Computing a reduced lattice basis from a generating system

Johannes Buchmann
FB-Informatik
Universität des Saarlandes
6600 Saarbrücken

Volker Kessler
Mathematisches Institut
Universität zu Köln
Weyertal 86-90
5000 Köln 41

August 4, 1993

Abstract

A polynomial time algorithm is presented that given a rational approximation to a lattice in real n-space and a lower bound for the first successive minimum calculates a reduced basis of that lattice.

1 Introduction

In this paper we study the following problem: Suppose that the vectors $\mathbf{a}_1, \ldots, \mathbf{a}_k$ in $\mathcal{Z}^{n_1} \times R^{n_2}, n = n_1 + n_2$, generate an r-dimensional lattice L, i.e.

$$L = \sum_{j=1}^{k} \mathcal{Z}\mathbf{a}_j.$$

Assume that we are given an algorithm that on input of some $q \in N$ calculates approximations to all the coordinates of those vectors such that the error is at most 2^{-k-1} Find a basis of that lattice; more precisely, an integer matrix that transforms the generating system into a basis of L.

This problem arises, for example, if we wish to compute a reduced $\mathcal{Z}$-basis of an order of an algebraic number field (see section 5), if we want to calculate a system of fundamental units of a number field from a generating system for the unit group (see [1],) or if we need to determine relations between logarithm vectors of units in the factoring algorithm number field sieve (see [4]).

The problem can be solved by means of the LLL reduction algorithm [3]. This has been shown in [2]. In that paper, however, the authors did not present bounds on the entries of the transformation matrix and on the size of the basis vectors. But the knowledge of such bounds is crucial in the analysis of algorithms that require a basis of L as an input.

In this paper we present a refined version of the method [2]. As in [2] we assume that we know bounds

$$\begin{aligned} \mu &\leq \lambda_1(L) = \min\{||\mathbf{v}|| \mid 0 \neq \mathbf{v} \in L\}, \\ \alpha &\geq \max\{||\mathbf{a}_j|| \mid 1 \leq j \leq k\}. \end{aligned}$$

where $||.||$ denotes the euclidean norm.

Our main result is the following: if the rational approximations to the generating vectors can be computed in polynomial time then it is possible to compute in time polynomial in $\log(\alpha/\mu)$ and $k + n$ an integer transformation to a basis $\mathbf{b}_1, \ldots, \mathbf{b_r}$ of L satisfying

$$||\mathbf{b}_j|| \leq (\sqrt{kn_2} + 2) \cdot \lambda_j(L) \quad (1 \leq j \leq n).$$

where $\lambda_j(L)$ denotes the j-th successive minimum in L, i.e. the radius of the smallest sphere containing j linearly independent vectors of L. This bound is only slightly weaker than the bound that is obtained if one applies the LLL-algorithm to linearly independent integer vectors. We will apply this result to the problem of computing reduced bases for orders of algebraic number fields.

2 Relations among the generators

We will compute a basis for L by applying the LLL-algorithm to a lattice that is constructed from rational approximations to the generating vectors and which has the property that short vectors in that lattice correspond to relations among the generators. Therefore, we discuss in this section rational approximations and relations for the generating system.

By $||.||_1, ||.||_\infty$ we denote the l_1-norm and the l_∞-norm, respectively. By $d(L)$ we denote the determinant of L.

Let $q \in N$ be a precision constant which will be specified below. Let

$$\mathbf{a}_j = (a_{1j}, \ldots, a_{nj})^t \quad (1 \le j \le k)$$

and

$$\hat{a}_{ij} := < 2^q a_{ij} > \quad (1 \le i \le n, 1 \le j \le k)$$

where $<>$ denotes the nearest integer function.

We define

$$\hat{\mathbf{a}}_j := (\hat{a}_{1j}, \ldots, \hat{a}_{nj})^t \in \mathcal{Z}^n \quad (1 \le j \le k).$$

Then we have

$$||\hat{\mathbf{a}}_j - 2^q \mathbf{a}_j|| \le \frac{\sqrt{n_2}}{2} \qquad (1 \le j \le k) \tag{1}$$

which implies

$$\begin{aligned} ||\hat{\mathbf{a}}_j|| &\le ||\hat{\mathbf{a}}_j - 2^q \mathbf{a}_j|| + 2^q ||\mathbf{a}_j|| \\ &\le \frac{\sqrt{n_2}}{2} + 2^q \alpha \quad (1 \le j \le k). \end{aligned} \tag{2}$$

