THE COMPUTATIONAL COMPLEXITY OF INTEGER PROGRAMMING WITH ALTERNATIONS

DANNY NGUYEN* AND IGOR PAK*

ABSTRACT. We prove that integer programming with three alternating quantifiers is $\text{NP}$-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 $P, Q \subseteq \mathbb{R}^3$, counting the projection of integer points in $Q \setminus P$ is $\#\text{P}$-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.

1. Introduction

1.1. Background. In a pioneer paper [Len83], 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 [Eis10]).

Theorem 1.1 (Parametric Integer Programming [Kan90]). 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 $\overline{b} \in \mathbb{Z}^m$, the following sentence can be decided in polynomial time:

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

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

In [Kan92], Kannan asked if Theorem 1.1 can be extended to three alternating quantifiers. We give an answer in the negative direction to this question:

Theorem 1.2. 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 $\overline{b} \in \mathbb{Z}^m$, then deciding the sentence

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

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

Let us emphasize that in both Theorem 1.1 and 1.2, there is no bound on the number of inequalities involved. In other words, the parameters $m, n$ and $q$ are not fixed. Theorem 1.2 is especially surprising for the following reasons. First, in [NP17a], we gave strong evidence

*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: {ldnguyen, pak}@math.ucla.edu. September 10, 2017.
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 8.1) as in (1.2). Still, in [NP17a], we speculated that a more involved reduction argument might still apply to (1.2). Theorem 1.2 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 \(P = NP\). In fact, Theorem 1.2 holds even when \(P\) is an interval and \(Q\) is an axis-parallel rectangles (see Theorem 4.1 and §8.8). Thus, the problem (1.2) is already hard when \(n, q\) are fixed and only \(m\) is unbounded.

In [Sch97], Schöning proved that it is NP-complete to decide whether

\[
\exists x \in \mathbb{Z} \forall y \in \mathbb{Z} : \Psi(x, y).
\]

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 1.2 tells us that disjunctions can be discarded at the cost of adding one extra alternation. In the next subsection, we generalize this observation.

On can also consider a “hybrid” version of (1.2) and (1.3) with only 2 quantifiers \(\exists\forall\) and only 2 disjunctions in \(\Psi\). In Section 7, we show this is still \(NP\)-complete to decide.

1.2. Presburger sentences. In [Grä87], 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 [Sch97]. They can be summed up as follows:

**Theorem 1.3 ([Sch97]).** Fix \(k \geq 1\). Let \(\Psi(x, y)\) be a Boolean combination of linear inequalities with integer coefficients in the variables \(x = (x_1, \ldots, x_k) \in \mathbb{Z}^k\) and \(y = (y_1, \ldots, y_3) \in \mathbb{Z}^3\). Then deciding the sentence

\[
Q_1x_1 \in \mathbb{Z} \ldots Q_k x_k \in \mathbb{Z} Q_{k+1}y \in \mathbb{Z}^3 : \Psi(x, y)
\]

is \(\Sigma^P_k\)-complete if \(Q_1 = \exists\), and \(\Pi^P_k\)-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 \(\Psi\) 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 1.2:

**Theorem 1.4.** Integer programming in a fixed number of variables with \(k + 2\) alternating quantifiers is \(\Sigma^P_k/\Pi^P_k\)-complete, depending on whether \(Q_1 = \exists/\forall\). Here the problem is allowed to contain only a system of inequalities.

We refer to Theorem 5.1 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 1.4, the linear system is still allowed many inequalities.
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 1.5** ([Bar93]). 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 \(Ax \leq b\), with \(A \in \mathbb{Z}^{m \times d}, \ b \in \mathbb{Z}^m\).

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

Theorem 1.5 was later generalized by Barvinok and Woods to count the number of integer points in projections of polytopes:

**Theorem 1.6** ([BW03]). 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 \(Ax \leq b\), and \(T\) is described by a matrix \(M\), where \(A \in \mathbb{Z}^{m \times d_1}, \ b \in \mathbb{Z}^m\) and \(M \in \mathbb{Z}^{d_2 \times d_1}\).

For a set \(S \subset \mathbb{R}^d\), denote by \(E_1(S)\) the projection of \(S \cap \mathbb{Z}^d\) on the first coordinate, i.e.,

\[
E_1(S) := \{ x \in \mathbb{Z} : \exists z \in \mathbb{Z}^{d-1} \ (x, z) \in S \}.
\]

By Theorem 1.6, \(|E_1(P)|\) can be computed in polynomial time for every polytope \(P \subset \mathbb{R}^d\).

We prove the following result:

**Theorem 1.7.** Given two polytopes \(P \subset Q \subset \mathbb{R}^3\), computing \(|E_1(Q \setminus P)|\) is \#P-complete.

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

\[
E_1(Q \setminus P) = \{ x \in \mathbb{Z} : \exists z \in \mathbb{Z}^2 \ (x, z) \in Q \setminus P \}.
\]

Note that the corresponding decision problem \(|E_1(Q \setminus P)| \geq 1\) is equivalent to \(|E(Q \setminus P)| \geq 1\), and thus can be decided in polynomial time by applying Theorem 1.5.

The contrast between Theorem 1.6 and our negative result can be explained as follows. The proof Theorem 1.6 depends on the polytopal structure of \(P\) and exploited convexity in a crucial way. By taking the complement \(Q \setminus P\), we no longer have a convex set. In other words, we show that projection of the complement \(Q \setminus P\) is complicated enough to allow encoding of hard counting problems, even in \(\mathbb{R}^3\) (see also §8.5).

