COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 13 (3) (1993) 363–376

SIMULTANEOUS REDUCTION OF A LATTICE BASIS AND ITS RECIPROCAL BASIS

M. SEYSEN

Received July 23, 1990
Revised August 7, 1991

Given a lattice L we are looking for a basis $\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]$ of L with the property that both $\mathbf{B}$ and the associated basis $\mathbf{B}^*=[\mathbf{b}_1^*,\ldots,\mathbf{b}_n^*]$ of the reciprocal lattice L^* consist of short vectors. For any such basis $\mathbf{B}$ with reciprocal basis $\mathbf{B}^*$ let $S(\mathbf{B})=\max\limits_{1\le i\le n}(|\mathbf{b}_i|\cdot|\mathbf{b}_i^*|)$. Håstad and Lagarias [7] show that each lattice L of full rank has a basis $\mathbf{B}$ with $S(\mathbf{B})\le\exp(c_1\cdot n^{1/3})$ for a constant c_1 independent of n. We improve this upper bound to $S(\mathbf{B})\le\exp(c_2\cdot(\ln n)^2)$ with c_2 independent of n.

We will also introduce some new kinds of lattice basis reduction and an algorithm to compute one of them. The new algorithm proceeds by reducing the quantity $\sum\limits_{i=1}^{n}|\mathbf{b}|^2\cdot|\mathbf{b}_i^*|^2$. In combination with an exhaustive search procedure, one obtains an algorithm to compute the shortest vector and a Korkine–Zolotarev reduced basis of a lattice that is efficient in practice for dimension up to 30.

1. Introduction and notation

In this paper we study n-dimensional lattices of full rank. A lattice (of full rank) is the additive subgroup $\sum\limits_{i=1}^{n}\mathbf{b}_i\mathbb{Z}$ generated by a basis $\mathbf{B}=[\mathbf{b}_1,\ldots,\mathbf{b}_n]$ of $\mathbb{R}^n$ with nonzero determinant. We will denote the basis vectors of a lattice as column vectors. Then the basis itself is an $n\times n$-matrix which consists of the column vectors of the basis.

For any two vectors $\mathbf{u}$, $\mathbf{v}\in\mathbb{R}^n$ we denote their scalar product by $\mathbf{u}\cdot\mathbf{v}$ and we write $|\mathbf{v}|$ for the Euclidean norm $(\mathbf{v}\cdot\mathbf{v})^{1/2}$ of $\mathbf{v}$. For $n\times n$-matrices $\mathbf{A}$, $\mathbf{B}$, ... the column vectors are denoted by $\mathbf{a}_i$, $\mathbf{b}_i$, ... and the entry in row i, column j is denoted by $a_{i,j}$, $b_{i,j}$, ..., for i, $j=1,\ldots,n$. We write $\mathbf{A}^{-1}$ for the inverse matrix of $\mathbf{A}$. The basis $\mathbf{B}^*=[\mathbf{b}_1^*,\ldots,\mathbf{b}_n^*]$ defined by $\mathbf{B}^*=(\mathbf{B}^{-1})^{\mathsf{T}}$ is called the reciprocal basis of $\mathbf{B}$. It satisfies $\mathbf{b}_i\cdot\mathbf{b}_j^*=\delta_{i,j}$ (with $\delta_{i,i}=1$ and $\delta_{i,j}=0$ for $i\ne j$); the vectors $\mathbf{b}_i^*$, $i=1,\ldots,n$ denote the column vectos of the reciprocal basis $\mathbf{B}^*$.

Multiplying a lattice basis $\mathbf{B}$ with an orthogonal matrix $\mathbf{K}$ from the left hand side corresponds to a rotation of the coordinate system; such a rotation does not change the lengths of the basis vectors of a lattice basis $\mathbf{B}$ or its reciprocal basis $\mathbf{B}^*$. If $\mathbf{K}$ is an orthogonal matrix we consider the two bases $\mathbf{B}$ and $\mathbf{K}\cdot\mathbf{B}$ as equivalent.

AMS subject classification code (1991): 11 H 55

The basis transformations of a lattice basis $\mathbf{B}$ are obtained by multiplying the basis $\mathbf{B}$ with an $SL_n(\mathbb{Z})$-matrix on the right hand side. For any transformation matrix $\mathbf{T} \in SL_n(\mathbb{Z})$ the two lattice bases $\mathbf{B}$ and $\tilde{\mathbf{B}} = \mathbf{B} \cdot \mathbf{T}$ define the same lattice $\sum_{i=1}^{n} \mathbf{b}_i\mathbb{Z}$. The lattice reduction theory deals with identifying and computing a *reduced* basis for a given lattice. There are several concepts of reduced lattice bases, see e. g. [5], supplement to chapter 2, for an overview.

We are going to study lattice bases where the basis vectors of the lattice and also the basis vectors of its reciprocal lattice are short. For any lattice basis $\mathbf{B}$ of dimension n let $S(\mathbf{B})$ the the quantity $\sum_{i=1}^{n} |\mathbf{b}_i|^2 \cdot |\mathbf{b}_i^*|^2$. We have $S(\mathbf{B}) = n$ if and only if the basis vectors are orthogonal, otherwise $S(\mathbf{B}) > n$. A small value of $S(\mathbf{B})$ indicates that both the basis vectors of $\mathbf{B}$ and the basis vectors of the reciprocal basis $\mathbf{B}^*$ are short.

In section 4 we will show that every lattice of dimension n has a basis $\mathbf{B}$ which satisfies $S(\mathbf{B}) = \exp(O((\ln n)^2))$. This improves an earlier result of Håstad and Lagarias [7]. To obtain this result we will have to consider lattice bases which are reduced in the sense of Korkine and Zolotarev [10] and we will also have to study the group $N(n, \mathbb{R})$ of all upper triangular unipotent $n \times n$-matrices with diagonal equal to one. This will be done in sections 2 and 3.

In section 5 we will introduce a new concept of lattice basis reduction. A lattice basis $\mathbf{B}$ will be called S-reduced if $S(\mathbf{B})$ is minimal. We will also introduce the weaker concept of S_2-reduction, and we present a simple algorithm to compute an S_2-reduced basis of a given lattice.

The new reduction algorithm is similar to the lattice basis reduction algorithm of Dieter [3] and Knuth [9], section 3.3.4, which reduces the size of the basis vectors and the size of the vectors of the reciprocal basis of a lattice in separate steps. In contrast to the well known lattice basis reduction algorithm of Lovász, as described in [14], we cannot prove a bound for the running time of the new algorithm or the size of the basis vectors after the reduction has been completed.

