Approximating Good Simultaneous Diophantine Approximations is almost NP-hard

Carsten Rössner and Jean-Pierre Seifert*

Dept. of Math. Comp. Science,
University of Frankfurt, P. O. Box 111932,
60054 Frankfurt/Main, Germany
{roessner,seifert}@cs.uni-frankfurt.de

Abstract. Given a real vector $\alpha=(\alpha_1,\ldots,\alpha_d)$ and a real number $\varepsilon > 0$ a good Diophantine approximation to α is a number Q such that $\|Q\alpha \bmod \mathbb{Z}\|_\infty \leq \varepsilon$, where $\|\cdot\|_\infty$ denotes the ℓ_∞-norm $\|\mathbf{x}\|_\infty := \max_{1\leq i\leq d} |x_i|$ for $\mathbf{x} = (x_1,\ldots,x_d)$.

Lagarias [12] proved the **NP**-completeness of the corresponding decision problem, i.e., given a vector $\alpha \in \mathbb{Q}^d$, a rational number $\varepsilon > 0$ and a number $N \in \mathbb{N}_+$, decide whether there exists a number Q with $1 \leq Q \leq N$ and $\|Q\alpha \bmod \mathbb{Z}\|_\infty \leq \varepsilon$.

We prove that, unless $\mathbf{NP} \subseteq \mathbf{DTIME}(n^{\mathrm{poly}(\log n)})$, there exists no polynomial-time algorithm which computes on inputs $\alpha \in \mathbb{Q}^d$ and $N \in \mathbb{N}_+$ a number Q^* with $1 \leq Q^* \leq 2^{\log^{0.5-\gamma} d} N$ and

$$\|Q^*\alpha \bmod \mathbb{Z}\|_\infty \leq 2^{\log^{0.5-\gamma} d} \min_{1\leq q\leq N} \|q\alpha \bmod \mathbb{Z}\|_\infty,$$

where γ is an arbitrary small positive constant. To put it in other words, it is almost **NP**–hard to approximate a minimum good Diophantine approximation to α in polynomial-time within a factor $2^{\log^{0.5-\gamma} d}$ for an arbitrary small positive constant γ.

We also investigate the nonhomogeneous variant of the good Diophantine approximation problem, i.e., given vectors $\alpha, \beta \in \mathbb{Q}^d$, a rational number $\varepsilon > 0$ and a number $N \in \mathbb{N}_+$, decide whether there exists a number Q with $1 \leq Q \leq N$ and $\|Q\alpha - \beta \bmod \mathbb{Z}\|_\infty \leq \varepsilon$.

This problem is particularly interesting since finding good nonhomogeneous Diophantine approximations enables us to factor integers and compute discrete logarithms (see Schnorr [17]).

We prove that the problem Good Nonhomogeneous Diophantine Approximation is **NP**-complete and even approximating it in polynomial-time within a factor $2^{\log^{1-\gamma} d}$ for an arbitrary small positive constant γ is almost **NP**-hard.

Our results follow from recent work in the theory of probabilistically checkable proofs [4] and 2-prover 1-round interactive proof-systems [7, 14].

Key Words. approximation algorithm, computational complexity, **NP**-hard, probabilistically checkable proofs, Diophantine approximation, 2-prover 1-round interactive proof-systems

* Supported by DFG under grant DFG-Leibniz-Programm Schn 143/5-1

1 Introduction

Since **NP** optimization problems are unlikely to be solved in polynomial-time, unless **P** = **NP**, a lot of work has been done to find polynomial-time approximation algorithms for these problems. An algorithm is said to *approximate* a positive real-valued function $opt(\cdot)$ *within a factor* f if on every input I its output is within a factor f of $opt(I)$.

Unfortunately, for many **NP**-hard optimization problems it is even **NP**-hard or almost **NP**-hard to compute such approximate solutions, see, e.g., Crescenzi and Kann [6] or Arora and Lund [3]. Therefore, it is quite important, both from the practical point of view and from the point of view of complexity theory, to find conditions which enable or disable us to design polynomial-time approximation algorithms for **NP**-hard optimization problems

In this paper we investigate the approximability of the following **NP** optimization problems:

MINIMUM GOOD DIOPHANTINE APPROXIMATION in ℓ_∞-norm (MINGDA$_\infty$)
INSTANCE: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and a number $N \in \mathbb{N}$
SOLUTION: A number $Q \in [1, N] \cap \mathbb{Z}$
MEASURE: The ℓ_∞-norm $\|Q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty := \max_{1 \le i \le d} \min_{n \in \mathbb{Z}} |Q\alpha_i - n|$.

MINIMUM GOOD NONHOMOGENEOUS DIOPHANTINE APPROXIMATION in ℓ_∞-norm (MINGNDA$_\infty$)
INSTANCE: Rational vectors $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d), \boldsymbol{\beta} = (\beta_1, \ldots, \beta_d) \in \mathbb{Q}^d$ and a number $N \in \mathbb{N}$
SOLUTION: A number $Q \in [1, N] \cap \mathbb{Z}$
MEASURE: The ℓ_∞-norm $\|Q\boldsymbol{\alpha} - \boldsymbol{\beta} \bmod \mathbb{Z}\|_\infty := \max_{1 \le i \le d} \min_{n \in \mathbb{Z}} |Q\alpha_i - \beta_i - n|$.

