Block Korkin–Zolotarev Bases and Successive Minima

C.P.Schnorr

Universitt Frankfurt

Fachbereich Mathematik/Informatik

February 5, 1996

Abstract

Let $b_1, \ldots, b_m \in \mathbb{R}^n$ be an arbitrary basis of lattice L that is a block Korkin–Zolotarev basis with block size β and let $\lambda_i(L)$ denote the successive minima of lattice L. We prove that for $i = 1, \ldots, m$

$$\frac{4}{i+3}\, \gamma_\beta^{-2\frac{i-1}{\beta-1}} \;\leq\; \|b_i\|^2/\lambda_i(L)^2 \;\leq\; \gamma_\beta^{2\frac{m-i}{\beta-1}}\, \frac{i+3}{4}$$

where γ_β is the Hermite constant. For $\beta = 3$ we establish the optimal upper bound

$$\|b_1\|^2/\lambda_1(L)^2 \;\leq\; \left(\frac{3}{2}\right)^{\frac{m-1}{2}-1}$$

and we present block Korkin–Zolotarev lattice bases for which this bound is tight.

We improve the Nearest Plane Algorithm of Babai (1986) using block Korkin–Zolotarev bases. Given a block Korkin–Zolotarev basis $b_1, \ldots, b_m$ with block size β and $x \in L(b_1, \ldots, b_m)$ a lattice point v can be found in time $\beta^{O(\beta)}$ satisfying $\|x - v\|^2 \leq m\, \gamma_\beta^{\frac{2m}{\beta-1}}\, \min_{u \in L} \|x - u\|^2$.

1 Introduction

The problem of selecting from all bases for a lattice a canonical basis consisting of short vectors is called *reduction theory*. Classical reduction theory was developed in the language of quadratic forms by Lagrange (1773), Hermite (1850) and Korkin and Zolotarev (1873) in order to determine the minima of positive definite integral quadratic forms. Recently there has been renewed interest in reduction theory stimulated by a new method in integer programming (H.W. LENSTRA, JR. 1983) and by Lovász' lattice basis reduction algorithm, see A.K. LENSTRA, H.W. LENSTRA JR. and L. LOVÁSZ (1982), which has had various applications.

From the computational point of view the reduction theory introduced by HERMITE and by KORKIN and ZOLOTAREV is the most natural one. On the other hand Korkin–Zolotarev reduced lattice bases are not easy to find for lattices of higher dimensions, see KANNAN (1987) and SCHNORR (1987) for algorithms. This led SCHNORR (1987) to introduce a hierarchy of block Korkin–Zolotarev bases comprising for block size 2 the L^3–reduced bases introduced by LENSTRA, LENSTRA, LOVÁSZ (1982). Block Korkin–Zolotarev bases with maximal block size are just Korkin–Zolotarev bases.

In this paper we prove new upper and lower bounds for the ratio $\|b_i\|^2/\lambda_i^2$ where $b_1, \ldots, b_m$ is any block Korkin–Zolotarev basis and λ_i is the i–th successive minimum of the lattice. These bounds extend the known bounds for L^3–reduced bases and for Korkin–Zolotarev bases.

We state in Section 2, Theorems 3 and 4 the new lower and upper bounds for the ration $\|b_i\|^2/\lambda_i^2$. We prove these bounds in Section 3. In Section 4 we apply block Korkin–Zolotarev bases to the problem of finding approximate nearest lattice points. In Section 5 we prove that the upper bound $\|b_1\|^2 \leq \left(\frac{3}{2}\right)^{\frac{m-1}{2}-1} \lambda_1^2$ is optimal for block Korkin–Zolotarev bases of block size 3. We present block Korkin–Zolotarev bases for which this bound is tight.

2 Reduced Bases and Successive Minima

Let $\mathbb{R}^n$ be the n–dimensional real vector space with the Euclidean inner product $<,>$ and the Euclidean norm, called the length, $\|y\| = \langle y, y\rangle^{1/2}$. A *lattice* $L \subset \mathbb{R}^n$ is a discrete, additive subgroup of the $\mathbb{R}^m$. Its *rank* is the dimension of the minimal subspace $\mathrm{span}(L)$ that contains L. Each lattice L of rank m has a *basis*, i.e. a sequence $b_1, \ldots, b_m$ of linearly independent vectors that generate L as an abelian group,

$$L = \{t_1 b_1 + \ldots + t_m b_m \mid t_1, \ldots, t_m \in \mathbb{Z}\}.$$

Let $L(b_1, \ldots, b_m)$ denote the lattice with basis $b_1, \ldots, b_m$. Its *determinant* $d(L)$ is defined as

$$d(L) = \det[\langle b_i, b_j\rangle]^{1/2}_{1\leq i,j\leq m}.$$

This does not depend on the choice of the basis. The i–th *successive minimum* $\lambda_i(L)$ of a lattice L (with respect to the Euclidean norm) is the smallest real number r such that there are i linearly independent vectors in L of length at most r.

With an ordered lattice basis $b_1, \ldots, b_m \in \mathbb{R}^n$ we associate the *Gram–Schmidt orthogonalization* $\widehat{b}_1, \ldots, \widehat{b}_m \in \mathbb{R}^n$ which can be computed together with the Gram–Schmidt coefficients $\mu_{i,j} = \langle b_i, \widehat{b}_j \rangle \,/\, \langle \widehat{b}_j, \widehat{b}_j \rangle$ by the recursion

$$\widehat{b}_1 = b_1,\ \widehat{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \widehat{b}_j \quad for \quad i = 2, \ldots, m.$$

We have $\mu_{i,i} = 1$ and $\mu_{i,j} = 0$ for $i < j$. From the above equations we have the Gram–Schmidt decomposition

$$[b_1, \ldots, b_m] = [\widehat{b}_1, \ldots, \widehat{b}_m]\ [\mu_{i,j}]^{\top}_{1 \le i,j \le m},$$

where $[b_1, \ldots, b_m]$ denotes the matrix with column vectors $b_1, \ldots, b_m$.

With an ordered lattice basis $b_1, \ldots, b_m$ of the lattice L we associate the orthogonal projections

$$\pi_i : \mathrm{span}(b_1, \ldots, b_m) \ \mapsto\ \mathrm{span}(b_1, \ldots, b_{i-1})^{\perp} \quad i = 1, \ldots, m\ ,$$

where $\mathrm{span}(b_1, \ldots, b_m)$ denotes the linear space generated by the vectors $b_1, \ldots, b_m$. We let L_i denote the lattice

$$L_i = \pi_i(L)\ .$$

The lattice L_i has rank $m - i + 1$ and basis $\pi_i(b_i),\ \pi_i(b_{i+1}), \ldots, \pi_i(b_m)$. We have $\pi_i(b_i) = \widehat{b}_i$ and $\pi_i(b_j) = \sum_{k=i}^{m} \mu_{j,k} \widehat{b}_k$.