It is not known whether $S(\mathbf{B})$ is bounded for all S_2-reduced lattice bases of a given dimension n. Experimental results obtained by running the new algorithm with random lattices of dimension 30...80 make it seem unlikely that there is a (small) polynomial bound for $S(\mathbf{B})$ for S_2-reduced lattice bases. We also do not know a bound for the number of different S_2-reduced bases of a lattice of a given dimension.

The new algorithm for S_2-reduction can also combined with an exhaustive search procedure (see e. g. [8]) to find the shortest nonzero vector in a lattice. The computational problem of finding a reduced basis of a general lattice in the sense of Korkine and Zolotarev is polynomial time equivalent to the problem of finding the shortest nonzero vector in a general lattice, see [5] or [11] for details. The above procedure can easily be extended to an algorithm which computes a reduced lattice basis in the sense of Korkine and Zolotarev. Some possible variations of the new reduction algorithm will be discussed in section 6.

In section 7 we discuss some practical results obtained with the algorithm for S_2-reduction. The new algorithm works well in practice for lattices of dimension up to 30; there it will usually compute very short basis vectors. For dimension ≥ 35

the basis vectors found by the new algorithm are much larger than the basis vectors obtained by the algorithm of Lovász. The algorithm has also been implemented by LaMacchia, see [13]. He found a similar behaviour of the new algorithm and also observed that the new algorithm is faster than the algorithm of Lovász.

The procedure for Korkine–Zolotarev reduction works well for lattices of dimension up to 25. With some refinements of the original procedure, a Korkine–Zolotarev reduced basis for most lattices of dimension 30 can be computed within only a few minutes of computer time.

Lattice basis reduction is a fundamental technique for solving various types of combinatorial problems such as integer programming [8], [15], factoring polynomials [14], finding integer relations [6] and factoring integers [18]. Most recently lattice reduction techniques have been succesfully applied to subset sum problems, see [2], [4], [12], [13]. In most of these applications the algorithms for lattice reduction are extensions or improved versions of the algorithm of Lovász; see Schnorr [16], [17] for efficient lattice reduction algorithms. In [13] our new algorithm has also been applied to subset sum problems.

2. Gram–Schmidt orthogonalization and Korkine–Zolotarev reduction

A nonsingular $n \times n$-matrix $\mathbf{B}$ can be uniquely decomposed into a product $\mathbf{B} = \mathbf{K} \cdot \mathbf{H}$ of an orthogonal matrix $\mathbf{K}$ and an upper triangular matrix $\mathbf{H} = (h_{i,j})$ with positive diagonal entries $h_{i,i}$.

For an ordered lattice basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ this means that there is a uniquely defined orthogonal matrix $\mathbf{K}$ such that the basis $\mathbf{H} = \mathbf{K}^{-1} \cdot \mathbf{B}$ (which is equivalent to the basis $\mathbf{B}$) satisfies $h_{i,i} > 0$, $h_{i,j} = 0$ for $i > j$. Given a basis $\mathbf{B}$ the basis $\mathbf{H}$ can be computed as follows:

First we compute the Gram–Schmidt orthogonalized basis $\hat{\mathbf{B}} = [\hat{\mathbf{b}}_1, \dots, \hat{\mathbf{b}}_n]$ associated with $\mathbf{B}$ which is defined by:

$$\hat{\mathbf{b}}_1 = \mathbf{b}_1, \qquad \hat{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \hat{\mathbf{b}}_j, \qquad 2 \le i \le n;$$

$$\mu_{i,j} = \frac{\mathbf{b}_i \cdot \hat{\mathbf{b}}_j}{\hat{\mathbf{b}}_j \cdot \hat{\mathbf{b}}_j}, \qquad \text{for} \quad i > j.$$

Then we put

$$\mathbf{K} := \left(\frac{\hat{\mathbf{b}}_1}{|\hat{\mathbf{b}}_1|}, \dots, \frac{\hat{\mathbf{b}}_n}{|\hat{\mathbf{b}}_n|} \right).$$

(Here $\hat{\mathbf{b}}_i / |\hat{\mathbf{b}}_i|$ denotes the i-th column vector of $\mathbf{K}$.) Let $\mathbf{H} := (h_{i,j})$ be the matrix defined by:

$$h_{i,j} = \begin{cases} 0 & \text{if } j < i \\ |\hat{\mathbf{b}}_i| & \text{if } j = i \\ \mu_{j,i} \cdot |\hat{\mathbf{b}}_i| & \text{if } j > i \end{cases}.$$

Then we have $\mathbf{B} = \mathbf{K}{\cdot}\mathbf{H}$, $\mathbf{K}$ is an orthogonal matrix, (since the vectors $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$ are orthogonal,) and $\mathbf{H}$ is upper triangular.

For simplicity we call $\mathbf{H}$ the *Gram–Schmidt orthogonalization* of the lattice basis $\mathbf{B}$.

We will now introduce the notion of lattice basis reduction in the sense of Korkine and Zolotarev (see [10]):

Definition 1. A lattice basis $\mathbf{B}$ is Korkine–Zolotarev reduced if its Gram–Schmidt orthogonalization $\mathbf{H}$ satisfies the following conditions:

1.1 The first basis vector $\mathbf{h}_1$ of $\mathbf{H}$ is the shortest nonzero vector in the lattice $\sum_{i=1}^{n} h_i\mathbb{Z}$ generated by $\mathbf{H}$.

1.2 $|h_{1,i}| \leq \frac{1}{2} \cdot |h_{1,1}|$ for $i = 2, \ldots, n$.

1.3 If $n > 1$, the submatrix $\mathbf{H}_2$ of $\mathbf{H}$ which consists of the rows and columns $2, \ldots, n$ of $\mathbf{H}$ defines a Korkine–Zolotarev reduced lattice basis of dimension $n-1$.

Each lattice has (at least) one Korkine–Zolotarev reduced basis. Korkine–Zolotarev reduced bases are extensively studied in [11]. We take the following result from [11]:

Theorem 2. *For the Gram–Schmidt orthogonalization H of a Korkine–Zolotarev reduced lattice basis we have*

$$(h_{i,i})^2 > (h_{1,1})^2 \cdot i^{-1-\ln i}$$

for $i > 1$.

Proof. See [11], Proposition 4.2. ∎

Since the concept of Korkine–Zolotarev reduction is recursive Theorem 2 immediately implies

Corollary 3. *For the Gram–Schmidt orthogonalization H of a Korkine–Zolotarev reduced lattice basis of dimension n we have*

$$h_{i,i}/h_{j,j} = \exp(O((\ln n)^2)$$

for $j \geq i$.