We refer to MINGDA$_\infty$ and MINGNDA$_\infty$ also as the problem Minimum Good Simultaneous Diophantine Approximation and Minimum Good Nonhomogeneous Simultaneous Diophantine Approximation, respectively, and to the solution $Q \in [1, N] \cap \mathbb{Z}$ as the common denominator of the good (nonhomogeneous) simultaneous diophantine approximation.

In fact, good simultaneous diophantine approximations have wide practical impact. Algorithms for finding such approximations may be used to find strongly polynomial-time algorithms in combinatorial optimization [8], to factor univariate integer polynomials [18] and to compute minimal polynomials of an algebraic number [11].

The motivation for our first result comes from the following conjecture raised by Lagarias [12]: If there is a polynomial-time algorithm which computes on inputs $\boldsymbol{\alpha} \in \mathbb{Q}^d$ and $N \in \mathbb{N}_+$ a denominator $Q^* \in [1, f(d)N]$ satisfying

$$\|Q^*\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \le f(d) \min_{1 \le q \le N} ||q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty,$$

where $f(d)$ is some polynomial in d, then **P** = **NP**. Conversely, Lagarias gave an algorithm which computes for inputs $\boldsymbol{\alpha} \in \mathbb{Q}^d$ and $N \in \mathbb{N}_+$ a denominator

$Q^* \in [1, 2^{d/2}N]$ satisfying

$$\|Q^*\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \sqrt{5d}\, 2^{(d-1)/2} \min_{1 \leq q \leq N} ||q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty.$$

We prove, that approximating MINGDA$_\infty$ in polynomial-time within a factor $2^{\log^{0.5-\gamma} d}$ for an arbitrary small positive constant γ implies **NP** $\subseteq$ **DTIME**$(n^{\mathrm{poly}(\log n)})$. Thus, in the sense of Lagarias' conjecture, our result may be regarded as a step towards narrowing the gap between approximability and inapproximability of MINGDA$_\infty$ in polynomial-time.

Our results follow by a chain of gap-preserving reductions from two well-known lattice problems: SHORTEST VECTOR in ℓ_∞-norm and NEAREST VECTOR in ℓ_∞-norm. Using previous results [7, 4] on interactive proof-systems, Arora et al. [2] proved that, unless **NP** $\subseteq$ **DTIME**$(n^{\mathrm{poly}(\log n)})$, no polynomial-time algorithm can approximate the shortest non-trivial vector in the ℓ_∞-norm in a lattice within a factor $2^{\log^{0.5-\gamma} n}$ for an arbitrary small positive constant γ. They also showed the same inapproximability result for the nearest vector problem in the ℓ_∞-norm. By a recent result of Raz [14] the inapproximability factor in case of approximating the nearest vector in the ℓ_∞-norm in a lattice can be amplified to $2^{\log^{1-\gamma} n}$ for an arbitrary small positive constant γ.

We transfer these inapproximability gaps to MINGDA$_\infty$ and MINGNDA$_\infty$, respectively, via two intermediate problems.

Roadmap In section 2 we introduce some notation and the problem SHORTEST INTEGER RELATION in ℓ_∞-norm (SIR$_\infty$) which is known to be almost **NP**-hard to approximate within a factor $2^{\log^{0.5-\gamma} n}$, for γ an arbitrary small positive constant and n the input size, see Rőssner and Seifert [16]. In section 3 we give a gap-preserving reduction from SIR$_\infty$ to MINGDA$_\infty$ proving the first result. In section 4 we define the problem MINIMUM DIOPHANTINE EQUATION SOLUTION in ℓ_∞-norm (MINDES$_\infty$) and sketch a gap-preserving reduction from MINDES$_\infty$ to MINGNDA$_\infty$. This implies our second result.

2 Preliminaries

2.1 Definitions

We briefly introduce some notation, see [5].

Definition 1. An *optimization problem* Π is a set $\mathcal{I} \subseteq \{0,1\}^*$ of instances, a set $\mathcal{S} \subseteq \{0,1\}^*$ of feasible solutions and a polynomial-time computable positive measure function $m : \mathcal{I} \times \mathcal{S} \to \mathbb{R}_+$, that assigns each tuple of an instance I and a solution S, a positive real number $m(I,S)$, called the *value* of the solution S. The optimization problem is to find, for a given input $I \in \mathcal{I}$ a solution $S \in \mathcal{S}$ such that $m(I,S)$ is optimum over all possible $S \in \mathcal{S}$.

If the optimum is $\min_{S \in \mathcal{S}}\{m(I,S)\}$ (resp. $\max_{S \in \mathcal{S}}\{m(I,S)\}$) we refer to Π as a *minimization* (resp. *maximization*) problem.

Definition 2. For an input I of a minimization (resp. maximization) problem Π whose optimal solution has value $opt(I)$, an algorithm A is said to *approximate* $opt(I)$ *within a factor* $f(I)$ iff

$$opt(I) \leq A(I) \leq opt(I)f(I) \qquad \text{(resp. } opt(I)/f(I) \leq A(I) \leq opt(I)\text{)},$$

where $f(I) \geq 1$ and $A(I) > 0$.

