THE COMPUTATIONAL COMPLEXITY OF INTEGER PROGRAMMING WITH ALTERNATIONS[†]

DANNY NGUYEN[⋆] AND IGOR PAK[⋆]

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 $P, Q \subset \mathbb{R}^3$, counting the projections of integer points in $Q \setminus P$ is #P-complete. This contrasts the 2003 result by Barvinok and Woods, which allows counting in polynomial time the projections 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:*

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

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

Here we slightly abuse the notation by writing $A(\mathbf{x}, \mathbf{y})$ to denote the multiplication of A with the (column) vector $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^{d_1+d_2}$. 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 $d_1 \ge 1, d_2 \ge 2$ and $d_3 \ge 3$. 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*

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

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

[†]Earlier proceeding version: Danny Nguyen and Igor Pak, The Computational Complexity of Integer Programming with Alternations, in *Proceedings of the 32nd Computational Complexity Conference (CCC 2017)*, Leibniz International Proceedings in Informatics (LIPIcs), 6:1–6:18.

[⋆]Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: {ldnguyen,pak}@math.ucla.edu.

September 12, 2018.

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 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 [Sch86, §16.5], the sentence (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 done in polynomial time, unless $\mathsf{P} = \mathsf{NP}$. In fact, Theorem 1.2 holds even when P is an interval and Q is an axis-parallel rectangle (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

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

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 arbitrarily 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.

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

1.2. **Presburger sentences.** In [Grä87, Grä88], Grädel considered the theory of *Presburger Arithmetic*, and proved many completeness results in this theory when the numbers 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 $\Psi(\mathbf{x}, \mathbf{y})$ 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 $\mathbf{y} = (y_1, y_2, y_3) \in \mathbb{Z}^3$. 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 $\mathbf{\Sigma}_k^{\mathsf{P}}$-complete if $Q_1 = \exists$, and $\mathbf{\Pi}_k^{\mathsf{P}}$-complete if $Q_1 = \forall$. Here $Q_1, \ldots, Q_{k+1} \in \{\forall, \exists\}$ are $m + 1$ alternating quantifiers.

Here $\mathbf{\Sigma}_k^{\mathsf{P}}$ and $\mathbf{\Pi}_k^{\mathsf{P}}$ denote the k-level in the standard *Polynomial Hierarchy*, which basically characterized the complexity of the satisfiability problem in Boolean logic with k alternating quantifiers (see [MM11, Pap94, AB09]). 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 arbitrarily many inequalities. This flexibility allows effective reductions of classical decision problems such as QSAT. For some time, it has remained unknown 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 $\mathbf{\Sigma}_k^{\mathsf{P}}/\mathbf{\Pi}_k^{\mathsf{P}}$-complete, depending on whether $Q_1 = \exists/\forall$. Here the problem is allowed to contain only a system of inequalities.*

We refer to Theorem 5.1 for the precise statement, and to Remark 5.2 for the reason why the innermost quantifier of integer programming should always be $\exists$. Thus, we see that integer programming requires only one extra quantifier alternation to achieve the complexity of Presburger Arithmetic as given by Theorem 1.3. Again, we emphasize that while the number of variables and quantifiers are fixed in Theorem 1.4, the linear system is still allowed to have arbitrarily many inequalities.

1.3. **Counting points in projections of non-convex polyhedra.** Counting integer points in polytopes of arbitrary dimensions is classically #P-complete, even for those with 0/1 vertices. 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 $A\mathbf{x} \le \overline{b}$, with $A \in \mathbb{Z}^{m\times d}$, $\overline{b} \in \mathbb{Z}^m$.*

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 $|\mathrm{E}(Q\setminus P)| = |\mathrm{E}(Q)| - |\mathrm{E}(P)|$. 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 projections of integer points in 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 $A\mathbf{x} \le \overline{b}$ and T is described by a matrix M, where $A \in \mathbb{Z}^{m\times d_1}$, $\overline{b} \in \mathbb{Z}^m$ 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 1.6, $|\mathrm{E}_1(P)|$ can be computed in polynomial time for every polytope $P \subset \mathbb{R}^d$.

Recall the class #P, which consists of counting problems where counted objects are polynomial time verifiable. Solving a #P-complete problem naturally imply solving any NP problems. We prove the following result:

Theorem 1.7. *Given two polytopes $P \subset Q \subset \mathbb{R}^3$, computing $|\mathrm{E}_1(Q\setminus P)|$ is #P-complete.*

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

$$\mathrm{E}_1(Q\setminus P) \,=\, \{x \in \mathbb{Z} \,:\, \exists \mathbf{z} \in \mathbb{Z}^2 \quad (x, \mathbf{z}) \in Q\setminus P\}. \tag{1.4}$$

Note that the corresponding decision problem $|\mathrm{E}_1(Q\setminus P)| \ge 1$ is equivalent to $|\mathrm{E}(Q\setminus P)| \ge 1$, 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 of Theorem 1.6 depends on the polytopal structure of P and exploits 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).

Remark 1.8. To illustrate the theorem, consider three examples of polygons $P, Q \subset \mathbb{R}^2$ as in Figure 1. Note that the vertical projections of P and Q (as real sets) are the same in all three cases, but the projections of $(Q\setminus P) \cap \mathbb{Z}^2$ are quite different.

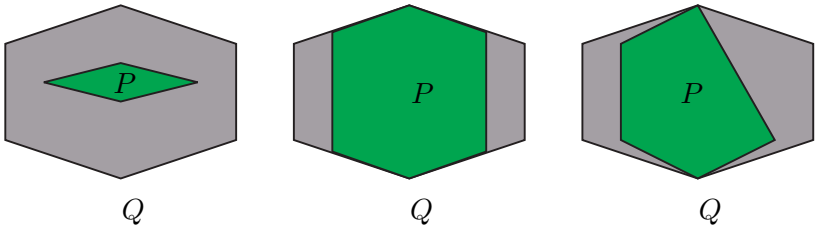

FIGURE 1. Three examples of convex polygons $P, Q \subset \mathbb{R}^2$.

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 $|\mathrm{E}_1(T_1 \cup \cdots \cup T_r)|$ 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 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 $\overline{a}, \overline{b}, \overline{x}, \overline{y}, \overline{t}$ 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 $\mathbf{x} \le \mathbf{y}$ if $x_j \le y_j$ 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:

$$\overline{\phi}_1 = (F_1, F_0),\ \overline{\phi}_2 = (F_3, F_2),\ \ldots,\ \overline{\phi}_d = (F_{2d-1}, F_{2d-2}). \tag{3.1}$$

Let

$$\Phi = \big\{\overline{\phi}_1, \ldots, \overline{\phi}_d\big\} \subset \mathbb{Z}^2 \quad \text{and} \quad J = [1, F_{2d-1}] \times [0, F_{2d-2}] \cap \mathbb{Z}^2. \tag{3.2}$$

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

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

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

and

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

The following properties are straightforward from the above definitions:

(F1) The points $\overline{\phi}_1, \ldots, \overline{\phi}_d$ are in convex position. The curve $\mathcal{C}$ connecting them is convex (upwards). See Figure 2.

(F2) Each segment $(\overline{\phi}_i \, \overline{\phi}_{i+1})$ and each triangle $\Delta_i = (0 \, \overline{\phi}_i \, \overline{\phi}_{i+1})$ have 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 $J \setminus \Phi$ can be partitioned into 2 parts: those lying strictly above the convex curve $\mathcal{C}$, and those lying strictly below it.

(F4) The integer points in $J \setminus \Phi$ that lie above $\mathcal{C}$ are exactly $R_1 \cap \mathbb{Z}^2$. This can be seen as follows. The line ℓ connecting 0 and $\overline{\phi}_d$ 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 integer points in $J \setminus \Phi$ that lie below $\mathcal{C}$ are exactly $R_2 \cap \mathbb{Z}^2$. This can be seen as follows. The line connecting $\overline{\phi}_i$ and $\overline{\phi}_{i+1}$ is defined by

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

So all integer points below that line satisfy:

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

This gives $d - 1$ edges for R_2, one for each $1 \leq i \leq d - 1$. The other two edges 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 a polygon:

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

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

$$P'_i = \big\{ (x, \overline{\phi}_i, w) \ : \ (x, w) \in P_i \big\} \subset \mathbb{R}^4. \tag{3.6}$$

