MATHEMATICS OF COMPUTATION
VOLUME 52, NUMBER 185
JANUARY 1989, PAGES 149-159

Computation of Independent Units in Number Fields by Dirichlet's Method*

By Johannes Buchmann and Attila Pethö

Abstract. Using the basis reduction algorithm of A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász [8] and an idea of Buchmann [4], we describe a method for computing maximal systems of independent units in arbitrary number fields. The tables in the supplements section display such systems for the fields $\mathbf{Q}(\sqrt[n]{D})$ where $6 \leq n \leq 11$.

1. Introduction. Let K be an algebraic number field of degree $n \geq 2$ over $\mathbf{Q}$, let R be an order in K and let E be the group of units of R. The structure of E was described in 1846 by Dirichlet [6]. He proved that if K has s real and $2t$ nonreal conjugate fields, then E is the direct product of the finite group of the roots of unity in E and $r = s+t-1$ infinite cyclic groups. In the sequel we assume $r \geq 1$.

Dirichlet's proof was based on his diophantine approximation theorem: Let $\alpha_1, \dots, \alpha_n \in R$, $n \geq 2$; then there exist for any $Q \in R$, $Q > 1$, integers $x_1, \dots, x_n$ which are not all zero such that

$$\begin{aligned} &|x_i| \leq Q, \qquad i = 2, \dots, n, \\ &\left|\sum \alpha_i x_i\right| \leq |\alpha_1| Q^{-(n-1)}. \end{aligned} \tag{1.1}$$

One can find this proof, for example, in Dedekind's classical book [5, §183]. If $n = 2$, then the convergents of the continued fraction expansion of α_1/α_2 solve (1.1).

Unfortunately, there exists for $n > 2$ no general practical method for the solution of the approximation problem (1.1).

The importance of the unit group inspired many mathematicians to find algorithms which produce systems of fundamental units, or at least systems of independent units. A system $\{\varepsilon_1, \dots, \varepsilon_u\} \subseteq E$ is called *independent* if $\varepsilon_1^{m_1} \cdots \varepsilon_u^{m_u} = 1$ implies $m_1 = \cdots = m_u = 0$ for every system of integers $\{m_1, \dots, m_u\}$. $\{\varepsilon_1, \dots, \varepsilon_r\} \subseteq E$ is called a system of *fundamental units* if it generates the maximal torsion free subgroup of E. Most of the former algorithms are based on generalizations of the continued fraction algorithm and are applicable only to special number fields. For a complete list of references we refer to Brentjes [2] and Buchmann [3].

The method of Pohst and Zassenhaus [10] has another foundation. It produces many integers of bounded norm by solving certain inequalities. This procedure

Received July 22, 1985; revised November 26, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R27; Secondary 11J68, 12-04.

*This work was written when the second author was a visitor at the University of Köln on a fellowship of the Alexander von Humboldt-Stiftung.

yields units because there are only finitely many nonassociated elements of bounded norm in the order R. This method was improved by Fincke and Pohst [7].

The basis reduction algorithm of Lenstra, Lenstra and Lovász [8]—in the following LLL-algorithm—solves the following approximation problem very fast:

$$\begin{aligned} &|x_i| \le 2^{n/4}Q, \qquad i = 2, \ldots, n, \\ &\left|\sum x_i\alpha_i\right| \le |\alpha_1| Q^{-(n-1)}, \end{aligned} \tag{1.2}$$

which is slightly weaker than (1.1). Thus, the LLL-algorithm combined with Dirichlet's original idea yields theoretically a useful method for finding independent units. But in practical computation, this combination has the disadvantage that if Q increases, then $\sum x_i\alpha_i$ decreases very fast, and one must use multiprecision arithmetic. We were able to remove this disadvantage using an idea of Buchmann [4].

We do not vary Q but the α_i's. We apply the LLL-algorithm in each step two times. First we vary the α_i's in such a way that all their conjugates have always the same "small" order of magnitude, and then we solve (1.2) for the new α_i's and with the unchanged Q. In this way we compute independent units without handling too large or too small numbers. We are working with such numbers only if we want to calculate the coefficients of the units in the original basis of the order.

The comparison of our computational results in pure quintic fields with tables of fundamental units, computed by the method [3], showed that our method yields often fundamental units. If this is not the case, then one can compute such a system from a set of independent units, for example by the method of Fincke and Pohst [7].