For exhibiting the hardness of approximation problems we introduce the following reduction due to Arora [1].

Definition 3. Let Π and Π' be two minimization problems and ρ, $\rho' \geq 1$. A *gap-preserving reduction from* Π *to* Π' *with parameters* $((c,\rho),(c',\rho'))$ is a polynomial-time transformation τ mapping every instance I of Π to an instance $I' = \tau(I)$ of Π' such that for the optima $opt_\Pi(I)$ and $opt_{\Pi'}(I')$ of I and I', respectively, the following holds:

$$opt_\Pi(I) \leq c \Longrightarrow opt_{\Pi'}(I') \leq c'$$
$$opt_\Pi(I) > c \cdot \rho \Longrightarrow opt_{\Pi'}(I') > c' \cdot \rho',$$

where c, ρ and c', ρ' depend on the instance sizes $|I|$ and $|I'|$, respectively.

2.2 Previous Results

The proof of our first result will mainly rely on a gap-preserving reduction to MinGDA$_\infty$ from the problem Shortest Integer Relation in ℓ_∞-norm stated as follows:

Shortest Integer Relation in ℓ_∞-norm (SIR$_\infty$)
INSTANCE: A rational vector $\mathbf{a} \in \mathbb{Q}^d$
SOLUTION: A nonzero vector $\mathbf{x} \in \mathbb{Z}^d$ such that $\langle \mathbf{a}, \mathbf{x} \rangle = 0$
MEASURE: The ℓ_∞-norm $\|\mathbf{x}\|_\infty := \max_{1 \leq i \leq n} |x_i|$ of the vector $\mathbf{x}$

The Shortest Integer Relation problem in ℓ_∞-norm was proven to be **NP**-complete by van Emde Boas [19]. Very recently, Rőssner and Seifert [16] showed the following Theorem, stating that it is even almost **NP**-hard to approximate SIR$_\infty$ in polynomial-time within a factor $2^{\log^{0.5-\gamma} n}$, where γ is an arbitrary small positive constant and n the size of the SIR$_\infty$ instance I.

Theorem 4. *There exists an almost polynomial-time, i.e.,* $\mathbf{DTIME}(n^{\mathrm{poly}(\log n)})$ *transformation* τ *from* 3-Sat *to* Shortest Integer Relation *in* ℓ_∞*-norm such that, for all instances* I*,*

$$I \in \text{3-Sat} \Longrightarrow opt_{\mathrm{SIR}_\infty}(\tau(I)) = 1$$
$$I \notin \text{3-Sat} \Longrightarrow opt_{\mathrm{SIR}_\infty}(\tau(I)) > 2^{\log^{0.5-\gamma} |\tau(I)|},$$

where γ *is an arbitrary small positive constant.*

The above Theorem, in turn, was proven by a reduction from the Shortest Vector problem in the ℓ_∞-norm, involving techniques from the Feige and Lovász [7] 2-prover 1-round interactive proof-system, see [2, 16] for more details.

3 The Reduction

3.1 Reducing SIR_∞ to MinGDA_∞

Theorem 5. *There exists a polynomial-time transformation τ from* Shortest Integer Relation *in ℓ_∞-norm to* Minimum Good Diophantine Approximation *in ℓ_∞-norm, $\tau : I \mapsto \langle (a_0/b_0, \ldots, a_d/b_d), N\rangle$, such that, for all instances I and for all $\rho \geq 1$,*

$$opt_{\mathrm{SIR}_\infty}(I) = 1 \Longrightarrow \min_{1 \leq q \leq N} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \tfrac{1}{b_1}$$
$$opt_{\mathrm{SIR}_\infty}(I) > \rho \Longrightarrow \min_{1 \leq Q^* \leq \rho N} \|Q^*\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty > \rho\tfrac{1}{b_1}.$$

Proof. Our proof follows closely [12]. Due to a few changes specific to our claim, we include the complete proof here. Let $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d$ be the vector of a given SIR_∞ instance I. First, we encode the task to find a non-trivial $\mathbf{x} \in \mathbb{Z}^d$ with $\|\mathbf{x}\|_\infty \leq \rho$ and

$$\sum_{j=1}^{d} x_j a_j = 0 \tag{1}$$

as a congruence. Let $A := \rho \sum_{j=1}^{d} |a_j|$ and let p_0 be the smallest prime with $p_0 \not| \prod_{j=1}^{d} a_j$. We set $R := \lfloor \log_{p_0} A \rfloor + 1$. The following steps will crucially use the following Lemma whose proof is deferred to the Appendix.

Lemma A. *There exists a polynomial-time (polynomial in $|I|$) computable set of primes $\{Q_1, \ldots, Q_d\}$ and an integer $T \in \mathbb{N}_+$ such that*

(a) $Q_i < Q_{i+1}$, $i = 1, \ldots, d-1$,
(b) $\gcd(Q_i, p_0 \prod_{j=1}^{d} a_j) = 1$, $i = 1, \ldots, d$,
(c) $Q_1^T \geq 4\,\rho\,(d+1)\,p_0^R$ *and*
(d) $\rho^{1/T} Q_d < (\rho+1)^{1/T} Q_1$.

