

# Properties of Lattices

## A Semidefinite Programming Approach

Stefan van Zwam

November 17, 2005

# Lattices

A set  $\Lambda$  of vectors in  $\mathbb{R}^n$  is called a *lattice* if

$$\Lambda = \{x_1 \mathbf{a}_1 + \cdots + x_m \mathbf{a}_m \mid x_1, \dots, x_m \in \mathbb{Z}\}$$

for some linearly independent column vectors  $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathbb{R}^n$ . Matrix  $A = (\mathbf{a}_1, \dots, \mathbf{a}_m)$ . Basis is not unique. Two lattice bases are equivalent if

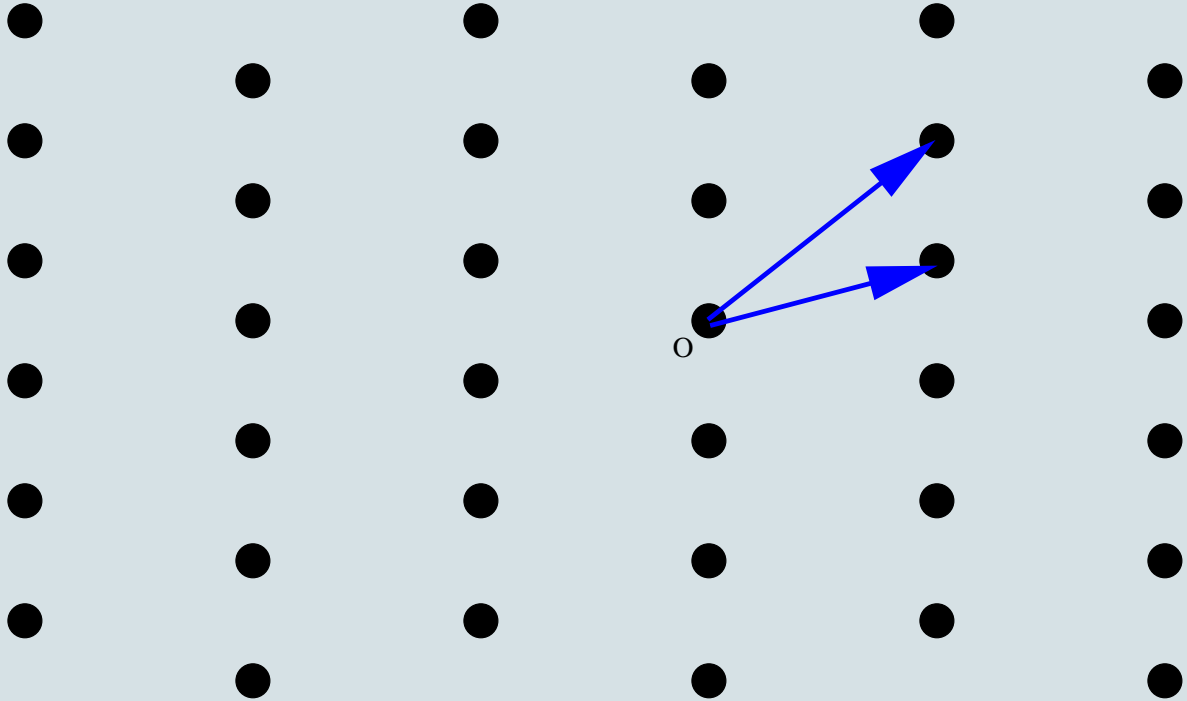
$$AZ^m = \tilde{A}Z^m.$$