![Figure 1](image_url) Three examples of convex polygons \(P, Q \subset \mathbb{R}^2\).
Remark 1.8. 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 $Q \setminus P$ are quite different.

As an easy consequence of Theorem 1.7 we obtain:

Corollary 1.9. Given $r$ simplices $T_1, \ldots, T_r \subset \mathbb{R}^3$, computing $|E_1(T_1 \cup \cdots \cup T_r)|$ 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 1.2 via a reduction of the GOOD SIMULTANEOUS APPROXIMATION (GSA) Problem in Number Theory, which is known to be NP-complete. The proof of Theorem 1.4 is via a reduction of QSAT (Section 5). The proof of Theorem 1.7 follows a similar route via reduction of $\#$GSA (Section 6). Then we show that a “hybrid” version of (1.2) and (1.3) with only 2 quantifiers and 2 disjunctions is still NP-complete to decide (Section 7). Finally, we conclude with final remarks and open problems (Section 8).

2. Notations

We use $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}_+ = \{1, 2, \ldots\}$.

All constant vectors are denoted $\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}, \mathbf{t}$ 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:

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

Let

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

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

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

$$R_1 = \left\{ \mathbf{y} = (y_1, y_2) \in \mathbb{R}^2 : \frac{y_1}{y_2} \geq \frac{1}{F_{2d-2}} \geq \frac{y_1 - y_2 F_{2d-1}}{y_2} \right\}.$$
and

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

The following properties are straightforward from the above definitions:

(F1) The points $\phi_1, \ldots, \phi_d$ are in convex position. The curve $C$ 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

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

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

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

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

So every integer point $y = (y_1, y_2)$ lying above $\ell$ satisfies:

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

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

(F5) The part of $J \setminus \Phi$ lying below $C$ is exactly $R_2 \cap \mathbb{Z}^2$. This can be seen as follows. The line connecting $\phi_1$ and $\phi_{i+1}$ 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.

\[ \text{Figure 2. The points } \phi_1, \ldots, \phi_d \in \Phi \text{ form a convex curve } C \text{ (blue).} \]
3.2. The polytopes. Given $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and $\epsilon \in (0, \frac{1}{2}) \cap \mathbb{Q}$, for each $1 \leq i \leq d$, we define a polygon:

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

Next, for each $1 \leq i \leq d$, we define a new polygon

\[(3.6) \quad P'_i = \{(x, \phi_i, w) : (x, w) \in P_i\} \subset \mathbb{R}^4.\]

Finally, we define the convex hull:

\[(3.7) \quad P = \text{conv}(P'_1, \ldots, P'_d) \subset \mathbb{R}^4.\]

The following properties are straightforward from the above definitions:

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

(P2) Each $P'_i$ is a parallelogram in $\mathbb{R}^4$ (i.e., a Minkowski sum of two intervals), with vertices $\{(1, \phi_i, \alpha_i \pm \epsilon), (N, \phi_i, \alpha_i N \pm \epsilon)\}$.

(P3) The set of all vertices from $P'_1, \ldots, P'_d$ are in convex position. Each $P'_i$ forms a 2-dimensional face of $P$. This follows from (3.6) and (F1).

(P4) The polytope $P$ has $4d$ vertices, which are all the vertices of $P'_1, \ldots, P'_d$.

(P5) For every vertex $(x, y, w)$ of $P$, we have $y = \phi_i \in \Phi$ for some $1 \leq i \leq d$. Conversely, for every $\phi_i \in \Phi$, we have:

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

We will be using these properties in the latter sections.

4. Proof of Theorem 1.2

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 1.2.

Theorem 4.1. Given a polytope $U \subset \mathbb{R}^6$ and two finite boxes $I \subset \mathbb{Z}$, $J \subset \mathbb{Z}^2$, deciding the sentence

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

is an NP-complete problem. Here $U$ is described by a system $A(x, y, z) \leq \overline{b}$, 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 1.2 for every $d_1 \geq 1, d_2 \geq 3$ and $d_3 \geq 3$. Compared to Theorem 1.2, 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 $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and an integer $x \in \mathbb{Z}$, we define

\[(4.2) \quad \{\{x\alpha\}\} = \max_{1 \leq i \leq d} \{\{q\alpha_i\}\},\]

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

\[\{\beta\} := \min_{n \in \mathbb{Z}} |\beta - n| = \min\{\beta - [\beta], [\beta] - \beta\}.\]
GOOD SIMULTANEOUS APPROXIMATION (GSA)

**Input:** A rational vector \( \alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d \) and \( N \in \mathbb{N}, \epsilon \in \mathbb{Q} \).

**Decide:** Is an integer \( x \in [1, N] \) such that \( \{x\alpha\} \leq \epsilon \)?

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

**Theorem 4.2 ([Lag85]).** 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 [Lag85] and [GLS89, 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:

\[
\exists x, w_1, \ldots, w_d \in \mathbb{Z} : 1 \leq x \leq N, -\epsilon \leq \alpha_i x - w_i \leq \epsilon.
\]

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:

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

**Lemma 4.3.** Let \( \Phi = \{\phi_1, \ldots, \phi_d\} \) be as in (3.2) and \( P \) be as in (3.7). We have:

\[
\{x\alpha\} \leq \epsilon \iff \forall y \in \Phi \exists w \in \mathbb{Z} : (x, y, w) \in P.
\]

**Proof.** Indeed, assume \( \{x\alpha\} \leq \epsilon \), i.e., \( x \) satisfies GSA. By (4.4), for every \( i = 1, \ldots, d \), there exists \( w_i \in \mathbb{Z} \) with \( (x, w_i) \in P_i \). Now (P5) 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 (P5), we have \( (x, w_i) \in P_i \). By (4.4), \( x \) satisfies GSA, i.e., \( \{x\alpha\} \leq \epsilon \).