By the Chinese Remainder Theorem we find for every $j = 1, \ldots, d$ a smallest positive integer r_j satisfying

$$r_j \equiv 0 \pmod{\textstyle\prod_{\substack{i=1 \\ i \neq j}}^{d} Q_i^T} \tag{2a}$$
$$r_j \equiv a_j \pmod{p_0^R} \tag{2b}$$
$$r_j \not\equiv 0 \pmod{Q_j}, \tag{2c}$$

where $Q_1, \ldots, Q_d$ are given as above. $(2c)$ is a consequence of $(2a)$ and $(2b)$, for if r_j^0 is the smallest positive solution satisfying $(2a)$ and $(2b)$, we set

$$r_j := \begin{cases} r_j^0, & \text{if } r_j^0 \not\equiv 0 \pmod{Q_j}; \\ r_j^0 + p_0^R \left(\prod_{\substack{i=1 \\ i \neq j}}^{d} Q_i^T \right), & \text{otherwise.} \end{cases}$$

As $\gcd(p_0^R \prod_{i=1}^d Q_i^T/Q_j^T, Q_j) = 1$ by (b) of Lemma A, we infer that $r_j \not\equiv 0 \pmod{Q_j}$, $j = 1, \ldots, d$, i.e., (2c) holds for either choice of r_j.

By $(2b)$ and $A < p_0^R$, we see that the systems

$$\sum_{j=1}^{d} x_j a_j = 0, \qquad (1a) \qquad \text{and} \qquad \sum_{j=1}^{d} x_j r_j \equiv 0 \pmod{p_0^R}, \quad (3a)$$

$$1 \le \|\mathbf{x}\|_\infty \le \rho \qquad (1b) \qquad 1 \le \|\mathbf{x}\|_\infty \le \rho. \qquad (3b)$$

have identical integral solutions sets.

For an integral vector $\mathbf{x}$ with $1 \le \|\mathbf{x}\|_\infty \le \rho$ we define

$$Z := \sum_{j=1}^{d} x_j r_j, \qquad H := \sum_{j=1}^{d} r_j \qquad \text{and} \qquad B := \prod_{j=1}^{d} Q_j^T.$$

We clearly have $|Z| \le \rho H$. Moreover, (c) of Lemma A implies

$$r_j \le r_j^0 + p_0^R \left(\prod_{\substack{i=1 \\ i \ne j}}^{d} Q_i^T \right) \le 2 p_0^R \frac{B}{Q_j^T} \le \frac{1}{2\rho(d+1)} B, \qquad \text{thus} \qquad \rho H < 1/2B.$$

Lemma 3.6. *Let $opt_{\mathrm{modSIR}_\infty}(3a)$ denote the ℓ_∞-norm of the ℓ_∞-shortest non-trivial integral solution of $(3a)$. Then, we have*

$$\begin{aligned}
& opt_{\mathrm{modSIR}_\infty}(3a) = 1 \\
\Longrightarrow\ & \exists Z\colon Z \ne 0 \wedge |Z| \le H \wedge Z \equiv 0 \pmod{p_0^R} \wedge \bigwedge_{1 \le j \le d} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \\
& \qquad \wedge \bigwedge_{1 \le j \le d} \hat{x}_j \in \{0, \pm 1\} \\
& opt_{\mathrm{modSIR}_\infty}(3a) > \rho \\
\Longrightarrow\ & \forall Z\colon Z \ne 0 \wedge |Z| \le \rho H \wedge Z \equiv 0 \pmod{p_0^R} \wedge \bigwedge_{1 \le j \le d} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \\
& \qquad \Rightarrow \bigvee_{1 \le j \le d} \hat{x}_j \notin [-\rho, \rho] \cap \mathbb{Z}
\end{aligned}$$

Proof. First, assume that $opt_{\mathrm{modSIR}_\infty}(3a) = 1$ and let $\mathbf{x}$ be the corresponding solution of $(3a)$. For $Z := \sum_{j=1}^{d} x_j r_j$ we have

- $Z \ne 0$ by (2a), (2c) and since there exists an index j with $x_j \ne 0$,
- $|Z| \le H$ as $\|\mathbf{x}\|_\infty \le 1$,
- $Z \equiv \sum_{j=1}^{d} x_j r_j \equiv 0 \pmod{p_0^R}$ by definition and,
- $\bigwedge_{1 \le j \le d} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \wedge \bigwedge_{1 \le j \le d} \hat{x}_j \in \{0, \pm 1\}$ by (2a) and $\|\mathbf{x}\|_\infty \le 1$.

In order to show the second implication let us assume it exists $Z \ne 0$ with

$$|Z| \le \rho H \wedge Z \equiv 0 \pmod{p_0^R} \wedge \bigwedge_{1 \le j \le d} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \wedge \bigwedge_{1 \le j \le d} \hat{x}_j \in [-\rho, \rho] \cap \mathbb{Z}.$$

To prove the claim we will show the existence of a solution $\mathbf{x} \in \mathbb{Z}^d$ for $\sum_{j=1}^{d} x_j r_j \equiv 0 \pmod{p_0^R}$ satisfying $1 \leq \|\mathbf{x}\|_\infty \leq \rho$. For that we consider a candidate solution $\mathbf{x} = (x_1, \ldots, x_d) \in \mathbb{Z}^d$ by setting $\sum_{j=1}^{d} x_j r_j := Z$. Then, by (2a) we have $x_j r_j \equiv Z \pmod{Q_j^T}$, $1 \leq j \leq d$.

We show how to uniquely recover $x_j \pmod{Q_j^T}$ from the given Z. By (2c) and $\gcd(r_j, Q_j^T) = 1$ we can find the unique $r_j^\star$ with $1 \leq r_j^\star < Q_j^T$ satisfying $r_j r_j^\star \equiv 1 \pmod{Q_j^T}$, $1 \leq j \leq d$, using, e.g., the Extended Euclidean Algorithm. Consequently, we have

$$\underset{1 \leq j \leq d}{\forall} x_j \equiv x_j r_j r_j^\star \equiv Z r_j^\star \equiv \hat{x}_j r_j r_j^\star \equiv \hat{x}_j \pmod{Q_j^T} \text{ with } \underset{1 \leq j \leq d}{\forall} \hat{x}_j \in [-\rho, \rho] \cap \mathbb{Z}.$$

We now prove that even $x_j \in [-\rho, \rho] \cap \mathbb{Z}$. From the Chinese Remainder Theorem we infer that the system of congruences

$$Z \equiv \hat{x}_j r_j \pmod{Q_j^T}, \quad \hat{x}_j \in [-\rho, \rho] \cap \mathbb{Z}, \quad 1 \leq j \leq d$$

has exactly $(2\rho + 1)^d$ solutions in the interval

$$-1/2B < Z < 1/2B$$

since $B := \prod_{j=1}^{d} Q_j^T$. From the inequality $\rho H < 1/2B$ we see that we have at most $(2\rho + 1)^d$ solutions for the system

$$\begin{aligned} &|Z| \leq \rho H, \\ &Z \equiv \hat{x}_j r_j \pmod{Q_j^T}, \quad \hat{x}_j \in [-\rho, \rho] \cap \mathbb{Z}, \quad 1 \leq j \leq d. \end{aligned}$$

But it is an easy task to come up with $(2\rho+1)^d$ distinct solutions, namely those with all

$$x_j \in [-\rho, \rho] \cap \mathbb{Z}.$$

These solutions are all distinct by $x_j r_j \equiv Z \pmod{Q_j^T}$, for if

$$x_j' \neq x_j'' \qquad \text{then} \qquad Z' \equiv x_j' r_j \pmod{Q_j^T} \;\neq\; Z'' \equiv x_j'' r_j \pmod{Q_j^T}.$$

This means that we have found all $(2\rho+1)^d$ solutions which, in fact, satisfy $x_j \in [-\rho, \rho] \cap \mathbb{Z}$. Also note that $Z \neq 0$ if and only if $\mathbf{x}$ is not the all-zero vector. Since $Z = \sum_{j=1}^{d} x_j r_j$ and $Z \equiv 0 \pmod{p_0^R}$ we have shown that $opt_{\text{modSIR}_\infty}(3a) \leq \rho$. □

Lemma 3.7. *Let I be the* Minimum Good Diophantine Appoximation *instance defined by*

$$\begin{aligned} \alpha_0 &:= \tfrac{1}{p_0^R}, \\ \alpha_j &:= \tfrac{r_j^\star}{Q_j^T}, \quad 1 \leq j \leq d, \end{aligned}$$

where $r_j^\star$, $1 \le r_j^\star < Q_j^T$, is the unique inverse of $r_j \pmod{Q_j^T}$. Then, we have

$$\begin{aligned}
&\exists Z\colon Z \neq 0 \wedge |Z| \le H \wedge Z \equiv 0 \pmod{p_0^R} \wedge \underset{1\le j\le d}{\forall} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \\
&\qquad \wedge \underset{1\le j\le d}{\forall} \hat{x}_j \in \{0, \pm 1\} \\
\Longrightarrow\ &\exists Z\colon Z \neq 0 \wedge |Z| \le H \wedge \underset{0\le j\le d}{\forall} \min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \tfrac{1}{Q_1^T} \\
&\forall Z\colon Z \neq 0 \wedge |Z| \le \rho H \wedge Z \equiv 0 \pmod{p_0^R} \wedge \underset{1\le j\le d}{\forall} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \\
&\qquad \Rightarrow \underset{1\le j\le d}{\exists} \hat{x}_j \notin [-\rho, \rho] \cap \mathbb{Z} \\
\Longrightarrow\ &\forall Z\colon Z \neq 0 \wedge |Z| \le \rho H \Rightarrow \underset{0\le j\le d}{\exists} \min_{n\in\mathbb{Z}} |Z\alpha_j - n| > \tfrac{\rho}{Q_1^T}
\end{aligned}$$

