Theoretical Computer Science 53 (1987) 201-224
North-Holland

A HIERARCHY OF POLYNOMIAL TIME LATTICE BASIS REDUCTION ALGORITHMS

C.P. SCHNORR

Fachbereich Mathematik/Informatik, Universität Frankfurt, D-6000 Frankfurt, Fed. Rep. Germany

Communicated by A. Schönhage
Received December 1986
Revised April 1987

Abstract. We present a hierarchy of polynomial time lattice basis reduction algorithms that stretch from Lenstra, Lenstra, Lovász reduction to Korkine-Zolotareff reduction. Let $\lambda(L)$ be the length of a shortest nonzero element of a lattice L. We present an algorithm which for $k \in \mathbb{N}$ finds a nonzero lattice vector b so that $|b|^2 \leq (6k^2)^{n/k}\lambda(L)^2$. This algorithm uses $O(n^2(\sqrt{k}^{k+o(k)}+n^2)\log B)$ arithmetic operations on $O(n \log B)$-bit integers. This holds provided that the given basis vectors $b_1, \ldots, b_n \in \mathbb{Z}^n$ are integral and have the length bound B. This algorithm successively applies Korkine-Zolotareff reduction to blocks of length k of the lattice basis. We also improve Kannan's algorithm for Korkine-Zolotareff reduction.

1. Introduction

We introduce and analyse novel algorithms for the reduction of lattice bases $b_1, \ldots, b_n \in \mathbb{R}^d$ of arbitrary rank n. This computational problem is equivalent to the reduction of positive definite quadratic forms. Gauss [4] gave reduction algorithms for rank 2 and 3. Let B be the maximal Euclidean length of the input basis vectors. The Gaussian reduction algorithm on an integer input basis $b_1, \ldots, b_n \in \mathbb{Z}^n$, $n = 2$ or 3, terminates after at most $O(\log B)$ arithmetic operations, see [11]. All arithmetic steps are on integers with at most $O(\log B)$ bits.

Reduction for quadratic forms of arbitrary dimension was first studied by Hermite [7], Korkine, Zolotareff [9] and Minkowski [15]. Korkine and Zolotareff as well as Minkowski considered lattice bases $b_1, \ldots, b_n$ with the property that b_1 is a shortest (nonzero) lattice element. Minkowski requires this property for all subbases $b_i, \ldots, b_n$ for $i = 1, \ldots, n$. Korkine and Zolotareff considered bases so that this property holds for the orthogonal projection of the subbases $b_i, \ldots, b_n$ in the linear space $(\sum_{j<i} b_j \mathbb{R})^{\perp}$. No efficient algorithm is known for finding a shortest element in lattices of arbitrary rank. Van Emde Boas [2] proved that deciding whether a given lattice element is $\| \ \|_\infty$-shortest ($\| \ \|_\infty$ is the maximum norm) is NP-complete. So presumably this problem is intractable and the problem of finding a shortest lattice element is likely to be hard.

Recently, Lovász [13] proposed a natural extension of the Gaussian reduction algorithm to lattices of arbitrary rank, see [13]. The Lovász algorithm, called

LLL-reduction, applied to a lattice basis $b_1, \ldots, b_n \in \mathbb{Z}^n$ successively performs a Gaussian reduction step for the smallest reasonable i to the projection of b_i, b_{i+1} in the subspace $(\sum_{j<i} b_j \mathbb{R})^{\perp}$. This algorithm finds a lattice element that is at most $2^{(n-1)/2}$ times longer than the shortest lattice element. The algorithm runs in $O(n^4 \log B)$ arithmetic steps on integers with at most $O(n \log B)$ bits. LLL-reduction is a basic tool for solving various Diophantine computational problems, such as factoring polynomials with rational coefficients, solving linear systems of inequalities over the integers, finding linear Diophantine approximations, breaking knapsack cryptosystems, a.s.o. The disproof of the Mertens conjecture by Odlyzko and Te Riele [16] is also based on this algorithm.

Subsequently to the Lovász algorithm, Kannan [8] proposed an algorithm for Korkine-Zolotareff reduction which runs in $n^{O(n)} \log B$ arithmetic steps on $O(n^2 \log B)$-bit integers. Helfrich [6] using the techniques of Lovász and Kannan has shown that Minkowski reduction can be done within $n^{O(n^3)} \log B$ arithmetic steps.

In this paper we introduce a hierarchy of reduction concepts that stretch from LLL-reduction to Korkine-Zolotareff reduction, and which run in polynomial time for lattices of arbitrary rank. We call a lattice basis $b_1, \ldots, b_n$ *k-reduced* if for $i = 1, \ldots, n-k+1$ the projection of $b_i, \ldots, b_{i+k-1}$ in $(\sum_{j<i} b_j \mathbb{R})^{\perp}$ forms a Korkine-Zolotareff-reduced basis of rank k. Thus k-reduced lattice bases are locally Korkine-Zolotareff reduced. For $k = 2$ the concept of k-reduced bases is essentially equivalent to LLL-reduction; for $n = k = 2$ it coincides with Gauss reduction and for $n = k$ it is Korkine-Zolotareff reduction. We call a lattice basis $b_1, \ldots, b_{mk}$ *block 2k-reduced*, if the projections of all *2k-blocks* $b_{ik+1}, \ldots, b_{(i+2)k}$ for $i = 0, \ldots, m-2$ are Korkine-Zolotareff reduced. By Theorems 2.6 and 2.7, every block $2k$-reduced basis $b_1, \ldots, b_n$ contains a vector that is at most $(4k^2)^{n/k}$ times as long as the shortest lattice vector. We express this worst-case performance of k-reduced and of block $2k$-reduced lattice bases in terms of fundamental constants α_k, β_k for Korkine-Zolotareff reduction.

In Section 3 we present relaxed reduction concepts that permit proving polynomial time bounds. To obtain a polynomial time bound we restrict Korkine-Zolotareff reduction to pairwise disjoint *blocks*. We discuss two alternatives to relate the reduction of adjacent blocks, *semi k-reduction* and *semi block 2k-reduction*. Semi block $2k$-reduction of an integer lattice basis $b_1, \ldots, b_n$ is performed within $O(n^2(k^{k/2+o(k)} + n^2) \log B)$ arithmetic steps with $O(n \log B)$-bit integers. This time bound differs from that for LLL-reduction only by a constant factor depending on k. Semi block $2k$-reduction finds a lattice vector that is at most $(6k^2)^{n/k}$ times as long as the shortest lattice vector. Semi k-reduction has the same time bound and uses simpler subroutines, but may yield slightly longer basis vectors. Using the improvements of Schnorr [17] to the Lovász reduction algorithm, the integers occurring in these algorithms can be reduced to $O(\log B)$-bit integers.

In Section 4 we present an improved version of Kannan's algorithm for Korkine-Zolotareff reduction of lattice bases of arbitrary rank. This algorithm uses a novel method to extend a given shortest lattice vector to a lattice basis. The algorithm

merely performs a sequence of Lovász reduction steps and from time to time an exhaustive search for a shortest lattice vector. As a consequence, all integers occurring in the computation have at most $O(n \log B)$ bits. On an integer input basis $b_1, \ldots, b_n$ the algorithm performs at most $n^{n/2+o(n)} + O(n^4 \log B)$ arithmetic operations on $O(n \log B)$-bit integers.

In Section 5 we prove the above-mentioned time bound for semi k-reduction and for semi block $2k$-reduction. In particular, we explain how to apply Korkine-Zolotareff reduction to k-blocks and how to keep track of block transformations. In Appendix A we outline the reduction algorithm of Lovász for LLL-reduction and of Gauss for the reduction of rank 2 lattice bases. We also give a practical algorithm for Korkine-Zolotareff reduction of lattices with rank ≤ 5.

2. Various concepts of basis reduction

Let $\mathbb{R}^d$ be the d-dimensional real vector space with the usual inner product $\langle\ ,\ \rangle$ and Euclidean length $|y| = \langle y, y\rangle^{1/2}$. A discrete, additive subgroup $L \subset \mathbb{R}^d$ is called a *lattice*. Every lattice L is generated by some set of linearly independent elements $b_1, \ldots, b_n \in L$, called a *basis* of L,

$$L = \sum_{i=1}^{n} b_i \mathbb{Z} = \{\alpha_1 b_1 + \cdots + \alpha_n b_n \mid \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}.$$

The *rank* of L is n and the *determinant* $d(L)$ of lattice L is defined by $d(L) = \det[\langle b_i, b_j\rangle_{1 \leq i,j \leq n}]^{1/2}$. Let $\lambda(L)$ be the length of a shortest (nonzero) element in L. The determinant and the rank of L do not depend on the choice of a basis. The purpose of reduction theory is to find a basis consisting of short vectors or, equivalently, a basis that is nearly orthogonal.

To describe the concepts of reductions we use the Gram-Schmidt orthogonalization process. Let $b_1, \ldots, b_n \in \mathbb{R}^d$ be a sequence of linearly independent vectors. We denote by $b_i(j)$ the component of b_i which is orthogonal to $b_1, \ldots, b_{j-1}$, and we set $b_j^* = b_j(j)$. The vectors $b_1^*, \ldots, b_n^*$ are linearly independent and mutually orthogonal; they are called the Gram-Schmidt orthogonalization of $b_1, \ldots, b_n$, and they can be computed from $b_1, \ldots, b_n$ by the recurrence

$$b_1^* = b_1,$$

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \quad i = 1, \ldots, n \text{ with } \mu_{i,j} = \langle b_i, b_j^*\rangle / \langle b_j^*, b_j^*\rangle.$$

For completeness let $\mu_{i,i} = 1$ and $\mu_{i,j} = 0$ for $i < j$. Then $L_i = \sum_{j \geq i} b_j(i) \mathbb{Z}$ is the orthogonal projection of L on the orthogonal complement of $\sum_{j<i} b_j \mathbb{R}$. L_i is a lattice with rank $n - i + 1$. The above notions depend on the order of the basis vectors $b_1, \ldots, b_n$. This will also be the case for the following reduction concepts.

We call a basis $b_1, \ldots, b_n \in \mathbb{R}^d$ *size-reduced*, if

$$|\mu_{i,j}| \leq \tfrac{1}{2} \quad \text{for } 1 \leq j < i \leq n. \tag{2.1}$$

The basis vector b_i is *size-reduced*, if (2.1) holds for this i.

