# New Hardness Results for Diophantine Approximation

Friedrich Eisenbrand* and Thomas Rothvoß

Institute of Mathematics
EPFL, Lausanne, Switzerland
{friedrich.eisenbrand,thomas.rothvoss}@epfl.ch

**Abstract** We revisit *simultaneous Diophantine approximation*, a classical problem from the geometry of numbers which has many applications in algorithms and complexity. The input to the decision version of this problem consists of a rational vector $\alpha \in \mathbb{Q}^n$, an error bound $\varepsilon$ and a denominator bound $N \in \mathbb{N}_+$. One has to decide whether there exists an integer, called the *denominator* $Q$ with $1 \leq Q \leq N$ such that the distance of each number $Q \cdot \alpha_i$ to its nearest integer is bounded by $\varepsilon$. Lagarias has shown that this problem is NP-complete and optimization versions have been shown to be hard to approximate within a factor $n^{c/\log\log n}$ for some constant $c > 0$. We strengthen the existing hardness results and show that the optimization problem of finding the *smallest denominator* $Q \in \mathbb{N}_+$ such that the distances of $Q \cdot \alpha_i$ to the nearest integer are bounded by $\varepsilon$ is hard to approximate within a factor $2^n$ unless P = NP.
We then outline two further applications of this strengthening: We show that a directed version of Diophantine approximation is also hard to approximate. Furthermore we prove that the *mixing set* problem with arbitrary capacities is NP-hard. This solves an open problem raised by Conforti, Di Summa and Wolsey.

## 1 Introduction

Diophantine approximation is one of the fundamental topics in mathematics. Roughly speaking, the objective is to replace a number or a vector, by another number or vector which is very close to the original, but less complex in terms of fractionality. A famous example is the Gregorian calendar, which approximates a solar year with its leap year rule.

Since the invention of the LLL algorithm [15], simultaneous Diophantine approximation has been a very important object of study also in computer science. One powerful result, for example, is the one of Frank and Tardos [7] who provided an algorithm based on Diophantine approximation and the LLL algorithm

* Supported by the Deutsche Forschungsgemeinschaft (DFG) within Priority Programme 1307 "Algorithm Engineering" and by the Swiss National Science Foundation (SNSF)

which, among other things, shows that a combinatorial 0/1-optimization problem is polynomial if and only if it is strongly polynomial.

Let us denote the distance of a real number $x \in \mathbb{R}$ to its nearest integer by $\{x\} = \min\{|x - z| \colon z \in \mathbb{Z}\}$ and the distance of a vector $v \in \mathbb{R}^n$ to its nearest integer vector w.r.t. the infinity norm $\ell_\infty$ by $\{\{v\}\} = \min\{\|v - z\|_\infty \colon z \in \mathbb{Z}^n\}$.

Lagarias [14] has shown that it is NP-complete to decide whether there exists an integer $Q \in \{1, \ldots, N\}$ with $\{\{Q \cdot \alpha\}\} \leq \varepsilon$, given $\alpha \in \mathbb{Q}^n$, $N \in \mathbb{N}_+$ and $\varepsilon > 0$. The *best approximation error* $\delta_N$ of a vector $\alpha \in \mathbb{Q}^n$ with denominator bound $N \in \mathbb{N}_+$ is defined as $\delta_N = \min\{\, \{\{Q \cdot \alpha\}\} \colon Q \in \{1, \ldots, N\}\,\}$. Lagarias [14] showed also that the existence of a polynomial algorithm, which computes on input $\alpha \in \mathbb{Q}^n$ and $N \in \mathbb{N}_+$ a number $Q \in \{1, \ldots, 2^{n/2} \cdot N\}$ with $\{\{Q \cdot \alpha\}\} \leq \delta_N$ implies NP = co-NP.

Lagarias' reduction was then sharpened to an inapproximability result by Rössner and Seifert [21] and Chen and Meng [1] to the extent that, given $\alpha \in \mathbb{Q}^n$ and $N$ as above, it is NP-hard to compute a $Q \in \{1, \ldots, \lfloor n^{c/\log\log n} \rfloor N\}$ with $\{\{Q \cdot \alpha\}\} \leq n^{c/\log\log n} \delta_N$ where $c > 0$ is a constant. We revisit the reduction technique of Lagarias [14] and its sharpening by Rössner and Seifert [21] to obtain the following theorem.

**Theorem 1.** *There exists a constant $c > 0$ and a polynomial time transformation which maps an instance $C$ of SAT to an instance $\alpha \in \mathbb{Q}^n$, $N \in \mathbb{N}_+$, $\varepsilon \in \mathbb{Q}_+$ of simultaneous Diophantine approximation such that the following holds.*

*i) If $C$ is satisfiable, then there is a $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ with $\{\{Q \cdot \alpha\}\} \leq \varepsilon$.*
*ii) If $C$ is not satisfiable, then one has $\{\{Q \cdot \alpha\}\} \geq n^{c/\log\log n} \cdot \varepsilon$ for each $Q \in \{1, \ldots, 2^n \cdot N\}$.*
*iii) The error bound $\varepsilon$ satisfies $\varepsilon \leq 1/(2^{2n})$.*

The crucial differences between our result and the result in [21] are as follows. In case i), there exists a good $Q$ which is at least $\lceil N/2 \rceil$ whereas the result in [21] guarantees only a good $Q$ in the interval $\{1, \ldots, N\}$. In case ii) each $Q$ which is bounded by $2^n \cdot N$ is violating the distance bound by $n^{c/\log\log n}$, whereas the reduction of [21] together with the result of [1] guarantees this violation only for $Q \in \{1, \ldots, \lfloor n^{c/\log\log n} \rfloor \cdot N\}$. These differences facilitate the application of our hardness result to other problems from the geometry of numbers and integer programming. We describe three such applications in this paper.

