The Computational Complexity of Integer Programming with Alternations*

Danny Nguyen[1] and Igor Pak[2]

1 **Department of Mathematics, UCLA, Los Angeles, CA, USA**
ldnguyen@math.ucla.edu

2 **Department of Mathematics, UCLA, Los Angeles, CA, USA**
pak@math.ucla.edu

Abstract

We prove that integer programming with three alternating quantifiers is NP-complete, even for a fixed number of variables. This complements earlier results by Lenstra and Kannan, which together say that integer programming with at most two alternating quantifiers can be done in polynomial time for a fixed number of variables. As a byproduct of the proof, we show that for two polytopes $P, Q \subset \mathbb{R}^4$, counting the projection of integer points in $Q \backslash P$ is #P-complete. This contrasts the 2003 result by Barvinok and Woods, which allows counting in polynomial time the projection of integer points in P and Q separately.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, G.1.6 Optimization

Keywords and phrases integer programming, alternations, projection of integer points

Digital Object Identifier 10.4230/LIPIcs.CCC.2017.6

1 Introduction

1.1 Background

In a pioneer paper [19], Lenstra showed that Integer Programming in a bounded dimension can be solved in polynomial time. The next breakthrough was obtained by Kannan in 1990 and until recently remained the most general result in this direction (see [11]).

▶ **Theorem 1** (Parametric Integer Programming [16]). *Fix d_1 and d_2. Given a polyhedron $P \subseteq \mathbb{R}^{d_1}$, a matrix $A \in \mathbb{Z}^{m \times (d_1+d_2)}$ and a vector $\bar{b} \in \mathbb{Z}^m$, the following sentence can be decided in polynomial time:*

$$\forall \mathbf{x} \in P \cap \mathbb{Z}^{d_1} \quad \exists \mathbf{y} \in \mathbb{Z}^{d_2} \quad : \quad A\,(\mathbf{x}, \mathbf{y}) \leq \bar{b}. \tag{1.1}$$

Here P is given by a system $C\,\mathbf{x} \leq \bar{\gamma}$, with $C \in \mathbb{Z}^{n \times d_1}$ and $\bar{\gamma} \in \mathbb{Z}^n$. The numbers m, n are part of the input.

In [17], Kannan asked if Theorem 1 can be extended to three alternating quantifiers. We give an answer in the negative direction to this question:

▶ **Theorem 2.** *Fix $d_1 \geq 1, d_2 \geq 2$ and $d_3 \geq 3$. Given two polyhedra $P \subseteq \mathbb{R}^{d_1}$, $Q \subseteq \mathbb{R}^{d_2}$, a matrix $A \in \mathbb{Z}^{m \times (d_1+d_2+d_3)}$ and a vector $\bar{b} \in \mathbb{Z}^m$, then deciding the sentence*

$$\exists \mathbf{x} \in P \cap \mathbb{Z}^{d_1} \quad \forall \mathbf{y} \in Q \cap \mathbb{Z}^{d_2} \quad \exists \mathbf{z} \in \mathbb{Z}^{d_3} \quad : \quad A\,(\mathbf{x}, \mathbf{y}, \mathbf{z}) \leq \bar{b} \tag{1.2}$$

is an NP-complete problem. Here P and Q are given by two systems $C\,\mathbf{x} \leq \bar{\gamma}$ and $D\,\mathbf{y} \leq \bar{\delta}$, with $C \in \mathbb{Z}^{n \times d_1}$, $\bar{\gamma} \in \mathbb{Z}^n$, $D \in \mathbb{Z}^{q \times d_2}$, and $\bar{\delta} \in \mathbb{Z}^q$.

[*] The second author was partially supported by the NSF.

32nd Computational Complexity Conference (CCC 2017).
Editor: Ryan O'Donnell; Article No. 6; pp. 6:1–6:18
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Let us emphasize that in both Theorem 1 and 2, there is no bound on the number of inequalities involved. In other words, the parameters m, n and q are *not* fixed. Theorem 2 is especially surprising for the following reasons. First, in [22], we gave strong evidence that (1.2) is decidable in polynomial time if m, n and q are fixed. Second, by an easy application of the Doignon–Bell–Scarf theorem, (1.1) is polynomial time reducible to the case with m and n fixed. Unfortunately, this simple reduction breaks down when there are more than two quantifiers (see Section 7.1) as in (1.2). Still, in [22], we speculated that a more involved reduction argument might still apply to (1.2). Theorem 2 refutes the possibility of any reduction from (1.2) to an easier form with m, n and q bounded for which decision could be in polynomial time, unless $\mathsf{P} = \mathsf{NP}$. In fact, Theorem 2 holds even when P is an interval and Q is an axis-parallel rectangles (see Theorem 9 and §7.8). Thus, the problem (1.2) is already hard when n, q are fixed and only m is unbounded.

In [25], Schöning proved that it is NP-complete to decide whether

$$\exists x \in \mathbb{Z} \quad \forall y \in \mathbb{Z} \quad : \quad \Psi(x, y). \tag{1.3}$$

Compared to (1.2), this has only two quantifiers. However, here the expression $\Psi(x, y)$ is allowed to contain both conjunctions and disjunctions of many inequalities. So Theorem 2 tells us that disjunctions can be discarded at the cost of adding one extra alternation. In the next subsection, we generalize this observation.

1.2 Presburger sentences

In [14], Grädel considered the theory of *Presburger Arithmetic*, and proved many completeness results in this theory when the number of variables and quantifiers are bounded. Those results were later strengthened by Schöning in [25]. They can be summed up as follows:

▶ **Theorem 3** ([25]). *Fix $k \geq 1$. Let $\Psi(\mathbf{x}, \mathbf{y})$ be a Boolean combination of linear inequalities with integer coefficients in the variables $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{Z}^k$ and $\mathbf{y} = (y_1, \ldots, y_3) \in \mathbb{Z}^3$. Then deciding the sentence*

$$Q_1\, x_1 \in \mathbb{Z} \quad \ldots \quad Q_k\, x_k \in \mathbb{Z} \quad Q_{k+1}\, \mathbf{y} \in \mathbb{Z}^3 \quad : \quad \Psi(\mathbf{x}, \mathbf{y})$$

is $\boldsymbol{\Sigma}_k^{\mathsf{P}}$-complete if $Q_1 = \exists$, and $\boldsymbol{\Pi}_k^{\mathsf{P}}$-complete if $Q_1 = \forall$. Here $Q_1, \ldots, Q_{k+1} \in \{\forall, \exists\}$ are $m + 1$ alternating quantifiers.

This result characterizes the complexity of so called *Presburger sentences* with $k + 1$ quantifiers in a fixed number of variables. The main difference between Presburger Arithmetic versus integer programming is that the expression Ψ allows both conjunction and disjunction of many inequalities. This flexibility allows effective reductions of classical decision problems such as QSAT. For some time, it remains a question whether such reductions can be carried with only conjunctions, and at the same time keeping the number of variables fixed. We prove the following result, which generalizes Theorem 2:

▶ **Theorem 4.** *Integer programming in a fixed number of variables with $k + 2$ alternating quantifiers is $\boldsymbol{\Sigma}_k^{\mathsf{P}}/\boldsymbol{\Pi}_k^{\mathsf{P}}$-complete, depending on whether $Q_1 = \exists/\forall$. Here the problem is allowed to contain only a system of inequalities.*

We refer to Theorem 13 for the precise statement. Thus, we see that integer programming requires only one more quantifier alternation to achieve the same complexity as Presburger Arithmetic. Again, we emphasize that while the number of variables and quantifiers are fixed in Theorem 4, the linear system is still allowed many inequalities.

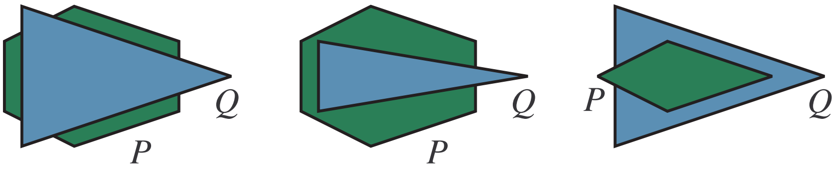

Figure 1 Three examples of convex polygons $P, Q \subset \mathbb{R}^2$.

1.3 Counting points in projections of non-convex polyhedra

For polytopes in arbitrary dimension, counting the number of integer points is classically #P-complete, even for 0/1 polytopes. In a fixed dimension d, Barvinok famously showed this can be done in polynomial time:

▶ **Theorem 5** ([2]). *Fix d. Given a polytope $P \subset \mathbb{R}^d$, the number of integer points in $P \cap \mathbb{Z}^d$ can be computed in polynomial time. Here P is described by a system $A\mathbf{x} \le \bar{b}$, with $A \in \mathbb{Z}^{m \times d}$, $\bar{b} \in \mathbb{Z}^m$.*

For a set $S \subset \mathbb{R}^d$, denote by $\mathrm{E}(S) := S \cap \mathbb{Z}^d$. The previous results say that $|\mathrm{E}(P)|$ is computable in polynomial time. Given two polytopes $P \subset Q \subset \mathbb{R}^d$, we clearly have $|\mathrm{E}(Q \backslash P)| = |\mathrm{E}(Q)| - |\mathrm{E}(P)|$. So the number of integer points in a complement can also be computed effectively.