By the above lemma, GSA is equivalent to:

\[
\exists x \in I \forall y \in \Phi \exists w \in \mathbb{Z} : (x, y, w) \in P.
\]

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

\[
\exists x \in I \forall y \in J \left[ (y \in J \setminus \Phi) \lor \exists w \in \mathbb{Z} : (x, y, w) \in P \right].
\]

Recall the polygons \( R_1 \) and \( R_2 \) defined in (3.3) and (3.4). By properties (F3), (F4) and (F5), we can rewrite \( y \in J \setminus \Phi \) as \( (y \in R_1) \lor (y \in R_2) \). Now, we can rewrite (4.7) as:

\[
\exists x \in I \forall y \in J \left[ (y \in R_1) \lor (y \in R_2) \lor \exists w \in \mathbb{Z} : (x, y, w) \in P \right].
\]

Next, define two polytopes \( R'_1 \) and \( R'_2 \) as follows:

\[
R'_i := \{(x, y, 0) \in \mathbb{R}^d : 0 \leq x \leq N, y \in R_i \} \subseteq \mathbb{R}^d \text{ for } i = 1, 2.
\]

Polytopes \( R'_1 \) and \( R'_2 \) are defined in such a way so that for every \( x \in I \) and \( y \in J \), we have \( y \in R_i \) if and only if there exists \( w \in \mathbb{Z} \) such that \( (x, y, w) \in R'_i \).

Now, it is clear that (4.8) is equivalent to:

\[
\exists x \in I \forall y \in J \left[ \left( \bigvee_{i=1}^2 \exists w \in \mathbb{Z} : (x, y, w) \in R'_i \right) \lor \left( \exists w \in \mathbb{Z} : (x, y, w) \in P \right) \right].
\]

\[\text{Such a } w \text{ must automatically be 0 by the definition of } R'_i.\]
which is equivalent to:

\[(4.10) \quad \exists x \in I \quad \forall y \in J \quad \exists w \in \mathbb{Z} \quad : \quad (x, y, w) \in R'_1 \cup R'_2 \cup P.\]

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

4.2. The final step is to two compress three polytopes \(R'_1, R'_2\) and \(P\) into one polytope. Recall from (P4) that \(P\) has \(4d\) vertices, which correspond to the vertices of all \(P_i\) for \(1 \leq i \leq d\).

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:

\[(4.11) \quad P = \{(x, y, w) \in \mathbb{R}^4 : A_1(x, y, w) \leq \bar{b}_1\},\]

\[R'_1 = \{(x, y, w) \in \mathbb{R}^4 : A_2(x, y, w) \leq \bar{b}_2\},\]

\[R'_2 = \{(x, y, w) \in \mathbb{R}^4 : A_3(x, y, w) \leq \bar{b}_3\}.\]

The above three systems all have lengths polynomial in the input \(\alpha, N\) and \(\epsilon\). Next, we need the following lemma:

**Lemma 4.4.** Fix \(n\) and \(r\). Given \(r\) polytopes \(R_1, \ldots, R_r \subset \mathbb{R}^n\) described by \(r\) systems

\[R_i = \{x \in \mathbb{R}^n : A_i x \leq \bar{b}_i\},\]

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

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

Furthermore, the system \(A(x, t) \leq \bar{b}\) 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 \(2^\ell \geq r\). Pick \(\bar{t}_1, \ldots, \bar{t}_r \in \{0, 1\}^\ell\) as \(r\) different vertices of the \(\ell\)-dimensional unit cube. Define

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

and

\[U = \text{conv}(U_1, \ldots, U_r).\]

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

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

So we have (4.12).

For each \(R_j\), its vertices can be computed in polynomial time from the system \(A_1 x \leq \bar{b}_i\). 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 \(\ell\) are fixed. Therefore, we can find in polynomial time all the facets of \(U\) using those vertices. This gives us a system \(A(x, t) \leq \bar{b}\) of polynomial length that describes \(U\). \(\square\)
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:

\[
(x, y, w) \in (R'_1 \cup R'_2 \cup P) \cap \mathbb{Z}^4 \iff \exists t \in \mathbb{Z}^\ell : (x, y, w, t) \in U \cap \mathbb{Z}^{4+\ell}.
\]

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

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

which is equivalent to

\[
\exists x \in I \ \forall y \in J \ \exists z \in \mathbb{Z}^3 : A(x, y, z) \leq \overline{b}.
\]

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

It remains to show that (4.1) is in \( \mathsf{NP} \). We argue that more general sentence (1.2) is also in \( \mathsf{NP} \). From a result in [Grä87], if (1.2) is true, there must be an \( x \) satisfying it with length polynomial in the input \( P, A \) and \( \overline{b} \). For such an \( x \), we can apply Theorem 1.1 to check the rest of the sentence, which has the form \( \forall y \exists z \), in polynomial time. This shows that deciding (1.2) is in \( \mathsf{NP} \), and thus \( \mathsf{NP} \)-complete. \( \square \)

## 5. Proof of Theorem 1.4

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

**Theorem 5.1.** Fix \( k \geq 1 \). Given a polytope \( U \subset \mathbb{R}^{k+7} \) and finite boxes \( I_1, \ldots, I_k \subset \mathbb{Z}, J \subset \mathbb{Z}^2, K \subset \mathbb{Z}^5 \), then the problem of deciding:

\[
(5.1) \quad Q_1 x_1 \in I_1 \ldots Q_k x_k \in I_k \ \forall y \in J \ \exists z \in K : (x, y, z) \in U
\]

is \( \Sigma_k \) complete if \( Q_1 = \exists \), and \( \Pi_k \) complete if \( Q_1 = \forall \). Here \( Q_1, \ldots, Q_k \in \{\exists, \forall\} \) are \( k \) alternating quantifiers with \( Q_k = \exists \). The polytope \( U \) is described by a system \( A(x, y, z) \leq \overline{b} \), where \( A \in \mathbb{Z}^{n \times (k+7)} \) and \( \overline{b} \in \mathbb{Z}^n \).

