THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth
Algorithmic Number Theory Symposium

Finding simultaneous Diophantine approximations with prescribed quality

Wieb Bosma and Ionica Smeets

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.167

Finding simultaneous Diophantine approximations with prescribed quality

Wieb Bosma and Ionica Smeets

We give an algorithm that finds a sequence of approximations with Dirichlet coefficients bounded by a constant only depending on the dimension. The algorithm uses LLL lattice basis reduction. We present a version of the algorithm that runs in polynomial time of the input.

1. Introduction

The regular continued fraction algorithm is a classical algorithm to approximate reals by rational numbers. The denominators of continued fraction convergents furnish, for every $a \in \mathbb{R}$, infinitely many integers q such that

$$\|q\,a\| < q^{-1},$$

where $\|x\|$ denotes the distance between x and the nearest integer. The exponent -1 of q is minimal; if it is replaced by any number $e < -1$, then there exist real numbers a such that only finitely many integers q satisfy $\|q\,a\| < q^e$.

Hurwitz [9] proved that the continued fraction algorithm finds, for every $a \in \mathbb{R} \setminus \mathbb{Q}$, an infinite sequence of increasing integers q_n with

$$\|q_n\,a\| < \frac{1}{\sqrt{5}}\,q_n^{-1}.$$

If the constant $1/\sqrt{5}$ is replaced by any smaller one, then this statement is false. Legendre [15] showed that the continued fraction algorithm finds all good approximations, in the sense that if for some positive integer q

$$\|q\,a\| < \tfrac{1}{2}\,q^{-1},$$

then q is one of the q_n found by the algorithm.

MSC2010: primary 11J13; secondary 11Y16, 11J70.
Keywords: simultaneous Diophantine approximation, LLL lattice reduction.

As to the generalization of approximations in higher dimensions Dirichlet [16] proved the following theorem; see Chapter II of [19].

Theorem 1.1. *Let an $n \times m$ matrix A with entries $a_{ij} \in \mathbb{R} \setminus \mathbb{Q}$ be given and suppose that $1, a_{i1}, \dots, a_{im}$ are linearly independent over $\mathbb{Q}$ for some i with $1 \le i \le n$. There exist infinitely many coprime m-tuples of integers $(q_1, \dots, q_m)$ such that, with $q = \max_j |q_j| \ge 1$, we have*

$$\max_i \|q_1 a_{i1} + \dots + q_m a_{im}\| < q^{-m/n}. \tag{1}$$

If the exponent $-m/n$ is replaced by any smaller number, there exists a matrix A for which the inequality holds for only finitely many coprime tuples $(q_1, q_2, \dots, q_m)$.

Definition 1.2. Let an $n \times m$ matrix A with entries $a_{ij} \in \mathbb{R} \setminus \mathbb{Q}$ be given. The *Dirichlet coefficient* of an m-tuple $(q_1, \dots, q_m)$ is $q^{m/n} \max_i \|q_1 a_{i1} + \dots + q_m a_{im}\|$.

The proof of the theorem does not give an efficient way of finding a series of approximations with a Dirichlet coefficient less than 1. For the case $m = 1$ the first multidimensional continued fraction algorithm was given by Jacobi [10]. Many more followed, see for instance Perron [18], Brun [5; 6], Lagarias [14] and Just [11]. Brentjes [4] gives a detailed history and description of such algorithms. Schweiger's book [20] gives a broad overview. For $n = 1$ there is, amongst others, the algorithm by Ferguson and Forcade [8]. However, there is no efficient algorithm guaranteed to find a series of approximations with Dirichlet coefficient smaller than 1.

In 1982 the LLL algorithm for lattice basis reduction was published in [17]. The authors noted that their algorithm could be used for finding Diophantine approximations of given rationals with Dirichlet coefficient only depending on the dimension; see Corollary 2.4. Just [11] developed an algorithm based on lattice reduction that detects $\mathbb{Z}$-linear dependence in the a_i, in the case $m = 1$. If no such dependence is found her algorithm returns integers q with

$$\max_i \|q a_i\| \le c \left(\sum_{i=1}^{n} a_i^2 \right)^{1/2} q^{-1/(2n(n-1))},$$

where c is a constant depending on n. The exponent $-1/(2n(n-1))$ is larger than the Dirichlet exponent $-1/n$. Lagarias [13] used the LLL algorithm in a series of lattices to find good approximations for the case $m = 1$. Let $a_1, \dots, a_n \in \mathbb{Q}$ and let N be a positive integer; suppose there exists $Q \in \mathbb{N}$ with $1 \le Q \le N$ such that $\max_j \|Q a_j\| < \varepsilon$. Then Lagarias's algorithm on input $a_1, \dots, a_n$ and N finds in polynomial time a q with $1 \le q \le 2^{n/2} N$ such that $\max_j \|q a_j\| \le \sqrt{5n} 2^{(n-1)/2} \varepsilon$. One difference with our work is that Lagarias focuses on the quality $\|q a_j\|$, while we focus on the Dirichlet coefficient $q^{1/n} \|q a_j\|$. We also consider the case $m > 1$.

The main result of the present paper is an algorithm that by iterating the LLL algorithm gives a series of approximations of given rationals with optimal Dirichlet exponent. Where the LLL algorithm gives one approximation, our dynamic algorithm gives a series of successive approximations. To be more precise: For a given $n \times m$-matrix A with entries $a_{ij} \in \mathbb{Q}$ and a given upper bound $q_{\max}$ the algorithm returns a sequence of m-tuples $(q_1, \dots, q_m)$ such that for every Q with $2^{(m+n+3)(m+n)/(4m)} \le Q \le q_{\max}$ one of these m-tuples satisfies

$$\max_j |q_j| \le Q$$

and

$$\max_i \|q_1 a_{i1} + \dots + q_m a_{im}\| \le 2^{(m+n+3)(m+n)/(4n)} Q^{-m/n}.$$

The exponent $-m/n$ of Q can not be improved, and therefore we say that these approximations have *optimal Dirichlet exponent*.