There is a fast algorithm to obtain a size-reduced basis from a given basis. Given the coefficients $\mu_{i,j}$ we can in $O(nd)$ airthmetic operations reduce a single b_i in size and update the coefficients $\mu_{i,j}$ as follows (by $\lceil r \rfloor$ we denote the integer that is nearest to the real number r):

for $j = i-1, \ldots, 1$
  begin
    $b_i := b_i - \lceil \mu_{i,j} \rfloor \, b_j$
    for $\nu = 1, \ldots, j \quad \mu_{i,\nu} := \mu_{i,\nu} - \lceil \mu_{i,j} \rfloor \, \mu_{j,\nu}$
  end

This does not change the coefficients $\mu_{k,i}$ for $k > i$. In order to reduce a basis $b_1, \ldots, b_n$ in size we can apply size-reduction to the basis elements in any order but to keep numbers small one should use the order $b_1, \ldots, b_n$.

A basis $b_1, \ldots, b_n$ is *Korkine–Zolotareff reduced* (according to [9]) if it is size-reduced and if

$$|b_i^*| = \lambda(L_i) \quad \text{for } i = 1, \ldots, n. \tag{2.2}$$

The conditions (2.1) and (2.2) were originally introduced in the reduction theory of positive definite quadratic forms. Hermite [7] in his second letter to Jacobi used property (2.1) and Korkine and Zolotareff [9] introduced property (2.2).

A basis $b_1, \ldots, b_n \in \mathbb{R}^d$ is *LLL-reduced* (according to [13]) if it is size-reduced and if

$$|b_i^*|^2 \leq \tfrac{4}{3} |b_{i+1}(i)|^2 \quad \text{for } i = 1, \ldots, n-1. \tag{2.3}$$

The number $\frac{4}{3}$ in condition (2.3) is there to permit proving a polynomial time bound for LLL-reduction. The number $\frac{4}{3}$ can be replaced by any number which is greater than 1.

Basic properties of LLL-reduced bases have been established in [13]. It follows from

$$\tfrac{3}{4} |b_i^*|^2 \leq |b_{i+1}(i)|^2 \quad \text{and} \quad |\mu_{i+1,i}| \leq \tfrac{1}{2}$$

(where (2.3) respectively (2.1) have been used) that

$$|b_i^*|^2 = 2(\tfrac{3}{4} - \tfrac{1}{4}) |b_i^*|^2 \leq 2(|b_{i+1}(i)|^2 - \tfrac{1}{4} |b_i^*|^2).$$

Hence,

$$|b_i^*|^2 \leq 2 |b_{i+1}^*|^2. \tag{2.4}$$

Let $\lambda_1, \ldots, \lambda_n, \lambda_1 = \lambda$ denote the successive minima of lattice L, i.e., $\lambda = \lambda_i(L)$ is smallest real number c for which there exist i linearly independent lattice vectors of length $\leq c$. The lengths of the basis vectors $b_1, \ldots, b_n$ of an LLL-reduced basis give a rough approximation of the successive minima of L.

Theorem 2.1 (Lenstra et al. [13]). *Every LLL-reduced basis $b_1, \ldots, b_n$ of lattice L satisfies*

$$2^{1-i} \leqslant |b_i|^2/\lambda_i^2 \leqslant 2^{n-1} \quad \text{for } i = 1, \ldots, n.$$

A tighter approximation of the successive minima is obtained by Korkine-Zolotareff reduced bases (see [11]) as follows.

Theorem 2.2. *Every Korkine-Zolotareff reduced basis $b_1, \ldots, b_n$ of lattice L satisfies*

$$\frac{4}{(i+3)} \leqslant \frac{|b_i|^2}{\lambda_i^2} \leqslant \frac{(i+3)}{4} \quad \text{for } i = 1, \ldots, n.$$

We are going to introduce lattice bases that are locally Korkine-Zolotareff reduced. Let us call a basis $b_1, \ldots, b_n$ *k-reduced* if it is size-reduced and if $b_i(i), \ldots, b_{i+k-1}(i)$ is a Korkine-Zolotareff reduced basis for $i = 1, \ldots, n-k+1$. We call the vector sequence $b_i(i), \ldots, b_{i+k-1}(i)$ a *k-block*. This notion extends the role of 2-blocks in LLL-reduction to arbitrary k-blocks. The 2-blocks $b_i(i)$, $b_{i+1}(i)$ of an LLL-reduced basis are semi-Korkine-Zolotareff reduced (they would be Korkine-Zolotareff reduced if the number $\frac{4}{3}$ in (2.3) were replaced by 1).

We call a lattice basis $b_1, \ldots, b_{mk}$ *block 2k-reduced* if it is size-reduced and if all $2k$-blocks

$$b_{ik+1}(ik+1), \ldots, b_{(i+2)k}(ik+1) \quad \text{for } i = 0, \ldots, m-2$$

are Korkine-Zolotareff reduced. Every $2k$-reduced basis is block $2k$-reduced. Every block 2-reduced basis is LLL-reduced.

The quality of k-reduced bases is closely related to the lattice constant

$$\alpha_k := \max \frac{|b_1|^2}{|b_k^*|^2}$$

where the maximum is taken over all Korkine-Zolotareff reduced bases $b_1, \ldots, b_k$ of rank k lattices. We call the numbers α_k the *Korkine-Zolotareff constants*. Note that $\alpha_k \leqslant \alpha_{k+1}$ holds for all k. This is true since every Korkine-Zolotareff reduced basis $b_2, \ldots, b_{k+1}$ extends to a Korkine-Zolotareff reduced basis $b_1, \ldots, b_{k+1}$ by adjoining an arbitrary vector b_1 that is orthogonal to $b_2, \ldots, b_{k+1}$ and which has the same length as b_2.

Theorem 2.3. *Every k-reduced basis $b_1, \ldots, b_n$ satisfies $|b_1|^2 \leqslant \alpha_k^{(n-1)/(k-1)} \lambda(L)^2$ provided that $k-1$ divides $n-1$.*

Proof. Let $v = \sum_{i=1}^n v_i b_i = \sum_{i=1}^n \bar{v}_i b_i^*$ be a shortest lattice element, and let $\mu := \max\{i \mid v_i \neq 0\}$. We have $\bar{v}_\mu = v_\mu \in \mathbb{Z}$ and $\lambda(L)^2 = |v|^2 \geqslant v_\mu^2 |b_\mu^*|^2 \geqslant |b_\mu^*|^2$. On the other hand, every k-reduced basis $b_1, \ldots, b_n$ satisfies

$$|b_i^*|^2 \leqslant \alpha_k |b_{i+j}^*|^2 \quad \text{for } j \leqslant k-1,\ i+j \leqslant n.$$

Inductive application of this bound yields

$$|b_i^*|^2 \leq \alpha_k^{\nu}|b_{i+j}^*|^2 \quad \text{for } j \leq \nu(k-1),\ i+j \leq n.$$

Thus we obtain

$$|b_1|^2 = |b_1^*|^2 \leq \alpha_k^{(n-1)/(k-1)}|b_\mu^*|^2 \leq \alpha_k^{(n-1)/(k-1)}\lambda(L)^2 \qquad \square$$

The strength of Theorem 2.3 depends on the Korkine-Zolotareff constants α_k. It can easily be seen that $\alpha_2 = \frac{4}{3}$, $\alpha_3 = \frac{3}{2}$, $\alpha_2^{-1/2}$ ($\alpha_3^{-1/2}$ respectively) is the height of the regular triangle (tetrahedron respectively) with unit edge length. Thus, for $k=2$ the upper bound $|b_1|^2 \leq (\frac{4}{3})^{n-1}\lambda_1^2$ of Theorem 2.3 improves the upper bound $|b_1|^2 \leq 2^{n-1}\lambda_1^2$ of Theorem 2.1. This improvement is achieved by replacing the number $\frac{4}{3}$ in condition (2.3) by 1.

We will establish upper bounds on α_k depending on the Hermite constants. The *Hermite constant* γ_n is the maximal value of $\lambda(L)^2\,\mathrm{d}(L)^{-2/n}$ where L ranges over all lattices of rank n. The values γ_n are known for $n \leq 8$, see [1], and Appendix A: $\gamma_1 = 1$, $\gamma_2 = \sqrt{\frac{4}{3}}$, $\gamma_3 = 2^{1/3}$, $\gamma_4 = \sqrt{2}$. For arbitrary n, Minkowski's Convex Body Theorem implies (see [1, chapter IX.7]):

$$\gamma_n \leq \frac{4}{\pi}\Gamma\left(1+\frac{n}{2}\right)^{2/n}$$

which yields $\gamma_n \leq \frac{2}{3}n$ for all $n \geq 2$.

Lemma 2.4. *Let $b_1, \ldots, b_n$ be a Korkine-Zolotareff reduced basis; then*

$$|b_1^*|^2 \leq \gamma_n^{n/(n-1)} \prod_{i=1}^{j-1} \gamma_{n-i}^{1/(n-i-1)} \left(\prod_{i=j+1}^{n} |b_i^*|\right)^{2/(n-j)}$$

holds for $j = 1, \ldots, n-1$. Here we take $\prod_{i=1}^{0}$ to be 1.

Proof. By definition of γ_n we have

$$|b_1|^2 = \lambda(L)^2 \leq \gamma_n\,\mathrm{d}(L)^{2/n} = \gamma_n\left(\prod_{i=1}^{n}|b_i^*|\right)^{2/n}.$$

By eliminating $|b_1^*|^2 = |b_1|^2$ on the right-hand side this yields

$$|b_1|^2 \leq \gamma_n^{n/(n-1)}\left(\prod_{i=2}^{n}|b_i^*|\right)^{2/(n-1)}$$

which proves the lemma for $j=1$. We prove the inequality of the lemma by induction on j. On the right-hand side of the induction hypothesis for j we replace $|b_{j+1}^*|^2$ by the upper bound

$$|b_{j+1}^*|^2 \leq \gamma_{n-j}^{(n-j)/(n-j-1)}\left(\prod_{i=j+2}^{n}|b_i^*|\right)^{2/(n-j-1)}$$

(which is the case $j=1$ for the Korkine-Zolotareff reduced basis $b_{j+1}(j+1), \ldots, b_n(j+1)$), and we obtain the inequality of the lemma for $j+1$. $\square$

Corollary 2.5. $\alpha_k \leq k^{1+\ln k}$ *for all* $k \geq 2$, *where* ln *is the logarithm to basis* e.

Proof. Applying the inequality of Lemma 2.4 to a Korkine-Zolotareff reduced basis $b_1, \ldots, b_k$ with $j = k-1$ yields

$$|b_1|^2 \leq \gamma_k^{k/(k-1)} \prod_{i=1}^{k-2} \gamma_{k-i}^{1/(k-i-1)} |b_k^*|^2$$

$$\leq \gamma_k \delta_k |b_k^*|^2 \quad \text{with } \delta_k = \gamma_k^{1/(k-1)} \gamma_{k-1}^{1/(k-2)} \cdots \gamma_2^1.$$

We conclude from $\gamma_k \leq \frac{2}{3}k$ and $1/(k-1) + \cdots + \frac{1}{2} \leq \ln k$ that $\delta_k \leq k^{\ln k}$ for $k \geq 2$. □

Corollary 2.5 implies that $\lim_k \alpha_k^{1/k} = 1$. Therefore, by Theorem 2.3, every k-reduced basis $b_1, \ldots, b_n$ of lattice L satisfies

$$|b_1|^2 \leq (1+\varepsilon_k)^{n-1} \lambda(L)^2$$

where ε_k is a constant that only depends on k and which converges to 0 as k increases. It is an open problem whether $\alpha_k = k^{O(1)}$.

The upper bound on α_k may be weak. We give a second method to bound $|b_1|^2/\lambda(L)^2$ for k-reduced bases depending on the constant

$$\beta_k := \max\left(\frac{|b_1^*|^2 \cdots |b_k^*|^2}{|b_{k+1}^*|^2 \cdots |b_{2k}^*|^2} \right)^{1/k}$$

where the maximum is taken over all Korkine-Zolotareff reduced bases $b_1, \ldots, b_{2k}$ of rank $2k$ lattices.

Theorem 2.6. *Every block* $2k$*-reduced basis* $b_1, \ldots, b_{mk}$ *of lattice* L *satisfies* $|b_1|^2 \leq \gamma_k \beta_k^{m-1} \lambda(L)^2$.

Proof. Every block $2k$-reduced basis $b_1, \ldots, b_{mk}$ satisfies

$$|b_{ik+1}^*|^2 \cdots |b_{ik+k}^*|^2 \leq \beta_k^k |b_{ik+k+1}^*|^2 \cdots |b_{ik+2k}^*|^2 \quad \text{for } i = 0, \ldots, m-2.$$

Recursive application of this bound yields

$$|b_1^*|^2 \cdots |b_k^*|^2 \leq \beta_k^{\nu k} |b_{\nu k+1}^*|^2 \cdots |b_{\nu k+k}^*|^2. \tag{2.5}$$

Let $v = \sum_{i=1}^{mk} z_i b_i$ be a shortest lattice element. Set $\mu = \max\{i \mid v_i \neq 0\}$, and suppose $(\nu+1)k \leq \mu \leq (\nu+2)k$. If $\mu \leq 2k$, then $|b_1| = \lambda(L)$, so let $\nu \geq 1$. Since $b_1, \ldots, b_{mk}$ is block $2k$-reduced and $v(\mu) \neq 0$ we have

$$|b_{\nu k+i}(\nu k+1)| \leq |v(\nu k+1)| \leq \lambda(L) \quad \text{for } i = 1, \ldots, k.$$

Hence, we obtain from (2.5)

$$|b_1^*|^2 \cdots |b_k^*|^2 \leq \beta_k^{\nu k} \lambda(L)^{2k}.$$

Since $|b_1|^2 \leq \gamma_k (|b_1^*| \cdots |b_k^*|)^{2/k}$ this implies

$$|b_1|^2 \leq \gamma_k \beta_k^{\nu} \lambda(L)^2 \leq \gamma_k \beta_k^{m-1} \lambda(L)^2. \qquad \square$$

An upper bound for β_k can be obtained from Lemma 2.4.

Theorem 2.7. $\beta_k \leq 4k^2$.

Proof. Let $b_1, \ldots, b_{2k}$ be a $2k$-reduced basis. Application of Lemma 2.4 to $b_i(i), \ldots, b_{2k}(i)$, $n = 2k-i+1$ and using the bound $\gamma_{2k-j} \leq 2k$ yields

$$|b_i^*|^2 \leq (2k)^{(2k-i+1)/(2k-i)+1/(2k-i-1)+\cdots+1/k}(|b_{k+1}^*| \cdots |b_{2k}^*|)^{2/k}$$

$$\leq (2k)^2(|b_{k+1}^*| \cdots |b_{2k}^*|)^{2/k} \quad \text{for } i = 1, \ldots, k.$$

This implies

$$|b_1^*|^2 \cdots |b_k^*|^2 \leq (2k)^{2k}|b_{k+1}^*|^2 \cdots |b_{2k}^*|^2$$

and thus proves the theorem. □

Theorem 2.6 yields a stronger performance bound than Theorem 2.3 when using the above upper bounds on α_k, β_k. Every $2k$-reduced basis $b_1, \ldots, b_n$ of a lattice L of rank n with k dividing n satisfies, by Theorem 2.6,

$$|b_1|^2 \leq (4k)^{n/k}\lambda(L)^2,$$

whereas Theorem 2.3 only shows

$$|b_1|^2 \leq (2k)^{(1+\ln(2k))n/2k}\lambda(L)^2$$

Substituting the result of Lemma 2.4 into the definition of β_k and simplifying yields the bound

$$\beta_k \leq \prod_{i=1}^{k} \gamma_{2k-i+1}^{2/(2k-i)}. \tag{2.6}$$

In particular, $\beta_1 = \frac{4}{3}$, $\beta_2 \leq 1.59$, $\beta_3 \leq 1.91$, $\beta_4 \leq 2.25$; hence, $\beta_1^{1/1} = \frac{4}{3} \leq 1.34$, $\beta_2^{1/2} \leq 1.26$, $\beta_3^{1/3} \leq 1.24$, $\beta_4^{1/4} \leq 1.23$.

3. Polynomial time algorithms for semi block $2k$-reduction and semi k-reduction

No polynomial time algorithm is known for k-reduction and for block $2k$-reduction. To obtain polynomial time bounds we relax these concepts to semi k-reduction and to semi block $2k$-reduction. A similar relaxation accounts for the transition from 2-reduction to LLL-reduction.

The time analysis for LLL-reduction is based on the observation that a reduction step changes only a single Gramian determinant $d_i := \prod_{j \leq i} |b_j^*|^2$, $i = 1, \ldots, n$, and this d_i is decreased by at least a factor $\frac{4}{3}$. Korkine-Zolotareff reduction of a k-block $b_{s+j}(s+1)$, $j = 1, \ldots, k$, may change d_i for $i = s+1, \ldots, s+k-1$ and possibly some of these d_i increase. To enable an analysis similar to LLL-reduction we apply

Korkine-Zolotareff reduction only to pairwise disjoint k-blocks $b_{ik+j}(ik+1)$, $j=1,\ldots,k$. Let the rank n of the lattice be $n=mk$. For a lattice basis $b_1,\ldots,b_{mk}$, let

$$C_i=\prod_{j=1}^{k}|b_{ik+j}^*|^2, \qquad D_i=\prod_{j=0}^{i-1}C_j \quad \text{for } i=0,\ldots,m-1.$$

Then Korkine-Zolotareff reduction of the $2k$-block $b_{ik+j}(ik+1)$, $j=1,\ldots,2k$, leaves all D_j with $j\neq i$ unchanged and if $C_i\geqslant\frac{4}{3}\beta_k^k C_{i+1}$, it decreases D_i by at least a factor $\frac{4}{3}$.

We call a size-reduced basis $b_1,\ldots,b_{mk}$ *semi block $2k$-reduced* if properties (3.1)-(3.3) below hold. We call it *semi k-reduced* if only properties (3.2) and (3.3) hold.

$$C_i\leqslant\tfrac{4}{3}\beta_k^k C_{i+1} \quad \text{for } i=1,\ldots,m-1. \tag{3.1}$$

$$|b_{ik}^*|^2\leqslant 2|b_{ik+1}^*|^2 \quad \text{for } i=1,\ldots,m-1. \tag{3.2}$$

the k-blocks $b_{ik+j}(ik+1)$ for $j=1,\ldots,k$ are Korkine-Zolotareff reduced for $i=0.\ldots,m-1$. (3.3)

Every block $2k$-reduced basis is semi block $2k$-reduced. Every k-reduced basis is semi k-reduced. The presence of the numbers $\frac{4}{3}$ in (3.1) and 2 in (3.2) is to permit proving a polynomial time bound. We can replace $\frac{4}{3}$ by any number larger than 1, and 2 by any number larger than $\frac{4}{3}$. Two disjoint, reduced k-blocks can be linked either by property (3.1) or (3.2).

Theorem 3.1. *Every basis $b_1,\ldots,b_{mk}$ of lattice L which is semi block $2k$-reduced satisfies $|b_1|^2\leqslant 2\gamma_k\alpha_k(\frac{4}{3}\beta_k)^{m-2}\lambda(L)^2$.*

Proof. Let $v=\sum_j v_j b_j$ be a shortest lattice element. Set $\mu=\max\{j\mid v_j\neq 0\}$ and suppose $ik<\mu\leqslant(i+1)k$. By definition of γ_k we have for $i\geqslant 2$

$$|b_1|^2\leqslant\gamma_k D_1^{1/k}=\gamma_k C_1^{1/k}\leqslant\gamma_k(\tfrac{4}{3}\beta_k)^{i-2}C_{i-1}^{1/k},$$

where the last inequality derives from condition (3.1). Since $\alpha_j\leqslant\alpha_{j+1}$, it follows from (3.3) that $|b_{(i-1)k+j}|^*\leqslant\alpha_k|b_{ik}^*|^2$ for $1\leqslant j\leqslant k$,

$$C_{i-1}^{1/k}=\prod_{j=1}^{k}|b_{(i-1)k+j}^*|^{2/k}\leqslant\alpha_k|b_{ik}^*|^2.$$

On the other hand, using first (3.2) and then (3.3) we find

$$|b_{ik}^*|^2\leqslant 2|b_{ik+1}^*|^2\leqslant 2|v|^2=2\lambda(L)^2.$$

Thus, if $i\geqslant 2$, we have

$$|b_1|^2\leqslant 2\gamma_k\alpha_k(\tfrac{4}{3}\beta_k)^{m-2}\lambda(L)^2.$$

For $i=1$ the above argument shows $|b_1|^2\leqslant 2\gamma_k\alpha_k\lambda(L)^2$, and $|b_1|=\lambda(L)$ holds if $i=0$. □

Algorithm A for semi block $2k$-reduction of a basis $b_1, \ldots, b_{mk}$

(1) (*start*) For $i = 0, \ldots, m-1$ apply Korkine-Zolotareff reduction to the k-block $b_{ik+j}(ik+1)$ for $j = 1, \ldots, k$.