An integer vector $\mathbf{z} = (z_1, \ldots, z_k)$ is called a *(non trivial) relation* for $\mathbf{a}_1, \ldots \mathbf{a}_k$ if $\mathbf{z} \ne 0$ and

$$\sum_{i=1}^{k} z_i \mathbf{a}_i = 0.$$

Proposition 2.1 *Let* $\mathbf{z} = (z_1, \ldots, z_n) \in \mathcal{Z}^k - \{0\}$ *and assume that*

$$2^q > \frac{\sqrt{n_2}}{\mu} ||\mathbf{z}||_1. \tag{3}$$

Then $\mathbf{z}$ *is a relation for* $\mathbf{a}_1, \ldots, \mathbf{a}_k$ *if and only if*

$$||\sum_{i=1}^{k} z_i \hat{\mathbf{a}}_i|| \le \frac{\sqrt{n_2}}{2} ||\mathbf{z}||_1. \tag{4}$$

Proof: If $\mathbf{z}$ is a relation then we have by (1)

$$||\sum_{i=1}^{k} z_i \hat{\mathbf{a}}_i|| \leq \sum_{i=1}^{k} |z_i| \; ||\hat{\mathbf{a}}_i - 2^q \mathbf{a}_i|| + 2^q ||\sum_{i=1}^{k} z_i \mathbf{a}_i|| \leq \frac{\sqrt{n_2}}{2} ||\mathbf{z}||_1.$$

On the other hand, if (4) holds then it follows from (1) and (3)

$$\begin{aligned} ||\sum_{i=1}^{k} z_i \mathbf{a}_i|| &\leq ||\sum_{i=1}^{k} z_i(\mathbf{a}_i - 2^{-q}\hat{\mathbf{a}}_i)|| + 2^{-q} ||\sum_{i=1}^{k} z_i \hat{\mathbf{a}}_i|| \\ &\leq 2 \cdot ||\mathbf{z}||_1 \cdot 2^{-q} \cdot \frac{\sqrt{n_2}}{2} < \mu. \end{aligned}$$

Since $\mu \leq \lambda_1(L)$ it follows that $\sum_{i=1}^{k} z_i \mathbf{a}_i = 0$. □

Proposition 2.2 *a) There are $k-r$ linearly independent relations $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ of $\mathbf{a}_1, \ldots, \mathbf{a}_k$ with*

$$||\mathbf{m}_j||_\infty \leq \frac{\alpha^r}{d(L).} \tag{5}$$

b) Assume that $\mathbf{a}_1, \ldots, \mathbf{a}_r$ are linearly independent. Let $\mathbf{v}_1, \ldots . \mathbf{v}_r \in L_r := \bigoplus_{i=1}^{r} \mathcal{Z}\mathbf{a}_i$ such that

$$||\mathbf{v}_j|| = \lambda_j(L_r) \quad (1 \leq j \leq r).$$

Let $\mathbf{x}_j = (x_{1j} \ldots, x_{rj}) \in \mathcal{Z}^r$ with

$$\mathbf{v}_j = \sum_{i=1}^{r} x_{ij} \mathbf{a}_i \quad (1 \leq j \leq r).$$

Then those coefficient vectors satisfy

$$||\mathbf{x}_j||_\infty \leq \lambda_j(L_r) \frac{\alpha^{r-1}}{d(L_r)} \quad (1 \leq j \leq r). \tag{6}$$

Proof: We construct an isometric embedding of L into R^r . Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of L and put $W := ((\mathbf{w}_i, \mathbf{w}_j)_{i,j})$ where $(.,.)$ denotes the standard inner product. Then there is a decomposition of $W = W'^t W'$ with $W' \in \mathrm{GL}_r(R)$. We denote the columns of W' by $\mathbf{w}'_1, \ldots, \mathbf{w}'_r$. The mapping

$$\begin{aligned} \varrho : L &\longrightarrow L' := \oplus_{i=1}^{r} \mathcal{Z}\mathbf{w}'_i \\ \sum x_i \mathbf{w}_i &\longmapsto \sum x_i \mathbf{w}'_i \end{aligned}$$

is an isometry between L and L' and we have $d(L) = d(L')$. We put $\mathbf{a}'_j = \varrho(\mathbf{a}_j)$ and

$$m_{ij} := \begin{cases} \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{i-1}, \mathbf{a}'_{j+r}, \mathbf{a}'_{i+1}, \ldots \mathbf{a}'_r)/d(L') & \text{for } 1 \leq i \leq r, 1 \leq j \leq k-r, \\ \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_r)/d(L') & \text{for } i = j + r, 1 \leq j \leq k-r, \\ 0 & \text{otherwise.} \end{cases}$$

