# Reducing Lattice Bases by Means of Approximations

Johannes Buchmann

Fachbereich Informatik
Universität des Saarlandes
Postfach 1150
D-66041 Saarbrücken
Germany

**Abstract** Let $L$ be a $k$-dimensional lattice in $\mathbb{R}^m$ with basis $B = (\underline{b}_1, \ldots, \underline{b}_k)$. Let $A = (a_1, \ldots, a_k)$ be a rational approximation to $B$. Assume that $A$ has rank $k$ and a lattice basis reduction algorithm applied to the columns of $A$ yields a transformation $T = (\underline{t}_1, \ldots, \underline{t}_k) \in \mathrm{GL}(k, \mathbb{Z})$ such that $A\underline{t}_i \leq s_i \lambda_i(L(A))$ where $L(A)$ is the lattice generated by the columns of $A$, $\lambda_i(L(A))$ is the $i$-th successive minimum of that lattice and $s_i \geq 1$, $1 \leq i \leq k$. For $c > 0$ we determine which precision of $A$ is necessary to guarantee that $B\underline{t}_i \leq (1+c)s_i\lambda_i(L)$, $1 \leq i \leq k$. As an application it is shown that Korkine-Zolotaref-reduction and LLL-reduction of a non integer lattice basis can be effected almost as fast as such reductions of an integer lattice basis.

## 1 Introduction

Let $m, k \in \mathbb{N}$. Let $L$ be a *$k$-dimensional lattice* in $\mathbb{R}^m$, $B = (\underline{b}_1, \ldots, \underline{b}_k)$ a *basis* of $L$, i.e. the elements of $B$ are linearly independent and

$$L = L(B) = \sum_{i=1}^{k} \underline{b}_i \, \mathbb{Z} \ .$$

Such a basis is uniquely determined up to multiplication from the right by elements of the set $\mathrm{GL}(k, \mathbb{Z})$ of all invertible $k \times k$-matrices with integer coefficients. Such matrices are called *unimodular transformations*.

It is a natural question to ask whether there are bases which are particularly simple, e.g. which have elements of short euclidean length or a special form or which are even uniquely determined by certain conditions. Those bases are usually called *reduced bases.* There are various notions of reduction such as Minkowski-reduction, Korkine-Zolotarev-reduction, LLL-reduction etc. (see [GrLoSchri]). If $L$ is an *integral lattice*, i.e. $L \subset \mathbb{Z}^m$, algorithms for computing those bases are known. If $L$ is not integral one can apply reduction algorithms to a rational approximation of a basis of $L$. In addition to the reduced approximation, which is, in general, useless, the algorithms yield a *reducing unimodular transformation.* In this paper we determine which precision guarantees that the reducing unimodular transformation of the approximate basis is a reducing transformation of the original basis. Reducing approximate lattice bases is important in many applications, e.g. for computing small integral bases or small systems of fundamental units in number fields.

The problem of reducing lattice bases by means of approximations has been previously considered in [BuPo] and [BuKe]. There, only the case of LLL-reduction was treated and the method is less efficient than the method presented here.

## 2 The Results

To state the results precisely we introduce some notation.

For $\underline{b} = (b_1, \ldots, b_m)$, $\underline{c} = (c_1, \ldots, c_m) \in \mathbb{R}^m$ the *inner product* of $\underline{b}$ and $\underline{c}$ is

$$\langle \underline{b}, \underline{c} \rangle = \sum_{i=1}^{m} b_i c_i \ .$$

The *(euclidean) length* of $\underline{b}$ is

$$||\underline{b}|| = \langle \underline{b}, \underline{b} \rangle^{1/2} \ .$$

For any set or sequence $S$ of vectors in $\mathbb{R}^m$ whose elements generate a subspace of dimension $k$ and for $1 \leq i \leq k$ the *ith successive minimum* of $S$ is

$$\lambda_i(S) = \min\{r \in \mathbb{R}_{>0} : \text{there are } i \text{ lin. indep. vectors in } S \text{ of length} \leq r\} \ .$$

