NEW KORKIN–ZOLOTAREV INEQUALITIES

R. A. PENDAVINGH, S. H. M. VAN ZWAM

Abstract. Korkin and Zolotarev showed that if

$$\sum_i A_i(x_i - \sum_{j>i} \alpha_{ij} x_j)^2$$

is the Lagrange expansion of a Korkin–Zolotarev reduced positive definite quadratic form, then $A_{i+1} \geq \frac{3}{4}A_i$ and $A_{i+2} \geq \frac{2}{3}A_i$. They showed that the implied bound $A_5 \geq \frac{4}{9}A_1$ is not attained by any KZ-reduced form.

We propose a method to optimize numerically over the set of Lagrange expansions of Korkin–Zolotarev reduced quadratic forms. Applying these methods, we show among other things that $A_{i+4} \geq (\frac{15}{32} - 2 \cdot 10^{-5})A_i$ for any KZ-reduced quadratic form, and we give a form with $A_5 = \frac{15}{32}A_1$.

We use the method to find bounds on Hermite's constant, and to compute estimates of the quality of k-block KZ-reduced lattice bases.

1. Preliminaries and Overview

An n-ary positive definite quadratic form q can be written uniquely as

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} A_i(x_i - \sum_{j>i} \alpha_{ij} x_j)^2. \tag{1}$$

This is the *Lagrange expansion* of q; the numbers A_i are the *outer coefficients* and the α_{ij} the *inner coefficients*. We write

$$q_k(x_k, \ldots, x_n) := \sum_{i=k}^{n} A_i(x_i - \sum_{j>i} \alpha_{ij} x_j)^2. \tag{2}$$

A positive definite quadratic form q in n variables with Lagrange expansion (1) is *Korkin–Zolotarev reduced (KZ-reduced)* if

$$|\alpha_{ij}| \leq \frac{1}{2} \text{ for all } i, j, \text{ and } \alpha_{i,i+1} > 0 \text{ for all } i; \tag{S}$$

and

$$A_k \leq q_k(x) \text{ for all nonzero } x \in \mathbb{Z}^{n-k+1}, k = 1, \ldots, n-1. \tag{M}$$

We say that two forms q, q' are *equivalent* if there is a unimodular matrix U such that $q'(x) = q(Ux)$. Any form is equivalent to a KZ-reduced form.

Korkin and Zolotarev proved that the outer coefficients of a KZ-reduced form satisfy $A_2 \geq \frac{3}{4}A_1$ (the *first KZ-inequality*) and $A_3 \geq \frac{2}{3}A_1$ (the *second KZ-inequality*) [3]. If q is KZ-reduced, then so is the quadratic form q_k for $k > 1$, and hence the inequalities

$$A_{k+1} \geq \frac{3}{4}A_k \text{ and } A_{k+2} \geq \frac{2}{3}A_k, \ k = 1, 2, \ldots \tag{3}$$

Date: April 28, 2006.

hold for the outer coefficients of any KZ-reduced form.

For each $n \in \mathbb{N}$, *Hermite's constant* is defined as

$$\gamma_n := \max\{\frac{m(q)}{\det(q)^{\frac{1}{n}}} \mid q \text{ is an } n\text{-ary positive definite quadratic form}\}, \tag{4}$$

where $m(q) := \min\{q(x) \mid x \in \mathbb{Z}^n, x \neq 0\}$ is the *minimum* of the form q. Equivalent forms have the same minimum and the same determinant, so we may as well restrict ourselves in (4) to KZ-reduced forms. Also, if $A_1, \ldots, A_n$ are the outer coefficients of a form q then $\det(q) = \prod_i A_i$, and if q is KZ-reduced then $m(q) = f(1, 0, \ldots, 0) = A_1$. Hence

$$\gamma_n^n = \max\{\frac{A_1^n}{\prod_i A_i} \mid (A_1, \ldots, A_n) = A(q) \text{ for some KZ-reduced form } q\}, \tag{5}$$

where $A(q) := (A_1, \ldots, A_n)$ denotes the sequence of outer coefficients of the quadratic form q. Using (3), this implies the tight bound

$$\gamma_4^4 \leq \max\{\frac{A_1^4}{\prod_{i=1}^4 A_i} \mid A_1 > 0, A_{i+1} \geq \frac{3}{4}A_i, A_{i+2} \geq \frac{2}{3}A_i\} = 4, \tag{6}$$

which is the main result of [2].

The proof of the second KZ-inequality was elementary but already quite involved. To prove an upper bound on γ_5, Korkin and Zolotarev developed other techniques [4]: they characterized the local optima of (4), which enabled them to enumerate all local optima for $n = 5$. This line of investigation has been continued and is still actively pursued [6].

In this paper, we focus again on the feasible set of (5). We develop a method to prove linear inequalities that hold for the outer coefficients of KZ-reduced forms. Our method is numerical, and uses recently developed semialgebraic optimization techniques. We apply our method in particular to forms in 5 variables, and obtain inequalities (Theorems 4 and 5) that imply, through (5), an upper bound on γ_n that is very close to the known value for $n = 5, 6, 7, 8$.

The structure of the paper is as follows. In the next section, we give preliminaries on KZ-reduced forms. In particular, we describe results of Novikova [7], that imply that the set of KZ-reduced forms can be defined by finitely many polynomial inequalities. Proving that a linear inequality on the outer coefficients holds for KZ-reduced forms thus amounts to minimizing the value of a polynomial under finitely many polynomial constraints.