### Applications

One immediate consequence of Theorem 1 is that the *best denominator problem*

$$\min\{Q \in \mathbb{N}_+ \colon \{\{Q \cdot \alpha\}\} \leq \varepsilon\}$$

cannot be approximated within a factor of $2^n$ unless P = NP, see Corollary 1. Furthermore, it follows that the existence of a polynomial algorithm, which computes on input $\alpha \in \mathbb{Q}^n, N \in \mathbb{N}_+$ a number $Q \in \{1, \ldots, 2^n \cdot N\}$ with $\{\{Q \cdot \alpha\}\} \leq \delta_N$ implies P = NP improving the result of Lagarias [14] mentioned above to the

extent of replacing the factor $2^{n/2}$ and the assumption NP $\neq$ co-NP by $2^n$ and P $\neq$ NP respectively, see Corollary 2.

We then provide a strong inapproximability result for *directed Diophantine approximation*, where the distance to the nearest integer vector which is greater than or equal to $Q \cdot \alpha$ has to be small. Directed Diophantine approximation was for example considered by Henk and Weismantel [12] in the context of an integer programming problem and an optimization version of directed Diophantine approximation was shown to be hard to approximate within a constant factor by the authors of this paper [6].

Finally we apply our results to solve an open problem raised by Conforti, Di Summa and Wolsey [3] concerning the complexity of a linear optimization problem over a *mixing set with arbitrary capacities*, a type of integer program which frequently appears in production planning.

## 2 A strengthening of the Lagarias, Rössner-Seifert reduction

The goal of this section is to prove Theorem 1. To do this, we rely on several results from the literature. Our starting point is a similar result for the *shortest integer relation* problem. Here, one is given a vector $a \in \mathbb{Z}^n$ and the goal is to find a nonzero integral solution $x \in \mathbb{Z}^n$ of the equation $a^T x = 0$ of minimum infinity norm. By modifying a reduction from *Super-Sat* to shortest vector in the infinity norm by Dinur [5], Chen and Meng [1] showed that there exists a reduction from SAT to shortest integer relation with the property that if $C$ is satisfiable, then the optimum value of the shortest integer relation problem is one and if $C$ is unsatisfiable, then the optimum value of the shortest integer relation problem is at least $n^{c/\log\log n}$ for some constant $c > 0$. This can be extended to the following result which we prove in the appendix. The only difference to the stated result above is the presence of condition c).

**Lemma 1.** *There exists a constant $c > 0$ and a polynomial time algorithm, which maps a SAT-formula $C$ to an instance $a \in \mathbb{Z}^n$ of shortest integer relation- with the following properties:*

*a) If $C$ is satisfiable, then* $\min\{\|x\|_\infty \colon a^T x = 0,\, x \in \mathbb{Z}^n - 0\} = 1$.
*b) If $C$ is not satisfiable, then* $\min\{\|x\|_\infty \colon a^T x = 0,\, x \in \mathbb{Z}^n - 0\} \geq n^{c/\log\log n}$.
*c) There exists an optimum solution $x$ of* $\min\{\|x\|_\infty \colon a^T x = 0,\, x \in \mathbb{Z}^n - 0\}$ *with* $x_1 \geq 1$.

We proceed from Lemma 1 to show the existence of a reduction from SAT to simultaneous Diophantine approximation with properties i), ii) and iii). For this, by Lemma 1 it is enough to provide a reduction from a shortest integer relation problem $\min\{\|x\|_\infty \colon a^T x = 0,\, x \in \mathbb{Z}^n - 0\}$ with the property that there exists an optimum solution $x$ with $x_1 \geq 1$ to an instance of simultaneous Diophantine approximation $\alpha_0, \ldots, \alpha_n, \varepsilon, N$ such that the following assertions hold.

I) If the optimum value of the shortest integer relation problem is one, then there exists a $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ with $\{\{Q \cdot \alpha\}\} \leq \varepsilon$.
II) For each $\rho \in \{1, \ldots, n\}$ the following statement is true: If the optimum value of the shortest integer relation problem is larger than $\rho$, then $\{\{Q \cdot \alpha\}\} > \rho \cdot \varepsilon$ for each $Q \in \{1, \ldots, 2^n \cdot N\}$.
III) The error bound $\varepsilon$ satisfies $\varepsilon \leq 1/(2^{2n})$.

The rest of the proof of Theorem 1 follows closely the proof of Lagarias [14] and the one of Rössner and Seifert [21]. Let $\min\{\|x\|_\infty : a^T x = 0,\, x \in \mathbb{Z}^n - 0\}$ be the instance of shortest integer relation. One can efficiently find different primes $p, q_1, \ldots, q_n$ as well as natural numbers $R$ and $T$ in polynomial time, such that

1. $n \cdot \sum_{j=1}^{n} |a_j| < p^R < q_1^T < q_2^T < \ldots < q_n^T < (1 + \frac{1}{n}) \cdot q_1^T$
2. $p$ and all $q_i$ are co-prime to all $a_j$
3. $q_1^T > 2^{2n} \cdot p^R$
4. The values of $T, R, p, q_1, \ldots, q_n$ are bounded by a polynomial in the input length of $a$.