The m_{ij} are 0 or indices of sublattices of L and therefore they are rational integers. Let $\mathbf{m}_j = (m_{1,j}, \ldots, m_{k,j})$ for $1 \le j \le k - r$. Since

$$(\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}) = \left(\begin{array}{ccc} & * & \\ \hline m_{r+1,1} & & 0 \\ & \ddots & \\ 0 & & m_{k,k-r} \end{array} \right)$$

with $m_{j+r,j} \neq 0$ for $1 \le j \le k - r$ the $\mathbf{m}_j$ are linearly independent. By Cramer's rule we obtain

$$\varrho\left(\sum_{i=1}^{k} m_{ij}\mathbf{a}_i\right) = \sum_{i=1}^{k} m_{ij}\mathbf{a}'_i = 0 \text{ for } 1 \le j \le k - r.$$

Using Hadamard's inequality we conclude that

$$|m_{ij}| \le \frac{\alpha^r}{d(L)}$$

which proves a).

Moreover, by Cramer's rule and Hadamard's inequality it follows from $\varrho(\mathbf{v}_j) = \sum_{i=1}^{r} x_{ij}\varrho(\mathbf{a}_j)$ that

$$|x_{ij}| = \left| \frac{\det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{i-1}, \varrho(\mathbf{v}_j), \mathbf{a}'_{i+1}, \ldots, \mathbf{a}'_r)}{\det(\mathbf{a}'_1, \ldots, \mathbf{a}'_r)} \right| \le \lambda_j(L_r)\frac{\alpha^{r-1}}{d(L_r}.$$

□

3 The approximate lattice

We define

$$\tilde{\mathbf{a}}_j = (\mathbf{e}_j, \hat{\mathbf{a}}_j) \quad (1 \le j \le k)$$

where $\mathbf{e}_j$ denotes the j-th unit vector of $\mathcal{Z}^k$. Then $\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_k$ are linearly independent and therefore a basis of the lattice

$$\tilde{L} = \bigoplus_{j=1}^{k} \mathcal{Z}\tilde{\mathbf{a}}_j.$$

Proposition 3.1 *Assume that*

$$2^q > \frac{(\sqrt{n_2 k} + 2) \cdot \lambda \cdot 2^{\frac{k-3}{2}}}{\mu} \tag{7}$$

with $\lambda \in R$. Suppose that $\mathbf{z} = (z_1, \ldots, z_k) \in \mathcal{Z}^k$ is not a relation for $\mathbf{a}_1, \ldots, \mathbf{a}_k$. Let $\tilde{\mathbf{x}} = \sum_{i=1}^{k} z_i\tilde{\mathbf{a}}_i$. Then we have

$$||\tilde{\mathbf{x}}|| > 2^{\frac{k-1}{2}}\lambda. \tag{8}$$

Proof: Write $\tilde{\mathbf{x}} = (\mathbf{z}, \hat{\mathbf{x}})$. Then we have

$$||\tilde{\mathbf{x}}||^2 = ||\mathbf{z}||^2 + ||\hat{\mathbf{x}}||^2.$$

If $||\mathbf{z}|| > 2^{\frac{k-1}{2}}\lambda$, then we are done. Otherwise we have

$$\begin{aligned}
||\tilde{\mathbf{x}}|| &\geq ||\hat{\mathbf{x}}|| \\
&= ||\sum_{i=1}^{k} z_i \hat{\mathbf{a}}_i|| \\
&\geq 2^q ||\sum_{i=1}^{k} z_i \mathbf{a}_i|| - ||\sum_{i=1}^{k} z_i (2^q \mathbf{a}_i - \hat{\mathbf{a}}_i)|| \\
&\geq 2^q ||\sum_{i=1}^{k} z_i \mathbf{a}_i|| - ||\mathbf{z}||_1 \cdot \frac{\sqrt{n_2}}{2} \\
&\geq 2^q \mu - \frac{\sqrt{n_2 \cdot k}}{2} ||\mathbf{z}|| \\
&\geq 2^q \mu - \sqrt{n_2 k} \cdot 2^{\frac{k-3}{2}} \lambda \\
&> 2^{\frac{k-1}{2}} \lambda.
\end{aligned}$$

$\square$

Proposition 3.2 *Assume that (7) holds with*

$$\lambda = (\frac{k\sqrt{n_2}}{2} + \sqrt{k}) \frac{\alpha^r}{d(L)}.$$

then

$$\begin{aligned}
\lambda_j(\tilde{L}) &\leq \lambda && \textit{for } 1 \leq j \leq k-r, \\
\lambda_j(\tilde{L}) &\leq 2^{q+1} \lambda_{j-k+r}(L_r) && \textit{for } k-r+1 \leq j \leq k.
\end{aligned}$$

Proof: Let $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ be the $(k-r)$ independent relations constructed in the proof of Proposition 2.2. We put

$$\tilde{\mathbf{m}}_j = \sum_{i=1}^{k} m_{ij} \tilde{\mathbf{a}}_i = (\mathbf{m}_j, \sum_{i=1}^{k} m_{ij} \hat{\mathbf{a}}_i) \quad (1 \leq j \leq k-r).$$