Our algorithm is a multidimensional continued fraction algorithm in the sense that we work in a lattice basis and that we only interchange basis vectors and add integer multiples of basis vectors to another. Our algorithm differs from other multidimensional continued fraction algorithms in that the lattice is not fixed across iterations. In Lemma 3.6 we show that if there exists an extremely good approximation, our algorithm finds a very good one. We derive in Theorem 3.8 how the output of our algorithm gives a lower bound on the quality of possible approximations with coefficients up to a certain limit. In Section 4 we show that a slightly modified version of our algorithm runs in polynomial time. In Section 5 we present some numerical data.

An earlier version of this paper appeared as Chapter V of Smeets's thesis [21].

2. Lattice reduction and the LLL algorithm

In this section we give the definitions and results that we need for our algorithm.

Let r be a positive integer. A subset L of the r-dimensional real Euclidean vector space $\mathbb{R}^r$ is called a *lattice* if there exists a basis $b_1, \dots, b_r$ of $\mathbb{R}^r$ such that

$$L = \sum_{i=1}^{r} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{r} z_i b_i \;\middle|\; z_i \in \mathbb{Z} \text{ for } i = 1, \dots, r \right\}.$$

We say that $b_1, \dots, b_r$ is a *basis* for L. The *determinant* of the lattice L is defined by $|\det(b_1, \dots, b_r)|$ and we denote it as $\det L$.

For any linearly independent $b_1, \dots, b_r \in \mathbb{R}^r$ the Gram-Schmidt process yields an orthogonal basis $b_1^*, \dots, b_r^*$ for $\mathbb{R}^r$, defined inductively by

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \quad \text{for } 1 \le i \le r$$

and

$$\mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)},$$

where $(\,,\,)$ denotes the ordinary inner product on $\mathbb{R}^r$.

We call a basis $b_1, \ldots, b_r$ for a lattice L *reduced* if

$$|\mu_{ij}| \le \tfrac{1}{2} \qquad \text{for } 1 \le j < i \le r$$

and

$$\left|b_i^* + \mu_{ii-1} b_{i-1}^*\right|^2 \le \tfrac{3}{4}|b_{i-1}^*|^2 \qquad \text{for } 1 \le i \le r,$$

where $|x|$ denotes the Euclidean length of x.

Proposition 2.1 [17, Proposition 1.6]. *Let $b_1, \ldots, b_r$ be a reduced basis for a lattice L in $\mathbb{R}^r$. Then*

(1) $|b_1| \le 2^{(r-1)/4}\,(\det L)^{1/r}$,

(2) $|b_1|^2 \le 2^{r-1}\,|x|^2$ *for every nonzero $x \in L$,*

(3) $\prod_{i=1}^{r} |b_i| \le 2^{r(r-1)/4} \det L$.

Proposition 2.2 [17, Proposition 1.26]. *Let $L \subset \mathbb{Z}^r$ be a lattice with a basis $b_1, b_2, \ldots, b_r$, and let $F \in \mathbb{R}$, $F \ge 2$, be such that $|b_i|^2 \le F$ for $1 \le i \le r$. Then the number of arithmetic operations needed by the LLL algorithm is $O(r^4 \log F)$ and the integers on which these operations are performed each have binary length $O(r \log F)$.*

In the following lemma the approach suggested in the original LLL-paper for finding (simultaneous) Diophantine approximations is generalized to the case $m > 1$.

Lemma 2.3. *Let an $n \times m$-matrix A with entries $a_{ij} \in \mathbb{R}$ and an $\varepsilon \in (0, 1)$ be given. Let L be the lattice formed by the columns of the $(m+n) \times (m+n)$-matrix*

$$B = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_{11} & \cdots & a_{1m} \\ 0 & 1 & & 0 & a_{21} & \cdots & a_{2m} \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & a_{n1} & \cdots & a_{nm} \\ 0 & \cdots & 0 & 0 & c & & 0 \\ \vdots & & \vdots & \vdots & & \ddots & \\ 0 & \cdots & 0 & 0 & 0 & & c \end{bmatrix}, \qquad (2)$$

with $c = (2^{-(m+n-1)/4}\varepsilon)^{(m+n)/m}$.

The LLL algorithm applied to L will yield an m-tuple $(q_1, \dots, q_m)$ of integers with

$$\max_j |q_j| \le 2^{(m+n-1)(m+n)/(4m)} \varepsilon^{-n/m} \tag{3}$$

and

$$\max_i \|q_1 a_{i1} + \dots + q_m a_{im}\| \le \varepsilon.$$

Proof. The LLL algorithm finds a reduced basis $b_1, \dots, b_{m+n}$ for the lattice L. For each vector b in this basis there exist $p_i \in \mathbb{Z}$, for $1 \le i \le n$, and $q_j \in \mathbb{Z}$, for $1 \le j \le m$, such that

$$b = \begin{bmatrix} q_1 a_{11} + \dots + q_m a_{1m} - p_1 \\ \vdots \\ q_1 a_{n1} + \dots + q_m a_{nm} - p_n \\ c q_1 \\ \vdots \\ c q_m \end{bmatrix}.$$

Proposition 2.1(i) gives an upper bound for the length of the first basis vector,

$$|b_1| \le 2^{(m+n-1)/4} c^{m/(m+n)}.$$

From this vector b_1 we find integers $q_1, \dots, q_m$, such that

$$\max_j |q_j| \le 2^{(m+n-1)/4} c^{-n/(m+n)} \tag{4}$$

and

$$\max_i \|q_1 a_{i1} + \dots + q_m a_{im}\| \le 2^{(m+n-1)/4} c^{m/(m+n)}. \tag{5}$$

Substituting $c = (2^{-(m+n-1)/4} \varepsilon)^{(m+n)/m}$ gives the results. □

From (4) and (5) we obtain the following corollary.

Corollary 2.4. *For any $n \times m$-matrix A with entries $a_{ij} \in \mathbb{R}$ the LLL algorithm can be used to obtain an m-tuple $(q_1, \dots, q_m)$ that satisfies, with $q = \max_j |q_j|$,*

$$\max_i \|q_1 a_{i1} + \dots + q_m a_{im}\| \le 2^{(m+n-1)(m+n)/(4n)} q^{-m/n}.$$

3. The iterated LLL algorithm

We iterate the LLL algorithm over a series of lattices to find a sequence of approximations. We start with a lattice determined by a basis of the form (2). After the LLL algorithm finds a reduced basis for this lattice, we decrease the constant c by dividing the last m rows of the matrix by a constant d greater than 1. By doing so, ε is divided by $d^{m/(m+n)}$. We repeat this process until the upper bound (3) for $\max |q_j|$ guaranteed by the LLL algorithm exceeds a given upper bound $q_{\max}$.

