tilde{\mathbb{S}}^n_+$ / $GL_n(\mathbb{Z})$

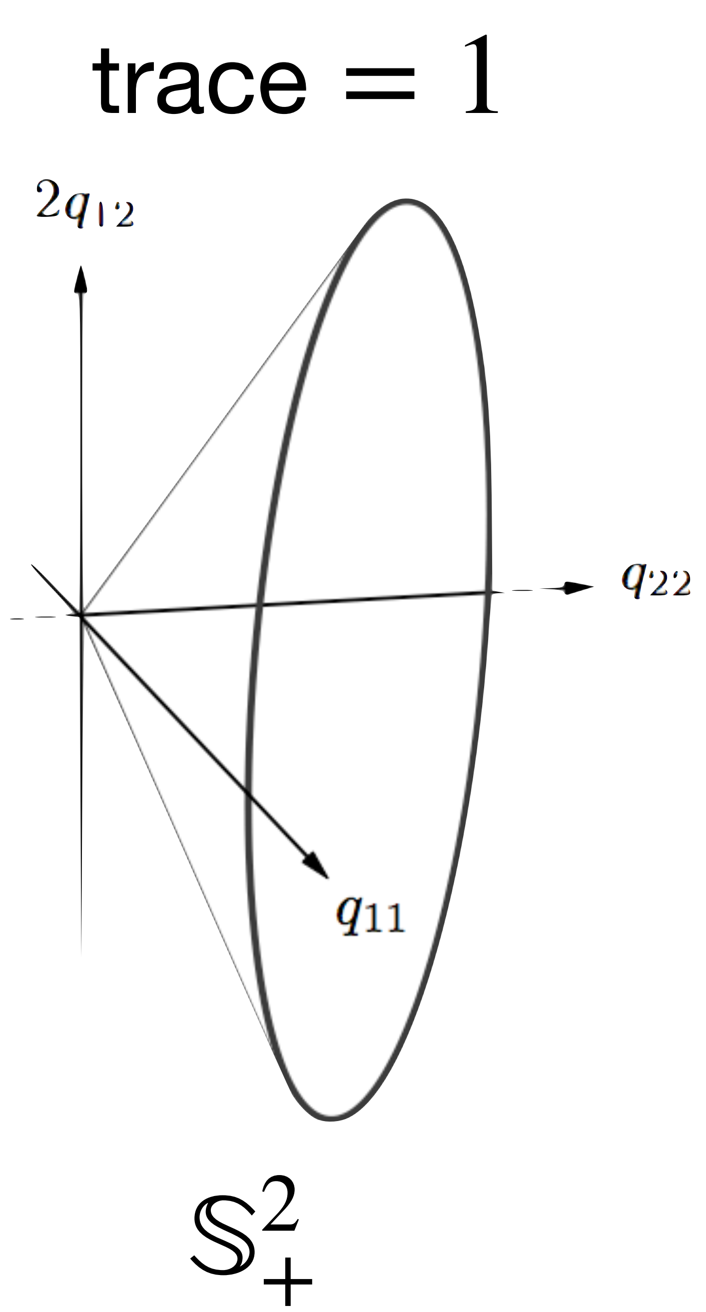
many constructions are known (coincide for $n = 2$, but not for $n > 2$)