Proof. First, assume there exists a $Z \neq 0$, such that:

$$|Z| \le H \wedge Z \equiv 0 \pmod{p_0^R} \wedge \underset{1\le j\le d}{\forall} Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \wedge \underset{1\le j\le d}{\forall} \hat{x}_j \in \{0, \pm 1\}.$$

Obviously, we have $Z \neq 0 \wedge |Z| \le H$ and also by $Z \equiv 0 \pmod{p_0^R}$

$$\min_{n\in\mathbb{Z}} \left| Z \tfrac{1}{p_0^R} - n \right| = 0.$$

Moreover, by (2c) and (a) of Lemma A we infer for $1 \le j \le d$

$$\min_{n\in\mathbb{Z}} \left| Z \tfrac{r_j^\star}{Q_j^T} - n \right| = \min_{n\in\mathbb{Z}} \left| \tfrac{\hat{x}_j r_j r_j^\star}{Q_j^T} - n \right| = \min_{n\in\mathbb{Z}} \left| \tfrac{\hat{x}_j}{Q_j^T} - n \right| \le \tfrac{1}{Q_j^T} \le \tfrac{1}{Q_1^T}.$$

Thus, there exists a denominator Z with the required properties.

In order to prove the second implication let us now assume

$$\exists Z\colon Z \neq 0 \wedge |Z| \le \rho H \wedge \underset{0\le j\le d}{\forall} \min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \tfrac{\rho}{Q_1^T}.$$

Obviously, again we have $Z \neq 0 \wedge |Z| \le \rho H$ and by (c) of Lemma A we have

$$\frac{1}{p_0^R} > \frac{\rho}{Q_1^T},$$

which together with $\min_{n\in\mathbb{Z}} |Z\frac{1}{p_0^R} - n| \le \frac{\rho}{Q_1^T}$ forces $\min_{n\in\mathbb{Z}} |Z\frac{1}{p_0^R} - n| = 0$. Thus, $Z \equiv 0 \pmod{p_0^R}$. By (a) and (d) of Lemma A it follows that

$$\frac{\rho + 1}{Q_j^T} > \frac{\rho}{Q_1^T},$$

which together with $\min_{n\in\mathbb{Z}} |Z\frac{r_j^\star}{Q_j^T} - n| \le \frac{\rho}{Q_1^T}$ enforces $\min_{n\in\mathbb{Z}} |Z\frac{r_j^\star}{Q_j^T} - n| \le \frac{\rho}{Q_j^T}$. But this is only possible if

$$Z \equiv \hat{x}_j r_j \pmod{Q_j^T} \wedge \hat{x}_j \in [-\rho, \rho] \cap \mathbb{Z}, \quad 1 \le j \le d.$$

This of course proves the lemma. □

Combining the solution equivalence of the systems $(1a, 1b)$ and $(3a, 3b)$ with Lemma 3.6 and Lemma 3.7 yields the desired polynomial-time transformation τ, since all operations of our reduction can clearly be carried out in time polynomial in $|I|$. □

3.2 Hardness of Approximating Diophantine Approximations

By piecing together the results of Theorem 4 and Theorem 5, we obtain the following:

Main Theorem 8 *Unless* $\mathbf{NP} \subseteq \mathbf{DTIME}(n^{\mathrm{poly}(\log n)})$, *there exists no polynomial-time algorithm which on input* $\boldsymbol{\alpha} \in \mathbb{Q}^d$ *and* $N \in \mathbb{N}_+$ *computes a denominator* Q^* *with* $1 \leq Q^* \leq 2^{\log^{0.5-\gamma} d} N$ *such that*

$$\|Q^* \boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq 2^{\log^{0.5-\gamma} d} \min_{1 \leq q \leq N} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty,$$

where γ *is an arbitrary small positive constant.*

Corollary 9. *Approximating* MinGDA$_\infty$ *in polynomial-time within a factor* $2^{\log^{0.5-\gamma} d}$ *for an arbitrary small positive constant* γ *is almost* **NP***-hard.*

4 The Nonhomogeneous Case

To capture the nonhomogeneous case, i.e., the problem MinGNDA$_\infty$, we will reduce from a well-suited problem, namely:

Minimum Diophantine Equation Solution in ℓ_∞-norm (MinDES$_\infty$)
INSTANCE: An equation $x_1 a_1 + \cdots + x_n a_n = b$ with $a_1, \ldots, a_n, b \in \mathbb{Z}$
SOLUTION: A vector $\mathbf{x} \in \mathbb{Z}^n$ such that $\sum_{i=1}^n x_i a_i = b$
MEASURE: The ℓ_∞-norm $\|\mathbf{x}\|_\infty := \max_{1 \leq i \leq n} |x_i|$ of the vector $\mathbf{x}$

Majewski and Havas [13] proved the **NP**-completeness of MinDES$_\infty$ in its feasibility recognition form. Using the Parallel Repetition Theorem of Raz [14] and the techniques of Arora et al. [2] it is not difficult to modify the proof of Theorem 4 from [16] such that even the following holds, see [15] for a detailed proof.

