MATHEMATICS OF COMPUTATION
VOLUME 54, NUMBER 189
JANUARY 1990, PAGES 467-477

INTEGER RELATIONS AMONG ALGEBRAIC NUMBERS

BETTINA JUST

ABSTRACT. A vector $m = (m_1, \ldots, m_n) \in \mathbf{Z}^n \setminus \{0\}$ is called an *integer relation* for the real numbers $\alpha_1, \ldots, \alpha_n$, if $\sum \alpha_i m_i = 0$ holds. We present an algorithm that, when given algebraic numbers $\alpha_1, \ldots, \alpha_n$ and a parameter ε, either finds an integer relation for $\alpha_1, \ldots, \alpha_n$ or proves that no relation of Euclidean length shorter than $1/\varepsilon$ exists. Each algebraic number is assumed to be given by its minimal polynomial and by a sufficiently precise rational approximation.

Our algorithm uses the Lenstra-Lenstra-Lovász lattice basis reduction technique. It performs

$$\operatorname{poly}\left(\log 1/\varepsilon,\ n,\ \log \max_i \operatorname{height}(\alpha_i),\ [\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]\right)$$

bit operations. The straightforward algorithm that works with a primitive element of the field extension $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ of $\mathbf{Q}$ would take

$$\operatorname{poly}\left(n,\ \log \max_i \operatorname{height}(\alpha_i),\ \prod_{i=1}^{n} \operatorname{degree}(\alpha_i)\right)$$

bit operations.

In order to prove the correctness of the algorithm, we show a lower bound for $|\sum \alpha_i m_i|$ if m is *not* an integer relation for $\alpha_1, \ldots, \alpha_n$, which may be interesting in its own right.

1. INTRODUCTION

For n real numbers $\alpha_1, \ldots, \alpha_n$, a nonzero integer vector $m = (m_1, \ldots, m_n)$ with $\sum \alpha_i m_i = 0$ is called an integer relation for $\alpha_1, \ldots, \alpha_n$. The problem of finding integer relations has been widely studied in the literature. Jacobi [10], Perron [15], Brun [5], Szekeres [19] and others studied this problem—among others—in the context of generalizing the continued fraction algorithm to higher dimensions. They used the unit cost model, that is, one step is one arithmetic operation on arbitrary real numbers. Only recently, the integer relation problem in this model has been solved. Ferguson and Forcade [6, 7] and Bergman [2] presented, and Hastad, Just, Lagarias, and Schnorr [9] analyzed, an algorithm for it. For given $\alpha_1, \ldots, \alpha_n$ and $\varepsilon > 0$, this algorithm performs $\operatorname{poly}(n, \log 1/\varepsilon)$ arithmetic operations on real numbers and either finds an integer relation for $\alpha_1, \ldots, \alpha_n$, or proves that no relation of Euclidean length shorter than $1/\varepsilon$ exists. Babai, Just, and Meyer auf der Heide [1] showed that

Received November 15, 1988; revised February 2, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 68Q25, 68Q40, 12F10.
Key words and phrases. Integer relation, algebraic number, lattice basis reduction.

the parameter ε cannot be omitted: in a very general model of computation there exists no algorithm that proves the nonexistence of integer relations.

Arbitrary real numbers cannot be represented in a computer, and for practical purposes the unit cost model is not a realistic one. So we turn to numbers that can be represented in a computer, namely rational and algebraic numbers. The computational model is now the one counting one bit operation as one step.

In [9], the integer relation problem for rational inputs is investigated. Of course, rational numbers $\alpha_1, \ldots, \alpha_n$ always satisfy integer relations, and in [9] it is shown how to find them in polynomial time. The present paper deals with algebraic numbers. An algebraic number α is a real or complex root of a univariate integer polynomial $p(x) \in \mathbf{Z}[x]$. It is represented in finitely many bits by the polynomial and by a rational approximation precise enough to separate it from the other roots of the polynomial. The algebraic numbers $\alpha_1, \ldots, \alpha_n$ may or may not satisfy an integer relation, so the situation is more complicated than the situation with rational inputs. We present a polynomial-time algorithm for the integer relation problem among algebraic numbers. Before we present our results in greater detail and discuss them, we recall some notation and facts about algebraic numbers.