To ease notation we put $d = 2$ and $\varepsilon = 1/2$.

Algorithm 3.1 (Iterated LLL algorithm (ILLL)).

Input: An $n \times m$-matrix A with entries a_{ij} in $\mathbb{R}$, and an upper bound $q_{\max} > 1$.

Output: For each integer $k \geq 1$ no larger than the k' defined in (8), a vector $q(k) \in \mathbb{Z}^m$ with

$$\max_j |q_j(k)| \leq 2^{(m+n-1)(m+n)/(4m)}\, 2^{kn/m} \tag{6}$$

and

$$\max_i \|q_1(k)\, a_{i1} + \cdots + q_m(k)\, a_{im}\| \leq 1/2^k. \tag{7}$$

1. Construct the basis matrix B as given in (2) from A.
2. Apply the LLL algorithm to B.
3. Deduce $q_1, \dots, q_m$ from the first vector in the reduced basis returned by the LLL algorithm.
4. Divide the last m rows of B by $2^{(m+n)/m}$
5. Stop if the upper bound for q guaranteed by the algorithm (6) exceeds $q_{\max}$; else go to Step 2.

Remark 3.2. The number $2^{(m+n)/m}$ in Step 4 may be replaced by $d^{(m+n)/m}$ for any real number $d > 1$. When we additionally set $\varepsilon = 1/d$ this yields

$$\max_j |q_j(k)| \leq 2^{(m+n-1)(m+n)/(4m)} d^{kn/m}$$

and

$$\max_i \|q_1(k)a_{i1} + \cdots + q_m(k)a_{im}\| < d^{-k}.$$

In this paper, with the exception of the numerical examples in Section 5, we always take $d = 2$ and $\varepsilon = 1/2$.

Define

$$k' := \left\lceil -\frac{(m+n-1)(m+n)}{4n} + \frac{m \log_2 q_{\max}}{n} \right\rceil. \tag{8}$$

Lemma 3.3. *Let an $n \times m$-matrix A with entries a_{ij} in $\mathbb{R}$ and an upper bound $q_{\max} > 1$ be given. With this input, the number of times the ILLL algorithm applies the LLL algorithm equals k' from* (8).

Proof. One derives the number of iterations by solving k from the stopping criterion (6)

$$q_{\max} \leq 2^{(m+n-1)(m+n)/(4m)} 2^{kn/m},$$

that is:

$$\frac{m}{n}\log_2 q_{\max} \le \frac{(m+n-1)(m+n)}{4n} + k.$$

We stop iterating as soon as the integer k reaches the ceiling k' as in (8). □

For each $k \ge 1$ we define

$$c(k) = (2^{-k-(m+n-5)/4}\varepsilon)^{(m+n)/m}.$$

Note that $c(1)$ is the constant c from Lemma 2.3. In the k-th iteration we are working in the lattice defined by the basis in (2) with c replaced by $c(k)$.

Lemma 3.4. *The output* $q(k) = (q_1(k), q_2(k), \dots, q_m(k))$ *of the ILLL algorithm satisfies* (6) *and* (7), *for* $1 \le k \le k'$.

Proof. Since we take $\varepsilon = 1/2$, in the k-th iteration we use

$$c(k) = (2^{-k-(m+n-1)/4})^{(m+n)/m}.$$

Substituting $c(k)$ for c in (4) and (5) yields (6) and (7), respectively. □

The following theorem gives the main result of the present paper, as mentioned in the introduction. The algorithm returns a sequence of approximations with all coefficients smaller than Q, optimal Dirichlet exponent and Dirichlet coefficient only depending on the dimensions m and n.

Theorem 3.5. *Let an* $n \times m$*-matrix* A *with entries* a_{ij} *in* $\mathbb{R}$, *and* $q_{\max} > 1$ *be given. The ILLL algorithm finds a sequence of* m*-tuples* $(q_1, \dots, q_m)$ *of integers such that for every* Q *with* $2^{(m+n+3)(m+n)/(4m)} \le Q \le q_{\max}$ *one of these* m*-tuples satisfies*

$$\max_j |q_j| \le Q \quad \text{and}$$

$$\max_i \|q_1 a_{i1} + \cdots + q_m a_{im}\| \le 2^{(m+n+3)(m+n)/(4n)} Q^{-m/n}.$$

Proof. Take $k \in \mathbb{N}$ such that

$$2^{(k-1)n/m} \le Q \cdot 2^{4m/((m+n+3)(m+n))} < 2^{kn/m}. \tag{9}$$

From Lemma 3.4 we know that $q(k) = (q_1(k), q_2(k), \dots, q_m(k))$ satisfies the inequality

$$\max_j |q_j(k)| \le 2^{(m+n+3)(m+n)/(4m)}\, 2^{(k-1)n/m} \le Q.$$

From the right side of inequality (9) it follows that

$$\frac{1}{2^k} < 2^{(m+n+3)(m+n)/(4n)} Q^{-m/n}.$$

From Lemma 3.4 and this inequality we derive that

$$\max_i \|q_1(k)\, a_{i1} + \cdots + q_m(k)\, a_{im}\| \leq \frac{1}{2^k} < 2^{(m+n+3)(m+n)/(4n)} Q^{-m/n}. \quad \square$$

Proposition 2.1(2) guarantees that if there exists an extremely short vector in the lattice, then the LLL algorithm finds a rather short lattice vector. We extend this result to the realm of successive approximations. In the next lemma we show that for every very good approximation (satisfying (11)), the ILLL algorithm finds a rather good one (satisfying (14)) not too far away from it (as specified by (13)).