Theorem 10. *There exists an almost polynomial-time, i.e.,* $\mathbf{DTIME}(n^{\mathrm{poly}(\log n)})$ *transformation* τ *from* 3-Sat *to* Minimum Diophantine Equation Solution *in* ℓ_∞*-norm such that, for all instances* I*,*

$$I \in \text{3-SAT} \Longrightarrow opt_{\text{MinDES}_\infty}(\tau(I)) = 1$$
$$I \notin \text{3-SAT} \Longrightarrow opt_{\text{MinDES}_\infty}(\tau(I)) > 2^{\log^{1-\gamma} |\tau(I)|},$$

where γ *is an arbitrary small positive constant.*

Adapting the reduction in the proof of Theorem 5 to the nonhomogeneous case, the following can be shown:

Theorem 11. *There exists a polynomial-time transformation τ from* Shortest Integer Relation *in ℓ_∞-norm to* Minimum Good Nonhomogeneous Diophantine Appoximation *in ℓ_∞-norm, $\tau : I \mapsto \langle (a_0/b_0, \ldots, a_d/b_d), \boldsymbol{\beta}, N \rangle$, such that, for all instances I and for all $\rho \geq 1$,*

$$opt_{\mathrm{MinDES}_\infty}(I) = 1 \Longrightarrow \min_{1 \leq q \leq N} \|q\boldsymbol{\alpha} - \boldsymbol{\beta} \bmod \mathbb{Z}\|_\infty \leq \tfrac{1}{b_1}$$

$$opt_{\mathrm{MinDES}_\infty}(I) > \rho \Longrightarrow \min_{1 \leq Q^* \leq \rho N} \|Q^*\boldsymbol{\alpha} - \boldsymbol{\beta} \bmod \mathbb{Z}\|_\infty > \rho \tfrac{1}{b_1}.$$

(For the reduction from the MinDES_∞–instance $\langle (a_1, \ldots, a_n, b) \rangle$ we have to ensure that $p_0 \not| \, b$. Then, defining the vector $\boldsymbol{\beta}$ of the instance of Minimum Good Nonhomogeneous Diophantine Approximation in ℓ_∞-norm by $\beta_0 = b/p_0^R$, $\beta_i = 0$, $i = 1, \ldots, d$, admits a straightforward adaption of the proof of Theorem 5.)

By the last Theorem and the **NP**-completeness of MinDES_∞ we infer:

Main Theorem 12 $\mathrm{MinGNDA}_\infty$ *is* **NP***-complete (in its feasibility recognition form).*

Moreover, Theorem 10 and Theorem 11 imply:

Main Theorem 13 *Unless* $\mathbf{NP} \subseteq \mathbf{DTIME}(n^{\mathrm{poly}(\log n)})$, *there exists no polynomial-time algorithm which on input $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Q}^d$ and $N \in \mathbb{N}_+$ computes a denominator Q^* with $1 \leq Q^* \leq 2^{\log^{1-\gamma} d} N$ such that*

$$\|Q^*\boldsymbol{\alpha} - \boldsymbol{\beta} \bmod \mathbb{Z}\|_\infty \leq 2^{\log^{1-\gamma} d} \min_{1 \leq q \leq N} \|q\boldsymbol{\alpha} - \boldsymbol{\beta} \bmod \mathbb{Z}\|_\infty,$$

where γ is an arbitrary small positive constant.

Corollary 14. *Approximating* $\mathrm{MinGNDA}_\infty$ *in polynomial-time within a factor $2^{\log^{1-\gamma} d}$ for an arbitrary small positive constant γ is almost* **NP***-hard.*

Acknowledgment

We would like to thank Jeff Lagarias for several helpful comments on possible improvements of this paper.

References

1. S. Arora. *Probabilistic Checking of Proofs and Hardness of Approximation Problems.* Ph.D. thesis, University of California at Berkeley, 1994.
2. S. Arora, L. Babai, J. Stern and Z Sweedyk. The hardness of approximate optima in lattices, codes and systems of linear equations. In *Proc. 34th IEEE Symp. on Foundations of Computer Science*, pages 724–730, 1993.