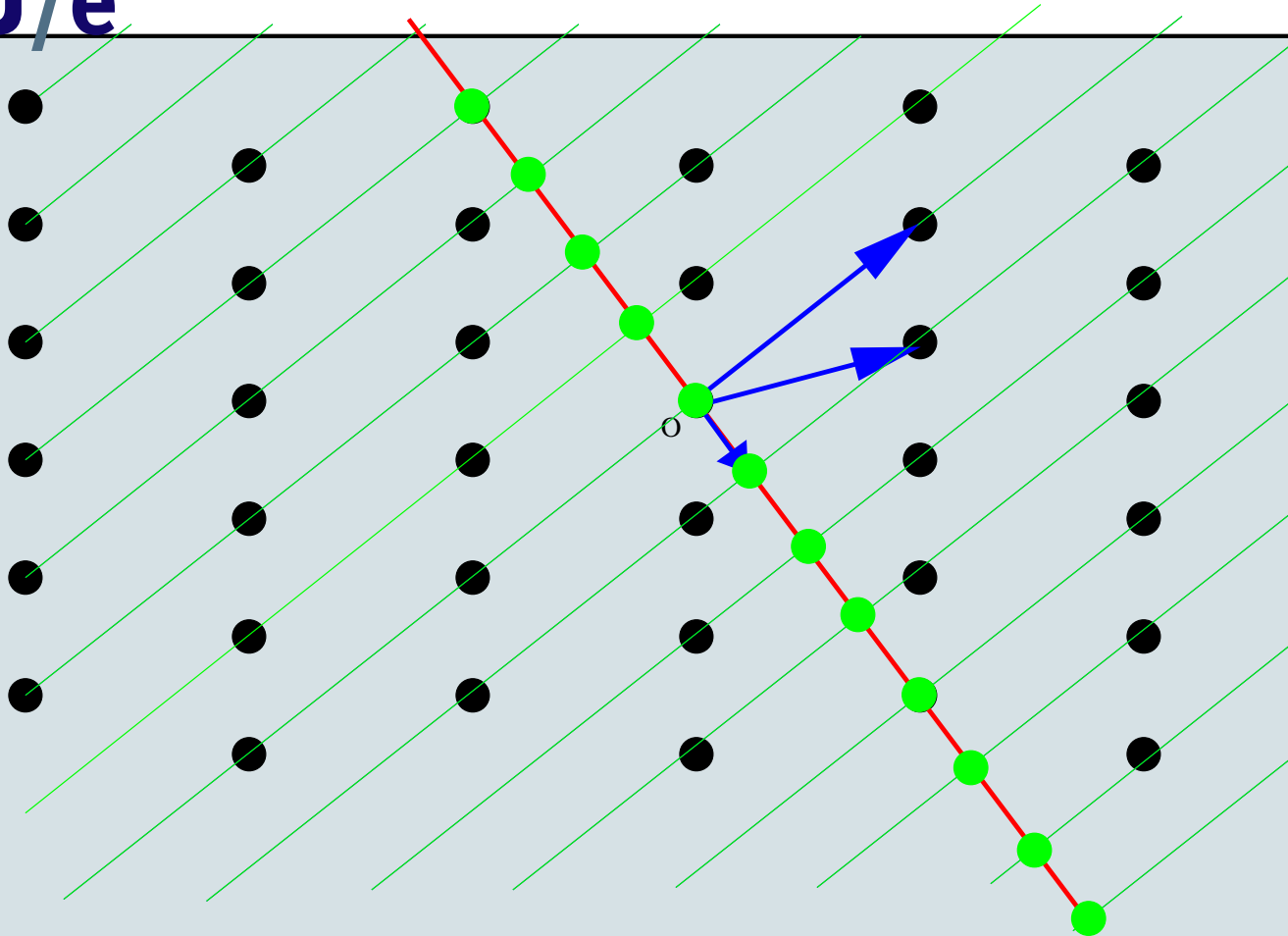
Two bases are equivalent iff there is a unimodular  $m \times m$  matrix  $U$  such that

$$A = \tilde{A}U$$

## Reduction Theory

- Goal: select a basis for  $\Lambda$  with “short” basis vectors.
- Many different notions: Gauss, Minkowski, LLL, . . .
- Very useful notion: *Korkin–Zolotarev* reduced bases. Uses projections.





## Quadratic Forms

Quadratic form associated with lattice  $\Lambda$ :

$$f(\mathbf{x}) := \mathbf{x}^T A^T A \mathbf{x} = \mathbf{x}^T B \mathbf{x}.$$

Matrix  $B$  is *positive semidefinite*.

