New Korkin-Zolotarev inequalities

Citation for published version (APA):
Pendavingh, R. A., & Zwam, van, S. H. M. (2007). New Korkin-Zolotarev inequalities. *SIAM Journal on Optimization*, *18*(1), 364-378. https://doi.org/10.1137/060658795

DOI:
10.1137/060658795

Document status and date:
Published: 01/01/2007

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

SIAM J. OPTIM.
Vol. 18, No. 1, pp. 364–378

NEW KORKIN–ZOLOTAREV INEQUALITIES*

R. A. PENDAVINGH† AND S. H. M. VAN ZWAM†

Abstract. Korkin and Zolotarev showed that if

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

is the Lagrange expansion of a Korkin–Zolotarev (KZ-) 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 KZ-reduced quadratic forms using a semidefinite relaxation combined with a branch and bound process. We use a rounding technique to derive exact results from the numerical data. Applying these methods, we prove several new linear inequalities on the A_i of any KZ-reduced form, one of them being $A_{i+4} \geq (\frac{15}{32} - 2 \cdot 10^{-5}) A_i$. We also give a form with $A_5 = \frac{15}{32} A_1$. These new inequalities are then used to study the cone of outer coefficients of KZ-reduced forms, to find bounds on Hermite's constant, and to give better estimates on the quality of k-block KZ-reduced lattice bases.

Key words. lattice, quadratic form, semidefinite programming, Korkin–Zolotarev reduction, Hermite's constant, sphere packing

AMS subject classifications. 11H55, 52C17, 90C22, 11H50

DOI. 10.1137/060658795

1. Preliminaries and overview.

The *Geometry of Numbers* is a field of mathematics initiated and named by Minkowski. The main objects studied are *lattices*, discrete subgroups of $\mathbb{R}^n$. Good introductions to the subject are the book by Cassels [2] and the excellent survey paper by Ryškov and Baranovskiĭ [13]. Typical problems are the search for a shortest vector within a given lattice and the search for a lattice with a dense *sphere packing*. Hermite's constant γ_n is a measure for the density of the densest lattice sphere packing in dimension n. This constant has been determined exactly for $n \leq 8$ and $n = 24$. Since Blichfeldt [1] determined γ_n for $n = 6, 7, 8$, no further low-dimensional cases have been computed. For example, the best known bounds for $n = 9$ are $512 \leq \gamma_9^9 < 913$, where the lower bound is the density of a specific lattice (see, for example, [4]), and the upper bound is the Cohn–Elkies bound [3].

Most of the early research in this subject was not in terms of lattices but in terms of quadratic forms. This approach proved very useful for our research, so in all but the last section we will talk exclusively about positive definite quadratic forms.

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

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} A_i \Big(x_i - \sum_{j>i} \alpha_{ij} x_j \Big)^2. \tag{1.1}$$

This is the *Lagrange expansion* of q; the numbers A_i are the *outer coefficients* and

*Received by the editors May 3, 2006; accepted for publication (in revised form) December 6, 2006; published electronically May 1, 2007. Parts of this research appeared previously in [16].
http://www.siam.org/journals/siopt/18-1/65879.html

†Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands (rudi@win.tue.nl, svzwam@win.tue.nl).

the α_{ij} the *inner coefficients.* We write

$$q_k(x_k,\dots,x_n) := \sum_{i=k}^{n} A_i\Big(x_i - \sum_{j>i}\alpha_{ij}x_j\Big)^2. \tag{1.2}$$

A positive definite quadratic form q in n variables with Lagrange expansion (1.1) is *Korkin–Zolotarev (KZ-)*[1] *reduced* if

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

and

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

We say that two forms q, q' are *equivalent* if there is a unimodular matrix U, i.e., $U \in GL_n(\mathbb{Z})$, such that $q'(x) = q(Ux)$. It can be shown that any form is equivalent to a KZ-reduced form (see, for example, [13]).

Korkin and Zolotarev proved that the outer coefficients of a KZ-reduced form satisfy $A_2 \ge \frac{3}{4}A_1$ (the *first KZ-inequality*) and $A_3 \ge \frac{2}{3}A_1$ (the *second KZ-inequality*) [7]. If q is KZ-reduced, then so is the quadratic form q_k for $k \ge 1$, and hence the inequalities

$$A_{k+1} \ge \frac{3}{4}A_k \text{ and } A_{k+2} \ge \frac{2}{3}A_k,\ k=1,2,\dots, \tag{1.3}$$

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

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

$$\gamma_n := \max\left\{\frac{m(q)}{\det(q)^{\frac{1}{n}}} \mid q \text{ is an } n\text{-ary positive definite quadratic form}\right\}, \tag{1.4}$$

where $m(q) := \min\{q(x) \mid x \in \mathbb{Z}^n, x \ne 0\}$ is the *minimum* of the form q and $\det(q) := \det(Q)$, where Q is the symmetric matrix such that $q(x) = x^tQx$. Equivalent forms have the same minimum and the same determinant, so we may as well restrict the feasible set of (1.4) to KZ-reduced forms. Also, if $A_1,\dots,A_n$ are the outer coefficients of a form q, then $\det(q) = \prod_i A_i$, and if q is KZ-reduced, then $m(q) = f(1,0,\dots,0) = A_1$. Hence

$$\gamma_n^n = \max\left\{\frac{A_1^n}{\prod_i A_i} \mid (A_1,\dots,A_n) = A(q) \text{ for some KZ-reduced form } q\right\}, \tag{1.5}$$

where $A(q) := (A_1,\dots,A_n)$ denotes the sequence of outer coefficients of the quadratic form q. Using (1.3), this implies the bound

$$\gamma_n^n \le \max\left\{\frac{A_1^n}{\prod_{i=1}^n A_i} \mid A_{i+1} \ge \frac{3}{4}A_i, A_{i+2} \ge \frac{2}{3}A_i, A_1 = 1\right\}, \tag{1.6}$$

[1] In the literature one encounters several different ways of writing the names of Korkin and Zolotarev. We decided to follow some of the more recent publications (notably [5]) and have kept the original spelling in the references to facilitate the search for these papers.

which is tight for $n = 2, 3, 4$, as was shown in [6, 7]. In the right-hand side of (1.6) we have removed the scale invariance by requiring $A_1 = 1$. The right-hand side is equal to the inverse of

$$\min \left\{ \prod_{i=1}^{n} A_i \mid A_{i+1} \geq \frac{3}{4} A_i, A_{i+2} \geq \frac{2}{3} A_i, A_1 = 1 \right\}, \tag{1.7}$$

which is the minimum of a concave function on a polyhedron. It is a basic fact of convex optimization that this minimum is attained at one of the vertices. Enumerating all vertices now suffices to determine the bound.

The proof of the first KZ-inequality is elementary. The proof of the second KZ-inequality also uses elementary techniques but is already quite involved. To prove an upper bound on γ_5, Korkin and Zolotarev developed other techniques [8]: they characterized the local optima of the objective function of (1.4), which enabled them to enumerate all local optima for $n = 5$. This line of investigation has been continued and is still actively pursued [10].

In this paper, we return to the first approach and focus on the feasible set of (1.5). 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 polynomial optimization techniques. We apply our method in particular to forms in five variables and obtain inequalities (Theorems 6.1 and 6.2) that imply, through (1.5), 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 [11] 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 on the lower bound that results from simply computing the semidefinite relaxation by performing a *branch and bound* procedure, which is familiar from integer programming. By splitting the semialgebraic set over which we are optimizing we obtain a number of problems on smaller sets. The relaxation for each of these smaller problems is stronger than the original relaxation and will yield a higher lower bound. Then the smallest of these lower bounds is again a lower bound for the original problem. The branch and bound procedure 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 only elementary rational arithmetic. The rounding method is described in section 5.

In section 6 we derive, using these tools, several new linear inequalities on the outer coefficients of KZ-reduced forms. We study the relation between these inequalities and the cone of outer coefficients of KZ-reduced forms. The most striking result is that only three of these new inequalities suffice to give very good bounds on Hermite's constant up to dimension 8.

Finally, in section 7 we show how our new inequalities on the outer coefficients lead to better quality estimates for the block KZ-reduction algorithm.

The implementation and verification of our numerical method is worked out in detail in [17].

2. A finite characterization of KZ-reduced forms.

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

$$A_1 \leq q(x) \text{ for all nonzero } x \in \mathbb{Z}^n. \tag{2.1}$$

In [11], Novikova stated the following.

THEOREM 2.1. *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* (1.1) *is KZ-reduced if and only if q_2 is KZ-reduced,* (**S**) *holds, and*

$$A_1 \leq q(x) \textit{ for all } x \in X_n. \tag{2.2}$$

The proof boils down to the fact that if q_2 is KZ-reduced, $q(0,1,0,\dots,0) \geq A_1$, and (**S**) holds, 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 [11], Novikova gives finite sets X_n for $n \leq 8$ and claims irredundancy of these sets for $n \leq 5$. It is unfortunate that the proofs were omitted from her paper, as 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 sufficient sets that are slightly larger, and for larger n the sets we compute are much smaller [16]. We have proven necessity for all vectors up to dimension 4 and all of Novikova's vectors in dimension 5.