Let $p = \sum_{i=0}^{d} p_i x^i \in \mathbf{Z}[x]$ be an integer polynomial with $p_d \neq 0$. Then d is the *degree* of p, and the Euclidean length $\|(p_0, \ldots, p_d)\|$ of the vector of coefficients is the *height* of p. We denote by $d(p)$ the degree and by $h(p)$ the height of p. The polynomial p is *primitive* if $\gcd(p_0, \ldots, p_d) = 1$ and $p_d > 0$ hold, and it is *monic* if $p_d = 1$.

For any algebraic number $\alpha = (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)) \in \mathbf{C}$ there exists a unique primitive polynomial $p_\alpha \in \mathbf{Z}[x]$ of smallest degree, the *minimal polynomial* of α. The *degree* $d(\alpha)$ and *height* $h(\alpha)$ of α are defined as the degree $d(p_\alpha)$ and height $h(p_\alpha)$, respectively, of the polynomial p_α. If p_α is monic, α is called an *algebraic integer*. The set of algebraic integers forms a ring.

Field extensions of $\mathbf{Q}$ by algebraic numbers are called *algebraic number fields*. We denote by $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$ the degree of the field extension $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbf{Q}$. By the theorem of the primitive element ([8, p. 167]) we know that this extension is generated also by a single algebraic number γ, thus $\mathbf{Q}(\alpha_1, \ldots, \alpha_n) = \mathbf{Q}(\gamma)$. A procedure of Loos ([4, p. 184]) constructs γ from $\alpha_1, \ldots, \alpha_n$ and represents $\alpha_1, \ldots, \alpha_n$ as rational polynomials in γ, so $\alpha_i = \sum_{j=0}^{d(\gamma)-1} c_j^{(i)} \gamma^j$. Now a nonzero integer vector $m = (m_1, \ldots, m_n)$ is an integer relation for $\alpha_1, \ldots, \alpha_n$ if and only if it solves the system of linear equations $\sum_{i=1}^{n} m_i c_j^{(i)} = 0$ for $j = 0, \ldots, d(\gamma) - 1$.

A first attempt to find integer relations among algebraic numbers uses Loos' procedure and then solves this system. The run time of this attempt is polynomial in $\prod d(\alpha_i)$, n and $\log \max_i h(\alpha_i)$. In this paper we do better. We present an algorithm which is polynomial not in $\prod d(\alpha_i)$, but only in $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$ (and, of course, in the sizes n and $\log \max_i h(\alpha_i)$). The difference between $\prod d(\alpha_i)$ and $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$ is large especially if there exist integer relations for $\alpha_1, \ldots, \alpha_n$. Our algorithm is described in §3 and is very different from the one described above. It uses lattice basis reduction as a fundamental feature. For the analysis, we prove in §2 a lower bound for $|\sum m_i \alpha_i|$ if

$m = (m_1, \ldots, m_n)$ is *not* an integer relation for $\alpha_1, \ldots, \alpha_n$. The lower bound may be interesting in its own right. Its logarithm is polynomial in $\log \|m\|$, n, $\log \max_i h(\alpha_i)$ and—most important—in $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$, but not in $\prod d(\alpha_i)$.

2. A LOWER BOUND FOR $|\sum \alpha_i m_i|$ IF $\sum \alpha_i m_i \neq 0$

The purpose of this section is to prove the following proposition.

Proposition 1. *Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers. Denote by s the integer $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$ and by h the real number $\max_i h(\alpha_i)$. For $m = (m_1, \ldots, m_n) \in \mathbf{Z} \setminus \{0\}$ define*

$$a(n, s, h, \|m\|) := \left((2n)^s (\|m\|^s \cdot h)^{ns(2+ns)} + 1\right)^{-1}.$$

If $\sum \alpha_i m_i \neq 0$, then $|\sum \alpha_i m_i| \geq a(n, s, h, \|m\|)$.

Proposition 1 will be proved with the help of Lemmas 2 and 3 below. Both lemmas will use the fact that for any algebraic number α we have

$$|\alpha| \leq h(\alpha) + 1.$$

This is an immediate consequence of the following *Cauchy Inequality* (cf. [4, Theorem 2, p. 259]):

Let $p = \sum_{i=0}^{d} p_i x^i \in \mathbf{Z}[x]$ be a polynomial of degree d. Then any root α of p satisfies

$$|\alpha| \leq 1 + \max_{0 \leq i \leq d} \frac{|p_i|}{|p_d|}.$$

Lemma 2. *If $\alpha_1, \ldots, \alpha_n$ are algebraic integers, then for $\alpha := \sum_{j=1}^{n} \alpha_j$ we have*

$$h(\alpha) \leq \left(2n \cdot \prod_{j=1}^{n} h(\alpha_j)\right)^{d(\alpha)}.$$

The proof of Lemma 2 requires basic facts on algebraic number fields and Galois theory, which can be found, for example, in [3].