Through recent developments in convex optimization it is possible to find lower bounds for such polynomial optimization problems using semidefinite optimization methods. We describe such a semidefinite 'relaxation' in Section 3.

We improve upon the lower bound that results from simply computing the semidefinite relaxation by splitting the semialgebraic set over which we are optimizing. Then the smallest of the lower bounds we obtain from each of the resulting semidefinite relaxations is again a lower bound. The *branch and bound* procedure for splitting the feasible set, familiar from integer programming, is described in Section 4.

Although we use a numerical method, our final results are exact in the sense that their validity does not depend on the accuracy with which the floating point computations were performed. Each of the many lower bounds we have computed is determined by a convex optimization problem which has a well-defined convex dual.

By rounding each optimal dual solution to a nearby rational and feasible solution, an exact lower bound is obtained. Its validity can be verified independently, using elementary rational arithmetic only. The rounding method is described in Section 5.

The remainder of the paper details the outcome of our computations, and gives applications to the analysis of lattice reduction algorithms and to the computation of Hermite's constant.

The implementation and verification of our numerical method is detailed in [12].

2. A finite characterization of KZ-reduced forms

One easily sees that a positive definite quadratic form q of two or more variables is KZ-reduced if (**S**) holds, if q_2 is KZ-reduced and if

$$A_1 \leq q(x) \text{ for all nonzero } x \in \mathbb{Z}^n.$$

In [7], Novikova stated the following:

Theorem 1. *For each $n \geq 2$, there is a finite set $X_n \subseteq \mathbb{Z}^n$ such that an n-ary form with Lagrange expansion* (1) *is KZ-reduced if and only if q_2 is KZ-reduced,* (**S**) *holds and*

$$A_1 \leq q(x) \text{ for all } x \in X_n.$$

The proof boils down to the fact that if q_2 is KZ-reduced, (**S**) holds, and $q(0,1,0,\ldots,0) \geq A_1$, then $q(x) \geq A_1$ is implied for all but finitely many $x \in \mathbb{Z}^n$. This argument yields highly redundant sets X_n. But the theorem implies the existence of a unique irredundant set X_n, which we will denote by X_n^*. In [7], Novikova gives finite sets X_n for $n \leq 8$ and claims irredundancy of these sets for $n \leq 5$. It is a shame that the proofs were omitted from her paper — it appears to be a significant challenge to determine these irredundant sets. We were only able to verify her claims for $n \leq 4$. For $n \in \{5, 6\}$ we find sets that are slightly larger, and for larger n the sets we compute are much smaller [11].

It is easy to see that $X_n^* = \{x \in \mathbb{Z}^n \mid (x, 0) \in X_{n+1}^*\}$ for any $n \geq 2$. Let $\bar{X} := \{(x, 0) \mid x \in X\}$. According to Novikova, one has

$$X_2^* = \{\begin{bmatrix}0\\1\end{bmatrix}\}, \tag{7}$$

$$X_3^* \setminus \bar{X}_2^* = \{\begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}\}. \tag{8}$$

Moreover, $X_4^* \setminus \bar{X}_3^*$ is a set of 12 vectors, and $X_5^* \setminus \bar{X}_4^*$ is a set of 52 vectors [7].

Using Theorem 1 we find that in the definition of KZ-reducedness requirement (**M**) is equivalent to

$$A_k \leq q_k(x) \text{ for all } x \in X_{n-k+1}^*, k = 1, \ldots, n-1. \tag{**N**}$$

Thus $(A_1, \ldots, A_n, \alpha_{12}, \ldots, \alpha_{nn})$ are the outer and inner coefficients of a KZ-reduced form if and only if they satisfy finitely many linear inequalities (**S**) and finitely many cubic inequalities (**N**).

It is even possible to characterize the KZ-reduced forms using only linear and quadratic inequalities. Let Q be a positive definite $n \times n$ matrix and let $q(x) :=$

x^tQx. Then the Lagrange expansion (1) yields a decomposition

$$Q = \sum_{i=1}^{n} a_i^t a_i = C^t C, \tag{9}$$

where

$$a_i = \sqrt{A_i}(0, \ldots, 0, 1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}) \tag{10}$$

is a row vector for $i = 1, \ldots, n$ and C is the matrix whose i-th row is a_i.

Thus C is upper triangular, and $Q = C^tC$ is the Choleski decomposition of Q.

Let $D^i := [0, \frac{1}{2}] \times [-\frac{1}{2}, \frac{1}{2}]^{n-i-1}$. Then

$$\{\sqrt{A_i}(0, \ldots, 0, 1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}) \mid A_i \geq 0, (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in D^i\} \tag{11}$$

is a polyhedral cone, so there is a finite set of vectors D_i such that (11) equals

$$\{a \in \mathbb{R}^n \mid ad \geq 0 \text{ for all } d \in D_i\}. \tag{12}$$

For $x \in \mathbb{Z}^m$, we write $\tilde{x} := (0, \ldots, 0, x_1, \ldots, x_m) \in \mathbb{Z}^n$. Then one easily verifies that $q(x) = x^tQx$ is KZ-reduced if and only if there are row vectors $a_i \in \mathbb{R}^n$ such that $Q = \sum_i a_i^t a_i$ and

$$a_k d \geq 0 \text{ for all } d \in D_k \text{ for } k = 1, \ldots, n; \tag{S'}$$

and

$$\sum_{i=k}^{n} (a_i \tilde{x})^2 \geq a_{kk}^2 \text{ for all } x \in X^*_{n-k+1}, k = 1, \ldots, n-1. \tag{N'}$$

3. A semidefinite relaxation

The characterizations above describe the coefficient domain of KZ-reduced forms as a semialgebraic set. There is by now a standard machinery for constructing semidefinite relaxations for the problem of minimizing a polynomial over a semialgebraic set, see [5, 8]. We describe a semidefinite formulation below, that has the virtue of yielding a reasonable lower bound while not being excessively large.