### Lagrange Expansion

$$\begin{aligned} f(\mathbf{x}) = & A_1(x_1 - \alpha_{12}x_2 - \cdots - \alpha_{1n}x_n)^2 \\ & + A_2(x_2 - \alpha_{23}x_3 - \cdots - \alpha_{2n}x_n)^2 \\ & + \cdots + A_n x_n^2. \end{aligned}$$

## KZ-reduced Forms

Lagrange expansion:

$$f(\mathbf{x}) = \sum_{k=1}^n A_k (x_k - \sum_{l=k+1}^n \alpha_{kl} x_l)^2.$$

Partial expansion:

$$f_{ij}(\mathbf{x}) = \sum_{k=i}^j A_k (x_k - \sum_{l=k+1}^j \alpha_{kl} x_l)^2.$$

Form  $f$  is KZ-reduced if

- $|\alpha_{ij}| \leq 1/2$  and  $\alpha_{i,i+1} \geq 0$
- $A_i$  is the minimum of  $f_{in}(\mathbf{x})$  over all  $\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}$

## KZ-reduced forms: characterization

**Theorem 1** (Novikova (1977)). *For each  $n > 0$  there is a finite set of vectors  $Y_n$  such that each quadratic form  $f$  satisfying*

$$f \text{ is size-reduced,} \quad (1)$$

$$f_{2n} \text{ is KZ-reduced} \quad (2)$$

$$f(\mathbf{x}) \geq A_1 \text{ for all } \mathbf{x} \in Y_n, \quad (3)$$

*is KZ-reduced.*

Proof uses the following theorem:

**Theorem 2** (First KZ-inequality, Korkin and Zolotarev (1873)). *In the Lagrange expansion of a KZ-reduced quadratic form  $f$  the outer coefficients satisfy*

$$A_{i+1} \geq \frac{3}{4}A_i.$$

# Decomposition of a symmetric matrix

$$B = \begin{matrix} \square & & \\ & B^1 & \\ & & \end{matrix} + \begin{matrix} 0 & \dots & 0 \\ \vdots & & \\ 0 & \square & \\ & & B^2 \end{matrix} + \dots + \begin{matrix} \square & & \\ & \emptyset & \\ & & \square \\ & & & B^n \end{matrix}$$

Notation:

$$B = \bar{B}^1 + \bar{B}^2 + \dots + \bar{B}^n.$$

Lagrange decomposition:  $B^i$  is symmetric, positive semidefinite, and of rank 1.

Can be found from Lagrange expansion by

$$B^i = A_i(1, -\alpha_{i,i+1}, \dots, -\alpha_{in})(1, -\alpha_{i,i+1}, \dots, -\alpha_{in})^T.$$

## Semidefinite formulation (1/2)

$$\begin{aligned}\mathcal{A}^i &:= \{ \sqrt{A_i}(1, -\alpha_{i,i+1}, \dots, -\alpha_{in}) \in \mathbb{R}^{n-i+1} \mid A_i \geq 0, \alpha_{i,i+1} \geq 0, \\ &\quad |\alpha_{ij}| \leq -1/2 \quad (j = i+1, \dots, n) \} \\ &= \{ \boldsymbol{\alpha}_i \in \mathbb{R}^{n-i+1} \mid \mathbf{d}^T \boldsymbol{\alpha}_i \geq 0 \text{ for all } \mathbf{d} \in \mathcal{D}^i \}.\end{aligned}$$

$$\mathcal{B}^i := \{ \boldsymbol{\alpha} \boldsymbol{\alpha}^T \mid \boldsymbol{\alpha} \in \mathcal{A}^i \}.$$

We have

$$\mathcal{B}^i \subseteq \{ B^i \in \mathbf{S}_+^{n-i+1} \mid \mathbf{d}_1 \mathbf{d}_2^T \star B^i \geq 0 \text{ for all } \mathbf{d}_1, \mathbf{d}_2 \in \mathcal{D}^i \} =: \mathcal{K}^i.$$

## Semidefinite formulation (2/2)

Definition:  $B$  is *almost KZ-reduced* if it has an expansion such that

$$B^i \in \mathcal{K}^i \quad \text{for all } 1 \leq i \leq n \quad (4)$$

$$\mathbf{x}^T \left( \sum_{k=i}^n \bar{B}^k \right) \mathbf{x} \geq b_{ii}^i \quad \text{for all } \mathbf{x} \in \mathbb{Z}^n, \text{ for all } i. \quad (5)$$

Optimization over this class:

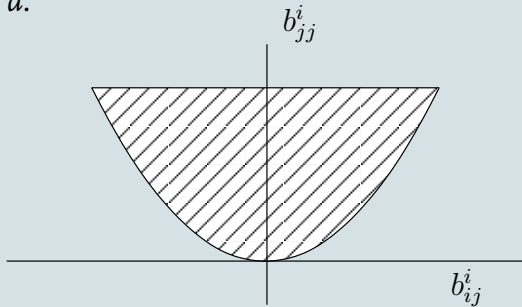
$$\text{minimize} \quad \sum_{i=1}^n C^i \star B^i \quad (\text{CP})$$

$$\text{subject to} \quad B^i \in \mathcal{K}^i \quad (1 \leq i \leq n) \quad (6)$$

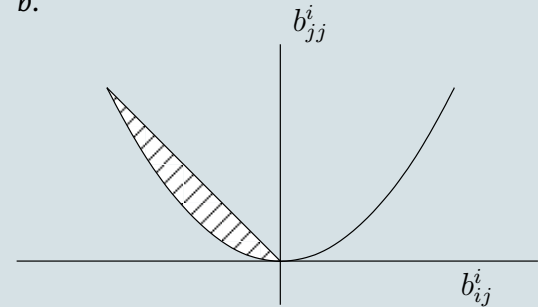
$$\sum_{i=1}^n F_j^i \star B^i \geq g_j \quad (1 \leq j \leq t). \quad (7)$$

# Branch-and-bound

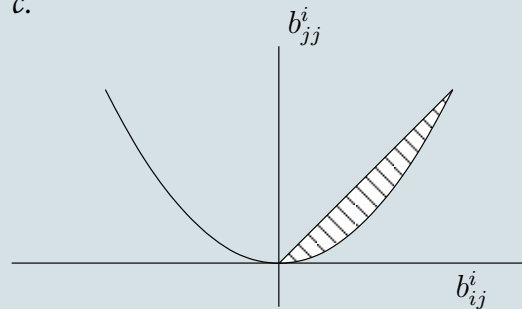
a.



b.



c.



Branch-and-bound policy: “Furthest from Rank One”.

## Application: finding small sets $X_j$ (1/2)

- Given are sufficient  $X_2, \dots, X_n$  and an  $\mathbf{x} \in X_n$ .
- Replace  $X_n$  by  $X_n \setminus \{\mathbf{x}\}$
- Compute minimum  $m_x$  of  $\mathbf{x}^T B \mathbf{x}$

If  $m_x \geq 1$  then  $\mathbf{x}$  is not an essential vector in  $X_n$  and can be removed. Sizes of the  $X_j$ :

	Dimension							
	2	3	4	5	6	7	8	
Novikova	1	3	12	52	408	21 294	1 655 885	
New methods	1	3	12	52	376	5 999	166 456	

## Application: minimality of set $X_j$ (2/2)

Use Branch-and-bound on SDP described previously to find a form violating only  $\mathbf{x}^T B \mathbf{x} \geq A_1$ . Example of such a form:

$$\begin{pmatrix} 720 & -360 & 360 \\ -360 & 720 & -450 \\ 360 & -450 & 720 \end{pmatrix}.$$

Lagrange expansion:  $f(\mathbf{x}) = 720(x_1 - 1/2x_2 + 1/2x_3)^2 + 540(x_2 - 1/2x_3)^2 + 405x_3^2$ .

$$f_{12}(0, 1) = 720 \geq A_1$$

$$f_{23}(0, 1) = 540 \geq A_2$$

$$f_{13}(0, 0, 1) = 720 \geq A_1$$

$$f_{13}(0, 1, 1) = 540 < A_1$$

$$f_{13}(1, 1, 1) = 1260 \geq A_1.$$

## Application: outer coefficients

Classical results (Korkin and Zolotarev, 1873):