(2) (*next i*) Take the smallest $i < m$ that violates either (3.1) or (3.2) and stop if there is no such i.

(3) (*reduction step*) If $|b_{ik}^*|^2 > 2|b_{ik+1}^*|^2$, reduce b_{ik+1} in size, permute b_{ik} and b_{ik+1}, and apply Korkine-Zolotareff reduction to the two k-blocks $b_{s+j}(s+1)$, $j = 1, \ldots, k$, for $s = (i-1)k$ and $s = ik$.
If $C_i > \frac{4}{3}\beta_k^k C_{i+1}$, then apply Korkine-Zolotareff reduction to the $2k$-*block* $b_{s+j}(s+1)$, $j = 1, \ldots, k$ with $s = (i-1)k$.

(4) Go to (2).

An algorithm for Korkine-Zolotareff reduction of an integer lattice basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ is given in Section 4 (see Algorithm C). In Section 5 it is explained how to apply this algorithm for Korkine-Zolotareff reduction of a $2k$-block (k-block, respectively). We give a high-level description of this subroutine which will be analysed in Section 5.

Subroutine for Korkine-Zolotareff reduction of the $2k$-block $b_{s+j}(s+1)$, $j = 1, \ldots, 2k$

(1) Find a unimodular $2k \times 2k$ matrix H such that right multiplication of the matrix $[b_{s+j}(s+1), j = 1, \ldots, 2k]$ by H yields a Korkine-Zolotareff reduced basis. For this, use Algorithm C as described in Section 5.

(2) $[b_{s+j}, j = 1, \ldots, 2k] := [b_{s+j}, j = 1, \ldots, 2k]H$.

(3) Reduce $b_{s+1}, \ldots, b_{s+2k}$ in size.

The constants β_k that occur in Algorithm A are not known. However, Algorithm A performs sufficiently well, even if β_k is replaced by a reasonable upper bound for β_k. For instance, we can use the upper bound $4k^2$ from Theorem 2.7. For the performance analysis of Algorithm A we will use known upper bounds for β_k rather than the unknown value β_k.

The number of Korkine-Zolotareff block reductions in Algorithm A

We assume that the given lattice basis $b_1, \ldots, b_{mk} \in \mathbb{Z}^d$ is integer and generates a lattice of rank $n = mk$ contained in $\mathbb{R}^d$ with $d = O(n)$. We also assume a bound $B \in \mathbb{N}$ such that, initially, $|b_i|^2 \leq B$ holds for $i = 1, \ldots, n$, and thus, $C_i \leq B^k$, $D_i \leq B^{ik} \leq B^n$. The Gramian determinants $D_i = \det[\langle b_s, b_t \rangle_{1 \leq s,t \leq ik}] = |b_1^*|^2 \cdots |b_{ik}^*|^2$ are positive integers and all components of $b_l(j)$ with $l \leq ik$ are integer multiples of D_i^{-1}.

The old and new values corresponding to a reduction step satisfy $D_i^{\text{new}} \leq \frac{3}{4} D_i^{\text{old}}$, $D_j^{\text{new}} = D_j^{\text{old}}$ for $j \neq i$. In case $|b_{ik}^*|^2 > 2|b_{ik+1}^*|^2$, this follows from

$$|b_{ik}^{\text{new}*}|^2 \leq (\tfrac{1}{2} + \mu_{ik+1,ik}^2)|b_{ik}^{\text{old}*}|^2 \leq \tfrac{3}{4}|b_{ik}^{\text{old}*}|^2.$$

Since, initially, $D_j \leq B^n$ and, on termination, $D_j \geq 1$ holds for $j = 1, \ldots, m$, the number of reduction steps is at most $O(mn \log B)$ and thus the number of Korkine-Zolotareff reductions of k-blocks ($2k$-blocks, respectively) is at most $O((n^2/k) \log B)$.

The time bound

In Section 5 we will show that Algorithm A performs at most

$$O(n^2(\sqrt{k^{k+o(k)}}+n^2)\log B)$$

arithmetical steps on integers with at most $O(n \log B)$ bits. This gives the following theorem.

Theorem 3.2. *Semi block $2k$-reduction of a lattice basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ with $n = mk$, $d = O(n)$, $\max_i |b_i|^2 \leq B$ can be done with at most $O(n^2(\sqrt{k^{k+o(k)}}+n^2)\log B)$ arithmetic operations on $O(n \log B)$-bit integers.*

For fixed k the asymptotic time bound for semi block $2k$-reduction differs only by the constant factor k from the time bound for LLL-reduction. Korkine-Zolotareff reduction of a k-block with $k \leq 5$ is almost as easy as LLL-reduction of a k-block, see Algorithm D in Appendix A.

It is interesting to consider Algorithm A for large k. We choose k as to equalize the time bound of Algorithm A and the guaranteed bound on $|b_1|^2\lambda(L)^{-2}$.

Corollary 3.3. *For $k = \lfloor 2\sqrt{n} \rfloor$, semi block $2k$-reduction uses $n^{\sqrt{n}/2+o(\sqrt{n})}+O(n^4 \log B)$ arithmetic steps on $O(n \log B)$-bit integers and finds a lattice vector $b_1 \neq 0$ with $|b_1|^2\lambda(L)^{-2} = n^{\sqrt{n}/2+o(\sqrt{n})}$.*

Proof. The time bound follows from Theorem 3.2 and the bound for $|b_1|^2\lambda(L)^{-2}$ from Theorems 2.6 and 2.7. □

Theorem 3.4. *Every semi k-reduced basis $b_1, \ldots, b_{mk}$ of lattice L satisfies $|b_1|^2 \leq 2^{m-1}\alpha_k^m\lambda(L)^2$.*

Proof. We clearly have $\lambda(L)^2 \geq \min\{|b_s^*| \mid 1 \leq s \leq km\}$ and for $ik < s \leq (i+1)k$, we have

$$\begin{aligned}
|b_1|^2 &\leq \alpha_k|b_k^*|^2 && \text{(by (3.3))}\\
&\leq 2\alpha_k|b_{k+1}^*|^2 && \text{(by (3.2))}\\
&\leq (2\alpha_k)^i|b_{ik+1}^*|^2 && \text{(by induction)}\\
&\leq (2\alpha_k)^i\alpha_k|b_s^*|^2 && \text{(by (3.3)).}
\end{aligned}$$

Thus we obtain $|b_1|^2 \leq 2^{m-1}\alpha_k^m\lambda(L)^2$. □

Algorithm B for semi k-reduction of a basis $b_1, \ldots, b_{mk}$

(1) (*start*) For $i = 1, \ldots, m$, apply Korkine-Zolotareff reduction to the k-block $b_{ik+j}(ik+1), j = 1, \ldots, k$.

(2) (*reduction step*) While there exists an $i < m$ such that $|b_{ik}^*|^2 > 2|b_{ik+1}^*|^2$, reduce b_{ik+1} in size, permute b_{ik} and b_{ik+1}, and then apply Korkine-Zolotareff reduction to the two k-blocks $b_{s+j}(s+1), j = 1, \ldots, k$, for $s = (i-1)k$ and $s = ik$.

Comparing the performance of semi block 2k-reduction and of semi k-reduction

The time bound of Theorem 3.2 also holds for Algorithm B. Since Algorithm B applies block reduction to smaller and pairwise disjoint blocks, it uses simpler subroutines. The generated lattice bases have the following properties:

Algorithm A: The conditions (3.2), (3.3) imply (use Theorem 2.3)

$$\log(|b_1|^2/\lambda(L)^2) \leq (m-1)\log(2\alpha_k)$$

$$\leq \frac{n}{k}(1+\ln k)\log k + \frac{n}{k} \quad \text{(by Corollary 2.5)}$$

$$= O\left(\frac{n}{k}(\log k)^2\right).$$

Algorithm B: Properties (3.1), (3.2), (3.3) imply (use Theorem 2.1 and Corollary 2.5)

$$\log(|b_1|^2/\lambda(L)^2) \leq 1+\log\gamma_k + (1+\ln k)\log k + \frac{n}{k^2}\log(\tfrac{4}{3}\beta_k)$$

$$= O\left(\frac{n}{k^2}k\log k\right) = O\left(\frac{n}{k}\log k\right).$$

In particular, Corollary 3.3 for Algorithm B becomes: *For* $k = \lfloor 2\sqrt{n} \rfloor$, *semi k-reduction uses at most* $n^{\sqrt{n}/2+o(n)} + O(n^4 \log B)$ *arithmetic steps on* $O(n \log B)$*-bit integers and finds a nonzero lattice vector* b_1 *satisfying* $|b_1|^2/\lambda(L)^2 = n^{(\sqrt{n}/2)\log n + o(\sqrt{n})}$.

These asymptotic bounds favor Algorithm A to Algorithm B even when Algorithm B works on double length blocks. However, this may be misleading due to the weakness of the known upper bound on α_k. For instance, we have $\alpha_3 = \frac{3}{2}$ ($\sqrt{\frac{2}{3}}$ is the height of the tetrahedron with unit edge length), thus, by Theorem 3.4, Algorithm B for $k=3$ finds a basis with $|b_1|^2 \leq 3 \cdot 3^{n/3-1}\lambda(L)^2$.

Finally, let us compare Algorithms A and B for $k=3$ and LLL-reduction for the case that the technical constants in (2.3), (3.1) and (3.2) are replaced by the infimum of the admissible values. We obtain the following performance guarantees:

LLL-reduction with $\frac{4}{3}$ *in* (2.3) *replaced by* 1, *i.e.*, 2*-reduction*

$$|b_1|^2 \leq (\tfrac{4}{3})^{n-1}\lambda(L)^2 \leq 1.34^{n-1}\lambda(L)^2.$$

Algorithm B *for* $k=3$ *with constant* 2 *in* (3.2) *replaced by* $\frac{4}{3}$

$$|b_1|^2 \leq (\tfrac{4}{3}\cdot\tfrac{3}{2})\lambda(L)^2 \quad \text{by Theorem 3.4 and } \alpha_3 = \tfrac{3}{2}$$

$$\leq 2^{n/3}\lambda(L)^2 \leq 1.26^n\lambda(L)^2.$$

Algorithm A *for* $k=3$ *with constant* 1 *in* (3.1) *and* $\frac{4}{3}$ *in* (3.2)

$$|b_1|^2 \leq \tfrac{4}{2}\alpha_3\gamma_3\beta_3^{m-2}\lambda(L)^2 \qquad \text{by Theorem 3.1}$$

$$\leq 2\cdot 2^{1/3}(1.91)^{n/3-2}\lambda(L)^2 \qquad \text{since } \alpha_3 = \tfrac{3}{2},\ \gamma_3 = 2^{1/3},\ \beta_3 \leq 1.91$$

$$\leq (1.91)^{n/3}\lambda(L)^2 \qquad \text{by (2.6)}$$

$$\leq 1.24^n\lambda(L)^2.$$

This comparison indicates that Algorithm B outperforms Algorithm A for small values k.

4. An improved version of Kannan's algorithm for Korkine–Zolotareff reduction

Korkine–Zolotareff reduction is a main building block for semi block $2k$-reduction and for semi k-reduction. Kannan [8] has proposed an algorithm for reducing a lattice basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ in the sense of Korkine–Zolotareff which is polynomial time for fixed n. We present this algorithm along with some improvements to speed up running time and to reduce the bit length of integers used in the computation. The main modifications to Kannan's algorithm occur in steps (2) and (5) of Algorithm C.

Algorithm C for Korkine–Zolotareff reduction

(1) (*initiation*) Let $b_1, \ldots, b_n \in \mathbb{Z}^d$ be the given basis. Apply the Lovász algorithm for LLL-reduction (see Appendix A) to the basis $b_1, \ldots, b_n$ but use the technical constant 1.01 instead of $\frac{4}{3}$.

(2) (*recursion step*) Apply Korkine–Zolotareff reduction to the basis $b_2(2), \ldots, b_n(2)$ of L_2; apply all basis transformations of this process to the vectors $b_2, \ldots, b_n$ rather than to their projections. After each exchange $b_i \leftrightarrow b_{i+1}$, make sure that $|\mu_{i,j}| \leq \frac{1}{2}$ for $j = i-1, \ldots, 1$.

(3) If $|b_1|^2 > 2|b_2^*|^2$, then apply Korkine–Zolotareff reduction to b_1, b_2 via the Gaussian algorithm (see Appendix A). Go to (2).

(4) (*search for a shortest vector* $v = \sum_{i=1}^n v_i b_i$) Enumerate all nonzero integer vectors $(v_1, \ldots, v_n)$ that satisfy $0 \leq v_n < |b_1|/|b_n^*|$ and

$$\left(\sum_{k=j}^{n} v_k \mu_{k,j}\right)^2 \geq |b_j^*|^{-2}\left(|b_1|^2 - \sum_{\nu=j+1}^{n}\left(\sum_{k=\nu}^{n} v_k \mu_{k,\nu}\right)^2 |b_\nu^*|^2\right) \quad \text{for } j = n-1, \ldots, 1.$$

Choose $(v_1, \ldots, v_n)$ that minimizes

$$|v|^2 = \sum_{\nu=1}^{n}\left(\sum_{k=\nu}^{n} v_k \mu_{k,\nu}\right)^2 |b_\nu^*|^2.$$

If $|v| = |b_1|$, go to (6).

(5) (*extend v to a lattice basis*) Put $b_0 := v$, apply the Lovász algorithm (see Appendix A) to the linearly dependent system $b_0, b_1, \ldots, b_n$, run this algorithm until $b_0 = 0$ and take the current vectors $b_1, \ldots, b_n$ as new basis.

(6) Apply Korkine–Zolotareff reduction to the basis $b_2(2), \ldots, b_n(2)$ of lattice L_2; apply all basis transformations to the vectors $b_2, \ldots, b_n$ rather than to their projections. After each exchange $b_i \leftrightarrow b_{i+1}$, make sure that $|\mu_{i,j}| \leq \frac{1}{2}$ for $j = i-1, \ldots, 1$.

Proof of correctness. On termination, the basis $b_1, \ldots, b_n$ is Korkine–Zolotareff reduced since it starts with a shortest lattice vector b_1 (by steps (4) and (5)); by

step (6), the basis $b_2(2), \ldots, b_n(2)$ is Korkine-Zolotareff reduced and $|\mu_{i,1}| \leq \frac{1}{2}$ holds for $i = 2, \ldots, n$. Step (4) finds a shortest nonzero lattice vector v as is shown in Lemma 4.1 below. It remains to be shown that step (5) extends $b_0 = v$ to a lattice basis $v = b_1, \ldots, b_n$. The Lovász algorithm in step (5) exchanges $b_0 = v$ and b_1 iff $|b_0|^2 > \frac{4}{3}|b_1 - \lceil \langle b_0, b_1\rangle / \langle b_0, b_0\rangle \rfloor b_0|^2$, and since $|b_0| = \lambda(L)$, this holds iff $b_1 \in b_0\mathbb{Z}$. (Here $\lceil r \rfloor$ is the integer nearest to the real number r.) Thus, after the first exchange $v = b_0 \leftrightarrow b_1$, we have $b_0 = 0$ and step (5) terminates with a lattice basis $v = b_1, \ldots, b_n$.

Lemma 4.1 (Kannan). *Step (4) of Algorithm C finds a shortest nonzero lattice vector and terminates after at most $n^{n/2+o(n)}$ arithmetic steps.*

Proof. All lattice vectors $v = \sum_{i=1}^{n} v_i b_i$ shorter than b_1 satisfy

$$|v|^2 = \sum_{j=1}^{n} \left(\sum_{k=j}^{n} v_k \mu_{k,j} \right)^2 |b_k^*|^2 < |b_1|^2.$$

Therefore, the search for a shortest lattice vector v can be confined to integer vectors $(v_1, \ldots, v_n)$ satisfying

$$0 \leq v_n < |b_1|/|b_n^*|$$

and

$$\left(\sum_{k=j}^{n} v_k \mu_{k,j} \right)^2 |b_j^*|^2 < |b_1|^2 - \sum_{\nu=j+1}^{n} \left(\sum_{k=\nu}^{n} v_k \mu_{k,\nu} \right)^2 |b_\nu^*|^2 \quad \text{for } j = 1, \ldots, n-1.$$

Since $|\sum_{k=j}^{n} v_k \mu_{k,j}| < |b_1|/|b_j^*|$, the number of values for v_j when given $v_{j+1}, \ldots, v_n$ is at most $\lfloor 2|b_1|/|b_j^*| \rfloor + 1$. Thus, at most

$$|b_1|/|b_n^*| \prod_{j=2}^{n-1} (\lfloor 2|b_1|/|b_j^*| \rfloor + 1)$$

choices for $(v_1, \ldots, v_n)$ need to be tested when searching for v. Following Kannan we perform the search for a shortest lattice vector v only when $|b_1|^2 \leq 2|b_2^*|^2$. To bound from above in this case the number of choices for $(v_1, \ldots, v_n)$, we assume, w.l.o.g., that $|b_j^*| < |b_1|$ for $j = 2, \ldots, n$ since otherwise $v_j = v_{j+1} = \cdots = v_n = 0$. This implies that the above number of choices for $(v_1, \ldots, v_n)$ is at most

$$3^{n-2} \prod_{j=1}^{n} \frac{|b_1|}{|b_j^*|} \leq 3^{n-2} (\sqrt{2}\lambda(L_2))^{n-1} \, d(L_2)^{-1}.$$

By definition of the Hermite constant γ_{n-1} we have the upper bound

$$\leq (18\gamma_{n-1})^{(n-1)/2} = \sqrt{n}^{\,n+o(n)}$$

since $\lim_n \sup \gamma_n / n \leq (e\pi)^{-1}$. From this we see that step (4) finds a shortest lattice vector v using $\sqrt{n}^{\,n+o(n)}$ arithmetic operations. □

Time analysis

Let λ be the first successive minimum of the lattice generated by $b_1, \ldots, b_n$.

Lemma 4.2. *Each pass through steps* (2), (3) *achieves* $|b_1^{\text{new}}|/\lambda \leq (\frac{4}{3})^{1/4}\sqrt{|b_1^{\text{old}}|/\lambda}$, *and steps* (2), (3) *are passed at most* $\lceil \log_2(n-1) \rceil + 2$ *times. Hence, step* (5) *is passed at most* $(\log_2 n)^{n+o(n)}$ *times throughout all recursive calls of Algorithm* C.

Proof. Let $b_1^{\text{old}}, b_2^{\text{old}}$ be the vectors b_1, b_2 upon entry of step (2). If $|b_1^{\text{old}}| > \lambda$, then Korkine-Zolotareff reduction in step (2) replaces b_2^{old} by a vector b_2 satisfying $|b_2^*| = \lambda_1(L_2) \leq \lambda$. Korkine-Zolotareff reduction in step (3) is applied to the basis b_1^{old}, b_2 of the lattice $L' := b_1^{\text{old}}\mathbb{Z} + b_2\mathbb{Z}$. Thus, step (3) finds a vector b_1^{new} satisfying

$$|b_1^{\text{new}}|^2 = \lambda_1(L')^2 \leq \gamma_2 \, d(L') = \sqrt{\tfrac{4}{3}}|b_1^{\text{old}}||b_2^*|.$$

Since $|b_2^*| \leq \lambda$ this implies $|b_1^{\text{new}}|/\lambda \leq (\frac{4}{3})^{1/4}\sqrt{|b_1^{\text{old}}|/\lambda}$.

Initially, when entering step (2) for the first time, we have by LLL-reduction in step (1) using the constant 1.01 instead of $\frac{4}{3}$:

$$|b_1|/\lambda \leq 1.352^{(n-1)/2} \quad \text{(by (A.3))}.$$

After passing steps (2), (3) m times, this yields

$$|b_1|/\lambda \leq 1.352^{(n-1)2^{-m-1}}(\tfrac{4}{3})^{(1+2^{-1}+\cdots+2^{-m})/4};$$

thus, after $\lceil \log_2(n-1) \rceil - 1$ passes, we have

$$|b_1|/\lambda \leq 1.352 \cdot (\tfrac{4}{3})^{1/2}.$$

To show that there are at most 3 more passes, we note that each pass decreases $|b_1|$ by at least a factor $(\frac{4}{3})^{1/2}$ and we have $1.352 < (\frac{4}{3})^{1.5}$. (In fact, each pass achieves

$$|b_1^{\text{new}}|^2 = |b_2^*|^2 + \mu_{2,1}^2|b_1^{\text{old}}|^2 \leq |b_2^{\text{old}^*}|^2 + \mu_{2,1}^2|b_1^{\text{old}}|^2 \leq (\tfrac{1}{2}+\tfrac{1}{4})|b_1^{\text{old}}|^2).$$

Thus, steps (2), (3) are passed at most $\lceil \log_2(n-1) \rceil + 2$ times. □

The number of arithmetic operations

We bound the number of arithmetic operations executed by Algorithm C on input bases $b_1, \ldots, b_n \in \mathbb{Z}^d$ with $|b_1|^2, \ldots, |b_n|^2 \leq B$. We partition the operations into two classes:

(1) $T_1(n)$ counts the operations executed within LLL-reduction and Korkine-Zolotareff reduction of steps (1), (3) and (5) including these same operations in the recursive calls of Korkine-Zolotareff reduction in steps (2) and (6).

(2) $T_2(n)$ counts the operation of step (4) including these same operations in the recursive calls of Korkine-Zolotareff reduction in steps (2) and (6).

- $T_2(n)$: We have

$$T_2(n) \leq \lceil 3 + \log_2 n \rceil T_2(n-1) + \sqrt{n^{n+o(n)}}.$$

Here $2 + \lceil \log_2 n \rceil$ bounds the number of passes through steps (2) and (3); $T_2(n-1)$ is a time bound for steps (2) and (6); $\sqrt{n^{n+o(n)}}$ bounds the number of operations of step (4) as has been shown above. The recursion formula yields $T_2(n) = \sqrt{n^{n+o(n)}}$.

- $T_1(n)$: The progress of the reduction process is related to the number

$$D := \prod_{i=1}^{n} |b_i^*|^{2(n-i)}.$$

Each exchange step $b_{k-1} \leftrightarrow b_k$ of the Lovász algorithm decreases D by at least a faactor 1.01^{-1}. The value of D can only increase in step (5) during LLL-reduction of the linearly dependent system $b_0, b_1, \ldots, b_n$. To keep track of this increase we take in step (5) a slightly different invariant $\bar{D}$ defined by

$$\bar{D} := \prod_{\substack{i=0 \\ \text{and } b_i^+ \neq 0}}^{n} |b_i^+|^{2(n-r_i)}$$

where b_i^+ is the component of b_i that is orthogonal to $b_0, \ldots, b_{i-1}$ and $r_i = \#\{j \mid b_j^+ \neq 0, 0 \leq j \leq i\}$. Since $b_\nu^+ = 0$ holds for exactly one ν, we have for this ν

$$r_i = \begin{cases} i+1 & \text{for } i < \nu, \\ i & \text{for } i > \nu. \end{cases}$$

Each exchange step $b_{k-1} \leftrightarrow b_k$ of the Lovász algorithm in step (5) decreases $\bar{D}$ by at least a factor $\frac{3}{4}$ as has been shown in [5, Lemma 2].

On termination of step (5) we have $b_0 = 0$ and thus $\bar{D}$ and D coincide. We show that

$$\bar{D} \leq 2^{n^2} D \tag{4.1}$$

holds upon entry of step (5).

To prove inequality (4.1) we note that

$$|b_0| \leq |b_1|, \qquad |b_i^+|^2 \leq |b_i^*|^2 \leq 2|b_{i+1}^*|^2 \quad \text{for } i = 1, \ldots, n-1.$$

Let $b_\nu^+ = 0$; then

$$|b_i^+|^{2(n-r_i)} \leq |b_i^*|^{2(n-i-1)} \leq (2|b_{i+1}^*|^2)^{n-i-1} \quad \text{for } i < \nu,$$

$$|b_i^+|^{2(n-r_i)} \leq |b_i^*|^{2(n-i)} \quad \text{for } i > \nu.$$

We obtain inequality (4.1) by multiplying the latter inequalities for $i = 0, \ldots, \nu-1, \nu+1, \ldots, n$.

Upon entry of Algorithm C we have $D \leq B^{n^2}$ and $D \geq 1$ on termination. Each exchange step of the Lovász algorithm decreases D by at least a factor 1.01^{-1}. Each pass of step (5) increases D by at most a factor $\leq 2^{n^2}$. It follows from Lemma 4.2 that the total number of passes of step (5) within all recursive calls of Korkine-Zolotareff reduction is at most $(\log n)^{n+o(n)}$. Therefore, the total number of exchange steps $b_{k-1} \leftrightarrow b_k$ made in Algorithm C is at most

$$O(n^2 \log B) + (\log n)^{n+o(n)}.$$

If $d = O(n)$, then each exchange step costs $O(n^2)$ arithmetic operations for size-reduction and thus

$$T_1(n) = O(n^4 \log B) + (\log n)^{n+o(n)}.$$

Combining the bounds for $T_1(n)$ and $T_2(n)$ we see that Algorithm C uses at most

$$\sqrt{n}^{n+o(n)} + O(n^4 \log B)$$

arithmetic steps.

The size of the integers involved

Algorithm C executes a sequence of Lovász reduction steps which either transform the current lattice basis $b_1, \ldots, b_n$ or in step (5) a linearly dependent set of $n+1$ generators of the lattice. Throughout these exchange steps we have by formulae (1.30)-(1.34) of [13]

$$|\mu_{i,j}| \leq 2^n (nB)^{(n-1)/2} \tag{4.2}$$

$$|b_i| \leq n^2 (4B)^n, \tag{4.3}$$

where B is a number such that $\max |b_i|^2 \leq B$ holds for the input basis $b_1, \ldots, b_n$. These bounds have been proved for the Lovász algorithm when working on a basis of the lattice but they also hold when the Lovász algorithm transforms a set of generators of the lattice. The bounds (4.2) and (4.3) hold throughout Algorithm D (see Appendix A). An exchange $b_i \leftrightarrow b_{i+1}$ is only performed when

$$|b_j^*|^2 \leq 2|b_{j+1}^*|^2 \text{ holds for } j = 1, \ldots, i-1,$$

and after an exchange $b_i \leftrightarrow b_{i+1}$ we make sure that $|\mu_{i,j}| \geq \frac{1}{2}$ holds for $j = 1, \ldots, i$.

We see from the above bounds that throughout the execution of Algorithm C the numerator and denominator of the rational number $|\mu_{i,j}|^2$ have at most $O(n \log B)$ bits. Therefore, all integers within execution of Algorithm C have at most $O(n \log B)$ bits.

So far we have proved the following theorem.

Theorem 4.3. *Let $b_1, \ldots, b_n \in \mathbb{Z}^d$ be a lattice basis with $|b_1|^2, \ldots, |b_n|^2 \leq B$, $d = O(n)$. Then Korkine-Zolotareff reduction is done via Algorithm C with at most $\sqrt{n}^{n+o(n)} + O(n^4 \log B)$ arithmetic operations on $O(n \log B)$-bit integers.*

Remarks. We have improved Kannan's algorithm and his analysis in several ways.

(i) Korkine-Zolotareff reduction of b_1, b_2 in step (3) is more efficient than a simple exchange $b_1 \leftrightarrow b_2$. The number of recursive Korkine-Zolotareff reductions of lattices of rank $n-1$ in Algorithm C is at most $\lceil \log_2 n \rceil + 2$ whereas it may be $\frac{5}{2}n$ in Kannan's algorithm.

(ii) Since our algorithm in step (5) executes a sequence of LLL-reduction steps on the current basis $b_1, \ldots, b_n$ we obtain an $O(n \log B)$ bound on the bit length of the integers occurring in the algorithm, whereas Kannan only proves a $O(n^2 \log B)$ bound.

(iii) We can decrease the bit length of the integers used by Algorithm C from $O(n \log B)$ to $O(n + \log B)$ by replacing the Lovász reduction algorithm by the reduction algorithm in [17]. This algorithm reduces an integer lattice basis $b_1, \ldots, b_n$ such that $|\mu_{i,j}| \leq 0.55$ holds for $1 \leq j < i \leq n$ and property (2.3) is satisfied. If the input basis vectors have length at most B, the algorithm terminates after at most $O(n^4 \log B)$ arithmetic steps on $O(n + \log B)$-bit integers.

(iv) The improved time bound for Korkine-Zolotareff reduction also improves the time bounds for the closest vector problem and for integer programming. In the

closest vector problem we are given an integer lattice basis $b_1, \ldots, b_n \in \mathbb{Z}^n$ and a rational point $b \in \mathbb{Q}^n$; we search for a lattice vector with minimal Euclidean distance to b. In integer programming we are given $m \times n$ and $m \times 1$ integer matrices A and b and we decide whether there is an integer vector $x \in \mathbb{Z}^n$ such that $Ax \leq b$. Each of these problems can be solved via Algorithm C using at most $n^{O(n)} + O(n^4 \log B)$ arithmetic steps on integers with polynomial length. This follows from corresponding algorithms in [8] and [3] which solve these problems via Korkine-Zolotareff reduction.

5. The time bound for semi block $2k$-reduction and for semi k-reduction

The unimodular transformations occurring in Korkine-Zolotareff subroutines

We consider the application of Korkine-Zolotareff reduction as a subroutine in Algorithms A and B. During Korkine-Zolotareff reduction of a k-block $b_{ik+j}(ik+1)$, $j = 1, \ldots, k$, the algorithm does not update the current block $b_{ik+1}, \ldots, b_{ik+k}$. Instead, it updates the numbers $\mu_{ik+\nu,ik+j}$ for $1 \leq j < \nu \leq k$, $|b^*_{ik+\nu}|^2$ for $\nu = 1, \ldots, k$ and the unimodular $k \times k$-matrix H that transforms the input block to the current block, i.e.,

$$[b^{\text{cur}}_{ik+1}, \ldots, b^{\text{cur}}_{ik+k}] = [b_{ik+1}, \ldots, b_{ik+k}]H.$$

Initially, $H = \mathrm{I}$ and each LLL-reduction step operates on H via multiplication from the right by the matrix

$$\begin{matrix} & & & & & & \nu, \nu+1 & & \\ \end{matrix}$$

$$\begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{bmatrix} \quad \text{for an exchange } b_{ik+\nu} \leftrightarrow b_{ik+\nu+1}$$

$$\begin{matrix} & & & & & & \nu & & \\ \end{matrix}$$

$$\begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & \ddots & & & & & \\ & & & \ddots & r & & & \\ & & & & \ddots & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ j \end{matrix} \quad \text{for a step } b_{ik+\nu} := b_{ik+\nu} + r b_{ik+j}.$$

When Algorithm C in step (5) extends the current basis by a shortest lattice vector $v = b_0$, the matrix H is extended by the Oth column with the coordinates of b_0. On termination of step (5) we have $b_0 = 0$ and the Oth column is eliminated from H. On termination of block reduction the new basis vectors are obtained by the matrix multiplication $[b_{ik+1}, \ldots, b_{ik+k}] := [b_{ik+1}, \ldots, b_{ik+k}]H$.

The additional arithmetic operations for updating the matrix H do not change the order of the time bound of Algorithm C. The entries of the matrix H have at most $O(n \log B)$ bits as is shown in the following lemma for the case $k = n$.

Lemma 5.1. *Let Algorithm C be given an input basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ with $|b_1|^2, \ldots, |b_n|^2 \leq B$. Then the transformation matrix H satisfies $\|H\| \leq n^{3.5} 2^n B^{(n+1)1.5}$ throughout the computation.*

Here H is the matrix that transforms the input basis $b_1, \ldots, b_n$ into the current basis, i.e., $[b_1^{\text{cur}}, \ldots, b_n^{\text{cur}}] = [b_1, \ldots, b_n]H$, and $\|H\|$ is the maximal absolute value of the entries of H.

Proof. The input basis $b_1, \ldots, b_n$ satisfies the equation

$$[b_1, \ldots, b_n] = [b_1^*, \ldots, b_n^*]M^{\mathsf{T}}$$

where the $(n \times n)$-matrix M has entries $\mu_{i,j}$. At any stage of Algorithm C the current basis satisfies a corresponding equation

$$[b_1^{\text{cur}}, \ldots, b_n^{\text{cur}}] = [b_1^{\text{cur}*}, \ldots, b_n^{\text{cur}*}]M_{\text{cur}}^{\mathsf{T}}.$$

It follows from

$$[b_1^{\text{cur}}, \ldots, b_n^{\text{cur}}] = [b_1, \ldots, b_n]H$$

and the two previous equations that

$$[\langle b_i^*, b_j^{\text{cur}*}\rangle |b_i^*|^{-2}]_{1 \leq i,j \leq k} M_{\text{cur}}^{\mathsf{T}} = M^{\mathsf{T}} H.$$

This implies

$$\|H\| \leq \|M^{-1}\| \max_{i,j} |\langle b_i^*, b_j^{\text{cur}*}\rangle |b_i^*|^{-2}| \, \|M_{\text{cur}}\| n^2. \tag{5.1}$$

We have $|b_j^{\text{cur}*}|^2 \leq B$ since $\max_i |b_i^*|$ does not increase. The inequality $|b_i^*|^2 \geq B^{-i}$ follows from $\max_i |b_i|^2 \leq B$. So we see

$$|\langle b_i^*, b_j^{\text{cur}*}\rangle| |b_i^*|^{-2} \leq |b_j^{\text{cur}*}| |b_i^*|^{-1} \leq B^{(i+1)/2}. \tag{5.2}$$

From the definition of the matrix M we see

$$\|M^{-1}\| \leq n \|[b_1, \ldots, b_n]^{-1}\| \, \|[b_1^*, \ldots, b_n^*]\|.$$

We have $\|[b_1, \ldots, b_n]^{-1}\| \leq B^{n/2}$ from $|b_i^*|^2 \leq B$ and thus $|b_i^*|^2 \leq B$ implies

$$\|M^{-1}\| \leq nB^{(n+1)/2}. \tag{5.3}$$

It remains to bound the entries $\mu_{i,j}^{\text{cur}}$ of M_{cur}. During LLL-reduction of a basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ with $|b_1|^2, \ldots, |b_n|^2 \leq B$, the numbers $\mu_{i,j}^{\text{cur}}$ are bounded as $|\mu_{i,j}^{\text{cur}}| \leq 2^n (nB^{n-1})^{1/2}$, see [13, formulae (1.32)–(1.34)]. This bound also holds when the Lovász algorithm, in step (5) of Algorithm C, transforms a linearly dependent generator system of the lattice. Thus $\|M_{\text{cur}}\| \leq 2^n (nB^{n-1})^{1/2}$ holds throughout Algorithm C.

From this and from the inequalities (5.1)-(5.3), we conclude $\|H\| \leq n^{3.5}2^n B^{(n+1)1.5}$. □

The size of the integers involved in Algorithms A and B

All integers occurring throughout the computation have at most $O(n \log B)$ bits. This holds for the integers occurring within LLL-reduction by the analysis in [13] for the integers occurring within Korkine-Zolotareff reduction by Theorem 4.2, and for the entries of the matrix H by Lemma 5.1. Also, throughout the computation, $\max_{j \leq i}|b_j^*|$ does not increase, and thus $|b_j|^2 \leq nB$ always holds after reducing b_j in size.

The time bound for Algorithms A and B. Proof of Theorem 3.2

We analyse the running time of Algorithm A. Korkine-Zolotareff reduction of a k-block ($2k$-block, respectively) occurs in the initial and in the reduction step of Algorithm A. Using Algorithm C this subroutine can be done within

$$k^{k/2+o(k)} + O(k^4 \log B) + O(k^2 n) + O(n^2 k) \tag{5.4}$$

arithmetical steps on $O(n \log B)$-bit integers. The first two terms count the operations for Algorithm C; they also count the operations for updating the unimodular matrix H which describes the block transformation. $O(k^2 n)$ operations are needed for multiplying the block vectors with H and $O(n^2 k)$ arithmetic steps are used for size-reduction of the block vectors after block reduction. We have seen in Section 3 that the number of subroutines for Korkine-Zolotareff block reduction throughout Algorithm A is at most $O((n^2/k) \log B)$.

We next show that the costs counted by the $O(k^4 \log B)$ term in (5.4) are majorized by the other costs when summing up over the $O((n^2/k) \log B)$ block subroutines in Algorithm A. The $O(k^4 \log B)$ term partly covers the costs for the exchange steps during block reduction. To prove the claim we analyse these costs in more detail. Upon entry of Algorithm A we have $D = \prod_{i=1}^{n} |b_i^*|^{2(n-i)} \leq B^{n^2}$ and $D \geq 1$ holds on termination. Each exchange $b_i \leftrightarrow b_{i+1}$ reduces D by at least a factor $\frac{4}{3}$ (1.01, respectively). We see from inequality (4.1) that D increases at most by a factor 2^{k^2} when Algorithm A during Korkine-Zolotareff reduction of a k-block enters step (5) of Algorithm C. Step (5) of Algorithm C is passed at most $(\log k)^{k+o(k)}$ times during Korkine-Zolotareff reduction of a k-block (this follows from Lemma 4.1). From these bounds we see that there are at most

$$O\left(n^2 \log B + (\log k)^{k+o(k)} \frac{n^2}{k} k^2 \log B\right)$$

exchange steps $b_i \leftrightarrow b_{i+1}$ over all block subroutines of Algorithm A. Each exchange step costs $O(k^2)$ arithmetic steps for updating the numbers μ_{ij} corresponding to the block. Therefore, all exchange steps within block subroutines of Algorithm A cost at most

$$O((\log k)^{k+o(k)} + k^3)(n^2 \log B)$$

arithmetic steps. It now follows from (5.4) that the $O((n^2/k)\log B)$ block subroutines of Algorithm A cost at most

$$O(n^4 \log B + k^{k/2+o(k)} n^2 \log B)$$

arithmetical steps on $O(n \log B)$-bit integers. This bound also covers the costs for all the other steps of Algorithm A and thus proves Theorem 3.2.

The same running time analysis carries over to Algorithm B.

Appendix A. Reduction algorithms

For completeness of the paper we include an outline of the basis reduction algorithm in [13] and explain its relation to the Gaussian algorithm for the reduction of rank 2 lattice bases. We also include a practical algorithm for Korkine-Zolotareff reduction of lattices of rank at most 5.

The Gaussian algorithm transforms a basis $b_1, b_2 \in \mathbb{R}^d$ into a basis of the same lattice that satisfies the reduction conditions (A.1) and (A.2).

$$|\mu_{2,1}| \leq \tfrac{1}{2}, \tag{A.1}$$

$$|b_1| \leq |b_2|. \tag{A.2}$$

The Gaussian algorithm (for Korkine–Zolotareff reduction of rank 2 lattice bases)
(1) $b_2 := b_2 - \lceil \langle b_2, b_1 \rangle |b_1|^{-2} \rfloor b_2$.
(2) If $|b_1| > |b_2|$, then (exchange b_1 and b_2, go to (1)); otherwise terminate.

Here $\lceil a \rfloor$ denotes the integer nearest to the real number a and $\langle b_2, b_1 \rangle |b_1|^{-2} = \mu_{2,1}$. On an integer input basis $b_1, b_2 \in \mathbb{Z}^d$ with length bound $|b_1|^2, |b_2|^2 \leq B$, the Gaussian algorithm takes at most $O(\log B)$ iterations, see [11].

The Lovász reduction algorithm successively applies Gaussian reduction to 2-blocks $b_{k-1}(k-1)$, $b_k(k-1)$. We outline this algorithm and omit the details to compute and to update the numbers $\mu_{i,j}$, $|b_{k-1}^*|$ and $|b_k(k-1)|$. The Lovász algorithm transforms an integer lattice basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ into an LLL-reduced basis, i.e., a basis that satisfies (2.1) and (2.2).

The Lovász algorithm for LLL-reduction of rank n lattice bases
(1) (*initiation*) $k := 2$.
(2) $b_k := b_k - \lceil \mu_{k,k-1} \rfloor b_{k-1}$.
(3) (*exchange step*) If $|b_{k-1}^*|^2 > \frac{4}{3}|b_k(k-1)|^2$, then (exchange b_k, b_{k-1}; if $k > 2$, then $k := k-1$, and go to (2)).
(4) For $j = k-2, \ldots, 1$ do $b_k := b_k - \lceil \mu_{k,j} \rfloor b_j$.
(5) If $k < n$, then ($k := k+1$, go to (2)); otherwise terminate.

For practical purposes the constant $\frac{4}{3}$ in step (3) should be replaced by 1.01. Then an exchange step achieves

$$|b_k^*|^2 = |b_k(k-1)|^2 - \mu_{k,k-1}^2 |b_{k-1}^*|^2 \geq (1.01^{-1} - 0.25)|b_{k-1}^*|^2.$$

Hence, we have, on termination of the Lovász algorithm,

$$|b_k^*|^2 < 1.352 |b_{k-1}^*|^2 \quad \text{for } k = 1, \ldots, n. \tag{A.3}$$

Algorithm D for Korkine–Zolotareff reduction of a basis with rank $n \leq 5$

(1) (*initiation*) Let $b_1, \ldots, b_n \in \mathbb{Z}^d$, $n \leq 5$, be the given lattice basis; $s := 1$.

(2) Apply LLL-reduction to the basis $b_s(s), \ldots, b_n(s)$ but use the technical constant 1.01 instead of $\frac{4}{3}$. Apply all basis transformations during this reduction to the vectors $b_s, \ldots, b_n$ rather than to their projections. (On termination we have $|b_i^*|^2 \leq 1.01\ |b_{i+1}(i)|^2$ and $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$, $\mu_{i,i} = 1$.)

(3) Reduce $b_s, \ldots, b_n$ in size.

(4) (*search for a shortest vector* $v(s) \in L_s$, $v = \sum_{j=s}^{n} v_j b_j$) For $t = n, n-1, \ldots, s+1$ enumerate all integer vectors $(v_s, \ldots, v_t)$ that satisfy $v_t = 1$ and, for $j = t-1, \ldots, s$,

$$\left| \sum_{k=j}^{t} v_k \mu_{k,j} \right| < \begin{cases} 1.32 & j = 4, \\ 1.14 & j = 3, \\ 0.98 & j = 2, \\ 0.84 & j = 1. \end{cases}$$

Choose $t, v_s, \ldots, v_t$ that minimizes

$$|v(s)|^2 = \sum_{j=s}^{t} \left(\sum_{\nu=j}^{t} v_\nu \mu_{\nu,j} \right)^2 |b_j^*|^2.$$

If $|v(s)| = |b_s^*|$ go to (6).

(5) $v := \sum_{i=s}^{t} v_i b_i$, $(b_s, b_t) := (v, b_s)$. If $s = n-1$, then $(b_n := b_n - \lceil \mu_{n,n-1} \rfloor b_{n-1}$ and terminate).

(6) $s := s+1$ go to (2).

Correctness of Algorithm D

Correctness of step (4): We show that a shortest vector $v(s)$ in L_s is found. Let $v = \sum_{\nu=1}^{n} v_\nu b_\nu$ be a shortest lattice vector and $t := \max\{\nu \mid |v_\nu| \neq 0\}$. Then we have

$$|b_1|^2 \geq |v|^2 \geq v_t^2 |b_t^*|^2 \geq v_t^2\ 1.352^{-t+1} |b_1|^2$$

by (A.3), and thus $v_t^2 < 4$; hence, $|v_t| = 1$. We can assume that $v_t = 1$; otherwise we replace v by $-v$. The integers $v_t, \ldots, v_1$ satisfy, for $j = t-1, \ldots, 1$,

$$\left(\sum_{\nu=j}^{t} v_\nu \mu_{\nu,j} \right)^2 |b_j^*|^2 \leq |b_1|^2 - |b_t^*|^2 \leq |b_1|^2 (1 - 1.352^{-4}),$$

hence

$$\left(\sum_{\nu=j}^{t} v_\nu \mu_{\nu,j} \right)^2 \leq 0.701 \cdot |b_1|^2 |b_j^*|^{-2} \leq 0.701 \cdot 1.352^{j-1},$$

and therefore,

$$\left|\sum_{\nu=j}^{t} v_\nu \mu_{\nu,j}\right| \leqslant \begin{cases} 1.32 & j=4, \\ 1.14 & j=3, \\ 0.98 & j=2, \\ 0.84 & j=1. \end{cases}$$

The number of possible choices for $(v_t, \ldots, v_1)$ is at most $3^2 2^2 = 36$ for $t=5$, $3 \cdot 2^2 = 12$ for $t=4$, 4 for $t=3$, and 2 for $t=2$. The total number of integer vectors $(v_1, \ldots, v_n)$ that are to be checked for dimension $n=5$ and $s=1$ is at most 54.

Correctness of step (5): since $v_t = 1$, b_t is an integer combination of $v = \sum_{i=s}^{t} v_i b_i$ and $b_s, \ldots, b_{t-1}$. Therefore, the transformation of step (5) yields a new basis $b_1, \ldots, b_n$ of the original lattice.

Time analysis

Suppose the input basis $b_1, \ldots, b_n \in \mathbb{Z}^d$ satisfies $|b_1|^2, \ldots, |b_n|^2 \leqslant B$ and $d = O(n)$. For fixed n, the LLL-algorithm runs in $O(\log B)$ arithmetic operations on $O(\log B)$-bit integers. Algorithm C for $t = n, n-1, \ldots, 2$ applies LLL-reduction to a basis of dimension t. To count the additional operations of step (4) we note that, for $s=1$, there at at most $36+12+4+2=54$ distinct integer vectors $(v_1, \ldots, v_t)$ to be checked for $t=4, 3, 2, 1$. The total number of integer vectors $(v_s, \ldots, v_t)$ that are checked in the stages $s = 1, 2, \ldots, n-1$ of Algorithm C is at most $54+18+6+2=80$. This proves the following proposition.

Proposition A.1. *Algorithm D applies Korkine-Zolotareff reduction to a basis* $b_1, \ldots, b_n \in \mathbb{Z}^d$ *with* $n \leqslant 5$. *If* $|b_1|^2, \ldots, |b_n|^2 \leqslant B$, *it uses at most* $O(d \log B)$ *arithmetic operations on* $O(\log B)$*-bit integers.*

Acknowledgment

I wish to thank the unknown referee for his or her comments.

References

[1] J.W.S. Cassels, *An Introduction to the Geometry of Numbers* (Springer, Berlin, 1971).

[2] P. van Emde Boas, Another NP-complete problem and the complexity of computing short vectors in a lattice, Tech. Rept., University Amsterdam, No. 81-04 (1981).

[3] A. Frank and E. Tardos, An application of simultaneous approximation in combinatorial optimization, Report, Universität Bonn (1985).

[4] C.F. Gauss, *Disquisitiones Arithmeticae* (Leipzig, 1801) German translation: *Untersuchungen über höhere Arithmetik* (Springer, Berlin, 1889) (reprints: Chelsea, New York, 1981).

[5] J. Hastad, B. Just, J.C. Lagarias and C.P. Schnorr, Polynomial time algorithms for finding integer relations among real numbers, in: *Proc. 3rd STACS 86, Symp. on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science **210** (Springer, Berlin, 1985) 105-118.

[6] B. Helfrich, Algorithms to construct Minkowski reduced and Hermite reduced lattice bases, *Theoret. Comput. Sci.* **41** (1985) 125-139.

[7] Ch. Hermite, Second letter to Jacobi, *Crelle Journal* **40** (1850) 279-290 (in French).

[8] R. Kannan, Improved algorithms for integer programming and related lattice problems, in: *Proc. 15th Ann. ACM Symp. on Theory of Computing* (1983) 193-206.

[9] A. Korkine and G. Zolotareff, Sur les forms quadratiques, *Math. Annalen* **6** (1873) 366-389.

[10] J.C. Lagarias, Worst case complexity bounds for algorithms in the theory of integral quadratic forms, *J. Algorithms* **1** (1980) 142-186.

[11] J.C. Lagarias, H.W. Lenstra, Jr. and C.P. Schnorr, Korkine-Zolotareff bases and successive minima of a lattice and its reciprocal lattice, Tech. Rept., MSRI 07718-86, Mathematical Sciences Research Institute, Berkeley.

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

[13] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Math. Annalen* **261** (1982) 515-534.

[14] L. Lovász, An algorithmic theory of numbers, graphs and convexity, Tech. Rept., Universität Bonn.

[15] H. Minkowski, Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen, *Crelles Journal für die reine und angewandte mathematik* **107** (1891) 278-297.

[16] A.M. Odlyzko and H. te Riele, Disproof of the Mertens conjecture, *Journal für die reine und angewandte Mathematik* **357** (1985) 138-160.

[17] C.P. Schnorr, A more efficient algorithm for lattice basis reduction (extended abstract), in: *Proc. 13th Coll. on Automata, Languages and Programming*, Rennes 1986, Lecture Notes in Computer Science **226** (Springer, Berlin, 1986) 359-369; complete version to appear in *J. Algorithms* (December 1987).

[18] A. Schönhage, Factorization of univariate integer polynomials by diophantine approximation and by an improved basis reduction algorithm, in: *Proc. 11th Coll. on Automata, Languages and Programming*, Antwerpen 1984, Lecture Notes in Computer Science **172** (Springer, Berlin, 1984).