Lemma 3.6. *Let an $n \times m$-matrix A with entries a_{ij} in $\mathbb{R}$, a real number $0 < \delta < 1$, and an integer $s > 1$ be given. If there exists an m-tuple $(s_1, \ldots, s_m)$ of integers with*

$$s = \max_j |s_j| > 2^{(m+n-1)n/(4m)} \left(\frac{n\delta^2}{m}\right)^{n/(2(m+n))} \tag{10}$$

and

$$\max_i \|s_1 a_{i1} + \cdots + s_m a_{im}\| \leq \delta s^{-m/n}, \tag{11}$$

then applying the ILLL algorithm with

$$q_{\max} > 2^{(m^2+m(n-1)+4n)/(4m)} \left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s \tag{12}$$

yields an m-tuple $(q_1, \ldots, q_m)$ of integers with

$$\max_j |q_j| \leq 2^{(m^2+m(n-1)+4n)/(4m)} \left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s \tag{13}$$

and

$$\max_i \|q_1 a_{i1} + \cdots + q_m a_{im}\| \leq 2^{(m+n)/2} \sqrt{n}\delta s^{-m/n}. \tag{14}$$

Proof. Let $1 \leq k \leq k'$ be an integer. Proposition 2.1(2) gives that for each m-tuple $q(k)$ found by the algorithm, we have

$$\sum_{i=1}^{n} \|q_1(k)a_{i1} + \cdots + q_m(k)a_{im}\|^2 + c(k)^2 \sum_{j=1}^{m} q_j(k)^2$$
$$\leq 2^{m+n-1} \Bigg(\sum_{i=1}^{n} \|s_1 a_{11} + \cdots + s_m a_{im}\|^2 + c(k)^2 \sum_{j=1}^{m} s_j^2 \Bigg).$$

From this and (10) and (11) it follows that

$$\max_i \|q_1(k)a_{i1} + \cdots + q_m(k)a_{im}\|^2 \leq 2^{m+n-1} \big(n\delta^2 s^{-2m/n} + c(k)^2 m s^2 \big). \tag{15}$$

Take the smallest positive integer K such that

$$c(K) \le \sqrt{\frac{n}{m}}\,\delta s^{-(m+n)/n}. \tag{16}$$

We find for the K-th iteration from (15) and (16)

$$\max_i \|q_1(K)a_{i1} + \cdots + q_m(K)a_{im}\| \le 2^{(m+n)/2}\sqrt{n}\delta s^{-m/n},$$

which gives (14).

We show that under assumption (12) the ILLL algorithm performs at least K iterations. We may assume $K > 1$, since the ILLL algorithm always performs at least 1 iteration. From Lemma 3.3 we find that if $q_{\max}$ satisfies

$$q_{\max} > 2^{Kn/m}2^{(m+n-1)(m+n)/(4m)},$$

then the ILLL algorithm performs at least K iterations. Our choice of K implies

$$c(K-1) = \frac{c(1)}{2^{(m+n)(K-2)/m}} = \frac{2^{-(m+n+3)(m+n)/(4m)}}{2^{(m+n)(K-2)/m}} > \sqrt{\frac{n}{m}}\delta s^{-(m+n)/n},$$

and we obtain

$$2^{Kn/m} < 2^{-(m+n-5)n/(4m)}\left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s.$$

From this we find that

$$q_{\max} > 2^{(m^2+m(n-1)+4n)/(4m)}\left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s$$

is a sufficient condition to guarantee that the algorithm performs at least K iterations.

Furthermore, either $2^{-(m+n)/m}\sqrt{n/m}\,\delta s^{-(m+n)/n} < c(K)$ or $K = 1$. In the former case we find from (4) that

$$\max_j |q_j(K)| \le 2^{(m+n-1)/4}c(K)^{-n/(m+n)} < 2^{(m+n-1)/4}2^{n/m}\left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s.$$

In the latter case we obtain from (4) that

$$\max_j |q_j(1)| \le 2^{(m+n-1)/4}c(1)^{-n/(m+n)} = 2^{(m+n-1)/4}2^{(m+n+3)n/(4m)}$$

and, by (10),

$$\begin{aligned} 2^{(m+n-1)/4}2^{(m+n+3)n/(4m)} &= 2^{(m+n-1)/4}2^{n/m}2^{(m+n-1)n/(4m)} \\ &< 2^{(m+n-1)/4}2^{n/m}\left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s. \end{aligned}$$

We conclude that for all $K \geq 1$,

$$\max_j |q_j(K)| \leq 2^{(m^2+m(n-1)+4n)/(4m)} \left(\frac{m}{n\delta^2}\right)^{n/(2(m+n))} s. \qquad \square$$

From (13) and (14) we obtain the following corollary.

Corollary 3.7. *With the assumptions of Lemma* 3.6, *the ILLL algorithm can be used to obtain an m-tuple $(q_1, \dots, q_m)$ of integers that satisfies*

$$q^{m/n} \max_i \|q_1 a_{i1} + \cdots + q_m a_{im}\| \\ \leq 2^{(m^2+m(3n-1)+4n+2n^2)/(4n)} m^{m/(2(m+n))} (n\delta^2)^{n/(2(m+n))},$$

where again $q = \max_j |q_j|$.

Theorem 3.8. *Let an $n \times m$-matrix A with entries a_{ij} in $\mathbb{R}$ and $q_{\max} > 1$ be given. Assume that γ is such that for every m-tuple $(q_1, \dots, q_m)$ returned by the ILLL algorithm, we have*

$$q^{m/n} \max_i \|q_1 a_{i1} + \dots q_m a_{im}\| > \gamma, \quad \textit{where } q = \max_j |q_j|. \tag{17}$$

Set

$$\delta = 2^{-(m+n)(m^2+m(3n-1)+4n+2n^2)/(4n^2)} m^{-m/(2n)} n^{-1/2} \gamma^{(m+n)/n}. \tag{18}$$

Let $(s_1, \dots, s_m)$ be an m-tuple of integers, and set $s = \max_j |s_j|$. If

$$s > 2^{(m+n-1)n/(4m)} \left(\frac{n\delta^2}{m}\right)^{n/(2(m+n))} \tag{19}$$

and

$$s < 2^{-(m^2+m(n-1)+4n)/(4m)} \left(\frac{n\delta^2}{m}\right)^{n/(2(m+n))} q_{\max} \tag{20}$$

then

$$s^{m/n} \max_i \|s_1 a_{i1} + \cdots + s_m a_{im}\| > \delta. \tag{21}$$

Proof. Assume that every vector returned by our algorithm satisfies (17) and that there exists an m-tuple $(s_1, \dots, s_m)$ satisfying (19) and (20) but not satisfying Equation (21). From Equation (20) it follows that $q_{\max}$ satisfies (12). We apply Lemma 3.6 and find that the algorithm finds an m-tuple $(q_1, \dots, q_m)$ that satisfies (17). Substituting δ as given in (18) gives

$$q^{m/n} \max_i \|q_1 a_{i1} + \cdots + q_m a_{im}\| \leq \gamma,$$

in contradiction with our assumption. $\square$

4. A polynomial time version of the ILLL algorithm

We have used real numbers in our theoretical results, but in a practical implementation of the algorithm we only use rational numbers. Without loss of generality we may assume that these numbers are in the interval $[0, 1]$. In this section we describe the changes to the algorithm and we show that this modified version of the algorithm runs in polynomial time.