A proof of this claim with weaker bounds is presented in [14,21]. The crucial difference to the results in these papers is the bound 3), which before stated that $p^R$ times a polynomial in the input encoding is at most $q_1^T$. Here we have the exponential factor $2^{2n}$ instead. The full proof is in the Appendix.

The following system of congruences appears already in [16] and is also crucial in the reductions presented in [14,21].

$$r_j \equiv_{p^R} a_j \tag{1}$$

$$r_j \equiv_{q_i^T} 0 \;\; \forall i \neq j \tag{2}$$

$$r_j \not\equiv_{q_j} 0 \tag{3}$$

For each $j$, this is a system of congruences with co-prime moduli and thus, the Chinese remainder theorem (see, e.g. [18]) guarantees that there exists a solution $r_j$ for each $j = 1, \ldots, n$.

**Lemma 2.** *The systems*

$$\sum_{j=1}^{n} x_j a_j = 0 \quad \textit{and} \quad \sum_{j=1}^{n} x_j r_j \equiv_{p^R} 0 \tag{4}$$

*have the same set of integral solutions $x \in \mathbb{Z}^n$ with $\|x\|_\infty \leq n$.*

*Proof.* Since $a_j \equiv_{p^R} r_j$, each solution $x \in \mathbb{Z}^n$ of the equation on the left is also a solution of the congruence equation on the right. If $x \in \mathbb{Z}^n$ is a solution for the congruence on the right, then $\sum_{j=1}^{n} a_j x_j \equiv_{p^R} 0$. Assume furthermore $\|x\|_\infty \leq n$. If we can infer that the absolute value of $\sum_{j=1}^{n} a_j x_j$ is strictly less than $p^R$, then $\sum_{j=1}^{n} a_j x_j = 0$ follows. But

$$|\sum_{j=1}^{n} x_j a_j| \leq n \cdot \sum_{j=1}^{n} |a_j| < p^R$$

by the choice of the prime numbers. □

We now provide the construction of the instance $\alpha_0, \ldots, \alpha_n, \varepsilon, N$ of the simultaneous Diophantine approximation problem for our reduction. By $r_j^{-1} \in \mathbb{Z}$ we denote the unique integer in $\{1, \ldots, q_j^T - 1\}$ with $r_j \cdot r_j^{-1} \equiv_{q_j^T} 1$. This must exist since $r_j \not\equiv_{q_j} 0$ implies that $r_j$ is a unit in the ring $\mathbb{Z}_{q_j^T}$. The instance is

$$\begin{aligned} \alpha_0 &= \frac{1}{p^R} \\ \alpha_j &= \frac{r_j^{-1}}{q_j^T}, \quad j = 1, \ldots, n \\ N &= \sum_{j=1}^{n} r_j \\ \varepsilon &= \frac{1}{q_1^T}. \end{aligned}$$

The bound iii) on $\varepsilon$ follows from $q_1^T > 2^{2n} \cdot p^R$. Let $x \in \mathbb{Z}^n$ be a solution of the shortest integer relation problem with $\|x\|_\infty \leq 1$. Consider the integer $Q = \sum_{j=1}^n r_j \cdot x_j$ whose absolute value is bounded by $N = \sum_{j=1}^n r_j$. What is the distance of $Q \cdot \alpha$ to the nearest integer vector in the infinity norm?

Since $\sum_{j=1}^n r_j \cdot x_j \equiv_{p^R} \sum_{j=1}^n a_j \cdot x_j = 0$ it follows that $p^R$ divides $\sum_{j=1}^n r_j \cdot x_j$ which means that $\{Q\alpha_0\} = 0$. For $i \geq 1$ one has $r_i^{-1} \cdot \sum_{j=1}^n r_j \cdot x_j \equiv_{q_i^T} x_i$ (since $r_j \equiv_{q_i^T} 0$ for $i \neq j$) and since $x_i \in \{0, \pm 1\}$ one has $\{Q \cdot \alpha_i\} \leq 1/q_i^T \leq 1/q_1^T = \varepsilon$. In other words, $Q$ is an integer whose absolute value is bounded by $N$ which satisfies $\{\{Q \cdot \alpha\}\} \leq \varepsilon$. This is almost condition I), except that $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ might not be satisfied.

To achieve this additional bound on $Q$ we use the fact that there exists an optimal solution of the shortest integer relation problem which satisfies $x_1 \geq 1$ and we choose $r_1$ significantly larger than the other $r_j$. Consider again the system of congruences (1-3). Let $B = p^R \prod_{j=1}^n q_j^T$ and let $0 \leq r'_j \leq B/q_j^T$ be a solution to (1) and (2). If $r'_j \not\equiv_{q_j^T} 0$, then $r_j = r'_j$ otherwise $r_j = r'_j + B/q_j^T$. Thus each $r_j$ is bounded by $0 \leq r_j \leq 2 \cdot B/q_j^T$. We choose $r_1$ however considerably larger, namely $r_1 = r'_1 + 12nB/q_1^T$ or $r'_1 + (12n+1)B/q_1^T$. In this way we have $r_1 \geq 6n \cdot r_j$. By choosing the $r_j$ in this way, we obtain the following lemma.