For the proof, we work with the canonical problem \( \mathsf{Q3SAT} \). Let \( \Psi \) a Boolean expression of the form:

\[
(5.2) \quad \Psi(u_1, \ldots, u_k) = \bigwedge_{i=1}^N (a_i \lor b_i \lor c_i).
\]

Here each \( u_j = (u_{j1}, \ldots, u_{j\ell}) \in \{0, 1\}^\ell \) is a tuple of \( \ell \) Boolean variables, and each \( a_i, b_i, c_i \) is a literal in the set \( \{u_{js}, \overline{u_{js}} : 1 \leq j \leq k, 1 \leq s \leq \ell\} \). From \( \Psi \), we construct a sentence:

\[
(5.3) \quad Q_1 u_1 \in \{0, 1\}^\ell \ \ Q_2 u_2 \in \{0, 1\}^\ell \ldots Q_k u_k \in \{0, 1\}^\ell : \ \Psi(u_1, \ldots, u_k).
\]

Here \( Q_1, Q_2, \ldots, Q_k \in \{\forall, \exists\} \) are \( k \) alternating quantifiers with \( Q_k = \exists \). The numbers \( \ell \) and \( N \) are part of the input.
For clarity, we use the notation \(Q3\text{SAT}_k\) to emphasize problem (5.3) for a fixed \(k\). It is well-known that \(Q3\text{SAT}_k\) is \(\Sigma^P_k\)-complete if \(Q_1 = \exists\) and \(\Pi^P_k\)-complete if \(Q_1 = \forall\) (see e.g. [Pap94, MM11] and [AB09]). We proceed to reduce (5.3) to (5.1). In fact, by representing each Boolean string \(u_j = (u_{j1}, \ldots, u_{j\ell}) \in \{0, 1\}^\ell\) as an integer \(x_j \in [0, 2^\ell]\), we will only need to use \(I_1 = I_2 = \cdots = I_k = [0, 2^\ell] \cap \mathbb{Z}\).

For every string \(u_j = (u_{j1}, \ldots, u_{j\ell}) \in \{0, 1\}^\ell\), 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 \([x_j/2^{s-1}]\) is odd or even. Observe that \(t = [x_j/2^{s-1}]\) 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:

\[
\begin{align*}
  u_{js} &\iff \exists w \in \mathbb{Z} : \left\{ \begin{array}{l}
    2w + 1 > x_j/2^{s-1} - 1 \\
    2w + 1 \leq x_j/2^{s-1}
  \end{array} \right\}, \\
  \neg u_{js} &\iff \exists w \in \mathbb{Z} : \left\{ \begin{array}{l}
    2w > x_j/2^{s-1} - 1 \\
    2w \leq x_j/2^{s-1}
  \end{array} \right\}.
\end{align*}
\]

(5.4)

Let \(x = (x_1, \ldots, x_k) \in [0, 2^\ell]^k\). Recall that each term \(a_i, b_i, c_i \in \{0, 1\}\) is \(u_{js}\) or \(\neg u_{js}\) for some \(j\) and \(s\). So each clause \(a_i \lor b_i \lor c_i\) can be expressed in \(x\) as:

\[
\begin{align*}
  a_i \lor b_i \lor c_i &\iff \exists w \in \mathbb{Z} : \left\{ \begin{array}{l}
    D_i(x, w) \leq \bar{d}_i \lor E_i(x, w) \leq \bar{e}_i \lor F_i(x, w) \leq \bar{f}_i,
  \end{array} \right\},
\end{align*}
\]

(5.5)

where three systems \(D_i(x, w) \leq \bar{d}_i, E_i(x, w) \leq \bar{e}_i, F_i(x, w) \leq \bar{f}_i\) 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 6.2). We define the polytopes:

\[
\begin{align*}
  K_i &= \left\{ (x, w) \in \mathbb{R}^{k+1} : x_1, \ldots, x_k, w \in [0, 2^\ell), D_i(x, w) \leq \bar{d}_i \right\}, \\
  L_i &= \left\{ (x, w) \in \mathbb{R}^{k+1} : x_1, \ldots, x_k, w \in [0, 2^\ell), E_i(x, w) \leq \bar{e}_i \right\}, \\
  M_i &= \left\{ (x, w) \in \mathbb{R}^{k+1} : x_1, \ldots, x_k, w \in [0, 2^\ell), F_i(x, w) \leq \bar{f}_i \right\}.
\end{align*}
\]

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

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

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

\[
\begin{align*}
  Q_1 x_1 \in I_1 &\land \ldots \land Q_k x_k \in I_k : \bigwedge_{i=1}^N \left[ \exists w \in \mathbb{Z} : (x, w) \in K_i \cup L_i \cup M_i \right].
\end{align*}
\]

(5.6)