As input for the rational algorithm we take

- the dimensions m and n,
- a rational number $\varepsilon \in (0, 1)$,
- an integer M that is large compared to $\frac{(m+n)^2}{m} - \frac{m+n}{m} \log \varepsilon$,
- an $n \times m$-matrix A with entries $0 < a_{ij} \leq 1$, where each $a_{ij} = p_{ij}/2^M$ for some integer p_{ij},
- an integer $q_{\max} < 2^M$.

Remark 4.1. In this rational algorithm all irrational numbers are approximated by rational numbers with denominator 2^M. Thus M denotes the precision that is used.

When we construct the matrix B in Step 1 of the ILLL algorithm we approximate c as given in (2) by a rational number

$$\hat{c} = 2^{-M} \lceil 2^M c \rceil = 2^{-M} \left\lceil 2^M \left(2^{-(m+n-1)/4} \varepsilon\right)^{(m+n)/m} \right\rceil. \tag{22}$$

Hence $c < \hat{c} \leq c + 2^{-M}$.

In iteration k we use a rational $\hat{c}\,(k)$ that for $k \geq 2$ is given by

$$\hat{c}\,(k) = 2^{-M} \left\lceil 2^M \hat{c}\,(k-1) 2^{-(m+n)/m} \right\rceil \quad \text{and} \quad \hat{c}\,(1) = \hat{c} \text{ as in (22),}$$

and we change Step 4 of the ILLL algorithm to "Multiply the last m rows of B by $\hat{c}\,(k-1)/\,\hat{c}\,(k)$." The other steps of the rational iterated algorithm are as described in Section 3.

The running time of the rational algorithm.

Theorem 4.2. *Let the input be given as described above. Then the number of arithmetic operations needed by the ILLL algorithm and the binary length of the integers on which these operations are performed are both bounded by a polynomial in m, n, and M.*

Proof. The number of times we apply the LLL algorithm is not changed by rationalizing c, so we find the number of iterations k' from Lemma 3.3

$$k' = \left\lceil -\frac{(m+n-1)(m+n)}{4n} + \frac{m \log_2 q_{\max}}{n} \right\rceil < \left\lceil \frac{mM}{n} \right\rceil.$$

It is obvious that Steps 1, 3, 4 and 5 of the algorithm are polynomial in the size of the input and we focus on the LLL-step. We determine an upper bound for the length of a basis vector used at the beginning of an iteration in the ILLL algorithm.

In the first application of the LLL algorithm the length of the initial basis vectors as given in (2) is bounded by

$$|b_i|^2 \le \max_j \left\{1, a_{1j}^2 + \cdots + a_{nj}^2 + m\hat{c}^{\,2}\right\} \le m+n \quad \text{for } 1 \le i \le m+n,$$

where we use that $0 < a_{ij} < 1$ and $\hat{c} \le 1$.

The input of each following application of the LLL algorithm is derived from the reduced basis found in the previous iteration by making some of the entries strictly smaller. Part (2) of Proposition 2.1 yields that for every vector b_i in a reduced basis we have

$$|b_i|^2 \le 2^{(m+n)(m+n-1)/2} (\det L)^2 \prod_{\substack{j=1 \\ j \ne i}}^{m+n} |b_i|^{-2}.$$

The determinant of our starting lattice is given by $\hat{c}^{\,m}$ and the determinants of all subsequent lattices are strictly smaller. Every vector b_i in the lattice is at least as long as the shortest nonzero vector in the lattice. Thus for each i we have $|b_i|^2 \ge \frac{1}{2^M}$. Combining this yields

$$|b_i|^2 \le 2^{(m+n+2M)(m+n-1)/2}\, \hat{c}^{\,2m} \le 2^{(m+n+2M)(m+n-1)/2}$$

for every vector used as input for the LLL-step after the first iteration.

Thus we have

$$|b_i|^2 < \max\left\{m+n\,,\ 2^{(m+n+2M)(m+n-1)/2}\right\} = 2^{(m+n+2M)(m+n-1)/2} \tag{23}$$

for any basis vector that is used as input for an LLL-step in the ILLL algorithm.

Proposition 2.2 shows that for a given basis $b_1, \dots, b_{m+n}$ for $\mathbb{Z}^{m+n}$ with $F \in \mathbb{R}$, $F \ge 2$ such that $|b_i|^2 \le F$ for $1 \le i \le m+n$ the number of arithmetic operations needed to find a reduced basis from this input is $O((m+n)^4 \log F)$. For matrices with entries in $\mathbb{Q}$ we need to clear denominators before applying this proposition. Thus for a basis with basis vectors $|b_i|^2 \le F$ and rational entries that can all be written as fractions with denominator 2^M the number of arithmetic operations is $O((m+n)^4 \log(2^{2M} F))$.

Combining this with (23) and the number of iterations yields the theorem. □

Approximation results from the rational algorithm. Assume that the input matrix A (with entries $a_{ij} = 2^{-M} p_{ij} \in \mathbb{Q}$) is an approximation of an $n \times m$-matrix $\mathcal{A}$

(with entries $\alpha_{ij} \in \mathbb{R}$), found by putting $a_{ij} = 2^{-M}\lceil 2^M \alpha_{ij} \rceil$. In this subsection we derive the approximation results guaranteed by the rational iterated algorithm for the $\alpha_{ij} \in \mathbb{R}$.