Proof of Lemma 2. Denote by $\mathcal{M}$ the field extension $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ of $\mathbf{Q}$, and let $\gamma \in \mathcal{M}$ be a primitive element, hence $\mathcal{M} = \mathbf{Q}(\gamma)$. Let $\mathcal{N}$ be the root field of the minimal polynomial p_γ of γ. Hence we have for all $1 \leq i \leq n$

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha_i) \subseteq \mathcal{M} \subseteq \mathcal{N}.$$

For any $\beta \in \mathcal{N}$ we denote by $\beta^{(1)}, \ldots, \beta^{(d(\beta))}$ the conjugates of β over $\mathbf{Q}$. We have $\beta^{(1)}, \ldots, \beta^{(d(\beta))} \in \mathcal{N}$, since $\mathcal{N}$ is the root field of a polynomial and thus the field extension $\mathcal{N} : \mathbf{Q}$ is normal.

Moreover, the fundamental theorem of Galois theory implies

(1) for $1 \leq j \leq d(\beta)$ there are exactly $[\mathcal{N} : \mathbf{Q}]$ automorphisms of $\mathcal{N}$ that map β to $\beta^{(j)}$.

Now for any polynomial $p = \sum_{i=0}^{d} p_i x^i \in \mathbf{Z}[x]$ of degree d with the (complex) roots $\delta^{(1)}, \ldots, \delta^{(d)}$ we define the *measure* $M(p)$ by

$$M(p) := |p_d| \cdot \prod_{j=1}^{d} \max\{1, |\delta^{(j)}|\}.$$

We know from M. Mignotte ([4, Theorem 2, p. 260]) that

$$M(p) \leq h(p). \tag{2}$$

Now we show

$$2^{-d} \cdot h(p) \leq M(p). \tag{3}$$

For any subset $\{\delta^{(i_1)}, \ldots, \delta^{(i_l)}\} \subseteq \{\delta^{(1)}, \ldots, \delta^{(d)}\}$ we have

$$\left| \prod_{j=1}^{l} \delta^{(i_j)} \right| \leq M(p)/|p_d|.$$

Moreover, $p = p_d \cdot \prod_{j=1}^{d}(x - \delta^{(j)})$; the p_i are symmetric functions of the $\delta^{(j)}$. This implies $|p_i| \leq \binom{d}{i} \cdot M(p)$ for all $0 \leq i \leq d$. Hence we have $\sum_{i=0}^{d} |p_i| \leq 2^d \cdot M(p)$, which implies (3).

In order to simplify notation, for any $z \in \mathbf{C}$ we shall write z^* instead of $\max\{1, |z|\}$.

For $z_1, \ldots, z_l \in \mathbf{C}$ we have

$$\max\left\{1, \left|\sum_{j=1}^{l} z_j\right|\right\} \leq l \cdot \max\left\{1, \max_{1 \leq j \leq l} |z_j|\right\} \leq l \cdot \prod_{j=1}^{l} z_j^*,$$

which implies

$$\left(\sum_{j=1}^{l} z_j\right)^* \leq l \cdot \prod_{j=1}^{l} z_j^*. \tag{4}$$

Now let p_α be the minimal polynomial of α. Since the algebraic integers form a ring, α is an algebraic integer, which implies $M(p_\alpha) = \prod_{i=1}^{d(\alpha)} \alpha^{(i)*}$. Now