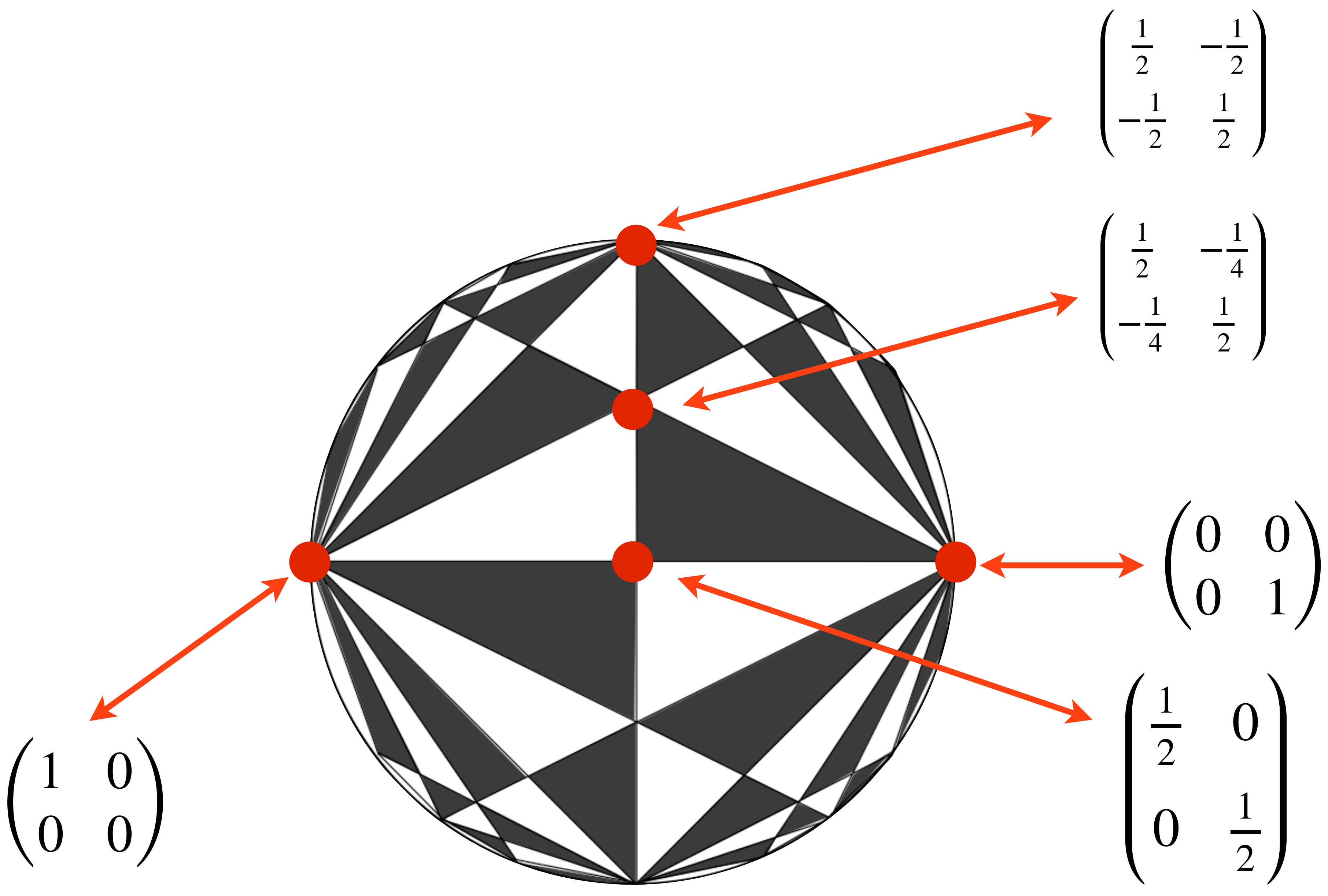
Minkowski, Voronoi (2x), …, LLL (Lenstra, Lenstra, Lovász)

„Best“ (= most expensive): Voronoi’s second reduction theory



Voronoi's second reduction theory





properties

infinite polyhedral face-to-face tiling

all triangular polyhedra $GL_2(\mathbb{Z})$-equivalent

Construction of Delaunay polyhedra

B.N. Delaunay
= Б.Н. Делоне
= B.N. Delone (1890–1980)

Empty sphere construction

Delaunay polyhedra of $Q \in \tilde{\mathbb{S}}^n_+$

$$P = \text{conv}\{v_1, v_2, \ldots\}, v_i \in \mathbb{Z}^n, \text{ where}$$

there is a center $c \in \mathbb{R}^n$ and a radius $r > 0$ so that

$$Q[v_i - c] = r^2 \text{ and } Q[w - c] > r^2 \text{ for all } w \in \mathbb{Z}^n \backslash \{v_1, v_2, \ldots\}$$

with $Q[x] = x^{\mathsf{T}} Q x$