Theorem 5 was later generalized by Barvinok and Woods to count the number of integer points in projections of polytopes:

▶ **Theorem 6** ([5]). *Fix d_1 and d_2. Given a polytope $P \subset \mathbb{R}^{d_1}$, and a linear transformation $T : \mathbb{Z}^{d_1} \to \mathbb{Z}^{d_2}$, the number of integer points in $T(P \cap \mathbb{Z}^{d_1})$ can be computed in polynomial time. Here P is described by a system $A\mathbf{x} \le \bar{b}$ and T is described by a matrix M, where $A \in \mathbb{Z}^{m \times d_1}$, $\bar{b} \in \mathbb{Z}^m$ and $M \in \mathbb{Z}^{d_2 \times d_1}$.*

For a set $S \subset \mathbb{R}^d$, denote by $\mathrm{E}_1(S)$ the projection of $S \cap \mathbb{Z}^d$ on the first coordinate, i.e.,

$$\mathrm{E}_1(S) := \{x \in \mathbb{Z} \quad : \quad \exists \mathbf{z} \in \mathbb{Z}^{d-1} \quad (x, \mathbf{z}) \in S\}.$$

By Theorem 6, $|\mathrm{E}_1(P)|$ can be computed in polynomial time for every polytope $P \subset \mathbb{R}^d$.

We prove the following result:

▶ **Theorem 7.** *Given two polytopes $P \subset Q \subset \mathbb{R}^4$, computing $|\mathrm{E}_1(Q \backslash P)|$ is #P-complete.*

In other words, it is #P-complete to compute the size of the set

$$\mathrm{E}_1(Q \backslash P) = \{x \in \mathbb{Z} \, : \, \exists \mathbf{z} \in \mathbb{Z}^3 \quad (x, \mathbf{z}) \in Q \backslash P\}. \tag{1.4}$$

Note that the corresponding decision problem $|\mathrm{E}_1(Q \backslash P)| \ge 1$ is equivalent to $|\mathrm{E}(Q \backslash P)| \ge 1$, and thus can be decided in polynomial time by applying Theorem 5.

The contrast between Theorem 6 and our negative result can be explained as follows. The proof Theorem 6 depends on the polytopal structure of P and exploited convexity in a crucial way. By taking the complement $Q \backslash P$, we no longer have a convex set. In other words, we show that projection of the complement $Q \backslash P$ is complicated enough to allow encoding of hard counting problems, even in $\mathbb{R}^4$ (see also §7.5).

▶ Remark 1. To understand the theorem, consider three examples of polygons $P, Q \subset \mathbb{R}^2$ as in Figure 1. Note that the sets of integer points of the vertical projections of P, Q and $P \cup Q$ are the same in all three cases, but the sets number of integer points of the vertical projections of $Q \backslash P$ are quite different.

As an easy consequence of Theorem 7 we obtain:

▶ **Corollary 8.** *Given r simplices $T_1, \ldots, T_r \subset \mathbb{R}^4$, computing $|\mathrm{E}_1(T_1 \cup \cdots \cup T_r)|$ is #*P*-complete.*

1.4 Outline of the paper

We begin with notations (Section 2) and a geometric construction of certain polytopes based on Fibonacci numbers (Section 3). In Section 4 we use this construction to prove Theorem 2 via a reduction of the GOOD SIMULTANEOUS APPROXIMATION (GSA) Problem in Number Theory, which is known to be NP-complete. The proof of Theorem 4 is via a reduction of QSAT (Section 5). The proof of Theorem 7 follows a similar route via reduction of #GSA (Section 6). Finally, we conclude with final remarks and open problems (Section 7).

2 Notations

- We a use $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}_+ = \{1, 2, \ldots\}$.
- All constant vectors are denoted $\overline{a}, \overline{b}, \overline{x}, \overline{y}, \overline{t}$ etc.
- Matrices are denoted A, B, C, etc.
- Variables are denoted x, y, z, etc.; vectors of variables are denoted $\mathbf{x}, \mathbf{y}, \mathbf{z}$, etc.
- We write $\mathbf{x} \leq \mathbf{y}$ if $x_j \leq y_j$ for all i.
- A *polyhedron* is an intersection of finitely many closed half-spaces in $\mathbb{R}^n$.
- A *polytope* is a bounded polyhedron.
- Polyhedra and polytopes are denoted by P, Q, R, etc.

3 Geometric constructions and properties

3.1 Fibonacci points

We consider the first $2d$ *Fibonacci numbers*:

$$F_0 = 0, F_1 = 1, F_2 = 1, \ldots, F_{2d-1}.$$

From these, we construct d integer points:

$$\phi_1 = (F_1, F_0),\ \phi_2 = (F_3, F_2),\ \ldots,\ \phi_d = (F_{2d-1}, F_{2d-2}). \tag{3.1}$$

Let

$$\Phi = \{\phi_1, \ldots, \phi_d\} \subset \mathbb{Z}^2 \quad \text{and} \quad J = [1, F_{2d-1}] \times [0, F_{2d-2}] \cap \mathbb{Z}^2. \tag{3.2}$$

We have $\Phi \subset J$. Denote by $\mathcal{C}$ the curve consisting of $d-1$ segments connecting ϕ_i to ϕ_{i+1} for $i = 1, \ldots, i-1$.

We also define the following two polygons. Their properties will be mentioned later.

$$R_1 = \left\{ \mathbf{y} = (y_1, y_2) \in \mathbb{R}^2 \ : \ \begin{bmatrix} y_1 & \geq & 1 \\ y_2 & \leq & F_{2d-2} \\ y_2 F_{2d-1} - y_1 F_{2d-2} & \geq & 1 \end{bmatrix} \right\}, \tag{3.3}$$

and

$$R_2 = \left\{ \mathbf{y} \in \mathbb{R}^2 \ : \ \begin{bmatrix} y_1 \leq F_{2d-1} \\ y_2 \geq \quad 0 \end{bmatrix} \ \text{and} \ \ y_2 F_{2i} - y_1 F_{2i-1} \leq -2 \ \ \text{for} \ \ i = 1, \ldots, d \right\}. \tag{3.4}$$

The following properties are straightforward from the above definitions:

(F1) The points $\phi_1, \ldots, \phi_d$ are in convex position. The curve $\mathcal{C}$ connecting them is convex (upwards). See Figure 2.

(F2) Each segment $(\phi_i \, \phi_{i+1})$ and each triangle $\Delta_i = (0 \, \phi_i \, \phi_{i+1})$ has no interior integer points. This can be deduced from the facts that two consecutive Fibonacci numbers are coprime, and also

$$F_i F_{i+3} - F_{i+1} F_{i+2} = (-1)^{i-1} \quad \text{for all } i \geq 0.$$

(F3) The set of integer points in $J \backslash \Phi$ can be partitioned into 2 parts: those lying strictly above the convex curve $\mathcal{C}$, and those lying strictly below it.

(F4) The part of $J \backslash \Phi$ lying above $\mathcal{C}$ is exactly $R_1 \cap \mathbb{Z}^2$. This can be seen as follows. The line ℓ connecting 0 and ϕ_d is defined by:

$$y_2 F_{2d-1} - y_1 F_{2d-2} = 0.$$

So every integer point $\mathbf{y} = (y_1, y_2)$ lying above ℓ satisfies:

$$y_2 F_{2d-1} - y_1 F_{2d-2} \geq 1.$$

By property (F2), there are no integer points $\mathbf{y}$ between $\mathcal{C}$ and ℓ. The other two edges of R_1 come from J. See Figure 2.

(F5) The part of $J \backslash \Phi$ lying below $\mathcal{C}$ is exactly $R_2 \cap \mathbb{Z}^2$. This can be seen as follows. The line connecting ϕ_i and ϕ_{i+1} is defined by

$$y_2 F_{2i} - y_1 F_{2i-1} = -1.$$

So all integer points below that line satisfies:

$$y_2 F_{2i} - y_1 F_{2i-1} \leq -2.$$

This gives $d-1$ faces for R_2, one for each $1 \leq i \leq d-1$. The other two faces of R_2 come from J. See Figure 2.