Theorem 2. *Let Q be an $n \times n$ positive definite matrix and let $q(x) = x^tQx$. Then q is KZ-reduced if and only if there are $n \times n$ matrices $B^1, \ldots, B^n$ such that $Q = B^1 + \cdots + B^n$ and*

$$B^k \text{ has rank } 1 \text{ for } k = 1, \ldots, n; \tag{r}$$

$$B^k \text{ is positive semidefinite for } k = 1, \ldots, n; \tag{p}$$

$$d_1^t B^k d_2 \geq 0 \text{ for all } d_1, d_2 \in D_k, \text{ for } k = 1, \ldots, n; \tag{s}$$

$$\sum_{i=k}^{n} \tilde{x}^t B^i \tilde{x} \geq B^k_{kk} \text{ for all } x \in X^*_{n-k+1}, \text{ for } k = 1, \ldots, n-1. \tag{n}$$

Proof. To see necessity, let q be KZ-reduced and let A_i, α_{ij} be its outer and inner coefficients. Put

$$a_i = \sqrt{A_i}(0, \ldots, 0, 1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}). \tag{13}$$

Then $a_1, \dots, a_n \in \mathbb{R}^n$ are row vectors satisfying (**S'**) and (**N'**), and such that $Q = \sum_{i=1}^n a_i^t a_i$. Let

$$B^i = a_i^t a_i = A_i \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & 1 & -\alpha_{i,i+1} & \cdots & -\alpha_{in} \\ \mathbf{0} & -\alpha_{i,i+1} & \alpha_{i,i+1}\alpha_{i,i+1} & \cdots & \alpha_{i,i+1}\alpha_{in} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & -\alpha_{in} & \alpha_{in}\alpha_{i,i+1} & \cdots & \alpha_{in}\alpha_{in} \end{bmatrix}. \tag{14}$$

(Here the **0**'s are zero matrices and vectors of appropriate sizes.) Then $(B^1, \dots, B^n)$ clearly satisfies (**r**), (**p**),(**s**) and (**n**).

For sufficiency, let $B^1, \dots, B^n$ be $Q = B^1 + \cdots + B^n$ and (**r**), (**p**),(**s**) and (**n**) hold. As B' has rank 1, we may write $B^i = a_i^t a_i$, where $a_{ii} \geq 0$. Then a_i clearly satisfies (**N'**). To see that a_i satisfies (**S'**), note that $e_i \in \operatorname{cone} D_i$ and that hence

$$e_i d^t \in \operatorname{cone}\{d_1 d_2^t \mid d_1, d_2 \in D_i\} \tag{15}$$

for any $d \in D_i$. From the fact that B^i satisfies (**s**) it follows that $(a_i^t a_i) \cdot D \geq 0$ for all $D \in \operatorname{cone}\{d_1 d_2^t \mid d_1, d_2 \in D_i\}$, and in particular that $(a_i e_i)(a_i d) \geq 0$ for all $d \in D_i$. Thus $a_i d \geq 0$ for all $d \in D_i$. □

So

$$\min\left\{ \sum_{i=1}^n c_i A_i \mid \sum_i A_i (x_i - \sum_{j>i} \alpha_{ij} x_j)^2 \text{ is KZ-reduced for some } \alpha_{ij}, A_n = 1 \right\} \tag{16}$$

equals

$$\min\left\{ \sum_k c_k B_{kk}^k \mid (B^1, \dots, B^n) \text{ satisfies } (\mathbf{r}), (\mathbf{p}), (\mathbf{s}), (\mathbf{n}) \text{ and } B_{nn}^n = 1 \right\}. \tag{17}$$

Here the extra condition at the end is added to remove scale invariance from the problem. Relaxing the rank-1 constraint (**r**) yields a lower bound that is a semi-definite optimization problem:

$$z(c) := \min\left\{ \sum_{k=1}^n c_k B_{kk}^k \mid (B^1, \dots, B^n) \text{ satisfies } (\mathbf{p}), (\mathbf{s}), (\mathbf{n}) \text{ and } B_{nn}^n = 1 \right\}. \tag{18}$$

Note that it is possible to determine the value of (18) without knowing the Novikova sets X_i^* in advance, by using a cutting plane algorithm for the constraints (**n**). That may even be the only practical way to do it for $n > 5$, since the cardinality of X_n^* increases very rapidly with n. The following theorem, similar to Theorem 1, implies that such a cutting plane algorithm will finish.

Theorem 3. *Let $(B^1, \dots, B^n)$ satisfy (**p**), (**s**), and suppose that*

$$\sum_{i=1}^n e_2^t B^i e_2 \geq B_{11}^1;$$

$$\sum_{i=k}^n \tilde{x}^t B^i \tilde{x} \geq B_{kk}^k \text{ for all nonzero } x \in \mathbb{Z}^{n-k+1}, k = 2, \dots, n-1.$$

Then there are only finitely many $x \in \mathbb{Z}^n \setminus \{0\}$ such that $\sum_{i=1}^n x^t B^i x < B_{11}^1$.