For $C \in \mathbb{R}^{m \times k}$ we define

$$||C|| = \left( \sum_{i=1}^{m} \sum_{j=1}^{k} c_{ij}^2 \right)^{1/2} \ .$$

Let $L$ be a lattice in $\mathbb{R}^m$ of dimension $k$, $B = (\underline{b}_1, \ldots, \underline{b}_k)$ a basis of $L$. The determinant of $L$ is

$$\det L = |\det(\langle \underline{b}_i, \underline{b}_j \rangle)_{1 \leq i,j \leq k}|^{1/2} \ .$$

The determinant is the volume of the parallelepiped spanned by the elements of $B$. It is an invariant of $L$. The *defect* of $B$ is

$$\mathrm{dft}(B) = \frac{\prod_{i=1}^{k} ||\underline{b}_i||}{\det L} \ .$$

The defect measures how far the basis vectors are from being pairwise orthogonal; in particular $\mathrm{dft}(B) = 1$ if and only if the basis vectors are pairwise orthogonal. Bases with small defect have short elements.

Let $A = (\underline{a}_1, \ldots, \underline{a}_k) \in \mathbb{R}^{m \times k}$ with

$$||B - A|| < 2^{-q} \tag{1}$$

for some $q \in \mathbb{N}$. In the main theorems of this paper we answer the following questions: When is $A$ of rank $k$? How close are the successive minima of $L(A)$ to those of $L$? What is the effect if we apply a reducing transformation for the approximate basis $A$ to the original basis $B$?

**Theorem 1.** *Let* $0 < c \leq 1$ *and*

$$q \geq q_1(B, c) = \lceil k + \log(\lambda_k(L)/\lambda_1(L)) + \log \mathrm{dft}(B) + \log(1/\lambda_1(B)) + \log(1/c) \rceil$$

*then the rank of* $A$ *is* $k$ *and*

$$\lambda_i(L(A)) \leq (1+c)\lambda_i(L), \quad 1 \leq i \leq k \ .$$

To formulate the next theorem we assume that $A$ is of rank $k$ (this will be guaranteed by the choice of $q$) and that $T = (\underline{t}_1, \ldots, \underline{t}_k) \in \mathbb{Z}^{k \times k}$ is non singular and such that

$$||A\underline{t}_i|| \leq s_i \lambda_i(L(A)), \quad 1 \leq i \leq k,$$

where $(s_1, \ldots, s_k)$ is a non decreasing sequence of real numbers $\geq 1$. Let $s = s_k$.

**Theorem 2.** *Let* $0 < c \leq 1$ *and*

$$q \geq q_2(B, c, s) = \lceil k + \log(\lambda_k(L)/\lambda_1(L)) + \log \mathrm{dft}(B) + \log(1/\lambda_1(B)) + \log(3s/c) \rceil.$$

*Then*

$$||\underline{t}_i|| \leq (3/2)^{k+1}\sqrt{k} s_i \mathrm{dft}(B) \lambda_i(L)/\lambda_1(B), \quad 1 \leq i \leq k$$

*and*

$$||B\underline{t}_i|| \leq (1+c) s_i \lambda_i(L), \quad 1 \leq i \leq k \ .$$

This result is applied in the special cases where $A$ is a rational approximation to $B$ and the transformation $T$ is obtained by Korkine-Zolotaref-reduction and LLL-reduction of $A$. Let $p \in \mathbb{Z}_{>0}$ and let $b$ be a real number. A rational number $a$ is called a *rational approximation of precision* $p$ to $b$ if

$$|a - b| < 2^{-p}$$

and

$$a \in 2^{-(p+1)}\mathbb{Z} \ .$$

Such an approximation always exists.

Put

$$\beta = \log(\lambda_k(B)/\lambda_1(L))$$

and for $c > 0, s \geq 1$ define

$$q_0(B, c, s) = \lceil q_2(B, c, s) + \log(\sqrt{km}) \rceil \ .$$

**Corollary 3.** *There is an algorithm which for $0 < c \leq 1$ when given an approximation of precision $p \geq q_0(B, c, \sqrt{(k+3)/4})$ to $B$ computes $T = (\underline{t}_1, \ldots, \underline{t}_k) \in \mathrm{GL}(k, \mathbb{Z})$ such that*

$$B\underline{t}_i \leq (1+c)\sqrt{(i+3)/4}\,\lambda_i(L), \quad 1 \leq i \leq k$$