3.2 The polytopes

Given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and $\epsilon \in (0, \frac{1}{2}) \cap \mathbb{Q}$, for each $1 \leq i \leq d$, we define two polygons:

$$P_i = \{(x, w) \in \mathbb{R}^2 \quad : \quad 1 \leq x \leq N, \quad \alpha_i x - \epsilon \leq w \leq \alpha_i x + \epsilon\}, \tag{3.5}$$

and

$$Q_i = \{(x, w) \in \mathbb{R}^2 \quad : \quad 1 \leq x \leq N, \quad \alpha_i x + \epsilon - 1 < w \leq \alpha_i x + \epsilon\}. \tag{3.6}$$

Next, for each $1 \leq i \leq d$, we define two new polytopes

$$P'_i = \{(x, \phi_i, w) : (x, w) \in P_i\} \subset \mathbb{R}^4, \tag{3.7}$$

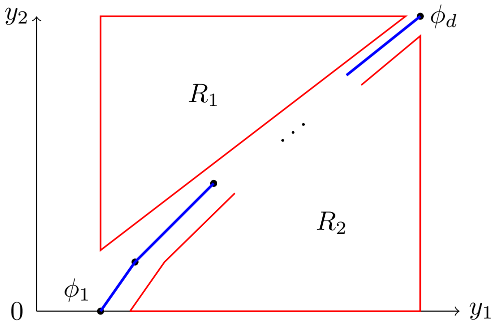

Figure 2 The points $\phi_1, \dots, \phi_d \in \Phi$ form a convex curve $\mathcal{C}$ (blue).

and

$$Q_i' = \{(x, \phi_i, w) : (x, w) \in Q_i\} \subset \mathbb{R}^4, \tag{3.8}$$

where ϕ_i is from (3.1). Finally, we define the convex hulls:

$$P = \operatorname{conv}(P_1', \dots, P_d') \subset \mathbb{R}^4, \tag{3.9}$$

and

$$Q = \operatorname{conv}(Q_1', \dots, Q_d') \subset \mathbb{R}^4. \tag{3.10}$$

The following properties are straightforward from the above definitions:

(P1) Each P_i is a parallelogram with vertices $\big\{(1, \alpha_i \pm \epsilon),\ (N, \alpha_i N \pm \epsilon)\big\}$.

(P2) Each Q_i is a (partially open) parallelogram with vertices

$$\big\{(1, \alpha_i + \epsilon),\ (1, \alpha_i + \epsilon - 1),\ (N, \alpha_i N + \epsilon),\ (N, \alpha_i N + \epsilon - 1)\big\}.$$

(P3) Each P_i' is a *parallelogram* in $\mathbb{R}^4$ (i.e., a Minkowski sum of two intervals), with vertices $\big\{(1, \phi_i, \alpha_i \pm \epsilon),\ (N, \phi_i, \alpha_i N \pm \epsilon)\big\}$.

(P4) Each Q_i' is a (partially open) parallelogram in $\mathbb{R}^4$, with vertices

$$\big\{(1, \phi_i, \alpha_i + \epsilon),\ (1, \phi_i, \alpha_i + \epsilon - 1),\ (N, \phi_i, \alpha_i N + \epsilon),\ (N, \phi_i, \alpha_i N + \epsilon - 1)\big\}.$$

(P5) We have $P_i \subsetneq Q_i$, $P_i' \subsetneq Q_i'$ and $P \subsetneq Q$. Each P_i' forms a 2-dimensional face of P. Each Q_i' forms a 2-dimensional face of Q.

(P6) All the vertices of $P_1', \dots, P_d'$ are in convex position. This follows from (3.7) and (F1).

(P7) The polytope P has $4d$ vertices, which are all the vertices of $P_1', \dots, P_d'$. For every vertex $(x, \mathbf{y}, w)$ of P, we have $\mathbf{y} \in \Phi$, by (P3) and (P6).

(P8) For every $\phi_i \in \Phi$, we have:

$$\big\{(x, w) \in \mathbb{R}^2 : (x, \phi_i, w) \in P\big\} = P_i.$$

(P9) All the vertices $Q_1', \dots, Q_d'$ are also in convex position, by (3.8) and (F1).

(P10) The polytope Q has $4d$ vertices, which are all the vertices of $Q_1', \dots, Q_d'$. For every vertex $(x, \mathbf{y}, w)$ of Q, we have $\mathbf{y} \in \Phi$, by (P4) and (P9).

(P11) For every $\phi_i \in \Phi$, we have:

$$\big\{(x, w) \in \mathbb{R}^2 : (x, \phi_i, w) \in Q\big\} = Q_i.$$

(P12) For every point $(x, \mathbf{y}, w) \in P \cap \mathbb{Z}^4$, we have either $\mathbf{y} \in \Phi$ or $\mathbf{y} \in R_2$. This follows from (3.9), (F1) and (F5). The same holds for Q.

We will be using these properties in the latter sections.

4 Proof of Theorem 2

4.1

By a *box* in $\mathbb{Z}^d$, we mean the set of integer points of the form $[\alpha_1, \beta_1] \times \cdots \times [\alpha_d, \beta_d] \cap \mathbb{Z}^d$. We will prove the following stronger version of Theorem 2.

▶ **Theorem 9.** *Given a polytope $U \subset \mathbb{R}^6$ and two finite boxes $I \subset \mathbb{Z}$, $J \subset \mathbb{Z}^2$, deciding the sentence*

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists \mathbf{z} \in \mathbb{Z}^3 \quad : \quad (x, \mathbf{y}, \mathbf{z}) \in U \tag{4.1}$$

is an NP*-complete problem. Here U is described by a system $A\,(x, \mathbf{y}, \mathbf{z}) \le \overline{b}$, where $A \in \mathbb{Z}^{m \times 6}$ and $\overline{b} \in \mathbb{Z}^m$.*

Since low dimensional boxes can be easily embedded into higher dimensions, the above implies Theorem 2 for every $d_1 \ge 1, d_2 \ge 3$ and $d_3 \ge 3$. Compared to Theorem 2, all parameters in the above theorem are fixed, except for m. So from now on, the symbols n and d will be reused for other purposes. For a vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{Q}^d$ and an integer $x \in \mathbb{Z}$, we define

$$\{\{x\boldsymbol{\alpha}\}\} = \max_{1 \le i \le d} \{\{q\alpha_i\}\}, \tag{4.2}$$

where for each rational $\beta \in \mathbb{Q}$, the quantity $\{\beta\}$ is defined as:

$$\{\{\beta\}\} \;:=\; \min_{n \in \mathbb{Z}} |\beta - n| \;=\; \min\big\{\beta - \lfloor \beta \rfloor, \lceil \beta \rceil - \beta\big\}.$$

GOOD SIMULTANEOUS APPROXIMATION (GSA)
Input: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{Q}^d$ and $N \in \mathbb{N}$, $\epsilon \in \mathbb{Q}$.
Decide: Is an integer $x \in [1, N]$ such that $\{\{x\boldsymbol{\alpha}\}\} \le \epsilon$?

Note that GSA is only non-trivial for $\epsilon < 1/2$. We need the following result by Lagarias:

▶ **Theorem 10** ([18]). GSA *is* NP*-complete.*

Let us emphasize that in GSA, the number d is part of the input. If d is fixed instead, then the problem can be decided in polynomial time (see [18] and [15, Ch. 5]). What follows is a reduction of GSA to a sentence of the form (4.1). GSA can be expressed as an integer programming problem:

$$\exists\, x, w_1, \dots, w_d \in \mathbb{Z} \quad : \quad 1 \le x \le N, \quad -\epsilon \le \alpha_i x - w_i \le \epsilon. \tag{4.3}$$

The inequalities on w_i can be expressed as $(x, w_i) \in P_i$, where P_i was defined in (3.5). Letting $I = [1, N] \cap \mathbb{Z}$, we see that GSA is equivalent to deciding:

$$\exists x \in I \quad : \quad \bigwedge_{i=1}^{d} \Big[\exists w \in \mathbb{Z} \;:\; (x, w) \in P_i \Big]. \tag{4.4}$$

▶ **Lemma 11.** *Let $\Phi = \{\phi_1, \dots, \phi_d\}$ be as in* (3.2) *and P be as in* (3.9)*. We have:*

$$\{\{x\boldsymbol{\alpha}\}\} \le \epsilon \quad \Longleftrightarrow \quad \forall \mathbf{y} \in \Phi \quad \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P. \tag{4.5}$$

Proof. Indeed, assume $\{\{x\boldsymbol{\alpha}\}\} \le \epsilon$, i.e., x satisfies GSA. By (4.4), for every $i = 1, \dots, d$, there exists $w_i \in \mathbb{Z}$ with $(x, w_i) \in P_i$. Now (P8) implies that $(x, \phi_i, w_i) \in P$. Since this holds for every $\phi_i \in \Phi$, the RHS in (4.5) is satisfied. For the other direction, assume the RHS in (4.5) holds. Then for every $\phi_i \in \Phi$, there exists $w_i \in \mathbb{Z}$ with $(x, \phi_i, w_i) \in P$. By (P8), we have $(x, w_i) \in P_i$. By (4.4), x satisfies GSA, i.e., $\{\{x\boldsymbol{\alpha}\}\} \le \epsilon$. ◀

By the above lemma, GSA is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in \Phi \quad \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P. \tag{4.6}$$

Consider J from (3.2), which contains Φ. We can rewrite the above sentence as:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \big[(\mathbf{y} \in J \backslash \Phi) \ \vee \ \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P\big]. \tag{4.7}$$

