ON MULTIDIMENSIONAL DIOPHANTINE APPROXIMATION OF ALGEBRAIC NUMBERS

ATTILA PETHŐ*, MICHAEL E. POHST AND CSANÁD BERTÓK

Abstract. In this article we develop algorithms for solving the dual problems of approximating linear forms and of simultaneous approximation in number fields F. Using earlier ideas for computing independent units by Buchmann, Pethő and later Pohst we construct sequences of suitable modules in F and special elements β contained in them. The most important ingredient in our methods is the application of the LLL-reduction procedure to the bases of those modules. For LLL-reduced bases we derive improved bounds on the sizes of the basis elements. From those bounds it is quite straight-forward to show that the sequence of coefficient vectors $(x_1, ..., x_n)$ of the presentation of β in the module basis becomes periodic. We can show that the approximations which we obtain are close to being optimal. Thus our algorithm can be considered as such a generalization of the continued fraction algorithm which is periodic on bases of real algebraic number fields.

1. Introduction

Let $\tau_1, ..., \tau_n$ be non-zero real numbers. In 1846 Dirichlet proved [4]: *For all $Q > 1$ there exist $x_1, ..., x_n \in \mathbb{Z}$, not all of them 0, such that*

$$|x_i| \leq Q \ \ (2 \leq i \leq n), \left| \sum_{i=1}^{n} x_i \tau_i \right| < |\tau_1| Q^{1-n} \ .$$

Further, for all $Q > 1$ there exist $x_1, ..., x_n \in \mathbb{Z}$, not all of them 0, such that

$$|x_1| \leq Q, \ \left| x_1 \frac{\tau_i}{\tau_1} - x_i \right| < Q^{-1/(n-1)} \ \ (2 \leq i \leq n) \ .$$

The first problem will be called *approximation of linear forms*, the second one *simultaneous approximation*. For $n = 2$ these inequalities are essentially identical which is not true for $n > 2$. However, by

Date: March 31, 2015.

Key words and phrases. Diophantine approximation, continued fractions, Jacobi-Perron algorithm, LLL-algorithm.

*Research supported in part by the OTKA grants NK100339 and NK104208.

the transference principle of Khintchine, see [5], [10] and [14], an approximation of a linear form can be transformed into a simultaneous approximation of the coefficients and vice versa.

For $n = 2$ the continued fraction algorithm - applied to $\frac{\tau_2}{\tau_1}$ - computes very efficiently solutions of Dirichlet's inequality. Moreover, the continued fraction of a real number τ is by a classical theorem of Lagrange [6] periodic if and only if τ is a quadratic algebraic number.

Since the early 19th century many attempts were made to find a generalization of the continued fraction algorithm for $n > 2$ and for the generalization of Lagrange's theorem for bases of algebraic number fields of degree $n > 2$. You find a good overview of these efforts in the book of Bernstein [1].

In 1902 H. Minkowski proved a generalization of Lagrange's theorem [9]. As his result is based on his multidimensional linear approximation process [8], which uses essentially the theory of successive minima, it does not yield an efficient method to find the periodic sequence. For algebraic numbers of special forms the Jacobi-Perron algorithm solves the problem, see again [1].

A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász published in 1982 a lattice basis reduction algorithm [7]. For integral lattices it has polynomial complexity in the size of the input vectors and of the discriminant. This algorithm is called nowadays LLL-algorithm. In that paper the authors showed that the LLL-algorithm solves a slightly weaker form of the simultaneous approximation problem for any given $Q > 1$, see Section 5. This method of solution is static in the sense that knowing a result for a constant Q we cannot use this information for calculating a solution for $\tilde{Q} > Q$. Recently W. Bosma and I. Smeets [2] published an iterated version of the LLL-algorithm for the computation of a sequence of solutions of the multidimensional diophantine approximation problem. Their algorithm handles several linear forms but has the same bottleneck as the original LLL-algorithm mentioned above.

J. Buchmann and A. Pethő [3] developed an algorithm for the computation of a system of independent units of full rank in algebraic number fields. Their method is based on a dynamical use of the LLL-algorithm and relies on successive computations of simultaneous

approximations of integral bases. In this way they made algorithmic the original proof of Dirichlet. M. Pohst [11] improved the efficiency of the method of Buchmann and Pethő.

In this paper we show that the method of Buchmann and Pethő is not only capable to produce a system of independent units of full rank in any algebraic number field, but also leads to an algorithmic generalization of Lagrange's theorem. Our algorithm for the approximation of linear forms uses in each iteration the LLL-algorithm twice; at first it is used to compute an approximation the result of which is an element with one small conjugate and all others big. With this element we divide the basis elements and compute an LLL-reduced basis of the module generated by them. This step has twofold advantages. First, as modules have only finitely many LLL-reduced bases, we get the periodicity. Usually the Jacobi-Perron-like algorithms do division by coordinates of the vector to be approximated. We do the same with a suitable linear combination of the coordinates. The absence of the combination of the coordinates can be a reason that efforts to prove periodicity of Jacobi-Perron-like algorithms on bases of algebraic number fields failed in general.

The second advantage is of numerical nature. The implementation of our algorithm works with rational approximations of algebraic numbers. [1] Without this step the first coordinates of the basis vectors would grow, while the other coordinates would decrease exponentially. To fix stability we would need much higher precision as in the present form.

The contents of the paper are ordered in the following way. In Section 2 we introduce our notations for number fields F of degree n and - in general - non-full modules M. We give estimates on the size of the basis vectors of LLL-reduced bases in terms of the degree n and the lattice determinant $d(M)$. The proof of those bounds is postponed to Section 6. Section 3 deals with approximation of linear forms the coefficients $\alpha_1, ..., \alpha_n$ of which form a basis of F. By Algorithm 1 we construct sequences of modules and integral vectors $(x_1, ..., x_n)$. In Subsection 3.1 the periodicity of that sequence $((x_{s,1}, ..., x_{s,n}))_{s\in\mathbb{N}}$ is proved. In Subsection 3.2 we discuss the quality of the approximations obtained in Algorithm 1. It turns out to be close to the best possible. They play a

[1] A good challenge for further investigations is to find complete periods for parametric families of bases of modules.

similar role as the partial quotients in continued fraction expansions. An Algorithm 2 - similar to Algorithm 1 - is developed in Section 4 for simultaneous approximation of algebraic numbers $\alpha_1, ..., \alpha_n$ of F. Again, it is shown that the produced sequence of coefficient vectors becomes periodic. In Section 5 we discuss the basics of both algorithms, i.e. the fundamental estimates of Dirichlet and by which margin those can be achieved by the corresponding approximations with the LLL-algorithm. In Section 6 we develop improved bounds on the sizes of the basis vectors of LLL-reduced bases of modules in number fields thus demonstrating Lemma 2. The final Section 7 contains various illustrative examples of calculations by both algorithms in number fields up to degree 10.

2. Notations and auxiliary results

Let F be an algebraic number field of degree d with r_1 real and $2r_2$ complex conjugates, i.e. $d = r_1 + 2r_2$. The conjugates $F = F^{(1)}, ..., F^{(d)}$ are ordered as usual:

$$F^{(j)} \subset \mathbb{R}\ (1 \le j \le r_1),\ F^{(j)} \not\subset \mathbb{R}\ (r_1 + 1 \le j \le d),$$

$$F^{(r_1+j)} = \overline{F^{(r_1+r_2+j)}}\,(1 \le j \le r_2)\ ,$$

where overlining means complex conjugation. Then we have the usual scalar product in F:

$$\langle\ ,\ \rangle : F \times F \to \mathbb{R} : (x, y) \mapsto \sum_{j=1}^{d} x^{(j)}\overline{y^{(j)}}\ . \tag{1}$$

We also put $T_2(x) = \langle x, x\rangle$ implying $\parallel x \parallel = \sqrt{T_2(x)}$ for elements $x \in F$.

Let $\tau_1, ..., \tau_n$ be $\mathbb{Q}$-linearly independent elements of F. With them we define the free $\mathbb{Z}$-module $M = \mathbb{Z}\tau_1 + ... + \mathbb{Z}\tau_n$ of rank n. Then M is a lattice with determinant $d(M) = \sqrt{\det(\langle\tau_i, \tau_j\rangle)_{1\le i,j\le n}}$. A basis $\alpha_1, \ldots, \alpha_n$ of M is called reduced if there exists a constant C depending only on n such that

$$\prod_{i=1}^{n} \parallel \alpha_i \parallel \le Cd(M) \tag{2}$$

holds. A nice and for us very helpful byproduct of the LLL-algorithm [7] is that applying it to any basis $\tau_1, ..., \tau_n$ of M it produces a LLL-reduced basis $LLL(\tau_1, \ldots, \tau_n)$ satisfying (2) with $C = 2^{n(n-1)/4}$.

Remark 1. *This inequality implies that M has only finitely many LLL-reduced bases. (Detailed estimates are listed in Section 6.)*

The next lemma is crucial in our investigations.

Lemma 2. *Let M be a free $\mathbb{Z}$-module of rank n with discriminant $d(M)$ in an algebraic number field F of degree $d \geq n$. Let $0 \neq \beta \in M, N = |N(\beta)|$ and $\tilde{M} = M/\beta$. If $\beta_1, \ldots, \beta_n$ is a LLL-reduced basis of $\tilde{M}$ then the absolute values of the conjugates $\beta_i^{(j)}$ are bounded from below and from above by constants depending on $n, d, N, d(\tilde{M})$. If M is a full module, i.e. $n = d$, then the dependency of the constants from N can be stated explicitely. We get*

$$C_{2i} N^{-1/n} \leq |\beta_i^{(j)}| \leq C_{3i} N^{-1/n} \tag{3}$$

with constants

$$C_{3i} = \left(\frac{C d(M)}{n^{(i-1)/2}} \right)^{1/(n+1-i)} \quad \text{and} \quad C_{2i} = C_{3i}^{1-n} \, .$$

We put $C_3 = C_{3n} = \max\{C_{3i} | i = 1, \ldots, n\}$ and $C_2 = C_3^{1-n}$.

We postpone the proof of this lemma to Section 6.

Unfortunately, for $d > n$ we were not able to establish a quantitative relation between $d(M)$ and $d(M/\beta)$ in general. In the next sections we will therefore only study full modules in number fields F.

There are two exceptions, however.