Of course, the $\tilde{\mathbf{m}}_1, \ldots, \tilde{\mathbf{m}}_{k-r}$ are linearly independent and using Proposition 2.1 we obtain

$$\begin{aligned}
||\tilde{\mathbf{m}}_j|| &\leq ||\mathbf{m}_j|| + ||\sum_{i=1}^{k} m_{ij} \hat{\mathbf{a}}|| \\
&\leq ||\mathbf{m}_j|| + \frac{\sqrt{n_2}}{2} ||\mathbf{m}_j||_1 \\
&\leq \sqrt{k} ||\mathbf{m}_j||_\infty + \frac{k \cdot \sqrt{n_2}}{2} ||\mathbf{m}_j||_\infty \\
&\leq \left(\frac{k \cdot \sqrt{n_2}}{2} + \sqrt{k} \right) \frac{\alpha^r}{d(L)} \leq \lambda.
\end{aligned}$$

Proposition 2.1 may be applied because

$$\frac{\sqrt{n_2}}{\mu}||\mathbf{m}_j||_1 \leq \frac{\sqrt{n_2}}{\mu}k||\mathbf{m}_j||_\infty \leq \frac{\sqrt{n_2}}{\mu}k\frac{\alpha^r}{d(L)} \leq \sqrt{n_2 k} \cdot \frac{\lambda}{\mu} < 2^q.$$

This proves the first inequality.

Furthermore, let $\mathbf{x}_1, \ldots, \mathbf{x}_r$ be defined as in Proposition 2.2) b). We put

$$\tilde{\mathbf{v}}_j := \sum_{i=1}^{r} x_{ij}\tilde{\mathbf{a}}_j.$$

Denoting the matrices $(\mathbf{x}_1, \ldots, \mathbf{x}_r), (\mathbf{v}_1, \ldots, \mathbf{v}_r), (\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_r), (\mathbf{a}_1, \ldots, \mathbf{a}_r), (\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_r)$ by $X, V, \tilde{V}, A, \tilde{A}$, respectively, we obtain

$$\begin{array}{rcl} V & = & AX, \\ \tilde{V} & = & \tilde{A}X. \end{array}$$

Since rank V = rank $A = r$, it follows from the first equation that X is non singular. This implies that rank $\tilde{V}$ = rank $\tilde{A} = r$.

Since the first $k + r$ rows of the matrix

$$(\tilde{\mathbf{m}}_1, \ldots \tilde{\mathbf{m}}_{k-r}, \tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_r) \in \mathcal{Z}^{(n+k)\times k}$$

are of the form

$$\left(\begin{array}{ccc|c} & * & & \mathrm{X} \\ \hline m_{1+r,1} & & 0 & \\ & \ddots & & * \\ 0 & & \mathbf{m}_{k+r,k} & \end{array}\right)$$

with $m_{j+r,j} \neq 0$ for $1 \leq j \leq k - r$, the system $\{\tilde{\mathbf{m}}_1, \ldots, \tilde{\mathbf{m}}_{k-r}, \tilde{\mathbf{v}}_1 \ldots, \tilde{\mathbf{v}}_r\}$ is linearly independant.

But the $\mathbf{x}_j$ are not relations for the $\mathbf{a}_j$, it follows from Proposition 3.1 that

$$||\tilde{\mathbf{v}}_j|| > 2^{\frac{k-1}{2}}\lambda \quad (1 \leq j \leq r).$$

On the other hand we obtain from Proposition 2.2 b)

$$\begin{array}{rcl} ||\tilde{\mathbf{v}}_j|| & \leq & ||\mathbf{x}_j|| + ||\sum_{i=1}^{r} x_{ij}\hat{\mathbf{a}}_i|| \\ & \leq & \sqrt{r}||\mathbf{x}_j||_\infty + ||\sum_{i=1}^{r} x_{ij}(\hat{\mathbf{a}}_i - 2^q\mathbf{a}_i)|| + ||\sum_{i=1}^{r} x_{ij}2^q\mathbf{a}_i|| \\ & \leq & \sqrt{r}||\mathbf{x}_j||_\infty + ||\mathbf{x}_j||_1\frac{\sqrt{n_2}}{2} + 2^q||\mathbf{v}_j|| \end{array}$$

$$
\begin{aligned}
&\leq \left(\sqrt{r} + \frac{r \cdot \sqrt{n_2}}{2}\right) ||\mathbf{x}_j||_\infty + 2^q \lambda_j(L_r) \\
&\leq 2^q \lambda_j(L_r) \cdot \left(1 + 2^{-q}\left(\sqrt{r} + \frac{r \cdot \sqrt{n_2}}{2}\right) \frac{\alpha^{r-1}}{d(L)}\right) \\
&\leq 2^q \lambda_j(L_r) \cdot \left(1 + 2^{-q}\frac{\lambda}{\alpha}\right) \\
&< 2^q \lambda_j(L_r)(1+1) = 2^{q+1}\lambda_j(L_r).
\end{aligned}
$$