$$A_2/A_1 \geq 3/4 \quad (8)$$

$$A_3/A_1 \geq 2/3 \quad (9)$$

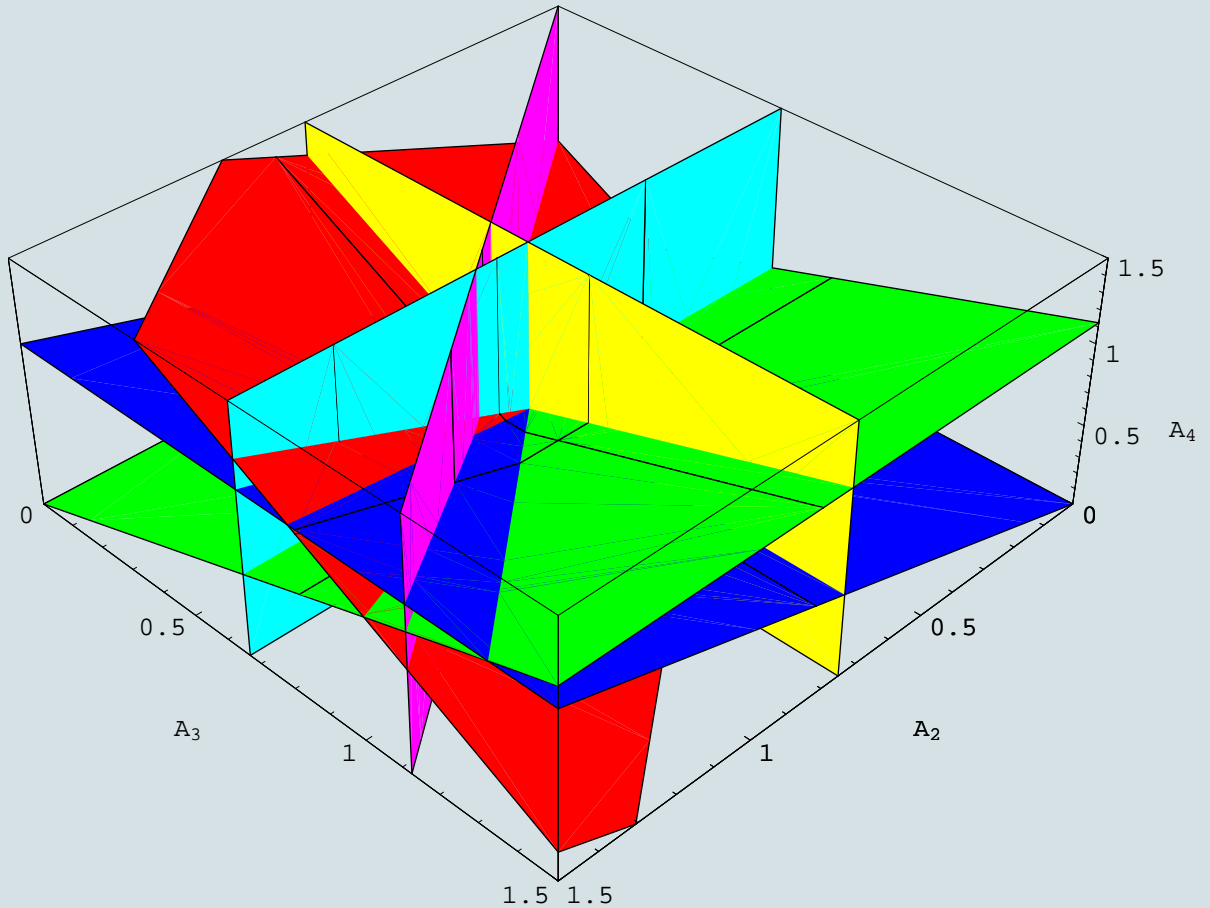
$$A_4/A_1 \geq 1/2 \quad (10)$$

All KZ-reduced forms reaching equality have been classified. Until now, no bounds known on  $A_5/A_1$  save  $A_5/A_1 > 4/9$ . Branch-and-bound yields

$$A_5/A_1 \geq 15/32$$

along with a KZ-reduced form reaching equality. Furthermore a new inequality in dimension 4:

$$-25A_1 - 36A_2 + 48A_3 + 40A_4 \geq 0.$$



## Numerical issues

- Results computed using floating-point arithmetic
- In some cases, limited numerical precision leads to infeasible solutions
- Rounding naively often destroys feasibility
- Rounding manually infeasible for branch-and-bound duals (over 20 000 for the proof of  $A_5/A_1 \geq 15/32$ ).

## Directions for future research

- An automated rounding mechanism providing exact solutions would turn conjectures into theorems.
- Complete investigation of dimensions 6 and above.
- Complete description of the (convex hull of) the set of outer coefficients  $(A_1, \dots, A_n)$ .
- Investigation of the complexity of an algorithm based on the sets  $X_j$ .