Compared to the method of Lasserre, in particular to a second-order moment relaxation of the polynomial optimization problem we have, our relaxation contains variables B^k_{ij} corresponding to products $a_{ki}a_{kj}$ but no variables corresponding to products $a_{ki}a_{lj}$ when $k \neq l$. Accordingly, we do not take products of linear inequalities $a_k d_1 \geq 0, a_l d_2 \geq 0$ into account.

4. Branch and bound

In the definition of KZ-reducedness, the size-reduction requirement (**S**) asks that for $i = 1, \ldots, n-1$ we have

$$(\alpha_{i,i+1}, \ldots, \alpha_{in}) \in D^i := [0, \frac{1}{2}] \times [-\frac{1}{2}, \frac{1}{2}]^{n-i-1}. \tag{19}$$

There is nothing particular about the polyhedra D^i that makes the semidefinite relaxation (18) possible. Taking any set of polyhedra P^i instead of the D^i, an analogous semidefinite lower bound $z(c, P^1, \ldots, P^{n-1})$ for

$$\min \Big\{ \sum c_i A_i \mid \sum_i A_i (x_i - \sum_{j>i} \alpha_{ij} x_j)^2 \text{ satisfies } (\mathbf{N}), \\ (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in P^i \text{ for } i = 1, \ldots, n-1, \text{ and } A_n = 1 \Big\} \tag{20}$$

may be constructed.

If we have a set of lists of polyhedra $N = \{(P^1_s, \ldots, P^{n-1}_s) \mid s = 1, \ldots, t\}$ so that

$$D^1 \times \cdots \times D^{n-1} = \bigcup_{(P^1, \ldots, P^{n-1}) \in N} P^1 \times \cdots \times P^{n-1} \tag{21}$$

then

$$\min\{z(c, P^1, \ldots, P^{n-1}) \mid (P^1, \ldots, P^{n-1}) \in N\} \tag{22}$$

is again a lower bound for (16).

We construct such a decomposition N of $D^1 \times \cdots \times D^{n-1}$ recursively in a branch-and-bound procedure. Initially, $N = \{(D^1, \ldots, D^{n-1})\}$. Then we iterate the following. Suppose the minimum of (22) is attained at $(P^1, \ldots, P^{n-1}) \in N$. Then we choose an $i \in \{1, \ldots, n-1\}$ and replace $(P^1, \ldots, P^{n-1})$ by the lists

$$(P^1, \ldots, P^{i-1}, Q, P^{i+1}, \ldots, P^{n-1}) \text{ and } (P^1, \ldots, P^{i-1}, Q', P^{i+1}, \ldots, P^{n-1}), \tag{23}$$

where Q, Q' are polyhedra such that $P^i = Q \cup Q'$ — so N retains property (21). This process of refining N continues until (22) is sufficiently close to the value of a known KZ-reduced form.

We choose i, Q, Q' with the aim of reducing the 'distance' of the optimal solution to a rank-1 solution, as follows. If the optimal solution of the problem defining $z(c, P^1, \ldots, P^{n-1})$ is $(B^1, \ldots, B^n)$, then we take i, j so that

$$\sum_{k=i}^{n} \frac{1}{B^i_{ii}} (B^i_{ii} B^i_{jk} - B^i_{ij} B^i_{ik}) \tag{24}$$

is maximal. Then we put

$$Q = \{(\alpha_{i,i+1}, \ldots, \alpha_{in}) \in P^i \mid \alpha_{ij} \leq \beta\},\ Q' = \{(\alpha_{i,i+1}, \ldots \alpha_{in}) \in P^i \mid \alpha_{ij} \geq \beta\} \tag{25}$$

where β is (a rational number with modest denominator number near) $\frac{-B^i_{ij}}{B^i_{ii}}$. One can show, by comparing for an element of B^i different bounds that follow from (**s**), that as the lengths of the admitted intervals for the α_{ij} tend to zero, the matrix B^i will converge to $\tilde{B}^i$.

We have tried other branching rules with equally good motives, but this turned out to work best, in the sense that the cardinality of N required to obtain a certain precision was the smallest we could attain. Only hand-crafted branching trees were better. We refer to [12] for further details.

5. Rounding to obtain exact bounds

Every feasible solution y to the dual of (18) gives a lower bound on $z(c)$ and hence on the optimal solution to (16). A dual solution is feasible if and only if a number of matrices, say $M_1(y), \ldots, M_k(y)$, is positive semidefinite. In fact, in our computations we only work with solutions y that are *strictly* positive definite. This simplifies the verification of feasibility, but the crucial advantage is that it helps to counter the imprecision inherent in the computation with limited-precision floating point numbers.

In the dual of (18) such solutions can be obtained by replacing a dual constraint $M_i(y) \succeq 0$ with $M_i(y) \succeq \varepsilon I$, where I is an identity matrix of suitable dimension, and ε is a small positive constant. Bringing this matrix to the other side we get the perturbed constraint

$$M_i(y) - \varepsilon I \succeq 0 \tag{26}$$

which corresponds to a perturbation of the function that is being optimized in the primal problem. Again we refer to [12] for further details.

A floating-point solution y to the perturbed problem can be approximated by a continuous fraction expansion. If this approximation, $\tilde{y}$, is sufficiently close to y, it might violate some of the perturbed dual constraints slightly, but it will be strictly feasible for the original problem. Positive definiteness can then be ascertained by evaluating $\sum_{i=1}^{k} \operatorname{rank}(M_i(\tilde{y}))$ determinants.