we have

$$
\begin{aligned}
h(\alpha) &\overset{(3)}{\leq} 2^{d(\alpha)} \cdot M(p_\alpha) = 2^{d(\alpha)} \cdot \prod_{i=1}^{d(\alpha)} \alpha^{(i)*} \\
&\overset{(1)}{=} 2^{d(\alpha)} \cdot \left(\prod_{\sigma \in \mathrm{Aut}(\mathcal{N})} \sigma(\alpha)^* \right)^{1/[\mathcal{N} : \mathbf{Q}(\alpha)]} \\
&= 2^{d(\alpha)} \cdot \left(\prod_{\sigma \in \mathrm{Aut}(\mathcal{N})} \left(\sum_{i=1}^{n} \sigma(\alpha_i) \right)^* \right)^{1/[\mathcal{N} : \mathbf{Q}(\alpha)]} \\
&\overset{(4)}{\leq} 2^{d(\alpha)} \cdot \left(n^{[\mathcal{N} : \mathbf{Q}]} \cdot \prod_{\sigma \in \mathrm{Aut}(\mathcal{N})} \prod_{i=1}^{n} \sigma(\alpha_i)^* \right)^{1/[\mathcal{N} : \mathbf{Q}(\alpha)]} \\
&= (2n)^{d(\alpha)} \cdot \left(\prod_{i=1}^{n} \prod_{\sigma \in \mathrm{Aut}(\mathcal{N})} \sigma(\alpha_i)^* \right)^{1/[\mathcal{N} : \mathbf{Q}(\alpha)]} \\
&\overset{(1)}{=} (2n)^{d(\alpha)} \cdot \left(\prod_{i=1}^{n} \left(\prod_{k=1}^{d(\alpha_i)} \alpha_i^{(k)*} \right)^{[\mathcal{N} : \mathbf{Q}(\alpha_i)]} \right)^{1/[\mathcal{N} : \mathbf{Q}(\alpha)]} \\
&= (2n)^{d(\alpha)} \cdot \prod_{i=1}^{n} M(p_{\alpha_i})^{[\mathbf{Q}(\alpha) : \mathbf{Q}]/[\mathbf{Q}(\alpha_i) : \mathbf{Q}]} \\
&\overset{(2)}{\leq} \left(2n \cdot \prod_{i=1}^{n} h(\alpha_i) \right)^{d(\alpha)}.
\end{aligned}
$$

This finishes the proof of Lemma 2. □

Lemma 3. *For* $m \in \mathbf{Z}^n \setminus \{0\}$ *and algebraic numbers* $\alpha_1, \ldots, \alpha_n$, *define* $\alpha := L = \sum_{i=1}^{n} \alpha_i m_i$. *Then we have*

$$
h(\alpha) \leq \left(2n \cdot \prod_{i=1}^{n} \left(\|m\|^{d(\alpha_i)} \cdot h(\alpha_i) \right)^{2 + \sum_{j=1}^{n} d(\alpha_j)} \right)^{d(\alpha)}.
$$

Proof of Lemma 3. Let for the moment β be an arbitrary algebraic number of degree d with minimal polynomial $p_\beta = \sum_{i=0}^{d} p_i x^i$. The number $p_d > 0$ is called the *leading coefficient* of β and is denoted by $F(\beta)$. We shall use the claims (1)–(4) below.

(1) $F(\beta) \cdot \beta$ is an algebraic integer.

Proof. The polynomial $\sum_{i=0}^{d} p_i F(\beta)^{d-i-1} x^i \in \mathbf{Z}[x]$ is monic of degree $d(\beta) = d(F(\beta) \cdot \beta)$ and has a root at $F(\beta) \cdot \beta$.

(2) For $k \in \mathbf{Z} \setminus \{0\}$ we have $h(k \cdot \beta) \leq |k|^d \cdot h(\beta)$.

Proof. The polynomial $\sum_{i=0}^{d} p_i k^{d-i} x^i \in \mathbf{Z}[x]$ is of height at most $|k|^d \cdot h(p)$ and is an integer multiple of the minimal polynomial of $k \cdot \beta$.

(3) For $k \in \mathbf{Z} \setminus \{0\}$ we have $h(\beta) \leq |k|^d \cdot h(k \cdot \beta)$.

Proof. If $\sum_{i=0}^{d} g_i x^i$ is the minimal polynomial of $k \cdot \beta$, then $\sum_{i=0}^{d} k^i g_i x^i$ is an integer multiple of p_β of height at most $|k|^d \cdot h(k \cdot \beta)$.