**Lemma 3.** *If* $\min\{\|x\|_\infty : a^T x = 0, x \in \mathbb{Z}^n - 0\} = 1$, *then there exists a* $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ *such that* $\{\{Q \cdot \alpha\}\} \leq \varepsilon$.

*Proof.* By our assumption, there exists an optimum solution $x \in \mathbb{Z}^n$ of the shortest integer relation problem with $x_1 = 1$. Let $Q$, as in the discussion above, be $Q = \sum_{j=1}^n r_j x_j$. We have already seen that $\{\{Q \cdot \alpha\}\} \leq \varepsilon$ holds and clearly $Q \leq \sum_{j=1}^n r_j = N$. On the other hand $x_1 \geq 1$, $\|x\|_\infty = 1$ and $r_1 \geq 6nr_j$ for each $j = 2, \ldots, n$ implies $Q \geq N/2$. □

The next lemma provides condition II).

**Lemma 4.** *Let $\rho$ be any number in $\{1,\ldots,n\}$ and suppose there exists a $Q \in \{1,\ldots,2^n N\}$ with $\{\{Q\cdot\alpha\}\} \le \rho\cdot\varepsilon$. Then, the optimum value of the shortest integer relation problem is at most $\rho$.*

*Proof.* We construct a solution $x$ of the shortest integer relation instance: Let $x_j$ be the smallest integer in absolute value with

$$Q r_j^{-1} \equiv_{q_j^T} x_j.$$

We need to show three things, namely

$$\|x\|_\infty \le \rho, \quad x \neq \mathbf{0} \quad \text{and} \quad a^T x = 0. \tag{5}$$

The first assertion of (5) follows from the fact that $q_1^T < q_j^T < (1+1/\rho)\cdot q_1^T$ which implies the strict inequality in

$$\left|\frac{x_j}{q_j^T}\right| = \left\{\frac{Q r_j^{-1}}{q_j^T}\right\} \le \rho\cdot\varepsilon = \frac{\rho}{q_1^T} < \frac{\rho+1}{q_j^T}.$$

Observe that $Q$ is a multiple of $p^R$. If this was not the case, then

$$\{Q\alpha_0\} = \left\{\frac{Q}{p^R}\right\} \ge \frac{1}{p^R} > \frac{\rho}{q_1^T} = \rho\cdot\varepsilon,$$

since $q_1^T > 2^{2\cdot n} p^R$ and $\rho \le n$. We next show that $Q = \sum_{i=1}^n x_i r_i$. This implies directly that $x \neq \mathbf{0}$, since $Q \ge 1$. Furthermore $Q \equiv_{p^R} 0$ and Lemma 2 imply together with $\|x\|_\infty \le \rho$ that $a^T x = 0$ and (5) is proved.

Multiplying the equation $Q\cdot r_j^{-1} \equiv_{q_j^T} x_j$ with $r_j$ yields $Q \equiv_{q_j^T} r_j x_j$. Let $D = \prod_{j=1}^n q_j^T$. We have $Q \equiv_{q_i^T} r_i x_i$ and $0 \equiv_{q_i^T} r_j x_j$ for $j \neq i$ and thus $Q \equiv_{q_i^T} \sum_{j=1}^n r_j x_j$. Since the moduli $q_i^T$ are co-prime, this implies that $Q \equiv_D \sum_{j=1}^n r_j x_j$. We are done with the proof, once we have shown that $Q < D/2$ and $|\sum_{j=1}^n x_j r_j| < D/2$, since then both values must coincide if they are congruent to each other modulo $D$.

We first bound the value of $|\sum_{j=1}^n x_j r_j|$. This is at most $\rho\cdot\sum_{j=1}^n r_j \le n\cdot N$. Applying the bound $r_j \le 13\cdot n p^R D/q_1^T$ and $q_1^T > 2^{2n}\cdot p^R$ we can bound $N$ by

$$N \le 13\cdot n^2\cdot D/2^{2n}.$$

Consequently

$$|\sum_{j=1}^n x_j r_j| \le 13\cdot n^3\cdot D/2^{2n}$$

which is smaller than $D/2$ for $n$ sufficiently large. Finally $Q$ is bounded by $2^n N$ which is also bounded by $D/2$ for $n$ large enough. The claim follows. □

This proves Theorem 1.

### 2.1 Hardness of the best denominator

We now discuss the hardness of the *best denominator problem*. The input to this problem is $\alpha_1, \ldots, \alpha_n, \varepsilon \in \mathbb{Q}$ and the task is to find a smallest $Q \in \mathbb{N}_+$ with $\{\{Q \cdot \alpha\}\} \leq \varepsilon$. The following corollary is an immediate consequence of Theorem 1.

**Corollary 1.** *If $P \neq NP$, then there does not exist a polynomial time approximation algorithm for the* best denominator problem *with an approximation factor $2^n$.*

Furthermore we can strengthen the result of Lagarias [14] which states that, if there exists a polynomial time algorithm which, on input $\alpha \in \mathbb{Q}^n$ and $N \in \mathbb{N}_+$ computes a $Q \in \{1, \ldots, 2^{n/2}N\}$ with $\{\{Q \cdot \alpha\}\} \leq \delta_N$, then NP = co-NP. Recall that $\delta_N = \min\{\, \{\{Q \cdot \alpha\}\} \colon Q \in \{1, \ldots, N\}\,\}$. The strengthening is as follows.