The last inequality follows from the fact that because of our choice of q we have

$$2^q > \frac{\lambda}{\mu} \geq \frac{\lambda}{\alpha}.$$

□

4 The algorithm

We apply the LLL-algorithm [3] to the lattice basis $\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_k$ and obtain the LLL-reduced basis $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_k$ which we write as

$$\tilde{\mathbf{b}}_j = (\mathbf{m}_j, \hat{\mathbf{b}}_j) \quad (1 \leq j \leq k)$$

with $\mathbf{m}_j = (m_{1j}, \ldots m_{kj}) \in \mathcal{Z}^k$ and $\hat{\mathbf{b}}_i = (\hat{b}_{1j}, \ldots, \hat{b}_{nj}) \in \mathcal{Z}^n$ $(1 \leq j \leq k)$. Using those basis vectors we can both find relations for $\mathbf{a}_1, \ldots, \mathbf{a}_k$ and a basis of L.

Theorem 4.1 *Assume that (7) holds with λ as in Proposition 3.2. Then we have*

$$||\mathbf{m}_j|| \leq \begin{cases} 2^{\frac{k-1}{2}}\lambda & \textit{for } 1 \leq j \leq k-r, \\ 2^{\frac{k-1}{2}+q+1}\lambda_{j-k+r} & \textit{for } k-r+1 \leq j \leq r. \end{cases} \tag{9}$$

Moreover, the vectors $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ are linearly independent relations for $\mathbf{a}_1, \ldots, \mathbf{a}_k$ and the vectors

$$\mathbf{b}_j = \sum_{i=1}^{k} m_{i,k-r+j}\mathbf{a}_i \quad (1 \leq j \leq r)$$

form a basis for L and satisfy

$$||\mathbf{b}_j|| \leq (\sqrt{kn_2} + 2) \cdot 2^{\frac{k-1}{2}} \cdot \lambda_{j-(k-r)}(L_r) \quad (1 \leq j \leq r). \tag{10}$$

Proof: From [3] (1.12) we know that

$$||\tilde{\mathbf{b}}_j|| \leq 2^{\frac{k-1}{2}} \cdot \lambda_j(\tilde{L}) \quad (1 \leq j \leq k)$$

and because of Proposition 3.2 we have

$$\begin{array}{ll} \|\tilde{\mathbf{b}}_j\| \le 2^{\frac{k-1}{2}}\lambda & \text{for } 1 \le j \le k-r, \\ \|\tilde{\mathbf{b}}_j\| \le 2^{\frac{k-1}{2}+q+1}\lambda_{j-(k-r)}(L_r) & \text{for } k-r+1 \le j \le r. \end{array}$$

Therefore it follows from Proposition 3.1 that $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ are relations for $\mathbf{a}_1, \ldots, \mathbf{a}_k$ and clearly

$$\|\mathbf{m}_j\| \le \|\tilde{\mathbf{b}}_j\| \le 2^{\frac{k-1}{2}}\lambda \text{ for } 1 \le j \le k-r.$$

To show that $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ are linearly independent and that $\{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$ is a basis of L we use the following abbreviations:

$$\begin{array}{rcllcl} M & = & (\mathbf{m}_1, \ldots, \mathbf{m}_k) & \in & \mathcal{Z}^{k\times k}, \\ A & = & (\mathbf{a}_1, \ldots, \mathbf{a}_k) & \in & R^{n\times k}, \\ \tilde{A} & = & (\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_k) & \in & \mathcal{Z}^{(n+k)\times k}, \\ B & = & AM & \in & R^{n\times k}, \\ \tilde{B} & = & (\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_k) & \in & \mathcal{Z}^{(n+k)\times k}. \end{array}$$

Then we have

$$\tilde{B} = \tilde{A}M$$

i.e. M is a basis transformation and therefore $M \in \mathrm{GL}_k(\mathcal{Z})$. In particular, the columns $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ are linearly independent.