For each \(i\), we apply Lemma 4.4 (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:

\[
(x, w) \in K_i \cup L_i \cup M_i \iff \exists v \in \mathbb{Z}^2 : (x, w, v) \in G_i.
\]

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

\[
\begin{align*}
  Q_1 x_1 \in I_1 &\land \ldots \land Q_k x_k \in I_k : \bigwedge_{i=1}^N \left[ \exists w \in \mathbb{Z}^3 : (x, w) \in G_i \right],
\end{align*}
\]

(5.7)

where \(w = (v, w) \in \mathbb{Z}^3\), 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 \((x, w)\) 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 (3.6) and (3.7). The variable \(y \in \mathbb{Z}^2\) is again needed to define \(G_i\), \(\Phi\) 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 4.4 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 $x \in \mathbb{Z}^k, y \in \mathbb{Z}^2$ and $z = (w, t) \in \mathbb{Z}^5$.

We have converted (5.3) to an equivalent sentence (5.1) with polynomial size. This shows that (5.1) is $\Sigma^P_k/\Pi^P_k$-hard depending when $Q_1 = \exists/\forall$. For each tuple $x = (x_1, \ldots, x_k)$, we can check in polynomial time whether $\forall y \in J \exists z \in K : A(x, y, z) \leq b$ by applying Theorem 1.1. This shows the membership of (5.1) in $\Sigma^P_k/\Pi^P_k$. We conclude that (5.1) is $\Sigma^P_k/\Pi^P_k$-complete when $Q_1 = \exists/\forall$. \hfill $\Box$

6. Proof of Theorem 1.7

6.1. Now we prove Theorem 1.7. We use the same construction as in the proof of Theorem 1.2. Recall the definition of $\{\{x\alpha\}\}$ from Section 4. We reduce the following counting problem to a problem of the form (1.4):

$\#\text{GOOD SIMULTANEOUS APPROXIMATIONS} (\#\text{GSA})$

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

Output: The number of integers $x \in [1, N]$ that satisfy $\{\{x\alpha\}\} \leq \epsilon$.

The argument in [Lag85] is based on a parsimonious reduction. Namely, it gives a bijection between solutions for $\#\text{GSA}$ and the following problem:

$\#\text{WEAK PARTITIONS}$

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

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

It is well known and easy to see that $\#\text{WEAK PARTITIONS}$ is $\#\text{P}$-complete. The decision version $\text{WEAK PARTITION}$ was earlier shown by [vEB81] to be $\text{NP}$-complete with a parsimonious reduction from $\text{KNAPSACK}$. Together with Lagarias’s reduction, we conclude:

Theorem 6.1. $\#\text{GSA}$ is $\#\text{P}$-complete.

6.2. Now we proceed with the reduction of $\#\text{GSA}$ to (1.4).

Just like the decision version, $\#\text{GSA}$ is only non-trivial for $\epsilon < 1/2$. Define:

\[(6.1) \quad Q_i = \{(x, w) \in \mathbb{R}^2 : 1 \leq x \leq N, \quad \alpha_i x + \epsilon < w < \alpha_i x - \epsilon + 1\} .\]

Let $I = [1, N] \cap \mathbb{Z}$. We have:

Observation 1. An $x \in I$ satisfies $\{\{x\alpha\}\} \leq \epsilon$ if and only if for every $1 \leq i \leq d$, there is no $w \in \mathbb{Z}$ such that $(x, w) \in Q_i$.

Indeed, consider $x \in I$. By (4.3), we have $\{\{x\alpha\}\} \leq \epsilon$ if and only if for each $i$, there exists $w_i \in \mathbb{Z}$ with $w_i \in [\alpha_i x - \epsilon, \alpha_i x + \epsilon]$. This interval of length $2\epsilon$ is contained in $[\alpha_i x - \epsilon, \alpha_i x + \epsilon + 1]$. The latter is a half-open unit interval, which always contains a unique integer $w_i$. So $w_i \in [\alpha_i x - \epsilon, \alpha_i x + \epsilon]$ if and only if $w_i \notin (\alpha_i x + \epsilon, \alpha_i x - \epsilon + 1)$. In other words, for each $1 \leq i \leq d$, there should be no $w \in \mathbb{Z}$ with $(x, w) \in Q_i$. The converse is also straightforward.
Remark 6.2. Note that each $Q_i$ has two open edges. They can actually be sharpened without affecting the integer points in $Q_i$. Indeed, we can multiply each inequality with the denominators in $\alpha_i$ and $\epsilon$, which have polynomial length. Each resulting inequality is of the form $a < b$, with $a$ and $b$ having integer values. This is equivalent to $a \leq b - 1$. Therefore, we can replace $Q_i$ with a (smaller) closed parallelogram containing the same integer points.

By the above observation, $\#GSA$ asks for:

\begin{equation}
N - \# \left\{ x \in I : \exists 1 \leq i \leq d \quad \exists w \in \mathbb{Z} \quad (x, w) \in Q_i \right\}.
\end{equation}

We convert the union of $Q_i$ into a complement $V \setminus U$ of two polytopes $U, V \subset \mathbb{R}^3$.