According to (4) and (5) the LLL algorithm, applied with $\hat{c}$ instead of c, is guaranteed to find an m-tuple $(q_1, \dots, q_m)$ such that

$$q = \max_j |q_j| \le 2^{(m+n-1)(m+n)/(4m)} \varepsilon^{-n/m}$$

and

$$\begin{aligned}\max_i \|q_1 a_{i1} + \cdots + q_m a_{im}\| \\ &\le 2^{(m+n-1)/4}\left(\left(2^{-(m+n-1)/4}\varepsilon\right)^{(m+n)/m} + 2^{-M}\right)^{m/(m+n)} \\ &\le \varepsilon + 2^{(m+n-1)/4 - Mm/(m+n)},\end{aligned}$$

the last inequality following from the fact that $(x+y)^\alpha \le x^\alpha + y^\alpha$ if $\alpha < 1$ and $x, y > 0$.

For the α_{ij} we find that

$$\begin{aligned}\max_i \|q_1 \alpha_{i1} + \cdots + q_m \alpha_{im}\| \\ &\le \max_i \|q_1 a_{i1} + \cdots + q_m a_{im}\| + mq\, 2^{-M} \\ &\le \varepsilon + 2^{(m+n-1)/4 - Mm/(m+n)} + m\, \varepsilon^{-n/m}\, 2^{(m+n-1)(m+n)/(4m) - M}.\end{aligned}$$

In the introduction to Section 4 we have chosen M large enough to guarantee that the error introduced by rationalizing the entries is negligible.

We show that the difference between $\hat{c}\,(k)$ and $c(k)$ is bounded by $2/2^M$.

Lemma 4.3. *For each integer* $k \ge 0$,

$$c(k) \le \hat{c}\,(k) < c(k) + 2^{-M} \sum_{i=0}^{k} 2^{-i(m+n)/m} < c(k) + \frac{2}{2^M}.$$

Proof. We use induction. For $k = 0$ we have $\hat{c}\,(0) = 2^{-M}\left\lceil c(0) 2^M \right\rceil$ and trivially

$$c(0) \le \hat{c}\,(0) < c(0) + \frac{1}{2^M}.$$

Assume that

$$c(k-1) \le \hat{c}\,(k-1) < c(k-1) + 2^{-M} \sum_{i=0}^{k-1} 2^{-i(m+n)/m}$$

and consider $\hat{c}\,(k)$. From the definition of $\hat{c}\,(k)$ and the induction assumption it follows that

$$\begin{aligned}\hat{c}\,(k) &= 2^{-M}\left\lceil \hat{c}\,(k-1)\,2^{-(m+n)/m}2^{M}\right\rceil \\ &\geq 2^{-(m+n)/m}\,\hat{c}\,(k-1) \geq 2^{-(m+n)/m}\,c(k-1) = c(k)\end{aligned}$$

and

$$\begin{aligned}\hat{c}\,(k) &= 2^{-M}\left\lceil \hat{c}\,(k-1)\,2^{-(m+n)/m}2^{M}\right\rceil \\ &< 2^{-(m+n)/m}\,\hat{c}\,(k-1) + 2^{-M} \\ &< 2^{-(m+n)/m}\Bigl(c(k-1) + 2^{-M}\sum_{i=0}^{k-1} 2^{-i(m+n)/m}\Bigr) + 2^{-M} \\ &= c(k) + 2^{-M}\sum_{i=0}^{k} 2^{-i(m+n)/m}.\end{aligned}$$

Finally note that $\sum_{i=0}^{k} 2^{-i(m+n)/m} < 2$ for all k. $\square$

One can derive analogues of Theorem 3.5, Lemma 3.6 and Theorem 3.8 for the polynomial version of the ILLL algorithm by carefully adjusting for the introduced error. We do not give the details, since in practice this error is negligible.

5. Experimental data

In this section we present some experimental data from the rational ILLL algorithm. In our experiments we choose the dimensions m and n and iteration speed d, so $\varepsilon = \frac{1}{d}$. We fill the $m \times n$ matrix A with random numbers in the interval [0, 1] and repeat the entire ILLL algorithm for a large number of these random matrices to find our results. First we look at the distribution of the approximation quality. Then we look at the growth of the denominators q found by the algorithm.

The distribution of the approximation qualities. For one-dimensional continued fractions the approximation coefficients Θ_k are defined as

$$\Theta_k = q_k^2 \left| a - \frac{p_k}{q_k} \right|,$$

where p_k/q_k is the kth convergent of a.

For the multidimensional case we define Θ_k in a similar way:

$$\Theta_k = q(k)^{m/n} \max_i \|q_1(k)\,a_{i1} + \cdots + q_m(k)\,a_{im}\|.$$

The one-dimensional case $m = n = 1$. We compare the distribution of the Θ_k found by the ILLL algorithm for $m = n = 1$ and various values of d with the distribution of the Θ_k as produced by the continued fraction algorithm with the best approximation properties. For this optimal continued fraction algorithm it was shown in [2] that for almost all a, the limit

$$\lim_{N\to\infty} \frac{1}{N}\#\{k : 1 \le k \le N \text{ and } \Theta_k \le z\}$$

is equal to $F(z)$, where

$$F(z) = \begin{cases} \dfrac{z}{\log G} & \text{if } 0 \le z \le 1/\sqrt{5},\\[2ex] \dfrac{1}{\log G}\left(\sqrt{1-4z^2} + \log\left(G\dfrac{1-\sqrt{1-4z^2}}{2z}\right)\right) & \text{if } 1/\sqrt{5} \le z \le 1/2,\\[2ex] 1 & \text{if } 1/2 \le z \le 1, \end{cases}$$

with $G = (\sqrt{5}+1)/2$.

The optimal continued fraction algorithm finds rational approximations of which the denominators grow with maximal rate, and it finds all approximations with $\Theta_k < 1/2$; for all this, see [1; 2; 3].

The following figures display distribution functions for Θ_k; that is, we show the fraction of the Θ_k found up to the value given on the horizontal axis.

We plot the distribution of the Θ_k found by the ILLL algorithm for $m = n = 1$ and $d = 2$ in Figure 1. The ILLL algorithm might find the same approximation more than once. We see in Figure 1 that for $d = 2$ the distribution function differs depending on whether we leave in the duplicates or sort them out. With the duplicate approximations removed the distribution of Θ_k strongly resembles $F(z)$ of the optimal continued fraction. The duplicates that the ILLL algorithm finds are usually good approximations: If they are much better than necessary they will also be an admissible solution in the next few iterations.