*and*

$$\lambda_i(T) \leq (3/2)^{k+1}\sqrt{k(i+3)/4}\mathrm{dft}(B)\lambda_i(L)/\lambda_1(B), \quad 1 \leq i \leq k \ .$$

*The algorithm performs*

$$mk^{O(k)}(\log m + \beta + \log(1/c))$$

*arithmetic operations on numbers of binary length*

$$O\left(k^2\left(k\left(\log k + \beta\right) + \log(1/c) + \log m\right)\right) \ .$$

**Corollary 4.** *There is an algorithm which for $0 < c \leq 1$ when given an approximation of precision $p \geq q_0(B, c, 2^{(k-1)/2})$ to $B$ computes $T \in \mathrm{GL}(k, \mathbb{Z})$ such that*

$$\lambda_i(BT) \leq (1+c)\,2^{(k-1)/2}\,\lambda_i(L), \quad 1 \leq i \leq k$$

*and*

$$\lambda_i(T) \leq (3/2)^{k+1}\sqrt{k}\,2^{(k-1)/2}\mathrm{dft}(B)\lambda_i(L)/\lambda_1(B), \quad 1 \leq i \leq k \ .$$

*The algorithm performs*

$$O\left(mk^3\left(k\left(\log k + \beta\right) + \log m + \log(1/c)\right)\right)$$

*arithmetic operations on numbers of binary length*

$$O\left(k\left(k\left(\log k + \beta\right) + \log(1/c) + \log m\right)\right) \ .$$

## 3 The Proof

Let $A$, $B$ be as in Section 2. We recall a few results from linear algebra.

**Lemma 5 (Cauchy-Schwarz inequality).** *Let $\underline{a}, \underline{b} \in \mathbb{R}^m$ then*

$$\langle \underline{a}, \underline{b} \rangle \leq ||a||\,||b|| \ .$$

Let $V$ be the vector space generated by the elements of $B$. Let $C = (\underline{c}_1, \ldots, \underline{c}_k)$ be a sequence of vectors in $V$. Then there is $T \in \mathbb{R}^{k \times k}$ such that $C = BT$. For the purpose of this proof we define

$$\det C = \det L \det T \ .$$

That determinant has the following properties.

**Lemma 6.** *1. The vectors in $C$ are linearly dependent if and only if* $\det C = 0$.

2. *For $1 \le i \le k$ the map $\mathbb{R}^m \to \mathbb{R}$, $\underline{c} \mapsto \det(\underline{c}_1, \dots, \underline{c}_{i-1}, \underline{c}, \underline{c}_{i+1}, \dots, \underline{c}_k)$ is a homomorphism of $\mathbb{R}$-vector spaces, i.e.* $\det$ *is multilinear.*

**Lemma 7 (Cramer's rule).** *Let $\underline{t} = (t_1, \dots, t_k) \in \mathbb{R}^k$, $\underline{b} \in \mathbb{R}^m$ with $\underline{b} = B\underline{t}$ then*

$$t_i = \frac{\det(\underline{b}_1, \dots, \underline{b}_{i-1}, \underline{b}, \underline{b}_{i+1}, \dots, \underline{b}_k)}{\det L} .$$

**Lemma 8 (Gram-Schmidt orthogonalization).** *Let $C = (\underline{c}_1, \dots, \underline{c}_k)$ be a basis of $V$. Define*

$$\underline{c}_1^* = \underline{c}_1,$$

$$\underline{c}_i^* = \underline{c}_i - \sum_{j=1}^{i-1} \frac{\langle \underline{c}_i, \underline{c}_j^* \rangle}{\langle \underline{c}_j^*, \underline{c}_j^* \rangle} \underline{c}_j^*, \quad 2 \le i \le k,$$

*and $C^* = (\underline{c}_1^*, \dots, \underline{c}_k^*)$. Then the elements of $C^*$ are pairwise orthogonal and we have*

$$||\underline{c}_i^*|| \le ||\underline{c}_i||, \quad 1 \le i \le k,$$

*and*

$$\det C = \det C^* = \prod_{i=1}^{k} ||\underline{c}_i^*|| \le \prod_{i=1}^{k} ||\underline{c}_i|| .$$