3 Unipotent matrices

Let $N(n,\mathbb{R})$ be the group of upper triangular unipotent $n \times n$-matrices, i. e., matrices $\mathbf{A}$ which satisfy $a_{i,j} = 0$ for $i > j$ and $a_{i,i} = 1$. Let $N(n,\mathbb{Z})$ be the subgroup of $N(n,\mathbb{R})$ which integer entries $a_{i,j}$.

For any real matrix $\mathbf{A}$ let

$$\|\mathbf{A}\|_\infty = \max_{i,j}\{|a_{i,j}|\}$$

and for any invertible real matrix $\mathbf{A}$ with inverse $\mathbf{A}^{-1}$ let

$$S'(\mathbf{A}) = \max\{\|\mathbf{A}\|_\infty, \|\mathbf{A}^{-1}\|_\infty\}.$$

Given a matrix $\mathbf{A} \in N(n,\mathbb{R})$, we are interested in a transformation matrix $\mathbf{T} \in N(n,\mathbb{Z})$ such that $S'(\mathbf{A}\cdot\mathbf{T})$ becomes as small as possible.

Definition 4. For all $n \in \mathbb{N}$ let

$$S(n) = \sup_{\mathbf{A}\in N(n,\mathbb{R})} \left\{ \inf_{\mathbf{T}\in N(n,\mathbb{Z})} \{S'(\mathbf{A}\cdot\mathbf{T})\} \right\}$$

Remark. For a fixed matrix $\mathbf{A} \in N(n,\mathbb{R})$ we can always find a $\mathbf{T}_0 \in N(n,\mathbb{Z})$ such that $S'(\mathbf{A}\cdot\mathbf{T}_0)$ is minimal in the set $\{S'(\mathbf{A}\cdot\mathbf{T})|\mathbf{T}\in N(n,\mathbb{Z})\}$.

To see this, note that $\|\mathbf{T}\|_\infty \le n\cdot\|\mathbf{A}^{-1}\|_\infty\cdot\|\mathbf{AT}\|_\infty$ and hence $S'(\mathbf{AT}) \ge \|\mathbf{AT}\|_\infty \ge \|\mathbf{T}\|_\infty\cdot(c_\mathbf{A})^{-1}$, where $c_\mathbf{A}$ is the positive number $n\cdot\|\mathbf{A}^{-1}\|_\infty$. Since the infimum of the set $\{S'(\mathbf{A}\cdot\mathbf{T})|\mathbf{T}\in N(n,\mathbb{Z})\}$ is at most $S'(\mathbf{A})$ we obtain it as the minimum of the finite set $\{S'(\mathbf{A}\cdot\mathbf{T})|\mathbf{T}\in N(n,\mathbb{Z}), \|\mathbf{T}\|_\infty \le S'(\mathbf{A})\cdot c_\mathbf{A}\}$. This implies that for every matrix $\mathbf{A}\in N(n,\mathbb{R})$ there is a transformation matrix $\mathbf{T}\in N(n,\mathbb{Z})$ such that $S'(\mathbf{A}\cdot\mathbf{T}) \le S(n)$ holds (with equality in the worst case).

In [7] it is shown $S(n) = \exp(O(n^{1/3}))$. We will now show $S(n) = \exp(O((\ln n)^2))$. This result follows immediately from the following proposition:

Proposition 5. $S(2\cdot n) \le S(n)\cdot\max\{1,\frac{n}{2}\}$.

Proof. We may assume $n \ge 2$. Let $\mathbf{A} \in N(2n,\mathbb{R})$. We decompose $\mathbf{A}$ into four $n\times n$-submatrices as follows:

$\mathbf{A} = \begin{pmatrix} \mathbf{P} & \mathbf{Q} \\ 0 & \mathbf{R} \end{pmatrix}$ with $\mathbf{P},\mathbf{R} \in N(n,\mathbb{R})$ and $\mathbf{Q}$ being any $n\times n$-matrix.

Since $\mathbf{P}$ and $\mathbf{R}$ belong to $N(n,\mathbb{R})$, there exist $n\times n$-matrices $\mathbf{T}$ and $\mathbf{U}$ in $N(n,\mathbb{Z})$ such that each of the values $\|\mathbf{PT}\|_\infty$,$\|(\mathbf{PT})^{-1}\|_\infty$,$\|\mathbf{RU}\|_\infty$ and $\|(\mathbf{RU})^{-1}\|_\infty$ is at most $S(n)$.

For any $x\in\mathbb{R}$ let $\lfloor x\rceil$ be the value of x rounded to the nearest integer (with $\lfloor x+\frac{1}{2}\rceil = x$ for $x\in\mathbb{Z}$). Given any matrix $\mathbf{A}=(a_{i,j})$, we write $\lfloor\mathbf{A}\rceil$ for the matrix $(\lfloor a_{i,j}\rceil)$, where each entry of $\mathbf{A}$ is rounded to the nearest integer.

Define

$$\mathbf{V} := \begin{pmatrix} \mathbf{T} & -\mathbf{T}\lfloor(\mathbf{PT})^{-1}\mathbf{QU}\rceil \\ 0 & \mathbf{U} \end{pmatrix}$$

Clearly, $\mathbf{V}$ belongs to $N(2n,\mathbb{Z})$. We show that both, $\|\mathbf{AV}\|_\infty$ and $\|(\mathbf{AV})^{-1}\|_\infty$ are at most $\frac{1}{2}n\cdot S(n)$.

To this end, define $\mathbf{W} := (\mathbf{PT})^{-1}\mathbf{QU} - \lfloor(\mathbf{PT})^{-1}\mathbf{QU}\rceil$. So $\|\mathbf{W}\|_\infty \le \frac{1}{2}$. Moreover,

$$\mathbf{AV} = \begin{pmatrix} \mathbf{PT} & \mathbf{PTW} \\ 0 & \mathbf{RU} \end{pmatrix}$$

and hence

$$(\mathbf{AV})^{-1} = \begin{pmatrix} (\mathbf{PT})^{-1} & -\mathbf{W}(\mathbf{RU})^{-1} \\ 0 & (\mathbf{RU})^{-1} \end{pmatrix}.$$

Since $\|\mathbf{PT}\|_\infty \le S(n)$, $\|\mathbf{RU}\|_\infty \le S(n)$, and $\|\mathbf{W}\|_\infty \le \frac{1}{2}$ it follows that $\|\mathbf{AV}\|_\infty \le \frac{1}{2}n \cdot S(n)$. Similarly, since $\|(\mathbf{PT})^{-1}\|_\infty \le S(n)$, $\|(\mathbf{RU})^{-1}\|_\infty \le S(n)$, and $\|\mathbf{W}\|_\infty \le \frac{1}{2}$ it follows that $\|(\mathbf{AV})^{-1}\|_\infty \le \frac{1}{2}n \cdot S(n)$. ∎

Proposition 5 immediately implies:

Theorem 6.

$$S(n) = \exp(O((\ln n)^2))$$

Remark. Given an $n \times n$-matrix $\mathbf{A} \in N(n,\mathbb{R})$, the number of arithmetic operations for finding a transformation matrix $\mathbf{T} \in N(n,\mathbb{Z})$ with $S'(\mathbf{A} \cdot \mathbf{T}) = \exp(O((\ln n)^2))$ can be bounded by $O(n^3)$.