Recall the polygons R_1 and R_2 defined in (3.3) and (3.4). By properties (F3), (F4) and (F5), we can rewrite $\mathbf{y} \in J \backslash \Phi$ as $(\mathbf{y} \in R_1) \vee (\mathbf{y} \in R_2)$. Now, we can rewrite (4.7) as:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \big[\,(\mathbf{y} \in R_1) \ \vee \ (\mathbf{y} \in R_2) \ \vee \ \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P\,\big]. \tag{4.8}$$

Next, define two polytopes R_1' and R_2' as follows:

$$R_i' := \big\{(x, \mathbf{y}, 0) \in \mathbb{R}^4 : 0 \le x \le N, \ \mathbf{y} \in R_i\big\} \subset \mathbb{R}^4 \quad \text{for} \quad i = 1, 2. \tag{4.9}$$

Polytopes R_1' and R_2' are defined in such a way so that for every $x \in I$ and $\mathbf{y} \in J$, we have $\mathbf{y} \in R_i$ if and only if there exists $w \in \mathbb{Z}$ such that $(x, \mathbf{y}, w) \in R_i'$.[1] Now, it is clear that (4.8) is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \left[\left(\bigvee_{i=1}^{2} \exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in R_i'\right) \ \vee \ \left(\exists w \in \mathbb{Z} : (x, \mathbf{y}, w) \in P\right)\right].$$

which is equivalent to:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists w \in \mathbb{Z} \quad : \quad (x, \mathbf{y}, w) \in R_1' \cup R_2' \cup P. \tag{4.10}$$

The difference between (4.10) and (4.1) is that we have 3 polytopes instead of just one.

4.2

The final step is two compress three polytopes R_1', R_2' and P into one polytope. Recall from (P7) that P has $4d$ vertices, which correspond to the vertices of all P_i for $1 \le i \le d$. The vertices of R_1 and R_2 can be computed in polynomial time from systems (3.3) and (3.4). From there we easily get the vertices of R_1' and R_2'. Since P, R_1' and R_2' are in the fixed dimension 4, we can write down all their facets in polynomial time using their vertices. So we can represent:

$$\begin{aligned} P &= \left\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \ : \ A_1\,(x, \mathbf{y}, w) \le \bar{b}_1\right\}, \\ R_1' &= \left\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \ : \ A_2\,(x, \mathbf{y}, w) \le \bar{b}_2\right\}, \\ R_2' &= \left\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \ : \ A_3\,(x, \mathbf{y}, w) \le \bar{b}_3\right\}. \end{aligned} \tag{4.11}$$

The above three systems all have lengths polynomial in the input $\boldsymbol{\alpha}, N$ and ϵ. Next, we need the following lemma:

[1] Such a w must automatically be 0 by the definition of R_i'.

▶ **Lemma 12.** *Fix n and r. Given r polytopes $R_1, \dots, R_r \subset \mathbb{R}^n$ described by r systems*

$$R_i = \{\mathbf{x} \in \mathbb{R}^n : A_i\, \mathbf{x} \le \bar{b}_i\},$$

there is a polytope $U \in \mathbb{R}^{n+\ell}$, where $\ell = \lceil \log_2 r \rceil$, such that

$$\mathbf{x} \in \bigcup_{i=1}^{r} R_i \cap \mathbb{Z}^n \quad \iff \quad \exists \mathbf{t} \in \mathbb{Z}^\ell : (\mathbf{x}, \mathbf{t}) \in U \cap \mathbb{Z}^{n+\ell}. \tag{4.12}$$

Furthermore, the system $A\,(\mathbf{x}, \mathbf{t}) \le \bar{b}$ that describes U can be found in polynomial time, given A_i's and $\bar{b}_i$'s as input.

Proof. Let $\ell = \lceil \log_2 r \rceil$, we have $2^\ell \ge r$. Pick $\bar{t}_1, \dots, \bar{t}_r \in \{0,1\}^\ell$ as r different vertices of the ℓ-dimensional unit cube. Define

$$U_j = \{(\mathbf{x}, \bar{t}_j) \in \mathbb{R}^{n+\ell} : \mathbf{x} \in R_j\} \quad \text{for} \quad j = 1, \dots, r\,,$$

and

$$U = \operatorname{conv}(U_1, \dots, U_r).$$

In other words, we form U_j by augmenting each R_j with ℓ coordinates of $\bar{t}_j$. Since $\bar{t}_1, \dots, \bar{t}_r$ are in convex position, so are the new polytopes $U_1, \dots, U_j$. So the vertices of U are all the vertices of all U_j. Note that for every $\mathbf{t} \in \operatorname{conv}(\bar{t}_1, \dots, \bar{t}_r)$, we have $\mathbf{t} \in \mathbb{Z}^\ell$ if and only if $\mathbf{t} = \bar{t}_j$ for some j. This implies that the only integer points in U are those in U_j's. In other words:

$$(\mathbf{x}, \mathbf{t}) \in U \cap \mathbb{Z}^{n+\ell} \quad \iff \quad \mathbf{x} \in R_j \cap \mathbb{Z}^n \;\text{ and }\; \mathbf{t} = \bar{t}_j \;\text{ for some }\; j = 1, \dots, r.$$

So we have (4.12).

For each R_j, its vertices can be computed in polynomial time from the system $A_i\, \mathbf{x} \le \bar{b}_i$. From these, we easily get the vertices for each U_j. Thus, we can find all vertices of U in polynomial time. Note that U is in a fixed dimension $n+\ell$, since n and r are fixed. Therefore, we can find in polynomial time all the facets of U using those vertices. This gives us a system $A\,(\mathbf{x}, \mathbf{t}) \le \bar{b}$ of polynomial length that describes U. ◀

Applying the above lemma for three polytopes R_1', R_2' and P with $n = 4$ and $r = 3$, we find a polytope $U \subset \mathbb{R}^{4+\ell}$ such that:

$$(x, \mathbf{y}, w) \in (R_1' \cup R_2' \cup P) \cap \mathbb{Z}^4 \quad \iff \quad \exists \mathbf{t} \in \mathbb{Z}^\ell : (x, \mathbf{y}, w, \mathbf{t}) \in U \cap \mathbb{Z}^{4+\ell}. \tag{4.13}$$

Here we have $\ell = \lceil \log_2 3 \rceil = 2$, which means $\mathbf{t} \in \mathbb{Z}^2$ and $U \subset \mathbb{R}^6$. The lemma also allows us to find a system $A\,(x, \mathbf{y}, w, \mathbf{t}) \le \bar{b}$ that describes U, which has size polynomial in the systems in (4.11). Now, we can rewrite (4.10) as:

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists w \in \mathbb{Z} \quad : \quad \exists \mathbf{t} \in \mathbb{Z}^2 \quad (x, \mathbf{y}, w, \mathbf{t}) \in U,$$

which is equivalent to

$$\exists x \in I \quad \forall \mathbf{y} \in J \quad \exists \mathbf{z} \in \mathbb{Z}^3 \quad : \quad A\,(x, \mathbf{y}, \mathbf{z}) \le \bar{b}.$$

Here $\mathbf{z} = (w, \mathbf{t}) \in \mathbb{Z}^3$. The final system $A\,(x, \mathbf{y}, \mathbf{z}) \le \bar{b}$ still has size polynomial in the original input $\boldsymbol{\alpha}, N$ and ϵ. Therefore, the original GSA problem is equivalent to (4.1). This implies that (4.1) is NP-hard.

It remains to show that (4.1) is in NP. We argue that more general sentence (1.2) is also in NP. From a result in [14], if (1.2) is true, there must be an $\mathbf{x}$ satisfying it with length polynomial in the input P, A and $\bar{b}$. For such an $\mathbf{x}$, we can apply Theorem 1 to check the rest of the sentence, which has the form $\forall \mathbf{y} \exists \mathbf{z}$, in polynomial time. This shows that deciding (1.2) is in NP, and thus NP-complete. ◀

5 Proof of Theorem 4

Recall the definition of boxes from Section 4. In this section, we prove:

▶ **Theorem 13.** *Fix $k \geq 1$. Given a polytope $U \subset \mathbb{R}^{k+7}$ and finite boxes $I_1, \dots, I_k \subset \mathbb{Z}$, $J \subset \mathbb{Z}^2$, $K \subset \mathbb{Z}^5$, then the problem of deciding:*

$$Q_1\, x_1 \in I_1 \quad \dots \quad Q_k\, x_k \in I_k \quad \forall \mathbf{y} \in J \quad \exists \mathbf{z} \in K \quad : \quad (\mathbf{x}, \mathbf{y}, \mathbf{z}) \in U \tag{5.1}$$

is $\mathbf{\Sigma}_k^{\mathsf{P}}$ complete if $Q_1 = \exists$, and $\mathbf{\Pi}_k^{\mathsf{P}}$ complete if $Q_1 = \forall$. Here $Q_1, \dots, Q_k \in \{\exists, \forall\}$ are k alternating quantifiers with $Q_k = \exists$. The polytope U is described by a system $A\,(\mathbf{x}, \mathbf{y}, \mathbf{z}) \leq \bar{b}$, where $A \in \mathbb{Z}^{m \times (k+7)}$ and $\bar{b} \in \mathbb{Z}^m$.