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 $\bar{X} := \{(x, 0) \mid x \in X\}$. One has

$$X_2^* = \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}, \tag{2.3}$$

$$X_3^* \setminus \bar{X}_2^* = \left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}. \tag{2.4}$$

Moreover, $X_4^* \setminus \bar{X}_3^*$ is a set of 12 vectors, and according to Novikova $X_5^* \setminus \bar{X}_4^*$ is a set of 52 vectors [11].

Using Theorem 2.1 we find that in the definition of KZ-reducedness, the requirement (**M**) is equivalent to

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

Thus $(A_1, \dots, A_n, \alpha_{12}, \dots, \alpha_{n-1,n})$ 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**). The number of inequalities of the second kind seems to grow much faster than that of the first kind as n increases.

It is possible to characterize the KZ-reduced forms using only linear and quadratic inequalities by using a different parametrization of the set of quadratic forms. Let Q

be a positive definite $n \times n$ matrix and let $q(x) := x^t Q x$. Then the Lagrange expansion (1.1) yields a decomposition

$$Q = \sum_{i=1}^{n} a_i^t a_i = C^t C, \tag{2.5}$$

where

$$a_i = \sqrt{A_i}(0, \ldots, 0, 1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}) \tag{2.6}$$

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

Thus C is upper triangular, and $Q = C^t C$ is the Cholesky decomposition of Q.

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

$$\left\{ \sqrt{A_i}(0, \ldots, 0, 1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}) \mid A_i \geq 0, (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in S^i \right\} \tag{2.7}$$

is a polyhedral cone, so there is a finite set of column vectors, which we call D_i, such that (2.7) equals

$$\{a \in \mathbb{R}^n \mid ad \geq 0 \text{ for all } d \in D_i\}. \tag{2.8}$$

For $x \in \mathbb{Z}^m$, $m \leq n$, we write $\widetilde{x} := (0, \ldots, 0, x_1, \ldots, x_m) \in \mathbb{Z}^n$. Now $q(x) = x^t Q x$ 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

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

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 [9, 12]. We describe a semidefinite formulation that has the virtue of yielding a reasonable lower bound while using only a moderate number of variables and constraints.

THEOREM 3.1. *Let Q be an $n \times n$ positive definite matrix and let $q(x) = x^t Q x$. 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*

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

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

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

$$\sum_{i=k}^{n} \widetilde{x}^t B^i \widetilde{x} \geq B_{kk}^k \text{ for all } x \in X_{n-k+1}^*, \text{ for } k = 1, \ldots, n-1. \tag{n}$$

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

$$a_i = \sqrt{A_i}(0, \ldots, 0, 1, -\alpha_{i,i+1}, \ldots, -\alpha_{in}). \tag{3.1}$$

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

$$B^i = a_i^t a_i = A_i \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & 1 & -\alpha_{i,i+1} & \cdots & -\alpha_{in} \\ \mathbf{0} & -\alpha_{i,i+1} & \alpha_{i,i+1}\alpha_{i,i+1} & \cdots & \alpha_{i,i+1}\alpha_{in} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & -\alpha_{in} & \alpha_{in}\alpha_{i,i+1} & \cdots & \alpha_{in}\alpha_{in} \end{bmatrix}. \tag{3.2}$$

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

For sufficiency, let $B^1, \dots, B^n$ be such that $Q = B^1 + \cdots + B^n$ and such that (**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 satisfies (**N'**). To see that a_i satisfies (**S'**), let e_i be the ith unit vector in $\mathbb{R}^n$. Note that $e_i \in \operatorname{cone} D_i$ and that hence

$$e_i d^t \in \operatorname{cone}\{d_1 d_2^t \mid d_1, d_2 \in D_i\} \tag{3.3}$$

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, for $(c_1, \dots, c_n) \in \mathbb{R}^n$, the minimum

$$\min\left\{ \sum_{i=1}^n c_i A_i \mid \sum_i A_i (x_i - \sum_{j>i} \alpha_{ij} x_j)^2 \text{ is KZ-reduced for some } \alpha_{ij}, A_n = 1 \right\} \tag{3.4}$$

equals

$$\min\left\{ \sum_k c_k B_{kk}^k \mid (B^1, \dots, B^n) \text{ satisfies } (\mathbf{r}), (\mathbf{p}), (\mathbf{s}), (\mathbf{n}), \text{ and } B_{nn}^n = 1 \right\}. \tag{3.5}$$

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

$$z(c) := \min\left\{ \sum_{k=1}^n c_k B_{kk}^k \mid (B^1, \dots, B^n) \text{ satisfies } (\mathbf{p}), (\mathbf{s}), (\mathbf{n}), \text{ and } B_{nn}^n = 1 \right\}. \tag{3.6}$$