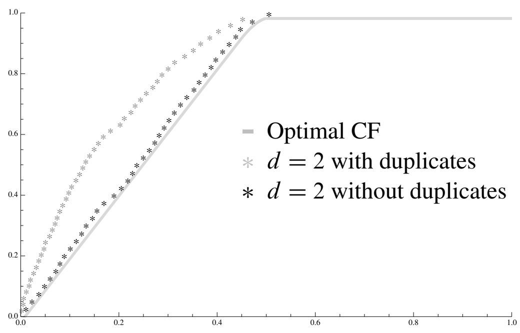

Figure 1. Distribution function for Θ_k from ILLL with $m = n = 1$ and $d = 2$, with and without the duplicate approximations, compared to that of Θ_k for optimal continued fractions.

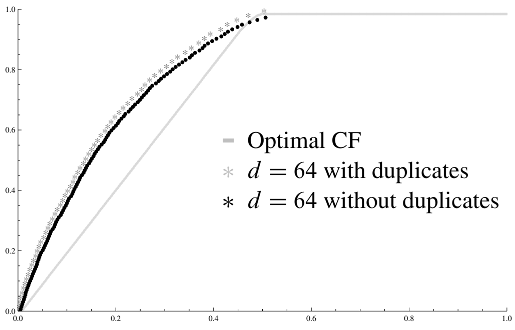

Figure 2. Distribution function for Θ_k from ILLL with $m = n = 1$ and $d = 64$, with and without the duplicate approximations, compared to that of Θ_k for optimal continued fractions.

For larger d we do not find so many duplicates, because the quality has to improve much more in every iteration; also see Figure 2 for an example with $d = 64$.

From now on we remove duplicates from our results.

The multidimensional case. In this section we show some results for the distribution of the Θ_k's found by the ILLL algorithm. For fixed m and n there also appears to be a limit distribution for Θ_k as d grows. See Figure 3 (right) for an example with $m = 3$ and $n = 2$, and compare this with the left half of the same figure. In this section we fix $d = 512$.

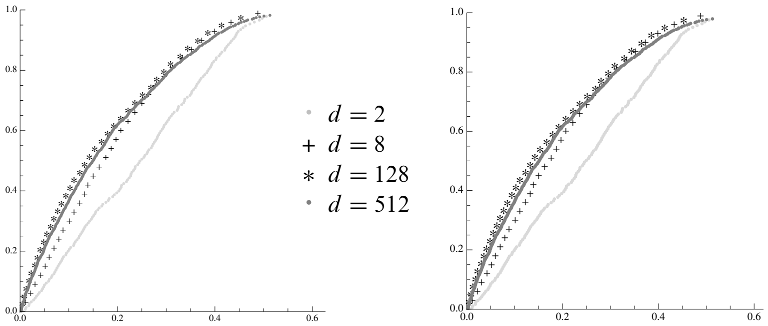

Figure 3. Distribution function for Θ_k from ILLL (with duplicates removed) for $d = 2, 8, 128$ and 512. Left: $m = n = 1$. Right: $m = 3$ and $n = 2$.

In Figure 4 we show some distributions for cases where either m or n is 1.

In Figure 5 we show some distributions for cases where $m = n$.

Remark 5.1. Very rarely the ILLL algorithm returns an approximation with $\Theta_k > 1$.

The denominators q. For regular continued fractions, denominators grow exponentially fast; to be more precise, for almost all x we have (see Section 3.5 of [7])

$$\lim_{k\to\infty} q_k^{1/k} = e^{\pi^2/(12\log 2)},$$

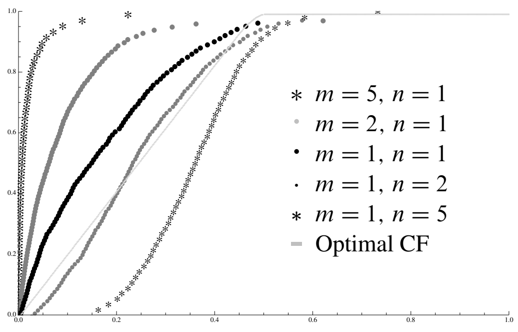

Figure 4. Distribution for Θ_k from ILLL when either $m = 1$ or $n = 1$.

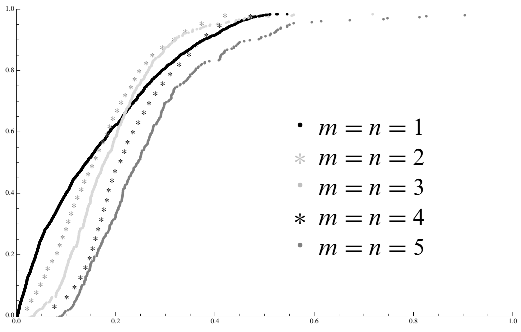

Figure 5. Distribution of Θ_k from ILLL when $m = n$.

For optimal continued fractions, the constant $\pi^2/(12\log 2)$ in this expression is replaced by $\pi^2/(12\log G)$, where $G = (\sqrt{5}+1)/2$. For multidimensional continued fraction algorithms little is known about the distribution of the denominators q_j. Lagarias defined in [12] the notion of a best simultaneous Diophantine approximation and showed that for the ordered denominators $1 = q_1 < q_2 < \cdots$ of best approximations for $a_1, \dots, a_n$ we have

$$\lim_{k\to\infty} \inf q_k^{1/k} \geq 1 + \frac{1}{2^{n+1}}.$$

We look at the growth of the denominators $q = \max_j |q_j|$ that are found by the ILLL algorithm. Dirichlet's Theorem 1.1 suggests that if q grows exponentially with a rate of m/n, then infinitely many approximations with Dirichlet coefficient smaller than 1 can be found. In the iterated LLL algorithm it is guaranteed by (6) that $q(k)$ is smaller than a constant times $d^{kn/m}$. Our experiments indicate that $q(k)$ is about $d^{kn/m}$, or equivalently that $e^{(m\log q_k)/(kn)}$ is about d; see Figure 6, which gives a histogram of solutions that satisfy $e^{(m\log q_k)/(kn)} = x$.