4. Proof of the main theorem

Theorem 7. *For every lattice L there is a basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ with reciprocal basis $\mathbf{B}^* = [\mathbf{b}_1^*, \dots, \mathbf{b}_n^*]$ which satisfies*

$$|\mathbf{b}_i| \cdot |\mathbf{b}_i^*| \le \exp(c_2 \cdot (\ln n)^2)$$

for $i = 1, \dots, n$ and c_2 fixed and independent of n.

Proof. The theorem is a simple consequence of Theorem 6 and Corollary 3. The proof is along the lines of [7], section 4.

Given a lattice L we start with a Korkine–Zolotarev reduced basis $\mathbf{B}$ of L. Let $\mathbf{H}$ be the Gram–Schmidt orthogonalization of $\mathbf{B}$. Then we have $\mathbf{B} = \mathbf{K} \cdot \mathbf{H}$, where $\mathbf{K}$ is orthogonal and $\mathbf{H}$ is an upper triangular matrix. Since $\mathbf{H}$ is upper triangular, it can be decomposed into a diagonal matrix $\mathbf{D}$ with $d_{i,i} = h_{i,i}$ and a unipotent matrix $\mathbf{A} \in N(n,\mathbb{R})$:

$$\mathbf{H} = \mathbf{D} \cdot \mathbf{A}.$$

By definition of $S(n)$ there is a tranformation matrix $\mathbf{T}$ with $S'(\mathbf{A} \cdot \mathbf{T}) \le S(n)$. Let $\tilde{\mathbf{B}} = \mathbf{B} \cdot \mathbf{T}$, $\tilde{\mathbf{H}} = \mathbf{H} \cdot \mathbf{T}$, $\tilde{\mathbf{A}} = \mathbf{A} \cdot \mathbf{T}$. Then $\tilde{\mathbf{B}}$ is the desired reduced basis of the lattice. So we have

$$\tilde{\mathbf{B}} = \mathbf{K} \cdot \mathbf{H} \cdot \mathbf{T} = \mathbf{K} \cdot \mathbf{D} \cdot \tilde{\mathbf{A}}, \qquad S(\tilde{\mathbf{A}}) \le S(n), \qquad \tilde{h}_{i,i} = h_{i,i} = d_{i,i}.$$

Let $\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_n$ be the basis vectors of $\tilde{\mathbf{B}}$ and let $\tilde{\mathbf{b}}_1^*, \dots, \tilde{\mathbf{b}}_n^*$ be the basis vectors of the reciprocal basis $\tilde{\mathbf{B}}^*$ of $\tilde{\mathbf{B}}$. Define $\tilde{\mathbf{A}}^* := (\tilde{\mathbf{A}}^{-1})^\mathsf{T}$, $\tilde{\mathbf{H}}^* := (\tilde{\mathbf{H}}^{-1})^\mathsf{T}$. Then we have $\|\tilde{\mathbf{A}}^*\|_\infty = \|\tilde{\mathbf{A}}^{-1}\|_\infty \le S(n)$; and $\tilde{\mathbf{B}}^* = \mathbf{K} \cdot \mathbf{D}^{-1} \cdot \tilde{\mathbf{A}}^* = \mathbf{K} \cdot \tilde{\mathbf{H}}^*$ holds for the reciprocal basis $\tilde{\mathbf{B}}^*$ of $\tilde{\mathbf{B}}$. Let $(\tilde{h}_{i,j})$, $(\tilde{a}_{i,j})$ and $(\tilde{a}_{i,j}^*)$ be the entries of the matrices $\tilde{\mathbf{H}}$, $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{A}}^*$, respectively.

For $i = 1, \ldots, n$ we have:

$$\begin{aligned}
|\tilde{\mathbf{b}}_i|^2 \cdot |\tilde{\mathbf{b}}_i^*|^2 &= |\tilde{\mathbf{h}}_i|^2 \cdot |\tilde{\mathbf{h}}_i^*|^2 && \text{(since } \tilde{\mathbf{B}} = \mathbf{K} \cdot \tilde{\mathbf{H}}, \mathbf{K} \text{ orthogonal)} \\
&= \sum_{j=1}^{i} (\tilde{h}_{j,j} \cdot \tilde{a}_{j,i})^2 \cdot \sum_{k=1}^{n} \left(\frac{\tilde{a}^*_{k,i}}{\tilde{h}_{k,k}} \right)^2 && \text{(since } \tilde{a}_{j,i} = \tilde{a}^*_{k,i} = 0 \text{ for } j > i > k) \\
&= \sum_{j=1}^{i} \sum_{k=1}^{n} \frac{h^2_{j,j}}{h^2_{k,k}} \cdot (\tilde{a}_{j,i} \cdot \tilde{a}^*_{k,i})^2 && \text{(note that } \tilde{h}_{i,i} = h_{i,i}) \\
&\leq n^2 \cdot \max_{k \geq j} \left\{ \frac{h^2_{j,j}}{h^2_{k,k}} \right\} \cdot (S(n))^4 && \text{(by definition of } S(n)) \\
&= n^2 \cdot \exp(O((\ln n)^2)) \cdot (S(n))^4 && \text{(by Corollary 3)} \\
&= \exp(O((\ln n)^2)) && \text{(by Theorem 6)} \ \blacksquare
\end{aligned}$$

Remark. It is not known whether the bound for $S(\mathbf{A})$ stated in the main theorem is sharp or whether it could be improved to a bound which is polynomial in the dimension of the lattice. Note that the bound in theorem 7 is basically n^2 multiplied by a constant power of the product of the bounds in theorem 2 and 6. Therefore it would be of great interest to improve the bounds in the theorem 2 and 6.

5. A new concept of lattice basis reduction

In this section we propose some new kinds of lattice basis reduction and an algorithm to compute one of them. The algorithm works directly with the symmetric matrix $\mathbf{A} = \mathbf{B}^\mathsf{T} \cdot \mathbf{B}$ which is associated to the lattice basis $\mathbf{B}$ and with the inverse $\mathbf{A}^{-1}$ of $\mathbf{A}$. The goal of the new algorithm is the simultaneous size reduction of the diagonal elements of the matrix $\mathbf{A}$ and its inverse $\mathbf{A}^{-1}$.

The quadratic form associated with a lattice basis

To each lattice basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ there is the associated positive definite quadratic form $\mathbf{A}$ which maps $\lambda = [\lambda_1, \ldots, \lambda_n] \in \mathbb{Z}^n$ onto $\left| \sum_{i=1}^{n} \lambda_i \mathbf{b}_i \right|^2 = \lambda^\mathsf{T} \mathbf{B}^\mathsf{T} \mathbf{B} \lambda$. This quadratic form will be identified with the symmetric matrix $\mathbf{A} = \mathbf{B}^\mathsf{T} \cdot \mathbf{B}$. (Here the basis vectors $\mathbf{b}_i$ are the column vectors of $\mathbf{B}$, and $\mathbf{B}^\mathsf{T}$ is the transposed matrix of $\mathbf{B}$). The inverse $\mathbf{A}^{-1}$ of $\mathbf{A}$ is also positive definite and symmetric. If $\mathbf{A}$ is a symmetric matrix, we will write $a^*_{i,j}$ for the entry of the matrix $\mathbf{A}^{-1}$ at row i, column j. Then we have $a_{i,i} = |\mathbf{b}_i|^2$ and $a^*_{i,i} = |\mathbf{b}^*_i|^2$ for the diagonal elements of $\mathbf{A}$ and $\mathbf{A}^{-1}$. The basis transformation $\mathbf{B} \to \mathbf{B} \cdot \mathbf{T}$, $\mathbf{T} \in SL_n(\mathbb{Z})$ corresponds to the transformation $\mathbf{A} \to \mathbf{T}^\mathsf{T} \cdot \mathbf{A} \cdot \mathbf{T}$ of the associated quadratic form $\mathbf{A}$. All quadratic forms considered in this paper will be positive definite.

S-Reduction

For any quadratic form $\mathbf{A} = (a_{i,j})$ with inverse $\mathbf{A}^{-1} = (a^*_{i,j})$ we define:

$$S(\mathbf{A}) = \sum_{i=1}^{n} a_{i,i} \cdot a^*_{i,i}$$

A lattice basis and its associated quadratic form $\mathbf{A}$ will be called S-reduced if $S(\mathbf{A}) \le S(\mathbf{T}^{\mathsf{T}} \cdot \mathbf{A} \cdot \mathbf{T})$ holds for all $\mathbf{T} \in SL_n(\mathbb{Z})$.

Theorem 7 immediately implies:

Every S-reduced quadratic form $\mathbf{A}$ satisfies $S(\mathbf{A}) \le \exp(O((\ln n)^2))$.

Successive minima

We will now introduce the concept of successive minima of a lattice (see e. g. [5], chapter 2), since this allows us to bound the coefficients of a quadratic form $\mathbf{A}$ and $\mathbf{A}^{-1}$ in terms of $S(\mathbf{A})$.

For any lattice L let $\lambda_i(L)$ be the i-th successive minimum of the lattice defined by:

$$\lambda_i(L) = \inf\{\lambda \ge 0 : \quad L \text{ contains (at least) } i \text{ linearly independent vectors } \mathbf{b}_\nu; \quad \nu = 1, \ldots, i \text{ with } |\mathbf{b}_\nu| \le \lambda\}.$$

If $\mathbf{B}$ is a basis of the lattice L, define $\lambda_i(\mathbf{B}) := \lambda_i(L)$. If $\mathbf{K}$ is any orthogonal $n \times n$-matrix and $\mathbf{T} \in SL_n(\mathbb{Z})$ we have $\lambda_i(\mathbf{K} \cdot \mathbf{B} \cdot \mathbf{T}) = \lambda_i(\mathbf{B})$. For any positive definite quadratic form $\mathbf{A}$ with $\mathbf{A} = \mathbf{B}^{\mathsf{T}} \cdot \mathbf{B}$ we define $\lambda_i(\mathbf{A}) := \lambda_i(\mathbf{B})$. (This definition is consistent, since $\mathbf{B}^{\mathsf{T}}\mathbf{B} = \tilde{\mathbf{B}}^{\mathsf{T}}\tilde{\mathbf{B}}$ implies $(\tilde{\mathbf{B}}\mathbf{B}^{-1})^{-1} = (\tilde{\mathbf{B}}\mathbf{B}^{-1})^{\mathsf{T}}$ and hence the matrix $\mathbf{K} := \tilde{\mathbf{B}}\mathbf{B}^{-1}$ satisfying $\tilde{\mathbf{B}} = \mathbf{K} \cdot \mathbf{B}$ is orthogonal). The successive minima of a quadratic form are invariant under $SL_n(\mathbb{Z})$ transformations; i. e. $\lambda_i(\mathbf{T}^{\mathsf{T}}\mathbf{A}\mathbf{T}) = \lambda_i(\mathbf{A})$ holds for any positive definite quadratic form $\mathbf{A}$ and $\mathbf{T} \in SL_n(\mathbb{Z})$.

The following theorem bounds the size of the coefficients of a positive definite quadratic form $\mathbf{A}$ and its inverse $\mathbf{A}^{-1}$ in terms of $S(\mathbf{A})$ and $\lambda_i(\mathbf{A})$:

Theorem 8. *For every positive definite quadratic form $A = (a_{i,j})$ with $a_{j,j} \ge a_{i,i}$ for $j > i$ we have:*

$$\lambda_i(\mathbf{A})^2 \le a_{i,i} \le S(\mathbf{A})^2 \cdot \lambda_i(\mathbf{A})^2$$
$$\frac{1}{S(\mathbf{A}) \cdot \lambda_i(\mathbf{A})^2} \le a^*_{i,i} \le \frac{S(\mathbf{A})}{\lambda_i(\mathbf{A})^2}.$$

Proof. $\lambda_i(\mathbf{A})^2 \le a_{i,i}$ follows immediately from the definition of the successive minima and $a_{\nu,\nu} \le a_{i,i}$ for $\nu < i$. Since $a_{i,i}a^*_{i,i} \le S(\mathbf{A})$, we have $a^*_{i,i} \le S(\mathbf{A}) \cdot \lambda_i(\mathbf{A})^{-2}$. For $j \ge i$ we have $a^*_{j,j} \le S(\mathbf{A}) \cdot (a_{j,j})^{-1} \le S(\mathbf{A}) \cdot (a_{i,i})^{-1} \le S(\mathbf{A}) \cdot (a^*_{i,i})$. Hence $(\lambda_{n+1-i}(\mathbf{A}^{-1}))^2 \le \max_{i \le j \le n}(a^*_{j,j}) \le S(\mathbf{A}) \cdot a^*_{i,i}$. Since $\lambda_i(\mathbf{A}) \cdot \lambda_{n+1-i}(\mathbf{A}^{-1}) \ge 1$ (see e. g. [5], chapter 2, Theorem 5), it follows $1 \le a^*_{i,i} \cdot \lambda_i(\mathbf{A})^2 \cdot S(\mathbf{A})$, and hence

$(\lambda_i(\mathbf{A}))^{-2}\cdot(S(\mathbf{A}))^{-1}\le a^*_{i,i}$. Finally, $a_{i,i}\le S(\mathbf{A})\cdot(a^*_{i,i})^{-1}$ and $1\le a^*_{i,i}\cdot\lambda_i(\mathbf{A})^2\cdot S(\mathbf{A})$ imply $a_{i,i}\le S(\mathbf{A})^2\cdot\lambda_i(\mathbf{A})^2$. ∎

Corollary 9. *For a fixed positive definite quadratic form* $\mathbf{A}$ *and a fixed positive real number* x *the number of transformations* $\mathbf{T}\in SL_n(\mathbb{Z})$ *with* $S(\mathbf{T}^\top\mathbf{A}\mathbf{T})\le x$ *is finite.*

Proof. The coefficients of the positive definite quadratic form $\mathbf{A}=(a_{i,j})$ can be bounded by $\mathrm{tr}(A):=\sum_{i=1}^{n}a_{i,i}$; and the coefficients of the transformation matrix $\mathbf{T}=(t_{i,j})$ can be bounded by $\|\mathbf{T}\|:=\left(\sum_{i,j=1}^{n}t^2_{i,j}\right)^{1/2}$. It is not difficult to check that $tr(\mathbf{T}^\top\mathbf{A}\mathbf{T})\ge(\|\mathbf{T}\|)^2/\mathrm{tr}(\mathbf{A}^{-1})$ holds if $\mathbf{T}$, $\mathbf{A}$ are $n\times n$-matrices and $\mathbf{A}$ is positive definite and symmetric. W.l.o.g. we may assume $a_{j,j}\ge a_{i,i}$ for $j>i$.

From Theorem 8 we obtain

$$\mathrm{tr}(\mathbf{T}^\top\mathbf{A}\mathbf{T})\le(S(\mathbf{T}^\top\mathbf{A}\mathbf{T}))^2\cdot\sum_{i=1}^{n}\lambda_i(\mathbf{A})^2\le n\cdot(S(\mathbf{T}^\top\mathbf{A}\mathbf{T}))^2\cdot\lambda_n(\mathbf{A})^2$$

and

$$\mathrm{tr}(\mathbf{A}^{-1})\le S(\mathbf{A})\cdot\sum_{i=1}^{n}(\lambda_i(\mathbf{A}))^{-2}\le n\cdot S(\mathbf{A})\cdot(\lambda_1(\mathbf{A}))^{-2}.$$

This proves $n\cdot(S(\mathbf{T}^\top\mathbf{A}\mathbf{T}))^2\cdot\lambda_n(\mathbf{A})^2\ge\|\mathbf{T}\|^2\cdot n^{-1}\cdot(\lambda_1(\mathbf{A}))^2\cdot(S(\mathbf{A}))^{-1}$ and hence $S(\mathbf{T}^\top\mathbf{A}\mathbf{T})\ge\|\mathbf{T}\|\cdot c_{\mathbf{A}}$ for the positive constant

$$c_{\mathbf{A}}:=n^{-1}\cdot\lambda_1(\mathbf{A})\cdot(S(\mathbf{A}))^{-1/2}\cdot(\lambda_n(\mathbf{A}))^{-1}.$$

But the number of different transformations $\mathbf{T}\in SL_n(\mathbb{Z})$ with $\|\mathbf{T}\|\cdot c_{\mathbf{A}}\le x$ is finite. ∎

S_2-reduction

Given a lattice L, it is computationally difficult to find an S-reduced basis for this lattice. But there is a very simple algorithm which reduces the value $S(\mathbf{A})$ by working on the 2×2 submatrices of $\mathbf{A}$. We introduce the concept of S_2-reduction for the presentation of this new algorithm.

Let $\mathbf{T}^k_{i,k}$ be the $SL_n(\mathbb{Z})$-matrix $\mathbf{I}_n+k\cdot\mathbf{E}_{i,j}$, where $\mathbf{I}_n$ is the identity matrix in $SL_n(\mathbb{Z})$ and $\mathbf{E}_{i,j}$ is the matrix with all entries zero except for the entry in row i, column j, which is one. The transformation $\mathbf{B}\to\mathbf{T}^k_{i,j}\cdot\mathbf{B}$ (respectively, $\mathbf{B}\to\mathbf{B}\cdot\mathbf{T}^k_{i,j}$) is simple row (respectively, column) operation on the $n\times n$-matrix B.

A quadratic form $\mathbf{A}$ will be called S_2-reduced if

$$S(\mathbf{A})\le S(\mathbf{T}^k_{j,i}\cdot\mathbf{A}\cdot\mathbf{T}^k_{i,j})$$

holds for all $i,j,k\in\mathbb{Z}$ with $1\le i\ne j\le n$.

For any $x \in \mathbb{R}$ let $\lfloor x \rceil$ be the value of x rounded to the nearest integer as in section 3.

The following simple algorithm performs an S_2-reduction of the quadratic form $\mathbf{A}$:

Algorithm S_2-reduction

```
do while ($\mathbf{A}$ is not $S_2$-reduced)
{
choose $i, j$ such that there is an integer $k$ with
        $S(\mathbf{A}) < S(\mathbf{T}^k_{j,i} \cdot \mathbf{A} \cdot \mathbf{T}^k_{i,j});$
then put
        $\mathbf{A} = \mathbf{T}^k_{j,i} \cdot \mathbf{A} \cdot \mathbf{T}^k_{i,j}$ with $k = \left\lfloor \frac{1}{2}\left(\frac{a^*_{i,j}}{a^*_{j,j}} - \frac{a_{i,j}}{a_{i,i}}\right) \right\rceil$
}
```

Remarks. The quantity $S(\mathbf{A})$ decreases after each reduction step of the algorithm, since for fixed i and j, the value $S(\mathbf{T}^k_{j,i} \cdot \mathbf{A} \cdot \mathbf{T}^k_{i,j})$ is minimal for $k = \left\lfloor \frac{1}{2}\left(\frac{a^*_{i,j}}{a^*_{j,j}} - \frac{a_{i,j}}{a_{i,i}}\right) \right\rceil$. (Note that $\mathbf{T}^k_{i,j}$ transforms $a_{j,j}$ and $a^*_{i,i}$ as follows:

$$a_{j,j} \rightarrow a_{j,j} + 2k \cdot a_{i,j} + k^2 \cdot a_{i,i},$$

$$a^*_{i,i} \rightarrow a^*_{i,i} - 2k \cdot a^*_{j,i} + k^2 \cdot a^*_{j,j};$$

all other diagonal elements of $\mathbf{A}$ and $\mathbf{A}^{-1}$ are left invariant.)

Since the number of transformation matrices $\mathbf{T} \in SL_n(\mathbb{Z})$ with $S(\mathbf{T}^\top \mathbf{A} \mathbf{T}) < S(\mathbf{T})$ is finite by corollary 9, the algorithm terminates after a finite number of steps.

In the algorithm we did not specify the sequence in which i and j are updated to test the violation of the condition for S_2-reduction. The easiest way to perform this testing sequence is lexicographically scanning through all pairs (i, j) and then repeating this process until $S(\mathbf{A})$ cannot be reduced any more. (This will be called the *lazy* selection method.) But also other methods for selecting a pair (i, j) are possible. LaMacchia [13] suggested selecting the pair (i, j) which yields the greatest possible descent of $S(A)$ in each reduction step. (This will be called the *greedy* selection method.)

6. Variations of the new algorithm

Several variations of the algorithm for S_2-reduction are possible. Instead of $S(\mathbf{A}) = \sum a_{i,i} \cdot a^*_{i,i}$ we can minimize e. g. the functions $\sum \sqrt{a_{i,i} \cdot a^*_{i,i}}$ or $\prod a_{i,i} \cdot a^*_{i,i}$ on the 2×2-submatrices of $\mathbf{A}$ and $\mathbf{A}^{-1}$.

These variations of the algorithm for S_2-reduction have been tested experimentally; they did not have a noticeable effect on the size of the reduced basis vectors.

Perhaps the most interesting variation of the new algorithm can be obtained by extending the notion of S_2-reduction as follows:

For $2 \leq m \leq n, m \in \mathbb{N}$ let $T_{m,n}$ be the set of $n \times n$-matrices defined by:

$$T_{m,n} = \left\{ \mathbf{I}_n + \sum_{\nu=1}^{m-1} \lambda_\nu \cdot \mathbf{E}_{i_\nu,k} \mid 1 \leq i_\nu, k \leq n; i_\nu \neq k; 1 \leq \nu < m; \nu, i_\nu, \lambda_\nu, k \in \mathbb{Z} \right\}$$
$$\cup \left\{ \mathbf{I}_n + \sum_{\nu=1}^{m-1} \lambda_\nu \cdot \mathbf{E}_{k,i_\nu} \mid 1 \leq i_\nu, k \leq n; i_\nu \neq k; 1 \leq \nu < m; \nu, i_\nu, \lambda_\nu, k \in \mathbb{Z} \right\}$$

Clearly, $T_{m,n} \subset SL_n(\mathbb{Z})$, and a matrix in $T_{m,n}$ has at most $m-1$ nonzero entries off the main diagonal, and all these $m-1$ entries must occur in the same row or in the same column of the matrix.

A positive definite symmetric $n \times n$-matrix will be called S_m-reduced if $S(\mathbf{T}^{\mathsf{T}} \cdot \mathbf{A} \cdot \mathbf{T}) \leq S(\mathbf{A})$ holds for all $T \in T_{m,n}$. An S_m-reduced matrix is also $S_{m'}$-reduced for $m' < m$, so that we obtain a hierarchy of reduction algorithms for $m = 2, \ldots, n$.

In practice it turns out that S_3-reduction can still be performed within in a reasonable amount of time. But an S_3-reduction step should be performed only on a matrix for which no further S_2-reduction steps are possible. We briefly state the formulae for an S_3-reduction step of an S_2-reduced matrix.

Consider the transformation matrix $\mathbf{T} := \mathbf{I}_n + \lambda_i \cdot \mathbf{E}_{i,k} + \lambda_j \cdot \mathbf{E}_{j,k}$ for fixed different values $i, j, k \in \mathbb{N}$ and variable integers λ_i, λ_j. (For a complete S_3-reduction we must also consider matrices of type $\mathbf{I}_n + \lambda_i \cdot \mathbf{E}_{k,i} + \lambda_j \cdot \mathbf{E}_{k,j}$ but this case is similar to the above one and it will not be investigated here.)

The transformation $\mathbf{A} \to \mathbf{T}^{\mathsf{T}} \cdot \mathbf{A} \cdot \mathbf{T}$ changes no entries in the main diagonal of $\mathbf{A}$ or $\mathbf{A}^{-1}$ apart from the entries $a_{k,k}$, $a^*_{i,i}$ and $a^*_{j,j}$:

$$a_{k,k} \to a_{k,k} + 2\lambda_i a_{i,k} + \lambda_i^2 a_{i,i} + 2\lambda_j a_{j,k} + \lambda_j^2 a_{j,j} + 2\lambda_i \lambda_j a_{i,j}$$
$$a^*_{\nu,\nu} \to a^*_{\nu,\nu} - 2\lambda_\nu a^*_{\nu,k} + \lambda_\nu^2 a^*_{k,k}; \quad \nu = i, j.$$

For $\Delta(\lambda_i, \lambda_j) := S(\mathbf{T}^{\mathsf{T}} \cdot \mathbf{A} \cdot \mathbf{T}) - S(\mathbf{A})$ we obtain:

$$\Delta(\lambda_i, \lambda_j) = 2a^*_{k,k} \cdot (\lambda_i^2 a_{i,i} + \lambda_j^2 a_{j,j} + \lambda_i \lambda_j a_{i,j} - \lambda_i a_{i,i} x_i - \lambda_j a_{j,j} x_j);$$

$$x_\nu = \frac{a^*_{\nu,k}}{a^*_{k,k}} - \frac{a_{\nu,k}}{a_{\nu,\nu}}; \quad \nu = i, j.$$

Note that $|x_\nu| \leq 1$, $\nu = i, j$ holds for an S_2-reduced matrix $\mathbf{A}$ and $(a_{i,j})^2 < a_{i,i} \cdot a_{j,j}$ holds since $\mathbf{A}$ is positive definite. We will assume $a_{j,j} \geq a_{i,i}$ otherwise the role of i and j must be exchanged.

We have to find a pair $(\lambda_i, \lambda_j) \subset \mathbb{Z}^2$ which minimizes $\Delta(\lambda_i, \lambda_j)$ under the above conditions. It turns out that one of pairs $(0,0)$ or $\left(\left\lfloor \frac{1}{2} x_i - \frac{1}{2} s \cdot a_{i,j}/a_{i,i} \right\rceil, s\right)$, with

$s = 1$ for $x_j \geq 0$ and $s = -1$ otherwise, is always an optimal solution for (λ_i, λ_j). Furthermore, $(0,0)$ is always optimal if $|x_j| \leq \frac{1}{2}$ and $|x_i| + |x_j| \leq 1$ hold.

When an S_2-reduced matrix is tested for being S_3-reduced, $O(n^3)$ triples (i,j,k) must be tested with the above formula. In most cases the number of necessary tests can be greatly reduced by a suitable arrangement of these triples. For a lattice of dimension 30...40, the basis vectors after S_3-reduction are usually much shorter than the basis vectors after S_2-reduction.

We can also consider transformations matrices $\mathbf{T}$ of type $T = \mathbf{I}_n + \sum_{i \neq k} \lambda_i \mathbf{E}_{i,k}$ which have nonzero entries in a whole column (or matrices with nonzero entries in a whole row). This type of transformation is also used in the basis reduction algorithm of Dieter [3] and Knuth [9]. It turns out that the *real* optimal solutions for the λ_i in the above matrix $\mathbf{T}$ are given by $\lambda_i = a^*_{i,k}/a^*_{k,k}$. It is natural to conjecture that the choice $\lambda_i = \lfloor a^*_{i,k}/a^*_{k,k} \rceil$ leads to a solution which is almost optimal for integer values λ_i. But with an implementation of this additional reduction step the author did not obtain significantly shorter basis vectors.

7. Practical results on computing the shortest lattice vector

The algorithm for S_2-reduction has been implemented on a PC-AT (20 MHz, with coprocessor 80287) in floating point arithmetic for effectively finding the shortest vector in a lattice. The implementation runs with a speed of roughly 130000 floating point operations per second. For dimension ≥ 20 a procedure for S_3-reduction has been added. S_3-reduction is about three to four times slower than S_2-reduction.

The reduced basis computed by the new algorithm is then ordered by the size of the reciprocal basis vectors. Finally, the shortest vector of the lattice is computed with a simple exhaustive search procedure, as described in [8] and [9], without any further changes on the lattice basis.

The algorithm has been tested with the Leech-lattice of dimension 24, (which is conjectured to be the densest lattice at dimension 24, see [1]). The run time of the above PC implementation for computing the shortest vector(s) of the Leech-lattice is approximately 15 minutes, where most of the running time is spent for the exhaustive search procedure. Fot a typical lattice of dimension 24 (generated at random) the run time for computing the shortest vector is about 15 seconds. The algorithm has also been applied to the search for the shortest vector of lattices with dimension 30. Here in most cases the shortest vector could be computed within 5 minutes.

For larger dimensions (up to dimension 80), the shortest basis vector computed by the algorithm for S_2- or S_3-reduction is much larger than the shortest non-zero vector of the lattice.

LaMacchia [13] has independently tested the algorithm for S_2-reduction. He observed that the lazy selection method needs roughly 2.5 times as many reduction steps as the greedy selection method (compare section 5). He found that the greedy selection method can be used with profit, if large integer arithmetic is used for the reduction steps, and floating point arithmetic is used for finding the optimal reduction step. If only floating point arithmetic is used, the lazy approach is superior to the greedy approach.

LaMacchia [13] also tested the S_2-reduction algorithm with random bases of the cubic lattice (with standard basis $\mathbf{I}_n$). He observed that the algorithm usually finds a standard basis for dimension ≤ 31, but for dimension ≥ 35 the algorithm halts at a local minimum.

Acknowledgement. I would like to thank J. C. Lagarias, A. M. Odlyzko and C. P. Schnorr for valuable discussions on this subject. I would also like to thank an unknown referee for simplifying the proof of Theorem 6.

References

[1] J. H. CONWAY, and N. J. A. SLOANE: *Sphere packings, lattices and groups*, Springer Verlag, New York, 1988.

[2] M. J. COSTER, B. A. LAMACCHIA, A. M. ODLYZKO, and C. P. SCHNORR: An improved low-density subset sum algorithm, to appear in *Computational Complexity.*

[3] U. DIETER: How to compute the shortest vector in a lattice, *Math. Comp.* **29** (1975), 827–833.

[4] M. EUCHNER, and C. P. SCHNORR: Lattice basis reduction: improved practical algorithms and solving subset sum problems, *Proceedings of Fundamentals of Computation Theory*, FTC '91, Ed. L. Budach, Springer LNCS **529** (1991) 68–85.

[5] P. M. GRUBER, and J. LEKKERKERKER: *Geometry of numbers*, North Holland, Amsterdam, 1987.

[6] JOHAN HÅSTAD, B. JUST, J. C. LAGARIAS, and C. P. SCHNORR: Polynomial time algorithms for finding integer relations among real numbers, *SIAM J. Comput.* **18** (1989), 859–881.

[7] JOHAN HÅSTAD, and J. C. LAGARIAS: Simultaneously good bases of a lattice and its reciprocal lattice, *Math. Ann.* **287** (1990), 163–174.

[8] R. KANNAN: Improved algorithms on integer programming and related lattice problems, *Proc. 15th Annual ACM Symp. on Theory of Computing* (1983), 293–206.

[9] D. E. KNUTH: *The art of computer programming, Vol. 2: Seminumerical algorithms*, 2nd edition, Addison–Wesley, 1981.

[10] A. KORKINE, and G. ZOLOTAREV: Sur les formes quadratiques, *Math. Ann.* **6** (1873), 366–389.

[11] J. C. LAGARIAS, H. W. LENSTRA, JR., and C. P. SCHNORR: Korkine Zolotarev bases and successive minima of a lattice and its reciprocal, *Combinatorica* **10** (1990), 333–348.

[12] J. C. LAGARIAS, and A. M. ODLYZKO: Solving low-density subset sum problems, *J. Assoc. Comp. Mach.* **32** (1985), 229–246.

[13] B. A. LAMACCHIA: Basis reduction algorithms and subset sum problems. Thesis for the degree of Master of Science, Department of Electrical engineering and Computer Science, Massachusetts Institute mof Technology, May 1991.

[14] A. K. LENSTRA, H. W. LENSTRA, JR., and L. LOVÁSZ: Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.

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

[16] C. P. SCHNORR: A hierarchy of polynomial time lattice basis reduction algorithms, *Theor. Comp. Sci.* **53** (1987), 201–227.

[17] C. P. SCHNORR: A more efficient algorithm for lattice basis reduction, *J. Algorithms* **9** (1988), 47–62.

[18] C. P. SCHNORR: Factoring integers and computing discrete logarithms via diophantine approximation, *Proceedings of Eurocrypt '91*, Brighton, May 1991, to appear in Springer LNCS.

M. Seysen

Scheißheimer Str. 339
D–80809 München
Germany