Note that this approach can also be applied to find feasible solutions of the primal semidefinite problem, but is quite useless when it comes to deriving an optimal solution of the original problem (16) or (20), i.e. a solution that also satisfies the rank-1 constraints (**r**). This is of no concern when one is interested in lower bounds, but it is also interesting to find KZ-reduced forms that give a good upper bound. We do not have a very reliable automated method to obtain such forms, not even from the optimal solution of our branch and bound procedure, which is nonetheless close to rank 1 in the sense that (24) is small for all i, j.

6. New linear inequalities on the outer coefficients of KZ-reduced forms

Let

$$K_n := \operatorname{cone}\{A(q) \mid q \text{ is an } n\text{-ary KZ-reduced form}\}. \tag{27}$$

Clearly

$$K_n = \{x \in \mathbb{R}^n \mid (0, x) \in K_{n+1}\} \tag{28}$$

and

$$K_n = \{x \in \mathbb{R}^n \mid (x, y) \in K_{n+1} \text{ for some } y \in \mathbb{R}\}. \tag{29}$$

Table 1 gives several KZ-reduced forms. The format is as follows: the columns labeled 'Outer' and 'Inner' hold the vector and matrix

$$\begin{bmatrix} A_1 \\ \vdots \\ A_n \end{bmatrix}, \begin{bmatrix} 1 & -\alpha_{12} & \cdots & -\alpha_{1n} \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -\alpha_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{bmatrix}, \tag{30}$$

respectively.

By the first KZ-inequality, K_2 is contained in

$$K_2' := \{(A_1, A_2) \in \mathbb{R}_+^2 \mid \ A_2 \geq \frac{3}{4} A_1\}. \tag{31}$$

It is clear from Table 1 that K_2 contains

$$K_2'' := \operatorname{cone}\left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 3/4 \end{bmatrix} \right\}. \tag{32}$$

Since $K_2' = K_2''$, we have equality throughout in $K_2' \supseteq K_2 \supseteq K_2''$.

Also, K_3 is contained in

$$K_3' := \{(A_1, A_2, A_3) \in \mathbb{R}_+^3 \mid \ A_2 \geq \frac{3}{4} A_1, \ A_3 \geq \frac{3}{4} A_2, \ A_3 \geq \frac{2}{3} A_1\} \tag{33}$$

by the first and second KZ-inequalities, and K_3 contains

$$K_3'' := \operatorname{cone}\left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 3/4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3/4 \\ 2/3 \end{bmatrix}, \begin{bmatrix} 1 \\ 8/9 \\ 2/3 \end{bmatrix} \right\}. \tag{34}$$

Again we have equality throughout in $K_3' \supseteq K_3 \supseteq K_3''$, as $K_3' = K_3''$.

For $n = 4$ the classical KZ-inequalities no longer suffice to determine K_n. Clearly K_4 is contained in

$$\{(A_1, A_2, A_3, A_4) \in \mathbb{R}_+^4 \mid \ A_{i+1} \geq \frac{3}{4} A_i, \ A_{i+2} \geq \frac{2}{3} A_i\} \tag{35}$$

by the first and second KZ-inequalities. But the extremal vector $(1, \frac{8}{9}, \frac{2}{3}, \frac{16}{27})$ of the latter cone cannot be realized as the sequence of outer coefficients of a KZ-reduced form:

Theorem 4. *Let $A_1, \ldots, A_4$ be the outer coefficients of a KZ-reduced form in four variables. Then*

$$-25A_1 - 36A_2 + 48A_3 + 40A_4 \geq -7 \cdot 10^{-6} A_4. \tag{36}$$

Thus $K_4 \subseteq K_4'$ where

$$K_4' := \{(A_1, A_2, A_3, A_4) \in \mathbb{R}_+^4 \mid \ A_{i+1} \geq \frac{3}{4} A_i, \ A_{i+2} \geq \frac{2}{3} A_i, \ (36)\} \tag{37}$$