6.3. Let $T = 1 + N \max_i \alpha_i$. Pick $d$ integers $0 < m_1 < m_2 < \cdots < m_d$ so that

\begin{equation}
\frac{m_{i-1} + m_{i+1}}{2} + 2T < m_i \quad \text{for} \quad 2 \leq i \leq d - 1.
\end{equation}

We embed each parallelogram $Q_i$ into $\mathbb{R}^3$ as

\begin{equation}
R_i = \left\{ (x, y, w) \in \mathbb{R}^3 : (x, w - m_i) \in Q_i, \ y = i \right\}.
\end{equation}

In other words, we translate $Q_i$ by $m_i$ in the direction $w$, and embed it into the plane $y = i$ inside $\mathbb{R}^3$ (see Figure 3). The following is obvious:

Observation 2. For each $x \in I$ and $1 \leq i \leq d$, there exists $w \in \mathbb{Z}$ with $(x, w) \in Q_i$ if and only if there exists $(y, w) \in \mathbb{Z}^2$ with $(x, y, w) \in R_i$.

Denote by $A_i, B_i, C_i$ and $D_i$ the vertices of $R_i$. Let $K_i = (N, i, 0)$ and $L_i = (1, i, 0)$ for each $1 \leq i \leq d$. Define:

\begin{equation}
U = \text{conv}\{ A_i, B_i, K_i, L_i : 1 \leq i \leq d \} \subset \mathbb{R}^3,
\end{equation}

\begin{equation}
V = \text{conv}\{ C_i, D_i, K_i, L_i : 1 \leq i \leq d \} \subset \mathbb{R}^3.
\end{equation}

Since $\text{conv}(A_i, B_i, K_i, L_i) \subset \text{conv}(C_i, D_i, K_i, L_i)$ for each $1 \leq i \leq d$, we have $U \subset V$. It is also clear that:

\begin{equation}
R_i = \text{conv}(C_i, D_i, K_i, L_i) \setminus \text{conv}(A_i, B_i, K_i, L_i).
\end{equation}

Denote by $\{y = i\}$ the plane $y = i$.

Observation 3. We have $U \cap \{y = i\} = \text{conv}(A_i, B_i, K_i, L_i)$. Similarly, $V \cap \{y = i\} = \text{conv}(C_i, D_i, K_i, L_i)$.
Indeed, from (6.5), it is clear that \( \text{conv}(A_i, B_i, K_i, L_i) \) lies in both \( U \) and the plane \( y = i \). On the other hand, if \((x, i, w) \in U\), it must be a convex combination of \( A_j, B_j, K_j, L_j \) for \( 1 \leq j \leq d \). First, assume that

\[
(6.7) \quad (x, i, w) \in \text{conv}\{A_j, B_j, K_j, L_j : j \neq i\}.
\]

From (6.1) and (6.4), the \( w \)-coordinates of \( A_j, B_j, C_j, D_j \) are within the range \([m_j, m_j + T]\). For \( K_j \) and \( L_j \), their \( w \)-coordinates are 0. Therefore, by the convexity condition (6.3), any point \((x, y, w)\) as in (6.7) must have \( w < m_i - T < m_i \). This implies that \((x, i, w) \in \text{conv}\{A_i, B_i, K_i, L_i\}\), because the \( w \)-coordinates of \( A_i \) and \( B_j \) are at least \( m_i \). So we have

\[
\text{conv}\{A_j, B_j, K_j, L_j : j \neq i\} \cap \{y = i\} \subset \text{conv}\{A_i, B_i, K_i, L_i\}.
\]

Adding \( A_i, B_i, C_i \) and \( D_i \) to the LHS, we have

\[
\text{conv}\{A_j, B_j, K_j, L_j : 1 \leq j \leq d\} \cap \{y = i\} = \text{conv}\{A_i, B_i, K_i, L_i\}.
\]

This proves the observation for \( U \). The same argument works for \( V \).

By Observation 3, for \((x, y, w) \in \mathbb{Z}^3\), we have \((x, y, z) \in V \setminus U\) if and only if

\[
(x, y, w) \in \text{conv}(C_i, D_i, K_i, L_i) \setminus \text{conv}(A_i, B_i, K_i, L_i)
\]

for some \( 1 \leq i \leq d \). Combined with (6.6) and Observation 2, for every \( x \in I \), we have:

\[
\exists (y, w) \in \mathbb{Z}^2 \quad (x, y, w) \in V \setminus Q \quad \iff \quad \exists 1 \leq i \leq d \quad \exists w \in \mathbb{Z} \quad (x, w) \in Q_i.
\]

From (6.2), we conclude that \(#\text{GSA}\) is exactly:

\[
N - \#\left\{x \in I : \exists (y, z) \in \mathbb{Z}^2 \quad (x, y, w) \in V \setminus U\right\} = N - \#\text{E}_1(V \setminus U).
\]

Let \( P = U, Q = V \) we have Theorem 1.7.

6.4. Proof of Corollary 1.9. By Theorem 1.7, counting \(#\text{E}_1(Q \setminus P)\) is \#P-complete for \( P \subset Q \subset \mathbb{R}^3 \). Nevertheless, the complement \( Q \setminus P \) 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 [Woo15], the systems describing all such \( T_i \) can be found in polynomial time. Therefore, counting \(#\text{E}_1(T_1 \sqcup \cdots \sqcup T_r)\) is \#P-complete.

7. Another Hard Decision Problem

Our construction with Fibonacci points also yields the following completeness result with only 2 quantifiers:

**Theorem 7.1.** Given three polytopes \( U_1, U_2, U_3 \subseteq \mathbb{R}^4 \) and two boxes \( I \subseteq \mathbb{Z}, K \subseteq \mathbb{Z}^3 \), deciding the sentence:

\[
(7.1) \quad \exists x \in I \quad \forall z \in K : \quad (x, z) \in U_1 \cup U_2 \cup U_3
\]

is NP-complete.