**Corollary 2.** *If there exists a polynomial time algorithm which computes on input $\alpha \in \mathbb{Q}^n$ and $N \in \mathbb{N}_+$ a $Q \in \{1, \ldots, 2^n \cdot N\}$ with $\{\{Q \cdot \alpha\}\} \leq \delta_N$, then $P = NP$.*

*Proof.* Consider an instance $\alpha, N, \varepsilon$ which stems from the reduction of a SAT-formula $C$ as in Theorem 1 and suppose that there exists an algorithm which computes in polynomial time a $Q \in \{1, \ldots, 2^n N\}$ with $\{\{Q \cdot \alpha\}\} \leq \delta_N$. If $\{\{Q \cdot \alpha\}\} \leq \varepsilon$, then $C$ is satisfiable. Otherwise, $C$ is unsatisfiable. This implies the assertion. □

## 3 Directed Diophantine Approximation

In this section we consider a variant of the classical Diophantine approximation problem, in which we measure the distance of the vector $Q \cdot \alpha$ to the nearest integer vector which is in each component greater or equal than $Q \cdot \alpha$. We use the notation $\{x\}^\uparrow$ for the distance of the real number $x \in \mathbb{R}$ to the nearest integer which is greater or equal to $x$, $\{x\}^\uparrow = \min\{z - x \colon z \in \mathbb{Z},\, z \geq x\}$. For a vector $\alpha \in \mathbb{R}^n$ we denote its distance to the nearest integer greater or equal to $\alpha$ by $\{\{\alpha\}^\uparrow\}$, in other words

$$\{\{\alpha\}^\uparrow\} = \min\{\|x - \alpha\|_\infty \colon x \in \mathbb{Z}^n, x \geq \alpha\}.$$

An instance of directed Diophantine approximation consists of $\alpha_1, \ldots, \alpha_n, \varepsilon, N$ with $\alpha_i \in \mathbb{Q}$, $\varepsilon \in \mathbb{Q}$ and $N \in \mathbb{N}_+$. The goal of this section is to show the following theorem.

**Theorem 2.** *There is a constant $c > 0$ and a polynomial time transformation which maps a SAT instance $C$ to an instance $\alpha_0, \ldots, \alpha_n, \varepsilon, N$ of directed Diophantine approximation such that the following conditions hold.*

*i') If $C$ is satisfiable, then there exists a $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ with $\{\{Q \cdot \alpha\}^\uparrow\} \leq \varepsilon$.*

*ii')* *If $C$ is unsatisfiable, then for each $Q \in \{1, \ldots, \lfloor n^{c/\log\log n} \rfloor N\}$ one has $\{\{Q \cdot \alpha\}^{\uparrow}\} > 2^n\varepsilon$.*

*iii')* *The error bound $\varepsilon$ satisfies $\varepsilon \leq 3/2^n$.*

*Proof.* For the proof of this theorem, we rely on Theorem 1. Let $\alpha_1, \ldots, \alpha_n, \varepsilon, N$ be a simultaneous Diophantine approximation instance which results from the transformation from SAT. From this, we construct an instance of directed Diophantine approximation $\alpha'_1, \ldots, \alpha'_{2n}, N, \varepsilon'$ with

$$\begin{aligned} \alpha'_i &= \alpha_i - \delta \quad i = 1, \ldots, n \\ \alpha'_{i+n} &= -\alpha_i - \delta \quad i = 1, \ldots, n \\ \varepsilon' &= 3\varepsilon, \end{aligned}$$

where $\delta = 2\varepsilon/N$.

Suppose that there exists a $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ with $\{\{Q\alpha\}\} \leq \varepsilon$ and let $z_i$ be the nearest integer to $Q \cdot \alpha_i$. Since $Q \cdot \delta \geq \varepsilon$ it follows that $Q(\alpha_i + \delta) \geq z_i$ and thus that the distance of $Q(\alpha_i + \delta)$ to $\lfloor Q(\alpha_i + \delta) \rfloor$ is bounded by $|Q(\alpha_i + \delta) - z_i| \leq |Q\alpha_i - z_i| + |Q\delta| \leq 3\varepsilon$. This means that $\{Q(-\alpha_i - \delta)\}^{\uparrow} \leq 3\varepsilon$. Similarly, $Q(\alpha_i - \delta) \leq z_i$ and thus $\{Q(\alpha_i - \delta)\}^{\uparrow}$ is bounded by $|Q(\alpha_i - \delta) - z_i| \leq |Q\alpha_i - z_i| + |Q\delta| \leq 3\varepsilon$. This implies property i').

Next let $\rho \in \{1, \ldots, n\}$ and suppose that there exists a $Q \in \{1, \ldots, \rho N\}$ with $\{\{Q\alpha'\}^{\uparrow}\} \leq 2^n\varepsilon'$. We show that this implies that $\{\{Q\alpha\}\} \leq 2\rho\varepsilon$ which in turn shows that property ii') holds.