In Section 2 we give an informal description of the basic steps of the algorithm. In Section 3 we study the connection between LLL-reduced bases of lattices, diophantine approximation and the algorithmization of Dirichlet's proof of the unit theorem. Section 4 contains the detailed description of the algorithm. To illustrate the efficiency of the method, we have computed maximal systems of independent units in number fields $\mathbf{Q}(\sqrt[n]{D})$, where $6 \le n \le 11$, which are presented in the tables of the supplements section at the end of this issue.

2. First Outline of the Method. Let K be an algebraic number field with s real conjugate fields $K^{(1)}, \ldots, K^{(s)}$ and t pairs of complex conjugate fields $K^{(s+1)}, \overline{K^{(s+1)}}, \ldots, K^{(s+t)}, \overline{K^{(s+t)}}$, and let R be an order of K. For every "conjugate direction" $i \in \{1, \ldots, s+t\}$ we construct a sequence $(\gamma_k)_{k\in\mathbf{N}}$ of numbers of bounded norm in R with

$$\begin{aligned} &|\gamma_k^{(i)}| < |\gamma_{k-1}^{(i)}| \quad \text{for } k \ge 2, \\ &|\gamma_k^{(j)}| > |\gamma_{k-1}^{(j)}| \quad \text{for } j \in \{1, \ldots, s+t\}, j \ne i, k \ge 2. \end{aligned} \tag{2.1}$$

Obviously, these numbers have to be pairwise distinct, and after a finite number of steps two of these numbers are associated with a nontrivial unit ε_i satisfying

$$|\varepsilon_i^{(i)}| < 1 \text{ and } |\varepsilon_i^{(j)}| > 1 \quad \text{for } j \ne i. \tag{2.2}$$

It is well known that every subsystem of cardinality $s+t-1$ in $\{\varepsilon_1, \ldots, \varepsilon_{s+t}\}$ is a maximal system of independent units in R (cf. [9]).

The sequence $(\gamma_k)_{k\in\mathbf{N}}$ is constructed as follows: To initialize the sequence, we set

$$\gamma_1 = 1. \tag{2.3}$$

Now suppose that we know γ_k. Then we define

$$R_k = \frac{1}{\gamma_k}R, \qquad N_k = |N_{K|\mathbf{Q}}(\gamma_k)|, \tag{2.4}$$

and using techniques of diophantine approximation, we compute a number β_k in the module R_k satisfying

$$|\beta_k^{(i)}| < 1, f_1 > |\beta_k^{(j)}| > 1 \quad \text{for } j \in \{1, \ldots, s+t\}, j \neq i, \tag{2.5}$$

and

$$|N_{K|\mathbf{Q}}(\beta_k)| \leq f_2 N_k^{-1},$$

where f_1, f_2 are constants depending only on the degree n of K and on the discriminant of the order R. Then we set

$$\gamma_{k+1} := \gamma_k \beta_k. \tag{2.6}$$

Obviously, the sequence $(\gamma_k)_{k\in\mathbf{N}}$ constructed like this satisfies the requirements of (2.1).

The advantage of our method is the following: All the conjugates of the numbers β_k and of the elements in the basis of R_k are—independent of k—of "small" size during the whole algorithm. Moreover, the question of whether two of the γ_k's, e.g., γ_{k_1} and γ_{k_2}, are associated can be answered in terms of the basis of the corresponding modules, since

$$\gamma_{k_1} \sim \gamma_{k_2} \Leftrightarrow R_{k_1} = R_{k_2}. \tag{2.7}$$

In fact, (2.7) follows directly from

$$\bigwedge_{\alpha \in K} (\alpha R = R \Leftrightarrow \alpha \text{ is a unit of } R). \tag{2.8}$$

Finally, if $\gamma_{k_1} \sim \gamma_{k_2}$ $(k_1 < k_2)$, then the corresponding unit can be computed by the formula

$$\varepsilon_i = \prod_{l=k_1}^{k_2-1} \beta_l. \tag{2.9}$$

So we do not have to know the γ_k's explicitly, and we can carry out all computations, except for the final computation of the unit ε_i, using only "small" numbers. For this reason, our method can be applied very efficiently to fields of high degrees and large discriminants.