We conjecture that in the above theorem we even have

$$-25A_1 - 36A_2 + 48A_3 + 40A_4 \geq 0. \tag{38}$$

Name	Outer	Inner	Form
E1	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$	$\begin{bmatrix}1\end{bmatrix}$
E2	$\begin{bmatrix}1\\3/4\end{bmatrix}$	$\begin{bmatrix}1&-1/2\\0&1\end{bmatrix}$	$\frac{1}{2}\begin{bmatrix}2&1\\1&2\end{bmatrix}$
E3a	$\begin{bmatrix}1\\3/4\\2/3\end{bmatrix}$	$\begin{bmatrix}1&-1/2&1/2\\0&1&-1/3\\0&0&1\end{bmatrix}$	$\frac{1}{2}\begin{bmatrix}2&-1&1\\-1&2&-1\\1&-1&2\end{bmatrix}$
E3b	$\begin{bmatrix}1\\8/9\\2/3\end{bmatrix}$	$\begin{bmatrix}1&-1/3&-1/3\\0&1&-1/2\\0&0&1\end{bmatrix}$	$\frac{1}{3}\begin{bmatrix}3&-1&-1\\-1&3&-1\\-1&-1&3\end{bmatrix}$
E4a	$\begin{bmatrix}1\\3/4\\2/3\\1/2\end{bmatrix}$	$\begin{bmatrix}1&-1/2&1/2&1/2\\0&1&-1/3&-1/3\\0&0&1&-1/2\\0&0&0&1\end{bmatrix}$	$\frac{1}{2}\begin{bmatrix}2&-1&1&1\\-1&2&-1&-1\\1&-1&2&0\\1&-1&0&2\end{bmatrix}$
E4b	$\begin{bmatrix}1\\8/9\\2/3\\5/8\end{bmatrix}$	$\begin{bmatrix}1&-1/3&-1/3&1/3\\0&1&-1/2&1/2\\0&0&1&-1/4\\0&0&0&1\end{bmatrix}$	$\frac{1}{6}\begin{bmatrix}6&-2&-2&2\\-2&6&-2&2\\-2&-2&6&-3\\2&2&-3&6\end{bmatrix}$
E4c	$\begin{bmatrix}1\\15/16\\45/64\\5/8\end{bmatrix}$	$\begin{bmatrix}1&-1/4&-1/4&-1/4\\0&1&-1/2&-1/2\\0&0&1&-1/3\\0&0&0&1\end{bmatrix}$	$\frac{1}{32}\begin{bmatrix}32&-8&-8&-8\\-8&32&-13&-13\\-8&-13&32&2\\-8&-13&2&32\end{bmatrix}$
E5a	$\begin{bmatrix}1\\3/4\\2/3\\1/2\\1/2\end{bmatrix}$	$\begin{bmatrix}1&-1/2&1/2&1/2&1/2\\0&1&-1/3&-1/3&-1/3\\0&0&1&-1/2&1/4\\0&0&0&1&-1/2\\0&0&0&0&1\end{bmatrix}$	$\frac{1}{2}\begin{bmatrix}2&-1&1&1&1\\-1&2&-1&-1&-1\\1&-1&2&0&1\\1&-1&0&2&0\\1&-1&1&0&2\end{bmatrix}$
E5b	$\begin{bmatrix}1\\8/9\\2/3\\5/8\\15/32\end{bmatrix}$	$\begin{bmatrix}1&-1/3&-1/3&-1/3&-1/3\\0&1&-1/2&7/16&-1/2\\0&0&1&-3/8&-1/4\\0&0&0&1&-1/2\\0&0&0&0&1\end{bmatrix}$	$\frac{1}{6}\begin{bmatrix}6&-2&-2&-2&-2\\-2&6&-2&3&-2\\-2&-2&6&-2&1\\-2&3&-2&6&-2\\-2&-2&1&-2&6\end{bmatrix}$
E5c	$\begin{bmatrix}1\\3/4\\2/3\\5/8\\15/32\end{bmatrix}$	$\begin{bmatrix}1&-1/2&1/2&-1/2&-1/2\\0&1&-1/3&1/3&1/3\\0&0&1&-1/4&-1/4\\0&0&0&1&-1/2\\0&0&0&0&1\end{bmatrix}$	$\frac{1}{16}\begin{bmatrix}16&-8&8&-8&-8\\-8&16&-8&8&8\\8&-8&16&-8&-8\\-8&8&-8&16&1\\-8&8&-8&1&16\end{bmatrix}$
E5d	$\begin{bmatrix}1\\3/4\\3/4\\9/16\\1/2\end{bmatrix}$	$\begin{bmatrix}1&-1/2&1/4&-1/4&1/2\\0&1&-1/2&-1/2&0\\0&0&1&-1/2&1/2\\0&0&0&1&-1/3\\0&0&0&0&1\end{bmatrix}$	$\frac{1}{4}\begin{bmatrix}4&-2&1&-1&2\\-2&4&-2&-1&-1\\2&-2&4&-1&2\\-1&-1&-1&4&-2\\2&-1&2&-2&4\end{bmatrix}$

TABLE 1. Some KZ-reduced forms

By Table 1, K_4 contains the cone

$$K_4'' := \text{cone}\left\{\begin{bmatrix}0\\0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\\3/4\end{bmatrix}, \begin{bmatrix}0\\1\\3/4\\2/3\end{bmatrix}, \begin{bmatrix}0\\1\\8/9\\2/3\end{bmatrix}, \begin{bmatrix}1\\3/4\\2/3\\1/2\end{bmatrix}, \begin{bmatrix}1\\8/9\\2/3\\5/8\end{bmatrix}, \begin{bmatrix}1\\15/16\\45/64\\5/8\end{bmatrix}\right\} \tag{39}$$

and we have

$$K_4'' = \{(A_1, A_2, A_3, A_4) \in \mathbb{R}^4_+ \mid \ A_{i+1} \geq \frac{3}{4}A_i, \ A_{i+2} \geq \frac{2}{3}A_i, \ (38)\} \tag{40}$$

Hence K_4 is nearly determined by $K_4'' \supseteq K_4 \supseteq K_4'$, and we suspect $K_4 = K_4''$.

In dimension 5, we could prove the following linear bounds:

Theorem 5. *Let $A_1, \ldots, A_5$ be the outer coefficients of a KZ-reduced form in five variables. Then*

$$-5A_1 + 2A_4 + 8A_5 \geq -3 \cdot 10^{-4} A_5 \tag{41}$$

and

$$-4A_1 - 3A_3 + 4A_4 + 8A_5 \geq -5 \cdot 10^{-5} A_5. \tag{42}$$

Of course, we conjecture

$$-5A_1 + 2A_4 + 8A_5 \geq 0 \tag{43}$$

and

$$-4A_1 - 3A_3 + 4A_4 + 8A_5 \geq 0 \tag{44}$$

As before, these inequalities describe a superset K_5' of K_5, and the forms of Table 1 generate a subset K_5'' of K_5. But there is now a fundamental discrepancy between K_5' and K_5''. Table 2 lists the known and conjectured inequalities for K_5 and with each inequality gives the forms of Table 1 that satisfy these inequalities with equality. Experimentation suggests that both inclusions in $K_5'' \subseteq K_5 \subseteq K_5'$ are strict (even if we replace, in the definition of K_5', the inequalities proven in Theorem 5 by their conjectured counterparts).