In the previous statement, the basis $C^*$ is called the *Gram-Schmidt orthogonalization* of $C$. The last inequality is *Hadamard's inequality.* As an immediate consequence of Cramer's rule and Hadamard's inequality we obtain an upper bound for the solution of a linear system. For a vector $\underline{v} = (v_1, \dots, v_m) \in \mathbb{R}^m$ set

$$|\underline{v}| = \max\{|v_i| : 1 \le i \le m\} .$$

Note that

$$||\underline{v}|| \le \sqrt{m}|\underline{v}| .$$

**Corollary 9.** *Let $\underline{b} \in \mathbb{R}^m$, $\underline{t} \in \mathbb{R}^k$ such that $B\underline{t} = \underline{b}$. Then*

$$|\underline{t}| \le ||\underline{b}|| \operatorname{dft}(B)/\lambda_1(B) .$$

For any $\underline{t} \in \mathbb{R}^k$ and $C \in \mathbb{R}^{m \times k}$ we have $||C\underline{t}|| \le ||C|| \, ||t||$. Therefore, we obtain from (1)

$$||B\underline{t} - A\underline{t}|| < 2^{-q} ||\underline{t}|| .$$

This implies the next lemma.

**Lemma 10.** *If $\underline{t} \in \mathbb{R}^k$, $c > 0$ and*

$$q \ge q_3(B, \underline{t}, c) = \lceil \log ||\underline{t}|| - \log(c||B\underline{t}||) \rceil$$

*then*

$$||A\underline{t} - B\underline{t}|| < c \cdot ||B\underline{t}|| .$$

Next we prove an upper bound for $\det B - \det A$.

**Lemma 11.** *If*

$$q \geq \lceil -\log \lambda_1(B) \rceil$$

*then*

$$|\det A - \det B| < 2^{-q+k} \mathrm{dft}(B) \det B / \lambda_1(B) \ .$$

*Proof.* In Lemma 10 choose $c = 1$ and for $\underline{t}$ any unit vector. Then $q_3(B, \underline{t}, c) \leq \lceil -\log \lambda_1(B) \rceil$. Hence, if $q \geq \lceil -\log \lambda_1(B) \rceil$ then we have by Lemma 10 for $1 \leq i \leq k$

$$||\underline{a}_i|| < 2 \, ||\underline{b}_i|| \ .$$

This and Hadamard's inequality implies

$$\begin{aligned}
|\det B - \det A| &= |\sum_{j=1}^{k} (\det(\underline{b}_1, \ldots, \underline{b}_{j-1}, \underline{a}_j, \ldots, \underline{a}_k) \\
&\quad - \det(\underline{b}_1, \ldots, \underline{b}_j, \underline{a}_{j+1}, \ldots, \underline{a}_k))| \\
&\leq \sum_{j=1}^{k} |\det(\underline{b}_1, \ldots, \underline{b}_{j-1}, \underline{a}_j - \underline{b}_j, \underline{a}_{j+1}, \ldots, \underline{a}_k)| \\
&\leq \sum_{j=1}^{k} (||\underline{a}_1|| \cdots ||\underline{a}_{j-1}|| \, ||\underline{b}_j - \underline{a}_j|| \, ||\underline{b}_{j+1}|| \cdots ||\underline{b}_k||) \\
&< 2^{-q} \sum_{j=1}^{k} 2^{j-1} \prod_{\substack{i=1 \\ i \neq j}}^{k} ||\underline{b}_i|| \\
&\leq 2^{-q}(2^k - 1) \mathrm{dft}(B) \det B / \lambda_1(B) \\
&< 2^{-q+k} \mathrm{dft}(B) \det B / \lambda_1(B) \ .
\end{aligned}$$

□

**Corollary 12.** *Let $c > 0$. If*

$$q \geq q_4(B, c) = \lceil k + \log(\mathrm{dft}(B)/\lambda_1(B)) - \log c \rceil$$

*then*

$$|\det A - \det B| < c \, |\det B| \ .$$

Now we prove Theorem 1. In order for $A$ to be non singular it suffices by Corollary 12 to have

$$q \geq q_4(B, 1) = \lceil k + \log(\mathrm{dft}(B)/\lambda_1(B)) \rceil \ .$$

Let $U = (\underline{u}_1, \ldots, \underline{u}_k) \in \mathbb{Z}^{k \times k}$ be non singular with

$$||B\underline{u}_i|| = \lambda_i(L), \quad 1 \leq i \leq k \ .$$

Applying Lemma 10 we find that for

$$q \geq \log \lambda_k(U) - \log(c\lambda_1(L)) \tag{2}$$

we have

$$\|A\underline{u}_i\| \le (1+c)\|B\underline{u}_i\| = (1+c)\lambda_i(L), \quad 1 \le i \le k$$

and therefore

$$\lambda_i(L(A)) \le (1+c)\lambda_i(L), \quad 1 \le i \le k \ .$$

It follows from Corollary 9 that

$$\lambda_k(U) \le \sqrt{k}\lambda_k(L)\mathrm{dft}(B)/\lambda_1(B) \ .$$

Therefore $q \ge q_1(B,c)$ implies (2). This concludes the proof of Theorem 1.

To prove Theorem 2 we need the following result.

**Lemma 13.** *If*

$$q \ge q_1(B, 1/3)$$

*then*

$$\mathrm{dft}(A)/\lambda_1(A) \le (3/2)^k \mathrm{dft}(B)/\lambda_1(B), \quad 1 \le i \le k \ .$$

*Proof.* By Corollary 12 we have

$$1/\det A \le (3/2)/\det B \ .$$

Finally, by Lemma 10 it follows that

$$\|\underline{a}_i\| \le (4/3)\|\underline{b}_i\|, \quad 1 \le i \le k \ .$$

This implies the assertion. □

Now we can prove Theorem 2. First, note that

$$q_2(B, c, s_k) \ge q_1(B, c/3) \ . \tag{3}$$

So $A$ is non singular by Theorem 1.

Applying Lemma 10 we find that for

$$q \ge \log \lambda_k(T) - \log((c/3)\lambda_1(L))$$

we have

$$\|B\underline{t}_i\| < (1/(1-c/3))\|A\underline{t}_i\| \le (s_i/(1-c/3))\lambda_i(L(A)) \ .$$

Theorem 1 and (3) implies that

$$\lambda_i(L(A)) \le (1+c/3)\lambda_i(L), \quad 1 \le i \le k \ .$$

Since

$$(1+c/3)/(1-c/3) \le 1+c$$

this implies

$$\|B\underline{t}_i\| < (1+c)s_i\lambda_i(L)$$

for

$$q \geq \max\{\log \lambda_k(T) - \log((c/3)\lambda_1(L)),\ q_2(B, c, s_k)\} \ .$$

It remains to estimate $||\underline{t}_i||$. It follows from Corollary 9 that

$$||\underline{t}_i|| \leq \sqrt{k} s_i \lambda_i(L(A)) \mathrm{dft}(A)/\lambda_1(A) \ .$$

So the assertion follows from Lemma 13 and Theorem 1.

Now can prove Corollary 3. Given a basis $C = (\underline{c}_1, \ldots, \underline{c}_k) \in \mathbb{Z}^{m\times k}$ of a $k$-dimensional integral lattice $\Lambda$. The algorithm of [He] determines a reduced basis $D \in \mathbb{Z}^{m\times k}$ such that

$$||\underline{d}_i|| \leq \sqrt{(i+3)/4}\, \lambda_i(\Lambda), \quad 1 \leq i \leq k \ .$$

The algorithm performs at most $mk^{O(k)} \log |C|$ arithmetic operations on integers of binary length $O(k^2(\log k + \log |C|))$. Here, $|C|$ denotes the maximum of the absolute values of the entries of $C$. Choose a rational approximation $A$ to $B$ of precision

$$p = q_0(B, c, \sqrt{(k+3)/4}) \ .$$

Then

$$||A - B|| < 2^{-q_2(B,c,s)} \ .$$

Hence, if we apply the reduction algorithm of [He] to

$$C = 2^{p+1} A$$

and determine the reducing transformation $T = (\underline{t}_1, \ldots, \underline{t}_k) \in \mathrm{GL}(k, \mathbb{Z})$ then by Theorem 2 we have

$$||B\underline{t}_i|| \leq (1+c)\sqrt{(i+3)/4}\, \lambda_i(L), \quad 1 \leq i \leq k \ .$$