An ordered basis $b_1, \ldots, b_m$ of the lattice $L \subset \mathbb{R}^n$ is a *Korkin–Zolotarev basis* if it satisfies the conditions

$$|\mu_{i,j}| \ \le\ 1/2 \qquad \text{for} \quad 1 \le j < i \le m, \tag{1}$$

$$\|\widehat{b}_i\| \ =\ \lambda_1(L_i) \quad \text{for} \quad i = 1, \ldots, m. \tag{2}$$

This definition is equivalent to the one given, in the language of quadratic forms, by Hermite in his second letter to Jacobi (1845) and by Korkin and Zolotarev (1873).

Let $b_1, \ldots, b_m$ be an ordered basis of the lattice $L \subset \mathbb{R}^n$. We call the basis $b_1, \ldots, b_m$ an β–BKZ basis, i.e. a *block Korkin–Zolotarev basis* with block size β, if it satisfies (1) and

$$\pi_i(b_i), \pi_i(b_{i+1}), \ldots, \pi_i(b_{i+\beta-1}) \text{ are Korkin–Zolotarev bases for } i = 1, \ldots, m - \beta + 1. \tag{3}$$

The condition (3) means that for $i = 1, \ldots, m-1$ the vector $\widehat{b}_i = \pi_i(b_i)$ is a shortest non–zero vector in the lattice $\pi_i(L(b_1, \ldots, b_{\min(i+\beta-1,m)})) = L(\pi_i(b_i), \ldots, \pi_i(b_{\min(i+\beta-1,m)}))$. If (1) holds and if $\beta = 2$ the condition (3) is equivalent to

$$\|\widehat{b}_i\|^2 \leq \|\pi_i(b_{i+1})\|^2 = \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2 \|\widehat{b}_i\|^2 \quad \text{for} \quad i = 1, \ldots, m-1. \quad (4)$$

We see that a basis $b_1, \ldots, b_m$ is 2 - BKZ iff it satisfies (1) and (4). These bases have been introduced by A.K. Lenstra, H.W. Lenstra, Jr. and Lovász (1982). We call a basis $b_1, \ldots, b_m$ *L^3-reduced* with $\delta \in (\frac{1}{4}, 1]$ if it satisfies (1) and

$$\delta \|\widehat{b}_i\|^2 \leq \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2 \|\widehat{b}_i\|^2 \quad \text{for} \quad i = 1, \ldots, m-1. \quad (5)$$

Lenstra et alii (1983) have in particular considered $\delta = 3/4$. From their work we have the following

Theorem 1 *Every basis $b_1, \ldots, b_m$ of lattice L that is L^3–reduced with $\delta \in (\frac{1}{4}, 1]$ satisfies with $\alpha = 1/(\delta - \frac{1}{4})$:*

$$\alpha^{1-i} \leq \|\widehat{b}_i\|^2 \lambda_i(L)^{-2} \leq \|b_i\|^2 \lambda_i(L)^{-2} \leq \alpha^{m-1} \quad \textit{for} \quad i = 1, \ldots, m.$$

In the limit case $\delta = 1$ we have $\alpha = 4/3$, and thus every 2 - BKZ basis $b_1, \ldots, b_m$ of lattice L satisfies for $i = 1, \ldots, m$

$$\left(\frac{3}{4}\right)^{i-1} \leq \|\widehat{b}_i\|^2 \lambda_i(L)^{-2} \leq \|b_i\|^2 \lambda_i(L)^{-2} \leq \left(\frac{4}{3}\right)^{m-1}. \quad (6)$$

A β–BKZ basis $b_1, \ldots, b_m$ with maximal block size $\beta = m$ is a Korkin–Zolotarev basis. For these bases we have the following bounds on $\|b_i\|^2 \lambda_i^{-2}$, where the upper bound is essentially due to Mahler (1938) and the lower bound is from Lagarias, H.W. Lenstra, Jr., Schnorr (1990).

Theorem 2 *Every Korkin–Zolotarev basis $b_1, \ldots, b_m$ of lattice L satisfies $\frac{4}{i+3} \leq \|b_i\|^2 \lambda_i(L)^{-2} \leq \frac{i+3}{4}$ for $i = 1, \ldots, m$.*

We are going to extend Theorems 1 and 2 to arbitrary β–BKZ bases. For this we use the Hermite constants γ_m which is defined as

$$\gamma_m = \sup\{\lambda_1(L)^2 d(L)^{-2/m} : \text{for lattices } L \text{ of rank } m\}.$$

Its value is known for $m \leq 8$, see CASSELS (1971), Appendix. We have $\gamma_2^2 = \frac{4}{3}$, $\gamma_3^3 = 2$, $\gamma_4^4 = 4$, $\gamma_5^5 = 8$, $\gamma_6^6 = 2^6/3$, $\gamma_7^7 = 2^6$, $\gamma_8^8 = 2^8$. It is known that $\gamma_m \leq \frac{2}{3}m$ for $m \geq 2$ and

$$\frac{m}{2\pi e} + O(m) \leq \gamma_m \leq \frac{0.872m}{\pi e}(1 + o(1)) \quad \text{as} \quad m \to \infty,$$

where the upper bound is due to KABATYANSKII and LEVENSHTEIN (1978) and the lower bound follows from the Minkowski–Hlawka theorem, see CASSELS (1971), VI. 2.2. Theorems 3 and 4 below will be proved in Section 2.

Theorem 3 *Every β-BKZ basis $b_1, \ldots, b_m$ of lattice L satisfies*

$$\|\widehat{b}_i\|^2 \lambda_i(L)^{-2} \leq \gamma_\beta^{2\frac{m-i}{\beta-1}} \qquad \textit{for } i = 1, \ldots, m$$

$$\|b_i\|^2 \lambda_i(L)^{-2} \leq \gamma_\beta^{2\frac{m-1}{\beta-1}} \; \frac{i+3}{4} \qquad \textit{for } i = 1, \ldots, m.$$

Theorem 3 improves and extends the inequality $\|b_1\|^2 \leq (6\beta^2)^{\frac{m}{\beta}} \lambda_1(L)^2$ of SCHNORR (1987). In particular we have for $\beta = 2$, $\gamma_2^2 = \frac{4}{3}$ that

$$\|\widehat{b}_i\|^2 \lambda_i(L)^{-2} \leq \left(\frac{4}{3}\right)^{m-i} \qquad \text{for } i = 1, \ldots, m$$

$$\|b_i\|^2 \lambda_i(L)^{-2} \leq \left(\frac{4}{3}\right)^{m-1} \frac{i+3}{4} \qquad \text{for } i = 1, \ldots, m$$

which is almost the upper bound of (6). It is remarkable that if the block size β is a fixed fraction of the rank, i.e. if m/β is fixed, then the upper bounds of Theorem 3 are polynomial in β.

We next consider lower bounds for $\|b_i\|^2 \lambda_i(L)^{-2}$, i.e. upper bounds for $\lambda_i(L)^2 \|b_i\|^{-2}$.

Theorem 4 *Every β-BKZ basis $b_1, \ldots, b_m$ of lattice L satisfies*

$$\lambda_i(L)^2 \|b_i\|^{-2} \leq \gamma_\beta^{2\frac{i-1}{\beta-1}} \; \frac{i+3}{4} \qquad \textit{for} \quad i = 1, \ldots, m.$$

For $i \leq \beta$ the bounds of Theorems 3 and 4 can be replaced by the stronger bounds of Theorem 2.

If the block size β is a fixed fraction of the rank m the upper bounds in Theorem 4 are polynomial in β. For block size $\beta = 2$, $\gamma_\beta^2 = \frac{4}{3}$ Theorem 4 yields

$$\left(\frac{4}{3}\right)^{i-1} \frac{i+3}{4} \leq \|\widehat{b}_i\|^2 \lambda_i(L)^2 \qquad \text{for} \quad i = 1, \ldots, m$$

which is almost the lower bound from (6).

The values $\gamma_\beta^{\frac{2}{\beta-1}}$, appearing in Theorems 3 and 4, are known for $\beta = 2,\ldots,8$:

β	2	3	4	5	6	7	8
$\gamma_\beta^{\frac{2}{\beta-1}}$	$\frac{4}{3}$	$2^{1/3}$	$2^{1/3}$	$2^{\frac{3}{10}}$	$2^{\frac{2}{5}}\,3^{-\frac{1}{15}}$	$2^{2/7}$	$2^{1/4}$
$\approx$	1.333	1.260	1.260	1.231	1.226	1.219	1.189

It is interesting to find the minimal constants $c_{\beta,m}$ for which

$$\|b_1\|^2\ \lambda_1(L)^{-2}\ \le\ c_{\beta,m}$$

holds for all β–BKZ bases $b_1,\ldots,b_m$ of rank m. Bachem and Kannan (1984) show that $c_{2,m} = \left(\frac{4}{3}\right)^{m-1}$. We prove in Section 5 that $c_{3,m} = \sqrt{\frac{3}{2}}^{m-3}$ holds for odd m. Thus the upper bounds from Theorem 3 are not optimal for $\beta \ge 3$. For $\beta = 3$ we can replace $\gamma_\beta^{\frac{2}{\beta-1}} = 2^{1/3}$ by $\sqrt{3/2} \approx 1.225$ which is even smaller than the value $\gamma_6^{\frac{2}{5}}$ for 6–BKZ bases.

3 Proofs for Theorems 3 and 4.

Proposition 5 *For every β–BKZ basis $b_1,\ldots,b_m$ with $m \ge \beta$ we have for $M = \max(\|\widehat{b}_{m-\beta+2}\|,\ldots,\|\widehat{b}_m\|)$ that $\|b_1\| \le \gamma_\beta^{\frac{m-1}{\beta-1}} M$.*

Proof. We extend the basis $b_1,\ldots,b_m$ by $\beta-2$ additional vectors to

$$b_{-\beta+3},\ldots,b_{-1},b_0,b_1,\ldots,b_m \tag{7}$$

such that

1. $\|b_i\| = \|b_1\|$ for $i \le 0$
2. $\langle b_i, b_j\rangle = 0$ for $i \le 0$, $i \ne j$ and for $j = -\beta+3,\ldots,m$.

The basis 7 is a β–BKZ basis of rank at least $2(\beta-1)$. By definition of the Hermite constant γ_β we have

$$\|\widehat{b}_i\|^\beta \le \gamma_\beta^{\beta/2}\|\widehat{b}_i\|\|\widehat{b}_{i+1}\|\cdots\|\widehat{b}_{i+\beta-1}\| \quad \text{for} \quad i = -\beta+3,\ldots,m-\beta+1.$$

Multiplication of these $m-1$ inequalities yields

$$\|\widehat{b}_{-\beta+3}\|^\beta\|\widehat{b}_{-\beta+4}\|^\beta\cdots\|\widehat{b}_{m-\beta+1}\|^\beta \le$$

$$\gamma_\beta^{\beta(m-1)/2} \|\widehat{b}_{-\beta+3}\|^1 \|\widehat{b}_{-\beta+4}\|^2 \cdots \|\widehat{b}_1\|^{\beta-1} \|\widehat{b}_2\|^\beta \cdots \|\widehat{b}_{m-\beta+1}\|^\beta$$

$$\|\widehat{b}_{m-\beta+2}\|^{\beta-1} \cdots \|\widehat{b}_{m-1}\|^2 \|\widehat{b}_m\|^1.$$

This implies

$$\|\widehat{b}_{-\beta+3}\|^{\beta-1} \|\widehat{b}_{-\beta+4}\|^{\beta-2} \cdots \|\widehat{b}_0\|^2 \; \|\widehat{b}_1\|^1 \leq$$

$$\gamma_\beta^{\beta(m-1)/2} \|\widehat{b}_{m-\beta+2}\|^{\beta-1} \cdots \|\widehat{b}_{m-1}\|^2 \|\widehat{b}_m\|^1.$$

Hence

$$\|b_1\|^{\binom{\beta}{2}} \leq \gamma_\beta^{\beta(m-1)/2} M^{\binom{\beta}{2}} \quad \text{and thus} \quad \|b_1\| \leq \gamma_\beta^{\frac{m-1}{\beta-1}} M. \qquad \square$$

Corollary 6 *Every β-BKZ basis $b_1, \ldots, b_m$ of the lattice L satisfies*

$$\|b_1\|^2 \leq \gamma_\beta^{2\frac{m-1}{\beta-1}} \; \frac{i+3}{4} \; \lambda_1(L)^2 \; .$$

Proof. If $m \leq \beta$ we have $\|b_1\| = \lambda_1(L)$ and the claim holds. Now let $m > \beta$ and let v be a shortest non–zero lattice vector. W.l.o.g. we can assume that $v \notin L(b_1, \ldots, b_{m-1})$ for otherwise we can reduce m and the claim holds by induction on m. If $v \notin L(b_1, \ldots, b_{m-1})$ we have

$$\lambda_1(L) = \|v\| \geq \lambda_1(L_i) = \|\widehat{b}_i\| \quad \text{for} \quad i = m - \beta + 1, \ldots, m.$$

This shows that $\lambda_1(L) \geq \max(\|\widehat{b}_{m-\beta+2}\|, \ldots, \|\widehat{b}_m\|)$ and thus the claim follows from Proposition 5. $\square$

Proof of Theorem 3. Application of Corollary 6 to the lattice $L_i = \pi_i(L)$ yields the inequalities

$$\|\widehat{b}_i\|^2 \leq \gamma_\beta^{2\frac{m-i}{\beta-1}} \lambda_1(L_i)^2 \quad \text{for} \quad i = 1, \ldots, m. \tag{8}$$

Moreover we have $\lambda_1(L_i) \leq \lambda_i(L)$. This is because there are i linearly independent vectors of length at most $\lambda_i(L)$ in L and at least one of these vectors v satisfies $\pi_i(v) \neq 0$. Hence $\lambda_1(L_i) \leq \|\pi_i(v)\| \leq \lambda_i(L)$. Using the Inequalities 8 and $\mu_{i,j}^2 \leq 1/4$ we obtain for $i = 1, \ldots, m$

$$\begin{aligned}
\|b_i\|^2 &= \|\widehat{b}_i\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \; \|\widehat{b}_j\|^2 \\
&\leq \gamma_\beta^{2\,\frac{m-i}{\beta-1}} \; \lambda_i(L)^2 + \frac{1}{4} \sum_{j=1}^{i-1} \gamma_\beta^{2\,\frac{m-j}{\beta-1}} \; \lambda_j(L)^2 \\
&\leq \gamma_\beta^{\frac{2m}{\beta-1}} \left(\gamma_\beta^{2\,\frac{-i}{\beta-1}} + \frac{1}{4} \sum_{j=1}^{i-1} \gamma_\beta^{2\,\frac{-j}{\beta-1}} \right) \lambda_i(L)^2 \\
&\leq \gamma_\beta^{2\frac{m-1}{\beta-1}} \; \frac{i+3}{4} \; \lambda_i(L)^2 \; .
\end{aligned}$$

This proves the second inequalities of Theorem 3. The first inequalities in Theorem 3 follows from 8 and $\lambda_1(L_i) \leq \lambda_i(L)$. □

Proof of Theorem 4. By definition of $\lambda_i = \lambda_i(L)$ we have

$$\lambda_i^2 \leq \max\{\|b_j\|^2 \text{ for } j = 1, \ldots, i\} \; .$$

It follows from $\|b_j\|^2 \leq \|\widehat{b}_j\|^2 + \sum_{k=1}^{j-1} \mu_{j,k}^2 \|\widehat{b}_k\|^2$ that

$$\lambda_i^2 \leq \frac{i+3}{4} \max\{\|\widehat{b}_j\|^2 \text{ for } j = 1, \ldots, i\} \; . \tag{9}$$

Proposition 5 applied to the β–BKZ basis $\pi_j(b_j), \ldots, \pi_j(b_i)$ yields the inequalities

$$\|\widehat{b}_j\| \leq \gamma_\beta^{\frac{i-j}{\beta-1}} \max\{\|\widehat{b}_{i-\beta+2}\|, \ldots, \|\widehat{b}_i\|\} \quad \text{for} \quad 1 \leq j \leq i - \beta + 1 \tag{10}$$

For $i - \beta + 2 \leq j \leq i$ we have that

$$\|\widehat{b}_j\| \leq \|\pi_j(b_i)\| \leq \|b_i\| \; .$$

From this and 10 we see that

$$\|\widehat{b}_j\| \leq \gamma_\beta^{\frac{i-j}{\beta-1}} \; \|b_i\| \qquad \text{for} \qquad 1 \leq j \leq i \; .$$

These inequalities and 9 prove Theorem 4:

$$\lambda_i^2 \leq \frac{i+3}{4} \; \gamma_\beta^{2\frac{i-1}{\beta-1}} \; \|b_i\|^2 \qquad \text{for} \quad i = 1, \ldots, m \; .$$ □

4 Approximate nearest lattice points

Babai (1986) shows how Lovász lattice reduction can be used to find a point of a given lattice L, nearest within a factor $2^{m/2}$ to a given point in $\mathrm{span}(L)$. Babai poses the question whether the factor $2^{m/2}$ can be improved using block Korkin–Zolotarev bases. We answer this question in the affirmative.

We let α_β denote the maximum of $\|b_1\|^2/\|\hat{b}_\beta\|^2$ over all Korkin–Zolotarev bases $b_1, \ldots, b_\beta$. The inequality $\alpha_\beta \le \beta^{1+\ln\beta}$ has been shown in Schnorr (1987).

Theorem 7 *Let* $b_1, \ldots, b_m \in \mathbb{Z}^n$ *be a* β*–BKZ basis of lattice* L *and* $x = \sum_{i=1}^m x_i b_i$ *an arbitrary point in* $\mathrm{span}(b_1, \ldots, b_m)$*. Then the lattice point* $v = \sum_{j=1}^m v_j b_j$*, where* $v_j = \lceil x_j - \sum_{i=j+1}^m v_i \mu_{i,j} \rfloor$*, satisfies*

$$\|x - v\|^2 \le C_{m,\beta} \min_{u \in L} \|x - u\|^2 \ , \ \text{where } C_{m,\beta} = m\ \gamma_\beta^{2\frac{m-1}{\beta-1}}\ \alpha_{\beta-1}\ .$$

Proof The definition of v implies that

$$\|x - v\|^2 \ \le\ (\|\hat{b}_1\|^2 + \cdots + \|\hat{b}_m\|^2)/4\ .$$

From Proposition 5 we have the inequality

$$\|\hat{b}_i\|^2 \ \le\ \gamma_\beta^{2\frac{m-i}{\beta-1}}\ \max(\|\hat{b}_{m-\beta+2}\|^2, \ldots, \|\hat{b}_m\|^2) \text{ for } 1 \le i \le m - \beta + 1\ .$$

This yields

$$\begin{aligned}
\|x - v\|^2 &\le \frac{1}{4} \sum_{j=1}^m \gamma_\beta^{2\frac{j-1}{\beta-1}}\ \max(\|\hat{b}_{m-\beta+2}\|^2, \ldots, \|\hat{b}_m\|^2) \\
&\le \frac{1}{4} \sum_{j=1}^m \gamma_\beta^{2\frac{j-1}{\beta-1}}\ \alpha_{\beta-1}\ \|\hat{b}_m\|^2 \\
&\le \frac{m}{4}\ \gamma_\beta^{2\frac{m-1}{\beta-1}}\ \alpha_{\beta-1}\ \|\hat{b}_m\|^2\ . \qquad (11)
\end{aligned}$$

Let $u \in L$ be the lattice point that is nearest to x. Following Babai we consider two cases.

CASE a: $u - v \in L(b_1, \ldots, b_{m-1})$. Then $u - v$ is a nearest lattice point to

$x'-v$ in $L(b_1,\ldots,b_{m-1})$ where $x'\in \mathrm{span}(b_1,\ldots,b_{m-1})$ is the orthogonal projection of x. Consequently we have by induction on m

$$\begin{aligned}\|x-v\|^2 &= \|x-x'\|^2+\|x'-v\|^2\\ &\le (1+C_{m-1,\beta})\ \|x-u\|^2\\ &\le C_{m,\beta}\ \|x-u\|^2\end{aligned}$$

CASE b: $u-v\notin L(b_1,\ldots,b_{m-1})$. In this case we have

$$\|x-u\|^2\ge \|\hat{b}_m\|^2/4.$$

Hence we have from 11 that

$$\begin{aligned}\|x-v\|^2 &\le \frac{m}{4}\ \gamma_\beta^{2\frac{m-1}{\beta-1}}\ \alpha_{\beta-1}\ 4\ \|x-u\|^2\\ &\le C_{m,\beta}\ \|x-u\|^2\ .\end{aligned}$$

□

We finally reduce with a different construction for v the constant $C_{m,\beta}$ of Theorem 7 to $m\,\gamma_\beta^{2\frac{m-1}{\beta-1}}$. The improved constant $m\,\gamma_\beta^{2\frac{m-1}{\beta-1}}$ is polynomial in β if β is a fixed fraction of m.

Theorem 8 *Let* $b_1,\ldots,b_m\in \mathbb{Z}^n$ *be a* β*-BKZ basis and* $x=\sum_{i=1}^m x_ib_i$. *Suppose that* $\|\widehat{b}_k\|=\max(\|\widehat{b}_{m-\beta+1}\|,\ldots,\|\widehat{b}_m\|)$, $m-k+1\le k\le m$. *Let* $v=\sum_{i=1}^m v_ib_i$ *be a lattice point such that* $\sum_{j=k}^m |x_j-\sum_{i=j}^m v_i\mu_{i,j}|^2\ \|\hat{b}_i\|^2$ *is minimal for all* $v_k,\ldots,v_m\in\mathbb{Z}$ *and* $|x_j-\sum_{i=j}^m v_i\mu_{i,j}|\le\frac12$ *for* $j=k-1,\ldots,1$. *Then we have* $\|x-v\|^2\le m\,\gamma_\beta^{2\frac{m-1}{\beta-1}}\ \min_{u\in L}\ \|x-u\|^2$.

Proof Let $u\in L$ be the lattice point that is nearest to x.

CASE a: $u-v\in L(b_1,\ldots,b_{m-1})$. Then $u-v$ is a nearest lattice point to $x'-v$ in $L(b_1,\ldots,b_{m-1})$ where $x'\in\mathrm{span}(b_1,\ldots,b_{m-1})$ is the orthogonal projection of x, $x'=x-\pi_{m-1}(x)$. Induction on m yields

$$\begin{aligned}\|x-v\|^2 &= \|x-x'\|^2+\|x'-v\|^2\\ &\le (1+(m-1)\gamma_\beta^{2\,\frac{m-2}{\beta-1}})\ \|x-u\|^2\\ &\le m\ \gamma_\beta^{2\frac{m-1}{\beta-1}}\ \|x-u\|^2\ .\end{aligned}$$

CASE b: $u-v\notin L(b_1,\ldots,b_{m-1})$. It follows from the choice of v and k that

$$\|x-u\|^2\ge\frac14\ \lambda_1(L_k)^2\ge\frac14\ \max(\ \|\hat{b}_{m-\beta+2}\|^2,\ldots,\|\hat{b}_m\|^2)\ .$$

As in the proof of Theorem 7 we have

$$\begin{aligned} \|x-v\|^2 &\le (\,\|\hat{b}_1\|^2 + \cdots + \|\hat{b}_m\|^2\,)\,/\,4 \\ &\le \frac{1}{4}\sum_{j=1}^{m} \gamma_\beta^{2\frac{j-1}{\beta-1}} \ \max(\|\hat{b}_{m-\beta+2}\|^2, \ldots, \|\hat{b}_m\|^2)\ . \end{aligned}$$

Consequently

$$\begin{aligned} \|x-v\|^2 &\le \sum_{j=1}^{m} \gamma_\beta^{2\frac{j-1}{\beta-1}} \ \|x-u\|^2 \\ &\le m\, \gamma_\beta^{2\frac{m-1}{\beta-1}} \ \|x-u\|^2\ . \qquad \square \end{aligned}$$

Computational bounds. Computing a lattice vector $v = \sum_{i=1}^{m} v_i b_i$ as in Theorem 7 can be done using the NEAREST VECTOR ALGORITHM of KANNAN (1987). Given a β–BKZ basis $b_1, \ldots, b_m$ this algorithm enumerates $\beta^{O(\beta)}$ many lattice vectors close to x and finds integers $v_{m-\beta+1}, \ldots, v_m$ that minimize $\sum_{j=m-\beta+1}^{m} |x_j - \sum_{i=j}^{m} v_i \mu_{i,j}|^2\, \|\hat{b}_i\|^2$. A β–BKZ basis can be computed from an arbitrary basis $b_1, \ldots, b_m \in \mathbb{Z}^n$ by the algorithm of SCHNORR (1987). This algorithm finds an "approximate" β–BKZ basis using $O(nm(\beta^{O(\beta)} + m^2)\log B)$ arithmetic operations on $O(m \log B)$ bit integers where B is the maximal length of the given basis vectors. This algorithm is theoretical.

For practical algorithms performing block Korkin–Zolotarev reduction see SCHNORR, EUCHNER (1991). The Schnorr, Euchner algorithm transforms an arbitrary lattice basis into a δ–*approximate* β–BKZ basis, $\delta < 1$, which by definition satisfies for $i = 1, \ldots, m$

$$\delta\ \|\widehat{b}_i\|^2 \le \lambda_1(\pi_i L(b_1, \ldots, b_{\min(i+\beta-1,m)}))^2\ .$$

The Schnorr, Euchner algorithm is not proven to be polynomial time, but in practice its time bound appears to be $O(nm(\beta^{O(\beta)} + m^2)\log B)$. No polynomial time algorithm is known for $\delta = 1$, not even for $\beta = 2$.

5 Critical β–BKZ bases for block size 2 and 3

We call a β–BKZ basis $b_1, \ldots, b_m$ of the lattice L *critical* for β, m if the value $\|b_1\|\,/\,\lambda_1(L)$ is maximal for all β–BKZ bases of rank m. BACHEM and KANNAN (1984) present critical 2–BKZ bases $b_1, \ldots, b_m$. We establish critical

3–BKZ bases $b_1, \ldots, b_m$. We evaluate the constant $\alpha_3 = \max \|b_1\|^2 / \|\widehat{b}_3\|^2$, where the maximum is taken over all Korkin–Zolotarev bases b_1, b_2, b_3. We prove $\alpha_3 = \frac{3}{2}$.

We describe a slight variant of the critical 2–BKZ bases of Bachem, Kannan (1984). Let $\rho = \sqrt{\frac{3}{4}}$. We define the basis matrix $A_m = [b_1, \ldots, b_m] \in M_{m,m}(\mathbb{R})$ by

$$A_m = \begin{bmatrix} 1 & \frac{1}{2} & & & & & \\ & \rho & \rho/2 & & \text{O} & & \\ & & \rho^2 & \rho^2/2 & & & \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & \text{O} & & & \rho^{m-2} & \rho^{m-2}/2 \\ & & & & & & \rho^{m-1} \end{bmatrix} \qquad (12)$$

The matrices A_m satisfy the recursion

$$A_m = \left[\begin{array}{c:c} 1 & \frac{1}{2} \quad \text{O} \\ \hdashline \text{O} & \rho \cdot A_{m-1} \end{array}\right] .$$

Theorem 9 (Bachem, Kannan *1984) The column vectors of the matrix A_m form a critical 2-BKZ basis.*

Proof. It can easily be seen that the vector b_m is a shortest vector in $L(b_1, \ldots, b_m) - L(b_1, \ldots, b_{m-1})$. We have

$$\|b_m\|^2 = \rho^{2m-4}(\rho^2 + \frac{1}{4}) = (\frac{3}{4})^{m-2} .$$

It follows that b_m is the shortest vector in the lattice $L(b_1, \ldots, b_m)$. Therefore $\lambda_1 = \lambda_1(L(b_1, \ldots, b_m))$ satisfies

$$\|b_1\|^2 \lambda_1^{-2} = \left(\frac{4}{3}\right)^{m-2} .$$

Now let $b_1, \ldots, b_m$ be an arbitrary 2–BKZ basis. Let $v = \sum_{i=1}^m t_i b_i$ be a shortest non–zero lattice vector and $\mu = \max\{i \,|\, t_i \neq 0\}$. Then $\lambda_1 = \lambda_1(L(b_1, \ldots, b_m))$ satisfies

$$\lambda_1^2 \overset{1.}{\geq} \|\pi_{\mu-1}(v)\|^2 \overset{2.}{\geq} \|\widehat{b}_{\mu-1}\|^2 \overset{3.}{\geq} \left(\frac{3}{4}\right)^{\mu-2} \|b_1\|^2 \ .$$

1. holds since $\pi_{\mu-1}(v) \neq 0$, 2. holds since $\pi_{\mu-1}(b_{\mu-1})$ is minimal in the lattice $\pi_{\mu-1} L(b_{\mu-1}, b_\mu)$ which contains $\pi_{\mu-1}(v)$, 3. follows from the inequality 6. We now see that

$$\|b_1\|^2 \lambda_1^{-2} \leq \left(\frac{4}{3}\right)^{\mu-2} \leq \left(\frac{4}{3}\right)^{m-2} \ .$$

This shows that the columns of the matrix 12 form a critical basis. $\square$

A sequence of 3–BKZ bases $b_1, \ldots, b_m$. We define the basis matrices $B_m = [b_1, \ldots, b_m]$ as follows.

$$B_4 = \begin{bmatrix} 1 & & & \\ & \frac{\sqrt{3}}{2} & & \mathrm{O} \\ \mathrm{O} & & \sqrt{\frac{2}{3}} & \\ & & & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & \frac{1}{3} & \frac{1}{3} \\ \mathrm{O} & & 1 & -\frac{1}{2} \\ & & & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & \frac{\sqrt{3}}{2} & \frac{1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} \\ & \mathrm{O} & \sqrt{\frac{2}{3}} & -\frac{1}{2}\sqrt{\frac{2}{3}} \\ & & & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{13}$$

The lattice $L^{(4)} = L(b_1, \ldots, b_4)$ yields a lattice packing of maximal density, i.e. $\lambda_1(L^{(4)})^2 \det L^{(4)-\frac{2}{4}} = \gamma_4 = \sqrt{2}$. Let B_2, B_3 denote the 2×2, 3×3–matrix in the upper left corner of B_4. For arbitrary $m = 1, 2, \ldots$ we define the $m \times m$ matrix

$$B_m = \mathrm{diag}(d_1, \ldots, d_m) \ [\mu_{i,j}]^{\top}_{1 \leq i,j \leq m}$$

where $\mathrm{diag}(d_1, \ldots, d_m)$ is the $m \times m$ diagonal matrix with positive diagonal entries $d_1, \ldots, d_m$ and $M_m = [\mu_{i,j}]^{\top}_{1 \leq i,j \leq m}$ is an upper diagonal matrix with ones on the diagonal. It follows that the $\mu_{i,j}$ are the Gram–Schmidt coefficients of the basis $b_1, \ldots, b_m$ consisting of the column vectors of B_m. We define for $i = 1, 2, \ldots$

$$d_{2i-1} = \sqrt{\frac{2}{3}}^{\,i-1} \quad , \quad d_{2i} = \frac{\sqrt{3}}{2} \ , \quad d_{2i-1}$$

$$-\mu_{2i,2i-1} = \mu_{2i+1,2i-1} = \mu_{2i+2,2i-1} = \frac{1}{2} \ , \ \mu_{2i+k,2i-1} = 0 \text{ for } k \geq 3$$

$$\mu_{2i+1,2i} = \mu_{2i+2,2i} = \frac{1}{3} \ , \ \mu_{2i+k,2i} = 0 \quad \text{for} \quad k \geq 3 \ .$$

The matrices M_m, B_m are upper triangular matrices with four non–zero diagonals. They satisfy for $m > 4$ the following recursion

$$M_m \quad = \quad \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & \ldots \\ & 1 & \frac{1}{3} & \frac{1}{3} & 0 & \ldots \\ & & \cdots & \cdots & \cdots & \cdots \\ \mathrm{O} & & \vdots & & M_{m-2} & \\ & & \vdots & & & \end{bmatrix}$$

$$B_m \quad = \quad \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & \ldots \\ & \frac{\sqrt{3}}{2} & \frac{1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} & 0 & \ldots \\ & & \cdots & \cdots & \cdots & \cdots \\ & & \vdots & & & \\ \mathrm{O} & & \vdots & & \sqrt{\frac{2}{3}}\, B_{m-2} & \\ & & \vdots & & & \end{bmatrix}$$

Let $b_1, \ldots, b_m$ be the column vectors of B_m, $B_m = [b_1, \ldots, b_m]$ and let $L^{(m)} = L(b_1, \ldots, b_m)$ be the lattice generated by $b_1, \ldots, b_m$.

Theorem 10 *The column vectors $b_1, \ldots, b_m$ of B_m form a 3–BKZ basis.*

Proof. The vectors $b_1, \dots, b_4$ form a Korkin–Zolotarev basis since the vector $\widehat{b}_i$ is minimal in $\pi_i(L^{(4)}$ for $i = 1, \dots, 4$. The lattice $L^{(4)}$ yields the lattice sphere packing E_4, the lattice packing of maximal density for dimension 4, see Conway, Sloane (1988). We see from the recursive structure of $B_m = [b_{i,j}]_{1 \le i,j \le m}$ that

$$[b_{i,j}]_{2k+1 \le i,j \le 2k+5} = \left(\frac{2}{3}\right)^{k/2} B_4 \quad \text{for } k = 0, \dots, \lfloor (m-5)/2 \rfloor \ .$$

This implies that the basis $\pi_i(b_i)$, $\pi_i(b_{i+1})$, $\pi_i(b_{i+2})$ is Korkin–Zolotarev for $i = 1, \dots, m-2$. □

We let $L^{(k)}$ denote the lattice that is generated by the column vectors $b_1, \dots, b_k$ of the matrix B_k.

Lemma 11 *The basis $b_1, \dots, b_{2k+1}$ consisting of the column vectors of B_{2k+1} satisfies* $\|b_1\| \,/\, \lambda_1(L^{2k+1}) = \sqrt{\frac{3}{2}}^{k-1}$ *for* $k = 1, 2, \dots$

Proof. We have for $k = 1, 2, 3, \dots$ that

$$\|b_{2k+1}\| = \sqrt{\frac{2}{3}}^{k-1} = \|\widehat{b}_{2k-1}\| \ .$$

Moreover b_{2k+1} is the shortest vector in $L(b_1, \dots, b_{2k+1}) - L(b_1, \dots, b_{2k-1})$. This is because $\|b_{2k+1}\| = \|\widehat{b}_{2k-1}\|$ and $b_1, \dots, b_{2k+1}$ is a 3–BKZ basis.

Applying the above property of b_{2k+1} inductively we see that the shortest non–zero vector in $L^{(2k+1)}$ has length $\sqrt{\frac{2}{3}}^{k-1}$ which proves the claim. □

In order to show that the basis $b_1, \dots, b_{2k+1}$ of lattice $L^{(2k+1)}$ is a critical 3–BKZ basis we need an upper bound on $\|b_1\| \,/\, \lambda_1(L)$ which holds for all 3–BKZ bases of any lattice L. Let α_β be the lattice constant

$$\alpha_\beta = \max \|b_1\|^2 \,/\, \|\widehat{b}_\beta\|^2$$

where the maximum is taken over all Korkin–Zolotarev bases $b_1, \dots, b_\beta$. The following theorem improves the upper bound $\|b_1\|^2 \, \lambda_1(L)^{-2} \le \alpha_\beta^k$ from Schnorr (1987).

Theorem 12 *Every β–BKZ basis $b_1, \dots, b_m$ of lattice L for which $k = (m-1)/(\beta-1)$ is integer satisfies $\|b_1\|^2 \, \lambda_1(L)^{-2} \le \alpha_\beta^{k-1}$.*

Proof. Let $v = \sum_{i=1}^{m} t_i b_i$ be a shortest non–zero vector in L. We can assume that $v \notin L(b_1, \ldots, b_{m-\beta+1})$ since otherwise we can reduce k and the induction hypothesis for $k-1$ yields $\|b_1\|^2\, \lambda_1(L)^{-2} \leq \alpha_\beta^{k-2}$. From $v \notin L(b_1, \ldots, b_{m-\beta+1})$ we see that $\pi_{m-\beta+1}(v) \neq 0$. Since $\pi_{m-\beta+1}(b_{m-\beta+1}), \ldots, \pi_{m-\beta+1}(b_m)$ is a Korkin–Zolotarev basis we have

$$\|\widehat{b}_{m-\beta+1}\| \leq \|\pi_{m-\beta+1}(v)\| \leq \lambda_1(L) \ .$$

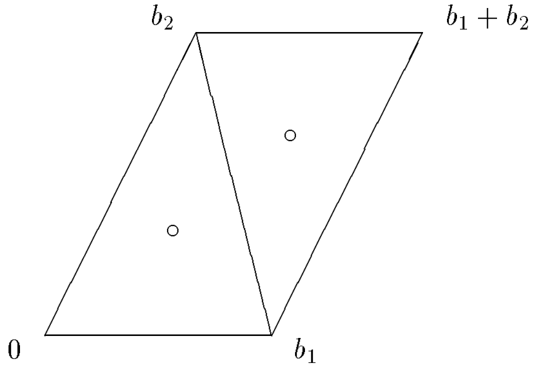
Moreover $\|\widehat{b}_{1+(\beta-1)(j-1)}\|^2 \leq \alpha_\beta \ \|\widehat{b}_{1+(\beta-1)j}\|^2$ holds for $j = 1, \ldots, k-1$ since the basis $b_1, \ldots, b_m$ is β–BKZ. Therefore

$$\|b_1\|^2 \leq \alpha_\beta^{k-1} \ \|\widehat{b}_{m-\beta+1}\|^2 \leq \alpha_\beta^{k-1} \ \lambda_1(L)^2 \ . \qquad \square$$

Theorem 13 $\alpha_3 = \frac{3}{2}$ *, i.e.* $\alpha_3^{-1/2}$ *is the height of the tetrahedron with side length* 1*.*

Proof. Let b_1, b_2, b_3 be a Korkin–Zolotarev basis with $\|b_1\| = 1$ and minimal $\|\widehat{b}_3\|$, i.e. $\alpha_3 = \|b_1\|^2\, \|\widehat{b}_3\|^{-2} = \|\widehat{b}_3\|^{-2}$. Consider the projection $\mu_{3,1} b_1 + \mu_{3,2} \widehat{b}_2$ of b_3 in span (b_1, b_2). We claim that $\mu_{3,1} b_1 + \mu_{3,2} \widehat{b}_2$ must be a "deep hole" for the lattice $L(b_1, b_2)$, i.e. a point that has maximal distance from the lattice points. If $\mu_{3,1} b_1 + \mu_{3,2} \widehat{b}_2$ is not a deep hole for the lattice $L(b_1, b_2)$ we can change $\mu_{3,1}, \mu_{3,2}$ such that the minimal distance of $\mu_{3,1} b_1 + \mu_{3,2} \widehat{b}_2$ from $L(b_1, b_2)$ increases. This permits to decrease $\|\widehat{b}_3\|$ without violating the properties of Korkin–Zolotarev bases.

There are at most two deep holes in the ground mesh of the basis b_1, b_2, namely the points that have equal distance to $0, b_1, b_2$ $(b_1, b_2, b_1 + b_2$, respectively).



deep holes $\circ$ in the ground mesh

W.l.o.g. we can assume that $\mu_{3,1}b_1 + \mu_{3,2}\widehat{b}_2$ has equal distance from $0, b_1$ and b_2. It follows from $\|b_2\|^2 = \mu_{2,1}^2 + \|\widehat{b}_2\|^2 \geq \|b_1\|^2 = 1$, $|\mu_{2,1}| \leq \frac{1}{2}$ that

$$\|\widehat{b}_2\| \geq \frac{\sqrt{3}}{2} \, . \tag{14}$$

Let $\|\widehat{b}_2\| = \frac{\sqrt{3}}{2} + \varepsilon$ with $\varepsilon \geq 0$. We have

$$\begin{aligned} \|\mu_{3,2}\widehat{b}_2\| &= \frac{\sqrt{3}}{6} \quad \text{if} \quad \varepsilon = 0 \\ \|\mu_{3,2}\widehat{b}_2\| &\leq \frac{\sqrt{3}}{6} + \varepsilon \quad \text{for} \quad \varepsilon \geq 0 \, . \end{aligned} \tag{15}$$

This is because $\varepsilon = 0$ implies that $\|b_1\| = \|b_2\| = \|b_1 - b_2\| = 1$ and thus $\mu_{3,1}b_1 + \mu_{3,2}\widehat{b}_2 = \frac{b_1+b_2}{3}$. Moreover the $\widehat{b}_2$–coordinate of the deep hole $\mu_{3,1}b_1 + \mu_{3,2}\widehat{b}_2$ does not increase faster in ε than $\|\widehat{b}_2\|$. We see from $\|\pi_2(b_3)\| \geq \|\widehat{b}_2\|$ that $\|\widehat{b}_3\|^2 + \mu_{3,2}^2\|\widehat{b}_2\|^2 \geq \|\widehat{b}_2\|^2$, and thus

$$\begin{aligned} \|\widehat{b}_3\|^2 &\geq \|\widehat{b}_2\|^2 - \mu_{3,2}\|\widehat{b}_2\|^2 \\ &\overset{15,16}{\geq} \left(\frac{\sqrt{3}}{2} + \varepsilon\right)^2 - \left(\frac{\sqrt{3}}{6} + \varepsilon\right)^2 \\ &\geq \frac{3}{4} - \frac{1}{12} = \frac{2}{3} \end{aligned}$$

holds for the basis matrix $B_3 = [b_1, b_2, b_3]$. This proves that $\alpha_3 = \frac{3}{2}$. $\square$

Theorem 14 *The lattice basis* $b_1, \ldots, b_{2k+1}$ *defined by the basis matrix* B_{2k+1} *is a critical 3–BKZ basis.*

Proof. Lemma 11 shows that $\|b_1\| \,/\, \lambda_1(L^{(2k+1)}) = \sqrt{\frac{3}{2}}^{\,k-1}$. On the other hand every 3–BKZ basis $b'_1, \ldots, b'_{2k+1}$ of lattice L satisfies $\|b'_1\| \,/\, \lambda_1(L) \leq \sqrt{\alpha_3}^{\,k-1}$ by Theorem 12, where $\alpha_3 = \frac{3}{2}$ by Theorem 13. This shows that $\|b_1\| \,/\, \lambda_1(L^{(2k+1)})$ is maximal for 3–BKZ bases of rank $2k+1$. $\square$

Acknowledgement. The author wishes to thank Brigitte Vallée for her participation in starting this work.

References

[1] L. Babai: *On Lovász' lattice reduction and the nearest lattice point problem.* Combinatorica, **6** (1986), 1–13.

[2] A. Bachem and R. Kannan: *Lattices and the basis reduction algorithm.* TR, Carnegie Mellon University (1984), 22 pages.

[3] J.W.S. Cassels: *An introduction to the geometry of numbers.* Springer-Verlag, Berlin, New York (1971).

[4] J.H. Conway and H.J.A. Sloane: *Sphere Packings, Lattices and Groups.* Springer–Verlag, New York Berlin (1988).

[5] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr and J. Stern: *An improved low–density subset sum algorithm.* To appear in computational complexity.

[6] M. Grtschel, L. Lovász, and A. Schrijver: *Geometric algorithms and combinatorial optimization.* Springer–Verlag, Berlin, **198**.

[7] C. Hermite: *Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres, Deuxième lettre du 6 août 1845.* J. Reine Angew. Math. **40** (1850), 279–290.

[8] R. Kannan: *Minkowski's convex body theorem and integer programming.* Math. Oper. Res. **12** (1987), 415–440.

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

[10] J.C. Lagarias, H.W. Lenstra, Jr., and C.P. Schnorr: *Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice.* Combinatorica, 10 (1990), 333–348.

[11] J.L. Lagrange: *Recherches d'arithmétique,* Nouv. Mém. Acad. Berlin (1773), 265–312. Œvres, vol. VIII, 693–753.

[12] A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász: *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982), 515–534.

[13] H.W. Lenstra, Jr.: *Integer programming with a fixed number of variables.* Math. Oper. Res. **8** (1983), 538–548.

[14] L. Lovász: *An algorithmic theory of numbers, graphs and convexity.* CBMS–NSF Regional Conference Series in Applied Mathematics **50**, SIAM, Philadelphia, Pennsylvania, **1986**.

[15] K. Mahler: *A theorem on inhomogeneous diophantine inequalities.* Nederl. Akad. Wetensch., Proc. **41** (1938), 634–637.

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

[17] C.P. Schnorr and M. Euchner: *Lattice basis reduction: improved algorithms and solving subset sum problems.* Proceedings of Fundamentals of Computation Theory, FCT'91, Ed. L. Budach, Springer LNCS **529**, (1991), pp. 68–85.