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

$$\Lambda = \{x_1a_1 + \cdots + x_ma_m \mid x_1, \ldots, x_m \in \mathbb{Z}\}$$

for some linearly independent column vectors $a_1, \ldots, a_m \in \mathbb{R}^n$. Matrix $A = (a_1, \ldots, a_m)$. 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, . . .
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

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

1. \( f \) is size-reduced,
2. \( f_{2n} \) is KZ-reduced
3. \( f(\mathbf{x}) \geq A_1 \) for all \( \mathbf{x} \in Y_n \),

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**

\[
B = \begin{bmatrix}
B^1 \\
\vdots \\
0
\end{bmatrix} + \begin{bmatrix}
0 & \cdots & 0 \\
\vdots & & B^2 \\
0 & & & \ddots & \ddots & \ddots \\
& & & & & \ddots & \ddots & \ddots \\
& & & & & & \ddots & \ddots & B^n \\
& & & & & & & \vdots & \ddots & \ddots & \ddots \\
& & & & & & & & \ddots & \ddots & \ddots & B^n
\end{bmatrix} + \cdots + \begin{bmatrix}
0
\end{bmatrix}
\]

Notation:

\[
B = \bar{B}^1 + \bar{B}^2 + \cdots + \bar{B}^n.
\]

Lagrange decomposition: \(B^i\) is symmetric, positive semidefinite, and of rank 1.
Can be found from Lagrange expansion by

\[
B^i = A_i(1, -\alpha_{i,i+1}, \ldots, -\alpha_{in})(1, -\alpha_{i,i+1}, \ldots, -\alpha_{in})^T.
\]
Semidefinite formulation (1/2)

\[ \mathcal{A}^i := \left\{ \sqrt{A_i}(1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}) \in \mathbb{R}^{n-i+1} \mid A_i \geq 0, \alpha_{i,i+1} \geq 0, \right. \\
\left. |\alpha_{ij}| \leq -1/2 \ (j = i + 1, \ldots, n) \right\} \]
\[ = \left\{ \alpha_i \in \mathbb{R}^{n-i+1} \mid \mathbf{d}^T \alpha_i \geq 0 \text{ for all } \mathbf{d} \in \mathcal{D}^i \right\} . \]

\[ \mathcal{B}^i := \{ \alpha \alpha^T \mid \alpha \in \mathcal{A}^i \} . \]

We have

\[ \mathcal{B}^i \subseteq \left\{ \mathcal{B}^i \in \mathbb{S}^{n-i+1}_+ \mid \mathbf{d}_1 \mathbf{d}_2^T \mathcal{B}^i \geq 0 \text{ for all } \mathbf{d}_1, \mathbf{d}_2 \in \mathcal{D}^i \right\} =: \mathcal{K}^i . \]
Semidefinite formulation (2/2)

Definition: \( B \) is almost KZ-reduced if it has an expansion such that

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

\[
x^T \left( \sum_{k=i}^{n} \overline{B}^k \right) x \geq b^i_{ii} \quad \text{for all } x \in \mathbb{Z}^n, \text{ for all } i. \quad (5)
\]

Optimization over this class:

\[
\begin{align*}
\text{minimize} & \quad \sum_{i=1}^{n} C^i \star B^i \\
\text{subject to} & \quad B^i \in \mathcal{K}^i \quad (1 \leq i \leq n) \quad (6) \\
& \quad \sum_{i=1}^{n} F^i_j \star B^i \geq g_j \quad (1 \leq j \leq t). \quad (7)
\end{align*}
\]
Branch-and-bound policy: “Furthest from Rank One”.

\[ b^i_{jj} \]
\[ b^i_{ij} \]
\[ b^i_{jj} \]
\[ b^i_{ij} \]
Application: finding small sets $X_j$ (1/2)

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

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

<table>
<thead>
<tr>
<th>Dimension</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Novikova</td>
<td>1</td>
<td>3</td>
<td>12</td>
<td>52</td>
<td>408</td>
<td>21</td>
<td>294</td>
</tr>
<tr>
<td>New methods</td>
<td>1</td>
<td>3</td>
<td>12</td>
<td>52</td>
<td>376</td>
<td>5</td>
<td>999</td>
</tr>
</tbody>
</table>
Application: minimality of set $X_j$ (2/2)

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

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

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

$$
f_{12}(0, 1) = 720 \geq A_1 \\
f_{23}(0, 1) = 540 \geq A_2 \\
f_{13}(0, 0, 1) = 720 \geq A_1 \\
f_{13}(0, 1, 1) = 540 < A_1 \\
f_{13}(1, 1, 1) = 1260 \geq A_1.
$$
Application: outer coefficients

Classical results (Korkin and Zolotarev, 1873):

\[ \frac{A_2}{A_1} \geq \frac{3}{4} \]  
(8)
\[ \frac{A_3}{A_1} \geq \frac{2}{3} \]  
(9)
\[ \frac{A_4}{A_1} \geq \frac{1}{2} \]  
(10)

All KZ-reduced forms reaching equality have been classified. Until now, no bounds known on \( \frac{A_5}{A_1} \) save \( \frac{A_5}{A_1} > \frac{4}{9} \).
Branch-and-bound yields

\[ \frac{A_5}{A_1} \geq \frac{15}{32} \]

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 \((A_1, \ldots, A_n)\).
- Investigation of the complexity of an algorithm based on the sets \(X_j\).