Since rank $A = r$ and since $M \in \mathrm{GL}_k(\mathcal{Z})$ it follows

$$\text{rank } B = r.$$

But $\mathbf{m}_1, \ldots, \mathbf{m}_{k-r}$ are relations for $\mathbf{a}_1, \ldots, \mathbf{a}_k$ and therefore the first $k-r$ columns of B are zero-vectors which implies that

$$\text{rank } (\mathbf{b}_{k-r+1}, \ldots, \mathbf{b}_k) = r.$$

Since M is invertible we conclude that $\mathbf{b}_{k-r+1}, \ldots, \mathbf{b}_k$ is also a generating system for $L = \sum\limits_{i=1}^{k} \mathcal{Z}\mathbf{a}_i$.

Finally, we have for $k-r+1 \le j \le k$

$$\begin{array}{rcl} \|\mathbf{b}_{j-k+r}\| & = & \|\sum\limits_{i=1}^{k} m_{ij}\mathbf{a}_i\| \\ & \le & \|\sum\limits_{i=1}^{k} m_{ij}(\mathbf{a}_i - 2^{-q}\hat{\mathbf{a}}_i)\| + 2^{-q}\|\sum\limits_{i=1}^{k} m_{ij}\hat{\mathbf{a}}_i\| \\ & \le & \|\mathbf{m}_j\|_1 2^{-q}\dfrac{\sqrt{n_2}}{2} + 2^{-q}\|\tilde{\mathbf{b}}_j\| \\ & \le & \sqrt{kn_2}\|\mathbf{m}_j\| 2^{-q-1} + 2^{-q}\|\tilde{\mathbf{b}}_j\| \\ & \le & (\sqrt{kn_2}+2)2^{-q-1}2^{\frac{k-1}{2}+q+1}\lambda_{j-(k-r)}(L_r) \\ & \le & (\sqrt{kn_2}+2)2^{\frac{k-1}{2}}\lambda_{j-(k-r)}(L_r). \end{array}$$

□

Theorem 4.2 *If q is chosen minimal such that (7) is satisfied with λ from Proposition 3.2 then the algorithm requires*

$$O\left((n+k)^6 \cdot k^3 (\log(\alpha/\mu))^3\right)$$

bit operations.

Proof:

We know from [3] Proposition 1.26 that LLL-reduction requires $O(\overline{n}^6(\log\overline{\alpha})^3)$ bit operations where $\overline{n}$ denotes the dimension of the lattice (in our case $\overline{n} = n + k$) and $\overline{\alpha}$ is an upper bound for the norms of the input vectors to which the LLL-algorithm is applied. By [5] p. 197 we have a lower bound for $d(L)$

$$d(L) \geq \left(\frac{\mu}{\gamma_r^{\frac{1}{2}}}\right)^r$$

where γ_r^r denotes the r-th Hermite constant.

We obtain from (2) and (7) that

$$\overline{\alpha} \leq (\sqrt{n_2 k} + 2)\left(\frac{k\sqrt{n_2}}{2} + \sqrt{k}\right) 2^{\frac{k-3}{2}} \left(\frac{\alpha}{\mu}\right)^{r+1} \gamma_r^{\frac{r}{2}} + \frac{\sqrt{n_2}}{2}$$

which implies that

$$\log\overline{\alpha} = O\left(k + r\log\left(\frac{\alpha}{\mu}\right)\right) = O\left(k \cdot \log\left(\frac{\alpha}{\mu}\right)\right).$$

□

The method described so far yields basis vectors whose lengths are bounded in terms of successive minima of sublattices of L. In practice, one would like to have estimates that depend only on the dimension and on the successive minima of the full lattice. Such a basis is computed by applying the same procedure a second time to the basis obtained from the generating system. The analysis of this second application of the LLL-algorithm is the same as above except that we must replace the upper bound α by

$$\alpha' = (\sqrt{k n_2} + 2) \cdot 2^{\frac{k-1}{2}} \cdot \alpha.$$

and λ by λ' which is obtained by replacing α with α' in the formula for λ. The upper bound for the lengths of the vectors to which the LLL-algorithm is applied becomes

$$\overline{\alpha} \leq \left(\sqrt{n_2 k} + 2\right)^{r+2} \left(\frac{k\sqrt{n_2}}{2} + \sqrt{k}\right) \cdot 2^{(r+2)\cdot\frac{k-1}{2}} \left(\frac{\alpha}{\mu}\right)^{r+1} \gamma_r^{\frac{r}{2}} + \frac{\sqrt{n_2}}{2}.$$

Therefore

$$\log \overline{\alpha} = O\left(r \cdot k + r \cdot \log\left(\frac{\alpha}{\mu}\right)\right) = O\left(k^2 \log\left(\frac{\alpha}{\mu}\right)\right)$$

and the second iteration takes

$$O\left((n+k)^6 \cdot k^6 \cdot (\log \frac{\alpha}{\mu})^3\right)$$

bit operations.