(1) Let M be a non-full module which is a full module in a proper subfield E of F. We assume that the degree of E is $(E : \mathbb{Q}) = n$ and that the relative degree $(F : E)$ equals m. Hence, we have $d = mn$. For elements α, $\beta \in E$ we obtain

$$\langle \alpha, \beta \rangle_F \, = \, m \langle \alpha, \beta \rangle_E \text{ and } N_{F/\mathbb{Q}}(\alpha) \, = \, N_{E/\mathbb{Q}}(\alpha)^m \, .$$

Then we can consider M as a full module in E and as a non-full module in F. Again, we denote by $\tilde{M}$ the module M/β for some $\beta \in M$. Accordingly, we immediately see that

$$d(M)_F \, = \, m^{n/2} d(M)_E$$

with the consequence

$$\begin{aligned} d(\tilde{M})_F &= m^{n/2} d(\tilde{M})_E = m^{n/2} \left(\frac{1}{N_{E/\mathbb{Q}}(\beta)} d(M)_E \right) \\ &= |N_{F/\mathbb{Q}}(\beta)|^{-1/m} d(M)_F \ . \end{aligned}$$

This puts us into a situation similar to full modules of F again.

(2) Let E, F, m, n, d as before. Let $M = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_m$ be a full module in E and $\alpha \in F \setminus E$. Then αM is a non-full module in F with $\mathbb{Z}$-basis $\tilde{\alpha}_i := \alpha\alpha_i$ $(1 \le i \le m)$. Such modules play an important role in the theory of norm form equations (see [13], [14], for example). Without loss of generality we can assume that the last basis is a LLL-reduced basis of the non-full module αM in F. In the next section we develop an algorithm for determining a suitable element β in αM, i.e. $\beta = x_1\tilde{\alpha}_1 + ... + x_n\tilde{\alpha}_n$ with $(x_1, ..., x_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$. Then we define a new module $\tilde{M} = \alpha M/\beta$. It has the basis $\alpha_i/(x_1\alpha_1 + ... + x_n\alpha_n)$ $(1 \le i \le n)$, hence $\tilde{M}$ is contained in E. The further construction of a sequence of modules (see Algorithm 1) is therefore with full modules in E only.

3. Approximation of linear forms

Let $\alpha_1, \ldots, \alpha_n$ be a basis of a real algebraic number field of degree $d = n$. In this section we present an algorithm for the computation of a sequence of integer vectors $\mathbf{x}_s = (x_{s,1}, ..., x_{s,n})$ $(s \in \mathbb{N})$ which is ultimately periodic. The values of the linear form $\alpha_1 X_1 + \cdots + \alpha_n X_n$ evaluated at suitable combinations of the $\mathbf{x}_s$ tend to zero with a speed which is close to best possible, see Theorem 5. Thus our algorithm has similar properties as the classical continued fraction algorithm applied to real quadratic irrationalities. The output sequence of integer vectors $\mathbf{x}_s$ of Algorithm 1 plays the same role as partial quotients.

For an easier understanding of that algorithm we explain the construction in some detail beforehand. The procedure incorporates several sequences. The first one is a sequence of varying modules M_s starting with $M_0 = M_1 = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_n$. The second one consists of vectors $(\alpha_{s,1}, ..., \alpha_{s,n})$ representing LLL-reduced bases of M_s. The third one incorporates special elements $\beta_s \in M_s$, where the presentation of $\beta_s = x_{s,1}\alpha_{s,1} + ... + x_{s,n}\alpha_{s,n}$ in a LLL-basis $\alpha_{s,1}, ..., \alpha_{s,n}$ of M_s incorporates the integer vectors $\mathbf{x}_s$ introduced at the beginning of this section. In each step $s \in \mathbb{N}$ we use a black box algorithm

for the computation of β_s. That algorithm contains an additional positive constant D. In Section 5 we show that we can use the LLL-algorithm also for solving that task by using the LLL-constant C for D. Eventually, we can increase s by 1 after putting $M_{s+1} = M_s/\beta_s$ and $(\alpha_{s+1,1}, ..., \alpha_{s+1,n}) = LLL(\alpha_{s,1}/\beta_s, ..., \alpha_{s,1}/\beta_s)$.

If we apply the algorithm below we encounter the phenomenon that the new basis in Step 4. can coincide with the previous one, namely for $\beta = 1$. This happens, for example, for $\alpha_1 = 1 < \alpha_2 \leq ... \leq \alpha_n$. In that case we always get $(x_1, ..., x_n) = (1, 0, ..., 0)$ in Step 3.. Obviously, the algorithm has period lenghth 1. To avoid such trivial periods we must enforce $\beta \neq 1$ in Step 3.. This can be achieved by choosing $Q > D^{1/(n-1)}$, for example.

In order to detect periodicity of the sequences we make use of Pollard's method [12]: For $k = 2^\ell \quad (\ell = 1, 2, ...)$ we store the LLL-reduced basis $(\alpha_{k,1}, ..., \alpha_{k,n})$ and check whether it coincides with any of the bases $\pm(\alpha_{s,1}, ..., \alpha_{s,n})$ for $s = k + 1, ..., 2k$.

We still mention that for the computation of simultaneous approximations of algebraic numbers we calculate suitable vectors $\mathbf{x}_s$ in a more sophisticated way, see Section 4.

Algorithm 1 Approximation of linear forms

Require: $\alpha_1, ..., \alpha_n$ a basis of a real algebraic number field of degree n, and constants $D > 1$ and $Q > D^{1/(n-1)}$

Ensure: an eventually periodic sequence of integer vectors $(x_1, ..., x_n)$

1: $s \leftarrow 1$, $\ell \leftarrow 1$, $(\alpha_1, ..., \alpha_n) \leftarrow LLL(\alpha_1, ..., \alpha_n)$
2: $\ell \leftarrow 2\ell$, $(\tilde{\alpha}_1, ..., \tilde{\alpha}_n) \leftarrow (\alpha_1, ..., \alpha_n)$
3: Compute $(x_1, \ldots, x_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ such that

$$|x_i| \leq Q \,, i = 2, \ldots, n \,,$$
$$\beta \leftarrow x_1\alpha_1 + \cdots + x_n\alpha_n \;\text{ satisfying }\; |\beta| < D|\alpha_1|Q^{1-n} \,,$$

output s, $(x_1, \ldots, x_n)$
4: $(\alpha_1, ..., \alpha_n) \leftarrow LLL(\frac{\alpha_1}{\beta}, ..., \frac{\alpha_n}{\beta})$
5: **if** $(\tilde{\alpha}_1, ..., \tilde{\alpha}_n) = \pm(\alpha_1, ..., \alpha_n)$ **return** period length $s - \ell/2 + 1$
6: $s \leftarrow s + 1$
7: **if** $s < \ell$ **then goto** 3. , **else goto** 2.

3.1. **Periodicity of Algorithm 1.**

Theorem 3. *For $Q > D^{1/(n-1)}$ Algorithm 1 terminates, i.e. the sequence of integer vectors $(x_1, \ldots, x_n)$ has a non-trivial period.*

Proof. We will prove that $(\alpha_1, \ldots, \alpha_n)$ can assume only finitely many values, say from the finite set S. Moreover Steps 3. to 6. define a mapping $S \to S$. Hence, the algorithm terminates after finitely many steps.

For simplicity's sake we assume that the module $M_0 = M_1$ is contained in the ring of integers o_F of the algebraic number field F under consideration. The general case can be easily deduced from this. We recall that we generate sequences of modules $(M_s)_{s\in\mathbb{N}}$, LLL-reduced bases $(\alpha_{s,1}, ..., \alpha_{s,n})$ for M_s and integer vectors $\mathbf{x}_s = (x_{s,1}, ..., x_{s,n})$. For $\beta_s = x_{s,1}\alpha_{s,1} + ... + x_{s,n}\alpha_{s,n}$ we set $M_{s+1} = M_s/\beta_s$ and proceed with a LLL-reduced basis $(\alpha_{s+1,1}, ..., \alpha_{s+1,n})$ of M_{s+1}. Additionally, we put $\gamma_s = \prod_{j=1}^{s} \beta_j$ implying $M_{s+1} = M_0/\gamma_s$.

Now we fix $s > 1$ and set $N = |N(\gamma_{s-1})|$. In Step 3. of the algorithm the vector $(x_{s,1}, \ldots, x_{s,n})$ satisfies the inequalities

$$|x_{s,i}| \ \leq \ Q \ , i = 2, \ldots, n \tag{4}$$

and the absolute value of the element $\beta_s = x_{s,1}\alpha_{s,1} + \cdots + x_{s,n}\alpha_{s,n}$ is bounded by

$$|\beta_s| \ < \ D|\alpha_{s,1}|Q^{1-n} \ . \tag{5}$$

We note that $\beta_s = \beta_s^{(1)}$ and that the absolute values of all $\alpha_{s,i}^{(j)}$ for $i, j = 1, ..., n$ are bounded from above by $C_3 N^{-1/n}$ and from below by $C_2 N^{-1/n}$ according to Lemma 2. The element β_s is the first basis element of a LLL-reduced basis and therefore non-zero. Also, $\beta_s \neq 0$ is tantamount to $(x_{s,1}, ..., x_{s,n}) \neq \mathbf{0}$.

An upper bound for $|x_{s,1}|$ is easily obtained from (4) and (5) via

$$|x_{s,1}\alpha_{s,1}| \ < \ D|\alpha_{s,1}|Q^{1-n} + (n-1)QC_3N^{-1/n} \ .$$

implying

$$|x_{s,1}| \ \leq \ C_4 Q \tag{6}$$

where we set $C_4 = DQ^{-n} + (n-1)C_3/C_2$.

From this upper bounds for the absolute values of all conjugates of β_s, hence also for $|N(\beta_s)|$, are immediate. We calculate

$$|\beta_s^{(j)}| \ < (C_4 + n - 1)C_3 Q N^{-1/n} \ \ (1 \leq j \leq n) \tag{7}$$

and

$$N^{-1} \leq |N(\beta_s)| = \prod_{j=1}^{n} |\beta_s^{(j)}| \leq C_5 N^{-1} \tag{8}$$

with $C_5 = (C_4 + n - 1)^{n-1} D C_3^n$. Finally, we have

$$|N(\gamma_s)| = |N(\gamma_{s-1})N(\beta_s)| \leq C_5. \tag{9}$$

Because of $\beta_s \in M_s = M_0/\gamma_{s-1}$ all elements γ_s belong to the module $M_0 \subseteq o_F$. Since o_F contains only finitely many pairwise non-associated elements of bounded norm there exists a subsequence $(M_{s_i})_{i\in\mathbb{N}}$ such that $\tilde{N} = |N(\gamma_{s_i})|$ for all $i \in \mathbb{N}$. Clearly, we have $\gamma_{s_i}^{-1} M_0 \subseteq \tilde{N}^{-1} o_F =: \tilde{M}$. Since there exist only finitely many elements of bounded T_2-norm in $\tilde{M}$ the set of all LLL-reduced bases of the modules $(M_{s_i})_{i\in\mathbb{N}}$ is finite. This implies that there exist (smallest) indices $\mu < \nu$ such that the LLL-reduced bases of M_{s_μ} and of M_{s_ν} coincide. From here on the process is periodic. □

Remark 4. *We note that for the proof of the finiteness of the set of LLL-reduced bases produced by Algorithm 1 we do not need to apply the same Q in Step 3. in each iteration. If the Q's form an arbitrary sequence of numbers bigger than one, then the sequence $(\mathbf{x}_s)_{s\in\mathbb{N}}$ will in general not be periodic. The periodicity does not only depend on the LLL-reduced bases of M_s, but also on the sequence of the Q's. However if the sequence of the Q's is bounded then there exist only finitely many pairwise different modules M_s.*

3.2. **Quality of the approximations.** For a vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{R}^n$ the maximum norm will be denoted by

$$|\mathbf{v}| = \max\{|v_i| \mid i = 1, \ldots, n\}.$$

Also, we introduce a function ψ on $\mathbb{R}$ satisfying: for all $a > 1$ there exists $x_0 > 0$ such that for all $x > x_0$ and $m \in \mathbb{N}$ we have $\psi(x^m)^{1/m} > a$.

Theorem 5. *Let $\alpha_1, \ldots, \alpha_n$ be $\mathbb{Q}$-linearly independent elements of a real algebraic number field F of degree n. Let $(\beta_s)_{s\in\mathbb{N}}$ be the sequence of elements of F computed by Algorithm 1. For $m \in \mathbb{N}$ we set $\gamma_m = \prod_{j=1}^{m} \beta_j$ and write*

$$\gamma_m = y_{m,1}\alpha_1 + \cdots + y_{m,n}\alpha_n \quad \textit{with} \quad \mathbf{y}_m = (y_{m,1}, ..., y_{m,n}) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}\ .$$

There exists a constant Q_0 depending only on $n, D, \alpha_1, \ldots, \alpha_n$ and ψ such that $Q > Q_0$ implies

$$|y_{m,1}\alpha_1 + \cdots + y_{m,n}\alpha_n| \le C_5|\mathbf{y}_m|^{1-n}\psi(|\mathbf{y}_m|^{1/m})^m \ .$$

Remark 6. *By a celebrated theorem of W. M. Schmidt* [14] *the inequality*

$$|y_1\alpha_1 + ... + y_n\alpha_n| \ \le \ |\mathbf{y}|^{1-n-\varepsilon}$$

with $\varepsilon > 0$ arbitrarily small has only finitely many solutions $\mathbf{y} = (y_1, ..., y_n) \in \mathbb{Z}^n$. The choice $\psi(x) = x^\delta$ with $\delta > 0$ shows that our algorithm produces an infinite sequence of integer vectors $\mathbf{y}$ satisfying

$$|y_1\alpha_1 + ... + y_n\alpha_n| \ \le \ C_5|\mathbf{y}|^{1-n+\delta}$$

Therefore our algorithm is close to best possible.

Proof. We recall that we construct a sequence of full modules $M_s = \mathbb{Z}\alpha_{s,1} + ... + \mathbb{Z}\alpha_{s,n}$ for $s \in \mathbb{Z}^{\ge 0}$ in a number field F of degree n. In general, the module M_0 will be an order of F. The bases of the modules are assumed to be LLL-reduced. The next element in that sequence is obtained from the previous one via a LLL-version of Dirichlet approximation (see Section 5). We construct $0 \ne \beta_s = \sum_{j=1}^n x_{s,j}\alpha_{s,j} \in M_s$ subject to

$$0 \le |x_{s,j}| \le Q \ (2 \le j \le n) \text{ and } |\beta_s| \le D|\alpha_{s,1}|Q^{1-n} \tag{10}$$

and set $M_{s+1} = M_s/\beta_s$.

Besides that sequence of modules M_s we obtain a sequence of algebraic integers

$$\gamma_s \ = \ \beta_1 \cdots \beta_s \tag{11}$$

which are of bounded norm. By (9) we have $|N(\gamma_s)| \le C_5$. Because of $M_s = M_0/\gamma_{s-1}$ we know that the absolute norms of non-zero elements $\alpha \in M_s$ satisfy $|N(\alpha)| \ge 1/C_5$. We recall that from (6) we get an upper bound for $|x_{s,1}|$ in the form

$$|x_{s,1}| \ \le \ C_4 Q \ . \tag{12}$$

Now we fix a positive integer m. We know that $\gamma_m \in M_0$, hence, there exists a presentation $\gamma_m = y_{m,1}\alpha_1 + ... + y_{m,n}\alpha_n$ with integral coefficients $y_{m,j}$. From the product in (11), from (3) and the definition of N, i.e.

$N = |N(\beta_{s-1})|$ with $N(\beta_0) = 1$, we derive an upper bound

$$\begin{aligned} |\gamma_m| = \prod_{j=1}^{m} |\beta_j| &\leq (DC_3)^m Q^{m(1-n)} \prod_{j=1}^{m} |N(\beta_{j-1})|^{-1/n} \\ &= (DC_3 Q^{1-n})^m |N(\gamma_{m-1})|^{-1/n} \\ &\leq C_5^{-1/n} (DC_3 Q^{1-n})^m. \end{aligned} \tag{13}$$

Next we estimate the size of $|y_{m,j}|$. As $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis of F there exist $r_{sij} \in \mathbb{Q}$ with

$$\alpha_{s,i} = r_{si1}\alpha_1 + \cdots + r_{sin}\alpha_n.$$

By Theorem 3 there exist only finitely many different modules in the sequene (M_s), moreover their LLL-reduced bases are effectively computable. Thus the set $\{|r_{sij}|, \mid 1 \leq, i, j \leq n, s \in \mathbb{N}\}$ is bounded, say by R. We obtain

$$\begin{aligned} \beta_s &= \sum_{j=1}^{n} x_{s,j}\alpha_{s,j} \\ &= \sum_{j=1}^{n} z_{s,j}\alpha_j \end{aligned}$$

with coefficients $z_{s,j} \in \mathbb{Q}$, $|z_{s,j}| \leq nRC_4Q$ for $1 \leq j \leq n$, $s \in \mathbb{N}$. Using this and the explicit presentations of the β_s we get

$$\begin{aligned} \gamma_m &= \gamma_{m-1}\beta_m \\ &= (y_{m-1,1}\alpha_1 + \cdots + y_{m-1,n}\alpha_n)(z_{m,1}\alpha_1 + \cdots + z_{m,n}\alpha_n)\ . \end{aligned}$$

Because of $\alpha_i\alpha_j \in F$ there exist constants $\tilde{r}_{ijk} \in \mathbb{Q},\ 1 \leq i, j, k \leq n$, satisfying

$$\alpha_i\alpha_j = \sum_{k=1}^{n} \tilde{r}_{ijk}\alpha_k \ \text{ for } \ 1 \leq i, j \leq n.$$

Let $R_1 = \max\{|\tilde{r}_{ijk}| \mid 1 \leq i, j, k \leq n\}$. Then

$$y_{m,k} = \sum_{i=1}^{n}\sum_{j=1}^{n} \tilde{r}_{ijk} y_{m-1,i} z_{m,j}$$

provides the upper bound

$$|\mathbf{y}_m| \leq n^2 R_1 nRC_4 Q |\mathbf{y}_{m-1}|\ .$$

It implies

$$|\mathbf{y}_m| \leq (C_6 Q)^m \tag{14}$$

with $C_6 = n^3 R_1 R C_4$ depending only on n, D and $\alpha_1, \ldots, \alpha_n$. From (14) and (13) we conclude that the elements of the sequence $(y_{m,1}, \ldots, y_{m,n})$ satisfy the system of inequalities

$$\begin{aligned} |y_{m,k}| &\leq (C_6 Q)^m \text{ for } 1 \leq k \leq n \\ |y_{m,1}\alpha_1 + \cdots + y_{m,n}\alpha_n| &\leq C_5^{-1/n}(DC_3C_6^{n-1}(C_6Q)^{1-n})^m . \end{aligned}$$

If Q_0 is so large that $\psi((C_6Q_0)^m) \geq (DC_3C_6^{n-1})^m$ then we obtain for $Q > Q_0$

$$|y_{m,1}\alpha_1 + \cdots + y_{m,n}\alpha_n| \leq C_5^{-1/n}|\mathbf{y}_m|^{1-n}\psi(|\mathbf{y}_m|^{1/m})^m$$

and the theorem is proved. □

4. Simultaneous approximation of algebraic numbers

In this section we turn to the classical problem to find a generalization of the continued fraction algorithm for simultaneous approximation of any dimension which is periodic for algebraic inputs. We give here a partial answer by presenting an algorithm which is periodic for bases of real algebraic number fields. By Khintchine's transference principle, see Khintchine [5], Perron [10] and Schmidt [14], the approximation of linear forms and simultaneous approximation of the coefficients of the form are dual problems. The solution of one of them can be transformed more or less easily to the solution of the other. Using this principle minor modifications of Algorithm 1 lead to simultaneous approximation of algebraic numbers.

In Steps 3. and 4. of Algorithm 2 we may use appropriate versions of the LLL-algorithm, see Section 5. One can replace these by other procedures which produce for all $Q > 1$ integer vectors satisfying the given inequalities, maybe with a different constant C. By Dirichlet's approximation theorems (see e.g. [14]) one should be able to achieve $C = 1$, but we do not know of any algorithm which computes efficiently approximation vectors of such a good quality in practice.

Theorem 7. *If $\alpha_1, ..., \alpha_n$ is a basis of a real algebraic number field F of degree n, and Q is large enough then Algorithm 2 is correct, i.e. the sequence of output vectors $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ is periodic.*

Proof. Our proof is based on the idea of the proof of Satz 1. of Perron [10]. We set $(\alpha_{s,1}, \ldots, \alpha_{s,n}), M_s, s = 0, 1, 2, \ldots$ and $(x_{s,1}, \ldots, x_{s,n}), \beta_s, s = 1, 2, \ldots$ as in the proof of Theorem 3. Additionally, we denote by $(k_{s,1}, \ldots, k_{s,n})$ for $s \in \mathbb{N}$ the vectors computed in Step 4. of Algorithm 2.

Algorithm 2 Simultaneous approximation of algebraic numbers

Require: $\alpha_1, ..., \alpha_n$ a basis of a real algebraic number field of degree n, and $Q > 1$

Ensure: an eventually periodic sequence of integer vectors $(x_1, ..., x_n)$

1: $s \leftarrow 1, \ell \leftarrow 1$, $(\alpha_1, ..., \alpha_n) \leftarrow LLL(\alpha_1, ..., \alpha_n)$
2: $\ell \leftarrow 2\ell$, $(\tilde{\alpha}_1, ..., \tilde{\alpha}_n) \leftarrow (\alpha_1, ..., \alpha_n)$
3: Compute $(k_1, \dots, k_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, $k_1 \neq 0$, such that

$$|k_1| \leq CQ \quad \text{and} \quad |k_j - k_1 \frac{\alpha_j}{\alpha_1}| < Q^{-1/(n-1)}, \ j = 2, \dots, n$$

with the constant $C = 2^{n(n-1)/4}$, output $s, (k_1, \dots, k_n)$
4: Compute a vector $(x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ such that

$$x_1 k_1 - \sum_{j=2}^{n} x_j k_j = 0 \quad \text{and} \quad |x_j| \leq 2^{n/2} |k_1|^{1/(n-1)}, j = 2, \dots, n$$

5: $\beta \leftarrow x_1\alpha_1 + \cdots + x_n\alpha_n$
6: $(\alpha_1, ..., \alpha_n) \leftarrow LLL(\frac{\alpha_1}{\beta}, ..., \frac{\alpha_n}{\beta})$
7: **if** $(\tilde{\alpha}_1, ..., \tilde{\alpha}_n) = \pm(\alpha_1, ..., \alpha_n)$ **return** period length is $s - \ell/2 + 1$
8: $s \leftarrow s + 1$
9: **if** $s < \ell$ **then goto** 3., **else goto** 2.

The vectors $(k_{s,1}, \dots, k_{s,n}) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ can be computed by the LLL-algorithm which we will show in Section 5. We note that $k_{s,1} \neq 0$ for all s. Indeed, if $k_{s,1} = 0$ for an $s \in \mathbb{N}$ the second inequality in Step 3., together with $Q > 1$ implies $k_{s,j} = 0$ for $j = 2, \dots, n$, thus $(k_{s,1}, \dots, k_{s,n}) = \mathbf{0}$, a contradiction.

Now we prove that the vectors $(x_{s,1}, \dots, x_{s,n})$ of Step 4., which also can be computed by the LLL-algorithm, are suitable approximations of the vectors $(\alpha_{s,1}, \dots, \alpha_{s,n})$. To simplify the notation we omit the index s.

Indeed, setting $Q_1 = 2^{n/2}|k_1|^{1/(n-1)}$ we can calculate $(x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ which satisfies the actualized form of the system of inequalities

(17)
$$\begin{aligned} |x_i| &\leq 2^{n/2}|k_1|^{1/(n-1)},\ i=2,\ldots,n \\ |x_1k_1-\sum_{j=2}^{n}x_jk_j| &< C|k_1|(2^{n/2}|k_1|^{1/(n-1)})^{1-n} \\ &= C^{-1}\,. \end{aligned}$$

Thus the absolute value of the integer $x_1k_1-\sum_{j=2}^{n}x_jk_j$ is less than one, hence it is zero, which justifies Step 4.

We assume that $(k_1,\ldots,k_n),(x_1,\ldots,x_n)\in\mathbb{Z}^n\setminus\{\mathbf{0}\}$, $k_1\neq 0$, are computed in Steps 3. and 4., respectively. Then we have

$$\begin{aligned} \alpha_1\left(x_1-\sum_{j=2}^{n}x_j\frac{\alpha_j}{\alpha_1}\right) &= \alpha_1\left(x_1-\sum_{j=2}^{n}x_j\frac{\alpha_j}{\alpha_1}-x_1+\sum_{j=2}^{n}\frac{x_jk_j}{k_1}\right) \\ &= \alpha_1\left(\sum_{j=2}^{n}\frac{x_j}{k_1}\left(\frac{k_1\alpha_j}{\alpha_1}-k_j\right)\right)\,. \end{aligned}$$

This implies

$$\begin{aligned} |\alpha_1x_1-\sum_{j=2}^{n}\alpha_jx_j| &< |\alpha_1|2^{n/2}|k_1|^{1/(n-1)}(n-1)Q^{-1/(n-1)}/|k_1| \\ &\leq |\alpha_1|2^{n/2}(CQ)^{1/(n-1)}(n-1)Q^{-1/(n-1)}/|k_1| \\ &= |\alpha_1|2^{n/2}C^{1/(n-1)}(n-1)/|k_1| \end{aligned}$$

Setting $Q_2=2^{n/2}|k_1|^{1/(n-1)}$ we obtain that $(x_1,\ldots,x_n)\in\mathbb{Z}^n\setminus\{\mathbf{0}\}$ satisfies the system of inequalities

$$|x_j|\leq Q_2 \text{ for } j=2,\ldots,n \text{ and } |\alpha_1x_1-\sum_{j=2}^{n}\alpha_jx_j|<|\alpha_1|DQ_2^{1-n}$$

with $D=(n-1)2^{n^2/2}C^{1/(n-1)}=(n-1)2^{n(2n+1)/4}$. Hence, the requirements of Step 3. in Algorithm 1 are satisfied. However, the direct application of Theorem 3 is not possible because Q_2 is not a constant, it depends on the computed value of k_1 and we know only that $|k_1|\leq CQ$. Thus the sequence of the Q_2's is bounded by $2^{n/2}(CQ)^{1/(n-1)}=2^{n(2n+1)/4}$. Hence, by Remark 4 in the sequence of the LLL-reduced bases in Step 4. of Algorithm 2 appear only finitely many different vectors. Let us assume that we have $(\alpha_{s,1},\ldots,\alpha_{s,n})=(\alpha_{t,1},\ldots,\alpha_{t,n})$ for some $s<t$ for the vectors computed in Step 6. of Algorithm 2. Then, as Q is fixed, we have $(k_{s+1,1},\ldots,k_{s+1,n})=(k_{t+1,1},\ldots,k_{t+1,n})$, i.e. from here on the sequence $(k_{s,1},\ldots,k_{s,n})$ is periodic. □

5. Dirichlet and LLL approximation

At the beginning of the introduction we already mentioned the following results of Dirichlet:
Let $\tau_1, ..., \tau_n$ be non-zero real numbers.
For all $Q > 1$ there exist $x_1, ..., x_n \in \mathbb{Z}$, not all of them 0, such that

$$|x_i| \leq Q \ \ (2 \leq i \leq n), \left| \sum_{i=1}^{n} x_i \tau_i \right| < |\tau_1| Q^{1-n} \ . \tag{15}$$

Further, for all $Q > 1$ there exist $x_1, ..., x_n \in \mathbb{Z}$, not all of them 0, such that

$$|x_1| \leq Q, \ \left| x_1 \frac{\tau_i}{\tau_1} - x_i \right| < Q^{-1/(n-1)} \ \ (2 \leq i \leq n), \ . \tag{16}$$

In [7] the authors proved that one can obtain slightly weaker results by LLL-reduction:

$$|x_i| \leq Q \ \ (2 \leq i \leq n), \left| \sum_{i=1}^{n} x_i \tau_i \right| < C |\tau_1| Q^{1-n} \ =: \ B_Q \tag{17}$$

as well as

$$|x_1| \leq CQ, \ \left| x_1 \frac{\tau_i}{\tau_1} - x_i \right| < Q^{-1/(n-1)} \ \ (2 \leq i \leq n), \ . \tag{18}$$

The constant C only depends on n. The LLL-property used in general implies

$$C \ = \ 2^{n(n-1)/4} \ . \tag{19}$$

With respect to the viewpoint of approximating we usually request that the last upper bound in (17) is smaller than $|\tau_1|$. This is achieved by requiring

$$Q \ > \ C^{1/(n-1)} \ . \tag{20}$$

We note that the last inequality is more restrictive than $Q > 1$ in Dirichlet's statement.
For completeness we recapitulate here how to compute the approximations (17) and (18) following essentially [7].

First we are dealing with the *approximation of linear forms*, i.e. with (17). Let δ be a positive constant which will be specified below. We consider a lattice Λ which is generated by the columns of the following

matrix.

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & \delta \\ 0 & 0 & 0 & \dots & \delta & 0 \\ & & & \dots & 0 & 0 \\ & & \delta & \dots & 0 & 0 \\ 0 & \delta & 0 & \dots & 0 & 0 \\ \tau_1 & \tau_2 & \tau_3 & \dots & \tau_{n-1} & \tau_n \end{pmatrix} . \tag{21}$$

Obviously, the lattice determinant is $d(\Lambda) = |\tau_1|\delta^{n-1}$. The first basis vector, say $\mathbf{a}$, of a LLL-reduced basis is of the form

$$\mathbf{a} = (x_n\delta, ..., x_2\delta, \sum_{i=1}^{n} x_i\tau_i)^{tr} .$$

Its Euclidean length is bounded by $B_{\mathbf{a}} := (C|\tau_1|)^{1/n}\delta^{(n-1)/n}$. For $2 \leq i \leq n$ this yields

$$|x_i| \leq (C|\tau_1|)^{1/n}\delta^{-1/n}$$

and the constant Q of (17) should be at least as large as the right-hand side of the last inequality. We therefore set

$$\delta \ = \ Q^{-n}C|\tau_1| . \tag{22}$$

In case of equality we find for the remaining coordinate of $\mathbf{a}$:

$$\left|\sum_{i=1}^{n} x_i\tau_i\right| \ \leq \ B_{\mathbf{a}} \ \leq \ |\tau_1|Q^{1-n}C \ = \ B_Q .$$

We note that those inequalities for the absolute values of the coordinates of $\mathbf{a}$ also lead to an upper bound for $|x_1|$. We know that

$$-B_Q \leq |x_1\tau_1| - \left|\sum_{i=2}^{n} x_i\tau_i\right| \leq B_Q$$

and obtain

$$|x_1| \leq \left(B_Q + Q\sum_{i=2}^{n} |\tau_i|\right)/|\tau_1| . \tag{23}$$

This procedure can be iterated by increasing Q in each step appropriately.

Our considerations above immediately lead to the following algorithm in which we make use of the well-known Kronecker symbol $\delta_{i,j}$ The value of $\delta_{i,j}$ is 1 for $i = j$ and it is 0 for $i \neq j$.

Algorithm 3 Dirichlet approximation

Require: an integer $n \geq 2$ and real numbers $\tau_1, ..., \tau_n$ and $Q > C^{1/(n-1)}$

Ensure: integers $x_1, ..., x_n$ such that (17) and (23) are satisfied (with $B_Q < 1$)

$C \leftarrow 2^{n(n-1)/4}$
$\delta \leftarrow Q^{-n} C|\tau_1|$
$i \leftarrow 1$
while $i \leq n$ **do**
    $\mathbf{a}_i \leftarrow (\delta\delta_{n+1-i,1}, ..., \delta\delta_{n+1-i,n-1}, \tau_i) \in \mathbb{R}^{1\times n}$
    $i \leftarrow i + 1$
end while
$(\mathbf{b}_1, ..., \mathbf{b}_n) \leftarrow LLL(\mathbf{a}_1, ..., \mathbf{a}_n)$ with $\mathbf{b}_1 = x_1\mathbf{a}_1 + ... + x_n\mathbf{a}_n$
return $x_1, ..., x_n$

Next we consider *simultaneous approximations* (18). In this case we consider a lattice Λ which is generated by the columns of the following matrix.

$$\begin{pmatrix} -\tau_2/\tau_1 & 1 & 0 & \dots & 0 & 0 \\ -\tau_3/\tau_1 & 0 & 1 & \dots & 0 & 0 \\ -\tau_4/\tau_1 & 0 & 0 & \dots & 0 & 0 \\ . & . & . & \dots & . & . \\ . & . & . & \dots & . & . \\ -\tau_n/\tau_1 & 0 & 0 & \dots & 0 & 1 \\ 2^{-n(n-1)/4}Q^{-n/(n-1)} & 0 & 0 & \dots & 0 & 0 \end{pmatrix}. \tag{24}$$

Obviously, the lattice determinant is $d(\Lambda) = 2^{-n(n-1)/4}Q^{-n/(n-1)}$. The first basis vector, say $\mathbf{a}$, of a LLL-reduced basis is of the form

$$\mathbf{a} = \left(x_2 - x_1\frac{\tau_2}{\tau_1}, ..., x_n - x_1\frac{\tau_n}{\tau_1}, x_1 2^{-n(n-1)/4}Q^{-n/(n-1)}\right)^{tr}.$$

Its Euclidean length is bounded by $B_{\mathbf{a}} = 2^{(n-1)/4}d(\Lambda)^{1/n} = Q^{-1/(n-1)}$. For $2 \leq i \leq n$ this yields

$$\left|x_1 - x_i\frac{\tau_i}{\tau_1}\right| < Q^{-1/(n-1)}$$

and

$$|x_1| \leq 2^{n(n-1)/4}Q^{n/(n-1)}Q^{-1/(n-1)} = CQ.$$

6. Proof of Lemma 2

Assume that $M = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_n$ is a free $\mathbb{Z}$-module of rank n in a number field F of degree d. There exists an integer $H > 0$ such that $HM \subseteq o_F$. In the sequel we assume $M \subseteq o_F$ and, if necessary, we adjust the result to the general case.

We choose $0 \neq \beta \in M$ and set $N = |N(\beta)|,\ \tilde{M} = M/\beta$. If $\beta_1, ..., \beta_n$ is a LLL-reduced basis for $\tilde{M}$ the new basis vectors satisfy

$$\prod_{i=1}^{n} \parallel \beta_i \parallel \leq Cd(\tilde{M}), \tag{25}$$

see (2). In order to produce upper and lower bounds for the absolute values of the conjugates $\beta_i^{(j)}$ we can proceed in analogy to Buchmann and Pethő [3]. They observe that any non-zero element $\tilde{\alpha}$ of $\tilde{M}$ has a norm whose absolute value is bigger than or equal to $1/N$. Using the inequality between arithmetic and geometric means yields

$$\frac{1}{N^2} \leq \left| \prod_{j=1}^{d} \tilde{\alpha}^{(j)} \right|^2 \leq \left(\frac{\sum_{j=1}^{d} |\tilde{\alpha}^{(j)}|^2}{d} \right)^d$$

hence, $N^{-2/d} d \leq T_2(\tilde{\alpha})$ implying

$$\parallel \tilde{\alpha} \parallel \geq \sqrt{d} N^{-1/d} . \tag{26}$$

From (25) we therefore obtain the upper bound

$$\parallel \beta_i \parallel \leq Cd(\tilde{M})(\sqrt{d}N^{-1/d})^{1-n} =: B_1 \tag{27}$$

and each conjugate $\beta_i^{(j)}$ also satisfies $|\beta_i^{(j)}| \leq B_1$. Then a crude lower bound for $|\beta_i^{(j)}|$ is obtained from

$$N^{-1} \leq |N(\beta_i)| \leq |\beta_i^{(j)}| B_1^{d-1}$$

via

$$|\beta_i^{(j)}| \geq B_1^{1-d} N^{-1} . \tag{28}$$

If $d = n$, i.e. M is a full module in F then we have

$$d(\tilde{M}) = d(M)/|N(\beta)| = d(M)/N ,$$

which does in general not hold for non-full modules. Using this relation we obtain

$$\begin{aligned} B_1 &= \frac{Cd(M)}{N}\left(\frac{\sqrt{n}}{N^{1/n}}\right)^{-(n-1)} \\ &= \frac{Cd(M)}{n^{(n-1)/2}}N^{-1/n} = C_3N^{-1/n}, \end{aligned}$$

which proves the upper bounds $|\beta_i^{(j)}| \leq C_3N^{-1/n}$ and $|N(\beta_i)| \leq C_3^nN^{-1}$. Combining the explicit form for B_1 with (28) we get

$$|\beta_i^{(j)}| \geq (C_3N^{-1/n})^{1-n}N^{-1} = C_3^{1-n}N^{-1/n}.$$

For full modules M we therefore obtain the bounds

$$C_2N^{-1/n} \leq |\beta_i^{(j)}| \leq C_3N^{-1/n}$$

with constants

$$C_3 = \frac{Cd(M)}{n^{(n-1)/2}} \text{ and } C_2 = C_3^{1-n}\ .$$

The bounds given above are rather crude and we can do much better, especially if i is small compared to n.

If necessary we reorder the reduced basis such that the basis vectors satisfy
$\| \beta_1 \| \leq \| \beta_2 \| \leq ... \leq \| \beta_n \|$. Then we obtain for the first basis vector from (25):

$$\| \beta_1 \| \leq \left(Cd(\tilde{M}\right)^{1/n}\ . \tag{29}$$

This is certainly much better than the estimate given above and also yields much better lower and upper bounds for the absolute values of the conjugates of β_1.

Analogously, for $i = 1, .., n$, we make use of (25) and of (26) to obtain
(30)

$$\| \beta_i \| \leq \left(\frac{Cd(\tilde{M})}{\prod_{j=1}^{i-1} \| \beta_j \|}\right)^{1/(n+1-i)} \leq \left(\frac{Cd(\tilde{M})}{(\sqrt{d}N^{-1/d})^{i-1}}\right)^{1/(n+1-i)} =: B_{2i}\ .$$

The bounds B_{2i} are easily seen to be much better than the bounds B_1. The quotients B_{2i}/B_1 are strictly increasing in i with $B_{2i}/B_1 = 1$ exactly for $i = n$. These new bounds immediately yield the better estimates for $|\beta_i^{(j)}|$ stated in Lemma 2.

The following example demonstrates the quality of the new bounds.

Example We choose an example from [11]. Let $F = \mathbb{Q}((-2)^{1/19})$. Let M be the maximal order o_F of F. It has a power integral basis. The discriminant d_F of F is $-19^{19}2^{18}$. Consequently, we have $d(M) = \sqrt{-d_F}$. We arbitrarily choose $N = 100$. This results in

$$B_1 = 9.58182 \cdot 10^{28} .$$

The following table contains the values B_{2i} and B_{2i}/B_1 for i from 1 to 19.

i	1	2	3	4	5
B_{2i}	107.48	130.17	161.25	205.15	269.53
B_{2i}/B_1	$1.12 \cdot 10^{-27}$	$1.36 \cdot 10^{-27}$	$1.68 \cdot 10^{-27}$	$2.14 \cdot 10^{-27}$	$2.81 \cdot 10^{-27}$

i	6	7	8	9	10
B_{2i}	368.19	527.68	803.02	1318.97	2392.47
B_{2i}/B_1	$3.84 \cdot 10^{-27}$	$5.51 \cdot 10^{-27}$	$8.38 \cdot 10^{-27}$	$1.38 \cdot 10^{-26}$	$2.50 \cdot 10^{-26}$

$i0$	11	12	13	14	15
B_{2i}	4953.69	12303.55	39629.50	$1.89 \cdot 10^5$	$1.67 \cdot 10^6$
B_{2i}/B_1	$5.17 \cdot 10^{-26}$	$1.28 \cdot 10^{-25}$	$4.14 \cdot 10^{-25}$	$1.97 \cdot 10^{-24}$	$1.75 \cdot 10^{-23}$

i	16	17	18	19
B_{2i}	$4.43 \cdot 10^7$	$1.04 \cdot 10^{10}$	$5.73 \cdot 10^{14}$	$9.58 \cdot 10^{28}$
B_{2i}/B_1	$4.62 \cdot 10^{-22}$	$1.08 \cdot 10^{-19}$	$5.98 \cdot 10^{-15}$	1

We emphasize that the quotient B_{2i}/B_1 is independent of N.

7. Numerical Examples

We present several illustrative examples for the performance of our algorithms in number fields F up to degree 10. We note that the calculations use floating point numbers which make LLL-reduction much more complicated in general. But using sufficiently good approximations we can always check the LLL-property of the results. The computations were made by using Magma and a database of Jürgen Klüners and Gunter Malle:
http://www.math.uni-duesseldorf.de/∼klueners/groups2.html

First we present a worked-out example regarding the approximation of linear forms. In the calculations we used floating point numbers with the precision of 3000, but for the sake of readability the results will be presented with a much lower precision.

Example Let $\rho = -3.4137$ be the smallest root of the polynomial $P(x) = x^4 - x^3 - 24x^2 - 22x + 29$, set $\alpha_i = \rho^{i-1}, i = 1, 2, 3, 4$ and consider the module $M = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_4$. The transformations matrix to the LLL-reduced basis is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -12 & -3 & 1 & 0 \\ 6 & -17 & -3 & 1 \end{pmatrix}$$

Hence, the reduced basis of M becomes $(1.0000, -3.4137, 9.8940, -10.7063)$. From here on we perform the steps of both Algorithm 1 and Algorithm 2. It turns out that the length of the pre-period in both cases is 1 and the length of the period is 6. In the next tables we use the following notations:

- x: the coefficient vector of β_i in the actual basis.
- β: the numerical value of β_i.
- γ repr.: the coordinates of γ in the original basis for $\gamma = \beta_1 \cdot \beta_2 \cdot \ldots \beta_i$.
- γ: the numerical value of γ.
- $N(\gamma)$: the norm of γ.

Algorithm 1:

Round	x	β	γ repr.	γ	$N(\gamma)$
1	$(-10, 0, 1, 0)$	-0.1060	$(-22, -3, 1, 0)$	$-1.0604 \cdot 10^{-1}$	191
2	$(-2, 0, 0, 1)$	0.1308	$(42, -13, -4, 1)$	$-1.3870 \cdot 10^{-2}$	-441
3	$(11, 0, 1, 0)$	-0.0086	$(370, -402, -71, 23)$	$1.1950 \cdot 10^{-4}$	191
4	$(-2, 0, 0, 1)$	0.1308	$(-1289, 1534, 263, -87)$	$1.5631 \cdot 10^{-5}$	-441
5	$(11, 0, 1, 0)$	-0.0086	$(-20177, 25110, 4274, -1410)$	$-1.3468 \cdot 10^{-7}$	191
6	$(2, 0, 0, 1)$	-0.1308	$(-74427, 92915, 15800, -5216)$	$1.7615 \cdot 10^{-8}$	-441
7	$(-11, 0, 1, 0)$	0.0086	$(1197896, -1497591, -254764, 83998)$	$1.5177 \cdot 10^{-10}$	191
8	$(-2, 0, 0, 1)$	0.1308	$(-4427704, 5536031, 941737, -310506)$	$1.9852 \cdot 10^{-11}$	-441

Algorithm 2:

Round	x	β	γ repr.	γ	$N(\gamma)$
1	$(-24, 1, -1, 1)$	-0.0139	$(42, -13, -4, 1)$	$-1.3870 \cdot 10^{-2}$	-441
2	$(-11, 0, 1, 0)$	0.0086	$(-370, 402, 71, -23)$	$1.1950 \cdot 10^{-4}$	191
3	$(2, 1, -1, 1)$	0.0106	$(-1712, 2136, 363, -120)$	$-1.2700 \cdot 10^{-6}$	1
4	$(-25, 1, 1, 1)$	0.0139	$(74427, -92915, -15800, 5216)$	$-1.7615 \cdot 10^{-8}$	-441
5	$(-11, 0, 1, 0)$	-0.0086	$(1197896, -1497591, -254764, 83998)$	$1.5177 \cdot 10^{-10}$	191
6	$(-2, -1, -1, 1)$	-0.0106	$(-6062683, 7580586, 1289640, -425145)$	$-1.6130 \cdot 10^{-12}$	1
7	$(25, 1, -1, 1)$	-0.0139	$(-263637360, 329643448, 56080993, -18487321)$	$2.2372 \cdot 10^{-14}$	-441
8	$(-11, 0, 1, 0)$	0.0086	$(4246685782, -5309914962, -903367628, 297791327)$	$1.9275 \cdot 10^{-16}$	191

In the next table we give the representation of the reduced bases. If $B = (\rho^0, \rho^1, \rho^2, \rho^3)^T$, and T is one of the transformation matrices from the second column of the next tables, then $T \cdot B$ equals the coordinates of the reduced basis.

Algorithm 1:

Number of steps	Trf. matrix (original→reduced)	Reduced bases
0	$\begin{pmatrix} 1.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 1.000 & 0.0000 & 0.0000 \\ -12.0000 & -3.0000 & 1.0000 & 0.0000 \\ 6.0000 & -17.0000 & -3.0000 & 1.0000 \end{pmatrix}$	$\begin{pmatrix} 1.0000 \\ -3.4137 \\ 9.8940 \\ -10.7063 \end{pmatrix}$
$1 = 7$	$\begin{pmatrix} 1.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.9372 & -0.3037 & -0.1518 & 0.0209 \\ 1.1100 & 1.0314 & 0.0157 & -0.0367 \\ -0.6545 & 1.6702 & 0.3351 & -0.1152 \end{pmatrix}$	$\begin{pmatrix} 1.0000 \\ -0.6286 \\ -0.7700 \\ 2.1308 \end{pmatrix}$
$2 = 8$	$\begin{pmatrix} 0.7143 & -0.8095 & -0.1429 & 0.0476 \\ -0.2857 & -0.8095 & -0.1429 & 0.0476 \\ 0.9524 & -0.1429 & -0.0476 & 0.0000 \\ -1.8571 & -0.5714 & 0.1429 & 0.0000 \end{pmatrix}$	$\begin{pmatrix} -0.0813 \\ -1.0813 \\ 0.8851 \\ 1.7582 \end{pmatrix}$
3	$\begin{pmatrix} 1.0000 & 0.0000 & 0.0000 & 0.0000 \\ -0.9372 & 0.3037 & 0.1518 & -0.0209 \\ -1.1100 & -1.0314 & -0.0157 & 0.0367 \\ -0.6545 & 1.6702 & 0.3351 & -0.1152 \end{pmatrix}$	$\begin{pmatrix} 1.0000 \\ 0.6286 \\ 0.7700 \\ 2.1308 \end{pmatrix}$
4	$\begin{pmatrix} 0.7143 & -0.8095 & -0.1429 & 0.0476 \\ 0.2857 & 0.8095 & 0.1429 & -0.0476 \\ 0.9524 & -0.1429 & -0.0476 & 0.0000 \\ 1.8571 & 0.5714 & -0.1429 & 0.0000 \end{pmatrix}$	$\begin{pmatrix} -0.0813 \\ 1.0813 \\ 0.8851 \\ -1.7582 \end{pmatrix}$
5	$\begin{pmatrix} 1.0000 & 0.0000 & 0.0000 & 0.0000 \\ -0.9372 & 0.3036 & 0.1518 & -0.0209 \\ 1.1100 & 1.0314 & 0.0157 & -0.0367 \\ 0.6545 & -1.6702 & -0.3351 & 0.1152 \end{pmatrix}$	$\begin{pmatrix} 1.0000 \\ 0.6286 \\ -0.7700 \\ -2.1308 \end{pmatrix}$
6	$\begin{pmatrix} 0.7143 & -0.8095 & -0.1429 & 0.0476 \\ 0.2857 & 0.8095 & 0.1429 & -0.0476 \\ -0.9524 & 0.1429 & 0.0476 & 0.0000 \\ -1.8571 & -0.5714 & 0.1429 & 0.0000 \end{pmatrix}$	$\begin{pmatrix} -0.0813 \\ 1.0813 \\ -0.8851 \\ 1.7582 \end{pmatrix}$
7	$\begin{pmatrix} 1.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.9372 & -0.3036 & -0.1518 & 0.0209 \\ 1.1100 & 1.0314 & 0.0157 & -0.0367 \\ -0.6545 & 1.6702 & 0.3351 & -0.1152 \end{pmatrix}$	$\begin{pmatrix} 1.0000 \\ -0.6286 \\ -0.7700 \\ 2.1308 \end{pmatrix}$
8	$\begin{pmatrix} 0.7143 & -0.8095 & -0.1429 & 0.0476 \\ -0.2857 & -0.8095 & -0.1429 & 0.0476 \\ 0.9524 & -0.1429 & -0.0476 & 0.0000 \\ -1.8571 & -0.5714 & 0.1429 & 0.0000 \end{pmatrix}$	$\begin{pmatrix} -0.0813 \\ -1.0813 \\ 0.8851 \\ 1.7582 \end{pmatrix}$

In our last two tables we give some more numerical results for both algorithms. For each polynomial the contents of the first line are results from Algorithm 1 and the contents of the second line are results from Algorithm 2. The detailed results can be viewed at: http://www.inf.unideb.hu/∼pethoe/cikkek/PPB_examples.pdf. We use the following notations:

- Polynomial: the coefficient list of the polynomial, starting with the highest power.
- Deg./Sig.: the degree/signature of the polynomial.
- Discriminant: the discriminant of the polynomial.
- Per., Pre.: the length of the period, and the pre-period.
- γ_{pre+1}: the value of the first γ which is part of the first period.
- $\gamma_{pre+per+1}$: the value of the first γ which is part of the second period.
- γ_{pre+1} coordinates: the coordinates of γ_{pre+1} in the original bases, or if at least one of the coordinates are larger than 10^8, then the value of the largest coordinate with high precision.
- $\gamma_{pre+per+1}$ coordinates: the coordinates of $\gamma_{pre+pre+1}$ in the original bases, or if at least one of the coordinates are larger than 10^8, then the value of the largest coordinate with high precision. If the period length is 1, then we write NA instead.

Polynomial	Deg./Sig.	Discriminant	Per.	Pre.	γ_{pre+1}	$\gamma_{pre+per+1}$
$[1,-1,0,-1]$	3/1	-31	1	0	0.1478990357	NA
			1	0	0.2167565720	NA
$[1,0,0,-2]$	3/1	-108	1	1	-0.01031475882	NA
			1	1	-0.01031475882	NA
$[1,-1,-7,8]$	3/3	733	6	0	-0.03307320014	$1.155078874 \cdot 10^{-8}$
			5	0	-0.03307320014	$3.124881318 \cdot 10^{-9}$
$[1,-1,-10,8]$	3/3	961	12	0	-0.08387235944	$-1.123134695 \cdot 10^{-15}$
			4	0	-0.08387235944	$-3.537628806 \cdot 10^{-5}$
$[1,0,-7,-4]$	3/3	940	4	1	0.005970873050	$1.155348006 \cdot 10^{-8}$
			16	0	-0.1600918016	$-1.159829197 \cdot 10^{-18}$
$[1,0,1,0,-1]$	4/2	-400	4	2	0.0001547484757	$1.771957548 \cdot 10^{-9}$
			1	1	-0.002660232816	NA
$[1,0,2,0,-1]$	4/2	-1024	12	1	0.001850570582	$3.770265157 \cdot 10^{-21}$
			2	4	$-5.554604813 \cdot 10^{-7}$	$-1.856206457 \cdot 10^{-9}$
$[1,-1,-5,2,4]$	4/4	2225	3	0	0.007333768640	$-2.892736132 \cdot 10^{-9}$
			3	2	-0.0006280450653	$3.944406040 \cdot 10^{-7}$
$[1,-1,-8,1,11]$	4/4	5225	4	1	0.01368639756	$-2.563701474 \cdot 10^{-6}$
			4	4	$-5.908036252 \cdot 10^{-9}$	$-6.020523158 \cdot 10^{-16}$
$[1,-1,-24,-22,29]$	4/4	107653	6	1	-0.01387009227	$1.985163973 \cdot 10^{-11}$
			6	1	-0.0001195040098	$1.927547951 \cdot 10^{-16}$

Polynomial	Deg./Sig.	Discriminant	Per.	Pre.	γ_{pre+1}	$\gamma_{pre+per+1}$
$[1,-2,2,-1,0,1]$	5/1	2209	12	3	$3.989638445 \cdot 10^{-5}$	$1.341840753 \cdot 10^{-21}$
			6	7	$-3.404369835 \cdot 10^{-14}$	$-7.944164774 \cdot 10^{-23}$
$[1,0,-1,-2,0,1]$	5/3	−4511	4	1	−0.0009241499083	$-1.875072548 \cdot 10^{-9}$
			5	2	$4.302227915 \cdot 10^{-6}$	$1.760427599 \cdot 10^{-15}$
$[1,-2,1,2,-2,-1]$	5/3	−5783	3	2	$7.759473941 \cdot 10^{-6}$	$-6.020943583 \cdot 10^{-11}$
			2	3	$1.223790015 \cdot 10^{-6}$	$1.353818232 \cdot 10^{-9}$
$[1,-1,-12,21,1,-5]$	5/5	923521	4	2	−0.0001213389130	$-7.288982377 \cdot 10^{-10}$
			12	0	0.01485732945	$1.682649967 \cdot 10^{-23}$
$[1,0,-6,0,5,-1]$	5/5	347317	5	0	0.02155902683	$1.004095262 \cdot 10^{-10}$
			5	0	0.02155902683	$1.004095262 \cdot 10^{-10}$
$[1,0,0,-1,0,0,-1]$	6/2	91125	6	8	$-1.869645053 \cdot 10^{-18}$	$-5.494465810 \cdot 10^{-28}$
			6	5	$1.939097227 \cdot 10^{-15}$	$-5.182320446 \cdot 10^{-30}$
$[1,-1,-1,-2,2,3,-1]$	6/4	−103243	3	3	$-1.951881582 \cdot 10^{-5}$	$1.152081869 \cdot 10^{-8}$
			4	51	$-8.677663447 \cdot 10^{-112}$	$-8.826714968 \cdot 10^{-121}$
$[1,-2,1,-4,3,3,-1]$	6/4	−199283	4	0	−0.05763787641	$-6.361211821 \cdot 10^{-7}$
			3	0	−0.008355381345	$-4.873770833 \cdot 10^{-9}$
$[1,0,-9,0,10,0,-1]$	6/6	7711729	1	0	−0.005525596300	NA
			1	0	−0.005525596300	NA
$[1,0,-6,0,9,0,-3]$	6/6	1259712	6	2	$2.805149578 \cdot 10^{-5}$	$-2.207334097 \cdot 10^{-14}$
			6	2	$-8.632038957 \cdot 10^{-10}$	$6.431913202 \cdot 10^{-28}$
$[1,-1,1,0,3,-1,3,1]$	7/1	−3442951	28	2	$-8.323974297 \cdot 10^{-7}$	$-1.950776012 \cdot 10^{-67}$
			14	2	$2.092963881 \cdot 10^{-11}$	$2.309095421 \cdot 10^{-64}$
$[1,-1,-3,1,4,-1,-1,1]$	7/3	2007889	12	13	$-1.647228687 \cdot 10^{-24}$	$-8.783348064 \cdot 10^{-42}$
			48	4	$-9.491426072 \cdot 10^{-16}$	$-4.397976140 \cdot 10^{-158}$
$[1,0,-3,-1,1,3,1,-1]$	7/5	−2306599	2	2	$-6.406356475 \cdot 10^{-5}$	$-1.483358613 \cdot 10^{-7}$
			8	23	$-3.766491584 \cdot 10^{-73}$	$-1.532005222 \cdot 10^{-103}$
$[1,-1,-7,2,12,0,-5,-1]$	7/7	55078981	6	2	$1.382995230 \cdot 10^{-5}$	$2.645221517 \cdot 10^{-15}$
			20	7	$-3.809798495 \cdot 10^{-21}$	$-8.553208776 \cdot 10^{-68}$
$[1,-3,-3,11,2,-8,0,1]$	7/7	55311169	3	0	0.05342486988	$8.146553091 \cdot 10^{-6}$
			12	0	$7.073085862 \cdot 10^{-5}$	$1.108960536 \cdot 10^{-54}$
$[1,-1,0,1,-2,-1,2,2,-1]$	8/2	−4286875	66	7	$-2.101278837 \cdot 10^{-14}$	$-5.381763601 \cdot 10^{-138}$
			12	3	$-2.371298164 \cdot 10^{-15}$	$-1.355721797 \cdot 10^{-55}$
$[1,-3,-2,9,0,-6,-2,-3,1]$	8/4	56953125	4	9	$-3.385657963 \cdot 10^{-19}$	$-1.982906599 \cdot 10^{-26}$
			16	1	$-1.667068964 \cdot 10^{-10}$	$9.944480428 \cdot 10^{-89}$
$[1,-3,0,2,4,3,-5,-2,1]$	8/6	−74671875	18	3	$9.172490293 \cdot 10^{-7}$	$2.243982075 \cdot 10^{-33}$
			48	3	$1.353104848 \cdot 10^{-16}$	$5.096932119 \cdot 10^{-207}$
$[1,0,-8,0,20,0,-16,0,1]$	8/8	1358954496	8	3	$8.570934720 \cdot 10^{-8}$	$-6.296287668 \cdot 10^{-22}$
			6	5	$2.625876375 \cdot 10^{-26}$	$2.697703239 \cdot 10^{-53}$
$[1,0,-8,0,20,0,-16,0,2]$	8/8	2147483648	3	14	$-5.951895140 \cdot 10^{-24}$	$8.261802401 \cdot 10^{-29}$
			8	3	$-5.856759036 \cdot 10^{-18}$	$-1.228450817 \cdot 10^{-53}$
$[1,0,0,-2,0,0,4,0,0,-2]$	9/1	3840162048	41	63	$-1.818962454 \cdot 10^{-117}$	$-2.961164149 \cdot 10^{-194}$
			45	17	$-5.483831446 \cdot 10^{-108}$	$-2.021298103 \cdot 10^{-380}$
$[1,-5,-1,4,2,3,-1,-3,0,1]$	9/3	−203297472	10	0	0.02475408815	$2.138534516 \cdot 10^{-18}$
			59	63	$-2.611546747 \cdot 10^{-321}$	$-8.096214101 \cdot 10^{-618}$
$[1,-3,3,4,-12,9,1,-9,6,-1]$	9/5	9829532736	32	1	$-1.367859970 \cdot 10^{-5}$	$-9.290267386 \cdot 10^{-93}$
			4	2	$8.707531739 \cdot 10^{-18}$	$1.559870294 \cdot 10^{-40}$
$[1,-2,-5,12,3,-19,7,7,-2,-1]$	9/7	−6221161471	3	7	$-8.536227087 \cdot 10^{-12}$	$-9.992046508 \cdot 10^{-16}$
			20	8	$1.168090160 \cdot 10^{-47}$	$7.442304417 \cdot 10^{-148}$
$[1,-1,-8,7,21,-15,-20,10,5,-1]$	9/9	16983563041	28	5	$-1.204658028 \cdot 10^{-11}$	$-1.920188967 \cdot 10^{-55}$
			12	50	$3.503498943 \cdot 10^{-266}$	$1.023410103 \cdot 10^{-328}$
$[1,0,0,0,0,-2,0,0,0,0,-1]$	10/2	320000000000	18	23	$-1.626833670 \cdot 10^{-46}$	$-5.056542887 \cdot 10^{-87}$
			30	31	$-1.111234100 \cdot 10^{-216}$	$-2.113640737 \cdot 10^{-425}$
$[1,-1,0,4,-2,-2,-1,1,0,-2,1]$	10/4	−91794884831	4	2	$-5.900596788 \cdot 10^{-6}$	$-7.178887031 \cdot 10^{-13}$
			18	12	$-5.992588896 \cdot 10^{-88}$	$3.869937527 \cdot 10^{-206}$
$[1,-3,1,1,-2,4,5,-2,-6,-1,1]$	10/6	23365118029	144	9	$-9.587213264 \cdot 10^{-45}$	$-2.432961495 \cdot 10^{-362}$
			8	1	$-1.042864950 \cdot 10^{-12}$	$-1.233503419 \cdot 10^{-60}$
$[1,0,-6,0,10,0,-1,0,-6,0,1]$	10/8	−219503494144	20	24	$-7.570706443 \cdot 10^{-55}$	$-2.585660777 \cdot 10^{-92}$
			12	21	$-2.523413550 \cdot 10^{-144}$	$-1.006573992 \cdot 10^{-219}$
$[1,-1,-10,10,34,-34,-43,43,12,-12,1]$	10/10	572981288913	10	1	$8.201394073 \cdot 10^{-5}$	$-3.043169065 \cdot 10^{-25}$
			36	97	$4.182998747 \cdot 10^{-641}$	$2.098225847 \cdot 10^{-870}$

Polynomial	γ_{pre+1} coordinates	$\gamma_{pre+per+1}$ coordinates
$[1,-1,0,-1]$	$[-2,0,1]$ $[1,-2,1]$	NA NA
$[1,0,0,-2]$	$[-5,9,-4]$ $[-5,9,-4]$	NA NA
$[1,-1,-7,8]$	$[-10,-1,1]$ $[-10,-1,1]$	$[26402,-2841,-4685]$ $[-124606,4685,18876]$
$[1,-1,-10,8]$	$[3,1,0]$ $[3,1,0]$	-44370512 $[1243,33,-120]$
$[1,0,-7,-4]$	$[26,-7,-8]$ $[-10,-2,1]$	$[-18534,-45607,-16368]$ -122170080922
$[1,0,1,0,-1]$	$[17,-26,15,-12]$ $[4,-7,4,-2]$	$[5101,-6554,3275,-4060]$ NA
$[1,0,2,0,-1]$	$[-4,3,5,0]$ $[88,-7,-199,-4]$	$[-2501077,4992804,-1477474,-376139]$ $[783,-576,-1870,1359]$
$[1,-1,-5,2,4]$	$[5,-2,-1,1]$ $[15,-2,-6,0]$	$[-213,934,-195,-453]$ $[81,-132,4,60]$
$[1,-1,-8,1,11]$	$[4,4,1,0]$ $[644,-905,-312,186]$	$[827,32,-864,-344]$ 11267442
$[1,-1,-24,-22,29]$	$[42,-13,-4,1]$ $[-370,402,71,-23]$	$[-4427704,5536031,941737,-310506]$ -5309914962
$[1,-2,2,-1,0,1]$	$[11,4,-19,13,1]$ $[1939,-983,-3809,5160,-2276]$	$[-1905746,394216,3767480,-3946799,1130929]$ $[-381673,304264,853440,-1161671,461023]$
$[1,0,-1,-2,0,1]$	$[5,-6,-5,3,1]$ $[-35,65,10,-54,19]$	$[127,256,-434,-850,687]$ $[-462549,714348,524419,-1022671,325258]$
$[1,-2,1,2,-2,-1]$	$[6,-18,5,21,-13]$ $[8,21,21,-19,-10]$	$[-36,490,372,-373,-141]$ $[-27,-205,-270,127,163]$
$[1,-1,-12,21,1,-5]$	$[-249,579,-225,-37,19]$ $[-14,10,0,-1,0]$	$[-1110349,2651571,-1144504,-148264,100843]$ $[-6141559,13159446,-6024907,-678767,544202]$
$[1,0,-6,0,5,-1]$	$[-6,0,11,0,-2]$ $[-6,0,11,0,-2]$	$[32440,-13336,-35319,2450,5745]$ $[32440,-13336,-35319,2450,5745]$
$[1,0,0,-1,0,0,-1]$	$[-19635,23726,-29113,14733,-16731,17869]$ $[-2625,-2224,1863,1650,1327,-1131]$	-122626395 -16586541
$[1,-1,-1,-2,2,3,-1]$	$[-21,9,-4,10,-4,1]$ $-3.760862090968621621612587 \cdot 10^{27}$	$[339,-144,-29,-141,49,21]$ $1.781051624046654510181610 \cdot 10^{30}$
$[1,-2,1,-4,3,3,-1]$	$[2,0,-4,0,-1,1]$ $[7,3,-9,1,-3,2]$	$[76,-131,-320,2,-65,81]$ $[-2418,-1357,2607,-282,1157,-686]$
$[1,0,-9,0,10,0,-1]$	$[2,-7,0,1,0,0]$ $[2,-7,0,1,0,0]$	NA NA
$[1,0,-6,0,9,0,-3]$	$[8,12,6,1,0,0]$ $[166,-126,-105,147,21,-27]$	$[-2852,-2754,2358,-4029,-8550,-2907]$ $[-3688156,4845960,2884995,-4498911,-609426,781434]$
$[1,-1,1,0,3,-1,3,1]$	$[-1,-4,-1,1,-4,1,-4]$ $[7,18,-32,-29,-7,-23,11]$	34986375304153 1149571479031
$[1,-1,-3,1,4,-1,-1,1]$	$[-41485,58947,144705,-28924,-113513,-11497,30992]$ $[533,-587,-2344,-95,2153,253,-553]$	440586763891 $1.102489989765776989020537 \cdot 10^{35}$
$[1,0,-3,-1,1,3,1,-1]$	$[-3,-2,6,-2,-7,3,1]$ 100632613641187286	$[-22,9,101,-20,-107,21,20]$ $-3.806667635599136876354076 \cdot 10^{25}$

Polynomial	γ_{pre+1} coordinates	$\gamma_{pre+per+1}$ coordinates
$[1,-1,-7,2,12,0,-5,-1]$	$[9,28,-3,-34,9,9,-3]$ $[12041,12760,-100412,-28895,74372,13214,-11612]$	$[1876,9316,2019,-12895,1345,3342,-874]$ 1188825840485144328047
$[1,-3,-3,11,2,-8,0,1]$	$[1,-7,2,11,-3,-3,1]$ $[13,3,-19,-12,10,4,-2]$	$[72,-189,-65,307,-43,-88,26]$ -32277024086450
$[1,-1,0,1,-2,-1,2,2,-1]$	$[-71,49,248,226,-49,5,74,-39]$ $[3,26,-32,-166,66,38,-33,65]$	$13706184263793962217370 0$ -1439528345
$[1,-3,-2,9,0,-6,-2,-3,1]$	$[21295,-57883,-118132,65325,95163,-42382,-24275,9941]$ $[-11,26,82,-46,-97,46,31,-13]$	-21788644 79767903836100705
$[1,-3,0,2,4,3,-5,-2,1]$	$[6,-25,12,17,17,12,-20,4]$ $[34,-537,1140,578,388,-243,-473,187]$	-75808490 $-2.017374966651652746587669 \cdot 10^{39}$
$[1,0,-8,0,20,0,-16,0,1]$	$[16,32,24,8,1,0,0,0]$ $[-11899,10993,186108,-171091,-128269,122281,20562,-20324]$	$[5980,-22624,-228528,-143848,70449,-62720,-134320,-40480]$ 46663166453
$[1,0,-8,0,20,0,-16,0,2]$	26616203 $[-7027,17647,11200,-25490,-5031,10605,667,-1348]$	1168468969 -31535162636746
$[1,0,0,-2,0,0,4,0,0,-2]$	657367096199957009499 -25495877647230	$-1.007553881434116028428424 \cdot 10^{35}$ $-6.844528020161353581312741 \cdot 10^{50}$
$[1,-5,-1,4,2,3,-1,-3,0,1]$	$[-1,2,3,-8,1,-4,-4,11,-2]$ $-1.528968471201757795897652 \cdot 10^{51}$	$[138167,736045,-2567689,1595444,361523,-194776,2649709,$ $-2997512,492554]$ $-4.942000499296591884530495 \cdot 10^{97}$
$[1,-3,3,4,-12,9,1,-9,6,-1]$	$[-88,255,-100,-161,330,-158,-64,85,-33]$ $[-275,1425,-756,-407,1650,-1101,-217,459,-198]$	$4066992114509623140869 2$ $[-1026497,4593321,-2166819,-2272107,5508362,-2959461,-1265808,$ $1438346,-418044]$
$[1,-2,-5,12,3,-19,7,7,-2,-1]$	$[447,-518,-3081,5228,761,-3902,699,680,-188]$ 593948596	$[-33984,51485,244968,-464787,-54775,342732,-61168,-59417,16058]$ $2.449803338384091414109826 \cdot 10^{29}$
$[1,-1,-8,7,21,-15,-20,10,5,-1]$	$[-62,421,-58,-655,305,330,-206,-51,35]$ $8.837137313149988272030788 \cdot 10^{36}$	-6675180932632324543 $-2.231841083474719943587546 \cdot 10^{48}$
$[1,0,0,0,0,-2,0,0,0,0,-1]$	$[-71680,78309,-86079,77942,-62148,-103553,59884,-5809,$ $-94024,118075]$ $-6.733541459691716998343494 \cdot 10^{25}$	-106481642097342 $5.321103441924805906151133 \cdot 10^{53}$
$[1,-1,0,4,-2,-2,-1,1,0,-2,1]$	$[-1,-4,-16,3,-3,-11,21,1,-4,5]$ -285353508217	$[-269,739,-475,-855,1691,-154,-845,361,13,-122]$ $-1.151733509425989597322430 \cdot 10^{27}$
$[1,-3,1,1,-2,4,5,-2,-6,-1,1]$	99240069 $[-5,19,-24,41,-15,7,-35,38,-27,7]$	$-5.403602864408824548030169 \cdot 10^{76}$ 54390697181
$[1,0,-6,0,10,0,-1,0,-6,0,1]$	-3177225612 -1706060737252341015	553617849365239263 $1.637037835043587312564276 \cdot 10^{28}$
$[1,-1,-10,10,34,-34,-43,43,12,-12,1]$	$[4,4,1,0,0,0,0,0,0,0]$ $-5.630520512455940668061489 \cdot 10^{82}$	$[-3797,-28139,-64295,-99495,-138490,-112574,-49863,-21538,$ $-10626,-2299]$ $-3.665318989712510095619541 \cdot 10^{112}$

References

[1] L. Bernstein, *The Jacobi-Perron Algorithm Its Theory and Application*, Lecture Notes in Mathematics, **207**, Springer Verlag, Berlin, Heidelberg, New York, 1971.

[2] W. Bosma and I. Smeets, *Finding simultaneous Diophantine approximations with prescribed quality*, ANTS X - Proceedings of the Tenth Algorithmic Number Theory Symposium, 167–185, Open Book Ser., 1, Math. Sci. Publ., Berkeley, CA, 2013.

[3] J.Buchmann and A.Pethő, *On the computation of independent units in number fields by Dirichlet's method*, Math. Comp. **52** (1989), 149–159.

[4] G. Lejeune Dirichlet, *Zur Theorie der complexen Einheiten*, Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften, 1846, 103–107.

[5] A. Khintchine, *Zwei Bemerkungen zu einer Arbeit des Herrn Perron*, Math. Annalen **83** (1921), 77–84.

[6] J.L. Lagrange, *Additions au Mémoire sur la résolution des équations numériques*, Œvres, Tome Deuxième, Gauthier-Villars, Paris, 1868, 581–652.
[7] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Annalen **261** (1982), 515–534.
[8] H. Minkowski, *Ein Kriterium für die algebraischen Zahlen*, Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, math.-phys. Klasse, 1899, 64–88.
[9] H. Minkowski, *Über periodische Approximationen algebraischer Zahlen*, Acta. mathematica, **26** (1902), 333–337.
[10] O. Perron, Über Diophantische Approximationen, Math. Annalen **83** (1921), 77–84.
[11] M. Pohst, *On computing fundamental units*, J. Number Theory **47** (1994), 93–105.
[12] J.M. Pollard, *A Monte-Carlo method for factorization*, BIT **15** (1975), 331–334.
[13] H. P. Schlickewei, *On Norm Form Equations*, J. Number Theory **9** (1977), 370–380.
[14] W.M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics, **785** Springer, Berlin, 1980.

Attila Pethő
University of Debrecen, Department of Computer Science
H–4010 Debrecen P.O. Box 12, Hungary
University of Ostrava, Faculty of Science
Dvořákova 7, 70103 Ostrava, Czech Republik
email: petho.attila@inf.unideb.hu

Michael E. Pohst
Technische Universtät Berlin, Institut für Mathematik
Straße des 17. Juni 136, 10623 Berlin, Germany
email: pohst@math.tu-berlin.de

Csanád Bertók
University of Debrecen, Institute of Mathematics
H–4010 Debrecen P.O. Box 12, Hungary
email: bertok.csanad@science.unideb.hu