3. Basis Reduction and Diophantine Approximation. First of all, let us briefly recall some definitions and results of the basis reduction theory of Lenstra, Lenstra and Lovász [8].

Let L be a complete lattice in $\mathbf{R}^n$, and let $d(L)$ be the volume of its fundamental parallelotope. For a basis $b_1, \ldots, b_n$ of L the vectors b_i^* $(1 \leq i \leq n)$ and the real numbers μ_{ij} $(1 \leq j < i \leq n)$ are inductively defined by

$$b_i^* := b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*,$$

$$\mu_{ij} := (b_i, b_j^*)/(b_j^*, b_j^*),$$

where (,) denotes the ordinary inner product on $\mathbf{R}^n$. The basis $b_1, \dots, b_n$ is called *LLL-reduced* if and only if

$$|\mu_{ij}| \le \tfrac{1}{2} \quad \text{for } 1 \le j < i \le n,$$

and

$$|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \ge \tfrac{3}{4}|b_{i-1}^*|^2 \quad \text{for } 1 < i \le n.$$

(3.1) LEMMA. *Let $b_1, \dots, b_n$ be a reduced basis of L; then we have*

$$d(L) \le \prod_{i=1}^{n} |b_i| \le 2^{n(n-1)/4} d(L), \tag{3.2}$$

$$|b_1| \le 2^{(n-1)/4} d(L)^{1/n}. \tag{3.3}$$

The LLL-algorithm yields an LLL-reduced basis of any lattice.

In view of (2.4) we now discuss free $\mathbf{Z}$-modules of rank n in K of the form

$$M = \frac{1}{\gamma} R \tag{3.4}$$

with a number $\gamma \in R$.

We apply the LLL-algorithm in two different situations:

(a) Since we want to carry out computations in M, we need a convenient basis of M. From the geometry of numbers it is well known that the mapping

$$K \to \mathbf{R}^n$$
$$\alpha \to \underline{\alpha}: (\alpha^{(1)}, \dots, \alpha^{(s)}, \operatorname{Re} \alpha^{(s+1)}, \dots, \operatorname{Re} \alpha^{(s+t)}, \operatorname{Im} \alpha^{(s+1)}, \dots, \operatorname{Im} \alpha^{(s+t)})^T$$

is a monomorphism of K, and that the image $\underline{M}$ of the module M is a complete lattice in $\mathbf{R}^n$ (cf. [1, Chapter II, §3]). We call a $\mathbf{Z}$-module basis of M *LLL-reduced*, if the corresponding lattice basis has this property.

(3.5) LEMMA. *Let $\alpha_1, \dots, \alpha_n$ be an LLL-reduced basis of M. Then we have*

$$C_1^{-(n-1)} N^{-1/n} \le |\alpha_i^{(j)}| \le C_1 N^{-1/n} \quad \text{for } 1 \le i \le n,\ 1 \le j \le s+t,$$

with $N := |N_{K|\mathbf{Q}}(\gamma)|$ and $C_1 = (2^{(n+2)/2} n^{-1})^{(n-1)/2} \Delta$, where Δ is the volume of the fundamental parallelotope of the lattice $\underline{R}$.

Proof. First of all, note that the volume of the fundamental parallelotope of $\underline{M}$ is given by the formula

$$d(\underline{M}) = N^{-1} \Delta. \tag{3.6}$$

Now it follows from (3.2) that

$$\prod_{i=1}^{n} |\underline{\alpha}_i| \le 2^{n(n-1)/4} N^{-1} \Delta, \tag{3.7}$$

where $|\underline{\alpha}_i|^2 = \sum_{j=1}^{s+t} |\alpha_i^{(j)}|^2$ for $1 \le i \le n$.