For the proof, we work with the canonical problem Q3SAT. Let Ψ a Boolean expression of the form:

$$\Psi(\mathbf{u}_1, \dots, \mathbf{u}_k) = \bigwedge_{i=1}^{N} (a_i \vee b_i \vee c_i). \tag{5.2}$$

Here each $\mathbf{u}_j = (u_{j1}, \dots, u_{j\ell}) \in \{0,1\}^\ell$ is a tuple of ℓ Boolean variables, and each a_i, b_i, c_i is a literal in the set $\{u_{js},\ \neg u_{js}\ :\ 1 \leq j \leq k,\ 1 \leq s \leq \ell\}$. From Ψ, we construct a sentence:

$$Q_1\, \mathbf{u}_1 \in \{0,1\}^\ell \quad Q_2\, \mathbf{u}_2 \in \{0,1\}^\ell \ \dots\ Q_k\, \mathbf{u}_k \in \{0,1\}^\ell \quad : \quad \Psi(\mathbf{u}_1, \dots, \mathbf{u}_k). \tag{5.3}$$

Here $Q_1, Q_2, \dots, Q_k \in \{\forall, \exists\}$ are k alternating quantifiers with $Q_k = \exists$. The numbers ℓ and N are part of the input.

QUANTIFIED 3-SATISFIABILITY (Q3SAT)
Input: A Boolean expression Ψ of the form (5.2).
Decide: The truth of the sentence (5.3).

For clarity, we use the notation Q3SAT_k to emphasize problem (5.3) for a fixed k. It is well-known that Q3SAT_k is $\mathbf{\Sigma}_k^{\mathsf{P}}$-complete if $Q_1 = \exists$ and $\mathbf{\Pi}_k^{\mathsf{P}}$-complete if $Q_1 = \forall$ (see e.g. [23, 20] and [1]). We proceed to reduce (5.3) to (5.1). In fact, by representing each Boolean string $\mathbf{u}_j \in \{0,1\}^\ell$ as an integer $x_j \in [0, 2^\ell)$, we will only need to use $I_1 = I_2 = \dots = I_k = [0, 2^\ell) \cap \mathbb{Z}$.

For every string $\mathbf{u}_j = (u_{j1}, \dots, u_{j\ell}) \in \{0,1\}^\ell$, let $x_j \in [0, 2^\ell)$ be the corresponding integer in binary. Then u_{js} is true or false respectively when the s-th binary digit of x_j is 1 or 0. In other words, u_{js} is true or false respectively when $\lfloor x_j / 2^{s-1} \rfloor$ is odd or even. Observe that $t = \lfloor x_j / 2^{s-1} \rfloor$ is the only integer that satisfies $x_j/2^{s-1} - 1 < t \leq x_j / 2^{s-1}$. Now, each term u_{js} or $\neg u_{js}$ can be expressed in x_j as follows:

$$\begin{aligned} u_{js} \iff \exists w \in \mathbb{Z}\ :\ &\begin{Bmatrix} 2w+1 & > & x_j/2^{s-1} - 1 \\ 2w+1 & \leq & x_j/2^{s-1} \end{Bmatrix}, \\ \neg u_{js} \iff \exists w \in \mathbb{Z}\ :\ &\begin{Bmatrix} 2w & > & x_j/2^{s-1} - 1 \\ 2w & \leq & x_j/2^{s-1} \end{Bmatrix}. \end{aligned} \tag{5.4}$$

Let $\mathbf{x} = (x_1, \dots, x_k) \in [0, 2^\ell)^k$. Recall that each term a_i, b_i, c_i in (5.2) is u_{js} or $\neg u_{js}$ for some j and s. So each clause $a_i \vee b_i \vee c_i$ can be expressed in $\mathbf{x}$ as:

$$a_i \vee b_i \vee c_i \iff \exists w \in \mathbb{Z}\ :\ \left[D_i\,(\mathbf{x}, w) \leq \bar{d}_i\right] \vee \left[E_i(\mathbf{x}, w) \leq \bar{e}_i\right] \vee \left[F_i\,(\mathbf{x}, w) \leq \bar{f}_i\right], \tag{5.5}$$

where three systems $D_i(\mathbf{x},w) \le \overline{d}_i$, $E_i(\mathbf{x},w) \le \overline{e}_i$, $F_i(\mathbf{x},w) \le \overline{f}_i$ are of the form (5.4) (with different j and s for each). Note that the strict inequalities in (5.4) can be sharpened without losing any integer solutions (see Remark 2). We define the polytopes:

$$\begin{aligned} K_i &= \bigl\{(\mathbf{x},w) \in \mathbb{R}^{k+1} \ : \ x_1,\dots,x_k,w \in [0,2^\ell),\ D_i(\mathbf{x},w) \le \overline{d}_i\bigr\},\\ L_i &= \bigl\{(\mathbf{x},w) \in \mathbb{R}^{k+1} \ : \ x_1,\dots,x_k,w \in [0,2^\ell),\ E_i(\mathbf{x},w) \le \overline{e}_i\bigr\},\\ M_i &= \bigl\{(\mathbf{x},w) \in \mathbb{R}^{k+1} \ : \ x_1,\dots,x_k,w \in [0,2^\ell),\ F_i(\mathbf{x},w) \le \overline{f}_i\bigr\}. \end{aligned}$$

So the RHS in (5.5) can be rewritten as:

$$\exists w \in \mathbb{Z} \ : \ (\mathbf{x},w) \in K_i \cup L_i \cup M_i.$$

Let $I_1 = I_2 = \cdots = I_k = [0,2^\ell) \cap \mathbb{Z}$, we see that (5.3) is equivalent to:

$$Q_1\, x_1 \in I_1 \quad \dots \quad Q_k\, x_k \in I_k \quad : \quad \bigwedge_{i=1}^{N} \Bigl[\exists w \in \mathbb{Z} \ : \ (\mathbf{x},w) \in K_i \cup L_i \cup M_i\Bigr]. \tag{5.6}$$

For each i, we apply Lemma 12 (with $n = k+1$, $r = 3$) to the polytopes $K_i, L_i, M_i \subset \mathbb{R}^{k+1}$. This gives us another polytope $G_i \subset \mathbb{R}^{k+3}$ that satisfies:

$$(\mathbf{x},w) \in K_i \cup L_i \cup M_i \qquad \Longleftrightarrow \qquad \exists \mathbf{v} \in \mathbb{Z}^2 \ : \ (\mathbf{x},w,\mathbf{v}) \in G_i.$$

Substituting this into (5.6), we have an equivalent sentence:

$$Q_1\, x_1 \in I_1 \quad \dots \quad Q_k\, x_k \in I_k \quad : \quad \bigwedge_{i=1}^{N} \Bigl[\exists \mathbf{w} \in \mathbb{Z}^3 \ : \ (\mathbf{x},\mathbf{w}) \in G_i\Bigr], \tag{5.7}$$

where $\mathbf{w} = (w,\mathbf{v}) \in \mathbb{Z}^3$, and each $G_i \subset \mathbb{R}^{k+3}$.

Notice that apart from the outer quantifiers, (5.7) is a direct analogue of (4.4), with G_i playing the role of P_i and $(\mathbf{x},\mathbf{w})$ in place of (x,w). The proof now proceeds similarly to the rest of Section 4 after (4.4). Along the proof, we need to define G'_i and G in similar manners to (3.7) and (3.9). The variable $\mathbf{y} \in \mathbb{Z}^2$ is again needed to define G'_i. Φ and J from (3.2) are reused without change. This gives us $G'_i, G \subset \mathbb{R}^{k+5}$. At the end of the proof, we also need to apply Lemma 12 one more time to produce a single polytope U, just like in (4.13). The dimension 4 in (4.13) is now $k+5$. As a result, the final polytope U has dimension $k+7$. In the final form (5.1), we will have $\mathbf{x} \in \mathbb{Z}^k, \mathbf{y} \in \mathbb{Z}^2$ and $\mathbf{z} = (\mathbf{w},\mathbf{t}) \in \mathbb{Z}^5$.

We have converted (5.3) to an equivalent sentence (5.1) with polynomial size. This shows that (5.1) is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-hard depending when $Q_1 = \exists/\forall$. For each tuple $\mathbf{x} = (x_1,\dots,x_k)$, we can check in polynomial time whether $\forall \mathbf{y} \in J \ \ \exists \mathbf{z} \in K \ \ : \ \ A(\mathbf{x},\mathbf{y},\mathbf{z}) \le \overline{b}$ by applying Theorem 1. This shows the membership of (5.1) in $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$. We conclude that (5.1) is $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete when $Q_1 = \exists/\forall$. ◀

6 Proof of Theorem 7

6.1

Now we prove Theorem 7. We use the same construction as in the proof of Theorem 2. Recall the definition of $\{\{x\boldsymbol{\alpha}\}\}$ from Section 4. We reduce the following counting problem to a problem of the form (1.4):

#GOOD SIMULTANEOUS APPROXIMATIONS (#GSA)

Input: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and positive integers N, s_1, s_2.