Finally, we define the convex hull:

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

The following properties are straightforward from the above definitions:

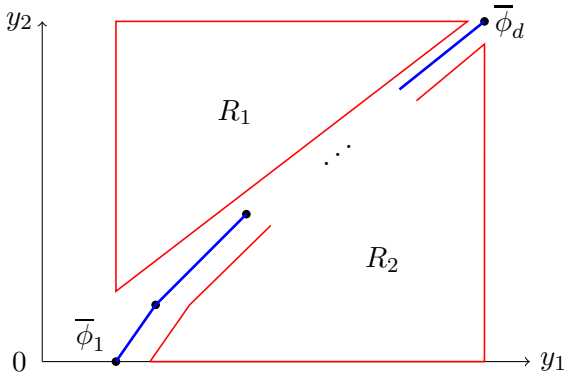

FIGURE 2. The points $\overline{\phi}_1, \ldots, \overline{\phi}_d \in \Phi$ form a convex curve $\mathcal{C}$ (blue).

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

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

(P3) All the vertices of $P'_1, \ldots, P'_d$ 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 $(x, \mathbf{y}, w)$ of P, we have $\mathbf{y} = \overline{\phi}_i \in \Phi$ for some $1 \le i \le d$. Conversely, for every $\overline{\phi}_i \in \Phi$, we have:

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

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*

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

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 result implies Theorem 1.2 for every $d_1 \ge 1, d_2 \ge 3$ and $d_3 \ge 3$. 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 $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and an integer $x \in \mathbb{Z}$, we define

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

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 $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Q}^d$ and $N \in \mathbb{N}$, $\epsilon \in \mathbb{Q}$.
Decide: Is there an integer $x \in [1, N]$ such that $\{\{x\boldsymbol{\alpha}\}\} \le \epsilon$?

Note that GSA is only non-trivial for $\epsilon < 1/2$. Also we can assume all $\alpha_i \ge 0$ in GSA, simply because $\{\{\cdot\}\}$ is an even function. 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:

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

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 4.3. *Let* $\Phi = \{\overline{\phi}_1, \ldots, \overline{\phi}_d\}$ *be as in* (3.2) *and* P *be as in* (3.7)*. 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 $i = 1, \ldots, d$, there exists $w_i \in \mathbb{Z}$ with $(x, w_i) \in P_i$. Now (P5) implies that $(x, \overline{\phi}_i, w_i) \in P$. Since this holds for every $\overline{\phi}_i \in \Phi$, the RHS in (4.5) is satisfied. For the other direction, assume the RHS in (4.5) holds. Then for every $\overline{\phi}_i \in \Phi$, there exists $w_i \in \mathbb{Z}$ with $(x, \overline{\phi}_i, w_i) \in P$. By (P5), we have $(x, w_i) \in P_i$. By (4.4), x satisfies GSA, i.e., $\{\{x\boldsymbol{\alpha}\}\} \le \epsilon$. □

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 to combine 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 $1 \le i \le d$. 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:

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

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

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

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

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

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

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

and

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

In other words, we form U_j by augmenting each R_j with ℓ coordinates of $\overline{t}_j$. Since $\overline{t}_1, \ldots, \overline{t}_r$ 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 $\mathbf{t} \in \operatorname{conv}(\overline{t}_1, \ldots, \overline{t}_r)$, we have $\mathbf{t} \in \mathbb{Z}^\ell$ if and only if $\mathbf{t} = \overline{t}_j$ for some j. This implies that the only integer points in U are those in U_j's. In other words:

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

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

So we have (4.12).

For each R_j, its vertices can be computed in polynomial time from the system $A_i \mathbf{x} \leq \overline{b}_i$. 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 $A(\mathbf{x}, \mathbf{t}) \leq \overline{b}$ 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 $A(x, \mathbf{y}, w, \mathbf{t}) \leq \overline{b}$ that describes U, which has size polynomial in the systems in (4.11). Now, we can rewrite (4.10) as:

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

which is equivalent to

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

Here $\mathbf{z} = (w, \mathbf{t}) \in \mathbb{Z}^3$. The final system $A(x, \mathbf{y}, \mathbf{z}) \leq \overline{b}$ 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.