Here the condition \((x, z) \in U_1 \cup U_2 \cup U_3\) is expressed as a disjunction of three systems in four variables \( x, z_1, z_2, z_3 \). Instead of many as in (1.3), we only need only 2 disjunctions to express \((x, z) \in U_1 \cup U_2 \cup U_3\). Also notice that the quantifiers are \( \exists \forall \) as opposed to \( \forall \exists \) in Theorem 1.1.

**Remark 7.2.** One way to think of our main result (Theorem 1.2) compared to the Schöning theorem, see (1.3), as a tradeoff: a long Boolean formula is replaced with a long system at the cost of extra variables and one more alternating quantifier. In this context, Theorem 7.1 can be viewed as an intermediate result.
Proof of Theorem 7.1. We again find a reduction of GSA. Let \( T = 1 + N \max_i \alpha_i \). Recall \( P_i \) from (3.5). For every \( 1 \leq i \leq d \), define two new polygons:
\[
L_i = \{(x, w) \in \mathbb{R}^2 : 1 \leq x \leq N, -1 \leq w \leq \alpha_i x + \epsilon - 1\},
\]
\[
M_i = \{(x, w) \in \mathbb{R}^2 : 1 \leq x \leq N, \alpha_i x - \epsilon \leq w \leq T\}.
\]

Observation 4. For every \( x \in [1, N] \) and \( 1 \leq i \leq d \), we have:
\[
\exists w \in \mathbb{Z} : (x, w) \in P_i \iff \forall w \in [-1, T] \cap \mathbb{Z} : (x, w) \in L_i \cup M_i.
\]

Indeed, by (3.5), we have \( \exists w \in \mathbb{Z} : (x, w) \in P_i \) if and only if \( [\alpha_i x - \epsilon, \alpha_i x + \epsilon] \) contains an integer point \( w \). Also notice that \( [\alpha_i x - \epsilon, \alpha_i x + \epsilon] \subset (\alpha_i x + \epsilon - 1, \alpha_i x + \epsilon) \) and
\[
[-1, T] = [-1, \alpha_i x + \epsilon - 1] \cup (\alpha_i x + \epsilon - 1, \alpha_i x + \epsilon) \cup (\alpha_i x + \epsilon, T).
\]

Since \( (\alpha_i x + \epsilon - 1, \alpha_i x + \epsilon) \) is a half-open unit interval, it contains a unique integer point \( w \). So \( w \) lies in \( [\alpha_i x - \epsilon, \alpha_i x + \epsilon] \) if and only if
\[
[-1, T] \cap \mathbb{Z} = \left([-1, \alpha_i x + \epsilon - 1] \cup [\alpha_i x - \epsilon, \alpha_i x + \epsilon] \cup (\alpha_i x + \epsilon, T)\right) \cap \mathbb{Z}
\]
\[
= \left([-1, \alpha_i x + \epsilon - 1] \cup [\alpha_i x - \epsilon, \alpha_i x + \epsilon]\right) \cap \mathbb{Z}.
\]

This last condition is exactly the RHS in (7.2).

Recall the Fibonacci points \( \Phi = \{\phi_1, \ldots, \phi_d\} \). We construct \( L', M' \) similarly to (3.6) and \( L, M \) similarly to (3.7) using the same Fibonacci points. As a direct analogy to (4.6), GSA is equivalent to:
\[
\exists x \in I \ \forall y \in \Phi \ \forall w \in [-1, T] \cap \mathbb{Z} : (x, y, w) \in L \cup M.
\]

Recall \( J \) from (3.2). Let \( K = J \times \left([-1, T] \cap \mathbb{Z}\right) \), which is a box in \( \mathbb{Z}^3 \). Let \( z = (y, w) \in K \). Also recall \( R_1 \) and \( R_2 \) from (3.3) and (3.4). Define
\[
U_1 = [1, N] \times R_1 \times [-1, T], \quad U_2 = \text{conv}([1, N] \times R_2 \times [-1, T], \ L), \quad U_3 = M.
\]

From properties (F3)–(F5), it is not hard to see that (7.3) is equivalent to:
\[
\exists x \in I \ \forall z \in K : (x, z) \in U_1 \cup U_2 \cup U_3.
\]

This completes the proof. \( \square \)

8. Final remarks and open problems

8.1. It is sufficient to prove Theorem 1.1 for the case when \( m, n \) are also bounded. In the system \( A(x, y) \leq b \), we view \( x \) as the parameters and \( y \) as the variables to be solved for. For a fixed \( d_0 \) and \( m \geq 2^{d_2} \), the Doignon–Bell–Scarf theorem [Sch86, §16.5] implies that the system \( A(x, y) \leq b \) is solvable in \( y \in \mathbb{Z}^{d_2} \) if and only if every subsystem \( A'(x, y) \leq \overline{b} \) is solvable. Here \( A' \) is a submatrix with \( 2^{d_2} \) rows from \( A \) with \( \overline{b} \) the corresponding subvector from \( b \). In other words:
\[
\exists y \in \mathbb{Z}^{d_2} \ A(x, y) \leq \overline{b} \iff \bigwedge_{(A', \overline{b})} \left[ \exists y \in \mathbb{Z}^{d_2} \ A'(x, y) \leq \overline{b} \right].
\]

The total number of pairs \( (A', \overline{b}) \) is \( \binom{m}{2^{d_2}} \), which is polynomial in \( m \).
Note that the conjunction over all \((A', \overline{\gamma})\) commutes with the universal quantifier \(\forall x\). Therefore:
\[
\forall x \in P \cap \mathbb{Z}^{d_1} \exists y \in \mathbb{Z}^{d_2} \ A(x, y) \leq \overline{\gamma} \iff \bigwedge \left( (A', \overline{\gamma}) \right) \left[ \forall x \in P \cap \mathbb{Z}^{d_1} \exists y \in \mathbb{Z}^{d_2} \ A'(x, y) \leq \overline{\gamma} \right].
\]