Output: The number of integers $x \in [1, N]$ that satisfy $\{\{x\boldsymbol{\alpha}\}\} \le s_1/s_2$.

The argument in [18] is based on a parsimonious reduction. Namely, it gives a bijection between solutions for #GSA and the following problem:

#WEAK PARTITIONS

Input: An integer vector $\overline{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d$.

Output: The number of $\mathbf{y} \in \{-1, 0, 1\}^d$ for which $\overline{a} \cdot \mathbf{y} = 0$.

It is well known and easy to see that #WEAK PARTITIONS is #P-complete. The decision version WEAK PARTITION was earlier shown by [27] to be NP-complete with a parsimonious reduction from KNAPSACK. Together with Lagarias's reduction, we conclude:

▶ **Theorem 14.** #GSA *is* #P*-complete.*

6.2

Now we proceed with the reduction of #GSA to (1.4).

Recall Φ and J from (3.2). We use the notations from section 3.1 and 3.2. Let P_i, P_i' and P be from (3.5), (3.7) and (3.9). Let Q_i, Q_i' and Q be from (3.6), (3.8) and (3.10). Let $I = [1, N] \cap \mathbb{Z}$. We have:

▶ **Observation 15.** *For every $x \in I$, there is a unique $w \in \mathbb{Z}$ such that $(x, w) \in Q_i$.*

Indeed, from (3.6), we have $(x, w) \in Q_i$ if and only if $x \in I$ and:

$$\alpha_i x + \epsilon - 1 < w \le \alpha_i x + \epsilon.$$

For each $x \in I$, we get a half-open interval of length 1 for w, which has a unique integer.

▶ Remark 2. Note that each Q_i has an open edge defined by $\alpha_i x + \epsilon - 1 < w$. This can actually be sharpened without losing any integer point. Indeed, we can multiply the inequality with the denominators in α_i and ϵ, which have polynomial length. Then the resulting strict integer inequality of the form $a < b$ is equivalent to $a \le b - 1$. Therefore, we can replace Q_i with a (smaller) closed parallelogram containing the same integer points. Taking the convex hull as in (3.10), we can similarly replace Q with a (smaller) closed polyhedron, without losing any integer points in Q.

▶ **Observation 16.** *For every $x \in I$ and $\phi_i \in \Phi$, there is a unique integer point $(x, \phi_i, w_i) \in Q$.*

Indeed, by (P11), for every $\phi_i \in \Phi$, we have $(x, \phi_i, w) \in Q$ if and only if $(x, w) \in Q_i$. Together with Observation 15, we have Observation 16.

Recall from (P5) that $P \subset Q$. Now consider the following set:

$$S = \big\{ x \in I \ : \ \exists (\mathbf{y}, w) \in \Phi \times \mathbb{Z} \quad (x, \mathbf{y}, w) \in Q \backslash P \big\}.^2 \tag{6.1}$$

▶ **Lemma 17.** *For every $x \in I$, we have $\{\{x\boldsymbol{\alpha}\}\} > \epsilon$ if and only if $x \in S$.*

Proof. Assume $x \in S$, then there exist some $\phi_j \in \Phi$ and $w_j \in \mathbb{Z}$ so that $(x, \phi_i, w_i) \in Q \backslash P$. By Observation 16 and the fact that $P \subset Q$, there is no $w \in \mathbb{Z}$ for which $(x, \phi_i, w) \in P$. By (4.5), we have $\{\{x\boldsymbol{\alpha}\}\} > \epsilon$. Conversely, assume $\{\{x\boldsymbol{\alpha}\}\} > \epsilon$. By (4.5), there exist $\phi_i \in \Phi$ so that there is no $w \in \mathbb{Z}$ with $(x, \phi_i, w) \in P$. By Observation 16, the unique point (x, ϕ_i, w_i) in Q must be outside of P, i.e., $(x, \phi_i, w_i) \in Q \backslash P$. We conclude that $x \in S$ by (6.1). ◀

By the above lemma, counting S is equivalent to #GSA. The formulation (6.1) is very similar to (1.4), with $(\mathbf{y}, w)$ in place of $\mathbf{z}$. We cannot conclude directly that S is $\mathrm{E}_1(Q \backslash P)$ because of the restricted quantifier $\exists \mathbf{y} \in \Phi$ instead of $\exists \mathbf{y} \in \mathbb{Z}^2$. To turn S into the form (1.4), we need to convert $\exists \mathbf{y} \in \Phi$ to $\exists \mathbf{y} \in \mathbb{Z}^2$.

6.3

The final step is to modify the polytopes P and Q. In (6.1), we only consider projections of integer points $(x, \mathbf{y}, w) \in Q \backslash P$ with $\mathbf{y}$ restricted to the set Φ. In general, the complement $Q \backslash P$ has some other integer points $(x, \mathbf{y}, w)$ with $\mathbf{y}$ not lying in Φ. By (P12) such a point must necessarily have $\mathbf{y} \in R_2$. We can eliminate all of them by taking the convex hulls of P and Q with a "high enough" box over R_2. Below are the details.

Let $T = 1 + N \max_i \alpha_i$. By (3.5) and (3.6), we have $P_i, Q_i \subset [1, N] \times [-1, T]$. Recall from (3.7) and (3.9) that P is the convex hull of all P_i', which is simply P_i with an added second component ϕ_i. This leads to the following observation:

▶ **Observation 18.** *For every vector $\overline{\gamma} \in \mathbb{R}^2$, we have:*

$$\big\{(x, \mathbf{y}, w) \in P \ : \ \mathbf{y} = \overline{\gamma}\big\} \subseteq [1, N] \times \{\overline{\gamma}\} \times [-1, T].$$

The same holds for Q.

Next, consider the rectangular box J containing Φ and the complement $J \backslash \Phi$, where J is from (3.2). From properties (F3), (F4) and (F5), integer points in the complement $J \backslash \Phi$ lie in two separate convex polygons R_1 and R_2, as described in (3.3) and (3.4). We will only need R_2, which contains integer points below Φ. Define

$$R = \big\{(x, \mathbf{y}, w) \in \mathbb{R}^4 \quad : \quad x \in [1, N], \quad \mathbf{y} \in R_2, \quad w \in [-1, T]\big\}. \tag{6.2}$$

and

$$\widetilde{P} = \operatorname{conv}(P, R) \ , \quad \widetilde{Q} = \operatorname{conv}(Q, R) \quad \subset \quad \mathbb{R}^4. \tag{6.3}$$

For $\overline{\gamma} \in \mathbb{R}^2$, we denote by $P_{\overline{\gamma}}$ the set:

$$P_{\overline{\gamma}} = \big\{(x, \mathbf{y}, w) \in P \ : \ \mathbf{y} = \overline{\gamma}\big\},$$

and analogously for $\widetilde{P}_{\overline{\gamma}}$, $Q_{\overline{\gamma}}$, $\widetilde{Q}_{\overline{\gamma}}$ and $R_{\overline{\gamma}}$.

By Observation 18, for every $\overline{\gamma}$, we have $P_{\overline{\gamma}}$, $Q_{\overline{\gamma}} \subseteq [1, N] \times \{\overline{\gamma}\} \times [-1, T]$. From (6.2), we have $R_{\overline{\gamma}} = [1, N] \times \{\overline{\gamma}\} \times [-1, T]$ for every $\overline{\gamma} \in R_2$. Since $\widetilde{P} = \operatorname{conv}(P, R)$ and $\widetilde{Q} = \operatorname{conv}(Q, R)$, we have

$$\widetilde{P}_{\overline{\gamma}} = \widetilde{Q}_{\overline{\gamma}} = [1, N] \times \{\overline{\gamma}\} \times [-1, T] \quad \text{for every } \overline{\gamma} \in R_2. \tag{6.4}$$

For $\overline{\gamma} \in \Phi$, we claim that:

$$\widetilde{P}_{\overline{\gamma}} = P_{\overline{\gamma}} \quad \text{and} \quad \widetilde{Q}_{\overline{\gamma}} = Q_{\overline{\gamma}}. \tag{6.5}$$

Indeed, since $\overline{\gamma} \in \Phi$, we have $\overline{\gamma} = \phi_i$ and $P_{\overline{\gamma}} = P_{\phi_i}$ for some i. By (3.7) and (P8), we have $P_{\phi_i} = P'_i$. Since $R_2 \cap \Phi = \varnothing$, we have $\phi_i \notin R_2$. This implies $P'_i \cap R = \varnothing$, because R is a box over R_2, and P'_i is a parallelogram over ϕ_i. Recall from (P5) that P'_i forms a 2-dimensional face of P. Therefore, it still remains a 2-dimensional face of the convex hull $\widetilde{P} = \operatorname{conv}(P, R)$. So $\widetilde{P}_{\overline{\gamma}} = P_{\overline{\gamma}} = P'_i$. The same argument applies to $\widetilde{Q}_{\overline{\gamma}}$ and $Q_{\overline{\gamma}}$.