Finally, from [Grä88, Th. 3.8], we know that deciding (4.1) is in NP. This concludes the proof of Theorem 4.1. □

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:*

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

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

Remark 5.2. At this point, it is worth noting that in all of (1.1), (1.2) and (5.1), the innermost quantifier is always $\exists$, which is naturally compatible with a system of inequalities. If the quantifiers are switched and the inner part is still a system, the problem would not make much sense. Indeed, consider a sentence of the form $\forall \mathbf{x} \exists \mathbf{y} \forall \mathbf{z} A(\mathbf{x}, \mathbf{y}, \mathbf{z}) \leq \overline{b}$. Then if some coefficients of $\mathbf{z}$ in A are non-zero, surely some $\mathbf{z} \in \mathbb{Z}^{d_3}$ must violate the system. So the statement degenerates to the form $\forall \mathbf{x} \exists \mathbf{y} A(\mathbf{x}, \mathbf{y}) \leq \overline{b}$. So when the quantifiers are switched, we should also naturally replace the system by a disjunction of inequalities.

Proof. We reduce the canonical Q3SAT problem to (5.1). Let Ψ be a Boolean expression of the form:

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

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

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

Here $Q_1, Q_2, \ldots, Q_k \in \{\forall, \exists\}$ 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 $\mathrm{Q3SAT}_k$ to emphasize problem (5.3) for a fixed k. It is well-known that $\mathrm{Q3SAT}_k$ 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. [Pap94, MM11, AB09]). 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 $I_1 = I_2 = \cdots = I_k = [0, 2^\ell) \cap \mathbb{Z}$.

For every string $\mathbf{u}_j = (u_{j1}, \ldots, u_{j\ell}) \in \{0,1\}^\ell$, 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 $\lfloor x_j / 2^{s-1} \rfloor$ is odd or even. Now, each term u_{js} or $\neg u_{js}$ can be expressed in x_j as follows:

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

Let $\mathbf{x} = (x_1, \ldots, x_k) \in [0, 2^\ell)^k$. 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:

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

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). We define the polytopes:

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

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:

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

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:

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

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

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

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 (3.6) and (3.7). 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 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 $\mathbf{x} \in \mathbb{Z}^k, \mathbf{y} \in \mathbb{Z}^2$ 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 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 1.1. 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 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 definitions of $\{\{x\boldsymbol{\alpha}\}\}$ and GSA from Section 4. We reduce the following counting problem to (1.4):

#GOOD SIMULTANEOUS APPROXIMATIONS (#GSA)
Input: A rational vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{Q}^d$ and $N \in \mathbb{N}$, $\epsilon \in \mathbb{Q}$.
Output: The number of integers $x \in [1, N]$ that satisfy $\{\{x\boldsymbol{\alpha}\}\} \le \epsilon$.

The argument in [Lag85] 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 $\overline{a} = (a_1, \dots, a_d) \in \mathbb{Z}^d$.
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 [vEB81] to be NP-complete with a parsimonious reduction from KNAPSACK. Together with Lagarias's reduction, we conclude:

Theorem 6.1. #GSA *is* #P*-complete.*

6.2. Now we proceed with the reduction of #GSA to (1.4). WLOG, we can assume $\alpha_i \geq 0$, simply because the function $\{\{\cdot\}\}$ is even. And just like the decision version, #GSA is only non-trivial for $\epsilon < 1/2$. Define:

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

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

Observation 1. An $x \in I$ satisfies $\{\{x\boldsymbol{\alpha}\}\} \leq \epsilon$ 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 $\{\{x\boldsymbol{\alpha}\}\} \leq \epsilon$ 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 2ϵ 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. Consider the open right edge $w < \alpha_i x - \epsilon + 1$ of Q_i. We can rewrite it as $c_i w < d_i x + e_i$ with some $c_i, d_i, e_i \in \mathbb{Z}$. Now this can be sharpened to $c_i w \leq d_i x + e_i - 1/2$ without losing any integer points in Q_i. Thus, from now on, we consider Q_i a parallelogram with one open left edge and 3 other closed edges.