Note that it is possible to determine the value of (3.6) without knowing the Novikova sets X_i^* in advance, by using a cutting plane algorithm as follows. Replace in (3.6) the constraints (**n**) by the following for certain small sets X_i (for example, take $X_2 = X_2^*$ and the other X_i empty):

$$\sum_{i=k}^n \widetilde{x}^t B^i \widetilde{x} \geq B_{kk}^k \text{ for all } x \in X_{n-k+1}, \text{ for } k = 1, \dots, n-1. \tag{\mathbf{n'}}$$

Repeatedly refine these constraints by solving the relaxation and finding, for some k, a nonzero vector $x \in \mathbb{Z}^{n-k+1}$ with $\sum_{i=k}^n \widetilde{x}^t B^i \widetilde{x} < B_{kk}^k$ for the optimal solution to the relaxation. Add this x to X^{n-k+1}. Eventually no such x will be found, and then the optimal solution to this relaxation will be equal to the optimal solution to (3.6).

One can use the techniques in the proof of Theorem 2.1 to bound the search space for these vectors.

A cutting plane algorithm may even be the only practical way to solve the relaxation for $n > 5$, since the cardinality of X_n^* seems to increase very rapidly with n. The following theorem, similar to Theorem 2.1, implies that such a cutting plane algorithm will finish.

THEOREM 3.2. *Let $(B^1, \ldots, B^n)$ satisfy* $(\mathbf{p})$, $(\mathbf{s})$, *and suppose that*

$$\sum_{i=1}^{n} e_2^t B^i e_2 \geq B_{11}^1, \tag{3.7}$$

$$\sum_{i=k}^{n} \widetilde{x}^t B^i \widetilde{x} \geq B_{kk}^k \text{ for all nonzero } x \in \mathbb{Z}^{n-k+1}, k = 2, \ldots, n-1. \tag{3.8}$$

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 [9], in particular to a second-order moment relaxation of our polynomial optimization problem, our relaxation contains variables B_{ij}^k 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 this section we give an overview of the branching process. We refer to [17] for further details and a full implementation. In the definition of KZ-reducedness, the size-reduction requirement $(\mathbf{S})$ asks that for $i = 1, \ldots, n-1$ we have

$$(\alpha_{i,i+1}, \ldots, \alpha_{in}) \in S^i := \left[0, \frac{1}{2}\right] \times \left[-\frac{1}{2}, \frac{1}{2}\right]^{n-i-1}. \tag{4.1}$$

There is nothing particular about the polyhedra S^i that makes the semidefinite relaxation (3.6) possible. Taking any set of polyhedra P^i instead of the S^i, a semidefinite lower bound $z(c, P^1, \ldots, P^{n-1})$ analogous to (3.6) for

$$\min \left\{ \sum c_i A_i \mid \sum_i A_i (x_i - \sum_{j>i} \alpha_{ij} x_j)^2 \text{ satisfies } (\mathbf{N}), \right.$$
$$\left. (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in P^i \text{ for } i = 1, \ldots, n-1, \text{ and } A_n = 1 \right\} \tag{4.2}$$

may be constructed. This new relaxation differs from (3.6) in the constraints $(\mathbf{s})$. If the diameter of these polyhedra P^i is small, then the matrix B^i is close to a rank-1 matrix in the following sense. Suppose the width of P^i is small, i.e., for all j,

$$\max\{\alpha_{ij} \mid (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in P^i\} - \min\{\alpha_{ij} \mid (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in P^i\} < \varepsilon, \tag{4.3}$$

where we assume $\varepsilon < 1$ and $\max\{\alpha_{ij} \mid (\alpha_{i,i+1}, \ldots, \alpha_{in}) \in P^i\} \leq 1/2$. Let $(B^1, \ldots, B^n)$ be any feasible solution corresponding to $z(c, P^1, \ldots, P^{n-1})$. Let $(\widetilde{B}^1, \ldots, \widetilde{B}^n)$ be any feasible solution corresponding to $z(c, P^1, \ldots, P^{n-1})$ such that $\widetilde{B}^i$ has rank 1. Then for all $j, k \in \{i, \ldots, n\}$,

$$|B_{jk}^i / B_{ii}^i - \widetilde{B}_{jk}^i / \widetilde{B}_{ii}^i| \leq 2\varepsilon. \tag{4.4}$$