For each $i \in \{1, \ldots, n\}$ there exists an integer $z_i$ which lies between $Q(\alpha_i - \delta)$ and $Q(\alpha_i + \delta)$, since otherwise one of the values $\{Q(\alpha_i - \delta)\}^{\uparrow}$ or $\{Q(-\alpha_i - \delta)\}^{\uparrow}$ is at least $1/2$. But $\{\{Q \cdot \alpha'\}^{\uparrow}\} \leq 2^n\varepsilon' = 2^n 3\varepsilon < 1/2$, a contradiction. Then $Q(\alpha_i - \delta) \leq z_i \leq Q(\alpha_i + \delta)$ implies

$$|Q\alpha_i - z_i| \leq Q\delta \leq 2\rho\varepsilon.$$

□

## 4 Hardness of Mixing Set

In recent integer programming approaches for production planning the study of simple integer programs which are part of more sophisticated models has become very successful in practice, see, e.g. [19]. One of these simple integer programs is the so-called *mixing set* [9,2]. The constraint system of a mixing set problem is of the form

$$\begin{aligned} s + a_i\, y_i &\geq b_i \quad i = 1, \ldots, n, \\ s &\geq 0 \\ y_i &\in \mathbb{Z} \quad i = 1, \ldots, n, \\ s &\in \mathbb{R}. \end{aligned} \tag{6}$$

where $a_i, b_i \in \mathbb{Q}$. Optimizing a linear function over this mixed integer set can be done in polynomial time if all $a_i$ are equal to one [9,17] or if $a_{i+1}/a_i$ is an integer for each $i = 1, \ldots, n-1$ [22], see also [3,4] for subsequent simpler approaches.

Conforti et al. [3] pose the problem, whether one can optimize a linear function over the set of mixed-integer vectors defined by (6) also in the general case, to which they refer as the case with *arbitrary capacities*, in polynomial time. In this section, we apply our results on directed Diophantine approximation to show that this problem is NP-hard.

Suppose we have an instance of the directed Diophantine approximation problem $\alpha, N, \varepsilon$, where we are supposed to round down to the nearest integer vector. By using the notation $\{x\}^{\downarrow} = \min\{x - z \colon z \leq x, z \in \mathbb{Z}\}$ for $x \in \mathbb{R}$ and $\{\{v\}^{\downarrow}\} = \min\{\|v - z\|_{\infty} \colon z \in \mathbb{Z}^n,\, z \leq v\}$ and the observation that $\{x\}^{\downarrow} = \{-x\}^{\uparrow}$ it follows that Theorem 2 is also true if the rounding up operation is replaced by rounding down. We next formulate an integer program to compute a $Q$ which yields a good approximation by rounding down and satisfies the denominator bound $Q \in \{1, \ldots, N\}$.

$$\begin{aligned} &\min \textstyle\sum_{i=1}^{n} (Q \cdot \alpha_i - y_i) \\ Q - 1/\alpha_i \cdot y_i &\geq 0 \quad i = 1, \ldots, n \\ Q &\geq 1 \\ Q &\leq N \\ Q, y_1, \ldots, y_n &\in \mathbb{Z}. \end{aligned}$$

The goal is to transform this integer program into a linear optimization problem over a mixing set. Consider the following mixing set.

$$\begin{aligned} Q - 1/\alpha_i \cdot y_i &\geq 0 \quad i = 1, \ldots, n \\ Q + 0 \cdot y_0 &\geq 1 \\ Q - y_{-1} &\geq 0 \\ Q &\in \mathbb{R} \\ y_{-1}, y_0, y_1, \ldots, y_n &\in \mathbb{Z}. \end{aligned} \tag{7}$$

We now argue that, if the linear optimization problem over this mixing set can be done in polynomial time, then P = NP.

Suppose that the linear optimization problem can be solved in polynomial time. Then, we can also solve the linear optimization problem over the nonempty face of the convex hull of the solutions which is induced by the inequality $Q - y_{-1} \geq 0$, see, e.g., [8]. This enforces $Q$ to be an integer. Next consider the following objective function

$$\min \sum_{i=1}^{n} (Q \cdot \alpha_i - y_i) + (2^{n-1}\varepsilon/N)(Q - N). \tag{8}$$

The sum on the left is measuring the distance of $Q \cdot \alpha$ to its nearest integer vector from below in the $\ell_1$-norm. The term on the right stems from the removal of the constraint $Q \leq N$, which would not be allowed in a system defining a mixing set. In fact, we thereby follow a Lagrangian relaxation approach, which is common in approximation algorithms, see e.g. [20], in order to show a hardness result.

**Theorem 3.** *Optimizing a linear function over a mixing set is NP-hard.*

*Proof.* Let $\alpha_1, \ldots, \alpha_n, N, \varepsilon$ be an instance of directed Diophantine approximation with rounding down, which stems from a transformation from SAT, as in Theorem 2 and suppose that one can solve the linear optimization problem with objective function (8) over the convex hull of the mixing set. Then we can also optimize this over the face induced by $Q - y_{-1} \geq 0$. This merely means that we can find a pure integer optimum solution over the mixing set (7).

Our instance $\alpha_1, \ldots, \alpha_n, N, \varepsilon$ has the following property. If the originating SAT formula is satisfiable, then there exists a $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ with $\{\{Q \cdot \alpha\}^{\downarrow}\} \leq \varepsilon$ and if not, then there does not exist a $Q \in \{1, \ldots, \lfloor n^{c/\log\log n} \rfloor N\}$ with $\{\{Q \cdot \alpha\}^{\downarrow}\} \leq 2^n \varepsilon$.

In the case where the SAT formula is satisfiable, let $Q \in \{\lceil N/2 \rceil, \ldots, N\}$ with $\{\{Q \cdot \alpha\}^{\downarrow}\} \leq \varepsilon$. The objective function value of this $Q$ with the appropriate $y_i$ yields an objective function value bounded by $n \cdot \varepsilon$.