Note that we also have $\widetilde{P} \subset \widetilde{Q}$, because $P \subset Q$. Consider the complement $\widetilde{Q} \backslash \widetilde{P}$. Assume $(x, \mathbf{y}, w) \in \mathbb{Z}^3$ is an integer point in $\widetilde{Q} \backslash \widetilde{P}$. By (6.4), such a point cannot exist for $\mathbf{y} \in R_2$. So we must have $\mathbf{y} \in \Phi$. Now by (6.5), we also have $(x, \mathbf{y}, w) \in Q \backslash P$. Therefore, from (6.1), we conclude that:

$$\begin{aligned} S &= \big\{x \in [1, N] \cap \mathbb{Z} \quad : \quad \exists (\mathbf{y}, w) \in \mathbb{Z}^3 \quad (x, \mathbf{y}, w) \in \widetilde{Q} \backslash \widetilde{P}\big\} \\ &= \big\{x \in [1, N] \cap \mathbb{Z} \quad : \quad \exists \mathbf{z} \in \mathbb{Z}^3 \quad (x, \mathbf{z}) \in \widetilde{Q} \backslash \widetilde{P}\big\}. \end{aligned}$$

Here $\mathbf{z} = (\mathbf{y}, w)$. The systems describing $\widetilde{Q}$ and $\widetilde{P}$ can be obtained in polynomial time from the input $\boldsymbol{\alpha}, N$ and ϵ. First, the vertices of P and Q are given by (P7) and (P10). The vertices of R directly come from those of R_2, which can be found from (3.4). By (6.3), we can obtain the vertices of $\widetilde{P}$ and $\widetilde{Q}$. The facets of $\widetilde{P}$ and $\widetilde{Q}$ can be found from their vertices in polynomial time, since both polytopes are in the fixed dimension 4. In summary, problem (1.4) applied to $\widetilde{P}$ and $\widetilde{Q}$ is #P-complete. This proves Theorem 7. ◀

6.4 Proof of Corollary 8

By Theorem 7, counting $|\mathrm{E}_1(Q \backslash P)|$ is #P-complete for $P \subset Q \subset \mathbb{R}^4$. Nevertheless, the complement $Q \backslash P$ can still be triangulated into polynomially many simplices $T_1 \sqcup \cdots \sqcup T_r$. In fact, by an application of Proposition 5.2.2 in [29], the systems describing all such T_i can be found in polynomial time. Therefore, counting $|\mathrm{E}_1(T_1 \sqcup \cdots \sqcup T_r)| = |\mathrm{E}_1(Q \backslash P)|$ is #P-complete. ◀

7 Final remarks and open problems

7.1

It is sufficient to prove Theorem 1 for the case when m, n are also bounded. In the system $A\,(\mathbf{x}, \mathbf{y}) \leq b$, we view $\mathbf{x}$ as the parameters and $\mathbf{y}$ as the variables to be solved for. For a fixed d_2 and $m \geq 2^{d_2}$, the *Doignon–Bell–Scarf theorem* [26, §16.5] implies that the system $A\,(\mathbf{x}, \mathbf{y}) \leq \overline{b}$ is solvable in $\mathbf{y} \in \mathbb{Z}^{d_2}$ if and only if every subsystem $A'\,(\mathbf{x}, \mathbf{y}) \leq \overline{b'}$ is solvable. Here A' is a submatrix with 2^{d_2} rows from A with $\overline{b'}$ the corresponding subvector from $\overline{b}$. In other words:

$$\exists \mathbf{y} \in \mathbb{Z}^{d_2} \quad A\,(\mathbf{x}, \mathbf{y}) \leq \overline{b} \qquad \Longleftrightarrow \qquad \bigwedge_{(A', \overline{b'})} \Big[\exists \mathbf{y} \in \mathbb{Z}^{d_2} \quad A'\,(\mathbf{x}, \mathbf{y}) \leq \overline{b'}\Big].$$

The total number of pairs $(A', \overline{b'})$ is $\displaystyle\binom{m}{2^{d_2}}$, which is polynomial in m.

Note that the conjunction over all $(A', \overline{b'})$ commutes with the universal quantifier $\forall \mathbf{x}$. Therefore:

$$\forall \mathbf{x} \in P \cap \mathbb{Z}^{d_1} \;\; \exists \mathbf{y} \in \mathbb{Z}^{d_2} \;\; A\,(\mathbf{x}, \mathbf{y}) \leq \overline{b} \;\; \Longleftrightarrow \;\; \bigwedge_{(A', \overline{b'})} \Big[\forall \mathbf{x} \in P \cap \mathbb{Z}^{d_1} \;\; \exists \mathbf{y} \in \mathbb{Z}^{d_2} \;\; A'\,(\mathbf{x}, \mathbf{y}) \leq \overline{b'}\Big].$$

Thus, it is equivalent to check each of the smaller subproblems, each of which has $m = 2^{d_2}$. Recall that the number of facets in P is n, which can still be large. However, given the system $C\,\mathbf{x} \le \overline{\gamma}$ describing P, we can triangulate P into to a union of simplices $P_1 \sqcup \cdots \sqcup P_k$. Since the dimension d_1 is bounded, we can find such a triangulation in polynomial time (see e.g. [9]). Now for each pair $(A', \overline{b'})$, we have:

$$\forall \mathbf{x} \in P \cap \mathbb{Z}^{d_1} \;\; \exists \mathbf{y} \in \mathbb{Z}^{d_2} \;\; A'\,(\mathbf{x}, \mathbf{y}) \le \overline{b'} \quad \Longleftrightarrow \quad \bigwedge_{i=1}^{k} \Big[\forall \mathbf{x} \in P_i \cap \mathbb{Z}^{d_1} \;\; \exists \mathbf{y} \in \mathbb{Z}^{d_2} \;\; A'\,(\mathbf{x}, \mathbf{y}) \le \overline{b'} \Big].$$

Each simplex $P_i \subset \mathbb{R}^{d_1}$ has $d_1 + 1$ facets. Each subsentence in the RHS now has $m = 2^{d_2}$ and $d_1 + 1$. Note that the total number of such subsentences is still polynomial, so it suffices to check each of them individually.

For three quantifiers $\exists \mathbf{x}\ \forall \mathbf{y}\ \exists \mathbf{z}$, this argument breaks down because the existential quantifier $\exists \mathbf{x}$ no longer commutes with a long conjunction.

7.2

By taking finite Boolean combinations, we see that Theorem 5 also allows counting integer points in a union of k polytopes, where k is bounded (see [3, 4]). In fact, Woods proved in [29, Prop. 5.3.1] that it is still possible to count all such points in polynomial time when k is arbitrary. By Corollary 8, we see that this is not the case for projection.

7.3

The GSA Problem plays an important role in both Number Theory and Integer Programming especially in connection to lattice reduction algorithms (see e.g. [15]). Let us mention that via a chain of parsimonious reductions one can show that #GSA is also hard to approximate (cf. [13]). Note also that GSA has been recently used in a somewhat related geometric context in [12].

7.4

An easy consequence of Lemma 12 proves the first part of the following result:

▶ **Proposition 19.** *Every set $S = \{\overline{p}_1, \ldots, \overline{p}_r\} \subset \mathbb{Z}^2$ is a projection of integer points of some convex polytope $P \subset \mathbb{R}^{2+d}$, where $d \le \lceil \log_2 r \rceil$. Moreover, the bound $d \le \lceil \log_2 r \rceil$ is tight.*

We only use the proposition to reduce the dimension of variable $\mathbf{z}$ in Theorem 9 from 4 to 3, but it is perhaps of independent interest. Note that a weaker inequality $d \le r$ is trivial.