By the above observation, #GSA asks for:

$$N \ - \ \#\Big\{x \in I \ : \ \exists 1 \leq i \leq d \quad \exists w \in \mathbb{Z} \quad (x,w) \in Q_i\Big\}. \tag{6.2}$$

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

$$\frac{m_{i-1} + m_{i+1}}{2} + 2T < m_i \quad \text{for} \quad 2 \leq i \leq d-1.^2 \tag{6.3}$$

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

$$R_i = \big\{(x,y,w) \in \mathbb{R}^3 \ : \ (x, w - m_i) \in Q_i, \ y = i\big\}. \tag{6.4}$$

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). Each R_i also has an open left edge (see Remark 6.2). The following is obvious:

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

Denote by A_i, B_i, C_i and D_i the vertices of R_i (see Figure 3). Let $K_i = (N,i,0)$ and $L_i = (1,i,0)$ for each $1 \leq i \leq d$. Define:

$$\begin{aligned} U &= \operatorname{conv}\big\{A_i, B_i, K_i, L_i \ : \ 1 \leq i \leq d\big\} \subset \mathbb{R}^3, \\ V &= \operatorname{conv}\big\{C_i, D_i, K_i, L_i \ : \ 1 \leq i \leq d\big\} \subset \mathbb{R}^3. \end{aligned} \tag{6.5}$$

Since $\operatorname{conv}(A_i, B_i, K_i, L_i) \subset \operatorname{conv}(C_i, D_i, K_i, L_i)$ for each $1 \leq i \leq d$, we have $U \subset V$. Since each R_i has an open left edge, we have:

$$R_i \ = \ \operatorname{conv}(C_i, D_i, K_i, L_i) \setminus \operatorname{conv}(A_i, B_i, K_i, L_i). \tag{6.6}$$

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

[2]Note that we can rescale any strictly concave sequence $0 < \mu_1 < \mu_2 < \cdots < \mu_d$ to satisfy this.

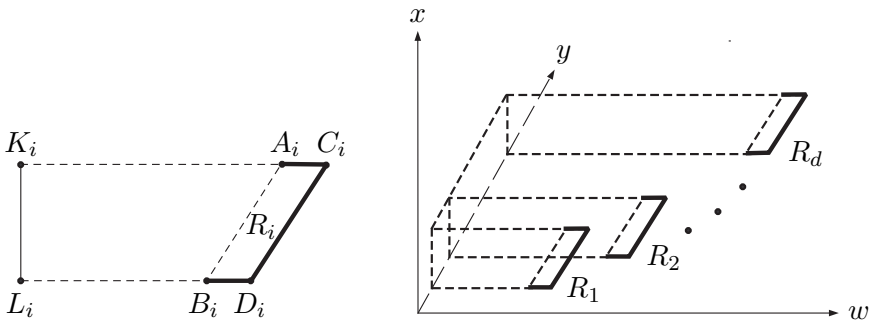

FIGURE 3. The parallelograms R_i.

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 $1 \le j \le d$. First, assume that

$$(x, i, w) \in \text{conv}\big\{A_j, B_j, K_j, L_j : j \neq i\big\}. \tag{6.7}$$

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 $(x, i, w) \in \text{conv}\big\{A_i, B_i, K_i, L_i\big\}$, because the w-coordinates of A_i and B_j are at least m_i. So we have

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

Combining with A_i, B_i, C_i and D_i, we have:

$$\text{conv}\big\{A_j, B_j, K_j, L_j : 1 \le j \le d\big\} \cap \{y = i\} = \text{conv}\big\{A_i, B_i, K_i, L_i\big\}.$$

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 $(x, y, z) \in V \backslash U$ if and only if

$$(x, y, w) \in \text{conv}(C_i, D_i, K_i, L_i) \backslash \text{conv}(A_i, B_i, K_i, L_i)$$

for some $1 \le i \le d$. Combined with (6.6), for every $x \in I$, we have:

$$\exists (y, w) \in \mathbb{Z}^2 \quad (x, y, w) \in V \backslash Q \quad \Longleftrightarrow \quad \exists 1 \le i \le d \quad \exists w \in \mathbb{Z} \quad (x, w) \in Q_i.$$

From (6.2), we conclude that #GSA is exactly:

$$N \;-\; \#\Big\{x \in I \;:\; \exists (y, z) \in \mathbb{Z}^2 \quad (x, y, w) \in V \backslash U\Big\} = N - |\mathrm{E}_1(V \backslash U)|.$$

Letting $P = U$ and $Q = V$, we have Theorem 1.7.

