Generalizing the Continued Fraction Algorithm to Arbitrary Dimensions

Bettina Just
FB Math. Univ. Frankfurt
Robert-Mayer-Str. 6-10, 6 Frankfurt/Main, West- Germany

Abstract

We present for the first time a higher dimensional continued fraction algorithm (abbreviated cfa), that produces diophantine approximations of more than linear goodness. On input $x_1, \cdots, x_{n-1} \in \mathbf{R}$, it produces vectors $(p_1^{(k)}, \ldots, p_{n-1}^{(k)}, q^{(k)}) \in \mathbf{Z}^n$, $k = 1, 2, \ldots$, such that

$$\max_{1 \leq i \leq n} |x_i - \frac{p_i^{(k)}}{q^{(k)}}| \leq \frac{\|x\| \cdot \mathrm{const}(n)}{|q^{(k)}|^{1+\frac{1}{2n(n-1)}}} \quad .$$

By a theorem of Dirichlet, there is no algorithm that replaces the term $\frac{1}{2n(n-1)}$ by a term bigger than $\frac{1}{n-1}$. The higher dimensional cfas analyzed so far do not achieve better than $\max_{1 \leq i \leq n} |x_i - \frac{p_i^{(k)}}{q^{(k)}}| \leq \frac{o(1)}{|q^{(k)}|}$. The $o(1)$ term decreases with k, but is not known to be related with $q^{(k)}$.

Other properties of the cfa are generalized by our algorithm, too. On input $x_1, \cdots, x_{n-1}$ it starts with the standard basis of $\mathbf{Z}^n$ and then constructs by performing elementary basis transformations a sequence $(\mathcal{B}^{(k)})_k$ of bases of $\mathbf{Z}^n$. The sequence $(\mathcal{B}^{(k)})_k$ is finite iff the numbers $x_1, \cdots, x_{n-1}, 1$ are $\mathbf{Z}$- linearly dependent; a linear dependence is found in case of existence. The maximal distance between the vectors of $\mathcal{B}^{(k)}$ and the straightline $(x_1, \cdots, x_{n-1}, 1)\,\mathbf{R}$ tends to zero exponentially fast in k. For each k, the above mentioned vector $(p_1^{(k)}, \ldots, p_{n-1}^{(k)}, q^{(k)})$ is the first vector of basis $\mathcal{B}^{(k)}$.

1 Introduction

The *continued fraction algorithm* (abbreviated cfa) is one of the fundamental mathematical algorithms. Its underlying computational model is the unit cost model, that is, one step is either an arithmetic operation +, -, *, /, or a trunc $\lfloor . \rfloor$ to the next lower integer, or a comparison $\geq$ among real numbers. The cfa accepts as input one arbitrary real number x_1, and outputs a sequence of bases of $\mathbf{Z}^2$ with several nice properties (see below).

In 1868 Jacobi [7] considered generalisations of the cfa. An *n-dimensional cfa* accepts as input real numbers $x_1, \cdots, x_{n-1}$ and outputs a sequence of bases of $\mathbf{Z}^n$. It obtains each basis from the previous one by performing a sequence of elementary basis transformations. (Remark: A *basis* of $\mathbf{Z}^n$, $n \geq 1$, is an ordered set $\{b_1, \cdots, b_n\} \subset \mathbf{Z}^n$ such that $\sum b_i \mathbf{Z} = \mathbf{Z}^n$. An *elementary basis transformation* transforms one basis of $\mathbf{Z}^n$ to another one by either interchanging two basisvectors, or by adding an integer multiple of one basis vector to another basis vector.)

One desires that the following four properties of the cfa carry over to higher dimensions.

Ideal convergence: If the sequence $(\{b_1^{(k)}, \cdots, b_n^{(k)}\})_k$ of bases of $\mathbf{Z}^n$ produced is infinite, then it should fulfill

$$\max_{1 \leq i \leq n} \mathrm{dist}(b_i^{(k)}, x\,\mathbf{R}) \to_k 0 \ .$$

Here and in the sequal we use the notation $x := (x_1, \ldots, x_{n-1}, 1)$.

Integer relations: The algorithm should detect integer relations for x, if they exist. An *integer relation* is a vector $(m_1, \ldots, m_n) \in \mathbf{Z}^n \setminus \{0\}$ such that $\sum_{i=1}^{n-1} m_i x_i + m_n = 0$.

Diophantine Approximations: Vectors $b = (p_1, \cdots, p_{n-1}, q) \in \mathbf{Z}^n$ such that $\max_{1 \leq i \leq n-1} |x_i - \frac{p_i}{q}|$ is "small" are called *(simultaneous) diophantine approximations* for $x_1, \cdots, x_{n-1}$. For arbitrary given denominator q one can find trivially nominators $p_1, ... v_{n-1}$, such that $\max_{1 \leq i \leq n-1} |x_i - \frac{p_i}{q}| \leq \frac{1}{2|q|}$ holds. The following is a theorem of Dirichlet:

> "For arbitrary $x_1, \cdots, x_{n-1} \in \mathbf{R}$ there exist infinitely many $(p_1, \ldots, p_{n-1}, q) \in \mathbf{Z}^n$ such that $\max_{1 \leq i \leq n-1} |x_i - \frac{p_i}{q}| \leq \frac{1}{|q|^{1+\frac{1}{n-1}}}$".

The bound is sharp in the sense, that the right side of the inequation cannot be replaced by $\frac{c}{|q|^s}$, where $s > 1 + \frac{1}{n-1}$ and c and s are constants [3].
For arbitrary dimensions it is not known, whether there exist entire bases of diophantine approximations fulfilling the Dirichlet-bound (ore some other nontrivial bound). But one desires, that some of the basisvectors are "good" (in some sense) diophantine approximations for the input numbers.

Periodicity: Periodicity was often demanded, but up to now no higher dimensional cfa (including the one presented here) achieved it. So a reference to the literature may suffice: [2].

Since Jacobi's paper, higher dimensional cfas where proposed by Poincare, Minkowski, Perron, Brun, Szekeres and others ([13,10,12,4,15]). However, none of these algorithms is proven to fulfill one of the four poperties above. Only results for specific inputs are known.

In several papers since 1979, Bergman, Ferguson and Forcade ([5,1]) presented variations of an algorithm for the integer relation problem. It was analyzed by Hastad, Just, Lagarias and Schnorr [6]. The algorithm is ideally convergent. Therefore it produces diophantine approximations $(p_1^{(k)}, \ldots, p_{n-1}^{(k)}, q^{(k)})$ such that $\max_{1 \leq i \leq n} |x_i - \frac{p_i^{(k)}}{q^{(k)}}| \leq \frac{o(1)}{|q^{(k)}|}$, where the $o(1)$-term decreases with k (cf. claim (24) of this paper). However, it is not known how the term is related to $q^{(k)}$.

CH2806-8/89/0000/0320/$01.00 © 1989 IEEE

The.present paper for the first time presents a higher dimensional continued fraction algorithm that produces approximations with

$$\max_{1\leq i\leq n} |x_i - \frac{p_i^{(k)}}{q^{(k)}}| \leq \frac{1}{|q^{(k)}|^{1+O(1)}} \quad .$$

The algorithm is also ideally convergent and detects integer relations. It is presented in section 2, where its performance is stated as a theorem. The theorem is proven in section 3.

2 The algorithm

For each $b \in \mathbf{R}^n$, we denote by πb the projection of b to the orthogonal complement of x. Hence the euclidean length $\|\pi b\|$ of πb is the distance between b and the straightline $x\,\mathbf{R}$. For any basis $\{b_1, \ldots, b_n\}$ of $\mathbf{Z}^n$, we denote by b_i^* the projection of b_i to the orthogonal complement of the linear space spanned by $x, b_1, \ldots, b_{i-1}$. If $b_n^* \neq 0$, then the vector c_n defined by $[c_1, \ldots, c_n] := ([b_1, \ldots, b_n]^t)^{-1}$ is an integer relation for x ([6]), so from now on we assume $b_n^* = 0$ for the bases occuring. For $i \in \{1, \ldots, n\}$, we denote by $\mu_{i,j}$ the coordinates of b_i with respect to $x, b_1^*, \ldots, b_{n-1}^*$, thus

(1) $\quad b_i = \mu_{i,0} \cdot x + b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} \cdot b_j^* \quad ,$

(2) $\quad \|\pi b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} |\mu_{i,j}|^2 \cdot \|b_j^*\|^2 \quad .$

Our aim is to decrease the $|\mu_{i,j}|$ and the $\|b_i^*\|$ for $1 \leq j < i \leq n$. To this end, size reduction steps and exchange steps are performed. Both transform one basis of $\mathbf{Z}^n$ to another one.

A *size reduction step* replaces b_i by $b_i - \lceil \mu_{i,j} \rfloor \cdot b_j$ for one pair (i, j) with $1 \leq j < i \leq n$. Here $\lceil . \rfloor$ denotes the nearest integer. This achieves $|\mu_{i,j}^{new}| \leq 1/2$. All b_i^* and all μs except the $\mu_{i,l}$ with $l \leq j$ are unchanged. The performance of size reduction steps in a nested loop for all $i = 1$ to n and for all $j = i - 1$ downto 1 achieves $|\mu_{i,j}| \leq 1/2$ for all $1 \leq j < i \leq n$.

An *exchange step* $i \leftrightarrow i+1$ (for $1 \leq i \leq n - 1$) is allowed only if $\|b_i^*\|^2 \geq 2 \cdot \|b_{i+1}^*\|^2$. It firstly performs – if $|\mu_{i+1,i}| > 1/2$ – a size reduction step to achieve $|\mu_{i+1,i}| \leq 1/2$. Then it interchanges b_i and b_{i+1}. This changes b_i^*, b_{i+1}^* and the $\mu_{r,l}$ with $\{r, l\} \cap \{i, i+1\} \neq \emptyset$. The exchange step decreases $\|b_i^*\|^2$ by at least a factor $\sqrt{3}/2$, and increases $\|b_{i+1}^*\|^2$ by the same factor. However, $\max_{1\leq j\leq n} \|b_j^*\|$ is not increased ([9,6]).

The Bergman Ferguson Forcade algorithm and the algorithm to be presented here both perform size reduction and exchange steps, but differ in where these steps are performed.

```
Higherdimensional cfa $(x_1, \cdots, x_{n-1})$;

Step 1 (initialisation):
    $x := (x_1, \cdots, x_{n-1}, 1)$;
    for $i \in \{1, \cdots, n\}$ let $b_i$ be the i-the unit vector;
    for all $1 \leq j \leq i \leq n$ compute $b_i^*$ and $\mu_{i,j}$;
Step 2 (exchange steps of the first basis vectors):
    while $\exists i < n - 1$ such that $\|b_i^*\|^2 \geq 2 \cdot \|b_{i+1}^*\|^2$ do
        i.) $b_{i+1} := b_{i+1} - \lceil \mu_{i+1,i} \rfloor \cdot b_i$ ;
        ii.) interchange $b_i$ and $b_{i+1}$;
        iii.) update $b_i^*$, $b_{i+1}^*$ and the $\mu$s;
Step 3 (size reduction):
    for $i = 2$ to $n$ do
        for $j = i - 1$ downto 1 do
            i.) $b_i := b_i - \lceil \mu_{i,j} \rfloor \cdot b_j$;
            ii.) update $\mu$s;
    output $\mathcal{B}^{(k)} := \{b_1, \cdots, b_n\}$;
Step 4 (exchange step $n - 1 \leftrightarrow n$):
    interchange $b_{n-1}$ and $b_n$;
    update $\mu$s and $b_{n-1}^*$, $b_n^*$;
    if $b_n^* \neq 0$
      then    $[c_1, \cdots, c_n] := ([b_1, \cdots, b_n]^{-1})^t$;
          output integer relation $c_n$ for x;
      else goto 2.                                              □
```

Theorem: On input $x_1, \cdots, x_{n-1} \in \mathbf{R}$ the algorithm starts with the standard basis of $\mathbf{Z}^n$ and performs a sequence of elementary basis transformations. It outputs a subsequence $(\mathcal{B}^{(k)})_k$ of the obtained bases.

a.) If the numbers $x_1, \cdots, x_{n-1}, 1$ are $\mathbf{Z}$-linearly independent, the sequence $(\mathcal{B}^{(k)})_k$ is infinite. Otherwise the algorithm stops after finitely many steps and outputs an integer relation c_n for x.

b.) If $\delta := \text{dist}(x\,\mathbf{R}, b_1^{(k)})$, then the basis $\mathcal{B}^{(k)}$ is obtained after at most $O(n^4(n + \log 1/\delta))$ elementary basis transformations. Moreover, each basis $\mathcal{B}^{(k)}$ fulfills

$$\max_{1\leq i\leq n} \text{dist}(x\,\mathbf{R}, b_i^{(k)}) \leq \sqrt{n-1} \cdot 2^{-(k-1)/(n-1)}$$

c.) The first basis vector $b_1^{(k)} := (p_1, \ldots, p_{n-1}, q)$ of each basis $\mathcal{B}^{(k)}$ fulfills $\max_{1\leq i\leq n-1} |x_i - \frac{p_i}{q}| \leq \frac{\|x\| \cdot 2^{(n+2)/4}}{|q|^{1+\frac{1}{2n(n-1)}}}$. □

3 Analysis of the algorithm

The purpose of this section is to proof the theorem of the last section. Parts a and b are proven with methods similair to those used in [6], and we omit the proofs in this extended abstract. The proof of part c is the main contribution of this paper. We use

(3) $\quad \max_{1\leq i\leq n-1} |x_i - \frac{p_i}{q}| \leq \frac{\|b_1^{(k)*}\| \cdot \|x\|}{|q|} \quad .$

This claim holds, since for each $i \in \{1, \ldots, n\}$

(4) $\frac{(p_i - x_i q)^2}{x_i^2+1} = \|(p_i, q) - \frac{<(x_i,1),(p_i,q)>}{x_i^2+1} \cdot (x_i, 1)\|^2$
$\quad = \text{dist}((p_i, q), (x_i, 1))\,\mathbf{R}^2 \leq \|b_1^{(k)*}\| \quad .$

Part c now follows from Proposition 3.

Proposition 3: The first vector $b_1^{(k)}$ of each outputbasis of the generalized cfa fulfills

(5) $\quad \|b_1^{(k)}\| \leq 2^{n+1} \cdot 2^{n(n-1)(n-2)/2} \cdot \|b_1^{(k)*}\|^{-2n(n-1)} \quad .$ □

The proof of Proposition 3 will fill the rest of this section. We have to bound $\|b_1^{(k)}\|^2 = \|b_1^{(k)*}\|^2 + |\mu_{1,0}^{(k)}|^2 \cdot \|x\|^2$ in terms of $\|b_1^{(k)*}\|$. We outline how to bound $|\mu_{1,0}^{(k)}| \cdot \|x\|$, the length of the component of $b_1^{(k)}$ parallel to $x\,\mathbf{R}$.

We shall bound $\mu^{(k)} := \max_{1\le i\le n} |\mu_{i,0}^{(k)}| \cdot \|x\|$. This will be done by induction on k, the number of exchange steps $n-1 \leftrightarrow n$. The induction will bound simultaneously $\mu^{(k)}$and $\nabla^{(k)}$, the norm of a linear map $f_{\mathcal{B}^{(k)}} : x\,\mathbf{R}^\perp \to \mathbf{R}$.

For any basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ of the algorithm (not only output bases) we define $f_\mathcal{B} : x\,\mathbf{R}^\perp \to \mathbf{R}$ by defining $f_\mathcal{B}(\pi b_i) := \mu_{i,0} \cdot \|x\|$ for $1 \le i \le n-1$. The map $f_\mathcal{B}$ only depends on $\ll b_1, \ldots, b_{n-1} \gg$; we have

$$\left\{ y + f_\mathcal{B}(y) \cdot \frac{x}{\|x\|} : y \in x\,\mathbf{R}^\perp \right\} = \ll b_1, \ldots, b_{n-1} \gg \quad .$$

For $b \in \ll b_1, \ldots, b_{n-1} \gg$ the length of the component of b parallel to $x\,\mathbf{R}$ is $\|f_\mathcal{B}(\pi b)\|$. The length of this component is bounded by $\|\pi b\| \cdot \nabla$, where ∇ is the norm of $f_\mathcal{B}$.

The exchange steps $n-1 \leftrightarrow n$ performed by our algorithm interchange b_{n-1} and b_n without size reduction. Hence they do not change $\mu := \max_{1\le i\le n} |\mu_{i,0}| \cdot \|x\|$. All the other basis transformations performed by the algorithm do not change $\ll b_1, \ldots, b_{n-1} \gg$, hence they leave $f_\mathcal{B}$ and thus ∇ unchanged. These observations will enable us to bound by "parallel induction" $\mu^{(k)}$and $\nabla^{(k)}$, the values of μ and ∇ for the bases $\mathcal{B}^{(k)}$(Lemma 4).

We now present the above sketched proof more completely and firstly recall what is the norm of a linear map. Let $E \subseteq \mathbf{R}^n$ be a linear subspace, and $f : E \to \mathbf{R}$ a linear map. Then the norm $\|f\|$ of f is defined by $\|f\| := \sup_{y\in E, \|y\|=1} |f(y)|$. If $\{o_1, \ldots, o_r\}$ is an orthonormal basis of E such that $f(o_i) = \tau_i$ for all $i \in \{1, \ldots, r\}$, then by Riesz' lemma ([14], p. 43) we know $\|f\| = \|(\tau_1, \ldots, \tau_r)\|$. The vector $(\tau_1, \ldots, \tau_r)$ is called the *representing vector* of f with respect to $\{o_1, \ldots, o_r\}$.

Now we turn to the above mentioned maps $f_\mathcal{B}$: Every basis $\mathcal{B}^{(k)}$output by our algorithm fulfills $b_n^* = 0$, since otherwise the algorithm had stopped previously. As the reader may verify, the representing vector of $f_\mathcal{B}$ with respect to $\left\{ \frac{b_1^*}{\|b_1^*\|}, \ldots, \frac{b_{n-1}^*}{\|b_{n-1}^*\|} \right\}$ is $V \cdot N^t \cdot D$, where $V = \|x\| \cdot (\mu_{1,0}, \ldots, \mu_{n-1,0})$, $D = (\delta_{ij}/\|b_i^*\|)_{1\le i,j\le n-1}$ and $N = \left((\mu_{i,j})_{1\le i,j\le n-1} \right)^{-1}$. Here δ_{ij} is the Kronecker delta. This implies

(6) $\|f_\mathcal{B}\| = \|V \cdot N^t \cdot D\|$.

The output basis $\mathcal{B}^{(k)}$is the basis $\mathcal{B}$efore the k-th exchange step $n-1 \leftrightarrow n$, and we denote by $\mathcal{A}^{(k)} = \{a_1^{(k)}, \ldots, a_n^{(k)}\}$ the basis of the algorithm $\mathcal{A}$fter the k-th exchange step $n-1 \leftrightarrow n$, so $\mathcal{A}^{(k)} = \{b_1^{(k)}, \ldots, b_{n-2}^{(k)}, b_n^{(k)}, b_{n-1}^{(k)}\}$ for $k \ge 1$. By $\mathcal{A}^{(0)}$ we denote the standard basis consisting of the unit vectors $e_1, \ldots, e_n$.

Then the value of μ is the same for $\mathcal{B}^{(k)}$and $\mathcal{A}^{(k)}$. Moreover, the maps $f_{\mathcal{A}^{(k-1)}}$ and $f_{\mathcal{B}^{(k)}}$ and thus their norms are equal. We shall bound $\mu^{(k)}$by looking at $\mathcal{B}^{(k)}$and $\nabla^{(k)}$by looking at $f_{\mathcal{A}^{(k-1)}}$.

Lemma 4: The following inequalities hold:

(7) $\nabla^{(1)} \le \prod_{i=1}^{n-1} \|e_i^*\|^{-1}$;

(8) $\mu^{(1)} \le (n+1) \cdot \prod_{i=1}^{n-1} \|e_i^*\|^{-1}$;

(9) $\nabla^{(k)} \le \nabla^{(k-1)} + \frac{1}{\|a_{n-1}^{(k-1)*}\|} \cdot (n-1)^{1/2} \cdot (1.5)^{n-2} \cdot \mu^{(k-1)}$ for all $k \ge 2$;

(10) $\mu^{(k)} \le \mu^{(k-1)} + \nabla^{(k)} \cdot 2^{n-1} \cdot \|b_{n-1}^{(k-1)*}\|$ for all $k \ge 2$. □

Proof of (7): For all $y \in x\,\mathbf{R}^\perp$ we have $f_{\mathcal{A}^{(0)}} \cdot \frac{x}{\|x\|} + y \in \ll e_1, \ldots, e_{n-1} \gg$, hence $f_{\mathcal{A}^{(0)}} \cdot \frac{e_n}{\|x\|} + y \in \ll e_1, \ldots, e_{n-1} \gg$. This implies $\|y\| \ge \|f_{\mathcal{A}^{(0)}}(y) \cdot e_n\| = \frac{|f_{\mathcal{A}^{(0)}}(y)|}{\|x\|}$, so we proved $\nabla^{(1)} \le \|x\|$. The claim follows from $1 = \det(L(x, e_1, \ldots, e_{n-1})) = \|x\| \cdot \prod_{i=1}^{n-1} \|e_i^*\|$.

Proof of (8): Since $\{\pi b_1^{(1)}, \ldots, \pi b_n^{(1)}\}$ is size reduced, we have $\|\pi b_j^{(1)}\| \le (n-1)^{1/2}$ for all $j \in \{1, \ldots, n\}$. Since $b_j^{(1)} \in \ll e_1, \ldots, e_{n-1} \gg$ for these j, this implies

$$\textbf{(11)} \qquad \begin{aligned} \max_{1\le i\le n-1} |\mu_{j,0}^{(1)}| \cdot \|x\| &\le \|\pi b_j^{(1)}\| \cdot \nabla^{(1)} \\ &\overset{(7)}{\le} (n-1)^{1/2} \cdot \prod_{i=1}^{n-1} \|e_i^*\|^{-1}. \end{aligned}$$

It remains to bound $|\mu_{n,0}^{(1)}| \cdot \|x\|$.

We have $b_n^{(1)} = e_n + v$ for some $v \in \ll e_1, \ldots, e_{n-1} \gg$. The bounds $\|\pi b_n^{(1)}\| \le (n-1)^{1/2}$ and $\|\pi e_n\| \le 1$ imply $\|\pi v\| \le 1 + (n-1)^{1/2}$, and thus $|< v, \frac{x}{\|x\|} >| \le (1 + (n-1)^{1/2}) \cdot \nabla^{(0)}$. So we have

$$\textbf{(12)} \qquad \begin{aligned} |\mu_{n,0}^{(1)}| \cdot \|x\| &\le |< e_n, \tfrac{x}{\|x\|} >| + |< v, \tfrac{x}{\|x\|} >| \\ &\le 1 + (1 + (n-1)^{1/2}) \cdot \nabla^{(0)} \\ &\le (n+1)^{1/2} \cdot \prod_{i=1}^{n-1} \|e_i^*\|^{-1} \quad . \end{aligned}$$

Claim (8) follows from (11) and (12).

Proof of (9): Let $g = (g_1, \ldots, g_{n-1})$ be the representing vector of $f_{\mathcal{B}^{(k-1)}}$ with resprect to $\left\{ \frac{b_1^{(k-1)*}}{\|b_1^{(k-1)*}\|}, \ldots, \frac{b_{n-1}^{(k-1)*}}{\|b_{n-1}^{(k-1)*}\|} \right\}$ and $\hat{g} = (\hat{g}_1, \ldots, \hat{g}_{n-1})$ the representing vector of $f_{\mathcal{A}^{(k-1)}}$ with respect to $\left\{ \frac{a_1^{(k-1)*}}{\|a_1^{(k-1)*}\|}, \ldots, \frac{a_{n-1}^{(k-1)*}}{\|a_{n-1}^{(k-1)*}\|} \right\}$. Then $\nabla^{(k-1)} = \|g\|$ and $\nabla^{(k)} = \|\hat{g}\|$. We have $g = v \cdot N^t \cdot D$ and $\hat{g} = \hat{V} \cdot \hat{N}^t \cdot \hat{d}$, with the following notations:

$V = \|x\| \cdot (\mu_{1,0}^{(k-1)}, \ldots, \mu_{n-1,0}^{(k-1)})$;

$\hat{V} = \|x\| \cdot (\mu_{1,0}^{(k-1)}, \ldots, \mu_{n-2,0}^{(k-1)}, \mu_{n,0}^{(k-1)})$;

$N = \left((\mu_{i,j}^{(k-1)})_{1\le i,j\le n-1} \right)^{-1}$;

$\hat{N} = \left((\hat{\mu}_{i,j}^{(k-1)})_{1\le i,j\le n-1} \right)^{-1}$ where

$$\hat{\mu}_{i,j} = \begin{cases} \mu_{i,j}, & \text{if } i \ne n-1 \\ \mu_{n,j}, & \text{if } i = n-1 \end{cases} ;$$

$D = (d_{i,j})_{1\le i,j\le n-1} = (\delta_{ij}/\|b_i^{(k-1)*}\|)_{1\le i,j\le n-1}$;

$\hat{D} = (\hat{d}_{i,j})_{1\le i,j\le n-1}$ where

$$\hat{d}_{i,j} = \begin{cases} d_{i,j} & , \text{if } i \ne n-1 \\ \delta_{n-1,j}/\|a_{n-1}^{(k-1)*}\|, & \text{if } i = n-1 \end{cases} .$$

Since $g_i = \hat{g}_i$ for all $i \in \{1, \ldots, n-2\}$, we have

(13) $\|(\hat{g}_1, \ldots, \hat{g}_{n-2})\| \le \|g\| \le \nabla^{(k-1)}$.

Since all $\hat{\mu}_{i,j}$ are of absolute value at most 1/2, each entry of the matrix $\hat{N}$ is of absolute value at most $(1.5)^{n-2}$. With this observation one checks

(14) $|\hat{g}_{n-1}| \leq \frac{1}{\|a_{n-1}^{(k-1)*}\|} \cdot (n-1)^{1/2} \cdot (1.5)^{n-2} \cdot \mu^{(k-1)}$.

Since $\nabla^{(k)} = \|\hat{g}\|$, the inequalities (13) and (14) yield the desired bound.

Proof of (10): The bound is proven similair to bound (8). One bounds separately $\max_{1\leq j\leq n-1} \|x\| \cdot |\mu_{j,0}|$ and $\|x\| \cdot |\mu_{n,0}|$. Inequalities (15) and (16) are used.

(15) $\|\pi b_l^{(k)}\|^2 \leq 2^{n-1} \cdot \|b_{n-1}^{(k)*}\|^2$ for all $l \in \{1, \ldots, n\}$ and $k \geq 1$.

(16) $\|b_{n-1}^{(k)*}\|^2 \leq 2^{n-2} \cdot \|b_{n-1}^{(k-1)*}\|^2$ for all $k \geq 2$.

Inequality (15) holds, since $2^{n-1}\|b_{n-1}^{(k)*}\|^2 = \max_{1\leq i\leq n} 2^i \|b_i^{(k)*}\|^2$ and since $\{\pi b_1^{(k)}, \ldots, \pi b_n^{(k)}\}$ is size reduced. Inequality (16) holds by virtue of
$\|b_{n-1}^{(k)*}\|^2 \leq \max_{1\leq i\leq n} \|b_i^{(k)*}\|^2 \leq 2^{n-2}\|b_{n-1}^{(k-1)*}\|^2$.
We do not go to further details here. □

Lemma 5 turns the bounds of Lemma 4 into non-inductive bounds. The proof is an induction on k, and is not carried out here. We only mention that claim (17) — with the notation $\|b_{n-1}^{(0)*}\| := 1$ — is used.

$$\textbf{(17)} \qquad \frac{\|a_{n-1}^{(k-1)*}\|}{\|b_{n-1}^{(k-2)*}\|} = \frac{\|a_{n-1}^{(k-1)*}\|}{\|b_{n-1}^{(k-1)*}\|} \cdot \frac{\|b_{n-1}^{(k-1)*}\|}{\|b_{n-1}^{(k-2)*}\|} \overset{(16)}{\leq} 2^{(n-4)/2} \text{ for all } k \geq 2.$$

Lemma 5: For all $k \geq 1$ we have

$$\textbf{(18)} \qquad \nabla^{(k)} \leq \frac{1}{\prod_{i=1}^{n-1} \|e_i^*\|} \cdot \frac{\prod_{l=1}^{k-2} \|b_{n-1}^{(l)*}\|}{\prod_{l=1}^{k-1} \|a_{n-1}^{(l)*}\|} \cdot 2^{(k-1)(2n-1)} \quad \text{and}$$

$$\textbf{(19)} \qquad \mu^{(k)} \leq \frac{1}{\prod_{i=1}^{n-1} \|e_i^*\|} \cdot \frac{\prod_{l=1}^{k-1} \|b_{n-1}^{(l)*}\|}{\prod_{l=1}^{k-1} \|a_{n-1}^{(l)*}\|} \cdot 2^n \cdot 2^{(k-1)(2n-1)} \quad .$$

Here the empty product as usual is defined to be 1. □

Now we are ready to complete the proof of Proposition 3 (claim (5)). We use lattice theory (cf. eg. [9]). For each basis $\{b_1, \ldots, b_n\}$ of $\mathbf{Z}^n$ occuring in our algorithm, the (linearly independent) vectors $\pi b_1, \ldots, \pi b_{n-1}$ span the *lattice* $L = \sum_{i=1}^{n-1} \pi b_i \mathbf{Z}$. The *determinant* $\det(L)$ of the lattice is defined by $\prod_{i=1}^{n-1} \|b_i^*\|$; it is invariant under elementary basis transformations of $b_1, \ldots, b_{n-1}$. Hence we have $\det(\sum_{i=1}^{n-1} \pi b_i^{(l)} \mathbf{Z}) = \det(\sum_{i=1}^{n-1} \pi a_i^{(l-1)} \mathbf{Z})$ for all $l \geq 1$; we call this size D_l. Then $D_1 = \prod_{i=1}^{n-1} \|e_i^*\|$ and $\frac{\|b_{n-1}^{(l)*}\|}{\|a_{n-1}^{(l)*}\|} = \frac{D_l}{D_{l+1}}$, so inequality (19) can be rewritten as $\mu^{(k)} \leq 2^n \cdot 2^{(k-1)(2n-1)}/D_k$. Thus since $\|b_1^{(k)}\| \leq \|b_1^{(k)*}\| + \mu^{(k)}$ we have

(20) $\|b_1^{(k)}\| \leq \frac{2^{n+1} \cdot 2^{(k-1)(2n-1)}}{D_k}$.

Since $D_1 \leq 1$ and $\frac{D_l}{D_{l+1}} \leq \frac{1}{2}$ for all $l \geq 1$, we know

(21) $k - 1 \leq \log D_k^{-1}$.

The bases $\mathcal{B}^{(k)}$, $k \geq 1$, fulfill $|\mu_{i,j}| \leq 1/2$ for all $1 \leq j < i \leq n-1$ and $\|b_i^*\|^2 \leq 2 \cdot \|b_{i+1}^*\|^2$ for all $1 \leq i \leq n-2$, so $\{\pi b_1^{(k)}, \ldots, \pi b_{n-1}^{(k)}\}$ is reduced in the sence of [9]. This implies (cf. [9])

(22) $\|b_1^{(k)*}\| \leq 2^{(n-2)/4} \cdot D_k^{1/(n-1)}$.

Applying (21) and then (22) to (20) proves Proposition 3. □

4 Remarks on the algorithm

First remark: If we apply inequality (22) of the last section to (20) without using (21), we obtain the bound

$$\|b_1^{(k)}\| \leq \frac{2^{n+1} \cdot 2^{(n-1)(n-2)/4} \cdot 2^{(k-1)(2n-1)}}{\|b_1^{(k)*}\|^{n-1}} \quad ,$$

and thus

(23) $\quad \max_{1\leq i\leq n-1} |x_i - \frac{p_i}{q}| \leq \frac{\|x\| \cdot \mathrm{const}(n) \cdot 2^{(k-1)(2n-1)}}{|q|^{1+(n-1)^{-1}}}$.

Thus the vectors $b_1^{(k)}$ produced by our algorithm fulfill the Dirichlet-bound up to some constant depending on n and x, and up to a latter factor increasing with k. May be, the latter factor comes from the inductive proof technique, and may be the algorithm really meets the Dirichlet-bound up to a constant depending on n (and $\|x\|$).

Second remark: The problem of diophantine approximations alone, without the intention to generalize the cfa, was investigated by Lagarias [8] in 1982. He proposed an algorithm for rational inputs, which can be immediately be carried over to real ones. The algorithm on input $x_1, \cdots, x_{n-1}$ and $Q > 0$ produces in polynomial time a diophantine approximation $(p_1, \cdots, p_{n-1}, q)$ for $x_1, \cdots, x_{n-1}$ such that $|q| \leq Q$ and

$$\max_{1\leq i\leq n-1} |x_i - \frac{p_i}{q}| \leq \frac{2^{n/2} \cdot n}{|q|^{1+\frac{1}{n-1}}} \quad .$$

So the Dirichlet bound is met up to some constant factor. Moreover, Lagarias proofs several NP-completeness results that suggest, that it may be hard to find approximations within the Dirichlet-bound. A higher dimensional cfa, however, must construct a sequence of bases of $\mathbf{Z}^n$ by performing elementary basis transformations.

Acknowledgement: The results of this paper are part of the author's Ph. D. thesis guided by Prof. Dr. C.P. Schnorr. Thanks to him for many helpfull discussions.

References

[1] G. Bergman, *Notes on Ferguson and Forcade's Generalized Euclidean Algorithm*, preprint, Dept. of Math. Univ. California, Berkeley (1980);

[2] L. Bernstein, *The Jacobi-Perron Algorithm*, Springer Lecture Notes in Math. 207 (1971);

[3] E. Borel, *Contribution à l'analyse arithmétique du continu*, J. Math. Pures Appl. 5, 9 (1903), 329-397;

[4] V. Brun, *En generalisation av kjedebroken I+II*, Skr. Vid. Selsk. Kristiana, Mat. Nat. Kl. 6 (1919), 1-29 and 6 (1920), 1-24

[5] H. Ferguson, R. Forcade, *Generalization of the Euclidean Algorithm for Real Numbers to All Dimensions Higher than Two*, Bull. Am. Math. Soc. 1, 6 (1979), 912-914;

[6] J. Hastad, B. Just, J. Lagarias, C.P. Schnorr, *Polynomial Time Algorithms for Finding Integer Relations Among Real Numbers*, to appear in Siam J. Comput., prelim. version in Proc. of STACS'86, Springer Lecture Notes in Comput. Sci. 210 (1986), 105-118;

[7] C.G.J. Jacobi, *Allgemeine Theorie der kettenbruchähnlichen Algorithmen*, J. Reine Angew. Math. 69 (1868), 29-64;

[8] J. Lagarias, *Computational Complexity of Simultaneous Diophantine Approximation Problems*, 23rd Ann. Symp. on the Foundations of Computer Science (1982), 32-39;

[9] A.K. Lenstra, H.W. Lenstra, L. Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann. 261 (1982), 513-534;

[10] H. Minkowski, *Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen*, J. Reine Angew. Math. 107 (1891), 278-297;

[11] R.E.A.C. Payley, H.D. Ursell, *Continued Fractions in Several Dimensions*, Proc. Cambridge Philos. Soc. 26 (1930), 127-144;

[12] O. Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus*, Math. Ann. 64 (1907), 1-76;

[13] H. Poincaré, *Sur une généralisation des fractions continues*, C.R. Acad. Sci. Paris 99 (1884), 1014-1016;

[14] M. Reed, B. Simon, *Functional analysis*, Vol. I, Academic Press Orlando, Florida (1980);

[15] G. Szekeres, *Multidimensional Continued Fractions*, Ann. Univ. Sci. Budapest, Eötvös Sect. Math. 13 (1970), 113-140.