(4) If $\gamma_1, \ldots, \gamma_r$ are algebraic numbers, then for $\gamma := \sum_{i=1}^{r} \gamma_i$ we have

$$h(\gamma) \leq \left(2r \cdot \prod_{i=1}^{r} h(\gamma_i)^{2+\sum_{j=1}^{r} d(\gamma_j)}\right)^{d(\gamma)}.$$

Proof. We first observe that for all $1 \leq i \leq r$ the number $\gamma_i \prod_{j=1}^{r} F(\gamma_j)$ is an algebraic integer. This follows from (1) and from the fact that algebraic integers form a ring. Now (2) implies for all $1 \leq i \leq r$

$$h\left(\gamma_i \prod_{j=1}^{r} F(\gamma_j)\right) \leq \left(\prod_{j=1}^{r} F(\gamma_j)\right)^{d(\gamma_j)} \cdot h(\gamma_i) \leq h(\gamma_i) \cdot \left(\prod_{j=1}^{r} h(\gamma_j)\right)^{d(\gamma_i)}.$$

Lemma 2 yields

$$h\left(\sum_{i=1}^{r}\left(\gamma_i \prod_{j=1}^{r} F(\gamma_j)\right)\right) \leq \left(2r \cdot \prod_{i=1}^{r} h(\gamma_i)^{1+\sum_{j=1}^{r} d(\gamma_j)}\right)^{d(\gamma)}.$$

Application of (3) with $k := \prod_{j=1}^{r} F(\gamma_j)$ implies

$$h(\gamma) \leq \left(\prod_{j=1}^{r} F(\gamma_j)\right)^{d(\gamma)} \cdot \left(2r \cdot \prod_{i=1}^{r} h(\gamma_i)^{1+\sum_{j=1}^{r} d(\gamma_j)}\right)^{d(\gamma)}.$$

This implies (4), since $F(\gamma_i) \leq h(\gamma_i)$.

Now in order to prove Lemma 3, we assume without loss of generality, that there exists an $r \in \{1, \ldots, n\}$ such that $m_i \neq 0$ for all $1 \leq i \leq r$ and $m_i = 0$ for all $i > r$. For $1 \leq i \leq r$ define $\gamma_i := \alpha_i m_i$. Then (2) implies

$$h(\gamma_i) \leq \|m\|^{d(\alpha_i)} \cdot h(\alpha_i).$$

Application of (4) then proves Lemma 3. □

We are now able to prove Proposition 1.

Proof of Proposition 1. Lemma 3 immediately implies

$$(1) \qquad h\left(\sum_{i=1}^{n} \alpha_i m_i\right) \leq (2n)^s \cdot \left(\|m\|^s \cdot h\right)^{2+ns}.$$

Now let α be an arbitrary nonzero algebraic number. If $\sum_{i=0}^{d} p_i x^i$ is the minimal polynomial of α, then $\sum_{i=0}^{d} p_i x^{d-i}$ is the minimal polynomial of α^{-1}. Since $|\alpha| \leq h(\alpha) + 1$, we have $|\alpha^{-1}| \leq h(\alpha) + 1$ and thus

$$(2) \qquad (h(\alpha) + 1)^{-1} \leq |\alpha|.$$

Now we get

$$\left|\sum_{i=1}^{n}\alpha_i m_i\right| \overset{(2)}{\geq} \left(h\left(\sum_{i=1}^{n}\alpha_i m_i\right)+1\right)^{-1} \overset{(1)}{\geq} \left((2n)^s\cdot(\|m\|^s\cdot h)^{ns(2+ns)}+1\right)^{-1},$$

and Proposition 1 is proven. □

3. The algorithm

We want to decide whether given algebraic numbers satisfy an integer relation shorter than a given bound. This will be done by deciding whether a suitably chosen lattice contains a short vector, which in turn is done by the famous LLL-lattice basis reduction algorithm. We briefly recall some lattice basis reduction theory.

Let $b_1, \ldots, b_n \in \mathbf{R}^k$ be linearly independent vectors. The set $L = \sum b_i\mathbf{Z}$ is called the *lattice* spanned by $b_1, \ldots, b_n$. The set $\{b_1, \ldots, b_n\}$ is called a *basis* of the lattice L, and n is the *dimension* of L. The dimension of L is unique, the basis is not. The purpose of lattice basis reduction theory is to find lattice bases that contain "short" vectors. The specification of "short" depends on the lattice, and also on the mathematical context. A very interesting algorithmic problem is to find the shortest (nonzero) vector of a given lattice. An exponential algorithm for this problem is presented in [11]. It is not known whether the problem is NP-complete, but up to now no subexponential algorithm has been found. There are polynomial-time algorithms to solve the problem approximately ([14, 16]).

LLL-Theorem ([14]). *There is an algorithm which constructs from rational* $b_1, \ldots, b_n$ *a vector* $b \in L \setminus \{0\}$ *such that* $\|b\|^2 \leq 2^{n-1}\|v\|^2$ *holds for all* $v \in L \setminus \{0\}$. *If the components of all* b_i *have common denominator* D, *and if* $\max_i D\cdot\|b_i\|$ *is at most* B *for some natural number* $B > 2$, *then the algorithm performs* $O(n^3 k \log B)$ *arithmetic operations on numbers of binary length* $O(n \log B)$.

(*Remark.* The algorithm actually constructs an entire basis of short lattice vectors, but this will not be used here. Variations of the algorithm are proposed by Schnorr [17] and Schönhage [18].)

We now present our algorithm to solve the integer relation problem for algebraic numbers. Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers, and let $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ be rational complex numbers approximating them. We assume without loss of generality that $|\alpha_i - \overline{\alpha}_i|$ is very small for all i (cf. Lemma 4). For given $\varepsilon > 0$ we want to find from $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ an integer relation for $\alpha_1, \ldots, \alpha_n$, or prove that no such relation shorter than $1/\varepsilon$ exists. To this end, we apply the

LLL-algorithm to the columns of the matrix

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ c \cdot \mathrm{Re}(\overline{\alpha}_1) & \cdots & c \cdot \mathrm{Re}(\overline{\alpha}_n) \\ c \cdot \mathrm{Im}(\overline{\alpha}_1) & \cdots & c \cdot \mathrm{Im}(\overline{\alpha}_n) \end{pmatrix}.$$

Here, c is a large integer specified in Lemma 4.

(*Remark.* Similar lattice bases are used in [12] to find the minimal polynomial of an algebraic number, and in [13] to solve Diophantine approximation problems.)

Let $b = (m_1, \ldots, m_n, c \cdot \sum m_i \mathrm{Re}(\overline{\alpha}_i), c \cdot \sum m_i \mathrm{Im}(\overline{\alpha}_i))$ be the vector produced by the algorithm. If $\|b\|^2 > 2^n/\varepsilon^2$, we claim that $\alpha_1, \ldots, \alpha_n$ do not satisfy an integer relation shorter than $1/\varepsilon$. Otherwise, we claim that $(m_1, \ldots, m_n)$ is an integer relation for $\alpha_1, \ldots, \alpha_n$ (which, in addition, is obviously of length at most $2^n/\varepsilon^2$).

The correctness of these two claims, and thus of our algorithm, will be shown with the help of Lemma 4.

Lemma 4. *Let $1 > \varepsilon > 0$ be given, and let $\alpha_1, \ldots, \alpha_n$, s, h and $a(n, s, h, \|m\|)$ be as in Proposition 1. Define*

$$q := \frac{\varepsilon}{4n \cdot 2^{n/2}} \cdot a(n, s, h, \|m\|)$$

and define $c := \lceil 1/(2nq) \rceil$. Let $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ be complex numbers such that $\max |\alpha_i - \overline{\alpha}_i| < q$ holds.

(a) *If $m = (m_1, \ldots, m_n) \in \mathbf{Z}^n \setminus \{0\}$ is an integer relation for $\alpha_1, \ldots, \alpha_n$ and $\|m\| \leq 1/\varepsilon$, then*

$$\|m\|^2 + c^2 \cdot \left| \sum_{i=1}^{n} \overline{\alpha}_i m_i \right|^2 \leq \frac{2}{\varepsilon^2}.$$

(b) *If $m = (m_1, \ldots, m_n) \in \mathbf{Z}^n \setminus \{0\}$ is not an integer relation for $\alpha_1, \ldots, \alpha_n$, then*

$$\|m\|^2 + c^2 \cdot \left| \sum_{i=1}^{n} \overline{\alpha}_i m_i \right|^2 > \frac{2^n}{\varepsilon^2}.$$

Proof of Lemma 4. For the proofs of (a) and (b) we need the following claim, which can be immediately verified.

(1) For all $m \in \mathbf{Z}^n$ we have

$$\left| \sum_{i=1}^{n} \overline{\alpha}_i m_i - \sum_{i=1}^{n} \alpha_i m_i \right| < n \cdot q \cdot \|m\|.$$

Proof of (a). Since $\|m\| \leq 1/\varepsilon$, and by (1), we have

$$\|m\|^2 + c^2 \cdot \left| \sum_{i=1}^{n} \overline{\alpha}_i m_i \right|^2 \leq \frac{1}{\varepsilon^2} + \frac{c^2 n^2 q^2}{\varepsilon^2}.$$

By construction, $c \cdot n \cdot q < 1$, hence claim (a) is proven.

Proof of (b). If $\|m\| > 2^{n/2}/\varepsilon$, the assertion is obvious. So we assume $\|m\| \leq 2^{n/2}\varepsilon$. By Proposition 1 we have

$$\left| \sum_{i=1}^{n} \alpha_i m_i \right| \geq a(n, s, h, \|m\|).$$

Since $a(n, s, h, \|m\|)$ is monotone decreasing in $\|m\|$, this implies

$$\left| \sum_{i=1}^{n} \alpha_i m_i \right| \geq a(n, s, h, 2^{n/2}/\varepsilon).$$

Applying (1), we get

$$\left| \sum_{i=1}^{n} \overline{\alpha}_i m_i \right| \geq a(n, s, h, 2^{n/2}/\varepsilon) - n \cdot q \cdot 2^{n/2}/\varepsilon.$$

By the choice of q, this implies

(2) $|\sum_{i=1}^{n} \overline{\alpha}_i m_i| > a(n, s, h, 2^{n/2}/\varepsilon) \cdot \frac{1}{2}$.

Now by choice of c we get the desired bound:

$$\|m\|^2 + c^2 \cdot \left| \sum_{i=1}^{n} \overline{\alpha}_i m_i \right|^2 \overset{(2)}{>} c^2 \cdot a(n, s, h, 2^{n/2}/\varepsilon)^2 \cdot \frac{1}{4} \geq \frac{4 \cdot 2^n}{\varepsilon^2} \cdot \frac{1}{4} = \frac{2^n}{\varepsilon^2}.$$

This finishes the proof of Lemma 4. □

The correctness of our algorithm can be derived from Lemma 4 as follows. If the algorithm outputs m, then m is an integer relation for $\alpha_1, \ldots, \alpha_n$, since otherwise by Lemma 4(b) the algorithm would not have put it out. If the algorithm claims that there is no integer relation shorter than $1/\varepsilon$, then we have $\|b\|^2 > 2^n/\varepsilon^2$, and hence each nonzero vector in the lattice we deal with is longer than $\sqrt{2}/\varepsilon$. So, by Lemma 4(a), the claim of the algorithm is correct also in this case.

In order to analyze the run time of the algorithm, we now specify the admissible inputs $\overline{\alpha}_1, \ldots, \overline{\alpha}_n, \varepsilon$. Certainly, we require $|\alpha_i - \overline{\alpha}_i| < q$ for the q of Lemma 4 in order to assure the correctness of the algorithm. But in order to maintain a run time polynomial in $\log 1/\varepsilon$, n, $\log \max_i h(\alpha_i)$ and $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$, we must also bound the binary length of the input by a bound polynomial in these sizes. Hence we assume that the input numbers $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ and ε are (real or complex) rationals with a common denominator t, where

$$t \leq \left\lceil \frac{2^{n^3 s^3} \cdot h^{2n^2 s^2}}{\varepsilon^{2n^2 s^3}} \right\rceil.$$

Here, as before, we use the abbreviations s and h for $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$ and $\log \max_i h(\alpha_i)$, respectively. Since $|\alpha| \leq h(\alpha) + 1$, this choice of t ensures that the binary length of the input is as small as required. One readily verifies that for each n-tuple $(\alpha_1, \ldots, \alpha_n)$ of algebraic numbers there exist rationals $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ admissible for the algorithm. Now it is straightforward to estimate the run time of our algorithm with the LLL-Theorem.

The analysis of the algorithm is summed up in the following theorem.

Theorem 5. *Let* $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ *be algebraic numbers, and let* t *be an integer not larger than* $\lceil (2^{n^3 s^3} \cdot h^{2n^2 s^2}) / \varepsilon^{2n^2 s^3} \rceil$. *Let* $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$, $\varepsilon \in \frac{1}{t}(\mathbf{Z} + i\mathbf{Z})$ *satisfy* $\max_{1 \leq i \leq n} |\alpha_i - \overline{\alpha}_i| \leq \frac{1}{t}$. *Then, for given* $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ *and* ε, *the algorithm performs* $O(n^6 s^2 \cdot (ns + \log h + s \log 1/\varepsilon))$ *arithmetic operations on rational numbers of binary length* $O(n^3 s^2 \cdot (ns + \log h + s \log 1/\varepsilon))$. *It either finds an integer relation* m *with* $\|m\|^2 \leq 2^n/\varepsilon^2$ *for* $\alpha_1, \ldots, \alpha_n$, *or it proves that the Euclidean length of the shortest integer relation for* $\alpha_1, \ldots, \alpha_n$ *is larger than* $1/\varepsilon$.

4. Open problem

Does a theorem of the following kind exist?

"If $\alpha_1, \ldots, \alpha_n$ satisfy an integer relation, then they also satisfy an integer relation of length bounded by w, where $\log w$ is polynomially bounded in n, $\log \max_i h(\alpha_i)$ and $[\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$."

Such a theorem would imply that the parameter ε in our algorithm could be omitted. One could instead always run the algorithm for $\varepsilon := 1/w$ in order to find an integer relation or to disprove the existence of any relation. This would still take $\text{poly}(n, \log \max_i h(\alpha_i), [\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}])$ bit operations.

Acknowledgment

The results of this paper are part of the author's Ph. D. thesis guided by Professor C. P. Schnorr. I thank him for many helpful discussions. Moreover, I thank Professor M. Mignotte for his valuable hints.

Bibliography

1. L. Babai, B. Just, and F. Meyer auf der Heide, *On the limits of computations with the floor function*, Inf. Comput. **78** (1988), 99–107.
2. G. Bergman, *Notes on Ferguson and Forcade's generalized Euclidean algorithm*, preprint, Dept. of Math., Univ. of California, Berkeley, 1980.
3. G. Birkhoff and S. Mac Lane, *A survey of modern algebra*, Macmillan, New York, 1965.
4. B. Buchberger, G. Collins, and R. Loos (eds.), *Computer algebra. Symbolic and algebraic computation*, Springer, Wien and New York, 1982.
5. V. Brun, *En generalisation av kjedebroken*. I; II, Skr. Vid. Selsk. Kristiana, Mat. Nat. Kl. **6** (1919), 1–29; **6** (1920), 1–24.
6. H. Ferguson and R. Forcade, *Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two*, Bull. Amer. Math. Soc. (N. S.) **1** (1979), 912–914.
7. ——, *Multidimensional Euclidean algorithms*, J. Reine Angew. Math. **334** (1982), 171–181.
8. G. Fischer and R. Sacher, *Einführung in die Algebra*, Teubner, Stuttgart, 1983.

9. J. Hastad, 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.
10. C. G. J. Jacobi, *Allgemeine Theorie der kettenbruchähnlichen Algorithmen*, J. Reine Angew. Math. **69** (1868), 29–64.
11. R. Kannan, *Improved algorithms for integer programming and related problems*, 15th ACM Sympos. on Theory of Computing, Association for Computing Machinery, New York, 1983, pp. 193–206.
12. R. Kannan, A. K. Lenstra, and L. Lovász, *Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers*, Math. Comp. **182** (1988), 235–250.
13. J. C. Lagarias, *The computational complexity of simultaneous Diophantine approximation problems*, 23rd Annual Sympos. on the Foundations of Computer Science, IEEE Computer Society Press, Los Angeles, Calif., 1982, pp. 32–39.
14. A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 513–534.
15. O. Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus*, Math. Ann. **64** (1907), 1–76.
16. C. P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theor. Comput. Sci. **53** (1987), 201–224.
17. ——, *A more efficient algorithm for lattice basis reduction*, J. Algorithms **9** (1988), 47–62.
18. A. Schönhage, *Factorization of univariate integer polynomials by Diophantine approximation and by an improved basis reduction algorithm*, Proc. of 11th ICALP Antwerpen, Lecture Notes in Comput. Sci., vol. 172, Springer, 1984.
19. G. Szekeres, *Multidimensional continued fractions*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **13** (1970), 113–140.

FACHBEREICH MATHEMATIK, JOHANN WOLFGANG GOETHE-UNIVERSITÄT, ROBERT-MAYER-STRASSE 6–10, 6 FRANKFURT/MAIN, WEST GERMANY