Proof of the Second Part of Proposition 19. Consider a set $S = \{\overline{p}_1, \ldots, \overline{p}_r\}$ of integer points in convex position and with even coordinates. Assume there is a polytope $P \subset \mathbb{R}^{2+\ell}$ with $\ell < \lceil \log_2 r \rceil$ so that S is exactly the projection of $P \cap \mathbb{Z}^{2+\ell}$ on $\mathbb{Z}^2$. Then there are integer points $\overline{q}_1, \ldots, \overline{q}_r \in \mathbb{Z}^\ell$ so that $(\overline{p}_i, \overline{q}_i) \in P$. Since $r > 2^\ell$, by the pigeonhole principle, we have $\overline{q}_i - \overline{q}_j \in 2\mathbb{Z}^\ell$ for some $i \ne j$. Then the midpoint of $(\overline{p}_i, \overline{q}_i)$ and $(\overline{p}_j, \overline{q}_j)$ is an integer point in $\mathbb{Z}^{2+\ell}$, which also lies in P by convexity. The projection of this midpoint on $\mathbb{Z}^2$ is $(\overline{p}_i + \overline{p}_j)/2$, which must lie in S. However, the points in S are in convex positions and thus contain no midpoints, a contradiction. ◀

7.5

Let us give another motivation behind Theorem 7 and put it into context of our other work. In this paper, we bypass the "short generating function" technology developed for computing $|\mathrm{E}_1(P)|$ for convex polytopes $P \subset \mathbb{R}^d$. Note, however, that for $X = Q \backslash P$ as in the theorem, the corresponding short GF $f_X(\mathbf{t})$ is simply the difference $f_Q(\mathbf{t}) - f_P(\mathbf{t})$, which can still be computed in polynomial time (see [2]). Thus, if one could efficiently present the projection of $f_X(\mathbf{t})$ on $\mathbb{Z}$ as a short generating function of polynomial size, then one would be able to compute $|\mathrm{E}_1(Q \backslash P)|$, a contradiction. In other words, Theorem 7 is an extension of a result by Woods [28], which shows that computing projecting short generating functions is NP-hard. It is also an effective but weaker version of the main result in [21, Th. 1.3], which deals with the size of short GFs of the projections rather than complexity of their computation.

7.6

Corollary 8 says that computing $|\mathrm{E}_1(T_1 \cup \cdots \cup T_k)|$ is #P-complete even for simplices $T_i \subset \mathbb{R}^4$. By a stronger version of Theorem 6 (see [5]), for each polytope T_i, there is a short generating function $g_i(t)$ representing $\mathrm{E}_1(T_i)$. The union of all those generating functions correspond to $\mathrm{E}_1(T_1 \cup \cdots \cup T_k)$. As a corollary we conclude that the union operation on short generating functions is #P-hard to compute. As in §7.5 above, one should compare this to a stronger result [21, Th. 1.1], which says that the union of short generating functions can actually have super-polynomial lengths unless #P $\subseteq$ FP/poly.

7.7

It would be interesting to see if the dimension 4 in Theorem 7 is sharp and cannot be reduced to 3. One can argue both in favor and against this possibility. First, one can think of the result as a claim about complexity of nonconvex polyhedra $Q \backslash P$ in $\mathbb{R}^d$. For $d = 3$, the three dimensional nonconvex polyhedra are well known to be notoriously complicated to study via triangulations (see e.g. [24], the proof of the Th. 1.2 in [7] and a lengthly discussion in [9]). This suggests that for the "long" first coordinate dimensions of Q, it is unlikely that there is a good way to triangulate $Q \backslash P$ which would allow to compute $|\mathrm{E}_1(Q \backslash P)|$ efficiently.

To argue in the opposite direction, the problem of computing the number of integer points for polytopes in $\mathbb{R}^d$ becomes simpler for $d \leq 3$ (see e.g. [6, 8, 10]), so perhaps there is an ad hoc approach in this case.

7.8

Note that Theorem 9 was proved for dimensions $d_1 = 1, d_2 = 2$ and $d_3 = 3$. One can ask if the problem still remains NP-complete when some of these dimensions are lowered. In particular, it would be interesting to see if the following problem is still NP-complete:

$$\exists x \in P \cap \mathbb{Z} \quad \forall \mathbf{y} \in Q \cap \mathbb{Z}^2 \quad \exists \mathbf{z} \in \mathbb{Z}^2 \quad : \quad (x, \mathbf{y}, \mathbf{z}) \in U,$$

where $P \subset \mathbb{R}$, $Q \subset \mathbb{R}^2$ and $U \subset \mathbb{R}^5$ are convex polytopes.

Acknowledgements. We are grateful to Iskander Aliev, Matthias Aschenbrenner, Sasha Barvinok, Matt Beck, Artëm Chernikov, Jesús De Loera, Matthias Köppe, Sinai Robins and Kevin Woods for interesting conversations and helpful remarks.

References

1 S. Arora and B. Barak. *Computational complexity: A modern approach*. Cambridge University Press, Cambridge, 2009. doi:10.1017/CBO9780511804090.

2 A. Barvinok. A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. In *34th Annual Symposium on Foundations of Computer Science (Palo Alto, CA, 1993)*, pages 566–572. IEEE Comput. Soc. Press, Los Alamitos, CA, 1993. doi:10.1109/SFCS.1993.366830.

3 A. Barvinok. *Integer points in polyhedra*. Zurich Lectures in Advanced Mathematics. European Mathematical Society (EMS), Zürich, 2008. doi:10.4171/052.

4 A. Barvinok and J. E. Pommersheim. An algorithmic theory of lattice points in polyhedra. In *New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97)*, volume 38 of *Math. Sci. Res. Inst. Publ.*, pages 91–147. Cambridge Univ. Press, Cambridge, 1999.

5 A. Barvinok and K. Woods. Short rational generating functions for lattice point problems. *J. Amer. Math. Soc.*, 16(4):957–979, 2003. doi:10.1090/S0894-0347-03-00428-4.

6 M. Beck and S. Robins. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2015. Integer-point enumeration in polyhedra, With illustrations by David Austin. doi:10.1007/978-1-4939-2969-6.

7 A. Below, U. Brehm, J. A. De Loera, and J. Richter-Gebert. Minimal simplicial dissections and triangulations of convex 3-polytopes. *Discrete Comput. Geom.*, 24(1):35–48, 2000. doi:10.1007/s004540010058.

8 M. Brion. Points entiers dans les polytopes convexes. *Séminaire N. Bourbaki*, 36 (1993–1994):145–169, 1995. Talk No. 780. URL: http://www.numdam.org/item?id=SB_1993-1994__36__145_0.

9 J. A. De Loera, J. Rambau, and F. Santos. *Triangulations*, volume 25 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2010. Structures for algorithms and applications. doi:10.1007/978-3-642-12971-1.

10 M. Dyer. On counting lattice points in polyhedra. *SIAM J. Comput.*, 20(4):695–707, 1991. doi:10.1137/0220044.

11 F. Eisenbrand. Integer programming and algorithmic geometry of numbers. In *50 years of integer programming 1958–2008*, pages xx+804. Springer-Verlag, Berlin, 2010. doi:10.1007/978-3-540-68279-0.

12 F. Eisenbrand and N. Hähnle. Minimizing the number of lattice points in a translated polygon. In *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1123–1130. SIAM, Philadelphia, PA, 2012.

13 F. Eisenbrand and T. Rothvoß. New hardness results for Diophantine approximation. In *Approximation, randomization, and combinatorial optimization*, volume 5687 of *Lecture Notes in Comput. Sci.*, pages 98–110. Springer, Berlin, 2009. doi:10.1007/978-3-642-03685-9_8.

14 E. Grädel. *The complexity of subclasses of logical theories*. PhD thesis, Universität Basel, 1978.

15 M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1993. doi:10.1007/978-3-642-78240-4.

16 R. Kannan. Test sets for integer programs, ∀∃ sentences. In *Polyhedral combinatorics (Morristown, NJ, 1989)*, volume 1 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 39–47. Amer. Math. Soc., Providence, RI, 1990.

17 R. Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, 1992. doi:10.1007/BF01204720.

18 J. Lagarias. The computational complexity of simultaneous Diophantine approximation problems. *SIAM J. Comput.*, 14(1):196–209, 1985. doi:10.1137/0214016.

19 H. Lenstra. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983. doi:10.1287/moor.8.4.538.

20 C. Moore and S. Mertens. *The nature of computation.* Oxford University Press, Oxford, 2011. doi:10.1093/acprof:oso/9780199233212.001.0001.

21 D. Nguyen and I. Pak. Complexity of short generating functions, preprint; arxiv:1702.08660, 2017.

22 D. Nguyen and I. Pak. Complexity of short presburger arithmetic. To appear in *STOC'17 – Proceedings of the 2017 ACM Symposium on Theory of Computing*, 2017.

23 C. H. Papadimitriou. *Computational complexity.* Addison-Wesley Publishing Company, Reading, MA, 1994.

24 J. Ruppert and R. Seidel. On the difficulty of triangulating three-dimensional nonconvex polyhedra. *Discrete Comput. Geom.*, 7(3):227–253, 1992. doi:10.1007/BF02187840.

25 U. Schöning. Complexity of Presburger arithmetic with fixed quantifier dimension. *Theory Comput. Syst.*, 30(4):423–428, 1997. doi:10.1007/s002240000059.

26 A. Schrijver. *Theory of linear and integer programming.* Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Ltd., Chichester, 1986. A Wiley-Interscience Publication.

27 P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. *Math. Dept. Report*, pages 81–04, 1981.

28 K. Woods. *Rational Generating Functions and Lattice Point Sets.* PhD thesis, University of Michigan, 2004.

29 K. Woods. Presburger arithmetic, rational generating functions, and quasi-polynomials. *J. Symb. Log.*, 80(2):433–449, 2015. doi:10.1017/jsl.2015.4.