If we have a set of $(n-1)$-tuples of polyhedra $N = \{(P_s^1, \dots, P_s^{n-1}) \mid s = 1, \dots, t\}$ so that

$$S^1 \times \cdots \times S^{n-1} = \bigcup_{(P^1,\dots,P^{n-1})\in N} P^1 \times \cdots \times P^{n-1}, \tag{4.5}$$

then

$$\min\{z(c, P^1, \dots, P^{n-1}) \mid (P^1, \dots, P^{n-1}) \in N\} \tag{4.6}$$

is again a lower bound for (3.4). If we partition $S^1 \times \cdots \times S^{n-1}$ so that in each part the diameter of each of the P^i is small, then we would obtain a good lower bound. However, this would make the cardinality of N very large, even for moderately small ε. Therefore, we take an iterative approach. Initially we choose $N = \{(S^1, \dots, S^{n-1})\}$. Then we repeat the following. Suppose that the minimum of (4.6) is attained at $(P^1, \dots, P^{n-1}) \in N$. Then we choose an $i \in \{1, \dots, n-1\}$ and replace $(P^1, \dots, P^{n-1})$ in N by the two tuples

$$(P^1, \dots, P^{i-1}, Q, P^{i+1}, \dots, P^{n-1}) \text{ and } (P^1, \dots, P^{i-1}, Q', P^{i+1}, \dots, P^{n-1}), \tag{4.7}$$

where Q, Q' are polyhedra such that $P^i = Q \cup Q'$—so N retains property (4.5). This process of refining N continues until (4.6) is sufficiently close to the desired value or some other stopping criterion applies.

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

$$\sum_{k=i}^{n} \frac{1}{B_{ii}^i}(B_{ii}^i B_{jk}^i - B_{ij}^i B_{ik}^i) \tag{4.8}$$

is maximal. Then we put

$$\begin{aligned} Q &= \{(\alpha_{i,i+1}, \dots, \alpha_{in}) \in P^i \mid \alpha_{ij} \le \beta\}, \\ Q' &= \{(\alpha_{i,i+1}, \dots, \alpha_{in}) \in P^i \mid \alpha_{ij} \ge \beta\}, \end{aligned} \tag{4.9}$$

where β is (a rational number with modest denominator near) $-B_{ij}^i / B_{ii}^i$.

We have tried other methods for picking i, Q, Q', but this turned out to work best in practice, in the sense that the cardinality of N required to obtain a certain bound was the smallest we could attain. Only by constructing N by hand did we achieve a smaller set for one problem.

5. Rounding to obtain exact bounds. Every feasible solution y to the dual of (3.6) gives a lower bound on $z(c)$ and hence on the optimal solution to (3.4). A dual solution is feasible if and only if a number of matrices, say, $M_1(y), \dots, M_k(y)$, is positive semidefinite. In fact, in our computations we work only 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 (3.6) 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

$$M_i(y) - \varepsilon I \succeq 0, \tag{5.1}$$

which corresponds to a perturbation of the function that is being optimized in the primal problem. Again we refer the reader to [17] for further details.

A floating-point solution y to the perturbed problem can be approximated by a continued fraction expansion, a technique recently used in [15]. If this approximation $\widetilde{y}$ 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 $\sum_{i=1}^{k} \operatorname{rank}(M_i(\widetilde{y}))$ 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 (3.4) or (4.2), that is, a solution that also satisfies the rank-1 constraints ($\mathbf{r}$). 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 (4.8) is small for all i, j.

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

$$K_n := \operatorname{cone}\{A(q) \mid q \text{ is an } n\text{-ary KZ-reduced form}\}. \tag{6.1}$$

We have

$$K_n = \{x \in \mathbb{R}^n \mid (0, x) \in K_{n+1}\} \tag{6.2}$$

and

$$K_n = \{x \in \mathbb{R}^n \mid (x, y) \in K_{n+1} \text{ for some } y \in \mathbb{R}\}. \tag{6.3}$$

Table 6.1 gives several KZ-reduced forms, some of which come from [13], whereas others were found by manually rounding and tweaking primal solutions to (4.2) for suitably chosen c and polyhedra P^i. The format is as follows: the columns labeled “Outer” and “Inner” hold the vector and matrix

$$\begin{bmatrix} A_1 \\ \vdots \\ A_n \end{bmatrix}, \begin{bmatrix} 1 & -\alpha_{12} & \cdots & -\alpha_{1n} \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -\alpha_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{bmatrix}, \tag{6.4}$$

respectively.

By the first KZ-inequality, K_2 is contained in

$$K_2' := \left\{(A_1, A_2) \in \mathbb{R}_+^2 \mid \; A_2 \geq \frac{3}{4} A_1\right\}. \tag{6.5}$$

It follows from Table 6.1 that K_2 contains

Table 6.1
Some KZ-reduced forms.

Name	Outer	Inner	Form
E1	$[1]$	$[1]$	$[1]$
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	$\begin{bmatrix}1\\3/4\\3/4\\9/16\\1/2\end{bmatrix}$	$\begin{bmatrix}1 & -1/2 & 1/4 & -1/4 & 1/2\\0 & 1 & -1/2 & -1/2 & 0\\0 & 0 & 1 & -1/2 & 1/2\\0 & 0 & 0 & 1 & -1/3\\0 & 0 & 0 & 0 & 1\end{bmatrix}$	$\frac{1}{4}\begin{bmatrix}4 & -2 & 1 & -1 & 2\\-2 & 4 & -2 & -1 & -1\\2 & -2 & 4 & -1 & 2\\-1 & -1 & -1 & 4 & -2\\2 & -1 & 2 & -2 & 4\end{bmatrix}$

$$K_2'' := \text{cone}\left\{ \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\3/4\end{bmatrix} \right\}. \tag{6.6}$$

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

Also, K_3 is contained in

$$K_3' := \left\{ (A_1, A_2, A_3) \in \mathbb{R}_+^3 \mid A_2 \geq \frac{3}{4}A_1,\ A_3 \geq \frac{3}{4}A_2,\ A_3 \geq \frac{2}{3}A_1 \right\} \tag{6.7}$$

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

$$K_3'' := \operatorname{cone}\left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 3/4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3/4 \\ 2/3 \end{bmatrix}, \begin{bmatrix} 1 \\ 8/9 \\ 2/3 \end{bmatrix} \right\}. \tag{6.8}$$

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. By the first and second KZ-inequalities, K_4 is contained in

$$\left\{ (A_1, A_2, A_3, A_4) \in \mathbb{R}^4_+ \mid A_{i+1} \geq \frac{3}{4} A_i,\ A_{i+2} \geq \frac{2}{3} A_i \right\}. \tag{6.9}$$

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

THEOREM 6.1. *Let $A_1, \dots, A_4$ be the outer coefficients of a KZ-reduced form in four variables. Then*

$$-25A_1 - 36A_2 + 48A_3 + 40A_4 \geq -7 \cdot 10^{-6} A_4. \tag{6.10}$$

This theorem was proven by the branch-and-bound and rounding processes described in the previous sections. The data required to verify this theorem can be found in [17].

Thus $K_4 \subseteq K_4'$, where

$$K_4' := \left\{ (A_1, A_2, A_3, A_4) \in \mathbb{R}^4_+ \mid\ A_{i+1} \geq \frac{3}{4} A_i,\ A_{i+2} \geq \frac{2}{3} A_i,\ (6.10) \right\}. \tag{6.11}$$

We conjecture that in the above theorem we even have

$$-25A_1 - 36A_2 + 48A_3 + 40A_4 \geq 0. \tag{6.12}$$

By Table 6.1, K_4 contains the cone

$$K_4'' := \operatorname{cone}\left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 3/4 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 3/4 \\ 2/3 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 8/9 \\ 2/3 \end{bmatrix}, \begin{bmatrix} 1 \\ 3/4 \\ 2/3 \\ 1/2 \end{bmatrix}, \begin{bmatrix} 1 \\ 8/9 \\ 2/3 \\ 5/8 \end{bmatrix}, \begin{bmatrix} 1 \\ 15/16 \\ 45/64 \\ 5/8 \end{bmatrix} \right\}, \tag{6.13}$$

and we have

$$K_4'' = \left\{ (A_1, A_2, A_3, A_4) \in \mathbb{R}^4_+ \mid\ A_{i+1} \geq \frac{3}{4} A_i,\ A_{i+2} \geq \frac{2}{3} A_i,\ (6.12) \right\}. \tag{6.14}$$

Hence K_4 is nearly determined by $K_4'' \supseteq K_4 \supseteq K_4'$, and our conjecture would imply $K_4 = K_4''$.

In dimension 5, we prove the following linear bounds.

THEOREM 6.2. *Let $A_1, \dots, A_5$ be the outer coefficients of a KZ-reduced form in five variables. Then*

$$-5A_1 + 2A_4 + 8A_5 \geq -3 \cdot 10^{-4} A_5 \tag{6.15}$$

and

$$-4A_1 - 3A_3 + 4A_4 + 8A_5 \geq -5 \cdot 10^{-5} A_5. \tag{6.16}$$

Table 6.2

Incidences between some inequalities and elements of K_5. The rightmost column gives the dimension of the face of K_5 defined by the inequality.

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

Of course, we conjecture

$$-5A_1 + 2A_4 + 8A_5 \geq 0 \tag{6.17}$$

and

$$-4A_1 - 3A_3 + 4A_4 + 8A_5 \geq 0. \tag{6.18}$$

As before, these inequalities describe a superset K_5' of K_5, and the forms of Table 6.1 generate a subset K_5'' of K_5. But there is now a fundamental discrepancy between K_5' and K_5''. Table 6.2 lists the known and conjectured inequalities for K_5 and with each inequality gives the forms of Table 6.1 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 6.2 by their conjectured counterparts).

As an example, the four forms E5a, E5b, E5c, and E5d satisfy the following inequality:

$$-8A_1 - 3A_3 + 4A_4 + 16A_5 \geq 0. \tag{6.19}$$

One could conjecture that this is a facet of K_5. This is false, however; it is violated by the KZ-reduced form

$$\begin{bmatrix} 134 & -54 & -40 & -54 & 54 \\ -54 & 134 & -40 & 67 & -67 \\ -40 & -40 & 134 & -40 & -27 \\ -54 & 67 & -40 & 134 & -67 \\ 54 & -67 & -27 & -67 & 134 \end{bmatrix}. \tag{6.20}$$

We could obtain several other extreme forms in five variables and more valid inequalities, but we never reached a close approximation of K_5. Therefore, we publish only the two inequalities that seemed most relevant to the applications here. We maintain a list of certified inequalities at our website,[2] where our software [17] can also be found.

[2] http://www.win.tue.nl/kz/

Table 6.3

Relation between Hermite's constant and the approximation found. The first row gives the exact value of γ_n^n for $n \leq 8$, and the best known lower bound for $n = 9$. The second row gives the upper bound found using our approximation of K_n.

Dimension	1	2	3	4	5	6	7	8	9
(Lower bound on) γ_n^n	1	4/3	2	4	8	64/3	64	256	512
Upper bound	1	4/3	2	4	8.00005	21.3336	64.0012	256.008	1024.11

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 well. Assuming the conjectured inequalities (6.12), (6.17), and (6.18), the upper bound on γ_n^n that would follow from the corresponding strengthening of (1.6) is exact for $n \leq 8$. Table 6.3 gives for $n = 1, \dots, 8$ the known values of γ_n^n, and the upper bound on γ_n^n that follows from the proven inequalities (6.10), (6.15), and (6.16). In dimension 9 there is suddenly a huge gap between our upper bound and the best known lower bound. This gap is also larger than the gap obtained by the Cohn–Elkies bound. One or more new inequalities are needed to close this gap.

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 6.1 are also counterexamples). Note that the inequalities we conjecture/approximate come near to this key inequality Blichfeldt suggests: (6.18) would imply that if $A_4 = \frac{3}{4}A_3$, then $A_5 \geq \frac{1}{2}A_1$, and (6.17) 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 $b_1, \dots, b_n \in L$ are linearly independent vectors such that

$$L = \{x_1 b_1 + \cdots + x_n b_n \mid x_1, \dots, x_n \in \mathbb{Z}\}, \tag{7.1}$$

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

$$q(x_1, \dots, x_n) := \|x_1 b_1 + \cdots + x_n b_n\|^2. \tag{7.2}$$

A lattice basis $b_1, \dots, b_n$ is said to be *KZ-reduced* if the associated form (7.2) is KZ-reduced.

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

$$b_k = b_k^* - \sum_{i=1}^{k-1} \alpha_{ik} b_i^* \text{ for } k = 1, \dots, n, \tag{7.3}$$

for some α_{ij}. Then these α_{ij} are exactly the inner coefficients of the associated form (7.2); and the outer coefficients of (7.2) satisfy

$$A_k = \|b_k^*\|^2. \tag{7.4}$$

So the classical KZ-inequalities and Theorems 6.1 and 6.2 can be read as inequalities relating the $\|b_i^*\|^2$ of a KZ-reduced lattice basis.

Block KZ-reduced lattice bases were introduced in [14] as a generalization of Lenstra–Lenstra–Lovasz (LLL-) reduced lattice bases. Such a basis gives a better estimate of the length of the shortest lattice vector and can still be computed in polynomial time when k is fixed. We say that a form

$$q(x_1,\ldots,x_n)=\sum_{i=1}^{n}A_i\Big(x_i-\sum_{j>i}\alpha_{ij}x_j\Big)^2, \tag{7.5}$$

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

$$q_m^{m+k-1}(x_m,\ldots,x_{m+k-1}):=\sum_{i=k}^{k+m-1}A_i\Bigg(x_i-\sum_{j=i+1}^{k+m-1}\alpha_{ij}x_j\Bigg)^2 \tag{7.6}$$

are KZ-reduced for $m=1,\ldots,n-k+1$. Then a lattice basis is k-BKZ-reduced if the associated form is. In the remainder of this paper we will give some improved bounds on constants used in [14] for the analysis of the quality of k-BKZ-reduced lattice bases.

Let

$$\beta_{k,n}:=\max\frac{\|b_1^*\|^2}{\|b_n^*\|^2}, \tag{7.7}$$

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 toward n, $\beta_{k,n}$ is expected to decrease. Schnorr [14] defines $\alpha_k:=\beta_{k,k}$ and shows that

$$\beta_{k,1+m(k-1)}\le\alpha_k^m. \tag{7.8}$$

In terms of quadratic forms, one has

$$\beta_{k,n}=\max\left\{\frac{A_1}{A_n}\mid(A_1,\ldots,A_n)=A(q),\ q\text{ a }k\text{-BKZ-reduced form}\right\} \tag{7.9}$$

and

$$\alpha_k=\max\left\{\frac{A_1}{A_k}\mid(A_1,\ldots,A_k)=A(q),\ q\text{ a KZ-reduced form}\right\}. \tag{7.10}$$

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 (6.15) and $-\frac{3}{4}A_4+A_5\ge0$ (the first KZ-inequality) is

$$-15A_1+32A_5\ge-9\cdot10^{-4}A_5, \tag{7.11}$$

which implies

$$\alpha_5\le\frac{32}{15}+6\cdot10^{-5}. \tag{7.12}$$

Since there exist KZ-reduced forms with $A_1/A_5=32/15$, we also have $\alpha_5\ge\frac{32}{15}$. For $k=4,5$, the bounds on $\beta_{k,n}$ that follow from (7.8) are only slightly weaker than those that follow directly from Theorems 6.1 and 6.2 by linear programming.

The limit

$$\widetilde{\beta}_k := \lim_{n\to\infty} \beta_{k,n}^{\frac{1}{n-1}} \tag{7.13}$$

also gives an indication of the relative effectiveness of k-BKZ-reduction. Observe that if an inequality $c_1A_i + \cdots + c_kA_{i+k-1} \geq 0$ with $c_1 < 0$ holds for the outer coefficients of a KZ-reduced form in k variables, then $\widetilde{\beta}_k$ is bounded from above by the largest root of the polynomial $c_1x^{k-1} + \cdots + c_k$. Thus the first KZ-inequality implies $\widetilde{\beta}_2 \leq 4/3 \approx 1.3333$, the second KZ-inequality implies $\widetilde{\beta}_3 \leq \sqrt{3/2} \approx 1.2247$, Theorem 6.1 implies $\widetilde{\beta}_4 \leq 1.2172$, and Theorem 6.2 (in particular (6.15)) implies $\widetilde{\beta}_5 \leq 1.2010$.

Acknowledgments. We thank Achill Schürmann and two anonymous referees for their comments, which improved the paper considerably.

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] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Classics in Mathematics, Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[3] H. Cohn and N. Elkies, *New upper bounds on sphere packings* I, Ann. of Math. (2), 157 (2003), pp. 689–714.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, 3rd ed., Grundlehren Math. Wiss. 290, Springer-Verlag, New York, 1999.

[5] B. N. Delone, *The St. Petersburg School of Number Theory*, Hist. Math. 26, AMS, Providence, RI, 2005.

[6] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives quaternaires*, Math. Ann., 5 (1872), pp. 581–583.

[7] A. Korkine and G. Zolotareff, *Sur les formes quadratiques*, Math. Ann., 6 (1873), pp. 366–389.

[8] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann., 11 (1877), pp. 242–292.

[9] J. B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim., 11 (2001), pp. 796–817.

[10] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren Math. Wiss. 327, Springer-Verlag, Berlin, 2003.

[11] 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 (in Russian). English translation in Soviet Math. Doklady, 27 (1983), pp. 557–560.

[12] P. A. Parrilo, *Semidefinite programming relaxations for semialgebraic problems*, Math. Program., 96 (2003), pp. 293–320.

[13] S. S. Ryškov and E. P. Baranovskiĭ, *Classical methods of the theory of lattice packings*, Uspekhi Mat. Nauk, 34 (1979), pp. 3–63, 256 (in Russian). English translation in Russian Math. Surveys, 34 (1979), pp. 1–68.

[14] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoret. Comput. Sci., 53 (1987), pp. 201–224.

[15] A. Schürmann and F. Vallentin, *Computational approaches to lattice packing and covering problems*, Discrete Comput. Geom., 35 (2006), pp. 73–116.

[16] S. H. M. van Zwam, *Properties of Lattices, a Semidefinite Programming Approach*, Master's thesis, Eindhoven University of Technology, Eindhoven, The Netherlands, 2005.

[17] S. H. M. van Zwam, *New Korkin–Zolotarev Inequalities: Implementation and Numerical Data*, SPOR report 2006-05, Eindhoven University of Technology, Eindhoven, The Netherlands, 2006. Available online at http://www.win.tue.nl/bs/spor/.