On the other hand, we have for every $0 \ne \alpha \in M$,

$$|\underline{\alpha}| \ge (n/2)^{1/2} N^{-1/n}. \tag{3.8}$$

In fact, if $\alpha \in M$, then there is a number $\tilde{\alpha} \in R$ with $\alpha = \tilde{\alpha}/\gamma$ and

$$2|\underline{\alpha}|^2 \geq \sum_{j=1}^{s} |\alpha^{(j)}|^2 + 2 \sum_{j=s+1}^{s+t} |\alpha^{(j)}|^2 \geq n|N_{K|\mathbf{Q}}(\alpha)|^{2/n}.$$

The second inequality of (3.5) follows from (3.7) and (3.8). In order to prove the first inequality, note that

$$N^{-1} \leq |N_{K|\mathbf{Q}}(\alpha_i)| \leq |\alpha_i^{(j)}| C_1^{(n-1)} N^{-(n-1)/n} \quad \text{for } 1 \leq i \leq n \text{ and } 1 \leq j \leq s+t. \quad \square$$

(b) In view of (2.2), the second application of the LLL-algorithm yields a number $\beta \in M$ satisfying

$$(3.9) \qquad |\beta^{(i)}| < 1, |\beta^{(j)}| > 1 \quad \text{for } j \neq i \text{ and } |N_{K|\mathbf{Q}}(\beta)| \leq CN^{-1}$$

for every conjugate direction $i \in \{1, \dots, s+t\}$. The constant C does not depend on M but only on R.

For the rest of this section we fix a conjugate direction $i \in \{1, \dots, s+t\}$, and we assume that $\alpha_1, \dots, \alpha_n$ is an LLL-reduced basis of M. Moreover, the numbers C_k, $k \in \mathbf{N}$, always denote effective constants depending only on the degree n of K and on the volume Δ of the fundamental parallelotope of R. Every number $\beta \in M$ has a representation

$$\beta = \sum_{l=1}^{n} x_l \alpha_l \quad \text{with } x_l \in \mathbf{Z} \text{ for } 1 \leq l \leq n.$$

We compute β of (3.9) solving the following approximation problem:

$$(3.10) \qquad \begin{aligned} |\beta^{(i)}|^{e_i} &< C_2 \kappa^{-(n-e_i)} N^{-e_i/n}, \\ |x_l| &< C_3 \kappa \quad \text{for } 1 \leq l \leq n, \end{aligned}$$

with $\kappa \geq 1$ and

$$e_i = \begin{cases} 1 & \text{if } 1 \leq i \leq s, \\ 2 & \text{if } s+1 \leq i \leq s+t. \end{cases}$$

(3.11) LEMMA. *If β satisfies* (3.10), *then we have*

$$C_4 \kappa N^{-1/n} \leq |\beta^{(j)}| \leq C_5 \kappa N^{-1/n} \quad \textit{for } j \neq i,$$
$$|N_{K|\mathbf{Q}}(\beta)| \leq C_6 N^{-1}.$$

Proof. Applying (3.5) and (3.10), we find

$$(3.12) \qquad |\beta^{(j)}| = \left| \sum_{l=1}^{n} x_l \alpha_l^{(j)} \right| \leq C_5 \kappa N^{-1/n}.$$

By virtue of the fact that

$$N^{-1} \leq |N_{K|\mathbf{Q}}(\beta)| = \prod_{l=1}^{s} |\beta^{(l)}| \prod_{l=s+1}^{s+t} |\beta^{(l)}|^2,$$

the first inequality follows from (3.10) and (3.12). $\square$

Since the bound for the norm of β does not depend on the constant κ, we choose κ such that (3.9) is satisfied. The approximation problem (3.10) is solved by means of the LLL-algorithm.

First of all, let us assume that i is a real direction, i.e., $1 \leq i \leq s$.

Consider the matrix

$$U := \begin{bmatrix} 0 & 0 & 0 & \cdots & \delta \\ 0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \delta & \cdots & 0 \\ 0 & \delta & 0 & \cdots & 0 \\ \alpha_1^{(i)} & \alpha_2^{(i)} & \alpha_3^{(i)} & \cdots & \alpha_n^{(i)} \end{bmatrix}, \tag{3.13}$$

where $\alpha_1, \ldots, \alpha_n$ is a L^3-reduced basis of M and

$$\delta := 2^{-n/4} |\alpha_1^{(i)}| \kappa^{-n}. \tag{3.14}$$

We apply the LLL-algorithm to the columns of U. The result is a matrix $\tilde{U}$ which we get from U by multiplication by a unimodular transformation matrix $T = (t_{ij})_{1 \leq i,j \leq n} \in \mathbf{Z}^{(n,n)}$. If we define

$$\begin{gathered} x_l := t_{li} \quad \text{for } 1 \leq l \leq n, \\ \beta := \sum_{l=1}^{n} x_l \alpha_l, \end{gathered}$$

then β solves (3.10).