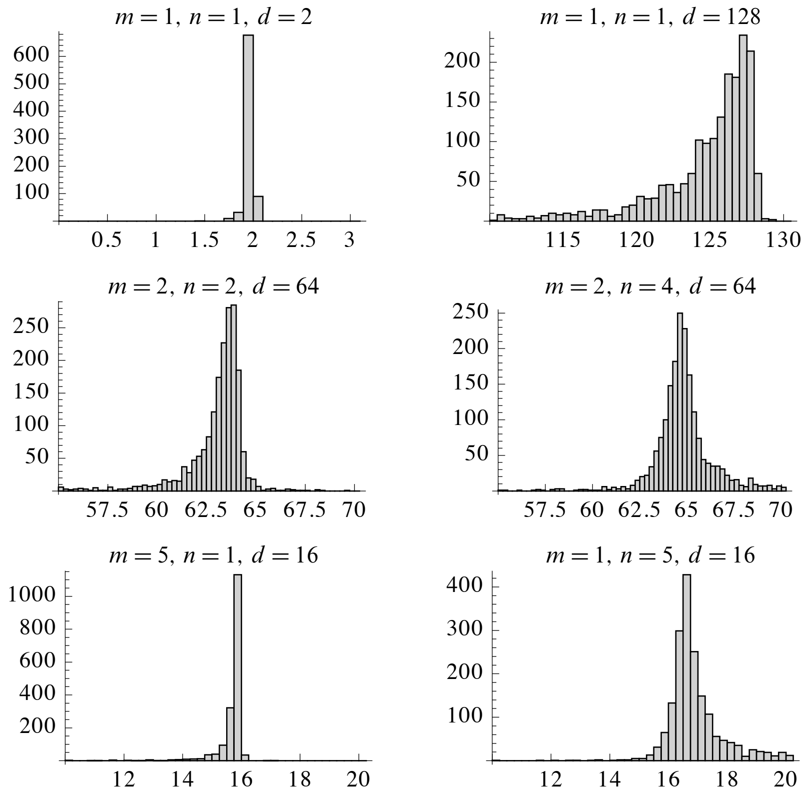

Figure 6. Histograms of $e^{(m \log q(k))/(kn)}$ for various values of m, n and d. In these experiments we used $q_{\max} = 10^{40}$ and repeated the ILLL algorithm $\lfloor 2000/k' \rfloor$ times, with k' from Lemma 3.3.

References

[1] Wieb Bosma, *Optimal continued fractions*, Nederl. Akad. Wetensch. Indag. Math. **49** (1987), no. 4, 353–379. http://dx.doi.org/10.1016/1385-7258(87)90001-1 MR 89b:40001

[2] Wieb Bosma and Cor Kraaikamp, *Metrical theory for optimal continued fractions*, J. Number Theory **34** (1990), no. 3, 251–270. MR 91d:11095

[3] ———, *Optimal approximation by continued fractions*, J. Austral. Math. Soc. Ser. A **50** (1991), no. 3, 481–504. MR 92f:11093

[4] A. J. Brentjes, *Multidimensional continued fraction algorithms*, Mathematical Centre Tracts, no. 145, Mathematisch Centrum, Amsterdam, 1981. http://tinyurl.com/brentjes145 MR 83b:10038

[5] Viggo Brun, *En generalisation av kjedebrøken, I*, Skr. Vidensk. Selsk. Kristiania I **1919** (1919), no. 6, 1–29, with an abstract in French. http://archive.org/stream/skrifterutgitavv1917chri#page/n764/ JFM 47.0168.01

[6] ———, *En generalisation av kjedebrøken, II*, Skr. Vidensk. Selsk. Kristiania I **1920** (1920), no. 6, 1–24, with an abstract in French. http://archive.org/stream/skrifterutgitavv201chri#page/n460/ JFM 47.0168.01

[7] Karma Dajani and Cor Kraaikamp, *Ergodic theory of numbers*, Carus Mathematical Monographs, no. 29, Mathematical Association of America, Washington, DC, 2002. MR 2003f:37014

[8] H. R. P. Ferguson and R. W. Forcade, *Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), no. 6, 912–914. MR 80i:10039

[9] A. Hurwitz, *Ueber die angenäherte Darstellung der Zahlen durch rationale Brüche*, Math. Ann. **44** (1894), no. 2-3, 417–436. MR 1510845

[10] C. G. J. Jacobi, *Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus* drei *vorhergehenden gebildet wird*, J. Reine Angew. Math. **69** (1868), 29–64.

[11] Bettina Just, *Generalizing the continued fraction algorithm to arbitrary dimensions*, SIAM J. Comput. **21** (1992), no. 5, 909–926. MR 93k:11065

[12] J. C. Lagarias, *Best simultaneous Diophantine approximations. I. Growth rates of best approximation denominators*, Trans. Amer. Math. Soc. **272** (1982), no. 2, 545–554. MR 84d:10039a

[13] ———, *The computational complexity of simultaneous Diophantine approximation problems*, SIAM J. Comput. **14** (1985), no. 1, 196–209. MR 86m:11048

[14] ———, *Geodesic multidimensional continued fractions*, Proc. London Math. Soc. (3) **69** (1994), no. 3, 464–488. MR 95j:11066

[15] A. M. Legendre, *Essai sur la théorie des nombres*, Chez Duprat, Paris, 1798. http://gallica.bnf.fr/ark:/12148/btv1b8626880r

[16] G. Lejeune Dirichlet, *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einige Anwendungen auf die Theorie der Zahlen*, Verh. Kön. Preuss. Akad. Wiss. (1842), 93–95, reprinted in *Mathematische Werke*, I, edited by L. Kronecker (G. Reimer, Berlin, 1889, and Chelsea, Bronx, NY, 1969, two volumes in one), pp. 635–638. http://books.google.com/books?id=cihJAAAAcAAJ&pg=PA93

[17] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR 84a:12002

[18] Oskar Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus*, Math. Ann. **64** (1907), no. 1, 1–76. MR 1511422

[19] Wolfgang M. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics, no. 785, Springer, Berlin, 1980. MR 81j:10038

[20] Fritz Schweiger, *Multidimensional continued fractions*, Oxford University Press, Oxford, 2000. MR 2005i:11090

[21] Ionica Smeets, *On continued fraction algorithms*, Ph.D. thesis, Leiden University, 2010. http://www.math.leidenuniv.nl/scripties/SmeetsThesis.pdf

WIEB BOSMA: bosma@math.ru.nl
Mathematics Department, Radboud University Nijmegen, PO Box 9010, 6500 Nijmegen, The Netherlands

IONICA SMEETS: ionica.smeets@gmail.com
Mathematical Institute, Leiden University, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS