A stable integer relation algorithm

Preliminary Version

Carsten Rössner* and Claus P. Schnorr†

FB Mathematik / Informatik, Universität Frankfurt,
Postfach 11 19 32, 60054 Frankfurt am Main, Germany

TR-94-016

April 1994

Abstract

We study the following problem: given $x \in \mathbb{R}^n$ either find a short integer relation $m \in \mathbb{Z}^n$, so that $< x, m >= 0$ holds for the inner product $< ., . >$, or prove that no short integer relation exists for x. Hastad, Just, Lagarias and Schnorr (1989) give a polynomial time algorithm for this problem.

We present a stable variation of the HJLS–algorithm that preserves lower bounds on $\lambda(x)$ for infinitesimal changes of x. Given $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{N}$ this algorithm finds a nearby point x' and a short integer relation m for x'. The nearby point x' is 'good' in the sense that no very short relation exists for points $\overline{x}$ within half the x'–distance from x. On the other hand if $x' = x$ then m is, up to a factor $2^{n/2}$, a shortest integer relation for x.

Our algorithm uses, for arbitrary real input x, at most $O(n^4(n + \log \alpha))$ many arithmetical operations on real numbers. If x is rational the algorithm operates on integers having at most $O(n^5 + n^3(\log \alpha)^2 + \log(\|qx\|^2))$ many bits where q is the common denominator for x.

*e-mail: roessner@cs.uni-frankfurt.de
†e-mail: schnorr@cs.uni-frankfurt.de

1 Introduction

Given a real vector $x \in \mathbb{R}^n$ an *integer relation* for x is a non–zero vector $m \in \mathbb{Z}^n$ with zero inner product $< m, x >= 0$. This paper studies the following computational problem: given $x \in \mathbb{R}^n$ find a nearby point x' to x and a short integer relation m for x' so that there is no much closer point $\overline{x}$ to x having a very short integer relation. Let $\lambda(x)$ denote the length $< m, m >^{1/2}$ of the shortest integer relation m for x. Given $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{N}$ our algorithm finds $x' \in \mathbb{R}^n$, $m \in \mathbb{Z}^n \setminus 0$ satisfying

- $\| m \| \leq 2^{O(n^4(\log \alpha)^2)}$, $< m, x' > = 0$
- $\lambda(\overline{x}) \geq \frac{\alpha}{2}$ holds for all $\overline{x} \in \mathbb{R}^n$ with $\| x - \overline{x} \| < \| x - x' \|/2$
- if $x = x'$ then $\| m \| < 2^{n/2}\lambda(x)$.

The *nearby* point $x' \in \mathbb{R}^n$ has a 'short' integer relation m, $\|m\| \leq 2^{O(n^4(\log \alpha)^2)}$. The nearby point is 'good' in the sense that there is no $\overline{x} \in \mathbb{R}^n$, within half the x'–distance from x, having an integer relation of length at most $\alpha/2$. On the other hand if $x' = x$ then m is, up to a factor $2^{n/2}$, a shortest integer relation for x.

For real input x the algorithm uses at most $O(n^4(n+\log \alpha))$ many arithmetic operations on real numbers using exact arithmetic. If the input x is rational, $x = (p_1, \ldots, p_n)/q$ with integers $p_1, \ldots, p_n, q$, then the arithmetic operations are on integers. The bit length of these integers is bounded polynomially in $n + \log \alpha + \log(\|qx\|^2)$. For non–rational x the solution $x' \in \mathbb{R}^n$ may be non–rational as well. The solution $(x',\ m)$ holds for all $\overline{x}$ satisfying $\| x - \overline{x} \| < \| x - x' \|/2$. Without this stability property the problem is easy to solve. A short integer relation for a close approximation x' to x can be found by the L^3–algorithm for lattice basis reduction. If x is rational and $\lambda(x) < 2^{O(n^4(\log \alpha)^2)}$ it suffices to construct by L^3–reduction a short integer relation for x. The problem is difficult if $\lambda(x) \gg 2^{O(n^4(\log \alpha)^2)}$ or if x is non–rational. The first polynomial time algorithm, which for arbitrary real x produces a 'good' lower bound for $\lambda(x)$ has been designed by Hastad, Just, Lagarias and Schnorr [HJLS89]. For given x , α the HJLS–algorithm either finds an integer relation m for x with $\| m \| < 2^{n/2}\alpha$ or it proves that $\lambda(x) > \alpha$.

The instability of the HJLS–algorithm is due to the goal of approximating $\lambda(x)$ which is a discontinuous function in x. To obtain a stable algorithm we changed the objectives of the algorithm somewhat. The new algorithm computes a point x' near to x and establishes the lower bound $\lambda(\overline{x}) > \alpha/2$ for all $\overline{x}$ satisfying $\| x - \overline{x} \| < \| x - x' \|/2$. The new algorithm is a variant of the HJLS–algorithm, which in turn is a variation of both the L^3–algorithm of Lenstra, Lenstra and Lovász [LLL82] and the generalized continued fraction algorithm presented by Bergman [B80] in his notes on Ferguson and Forcade's generalized Euclidean algorithm.

2 Notation and Definitions

Let $\mathbb{R}^n$ be the n–dimensional real vector space with the ordinary inner product $< .,. >$ and Euclidean length $\|y\| :=< y, y >^{1/2}$. A discrete additive subgroup $L \subset \mathbb{R}^n$ is called a *lattice.* Every lattice is generated by some set of linear independent vectors $b_1, \ldots, b_m \in L$ that is called a *basis* of L , $L = \{ \sum_{j=1}^{m} t_j b_j \ : \ t_j \in \mathbb{Z},\ 1 \leq j \leq m \}$. We let $L(b_1, ..., b_m)$ denote the lattice generated by the basis $b_1, ..., b_n$.

A non–zero vector $m \in \mathbb{Z}^n$ is called an *integer relation* for $x \in \mathbb{R}^n$ if $< x, m >= 0$. We let $\lambda(x)$ denote the length $\|m\| :=< m, m >^{1/2}$ of the shortest integer relation m for x, $\lambda(x) = \infty$ if no relation exists.

Throughout the paper we let $b_1, \ldots, b_n$ be an ordered basis of the integer lattice $\mathbb{Z}^n$ and let $b_0 := x$ be a non–zero vector in $\mathbb{R}^n$. We associate with this basis the orthogonal projections

$$\begin{aligned} \pi_{i,x} &: \mathbb{R}^n \longrightarrow span(x, b_1, , \ldots, , b_{i-1})^{\perp} \qquad \text{and} \\ \pi_i &: \mathbb{R}^n \longrightarrow span(b_1, , \ldots, , b_{i-1})^{\perp} \qquad \text{for } i = 1, \ldots, n\,, \end{aligned}$$

where $span(b_j, \ldots, , b_{i-1})$ denotes the linear space generated by $b_j, \ldots, b_{i-1}$ and $span(b_j, \ldots, b_{i-1})^{\perp}$ its orthogonal complement in $\mathbb{R}^n$. We abbreviate $\widehat{b}_{i,x} := \pi_{i,x}(b_i)$, $\widehat{b}_i := \pi_i(b_i)$ and $\widehat{x}_i := \pi_i(x)$. The vectors $\widehat{b}_{1,x}, \ldots, \widehat{b}_{n,x}$ (resp. $\widehat{b}_1, \ldots, \widehat{b}_n$) are pairwise orthogonal. They are called the *Gram–Schmidt orthogonalization* of $x, b_1, \ldots, b_n$ (resp. $b_1, \ldots, b_n$). The *Gram–Schmidt coefficients* for $b_0 = x, b_1, \ldots, b_n$ are defined as

$$\mu_{k,j} \;:=\; \frac{< b_k, \widehat{b}_{j,x} >}{\|\widehat{b}_{j,x}\|^2} \qquad \text{for } 1 \le k, j \le n\,,$$

where we set $\mu_{k,j} = 0$ if $\widehat{b}_{j,x} = 0$. We have

$$\pi_{i,x}(b_k) \;=\; \sum_{j=i}^{k} \mu_{k,j} \widehat{b}_{j,x} \qquad \text{for } 1 \le i \le k \le n\,.$$

We call the (ordered) system of vectors $b_0 := x, b_1, \ldots, b_n$ *size–reduced* if

$$|\mu_{k,j}| \le \tfrac{1}{2} \qquad \text{holds for } 1 \le j < k \le n$$

and L^3*–reduced* if it is size–reduced and the inequality

$$\tfrac{3}{4} \, \|\pi_{k-1,x}(b_{k-1})\|^2 \;\le\; \|\pi_{k-1,x}(b_k)\|^2 \;\text{ holds for } k = 2, \ldots, n\,.$$

The latter inequality is equivalent to

$$\tfrac{3}{4} \, \|\widehat{b}_{k-1,x}\|^2 \;\le\; \|\widehat{b}_{k,x}\|^2 + \mu_{k,k-1}^2 \, \|\widehat{b}_{k-1,x}\|^2\,.$$

We let $\lceil \,.\, \rfloor$ denote the nearest integer function to a real number r, $\lceil r \rfloor = \lfloor r + 0.5 \rfloor$. Let $[b_1, \ldots, b_n]$ denote the matrix with column vectors $b_1, \ldots, b_n$.

3 The method of the HJLS–algorithm

The HJLS–algorithm relies on Proposition 3.1 of [HJLS89] which states that

$$\lambda(x) \;\ge\; 1 / \max_{i=1,\ldots,n} \|\widehat{b}_{i,x}\| \tag{1}$$

holds for every basis $b_1, \ldots, b_n$ of the lattice $\mathbb{Z}^n$. This inequality already appears in somewhat weaker form in [FF79].

Initially the vector $x = b_0$ is extended to the linear dependent system $\{b_0, b_1, \ldots, b_n\} = \{x, e_1, \ldots, e_n\}$, where $e_1, \ldots, e_n$ are the unit–vectors in $\mathbb{R}^n$.

The algorithm transforms the basis $b_1, \ldots, b_n$ by exchange and size–reduction steps intending to minimize $\max_{i=1,\ldots,n} \|\widehat{b}_{i,x}\|$. For this the HJLS–algorithm uses the Bergman exchange rule which swaps b_{i-1}, b_i for an i that maximizes $\|\widehat{b}_{i,x}\|^2 \, 2^i$. The algorithm terminates if $\max_{i=1,\ldots,n} \|\widehat{b}_{i,x}\| < \alpha^{-1}$. There is one possible way that the HJLS–algorithm

fails to achieve $\max_{i=1,\ldots,n} \|\widehat{b}_{i,x}\| < \alpha^{-1}$. This is if an exchange $b_{n-1} \longleftrightarrow b_n$ results in a zero–vector $\widehat{b}_{n-1,x}$. In this case the new basis $b_1, \ldots, b_n$ yields an integer relation a_n, which is the last vector of the basis $a_1, \ldots, a_n$ that is *dual* to $b_1, \ldots, b_n$, i. e.

$$[b_1, \ldots, b_n]^{-1} \;=\; [a_1, \ldots, a_n]^{\top} \; .$$

This relation a_n is sufficiently short, we have $\quad \|a_n\| \le 2^{n/2}\, \alpha \, .$

Stability analysis. In Lemma 9 we show the inequalities

$$\begin{aligned} \|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| \;&\le\; \|\widehat{b}_{i,x}\| \, \frac{2\, \|\widehat{x}_i - \widehat{\overline{x}}_i\|}{\max\{\|\widehat{x}_{i+1}\| \, , \, \|\widehat{\overline{x}}_{i+1}\|\}} \\ &\le\; \|\widehat{b}_{i,x}\| \, \frac{2\, \|x - \overline{x}\|}{\|\widehat{x}_n\|} \qquad \text{for } i = 1, \ldots, n-1 \, ; \end{aligned} \tag{2}$$

where $\widehat{x}_i = \pi_i(x)$ and $\widehat{\overline{x}}_i = \pi_i(\overline{x})$. From this and (1) we see that

$$\lambda(\overline{x}) \ge \alpha/2 \tag{3}$$

holds provided that the inequalities (4) and (5) are satisfied:

$$\|x - \overline{x}\| \;<\; \|\widehat{x}_n\|/2 \tag{4}$$

$$\|\widehat{b}_{i,x}\| \;\le\; 2\, \alpha^{-1} \qquad \text{for } i = 1, \ldots, n \tag{5}$$

This is because inequalities (2), (4) and (5) imply

$$\|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| \;<\; \|\widehat{b}_{i,x}\|$$

and thus $\qquad 0 \;<\; \|\widehat{b}_{i,\overline{x}}\| \;<\; 2\, \alpha^{-1} \qquad \text{for } i = 1, \ldots, n \, .$

We modify the HJLS–algorithm so that the basis and its dual satisfy throughout the algorithm the inequalities

$$\|a_k\| \, , \; \|b_k\| \;\le\; 2^{O(n^4 + n^2 (\log \alpha)^2)} \qquad \text{for } k = 1, \ldots, n \, , \tag{6}$$

see Proposition 2. These inequalities hold for arbitrary real input x.

To obtain (6) we have to perform some size–reduction steps but we cannot afford a complete size–reduction as in the L^3–algorithm. We only reduce b_k versus b_j if $\|\widehat{b}_{j,x}\| \ge \alpha^{-1}$. In this case Lemma 6 shows that the reduction coefficient $\mu_{k,j}$ is at most

$$|\mu_{k,j}| \;=\; \frac{| < \pi_{j,x}(b_k), \widehat{b}_{j,x} > |}{\|\widehat{b}_{j,x}\|^2} \;\le\; 2^{n/2-1} \alpha \sqrt{n}$$

and thus the resulting reduction $b_k \longleftarrow b_k - \lceil \mu_{k,j} \rfloor b_j$ does not generate a very large vector b_k. Large values $\mu_{k,j}$ with $\|\widehat{b}_{j,x}\| < \alpha^{-1}$ will be oppressed in the further reduction process. The stable integer relation algorithm does not use Bergman's exchange rule, it uses the exchange rule of the L^3–algorithm. The L^3–exchange rule may be inefficient in case of extremely small orthogonalization vectors $\widehat{b}_{j,x}$. We overcome this inefficiency by collecting the vectors b_j with $\|\widehat{b}_{j,x}\| < \alpha^{-1}$ in the initial segment of the basis. For this we use an index s which, throughout the algorithm, satisfies

$$\|\widehat{b}_{j,x}\| \;\le\; \alpha^{-1} \qquad \text{for } j = 1, \ldots, s-1 \, .$$

The vectors b_j with $j < s$ will be excluded from all further exchange and reduction steps.

4 STABLE INTEGER RELATION ALGORITHM

Input $x \in \mathbb{R}^n$, $x \neq 0$, $\alpha \in \mathbb{N}$.

1. **FOR** $i = 1$ **TO** n **DO**
   $a_i := b_i := e_i$ the i–th unit–vector

   $s := k := 1$; $b_0 := x$; $c_0 :=< x, x >$; * k is the *stage* *

2. **WHILE** $s < n$ **DO**
   * upon entry of the loop we always have $c_j = \|\widehat{b}_{j,x}\|^2 > 0$ for $j = 1, \ldots, k-1$, $s \leq k$, $c_1, \ldots, c_{s-1} \leq \alpha^{-2}$, $\pi_{s,x}(b_s), \ldots, \pi_{s,x}(b_{k-1})$ is L^3–reduced. *

   $c_k :=< b_k, b_k >$;

   IF $k = 1$ **THEN** $k := 2$; $c_2 =< b_2, b_2 >$

2.1 **FOR** $j = 0$ **TO** $k-1$ **DO**
   $\mu_{k,j} := (< b_k, b_j > - \sum_{i=0}^{j-1} \mu_{k,i}\mu_{j,i}c_i)/c_j$; $c_k := c_k - \mu_{k,j}^2\, c_j$

   IF ($c_k = 0$ **AND** $k < n$) **THEN** **Output** $x' := x$, a_n ; **STOP**

2.2 **IF** ($c_k \leq \alpha^{-2}$ **AND** $k = s$) **THEN** $k := s := s + 1$; **GOTO** 2

2.3 **FOR** $j = k-1$ **DOWNTO** s **DO**
   $b_k := b_k - \lceil \mu_{k,j} \rfloor b_j$; $a_j := a_j + \lceil \mu_{k,j} \rfloor a_k$; update $\mu_{k,i}$ for $i = 0, \ldots, j$

2.4 **IF** $\frac{3}{4}\, c_{k-1} > c_k + \mu_{k,k-1}^2\, c_{k-1}$
   THEN swap b_{k-1}, b_k ; swap a_{k-1}, a_k ; $k := k - 1$
   ELSE $k := k + 1$

   END-WHILE

3. compute the orthogonal projection $\widehat{x}_n = \pi_n(x) \in span(b_1, \ldots, b_{n-1})^{\perp}$ of x ;
   Output $x' = x - \widehat{x}_n$, a_n .

Comments: 1. Upon entry of stage k we compute the Gram–Schmidt coefficients $\mu_{k,j}$, $j = 0, \ldots, k-1$ and the height square $c_k = \|\widehat{b}_{k,x}\|^2$. This computation uses the actual basis vectors $b_1, \ldots, b_{k-1}$ and the previously computed entities $\mu_{j,i}$ for $0 \leq i < j \leq k-1$ and $c_0, \ldots, c_{k-1}$.
2. The equality $[b_1, \ldots, b_n]^{-1} = [a_1, \ldots, a_n]^{\top}$ does always hold, i. e. the basis $a_1, \ldots, a_n$ is the dual of the basis $b_1, \ldots, b_n$. Therefore a reduction step $b_k \longleftarrow b_k - \lceil \mu_{k,j} \rfloor b_j$ implies the transformation $a_j \longleftarrow a_j + \lceil \mu_{k,j} \rfloor a_k$ in step 2.3.
3. The value $\max_{1 \leq i \leq n} c_i$ does never increase. Initially this maximum is at most 1.

Lemma 1. *Upon entry of the WHILE–loop in step 2 we always have*
1. $c_j = \|\widehat{b}_{j,x}\|^2 > 0$ *for* $j = 1, \ldots, k-1$,
2. $c_1, \ldots, c_{s-1} \leq \alpha^{-2}$,
3. $\pi_{s,x}(b_s), \ldots, \pi_{s,x}(b_{k-1})$ *is* L^3*–reduced.*

Proof. The claims are shown by induction on the number of passes of the WHILE–loop.
(1) The termination condition in step 2.1 implies that $c_j > 0$ holds for $j = 1, \ldots, k-1$.

(2) is an immediate consequence of the actualization of s in step 2.2. (3) holds because the previous steps 2.3 and 2.4 of stage $k-1$ finish the L^3–reduction of $\pi_{s,x}(b_s), \ldots, \pi_{s,x}(b_{k-1})$. □

5 Analysis and Correctness

We first prove an upper bound on the length of the vectors in the bases $b_1, \ldots, b_n$ and its dual $a_1, \ldots, a_n$ which holds throughout the algorithm. This bound holds no matter whether the input x is rational or irrational. The result is based on the restricted size-reduction of step 2.3. It becomes wrong if we change the algorithm to either perform full size-reduction or to perform no size-reduction at all.

Proposition 2. *Let the input x be an arbitrary real vector. Throughout the algorithm the basis $b_1, \ldots, b_n$ and its dual $a_1, \ldots, a_n$ satisfy $\|a_k\|, \|b_k\| \leq 2^{O(n^4+n^2(\log\alpha)^2)}$ for $k = 1, \ldots, n$.*

Thus the bit length of the coordinates of b_k and a_k is at most $O(n^4 + n^2(\log\alpha)^2)$. From this we obtain, for rational inputs x, a polynomial bound for the bit length of the integers occuring in the algorithm. As a consequence the algorithm has polynomial bit complexity for rational inputs x.

Theorem 3. *Let the input x be rational with $x = (p_1, \ldots, p_n)/q$ and $p_1, \ldots, p_n, q \in \mathbb{Z}$. Then the algorithm performs at most $O(n^4(n + \log\alpha))$ arithmetical operations using integers with at most $O(n^5 + n^3(\log\alpha)^2 + \log(\|qx\|^2))$ bits.*

Proof sketch. The number of arithmetic operations of the algorithm is about n times that of the HJLS–algorithm, see Theorem 3.2 of [HJLS89]. The additional factor n is for the size–reduction in step 2.3. Let the rational input be $x = b_0 = (p_1, \ldots, p_n)/q$ with $p_1, \ldots, p_n, q \in \mathbb{Z}$. Then a common denominator for the coordinates of the rational vector $\widehat{b}_{i,x}$ is the integer

$$q^2 \det(< b_j, b_l >)_{0 \leq j,l \leq i}\ .$$

We see from Proposition 2 and the Hadamard inequality that this integer is in absolute value at most $\|qx\|^2\, 2^{O(n^4 i + n^2 i(\log\alpha)^2)}$. It follows that all integers occuring in the algorithm are at most $\|qx\|^2\, 2^{O(n^5+n^3(\log\alpha)^2)}$ in absolute value. □

To prove Proposition 2 we analyse the effect of the size–reduction. All changes of the basis vectors are by the size–reduction in step 2.3. For an arbitrary pass of loop 2.3 let $b_k^{(l)}$, $\mu_{k,i}^{(l)}$ denote the vector b_k and the Gram–Schmidt coefficient $\mu_{k,i}$ after performing l iterations of this loop with l values j. So $b_k^{(0)}$ is b_k before entering the loop, and $b_k^{(k-s)}$ is the vector b_k upon termination of the loop.

Lemma 4. *We have for $i = k-l-1, \ldots, s$*

$$|\mu_{k,i}^{(l)}| \ \leq\ |\mu_{k,i}^{(0)}| + [(\tfrac{3}{2})^l - 1](\tfrac{1}{2} + \max_{j=k-1,\ldots,k-l} |\mu_{k,j}^{(0)}|)\ .$$

Proof. We prove by induction on l the inequality

$$|\mu_{k,i}^{(l)}| \ \leq\ |\mu_{k,i}^{(0)}| + \tfrac{1}{2}\sum_{j=0}^{l-1} (\tfrac{3}{2})^j (\tfrac{1}{2} + |\mu_{k,k-l+j}^{(0)}|) \qquad \text{for } l = 1, \ldots, k-s\ .$$

Since b_{k-l} is size–reduced we have

$$\begin{aligned} |\mu_{k,i}^{(l)}| &= |\mu_{k,i}^{(l-1)} - \lceil \mu_{k,k-l}^{(l-1)} \rfloor \mu_{k-l,i}| \\ &\leq |\mu_{k,i}^{(l-1)}| + \tfrac{1}{2}(\tfrac{1}{2} + |\mu_{k,k-1}^{(l-1)}|) \end{aligned}$$

which proves the claim for $l = 1$. The induction hypothesis for $l = 1$ applied to the latter inequality yields

$$\begin{aligned} |\mu_{k,i}^{(l)}| &\leq |\mu_{k,i}^{(0)}| + \tfrac{1}{2}\sum_{j=0}^{l-2}(\tfrac{3}{2})^j(\tfrac{1}{2} + |\mu_{k,k-l+j}^{(0)}|) \\ &+ \tfrac{1}{2}(\tfrac{1}{2} + |\mu_{k,k-l}^{(0)}| + \tfrac{1}{2}\sum_{j=0}^{l-2}(\tfrac{3}{2})^j(\tfrac{1}{2} + |\mu_{k,k-l+j}^{(0)}|)) \\ &\leq |\mu_{k,i}^{(0)}| + \tfrac{1}{2}\sum_{j=1}^{l-1}(\tfrac{3}{2})^j(\tfrac{1}{2} + |\mu_{k,k-l+j}^{(0)}|)) + \tfrac{1}{2}|\mu_{k,k-l}^{(0)}| \\ &\leq |\mu_{k,i}^{(0)}| + \tfrac{1}{2}\sum_{j=0}^{l-1}(\tfrac{3}{2})^j(\tfrac{1}{2} + |\mu_{k,k-l+j}^{(0)}|) \end{aligned}$$

Finally the claim follows from evaluating the geometrical sum. □

Corollary 5. *For every pass of step 2.3 we have*

$$\|b_k^{(k-s)}\| \leq \|b_k^{(0)}\| + \sum_{i=s}^{k-1}\|b_i^{(0)}\|(\tfrac{3}{2})^{k-1-i}(\tfrac{1}{2} + \max_{s\leq j\leq k-1}|\mu_{k,j}^{(0)}|) .$$

Proof. For the whole size–reduction loop with respect to $b_{k-1}, \ldots, b_s$ Lemma 4 yields

$$\begin{aligned} \|b_k^{(k-s)}\| &= \|b_k^{(0)} - \sum_{i=s}^{k-1}\mu_{k,i}^{(k-1-i)}b_i^{(0)}\| \leq \|b_k^{(0)}\| + \sum_{i=s}^{k-1}\|b_i^{(0)}\|\,|\mu_{k,i}^{(k-1-i)}| \\ &\leq \|b_k^{(0)}\| + \sum_{i=s}^{k-1}\|b_i^{(0)}\|\,[\,|\mu_{k,i}^{(0)}| + [(\tfrac{3}{2})^{k-1-i} - 1]\,(\tfrac{1}{2} + \max_{j=k-1,\ldots,i+1}|\mu_{k,j}^{(0)}|)\,] \\ &\leq \|b_k^{(0)}\| + \sum_{i=s}^{k-1}\|b_i^{(0)}\|(\tfrac{3}{2})^{k-1-i}(\tfrac{1}{2} + \max_{s\leq j\leq k-1}|\mu_{k,j}^{(0)}|) \qquad \square \end{aligned}$$

Lemma 6. *Upon entry of step 2.3 we have that* $|\mu_{k,i}| \leq 2^{n/2-1}\alpha\sqrt{n}$ *for* $s \leq i \leq k-1$.

Proof. CASE 1: b_k has not been reduced before.
Then $b_k = e_k$ and $\pi_{s,x}(b_s), \ldots, \pi_{s,x}(b_{k-1})$ is L^3–reduced. Using the properties of L^3–reduced bases [LLL82] we see that

$$\begin{aligned} |\mu_{k,i}| &= \frac{|<\pi_{i,x}(b_k), \widehat{b}_{i,x}>|}{\|\widehat{b}_{i,x}\|^2} \leq \frac{\|\pi_{i,x}(b_k)\|}{\|\widehat{b}_{i,x}\|} \leq \frac{\|b_k\|}{\|\widehat{b}_{i,x}\|} \\ &= \|\widehat{b}_{i,x}\|^{-1} \leq 2^{\frac{i-s}{2}}\|\widehat{b}_{s,x}\|^{-1} < 2^{\frac{n-1}{2}}\alpha . \end{aligned}$$

CASE 2: b_k has been reduced in a previous pass of step 2.3.
Let $b_{k'}$ be the old vector b_k after its last reduction on stage k' and before its transfer, via

exchange steps, from position k to position k'. Let s' be the value of s at stage k'. We have from $\|\widehat{b}_{j,x}\| \le 1$ for $j = 1, \ldots, n$ that

$$|\mu_{k',j}| \le \tfrac{1}{2} \text{ for } j = s' \le s, \ldots, k'-1 \text{ and}$$

$$\|\pi_{i,x}(b_k)\|^2 \;=\; \|\widehat{b}_{k',x}\|^2 + \sum_{j=i}^{k'-1} \mu_{k',j}^2 \|\widehat{b}_{j,x}\|^2 \;\le\; \frac{n+3}{4} \qquad \text{for } i = s, \ldots, k\,.$$

Finally we see from $2^{i-s}\,\|\widehat{b}_{i,x}\|^2 \ge \|\widehat{b}_{s,x}\|^2 \ge \alpha$ that for $s \le i \le k$

$$|\mu_{k,i}| \;\le\; \frac{\|\pi_{i,x}(b_k)\|}{\|\widehat{b}_{i,x}\|} \;\le\; 2^{\frac{i-s-2}{2}} \alpha \sqrt{n+3} \;\le\; 2^{n/2-1} \alpha \sqrt{n}\,. \qquad \square$$

Corollary 7. *The maximum* $B^{(l)} := \max_{1 \le k \le n} \|b_k^{(l)}\|$ *satisfies*

$$B^{(k-s)} \;\le\; B^{(0)} (\tfrac{3}{2})^{n-1} 2^{n/2} \alpha \sqrt{n}\,.$$

Proof. After the size–reduction of b_k with respect to $b_{k-1}, \ldots, b_s$ we have from Corollary 5

$$\begin{aligned} B^{(k-s)} &\le B^{(0)} [1 + \sum_{i=s}^{k-1} (\tfrac{3}{2})^{k-1-i} (\tfrac{1}{2} + \max_{s \le j \le k-1} |\mu_{k,j}^{(0)}|)] \\ &\le B^{(0)} (2(\tfrac{3}{2})^{k-s} - 1)(\tfrac{1}{2} + \max_{s \le j \le k-1} |\mu_{k,j}^{(0)}|) \\ \text{(by Lemma 6)} \quad &\le B^{(0)} (2(\tfrac{3}{2})^{k-s} - 1)(\tfrac{1}{2} + 2^{n/2-1} \alpha \sqrt{n}) \\ &\le B^{(0)} (\tfrac{3}{2})^{k-1} 2^{n/2} \alpha \sqrt{n}\,. \qquad \square \end{aligned}$$

Proof of Proposition 2. The number of passes of step 2.3 is at most "$n +$ the number of swaps in step 2.4". Hastad, Just, Lagarias and Schnorr show that the number of swaps is at most $\binom{n}{2}((\log_{4/3} 2)n + 2\log_2 \alpha)$. This is because every swap of b_{k-1}, b_k in step 2.4 decreases the product

$$\prod_{i=1}^{n-1} (\max\{\|\widehat{b}_{i,x}\|^2\, 2^n,\ \alpha^{-2}\})^{n-i}$$

by at least a factor $\frac{4}{3}$. Initially this product is at most $2^{n^3/2}$ and upon termination it is at least α^{-n^2}. Thus the number of passes of step 2.3 is at most $\binom{n}{2}((\log_{4/3} 2)n + 2\log_2 \alpha) + n$. Let B_{term}, B_{init} denote the maximum Euclidean length of the terminal, respectively initial, basis vectors. We have $B_{init} = \max_{1 \le k \le n} \|e_k\| = 1$, and thus Corollary 7 yields

$$B_{term} \;\le\; [\,(\tfrac{3}{2})^{n-1} 2^{n/2} \alpha \sqrt{n}\,]^{\binom{n}{2}((\log_{4/3} 2)n + 2\log_2 \alpha) + n} \;=\; 2^{O(n^4 + n^2 (\log \alpha)^2)}\,.$$

The claim on the vectors a_k of the dual basis holds by symmetry. $\square$

Lemma 8. *For* x, $\overline{x} \in \mathbb{R}^n$ *let* π_x, $\pi_{\overline{x}}$ *denote the orthogonal projection into* $span(x)^\perp$, $span(\overline{x})^\perp$ *respectively. Then we have for all* $b \in \mathbb{R}^n$

$$\|\pi_x(b) - \pi_{\overline{x}}(b)\| \;\le\; \frac{2\,\|b\|\,\|x - \overline{x}\|}{\max\{\|x\|, \|\overline{x}\|\}}\,.$$

Proof. Following Clarkson, [Cla92] Lemma 3.2, we have

$$\left| \frac{< b, x >}{\|x\|^2} - \frac{< b, \overline{x} >}{\|\overline{x}\|^2} \right| \;\le\; \frac{\|b\|\,\|x - \overline{x}\|}{\|x\|\,\|\overline{x}\|}\,. \tag{7}$$

This and the Cauchy–Schwarz inequality imply

$$\begin{aligned}
\|\pi_x(b) - \pi_{\overline{x}}(b)\| &\leq \left\| b - \frac{< b, x >}{\|x\|^2} x - (b - \frac{< b, \overline{x} >}{\|\overline{x}\|^2}\overline{x}) \right\| \\
&= \left\| \frac{< b, \overline{x} >}{\|\overline{x}\|^2}\overline{x} - \frac{< b, x >}{\|x\|^2}\overline{x} + \frac{< b, x >}{\|x\|^2}\overline{x} - \frac{< b, x >}{\|x\|^2} x \right\| \\
&\leq \|\overline{x}\| \left| \frac{< b, \overline{x} >}{\|\overline{x}\|^2} - \frac{< b, x >}{\|x\|^2} \right| + \frac{| < b, x > |}{\|x\|^2} \|\overline{x} - x\| \\
&\leq \frac{\|b\| \, \|\overline{x} - x\|}{\|x\|} + \frac{\|b\|}{\|x\|} \|\overline{x} - x\| \; = \; 2 \, \frac{\|b\| \, \|x - \overline{x}\|}{\|x\|} \; .
\end{aligned}$$

proves the claim. □

Lemma 9. *For x , $\overline{x} \in \mathbb{R}^n$ we have*

$$\|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| \; \leq \; 2 \, \|\widehat{b}_{i,x}\| \, \frac{\|x - \overline{x}\|}{\|\widehat{x}_n\|} \qquad \textit{for } i = 1, \ldots, n-1 \; .$$

Proof. We apply Lemma 8 with $b = \widehat{b}_i$, $x = \widehat{x}_i$, $\overline{x} = \widehat{\overline{x}}_i$. Using $\pi_{\widehat{x}_i}(\widehat{b}_i) = \widehat{b}_{i,x}$ and $\pi_{\widehat{\overline{x}}_i}(\widehat{b}_i) = \widehat{b}_{i,\overline{x}}$ this yields

$$\|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| \; \leq \; \|\widehat{b}_i\| \, \frac{2 \, \|\widehat{x}_i - \widehat{\overline{x}}_i\|}{\max\{\|\widehat{x}_i\| \, , \, \|\widehat{\overline{x}}_i\|\}} \; = \; \|\widehat{b}_{i,x}\| \, \frac{2 \, \|\widehat{x}_i - \widehat{\overline{x}}_i\|}{\max\{\|\widehat{x}_{i+1}\| \, , \, \|\widehat{\overline{x}}_{i+1}\|\}} \; .$$

The last equality follows from $\|\widehat{x}_i\| \, \|\widehat{b}_{i,x}\| = |\det(\pi_i(x) \, , \, \pi_i(b_i))| = \|\widehat{b}_i\| \, \|\widehat{x}_{i+1}\|$. Using $\|\widehat{x}_n\| \leq \|\widehat{x}_{i+1}\|$, $\|\widehat{x}_i - \widehat{\overline{x}}_i\| = \|\pi_i(x - \overline{x})\| \leq \|x - \overline{x}\|$ for $i = 1, \ldots, n-1$ we see that

$$\|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| \; \leq \; 2 \, \|\widehat{b}_{i,x}\| \, \frac{\|x - \overline{x}\|}{\|\widehat{x}_n\|} \; . \qquad \square$$

Theorem 10. *For arbitrary input $x \in \mathbb{Q}^n$, $\alpha \in \mathbb{N}$ the Stable Integer Relation Algorithm produces $x' \in \mathbb{Q}^n$, $m \in \mathbb{Z}^n \setminus 0$ such that*

1. $\| \, m \, \| \; \leq \; 2^{O(n^4 (\log \alpha)^2)}$, $< m, x' > \; = \; 0$,
   where $m = \pm \widehat{b}_n \|\widehat{b}_n\|^{-2}$ holds for the terminal vector b_n of the algorithm.
2. $\lambda(\overline{x}) \geq \frac{\alpha}{2}$ *holds for all $\overline{x} \in \mathbb{R}^n$ with $\| \, x - \overline{x} \, \| < \| \, x - x' \, \|/2$*
3. *if $x = x'$ then $\| \, m \, \| < 2^{n/2} \lambda(x)$.*

Proof. **3.** If $x' = x$ then $\widehat{b}_{n,x} \neq 0$ and thus $m = a_n$ is an integer relation for x by Proposition 3.1 of [HJLS89]. The same proposition shows that the length of a_n is at most $2^{n/2 - 1} \min\{\lambda(x), \alpha\}$.
1. The inequality $\| \, m \, \| \leq 2^{O(n^4 (\log \alpha)^2)}$ follows from Proposition 2. If $x \neq x'$ we have $x' \in span(b_1, \ldots, b_{n-1})$ and thus $\widehat{b}_{n,x'} = \widehat{b}_n \neq 0$ which implies $< a_n, x' >= 0$. The equality $a_n = \pm \widehat{b}_n \|\widehat{b}_n\|^{-2}$ follows from $< a_n, x' >= 0 =< obin, x' >$, see Proposition 3.1 of [HJLS89].
2. For every $\overline{x}$ satisfying $\|\overline{x} - x\| < \|\widehat{x}_n\|/2$ Lemma 9 implies $\|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| < \|\widehat{b}_{i,x}\|$ and thus

$$\|\widehat{b}_{i,\overline{x}}\| \; > \; 0 \qquad \text{and} \qquad \|\widehat{b}_{i,\overline{x}}\| \; < \; 2 \, \alpha^{-1} \qquad \text{for } i = 1, \ldots, n-1 \; .$$

From inequality 1 we see that $\lambda(\overline{x}) \geq \frac{\alpha}{2}$ holds for all $\overline{x} \in \mathbb{R}^n$ with $\|x - \overline{x}\| < \|x - x'\| \, /2$.
□

6 Closeness of the approximation

We prove an upper and an lower bound on the distance $\|x - x'\|$ of the input vector x from the output vector x'. We comment on diophantine approximation.

Proposition 11. *For arbitrary real input $x \in \mathbb{R}^n$ and output (x', m) we have*
$\|x - x'\| \;\le\; \|x\|\,\alpha^{1-n} \,/\, \|m\|$.

Proof. Let $b_1, \ldots, b_n$ be the terminal basis and $a_1, \ldots, a_n$ its dual, $m := a_n$. We can assume that $x \neq x'$ since otherwise the claim is trivial. If $x \neq x'$ the vectors $x, b_1, ..., b_{n-1}$ form the basis of a lattice $L = L(x, b_1, ..., b_{n-1})$. Its determinant $det(L)$ is the volume of the parallelepiped generated by the basis. We can compute $det(L)$ as the product of the lengths of the Gram–Schmidt orthogonalization vectors. Applying this to the bases $x, b_1, ..., b_{n-1}$ and $b_1, ..., b_{n-1}, x$ we see that

$$\det(L(x, b_1, \ldots, b_{n-1})) \;=\; \|x\| \prod_{j=1}^{n-1} \|\widehat{b}_{j,x}\| \;=\; \left(\prod_{j=1}^{n-1} \|\widehat{b}_j\| \right) \|\widehat{x}_n\| \,.$$

Throughout the algorithm the basis $b_1, ..., b_n$ generates the lattice $\mathbb{Z}^n$ and thus

$$\det(L(b_1, \ldots, b_n)) \;=\; \prod_{j=1}^{n} \|\widehat{b}_j\| \;=\; 1 \,.$$

These equations imply $\|\widehat{b}_n\|^{-1} = \prod_{j=1}^{n-1} \|\widehat{b}_j\| = \prod_{j=1}^{n-1} \|\widehat{b}_{j,x}\|\; (\|x\| \,/\, \|\widehat{x}_n\|)$. From this and $\|a_n\| = \|\widehat{b}_{n,x'}\|^{-1} = \|\widehat{b}_n\|^{-1}$ we see that

$$\|x - x'\| \;=\; \|\widehat{x}_n\| \;=\; \frac{\|x\|}{\|a_n\|} \prod_{j=1}^{n-1} \|\widehat{b}_{j,x}\| \;\le\; \|x\|\,\alpha^{1-n}\,\|a_n\|^{-1} \,,$$

where we use that $\|\widehat{b}_{j,x}\| \le \alpha^{-1}$ for $j = 1, \ldots, n-1$. □

Proposition 11 raises the question whether the distance $\|x - x'\|$ is for random x on the average proportional to $\|x\|\,\alpha^{1-n} \,/\, \|m\|$. This point requires further study.

Proposition 12. *Let the input x be rational, $x = (p_1, \ldots, p_n)/q$ with $p_1, \ldots, p_n, q \in \mathbb{Z}$, and $x' \neq x$. Then we have* $\|x - x'\| \;\ge\; q^{-1}\, 2^{-O(n^4 + n^2 (\log \alpha)^2)}$.

Proof. Since the vector $a_n = \pm \widehat{b}_n \|\widehat{b}_n\|^{-2}$ is integer we see that

$$(x - x')\,\|\widehat{b}_n\|^{-2} \;= < x, \frac{\widehat{b}_n}{\|\widehat{b}_n\|^2} > \frac{\widehat{b}_n}{\|\widehat{b}_n\|^2}$$

is a rational vector with denominator q. Thus Proposition 2 implies

$$\|x - x'\| \;\ge\; q^{-1}\,\|\widehat{b}_n\|^{-2} \;\ge\; q^{-1}\, 2^{-O(n^4 + n^2 (\log \alpha)^2)} \,. \qquad \square$$

Remarks. 1. B. Just [Ju92] analyzes diophantine approximations obtained by a variant of the HJLS–algorithm on inputs of the special form $x = (x_1, \ldots, x_{n-1}, 1) \in \mathbb{R}^n$. Her algorithm is the HJLS–algorithm with full reduction in size so that, before swapping

b_{k-1}, b_k, size-reduction is performed on the vector b_k with respect to $b_{k-1}, \ldots, b_1$. Formula (17), [Ju92] shows that the final basis $b_1, \ldots, b_n$ (and every basis in the algorithm that precedes a swap of the last two vectors $b_n,\ b_{n-1}$) satisfies with $b_1 = (p_1, \ldots, p_{n-1}, q)$

$$\max_{1 \le i \le n-1} |x_i - \frac{p_i}{q}| \ \le \ \|\widehat{b}_{1,x}\| \, \|x\| \, / |q| \tag{8}$$

Moreover Theorem 7, [Ju92] bounds the error of the diophantine approximation as

$$\max_{1 \le i \le n-1} |x_i - \frac{p_i}{q}| \ \le \ \frac{2^{(n+2)/4} \, \|x\|}{|q|^{1+1/2n(n-1)}} \ . \tag{9}$$

This algorithmic result must be compared with the existential bound of HERMITE, where the right hand side of inequality (9) is $\|x\|/|q|^{1+1/(n-1)}$. LAGARIAS has shown that diophantine approximations can be constructed by the L^3–algorithm for lattice basis reduction so that the right hand side in (9) is $2^{n/2} n/|q|^{1+1/(n-1)}$ [La83]. However this result does not use a continued fraction type algorithm.

2. The analysis of Just does not apply directly to our polynomial time algorithm, and the Just algorithm is not polynomial time. However the Just analysis is valid if we change our algorithm to perform a full size–reduction in step 2.3 so that the vector b_k gets reduced with respect to $b_{k-1}, ..., b_1$. Then the inequalities (8) and (9) hold for every basis occuring in our algorithm immediately before a swap of the last two vectors b_{n-1}, b_n. In particular these inequalities hold for the final basis of our algorithm, no matter whether $x = x'$ or not.

If step 2.3 of our algorithm is changed to perform a full size–reduction then Theorem 10 remains valid, in particular the upper bound on the length of $a_n = m$ holds true. This is because the inequalities

$$\|a_i\| \ \le \ 2^{O(n^4 + n^2 (\log \alpha)^2)} \qquad \text{for } i = s, \ldots, n \, . \tag{10}$$

of Proposition 2 still hold throughout the algorithm. The reason is that the vectors a_j , b_j with $j < s$ cannot be exchanged with vectors a_i , b_i , $i \ge s$, nor can a_j be added to a_i during the reduction in size. Thus the vectors a_j with $j < s$ do not influence the vectors a_i with $i \ge s$ in step 2.3 at a later stage. On the other hand the coefficients $\mu_{k,j}$ with $j < s$ and the vectors b_1,...,b_m, a_1,...,a_{s-1} may become very large if x is irrational. This point requires further study.

Our algorithm with full size–reduction in step 2.3 distinguishes from the algorithm in [Ju92] only in that we use the Lovász exchange rule whereas Bergman's exchange rule is used in [Ju92] and in the HJLS–algorithm.

3. It may be of interest to note that clauses (2), (3) of Theorem 10 also remain valid if we change step 2.3 to perform a size–reduction restricted to $j = k - 1$ so that b_k gets merely reduced with respect to b_{k-1} before swapping b_k and b_{k-1} . Also clauses (2), (3) of Theorem 10 remain valid if we replace in our algorithm the Lovász exchange rule by the Bergman exchange rule which is used in the HJLS–algorithm. This means that clauses (2), (3) also hold for the HJLS–algorithm provided that the corresponding output (x', m) is added to this algorithm in case that $x' \neq x$.

References

[B80] G. BERGMAN: Notes on Ferguson and Forcade's generalized Euclidean algorithm. TR. Department of Mathematics, University of California, Berkeley, CA, 1980.

[Cla92] K.L. Clarkson: Safe and Effective Determinant Evaluation. Proc. 33rd IEEE Symp. on Foundations of Computer Science (1992), pp. 387–395.

[FF79] H. Ferguson and R. Forcade: Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two. Bull. Amer. Math. Soc., Vol. 1 (1979), pp. 912–914.

[He1845] C. Hermite: Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres, Deuxième lettre du 6 août 1845. J. Reine Angew. Math. **40** (1850), pp. 279–290.

[HJLS89] J. Hastad, B. Just, J.C. Lagarias and C.P. Schnorr: Polynomial Time Algorithms For Finding Integer Relations Among Real Numbers. SIAM J. Comput., Vol. 18, No. 5 (1989), pp. 859-881.

[Ju92] B. Just: Generalizing the Continued Fraction Algorithm to Arbitrary Dimensions. SIAM J. Comput., Vol. 21, No. 5 (1992), pp. 909-926.

[La83] J. Lagarias: Computational complexity of simutaneous diophantine approximation problems. Proc. 23rd IEEE Symp. on Foundations of Computer Science (1982), pp. 32–39.

[LLL82] A.K. Lenstra, H.W. Lenstra,Jr. and L. Lovász: Factoring Polynomials With Rational Coefficients. Math. Ann., 21 (1982), pp. 515-534.