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 \(C x \leq \overline{\gamma}\) describing \(P\), we can triangulate \(P\) into 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. [DRS10]). Now for each pair \((A', \overline{\gamma})\), we have:
\[
\forall x \in P \cap \mathbb{Z}^{d_1} \exists y \in \mathbb{Z}^{d_2} \ A'(x, y) \leq \overline{\gamma} \iff \bigwedge \left( i=1 \right) \left[ \forall x \in P_i \cap \mathbb{Z}^{d_1} \exists y \in \mathbb{Z}^{d_2} \ A'(x, y) \leq \overline{\gamma} \right].
\]

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 \(\exists x \forall y \exists z\), this argument breaks down because the existential quantifier \(\exists x\) no longer commutes with a long conjunction.

### 8.2. By taking finite Boolean combinations, we see that Theorem 1.5 also allows counting integer points in a union of \(k\) polytopes, where \(k\) is bounded (see [Bar08, BP99]). In fact, Woods proved in [Woo15, Prop. 5.3.1] that it is still possible to count all such points in polynomial time when \(k\) is arbitrary. By Corollary 1.9, we see that this is not the case for projection.

### 8.3. The GSA Problem plays an important role in both Number Theory and Integer Programming especially in connection to lattice reduction algorithms (see e.g. [GLS89]). Let us mention that via a chain of parsimonious reductions one can show that \#GSA is also hard to approximate (cf. [ER09]). Note also that GSA has been recently used in a somewhat related geometric context in [EH12].

### 8.4. An easy consequence of Lemma 4.4 proves the first part of the following result:

**Proposition 8.1.** 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 \(d \leq \lceil \log_2 r \rceil\). Moreover, the bound \(d \leq \lceil \log_2 r \rceil\) is tight.

We only use the proposition to reduce the dimension of variable \(z\) in Theorem 4.1 from 4 to 3, but it is perhaps of independent interest. Note that a weaker inequality \(d \leq r\) is trivial.

**Proof of the second part of Proposition 8.1.** 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 \(\ell \leq \lceil \log_2 r \rceil\) 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 \(\overline{q}_i = \overline{q}_j \in \mathbb{Z}^{2\ell}\) for some \(i \neq j\). 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. \(\square\)
8.5. Let us give another motivation behind Theorem 1.7 and put it into context of our other work. In this paper, we bypass the “short generating function” technology developed for computing $|E_1(P)|$ for convex polytopes $P \subset \mathbb{R}^d$. Note, however, that for $X = Q \setminus P$ as in the theorem, the corresponding short GF $f_X(t)$ is simply the difference $f_Q(t) - f_P(t)$, which can still be computed in polynomial time (see [Bar93]). Thus, if one could efficiently present the projection of $f_X(t)$ on $\mathbb{Z}$ as a short generating function of polynomial size, then one would be able to compute $|E_1(Q \setminus P)|$, a contradiction. In other words, Theorem 1.7 is an extension of a result by Woods [Woo04], which shows that computing projecting short generating functions is $\text{NP}$-hard. It is also an effective but weaker version of the main result in [NP17b, Th. 1.3], which deals with the size of short GFs of the projections rather than complexity of their computation.

8.6. Corollary 1.9 says that computing $|E_1(T_1 \cup \cdots \cup T_k)|$ is $\#P$-complete even for simplices $T_i \subset \mathbb{R}^3$. By a stronger version of Theorem 1.6 (see [BW03]), for each polytope $T_i$, there is a short generating function $g_i(t)$ representing $E_1(T_i)$. The union of all those generating functions correspond to $E_1(T_1 \cup \cdots \cup T_k)$. As a corollary we conclude that the union operation on short generating functions is $\#P$-hard to compute. As in §8.5 above, one should compare this to a stronger result [NP17b, Th. 1.1], which says that the union of short generating functions can actually have super-polynomial lengths unless $\#P \subseteq \text{FP/poly}$.

8.7. Dimension 3 in Theorem 1.7 is optimal. Indeed, assume $P, Q \subset \mathbb{R}^2$. Then one can decompose $Q \setminus P = R_1 \cup \cdots \cup R_r$, where each $R_i$ is a polygon, so that the projection $E_1(R_i)$ onto the $x$-axis of each $R_i$ intersects at most one other $E_1(R_j)$. This can easily be done by drawing vertical lines through vertices of $P$, which together with $\partial P$ will divide $Q \setminus P$ into $R_1, \ldots, R_r$. By Theorem [BW03], we can find a generating function $g_i(t)$ for each $E_1(R_i)$ in polynomial time. From Corollary 3.7 in [BW03], the union $g(t)$ of all $g_i(t)$ can also be found in polynomial time, because each of them intersects at most one another in support. Evaluating $g(1)$, we get the count for $|E_1(Q \setminus P)|$.

8.8. Note that Theorem 4.1 was proved for dimensions $d_1 = 1$, $d_2 = 2$ and $d_3 = 3$. One can ask if the problem still remains $\text{NP}$-complete when some of these dimensions are lowered. In particular, it would be interesting to see if the following problem is still $\text{NP}$-complete:

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

where $P \subset \mathbb{R}$, $Q \subset \mathbb{R}^2$ and $U \subset \mathbb{R}^3$ 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. The second author was partially supported by the NSF.
References