Suppose now that the SAT formula is not satisfiable and consider a solution $Q$ with appropriate $y_i$ of the mixing set problem. If $Q \in \{1, \ldots, \lfloor n^{c/\log\log n} \rfloor N\}$, then the objective function is at least

$$2^n \varepsilon - 2^{n-1} \varepsilon = 2^{n-1} \varepsilon.$$

If $Q$ is larger than $\lfloor n^{c/\log\log n} \rfloor N$, then the objective function value is at least

$$2^{n-1} \varepsilon (\lfloor n^{c/\log\log n} \rfloor - 1).$$

Thus the problem of optimizing a linear function over a mixing set with arbitrary capacities is NP-hard. □

## References


1. W. Chen and J. Meng. An improved lower bound for approximating shortest integer relation in $l_\infty$ norm (SIR$_\infty$). *Information Processing Letters*, 101(4):174–179, 2007.
2. M. Conforti, M. Di Summa, and L. A. Wolsey. The mixing set with flows. *SIAM Journal on Discrete Mathematics*, 21(2):396–407 (electronic), 2007.
3. M. Conforti, M. D. Summa, and L. A. Wolsey. The mixing set with divisible capacities. In A. Lodi, A. Panconesi, and G. Rinaldi, editors, *The The 13th Conference on Integer Programming and Combinatorial Optimization, IPCO 08*, Lecture Notes in Computer Science, pages 435–449. Springer, 2008.
4. M. Conforti and G. Zambelli. The mixing set with divisible capacities: a simple approach. Manuscript.
5. I. Dinur. Approximating SVP$_\infty$ to within almost-polynomial factors is NP-hard. *Theoretical Computer Science*, 285(1):55–71, 2002. Algorithms and complexity (Rome, 2000).
6. F. Eisenbrand and T. Rothvoß. Static-priority realtime-scheduling: Response time computation is **NP**-hard. *RTSS'08*, 2008.
7. A. Frank and É. Tardos. An application of simultaneous Diophantine approximation in combinatorial optimization. *Combinatorica*, 7:49–65, 1987.
8. M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1993.

9. O. Günlük and Y. Pochet. Mixing mixed-integer inequalities. *Mathematical Programming. A Publication of the Mathematical Programming Society*, 90(3, Ser. A):429–457, 2001.
10. D. R. Heath-Brown. The number of primes in a short interval. *Journal für die Reine und Angewandte Mathematik*, 389:22–63, 1988.
11. D. R. Heath-Brown and H. Iwaniec. On the difference between consecutive primes. *American Mathematical Society. Bulletin. New Series*, 1(5):758–760, 1979.
12. M. Henk and R. Weismantel. Diophantine approximations and integer points of cones. *Combinatorica*, 22(3):401–407, 2002.
13. R. Kannan. Polynomial-time aggregation of integer programming problems. *Journal of the Association for Computing Machinery*, 30(1):133–145, 1983.
14. J. C. Lagarias. The computational complexity of simultaneous Diophantine approximation problems. *SIAM Journal on Computing*, 14(1):196–209, 1985.
15. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.
16. K. L. Manders and L. Adleman. NP-complete decision problems for binary quadratics. *Journal of Computer and System Sciences*, 16(2):168–184, 1978.
17. A. J. Miller and L. A. Wolsey. Tight formulations for some simple mixed integer programs and convex objective integer programs. *Mathematical Programming*, 98(1-3, Ser. B):73–88, 2003. Integer programming (Pittsburgh, PA, 2002).
18. I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991.
19. Y. Pochet and L. A. Wolsey. *Production planning by mixed integer programming*. Springer Series in Operations Research and Financial Engineering. Springer, New York, 2006.
20. R. Ravi and M. X. Goemans. The constrained minimum spanning tree problem (extended abstract). In *SWAT '96: Proceedings of the 5th Scandinavian Workshop on Algorithm Theory*, pages 66–75, London, UK, 1996. Springer-Verlag.
21. C. Rössner and J. P. Seifert. Approximating good simultaneous Diophantine approximations is almost NP-hard. In *Mathematical foundations of computer science 1996 (Cracow)*, volume 1113 of *Lecture Notes in Comput. Sci.*, pages 494–505. Springer, Berlin, 1996.
22. M. Zhao and I. R. de Farias, Jr. The mixing-MIR set with divisible capacities. *Mathematical Programming. A Publication of the Mathematical Programming Society*, 115(1, Ser. A):73–103, 2008.

## Appendix

### Shortest integer relation

By modifying a reduction from *Super-Sat* to shortest vector in the infinity norm by Dinur [5], Chen and Meng [1] showed that there exists a reduction from SAT to shortest integer relation with the property that if $C$ is satisfiable, then the optimum value of the shortest integer relation problem is one and if $C$ is unsatisfiable, then the optimum value of the shortest integer relation problem is at least $n^{c/\log\log n}$ for some constant $c > 0$. Here, we show that this can be extended such that there exists an optimum solution of shortest integer relation, whose first component is nonzero, thus give a proof of Lemma 1.

Let $\min\{\|x\|_\infty \colon a^T x = 0, x \in \mathbb{Z}^n - 0\}$ be an instance of a shortest integer relation problem. Consider the matrix

$$A = \begin{pmatrix} 0 & a^T & \mathbf{0}^T & \dots & \mathbf{0}^T \\ 0 & \mathbf{0}^T & a^T & \dots & \mathbf{0}^T \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \mathbf{0}^T & \mathbf{0}^T & \dots & a^T \\ -1 & e_1^T & e_2^T & \dots & e_n^T \end{pmatrix} \in \mathbb{Z}^{(n+1)\times(n^2+1)}$$

containing $n$ copies of $a^T$ on a shifted diagonal and having $(-1, e_1^T, e_2^T, \dots, e_n^T)$ as last row, where $e_i$ is the $i$-th $n$-dimensional unit column vector. The rest is filled by zeros.

Clearly, the optimization problems $\min\{\|x\|_\infty \colon a^T x = 0, x \in \mathbb{Z}^n - 0\}$ and $\min\{\|x\|_\infty \colon Ax = 0, x \in \mathbb{Z}^{n^2+1} - 0\}$ are equivalent and the second optimization problem has the property that there is always an optimum solution with nonzero first entry. Kannan [13] provided an algorithm replacing a system $Ax = 0$ by one equation $a'^T x = 0$ in polynomial time such that the sets $\{x \in \mathbb{Z}^{n^2+1} \colon Ax = 0, \|x\|_\infty \le \mu\}$ and $\{x \in \mathbb{Z}^{n^2+1} \colon a'x = 0, \|x\|_\infty \le \mu\}$ are identical. His algorithm is polynomial in the encoding length of $A$ and $\mu$. Choosing $\mu = n$ is enough for our purposes so that Kannan's algorithm yields the desired shortest integer relation instance $\min\{\|x\|_\infty \colon a'^T x = 0,\ x \in \mathbb{Z}^{n^2+1} - 0\}$.

### Computing dense primes

In the reduction from shortest integer relation to simultaneous Diophantine approximation (Sect. 2) we rely on the fact that one can efficiently compute prime numbers $p, q_1, \dots, q_n$ and integers $R$ and $T$ with

1. $n \cdot \sum_{j=1}^n |a_j| < p^R < q_1^T < q_2^T < \ldots < q_n^T < (1 + \frac{1}{n}) \cdot q_1^T$,
2. $p$ and all $q_i$ are co-prime to all $a_j$,
3. $q_1^T > 2^{2n} \cdot p^R$,
4. the values of $T, R, p, q_1, \dots, q_n$ are bounded by a polynomial in the input length of $a$.

The algorithm which we now present is almost identical, up to better bounds, to the one proposed by Lagarias [14] and uses two deep results from number theory. The first one is the *prime number theorem*, which states that $\pi(n) \approx n/\log n$, see, e.g. [18]. The second result is the following theorem by Heath-Brown and Iwaniec [10,11].

**Theorem 4.** *For each $\delta > 11/20$, there exists a constant $c_\delta$ such the interval $[z, z + z^\delta]$ contains a prime for each $z > c_\delta$.*

Let $m$ be the binary encoding length of $a$. The number of different primes which divide a component of $a$ is bounded by $m$. We can compute the first $m+1$ prime numbers with the sieve of Eratosthenes. Here the prime number theorem is used, since we run the sieve on the first $O(m \log m)$ natural numbers. Out of

these primes we choose one which is co-prime to all components of $a$. This is the prime $p$ from above. Next, we compute the smallest integers $R$ and $T$ such that $p^R > n \cdot \sum_{j=1}^{n} |a_j|$ and $2^T > 2^{2n} p^R$. The values of $R$ and $T$ are bounded by a polynomial in $m$.

Next, the result of Heath-Brown and Iwaniec comes into play. Let $\delta = 3/5$ and consider the sequence

$$z_i = T^{20} + i \cdot (2T)^{12}, \text{ for } i = 0, \ldots, T^2 - 1.$$

Each interval $[z_i, z_i + z_i^{3/5}]$ contains a prime number, since may may assume $T > c_\delta$. The number $z_i^{3/5}$ can be bounded by

$$\begin{aligned} z_i^{3/5} &= \left(T^{20} + i(2T)^{12}\right)^{3/5} \\ &< \left(T^{20} + T^2(2T)^{12}\right)^{3/5} \\ &\leq (2T)^{12}. \end{aligned}$$

From this it follows that $z_i + z_i^{3/5} < z_{i+1}$, which implies that the interval $[T^{20}, T^{20} + T^2(2T)^{12}]$ contains $T^2$ prime numbers. Since $T^2(2T)^{12} < T^{15}$ for $T$ large enough, we infer that the interval

$$[T^{20}, T^{20} + T^{15}]$$

contains $T^2$ primes. If we denote the largest and smallest prime in this interval by $p_{\max}$ and $p_{\min}$ respectively, then $p_{\max}/p_{\min} \leq 1 + (1/T)^5$ and consequently

$$(p_{\max}/p_{\min})^T \leq (1 + (1/T)^5)^T \leq e^{1/T^4} \leq 1 + 2/T^4 \leq 1 + \frac{1}{n}.$$

Here, we used the inequality $1 + x \leq e^x$ and $e^x \leq 1 + 2x$ for $x \in [0, 1]$.

By choosing $T$ larger than $m + n + 1$, we may obtain prime numbers $q_1 < \ldots < q_n$ from the interval $[T^{20}, T^{20} + T^{15}]$, which are co-prime to $p$ and each $a_j$ and hence satisfy the conditions (1–4).