The transformation $T$ can be determined by applying each reducing elementary transformation not only to the basis but also to the $k \times k$ identity matrix. We analyse the running time. We first estimate $\log |C|$. By Lemma 10 we have $|A| < 2\, \lambda_k(B)$ and therefore

$$\begin{aligned} \log |C| = O(&k + \log m + \log(\lambda_k(L)/\lambda_1(L)) + \\ &\log(\lambda_k(B)/\lambda_1(B)) + \log(\mathrm{dft}(B)) + \log(1/c)) \ . \end{aligned}$$

Since

$$\lambda_i(L) \leq \lambda_i(B), \quad 1 \leq i \leq k$$

and

$$|\det(B)| = \det L \geq \left(\lambda_1(L)/\gamma_k^{1/2}\right)^k$$

where $\gamma_k = O(k)$ (see [LaLeSch] and [WaGr68]) it follows that

$$\log |C| = O(k(\log k + \beta) + \log m + \log(1/c))$$

with $\beta$ from Corollary 3.

The number of arithmetic operations to find the transformation is bounded by the number of arithmetic operations to find the reduced basis, namely

$$mk^{O(k)}(\log m + \beta + \log(1/c)) \ .$$

Let $C'$ be a basis which is computed in the course of the reduction. Let $T' \in \mathrm{GL}(k, \mathbb{Z})$ with $CT' = C'$. It follows from Corollary 9 that

$$|T'| \leq \lambda_k(C')\mathrm{dft}(A)/(2^{p+1}\lambda_1(A)) \ .$$

Since

$$\log |C'| = O\left(k^2\left(k\left(\log k + \beta\right) + \log m + \log(1/c)\right)\right)$$

Lemma 13 implies that

$$\log |T'| = O\left(k^2\left(k\left(\log k + \beta\right) + \log m + \log(1/c)\right)\right) \ .$$

To prove Corollary 4 we apply the same method using the following result of [LeLeLo]. Given a basis $C = (\underline{c}_1, \ldots, \underline{c}_k) \in \mathbb{Z}^{m\times k}$ of a $k$-dimensional integral lattice $\Lambda$. The algorithm of [LeLeLo] determines a reduced basis $D \in \mathbb{Z}^{m\times k}$ such that

$$||\underline{d}_i|| \leq 2^{(k-1)/2}\,\lambda_i(\Lambda), \quad 1 \leq i \leq k \ .$$

The algorithm performs at most $O(k^3 m \log |C|)$ arithmetic operations on integers of binary length $O(k \log |C|)$.

## References


[BuPo] J. Buchmann, M. Pohst: *Computing a lattice basis from a system of generating vectors*, Proceedings EUROCAL 87, Springer Lecture Notes in Computer Science **378**, 54-63, 1989.

[BuKe] J. Buchmann, V. Kessler: *Computing a reduced lattice basis from a generating system*, preprint, 1993.

[LeLeLo] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász: *Factoring polynomials with rational coefficients*, Math. Ann. **261**, 515-534, 1982.

[GrLoSchri] M. Grötschel, L. Lovász, A. Schrijver: *Geometric algorithms and combinatorial optimization*, Springer-Verlag Berlin Heidelberg, 1988.

[HaMcCu] J.L. Hafner, K.S. McCurley: *Asymptotically fast triangularization of matrices over rings*, SIAM J. Computation **20**, no. 6, 1068-1083, 1991.

[He] B. Helfrich, *Algorithms to construct Minkowski reduced and Hermite reduced lattice bases*, Theoretical Computer Science **41**, 125-139, 1985.

[Po] M. Pohst: *A modification of the LLL Reduction Algorithm*, J. Symbolic Computation, **4**, 123-127, 1987.

[LaLeSch] J.C. Lagarias, H.W. Lenstra Jr., C.P. Schnorr: *Korkine-Zolotarev bases and successive minima of a lattice and its dual lattice*, Combinatorica **10**, no.4, 333-348, 1990.

[WaGr68] B.L. van der Waerden and H. Gross: *Studien zur Theorie der Quadratischen Formen*, Birkhäuser, Basel, 1968.