3. S. Arora and C. Lund. Hardness of approximation. In D. Hochbaum (editor), *Approximation Algorithms for NP–hard problems*, Chapter 11. PWS Publ., 1996.
4. S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof verification and hardness of approximation problems. In *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, pages 14–23, 1992.
5. G. Ausiello, P. Crescenzi and M. Protasi. Approximate solutions of NP optimization problems. *Theoretical Computer Science*, Volume 150, pages 1–55, 1995.
6. P. Crescenzi and V. Kann. A list of NP-complete optimization problems. Surveys on complexity, Electronic Colloqium on Computational Complexity, http://www.informatik.uni-trier.de/eccc/, 1996.
7. U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proc. 24th ACM Symp. Theory of Computing*, pages 643–654, 1992.
8. A. Frank and É. Tardos. An application of simultaneous diophantine approximation in combinatorial optimization. *Combinatorica*, Volume 7, pages 49–65, 1987.
9. D. R. Heath-Brown. The number of primes in a short interval. *J. reine angew. Math.*, Volume 389, pages 22–63, 1988.
10. D. R. Heath-Brown and H. Iwaniec. On the difference between consecutive primes. *Inventiones math.*, Volume 55, pages 49–69, 1979.
11. R. Kannan, A. K. Lenstra and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Math. Comp.*, Volume 50, pages 235–250, 1988.
12. J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM J. Comput.*, Volume 14, pages 196–209, 1985.
13. B. S. Majewski and G. Havas. The complexity of greatest common divisor computations. In *Proc. 1st International Symposium on Algorithmic Number Theory*, pages 184–193. Springer, 1994. LNCS 877.
14. R. Raz. A parallel repetition theorem. In *Proc. 27th ACM Symp. Theory of Computing*, pages 447–456, 1995.
15. C. Rőssner and J.-P. Seifert. The complexity of approximate optima for greatest common divisor computations. In *Proc. 2nd Algorithmic Number Theory Symposium*, pages ?–? Springer, 1996. LNCS.
16. C. Rőssner and J.-P. Seifert. On the hardness of approximating shortest integer relations among rational numbers. In *Proc. CATS'96 (Computing: The Australasian Theory Symposium)*, pages 180–186, 1996.
17. C. P. Schnorr. Factoring integers and computing discrete logarithms via diophantine approximations. *AMS DIMACS Series in Disc. Math. and Theoretical Comp. Science*, Volume 13, pages 171–181, 1993.
18. A. Schoenhage. Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. In *11th ICALP*, pages 436–447. Springer, 1987. LNCS 172.
19. P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, Math. Inst., University of Amsterdam, 1981.

Appendix

We will prove that for suitable choices of T we can find in $O(n^{50})$ bit operations an interval containing d prime numbers $Q_1, \ldots, Q_d$ satisfying the conditions (a)-

(d) of Lemma A.

Proof. (of Lemma A) Let $n := |I|$ denote the length of the given SIR_∞ instance I, i.e., the vector $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d$. Obviously, $n \geq d$.

As the binary length of $\prod_{i=1}^{d} a_i$ is bounded by dn, this product has at most $dn \leq n^2$ distinct prime factors. Therefore, p_0 will be one of the first (n^2+1) primes which can be found by a brute force trial division in $O(n^4)$ bit operations. Using $\rho \leq n$ and the specific choice of p_0 and R we have

$$2^{3n^2} \geq 2^{n^2+1} 2^{\log \rho} 2^{n \log d} \geq 2^{n^2+1} \rho \sum_{j=1}^{d} |a_j| \geq p_0^R.$$

Hence, setting $T := 4n^2$, guarantees $Q_1^T \geq 4\rho(d+1)p_0^R$, i.e., condition (c) holds.

In order to find a set of primes $\{Q_1, \ldots, Q_d\}$ satisfying the remaining conditions of Lemma A we invoke the following primitive search routine:

for every $x = 1, 2, \cdots$
  if $[\rho^{1/T}x, (\rho+1)^{1/T}x] =: I_x$ contains $\geq d + n^2 + 1$ distinct primes **then** stop;

If this search stops with x, we are guaranteed that for this choice of x at least d primes in I_x satisfy the condition (b) since $p_0 \prod_{i=1}^{d} a_i$ has at most n^2+1 distinct prime factors. Moreover, the conditions (a) and (d) are satisfied by selecting the suited primes in the interval I_x.

The main difficulty is now to prove that the above search routine performs at most n^k bit operations for some $k \in \mathbb{N}$. Thus, we must give an upper bound for the value of x for which the search algorithm stops. We use the following number-theoretic result on the number of primes in a short interval.

Theorem [10, 9]. *For each $\delta > \frac{11}{20}$ there exists a constant x_δ such that the interval $[x, x + x^\delta]$ contains for all $x > x_\delta$ a prime.*

From $\rho \leq n$, we derive

$$(\tfrac{\rho+1}{\rho})^{1/T} \geq 1 + \ln(\tfrac{\rho+1}{\rho})\tfrac{1}{T} \geq 1 + \tfrac{1}{2\rho}\tfrac{1}{4n^2} \geq 1 + \tfrac{1}{8n^3}.$$

Setting $x := \frac{n^{20}}{\rho^{1/T}}$, we infer

$$I_x = [\rho^{1/T}x, (\rho+1)^{1/T}x] = [n^{20}, (\tfrac{\rho+1}{\rho})^{1/T} n^{20}] \supseteq [n^{20}, n^{20} + \tfrac{1}{8}n^{17}].$$

For the choice of $\delta := \frac{3}{5}$ the above Theorem guarantees that we can find in the interval $[n^{20}, n^{20} + n^{12}]$ a prime, if n is sufficiently large. Since we can locate in the interval $[n^{20}, n^{20} + n^{17}]$ all the intervals of the form

$$[n^{20} + i\, n^{12}, n^{20} + (i+1)\, n^{12}], \qquad i = 0, \ldots, n^5 - 1,$$

we will be able to find at least n^5 distinct primes.

As the primality of each number x in I_x can be tested in $O((x^{3/2} + xn^2)(\log x)^2)$ bit operations, the above search routine uses at most $O(n^{50})$ bit operations. □

This article was processed using the LaTeX macro package with LLNCS style