Computation of Highly Regular Nearby Points

Carsten Rőssner* Claus P. Schnorr†

Dept. of Math./Comp. Science
University of Frankfurt
P. O. Box 11 19 32, 60054 Frankfurt on the Main, Germany

Abstract

We call a vector $x \in \mathbb{R}^n$ highly regular *if it satisfies $< x , m >= 0$ for some short, non–zero integer vector m where $< . , . >$ is the inner product. We present an algorithm which given $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{N}$ finds a highly regular nearby point x' and a short integer relation m for x'.*

The nearby point x' is 'good' in the sense that no short relation $\overline{m}$ of length less than $\alpha/2$ exists for points $\overline{x}$ within half the x'–distance from x. The integer relation m for x' is for random x up to an average 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.

1 Introduction

Let $L \subset \mathbb{R}^n$ be a lattice, i. e. a discrete subgroup of the real n–dimensional vector space that generates a linear subspace $span(L)$ of dimension n. Suppose we are given, e. g. by physical measurements, approximate lattice vectors $\overline{b_1}, \ldots, \overline{b_k}$, $k > n$. For nearly every lattice problem we need a basis and even a reduced basis of the lattice. However, the disturbed vectors $\overline{b_1}, \ldots, \overline{b_k}$ may generate a subgroup of the $\mathbb{R}^n$ that may be very different from L, possibly even non–discrete, so that it is impossible to obtain from $\overline{b_1}, \ldots, \overline{b_k}$ by unimodular basis transformations even an approximate basis of the lattice L. It is therefore necessary to correct $\overline{b_1}, \ldots, \overline{b_k}$. In the case $n = 1$ this amounts to replacing the given reals $\overline{x_i} = \overline{b_i}$ $i = 1, \ldots, k$ by the closest point $(x'_1, \ldots, x'_k)$ that admits $k - 1$ linear dependency relations that are linearly independent and have small integer coefficients. These linear relations define the generator of the lattice up to integer multiples. In this paper we propose an algorithm for solving this problem. For simplicity we concentrate on the case of single relations. The case of several linear independent integer relations can be solved by a straightforward extension of our algorithm.

The main problem solved in this paper can also be described as to find a stable version of the HJLS–algorithm of Hastad, Just, Lagarias and Schnorr [5] where the stability means that the algorithm corrects small distortions of the input. Interestingly, already the L^3–algorithm of Lenstra, Lenstra, Lovász [8] has the same stability problem in case that the given basis vectors are real vectors that are given with slight distortions. Following the analysis of Buchmann [2] the L^3–algorithm works fine if the distortions of the input are small compared to the first successive minimum λ_1 of the lattice. However, if λ_1 is arbitrarily small there is no way other than to correct the given input.

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 a nearby point x' and an integer relation m for x' satisfying

- $\lambda(\overline{x}) \geq \alpha/2$ holds for all $\overline{x} \in \mathbb{R}^n$ with $\|x - \overline{x}\| < \|x - x'\|/2$
- $\mathcal{E}_x(\|m\|/\lambda(x')) \leq 2^{n/2}$ where $\mathcal{E}_x$ is the expected value for random x with $\|x\| = 1$
- $\|m\| \leq 2^{O(n^4(\log \alpha)^2)}$
- if $x = x'$ then $\|m\| \leq 2^{\frac{n-2}{2}} \min\{ \lambda(x) , \alpha \}$.

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

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 $\alpha/2$. The integer relation m is for random x up to an average factor $2^{n/2}$ a shortest integer relation for x'. It is also short in an absolute sense satisfying the crude upper bound $\|m\| \leq 2^{O(n^4(\log \alpha)^2)}$.

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 above stated properties of the ouput (x', m) do not only hold for the input x but they hold for every $\overline{x}$ 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 [7]. However this does not exclude that a much closer point $\overline{x}$ admits a much shorter integer relation. 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 [5]. For given x, α the HJLS–algorithm either finds an integer relation m for x with $\|m\|^2 \leq 2^{n-2} \min\{ \lambda(x)^2, \alpha^2 \}$ or it proves that $\lambda(x) \geq \alpha$.

Our algorithm may be important in case that the given x is slightly inaccurate and one searches for a nearby point having a very short integer relation. We are not aware of any previous algorithm for solving this problem. The new algorithm can be extended to find for given $x \in \mathbb{R}^n$ and $r \in \mathbb{N}$ a nearby point x' that admits r linearly independent short integer relations $m_1, \ldots, m_r$. Our algorithm is a stable variant of the HJLS–algorithm, which in turn is a variation of both the L^3–algorithm of Lenstra, Lenstra and Lovász [8] and the generalized continued fraction algorithm presented by Bergman [1] in his notes on Ferguson and Forcade's generalized Euclidean algorithm [4].

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

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

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

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

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

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

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

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

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

$$\tfrac{3}{4} \|\pi_{k-1,x}(b_{k-1})\|^2 \leq \|\pi_{k-1,x}(b_k)\|^2$$

holds for $k = 2, \ldots, n$.
The latter inequality is equivalent to

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

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 algorithm

The new algorithm relies on the HJLS–algorithm of Hastad, Just, Lagarias and Schnorr. Given $x \in \mathbb{R}^n$

and $\alpha \in \mathbb{N}$ the HJLS–algorithm either finds an integer relation m for x with $\|m\|^2 \le 2^{n-2} \min\{ \lambda(x)^2 , \alpha^2 \}$ or it proves that $\lambda(x) \ge \alpha$. We will use Proposition 3.1 of [5] which states that

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

holds for every basis $b_1, \ldots, b_n$ of the lattice $\mathbb{Z}^n$. This inequality already appears in somewhat weaker form in [4].

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

$$\|a_n\| \le 2^{n/2} \, \alpha \ .$$

Stability analysis. In Lemma 5(2) we show for $i = 1, \ldots, n-1$ the inequalities

$$\begin{aligned} \|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| \ &\le \ \|\widehat{b}_{i,x}\| \, \frac{2 \, \|\widehat{x}_i - \widehat{\overline{x}}_i\|}{\max\{\|\widehat{x}_{i+1}\| \, , \, \|\widehat{\overline{x}}_{i+1}\|\}} \\ &\le \ \|\widehat{b}_{i,x}\| \, \frac{2 \, \|x - \overline{x}\|}{\|\widehat{x}_n\|} \qquad (2) \end{aligned}$$

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

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

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

$$\begin{aligned} \|x - \overline{x}\| \ &< \ \|\widehat{x}_n\|/2 \qquad (4) \\ \|\widehat{b}_{i,x}\| \ &\le \ 2 \, \alpha^{-1} \qquad \text{for } i = 1, \ldots, n \qquad (5) \end{aligned}$$

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

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

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

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

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

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 4 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 (SIRA)

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 $j = 1, \ldots, k-1$, $s \le k$,
   $c_1, \ldots, c_{s-1} \le \alpha^{-2}$,
   $\pi_{s,x}(b_s), \ldots, \pi_{s,x}(b_{k-1})$ is L^3–reduced. *

   $c_k :=< b_k, b_k >$;

IF $k = s = 1$ **THEN**
$c_1 := < b_1, b_1 > - < b_1, b_0 >^2 / c_0$;
$\mu_{1,0} := < b_1, b_0 > / c_0$;
IF $c_1 \leq \alpha^{-2}$ **THEN** $s := 2$;
$k := 2$; $c_2 := < b_2, b_2 >$;

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 $1c_j > 0$ 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 $\pi_{s,x}(b_s), \ldots, \pi_{s,x}(b_{k-1})$. □

Several linear independent integer relations. Modifying the termination condition in step 2.1 as '$c_k = 0$ **AND** $k < n - r + 1$' yields an algorithm which solves the problem of finding r linearly independent integer relations for a nearby point x' to the given input $x \in \mathbb{R}^n$. We only have to compute x' as $x' := x - \widehat{x}_{n-r+1}$. Then the last r vectors $a_{n-r+1}, \ldots, a_n$ of the dual basis are r linearly independent integer relations for x'. Our analysis given below applies to this case as well.

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*

$$\|a_k\| \, , \; \|b_k\| \; \leq \; 2^{O(n^4 + n^2 (\log \alpha)^2)} \, , \; k = 1, \ldots, n \, .$$

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 [5]. 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

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

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. The following can be proved by straightforward induction, see [9].

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

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

2. For every pass of step 2.3 we have

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

3. Upon entry of step 2.3 we have that

$$|\mu_{k,i}| \;\le\; 2^{n/2-1} \alpha \sqrt{n} \, , \; s \le i \le k-1 .$$

4. 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 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 Lemma 4(4) yields

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

The claim on the vectors a_k of the dual basis holds by symmetry. □

Lemma 5 *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.*

1. *$\|\pi_x(b) - \pi_{\overline{x}}(b)\| \;\le\; \frac{2\|b\| \, \|x - \overline{x}\|}{\max\{\|x\| \, , \, \|\overline{x}\|\}}$ holds for all $b \in \mathbb{R}^n$.*
2. *For every basis $b_1, \ldots, b_n \in \mathbb{Z}^n$ and $\widehat{x}_n := \pi_n(x)$ we have*

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

3. *For the terminal basis $b_1, \ldots, b_n$ and the output x' of SIRA we have*

$$\|\widehat{b}_{i,x} - \widehat{b}_{i,x'}\| \;\le\; \|\widehat{b}_{i,x}\| \, , \; i = 1, \ldots, n-1 .$$

Proof. **1.** Following Clarkson, [3] Lemma 3.2, we have

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

This and the Cauchy–Schwarz inequality imply

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

which proves the claim.

2. We apply (1) with $b = \widehat{b}_i$, $x = \widehat{x}_i$, $\overline{x} = \widehat{\overline{x}}_i$. Using $\pi_{\widehat{x}_i}(\widehat{b}_i) = \widehat{b}_{i,x}$ this yields

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

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

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

3. We see from $\widehat{b}_{i,x} = \widehat{b}_i - \frac{<\widehat{b}_i, \widehat{x}_i>}{\|\widehat{x}_i\|^2}\,\widehat{x}_i$ and $<\widehat{b}_i, \widehat{x}_i> = <\widehat{b}_i, \widehat{x}'_i>$ that

$$\|\widehat{b}_{i,x} - \widehat{b}_{i,x'}\| = |<\widehat{b}_i, \widehat{x}_i>|\,\|\frac{\widehat{x}_i}{\|\widehat{x}_i\|^2} - \frac{\widehat{x}'_i}{\|\widehat{x}'_i\|^2}\|\quad.$$

The inequality $\|\frac{b}{\|b\|^2} - \frac{c}{\|c\|^2}\| \leq \frac{\|b-c\|}{\|b\|\,\|c\|}$ and Cauchy's inequality yield

$$\begin{aligned} \|\widehat{b}_{i,x} - \widehat{b}_{i,x'}\| &\leq \frac{\|\widehat{b}_i\|\,\|\widehat{x}'_i\|\,\|\widehat{x}_i - \widehat{x}'_i\|}{\|\widehat{x}_i\|\,\|\widehat{x}'_i\|} = \frac{\|\widehat{b}_i\|\,\|\widehat{x}_n\|}{\|\widehat{x}_i\|} \\ &= \frac{\|\widehat{b}_{i,x}\|\,\|\widehat{x}_n\|}{\|\widehat{x}_{i+1}\|} \leq \|\widehat{b}_{i,x}\|\,. \qquad \square \end{aligned}$$

Main Theorem 6 *For arbitrary input $x \in \mathbb{Q}^n$, $\alpha \in \mathbb{N}$ SIRA produces a pair of dual terminal bases $b_1, \ldots, b_n$ and $a_1, \ldots, a_n$ and a nearby point $x' \in \mathbb{Q}^n$ and $m \in \mathbb{Z}^n$ such that*

1. $<m, x'> = 0$, *where* $m = a_n = \pm\widehat{b}_n\|\widehat{b}_n\|^{-2}$.
2. $\lambda(\overline{x}) \geq \alpha/2$ *holds for all* $\overline{x} \in \mathbb{R}^n$ *with* $\|x - \overline{x}\| < \|x - x'\|/2$.
3. $\mathcal{E}_x(\|m\|/\lambda(x')) \leq 2^{n/2}$ *holds for random* x, $\|m\| \leq 2^{O(n^4(\log\alpha)^2)}$.
4. *If* $x = x'$ *then* $\|m\|^2 \leq 2^{n-2}\,\min\{\,\lambda(x)^2\,,\,\alpha^2\,\}$.

Note that (4) has been proved by [5].

Proof. **1.** The output vector x' is in $span(b_1, \ldots, b_{n-1})$ no matter whether $x = x'$ or $x \neq x'$. Therefore $\widehat{b}_{n,x'} = \widehat{b}_n \neq 0$ which implies $<a_n, x'> = 0$. Since both $\widehat{b}_n$ and a_n are orthogonal to $x, b_1, \ldots, b_{n-1}$ and $<a_n, b_n> = 1$ we must have $a_n = \pm\widehat{b}_n\|\widehat{b}_n\|^{-2}$, $\|a_n\| = \|\widehat{b}_n\|^{-1} = \|\widehat{b}_{n,x'}\|^{-1}$.

2. For every $\overline{x}$ satisfying $\|\overline{x} - x\| < \|\widehat{x}_n\|/2$ Lemma 5(2) implies $\|\widehat{b}_{i,x} - \widehat{b}_{i,\overline{x}}\| < \|\widehat{b}_{i,x}\|$ and thus

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

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

3. Proposition 2 implies the rather crude upper bound $\|m\| \leq 2^{O(n^4(\log\alpha)^2)}$. We now prove that $\mathcal{E}_x(\|a_n\|/\lambda(x')) \leq 2^{n/2}$. Let $x \neq x'$ since otherwise the claim follows from (4). We see from $\lambda(x') \geq 1/\max_i\|\widehat{b}_{i,x'}\|$ and $\|a_n\| = \|\widehat{b}_{n,x'}\|^{-1}$ that

$$\begin{aligned} \frac{\|a_n\|}{\lambda(x')} &\leq \max_{1\leq i\leq n-1}\frac{\|\widehat{b}_{i,x'}\|}{\|\widehat{b}_{n,x'}\|} \\ &= \max_{1\leq i\leq n-1}\frac{\|\widehat{b}_{i,x'}\|}{\|\widehat{b}_{i,x}\|}\,\frac{\|\widehat{b}_{i,x}\|}{\|\widehat{b}_{n-1,x}\|}\,\frac{\|\widehat{b}_{n-1,x}\|}{\|\widehat{b}_{n,x'}\|}\,, \end{aligned}$$

where $\|\widehat{b}_{i,x}\|/\|\widehat{b}_{n-1,x}\| \leq 2^{\frac{n-i-1}{2}}$ since the basis $b_1, \ldots, b_n$ is L^3–reduced under the orthogonal projection into $span(x)^\perp$. From this and the inequality $\|\widehat{b}_{i,x'}\| \leq 2\,\|\widehat{b}_{i,x}\|$, which follows from Lemma 5(2) and $\widehat{b}_{n,x'} = \widehat{b}_n$, we infer

$$\frac{\|a_n\|}{\lambda(x')} \leq 2\cdot 2^{\frac{n-i-1}{2}}\,\frac{\|\widehat{b}_{n-1,x}\|}{\|\widehat{b}_{n,x'}\|} \leq 2^{n/2}\,\frac{\|\widehat{b}_{n-1,x}\|}{\|\widehat{b}_n\|}\quad.$$

Now the claim follows from $\mathcal{E}_x(\|\widehat{b}_{n-1,x}\|/\|\widehat{b}_n\|) \leq 1$ which is proved below.

Proof of $\mathcal{E}_x(\|\widehat{b}_{n-1,x}\|/\|\widehat{b}_n\|) \leq 1$ for random x.

Let b_{n-1}^{old}, b_{n-1}^{new} denote the vector b_{n-1} before and after the last swap $b_{n-1} \longleftrightarrow b_n$. We have $b_n = b_{n-1}^{old}$, $\pi_n(b_n) = \widehat{b}_n$ and thus

$$\frac{\|\widehat{b}_{n-1,x}\|}{\|\widehat{b}_n\|} = \frac{\|\widehat{b}_{n-1,x}\|}{\|\widehat{b}_{n-1,x}^{old}\|}\,\frac{\|\pi_{n-1,x}(b_n)\|}{\|\pi_n(b_n)\|}\,,$$

where $\pi_{n-1,x}(b_n)$, $\pi_n(b_n)$ are the parts of $\pi_{n-1}(b_n)$ that are orthogonal to $\widehat{x}_{n-1}$ and $\widehat{b}_{n-1}$. Due to the L^3–reduction $\widehat{b}_{n-1}/\|\widehat{b}_{n-1}\|$ is a close approximation to $\widehat{x}_{n-1}/\|\widehat{x}_{n-1}\|$ so that $\|\pi_{n-1,x}(b_n)\|/\|\pi_n(b_n)\|$ approaches 1. This follows from the error bounds for diophantine approximation by the generalized continued fraction algorithm proved in [6].

Moreover b_{n-1}^{old} is the vector b_n^{new} after the last swap $b_{n-1} \longleftrightarrow b_n$. The L^3–reduction subsequent to the last swap $b_{n-1} \longleftrightarrow b_n$ can still increase $\widehat{b}_{n-1,x}^{new}$ to the final $\widehat{b}_{n-1,x}$. However, for random x we must

have $\mathcal{E}_x(\|\widehat{b}_{n-1,x}\|/\|\widehat{b}^{old}_{n-1,x}\|) \leq 1$ since the last swap $b_{n-1} \longleftrightarrow b_n$ decreases

$$|\det[x, b_1, \ldots, b_{n-1}]| = \|x\| \, \|\widehat{b}_{1,x}\| \cdots \|\widehat{b}_{n-1,x}\|$$

and thus decreases, together with the subsequent L^3–reduction, each $\mathcal{E}_x(\|\widehat{b}_{i,x}\|)$ for $i = 1, \ldots, n-1$. Even so the case $\|\widehat{b}_{n-1,x}\| > \|\widehat{b}^{old}_{n-1,x}\|$ is not impossible it is very unlikely. □

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'.

Proposition 7 *For arbitrary real input $x \in \mathbb{R}^n$ and output (x', m) we have*

$$\|x - x'\| \leq \|x\| \, \alpha^{1-n} \, / \, \|m\| \, .$$

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

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

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

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

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

Proposition 7 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 8 *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*

$$\|x - x'\| \geq q^{-1} \, 2^{-O(n^4 + n^2 (\log \alpha)^2)} \, .$$

Proof. Since the vector $a_n = \pm \widehat{b}_n \|\widehat{b}_n\|^{-2}$ is integer and x' is of the special form 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

$$\begin{aligned} \|x - x'\| &\geq q^{-1} \, \|\widehat{b}_n\|^2 = q^{-1} \, \|a_n\|^{-2} \\ &\geq q^{-1} \, 2^{-O(n^4 + n^2 (\log \alpha)^2)} \, . \end{aligned}$$ □

References

[1] G. Bergman, "Notes on Ferguson and Forcade's Generalized Euclidean Algorithm", *TR, Department of Mathematics, University of California*, Berkeley, CA, 1980.

[2] J. Buchmann, "Reducing Lattice Bases by Means of Approximations", *Proc. 1st Algorithmic Number Theory Symposium*, Ithaca, NY, 1994.

[3] K.L. Clarkson, "Safe and Effective Determinant Evaluation", *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, pp. 387–395, 1992.

[4] 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, pp. 912–914, 1979.

[5] 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, pp. 859–881, 1989.

[6] B. Just, "Generalizing the Continued Fraction Algorithm to Arbitrary Dimensions", *SIAM J. Comput.*, Vol. 21, No. 5, pp. 909–926, 1992.

[7] J. Lagarias, "Computational Complexity of Simutaneous Diophantine Approximation Problems", *Proc. 23rd IEEE Symp. on Foundations of Computer Science*, pp. 32–39, 1982.

[8] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, "Factoring Polynomials With Rational Coefficients", *Math. Ann.*, Vol. 21 , pp. 515–534, 1982.

[9] C. Rőssner and C.P. Schnorr, "A Stable Integer Relation Algorithm", *TR-94-016, ICSI*, Berkeley, 1994.