In fact, since the fundamental parallelotope of the lattice spanned by the columns of U is of volume

$$d(U) = |\alpha_1^{(i)}| \delta^{n-1} = 2^{-n(n-1)/4} |\alpha_1^{(i)}|^n \kappa^{-n(n-1)},$$

it follows from (3.3) and (3.5) that

$$\begin{gathered} |\beta^{(i)}| \leq |\alpha_1^{(i)}| \kappa^{-(n-1)} \leq C_1 \kappa^{-(n-1)} N^{-1/n}, \\ |x_l| \leq 2^{n/4} \kappa \quad \text{for } 2 \leq l \leq n, \end{gathered} \tag{3.15}$$

and we are ready if we prove an upper bound for x_1. We get this upper bound if we divide

$$\begin{aligned} |x_1 \alpha_1^{(i)}| &= \left| \sum_{l=1}^{n} x_l \alpha_l^{(i)} - \sum_{l=2}^{n} x_l \alpha_l^{(i)} \right| \\ &\leq |\beta^{(i)}| + (n-1) 2^{n/4} C_1 \kappa N^{-1/n} \end{aligned}$$

by $|\alpha_1^{(i)}|$. In fact, this yields

$$|x_1| \leq C_7 \kappa N^{-1/n} / |\alpha_1^{(i)}| \leq C_3 \kappa. \tag{3.16}$$

Now assume that i is a "complex direction", i.e., $s < i \leq s+t$. This time we apply the LLL-algorithm to the columns of

$$U = \begin{bmatrix} 0 & 0 & 0 & \cdots & \delta \\ 0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \delta & \cdots & 0 \\ \operatorname{Re}\alpha_1^{(i)} & \operatorname{Re}\alpha_2^{(i)} & \operatorname{Re}\alpha_3^{(i)} & \cdots & \operatorname{Re}\alpha_n^{(i)} \\ \operatorname{Im}\alpha_1^{(i)} & \operatorname{Im}\alpha_2^{(i)} & \operatorname{Im}\alpha_3^{(i)} & \cdots & \operatorname{Im}\alpha_n^{(i)} \end{bmatrix}, \tag{3.17}$$

where

$$\delta = 2^{-n(n+1)/(4(n-2))} D^{1/2} \kappa^{-n/2}, \tag{3.18}$$

with

$$D = |\operatorname{Re}\alpha_1^{(i)} \operatorname{Im}\alpha_2^{(i)} - \operatorname{Re}\alpha_2^{(i)} \operatorname{Im}\alpha_1^{(i)}|.$$

Let $(t_{ij})_{1\leq i,j\leq n} \in \mathbf{Z}^{(n,n)}$ be the unimodular matrix which transforms U into the corresponding reduced matrix. Then we again fix

$$\begin{aligned} x_l &= t_{l1} \quad \text{for } 1 \leq l \leq n, \\ \beta &:= \sum_{l=1}^{n} x_l \alpha_l, \end{aligned} \tag{3.19}$$

and we prove that β satisfies (3.10).

Obviously, it follows from (3.5) that

$$D \leq C_8 N^{-2/n}. \tag{3.20}$$

But we also need a lower bound for D, and this is given in

(3.21) LEMMA. *For $l_1, l_2 \in \{1, \ldots, n\}$ set*

$$D_{l_1 l_2} := |\operatorname{Re}\alpha_{l_1}^{(i)} \operatorname{Im}\alpha_{l_2}^{(i)} - \operatorname{Re}\alpha_{l_2}^{(i)} \operatorname{Im}\alpha_{l_1}^{(i)}|.$$

Then there are numbers $l_1, l_2 \in \{1, \ldots, n\}$ such that

$$D_{l_1 l_2} \geq C_9 N^{-2/n}. \tag{3.22}$$

Proof. If $D^*_{l_1 l_2}$ for $l_1, l_2 \in \{1, \ldots, n\}$ denotes the absolute value of the adjoint determinant of $D_{l_1 l_2}$ in the matrix $(\underline{\alpha}_1, \ldots, \underline{\alpha}_n)$, then we get from (3.5), (3.6) and Laplace's formula

$$\begin{aligned} N^{-1}\Delta &\leq \sum_{1\leq l_1 < l_2 \leq n} D_{l_1 l_2} D^*_{l_1 l_2} \\ &\leq C_{10} N^{-(n-2)/n} \max_{1\leq l_1 < l_2 \leq n} D_{l_1 l_2}, \end{aligned}$$

and this proves the lemma. □

Without loss of generality we assume that (3.22) is true for $l_1 = 1$ and $l_2 = 2$. Then we have

$$D \geq C_{11} N^{-2/n}. \tag{3.23}$$

Notice that we have to renumber the basis at this point in order to get $D \neq 0$.

Now we are able to prove that β, defined in (3.19), satisfies (3.10). This time the fundamental parallelotope of the lattice spanned by the columns of U is of volume

$$d(U) = D \cdot \delta^{n-2} = 2^{-n(n+1)/4} \cdot D^{n/2} \cdot \kappa^{-n(n-2)/2},$$

and thus (3.3) and (3.20) yield

$$\begin{aligned} |\beta^{(i)}|^2 &\leq D \cdot \kappa^{-(n-2)} \leq C_2 \kappa^{-(n-2)} N^{-2/n}, \\ |x_l| &\leq 2^{(n^2+1)/(4(n-2))} \kappa \quad \text{for } 3 \leq l \leq n. \end{aligned} \tag{3.24}$$

An upper bound for x_1 and x_2 follows from

$$\begin{aligned} |x_1 \operatorname{Re} \alpha_1^{(i)} + x_2 \operatorname{Re} \alpha_2^{(i)}| &= \left| \operatorname{Re} \beta^{(i)} - \sum_{l=3}^{n} x_l \operatorname{Re} \alpha_l^{(i)} \right|, \\ |x_1 \operatorname{Im} \alpha_1^{(i)} + x_2 \operatorname{Im} \alpha_2^{(i)}| &= \left| \operatorname{Im} \beta^{(i)} - \sum_{l=3}^{n} x_l \operatorname{Im} \alpha_l^{(i)} \right|. \end{aligned}$$

Applying Cramer's rule, we get in view of (3.5), (3.23) and (3.24),

$$|x_l| \leq C_{12} \kappa N^{-2/n} D^{-1} \leq C_3 \kappa \quad \text{for } l = 1, 2. \quad \square \tag{3.25}$$

4. Computational Aspects of the Algorithm. Let $i \in \{1, \ldots, s+t\}$ be again a fixed conjugate direction. Before we give a detailed description of the algorithm, we give some preparatory explanations.

Assume that we know for a $k \in \mathbf{N}$ the number $N_k = |N_{K|\mathbf{Q}}(\gamma_k)|$ and an LLL-reduced basis $\alpha_1(k), \ldots, \alpha_n(k)$ of the module $R_k = R/\gamma_k$.

In order to compute the number β_k satisfying (2.5), we have to proceed as follows:

- choose κ,
- set δ according to (3.14) or (3.18),
- set U according to (3.13) or (3.17),
- apply the LLL-algorithm to the columns of U resulting in $\tilde{U} = U \cdot T$, with $T = (t_{l,j})_{1 \leq l,j \leq n} \in \mathbf{Z}^{(n,n)}$,
- set $x_l(k) \leftarrow t_{l1}$ for $1 \leq l \leq n$ and set $\beta_k \leftarrow \sum_{l=1}^{n} x_l \alpha_l(k)$.

But how to choose κ? To make sure that the algorithm yields a maximal system of independent units, we have to choose κ such that β_k satisfies (3.9). Since we know by (3.11) and (2.6) that

$$N_k \leq C_6, \tag{4.1}$$

this means

$$\kappa = \max\{C_4^{-1} C_6^{1/n}, C_2^{e_i/(n-e_i)}\} + \varepsilon \tag{4.2}$$

with an arbitrary small constant ε.

Now in almost all our examples it has turned out to be enough to choose κ such that only

$$|\beta_k^{(i)}| < 1, \tag{4.3}$$

in order to compute maximal systems of independent units. This condition is necessary to avoid trivial units. Recall that we have by (3.15) and (3.16), (3.24) and (3.25),

$$\begin{aligned} &|\beta_k^{(i)}|^{e_i} \leq \lambda_i \kappa^{-(n-e_i)}, \\ &|x_l| \leq C_{13}\kappa\lambda_i^{-1} \quad \text{for } 1 \leq l \leq e_i, \\ &|x_l| \leq C_{14}\kappa \qquad\quad \text{for } e_i < l \leq n, \end{aligned} \tag{4.4}$$

with

$$\lambda_i = \begin{cases} |\alpha_1^{(i)}| & \text{for } i \leq s, \\ |\operatorname{Re}\alpha_1^{(i)} \operatorname{Im}\alpha_2^{(i)} - \operatorname{Re}\alpha_2^{(i)} \operatorname{Im}\alpha_1^{(i)}| & \text{for } i > s. \end{cases} \tag{4.5}$$

Now on the one hand, we want to satisfy (4.3); on the other hand, we want to make the $|x_l|$ small in order to get units with small coefficients. Hence we have to choose κ such that

$$\lambda_i \kappa^{-(n-e_i)} = 1 - \varepsilon \tag{4.6}$$

with a small number ε, and this means that the bound for x_l, $1 \leq l \leq e_i$, increases if κ decreases, whereas for the bounds of x_l, $e_i < l \leq n$, the contrary is true.

So the best thing to do is to renumber $\alpha_1(k), \ldots, \alpha_n(k)$ such that $|\lambda_i - 1|$ is as small as possible and $D_{12} \neq 0$ if $i > s$, and then to fix

$$\kappa = \lambda_i^{1/(n-e_i)} + \varepsilon. \tag{4.7}$$

The next question we are going to discuss is the representation of the reduced basis $\alpha_1(k), \ldots, \alpha_n(k)$ and of the number β_k.

Note that all the basis elements have a representation

$$\alpha_j(k) = \frac{1}{N_k} \sum_{l=1}^{n} a_{lj}(k)\alpha_l(1) \quad \text{for } 1 \leq j \leq n, \tag{4.8}$$

with

$$A_k := (a_{lj}(k))_{1 \leq l,j \leq n} \in \mathbf{Z}^{(n,n)}. \tag{4.9}$$

Since by (3.5) the conjugates of the $\alpha_j(k)$'s are—independent of k—all of the same small size, the same is true for the elements of A_k. Similarly, the number β_k is representable as

$$\beta_k = \frac{1}{N_k} \sum_{l=1}^{n} b_l(k)\alpha_l(1), \qquad b_l(k) \in \mathbf{Z}, \tag{4.10}$$

and because of (3.11) also the $b_l(k)$'s are small.

Finally, we explain how to decide whether the algorithm terminates, i.e., whether $\gamma_{k+1} = \gamma_k\beta_k$ is associated with a γ_Z, $Z \leq k$.

By (2.7) we know that we have to check whether the corresponding modules are equal. A necessary condition is of course $N_{k+1} = N_Z$. If this condition is satisfied, then we have to test whether $A_Z \cdot A_{k+1}^{-1} \in \mathrm{GL}(n, \mathbf{Z})$. So we get:

(4.11) ALGORITHM.

Input: The conjugate direction $i \in \{1, \ldots, s+t\}$.

Rational approximations to the conjugates of the elements of an LLL-reduced basis $\alpha_1, \ldots, \alpha_n$ of the order R. A constant $\varepsilon > 0$.**

Output: The unit ε_i.

1. *Initialization.* $a_l(1) \leftarrow \alpha_l$ for $1 \leq l \leq n$,
   $N_1 \leftarrow 1$,
   $k \leftarrow 1$,

2. *Repeat.*
   a) Renumber $\alpha_1(k), \ldots, \alpha_n(k)$ such that $|\lambda_i - 1|$ is minimal and $D_{12} \neq 0$ if $i > s$, cf. (4.6).
   b) $\kappa \leftarrow \lambda_i^{1/(n-e_i)} + \varepsilon$.
   c) Set δ according to (3.14) or (3.18) and U according to (3.13) or (3.17).
   d) Apply the LLL-algorithm to the columns of U. The corresponding unimodular transformation is $T = (t_{lj})_{1 \leq l,j < n}$.
   e) Set $\beta_k \leftarrow \sum_{l=1}^{n} t_l \alpha_l(k)$, $N_{k+1} \leftarrow N_k |N_{K|\mathbf{Q}}(\beta_k)|$; compute the coefficients $b_l(k)$, $1 \leq l \leq n$ (cf. (4.10)).
   f) Compute an LLL-reduced basis $\alpha_1(k+1), \ldots, \alpha_n(k+1)$ of the module $R_{k+1} = (1/\beta_k) R_k$, applying the LLL-algorithm to $\{\alpha_1(k)/\beta_k, \ldots, \alpha_n(k)/\beta_k\}$. Compute the corresponding representation matrix A_k (cf. (4.8)).
   g) For $Z = 1$ until k:
      If $N_Z = N_{k+1}$ then
      if $A_Z \cdot A_{k+1}^{-1} \in \mathrm{GL}(n, \mathbf{Z})$ then set $\varepsilon_i \leftarrow \prod_{l=Z}^{k} \beta_l$.
      Return.
   h) $k \leftarrow k+1$.

After we have applied this algorithm to every coordinate direction, we know a set $\{\varepsilon_1, \ldots, \varepsilon_{s+t}\}$ of nontrivial units. If this set does not contain a subset of $s+t-1$ independent units, we apply our algorithm again, but with a bigger κ in 2b).

Tables (see the supplements section at the end of this issue). By the method described, we have computed maximal systems of independent units in the order $\mathbf{Z}[\rho]$ of the field $\mathbf{Q}(\rho)$, where $\rho = \sqrt[n]{D}$ for $6 \leq n \leq 11$. For $n \leq 5$ and $n = 6$, $D < 0$, there are efficient methods (cf. [3]) for computing fundamental units; therefore we have omitted these cases. In the tables we use D and n in the above sense. Moreover, we denote by

P : $\max_{i \in \{1, \ldots, s+t\}} \{\text{number of iterations in direction } i\}$,
R : regulator of the system,
$x_1, \ldots, x_n$: the coefficients of the units in the basis $1, \rho, \ldots, \rho^{n-1}$.

**It is possible to determine the necessary precision of approximation theoretically, but this theoretical value could hardly be realized. In our computation, double-precision floating-point arithmetic (26 decimal digits) was always sufficient.

For the sake of readability of the tables we decided not to list the coefficients to more than 8 decimal digits. All the computations were carried out on the CYBER 76 of the University of Cologne. The computation of the units of each field took at most a few CPU-seconds.

Mathematisches Institut der Universität zu Köln
Weyertal 86-90
5000 Köln 41
Federal Republic of Germany

Mathematical Institute
Kossuth Lajos University
4010 Debrecen Pf12, Hungary

1. Z. I. BOREVIČ & I. R. ŠAFAREVIČ, *Number Theory*, Pure and Appl. Math., vol. 20, Academic Press, New York, 1966.

2. A. J. BRENTJES, *Multi-Dimensional Continued Fraction Algorithm*, Proefschrift, Math. Centrum Amsterdam, 1981.

3. J. BUCHMANN, "A generalization of Voronoi's unit algorithm," *J. Number Theory*, v. 20, 1985, pp. 177–209.

4. J. BUCHMANN, *The generalized Voronoi Algorithm in Totally Real Algebraic Number Fields*, Proc. EUROCAL 85, Vol. 2, Lecture Notes in Comp. Sci., Vol. 204, Springer-Verlag, Berlin and New York, 1985, pp. 479–486.

5. R. DEDEKIND, *Über die Theorie der ganzen algebraischen Zahlen*, Vieweg, 1964.

6. G. LEJEUNE DIRICHLET, *Zur Theorie der complexen Einheiten*, Bericht über die Verhandlungen der Königl. Preuss, Akademie der Wissenschaften, 1846, pp. 103–107.

7. U. FINCKE & M. POHST, *A New Method of Computing Fundamental Units in Algebraic Number Fields*, Proc. EUROCAL 85, Vol. 2, Lecture Notes in Comp. Sci., Vol. 204, Springer-Verlag, Berlin and New York, 1985, pp. 470–478.

8. A. K. LENSTRA, H. W. LENSTRA, JR. & L. LOVÁSZ, "Factoring polynomials with rational coefficients," *Math. Ann.*, v. 261, 1982, pp. 515–534.

9. W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, Monograf. Mat., Vol. 51, PWN, Warsaw, 1974.

10. M. POHST, H. ZASSENHAUS (& P. WEILER), "On effective computation of fundamental units. I, II," *Math. Comp.*, v. 38, 1982, pp. 275–292 and 293–329.