It is tempting at this stage to conjecture

$$-8A_1 - 3A_3 + 4A_4 + 16A_5 \geq 0 \tag{45}$$

but this is false, as is witnessed by the form

$$\begin{bmatrix} 134 & -54 & -40 & -54 & 54 \\ -54 & 134 & -40 & 67 & -67 \\ -40 & -40 & 134 & -40 & -27 \\ -54 & 67 & -40 & 134 & -67 \\ 54 & -67 & -27 & -67 & 134 \end{bmatrix}. \tag{46}$$

We could obtain several other extreme forms in 5 variables and more valid inequalities, but we never reached a close approximation of K_5. Therefore we only publish the two inequalities that seemed most relevant to the applications here. We will maintain a list of certified inequalities at our website[1]. The reader is invited to contribute to this list, using the distributed software [12].

Even though we do not have a close approximation of K_5, we do have enough inequalities on the outer coefficients to bound Hermite's constant for $n \leq 8$ very

[1] `http://www.win.tue.nl/kz/`

Inequality	'Tight' forms	Rank
$-3A_1 + 4A_2 \geq 0$	E1, E2, E3a, E3b	4
$-3A_2 + 4A_3 \geq 0$	E1, E2, E4a, E5b	4
$-3A_3 + 4A_4 \geq 0$	E1, E3a, E4b, E4c	4
$-3A_4 + 4A_5 \geq 0$	E2, E3b, E4a, E5b	4
$-2A_1 + 3A_3 \geq 0$	E1, E2, E5a, E5b	4
$-2A_2 + 3A_4 \geq 0$	E1, E4a, E4b, E5a	4
$-2A_3 + 3A_5 \geq 0$	E3a, E3b, E5b	≥ 3
$-25A_1 - 36A_2 + 48A_3 + 40A_4 \geq 0$	E1, E5a, E5b	≥ 3
$-25A_2 - 36A_3 + 48A_4 + 40A_5 \geq 0$	E4a, E4b, E4c	≥ 3
$-5A_1 + 2A_4 + 8A_5 \geq 0$	E5a, E5b, E5c	≥ 3
$-4A_1 - 3A_3 + 4A_4 + 8A_5 \geq 0$	E5a, E5d	≥ 2

TABLE 2. Incidences between some inequalities and elements of K_5

Dimension	1	2	3	4	5	6	7	8
γ_n^n	1	4/3	2	4	8	64/3	64	2^8
Upper bound	1	4/3	2	4	8.00005	21.3336	64.0012	256.008
Relative error	0	0	0	0	$6 \cdot 10^{-6}$	$1 \cdot 10^{-5}$	$2 \cdot 10^{-5}$	$3 \cdot 10^{-5}$

TABLE 3. Relation between Hermite's constant and the approximation found

well. Assuming the conjectured inequalities (38), (43) and (44), the upper bound on γ_n^n that would follow through (5) is exact for $n \leq 8$. Table 3 gives, for $n = 1, \ldots, 8$ the known values of γ_n^n, and the upper bound on γ_n^n that follows from the proven inequalities (36), (41) and (42).

Blichfeldt observed in [1] that a tight upper bound on γ_n would follow for $n = 6, 7, 8$ from the two KZ-inequalities and 'a certain inequality that we would reasonably expect to be true, namely $A_{i+4} \geq \frac{1}{2}A_i$'. But he immediately exhibits a set of forms showing that this inequality is false (the forms E5b and E5c of Table 1 are also counterexamples). Note that the inequalities we conjecture/approximate come near to this key inequality Blichfeldt suggests: for (44) would imply that if $A_4 = \frac{3}{4}A_3$, then $A_5 \geq \frac{1}{2}A_1$, and (43) would imply that if $A_5 \leq (\frac{1}{2} - \epsilon)A_1$, then $A_4 \geq (\frac{1}{2} + 4\epsilon)A_1$.

7. The quality of block KZ-reduced lattice bases

If $L \subseteq \mathbb{R}^n$ is a full-dimensional lattice and $b_1, \ldots, b_n \in L$ are linearly independent vectors such that

$$L = \{x_1 b_1 + \cdots + x_n b_n \mid x_1, \ldots, x_n \in \mathbb{Z}\}, \tag{47}$$

then $b_1, \ldots, b_n$ is a *basis* of L. A basis of a lattice determines a positive definite quadratic form

$$q(x_1, \ldots, x_n) := \|x_1 b_1 + \cdots + x_n b_n\|^2. \tag{48}$$

A lattice basis $b_1, \ldots, b_n$ is said to be *KZ-reduced* if the associated form (48) is KZ-reduced.

Let $b_1^*, \ldots, b_n^*$ be the Gram-Schmidt orthogonalization of $b_1, \ldots, b_n$; that is, let $b_1^*, \ldots, b_n^*$ be pairwise orthogonal vectors so that

$$b_k = b_k^* - \sum_{i=1}^{k-1} \alpha_{ik} b_i^* \text{ for } k = 1, \ldots, n, \tag{49}$$

for some α_{ij}. Then these α_{ij} are exactly the inner coefficients of the associated form (48); and the outer coefficients of (48) satisfy

$$A_k = \|b_k^*\|^2. \tag{50}$$

So the classical KZ-inequalities and Theorems 4 and 5 can be read as inequalities relating the $\|b_i^*\|^2$ of a KZ-reduced lattice basis.