Corollary 4.1 *There is an algorithm that on input of μ, α, and $\hat{\mathbf{a}}_1, \ldots, \hat{\mathbf{a}}_k$ computes coefficient vectors $\mathbf{m}_j = (m_{1,j}, \ldots, m_{k,j})$ $(1 \le j \le r)$ with*

$$||\mathbf{m}_j|| \le 2^{k-2} \frac{(\sqrt{n_2 k} + 2)\lambda'}{\mu} \alpha' \quad (1 \le j \le r)$$

such that the vectors

$$\mathbf{b}_j = \sum_{i=1}^{k} m_{i,j} \mathbf{a}_i \quad (1 \le j \le r)$$

form a basis of L and satisfy

$$||\mathbf{b}_j|| \le (\sqrt{r n_2} + 2) \cdot 2^{\frac{r-1}{2}} \cdot \lambda_j(L) \quad (1 \le j \le r). \tag{11}$$

This algorithm requires

$$O\left((n+k)^6 \cdot k^6 (\log(\alpha/\mu))^3\right)$$

bit operations.

Using Minkowski's second fundamental theorem

$$\prod_{i=1}^{r} \lambda_i(L) \le 2^r \cdot d(L)$$

we obtain

Corollary 4.2 *The basis vectors $\mathbf{b}_i$ computed by the algorithm of Corollary 4.1 satisfy*

$$\prod_{i=1}^{r} ||\mathbf{b}_i|| \quad \le \quad (n+2)^r \cdot 2^{\frac{r(r-1)}{2}} d(L) \tag{12}$$

and

$$||\mathbf{b}_1|| \le (n+2) \cdot 2^{\frac{r-1}{2}} d(L)^{\frac{1}{r}}. \tag{13}$$

For large k (i.e. k is not bounded by a linear polynomial in n) it is more efficient to iteratively apply the above method to $r+1$ input vectors rather than dealing with all vectors at once.

A similar analysis as above yields the following statement:

Corollary 4.3 *The same results as in Theorem 4.1 and in Corollary 4.1 can be obtained using*

$$O(kn^{12}(\log(\alpha/\mu))^3)$$

bit operations.

5 Reducing $\mathcal{Z}$-bases of orders

Let $\mathcal{F}$ be an algebraic number field of degree n over the field $\mathcal{Q}$ of rational numbers. Let $\mathcal{O}$ be an order in $\mathcal{F}$ of absolute descriminant D. We assume that $\mathcal{O}$ is given in terms of the multiplication table of a $\mathcal{Z}$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}$:

$$\omega_i\omega_j = \sum_{k=1}^{n} w_{ijk}\omega_k \quad (1 \leq i, j \leq n) \tag{14}$$

where the coefficients w_{ijk} are rational integers.

In this section we describe a method for finding a $\mathcal{Z}$-basis for $\mathcal{O}$ where the coefficients in the multiplication table (14) are bounded by a polynomial in D. The basic facts about algebraic number fields can be found in [5].

For $1 \leq i \leq n$ we denote by

$$\mathcal{F} \longrightarrow C, \ \alpha \longmapsto \alpha^{(i)}$$

the isomorphisms of $\mathcal{F}$ into the field C of complex numbers. The first r_1 of those isomorphisms are real, the last $2r_2$ isomorphisms are non real and numbered such that for any $\alpha \in \mathcal{F}$ and $1 \leq i \leq r_2$ we have $\overline{\alpha^{(r_1+i)}} = \alpha^{(r_1+r_2+i)}$ where for $x \in C$ we denote by $\overline{x}$ the complex conjugate of x. The mapping

$$\begin{array}{lll} \mathcal{F} & \longrightarrow & R^n, \\ \alpha & \longmapsto & \underline{\alpha} = \left(\alpha^{(1)}, \ldots, \alpha^{(r_1)}, Re\ \alpha^{(r_1+1)},\ Im\ \alpha^{(r_1+1)}, \ldots, Re\ \alpha^{(r_1+r_2)}, Im\ \alpha^{(r_1+r_2)}\right) \end{array}$$

is a field monomorphism. The image $\underline{\alpha}$ of $\alpha \in \mathcal{F}$ is called its *conjugate vector.* The image $\underline{\mathcal{O}}$ is an n-dimensional lattice of determinant

$$d(\underline{\mathcal{O}}) = 2^{-r_2}\sqrt{D}.$$

We determine a $\mathcal{Z}$-basis of $\mathcal{O}$ with small coefficients in its multiplication table by applying the above method to a rational approximation of the lattice basis $\underline{\omega}_1, \ldots, \underline{\omega}_n$. Those approximations can be found in polynomial time since we can compute the characteristic polynomials of the basis elements from the multiplication table in polynomial time.

By Corollary 4.2 the reduced $\mathcal{Z}$-basis $\underline{\omega}'_1, \ldots, \underline{\omega}'_n$ has the property

$$\prod_{j=1}^{n} ||\underline{\omega}'_j|| \leq (n+2)^n \cdot 2^{n\cdot(n-1)/2-r_2}\sqrt{D}. \tag{15}$$

In order to find an upper bound on the conjugates of the new basis elements, we need the following result:

Proposition 5.1 *Let $\alpha \in \mathcal{O},\ \alpha \neq 0$. Then $||\underline{\alpha}|| \geq \sqrt{n/2}$.*

Proof: We have

$$\prod_{i=1}^{n} |\alpha^{(i)}| = |N(\alpha)| \geq 1 \tag{16}$$

where $N(\alpha)$ is the norm of α over $\mathcal{Q}$. Moreover, it follows from the inequality between the geometric and the arithmetic mean that

$$|N(\alpha)|^{2/n} \leq \frac{1}{n}\sum_{i=1}^{n} |\alpha^{(i)}|^2 \leq \frac{2}{n}\sum_{i=1}^{r_1+r_2} |\alpha^{(i)}|^2 = \frac{2}{n}||\underline{\alpha}||^2$$

and therefore by (16)

$$||\underline{\alpha}|| \geq \sqrt{n/2}.$$

□

From (15) and Proposition 5.1 we obtain the following statement:

Proposition 5.2 *We have the following estimate for the conjugate vector of the reduced basis elements*

$$||\underline{\omega'_j}|| \leq n^{(n+1)/2} \cdot 2^{(n^2-1)/2+r_1+r_2}\sqrt{D} \quad (1 \leq j \leq n)$$

Proof:

$$\begin{aligned} ||\underline{\omega'_j}|| &\leq \frac{(n+2)^n \cdot 2^{n(n-1)/2-r_2}\sqrt{D}}{(n/2)^{\frac{n-1}{2}}} = \frac{(n+2)^n}{n^{n-1/2}} \cdot 2^{n^2-1/2-r_2}\sqrt{D} \\ &\leq n^{(n+1)/2} \cdot 2^{n^2-1/2+r_1+r_2}\sqrt{D} \end{aligned}$$

□

This estimate is now used to find bounds on the coeffients $w'_{ijk} \in \mathcal{Z} \quad (1 \leq i,j,k \leq n)$ in the multiplication table

$$\omega'_i\omega'_j = \sum_{k=1}^{n} w'_{ijk}\omega'_k (1 \leq i,j \leq n) \tag{17}$$

of the reduced basis. Equation (17) is true for all the conjugates:

$$\left(\omega'_i\omega'_j\right)^{(l)} = \sum_{k=1}^{n} w'_{ijk}\left(\omega'_k\right)^{(l)} \quad (1 \leq l \leq n)(1 \leq i,j \leq n) \tag{18}$$

and therefore

$$\underline{\omega'_i\omega'_j} = \sum_{k=1}^{n} \omega'_{ijk}\underline{\omega'_k} \quad (1 \leq i,j \leq n). \tag{19}$$

It follows from (19), Proposition 5.2 and Cramer's rule that

$$\begin{aligned} |w'_{ijk}| &\leq \frac{(n^{n+1/2}2^{(n^2-1)/2+r_1+r_2}\sqrt{D})^{n+1}}{2^{-r_2}\sqrt{D}} \\ &\leq n^{(n+1)^{2/2}} \cdot 2^{(n+1)(n^2-1)/2+n(n-r_2)+n} D^{n/2}. \end{aligned}$$

Thus we have proved

Proposition 5.3 *There is a polynomical time algorithm that on input of the multiplication table of a $\mathcal{Z}$-basis of O calculates a $\mathcal{Z}$-basis $\omega'_1, \ldots, \omega'_n$ of O such that the coefficients w'_{ijk} in the multiplication table (17) satisfy*

$$|w'_{ijk}| \leq n^{(n+1)2/2} 2^{(n+1)(n^2+1)/2+n^2} D^{\frac{n}{2}} \quad (1 \leq i,j,k \leq n).$$

References

[1] J. Buchmann, S. Düllmann, *A probabilistic class group and regulator algorithm and its implementation*, Proceedings of the Colloquium on Computational number Theory, Drebrecen, 1989, de Gruyter, 1991, 73-72.

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

[3] A.K. Lenstra, H.W. Lenstra Jr. and C. Lovasz, *Factoring polynomials with rational coefficients*, Math Anm. 261 (1982), 515-534.

[4] A.K. Lenstra, H.W. Lenstra Jr., M.S. Manasse, J.M. Pollard, *The number field sieve*, Proceedings STOC 1990, 564-572.

[5] M. Pohst, H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press 1990.