Block KZ-reduced lattice bases were introduced in [10] as a generalization of LLL-reduced lattice bases. We say that a form

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} A_i (x_i - \sum_{j>i} \alpha_{ij} x_j)^2, \tag{51}$$

is *k-block KZ-reduced (k-BKZ-reduced)* if the derived forms

$$q_m^{m+k-1}(x_m, \ldots, x_{m+k-1}) := \sum_{i=k}^{k+m-1} A_i (x_i - \sum_{j=i+1}^{k+m-1} \alpha_{ij} x_j)^2. \tag{52}$$

are KZ-reduced for $m = 1, \ldots, n-k+1$. Then a lattice basis is k-BKZ-reduced if the associated form is.

Let

$$\beta_{k,n} := \max \frac{\|b_1^*\|^2}{\|b_n^*\|^2}, \tag{53}$$

where the maximum ranges over all k-BKZ reduced lattice bases. Many of the useful properties of k-BKZ reduced lattice bases are derived through upper bounds on $\beta_{k,n}$. As k increases towards n, $\beta_{k,n}$ is expected to decrease. Schnorr defines $\alpha_k := \beta_{k,k}$ [10] and he is aware that

$$\beta_{k,1+m(k-1)} \leq \alpha_k^m. \tag{54}$$

In terms of quadratic forms, one has

$$\beta_{k,n} = \max\{\frac{A_1}{A_n} \mid (A_1, \ldots, A_n) = A(q),\ q \text{ a } k\text{-BKZ-reduced form}\}. \tag{55}$$

and

$$\alpha_k = \max\{\frac{A_1}{A_k} \mid (A_1, \ldots, A_k) = A(q),\ q \text{ a KZ-reduced form}\} \tag{56}$$

It is immediate from the first KZ-inequality that $\alpha_2 = \frac{4}{3}$ and from the second KZ-inequality that $\alpha_3 = \frac{3}{2}$. A nonnegative combination of the inequalities (41) and $-\frac{3}{4}A_4 + A_5 \geq 0$ (the first KZ-inequality) is

$$-15A_1 + 32A_5 \geq -9 \cdot 10^{-4} A_5, \tag{57}$$

which implies

$$\alpha_5 \leq \frac{32}{15} + 6 \cdot 10^{-5}. \tag{58}$$

Since there exist KZ-reduced forms with $A_1/A_5 = 32/15$, we also have $\alpha_5 \geq \frac{32}{15}$. For $k = 4, 5$, the bounds on $\beta_{k,n}$ that follow from (54) are only slightly weaker than those that follow directly from Theorems 4 and 5 by linear programming.

The limit

$$\tilde{\beta}_k := \lim_{n\to\infty} \beta_{k,n}^{\frac{1}{n-1}} \tag{59}$$

also gives an indication of the relative effectiveness of k-BKZ-reduction. Observe that if an inequality $c_1 A_i + \cdots + c_k A_{i+k-1} \geq 0$ with $c_1 < 0$ holds for the outer coefficients of a KZ-reduced form in k variables, then $\tilde{\beta}_k$ is bounded from above by the largest root of the polynomial $c_1 x^{k-1} + \cdots + c_k$. Thus the first KZ-inequality implies $\tilde{\beta}_2 \leq 4/3 \approx 1.3333$, the second KZ-inequality implies $\tilde{\beta}_3 \leq \sqrt{3/2} \approx 1.2247$, Theorem 4 implies $\tilde{\beta}_4 \leq 1.2172$, and Theorem 5 (in particular (41)) implies $\tilde{\beta}_5 \leq 1.2010$.

8. Acknowledgements

We thank Monique Laurent for pointing out the reference [9]. Parts of this research appeared previously in [11].

References

[1] H. F. Blichfeldt, *The minimum values of positive quadratic forms in six, seven and eight variables*, Math. Z., 39 (1935), pp. 1–15.
[2] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives quaternaires*, Math. Ann., 5 (1872), pp. 581–583.
[3] ———, *Sur les formes quadratiques*, Math. Ann., 6 (1873), pp. 366–389.
[4] ———, *Sur les formes quadratiques positives*, Math. Ann., 11 (1877), pp. 242–292.
[5] J. B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim., 11 (2000/01), pp. 796–817 (electronic).
[6] J. Martinet, *Perfect lattices in Euclidean spaces*, vol. 327 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Berlin, 2003.
[7] N. V. Novikova, *Domains of Korkin-Zolotarev reduction of positive quadratic forms in $n \leq 8$ variables and reduction algorithms for these domains*, Dokl. Akad. Nauk SSSR, 270 (1983), pp. 48–51.
[8] P. A. Parrilo, *Semidefinite programming relaxations for semialgebraic problems*, Math. Program., 96 (2003), pp. 293–320. Algebraic and geometric methods in discrete optimization.
[9] V. Powers and B. Reznick, *A new bound for Pólya's theorem with applications to polynomials positive on polyhedra*, J. Pure Appl. Algebra, 164 (2001), pp. 221–229. Effective methods in algebraic geometry (Bath, 2000).
[10] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoret. Comput. Sci., 53 (1987), pp. 201–224.
[11] S. H. M. van Zwam, *Properties of lattices, a semidefinite programming approach*, master's thesis, Eindhoven University of Technology, 2005.
[12] ———, *New Korkin–Zolotarev inequalities: Implementation and numerical data*, SPOR Report 2006-05, Eindhoven University of Technology, 2006. available from `http://www.win.tue.nl/bs/spor/`.