6.4. Proof of Corollary 1.9. By Theorem 1.7, counting $|\mathrm{E}_1(Q \backslash P)|$ is #P-complete for $P \subset Q \subset \mathbb{R}^3$. 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 [Woo15], 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. 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 $U_1, U_2, U_3 \subset \mathbb{R}^4$ and two boxes $I \subset \mathbb{Z}, K \subset \mathbb{Z}^3$, deciding the sentence:*

$$\exists x \in I \quad \forall \mathbf{z} \in K \quad : \quad (x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3 \tag{7.1}$$

is NP*-complete.*

Here the condition $(x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3$ 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 $(x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3$. 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 $1 \le i \le d$, define two new polygons:

$$L_i = \{(x, w) \in \mathbb{R}^2 \ : \ 1 \le x \le N, \ -1 \le w \le \alpha_i x + \epsilon - 1\},$$
$$M_i = \{(x, w) \in \mathbb{R}^2 \ : \ 1 \le x \le N, \ \alpha_i x - \epsilon \le w \le T\}.$$

Observation 4. For every $x \in [1, N]$ and $1 \le i \le d$, we have:

$$\exists w \in \mathbb{Z} \ : \ (x, w) \in P_i \quad \iff \quad \forall w \in [-1, T] \cap \mathbb{Z} \ : \ (x, w) \in L_i \cup M_i. \tag{7.2}$$

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

$$[-1, T] \ = \ [-1, \alpha_i x + \epsilon - 1] \ \sqcup \ (\alpha_i x + \epsilon - 1, \alpha_i x + \epsilon] \ \sqcup \ (\alpha_i x + \epsilon, T].$$

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

$$\begin{aligned} [-1, T] \cap \mathbb{Z} \ &= \ \big([-1, \alpha_i x + \epsilon - 1] \ \sqcup \ [\alpha_i x - \epsilon, \alpha_i x + \epsilon] \ \sqcup \ (\alpha_i x + \epsilon, T]\big) \cap \mathbb{Z} \\ &= \ \big([-1, \alpha_i x + \epsilon - 1] \ \sqcup \ [\alpha_i x - \epsilon, T]\big) \cap \mathbb{Z}. \end{aligned}$$

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

Recall the Fibonacci points $\Phi = \{\overline{\phi}_1, \ldots, \overline{\phi}_d\}$. We construct L_i', M_i' 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:

$$\exists x \in I \quad \forall \mathbf{y} \in \Phi \quad \forall w \in [-1, T] \cap \mathbb{Z} \quad : \quad (x, \mathbf{y}, w) \in L \cup M. \tag{7.3}$$

Recall J from (3.2). Let $K = J \times \big([-1, T] \cap \mathbb{Z}\big)$, which is a box in $\mathbb{Z}^3$. Let $\mathbf{z} = (\mathbf{y}, w) \in K$. Also recall R_1 and R_2 from (3.3) and (3.4). Define

$$U_1 = [1, N] \times R_1 \times [-1, T], \quad U_2 = \operatorname{conv}\big([1, N] \times R_2 \times [-1, T], \ L\big), \quad U_3 = M.$$

From properties (F3)–(F5), it is not hard to see that (7.3) is equivalent to:

$$\exists x \in I \quad \forall \mathbf{z} \in K \quad : \quad (x, \mathbf{z}) \in U_1 \cup U_2 \cup U_3.$$

This completes the proof. □

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 $A(\mathbf{x}, \mathbf{y}) \le b$, we view $\mathbf{x}$ as the parameters and $\mathbf{y}$ as the variables to be solved for. For a fixed d_2 and $m \ge 2^{d_2}$, the *Doignon–Bell–Scarf theorem* [Sch86, §16.5] implies that the system $A(\mathbf{x}, \mathbf{y}) \le \overline{b}$ is solvable in $\mathbf{y} \in \mathbb{Z}^{d_2}$ if and only if every subsystem $A'(\mathbf{x}, \mathbf{y}) \le \overline{b'}$ 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:

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

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

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

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 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 $(A', \overline{b'})$, we have:

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

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 $n = d_1 + 1$. Note that the total number of 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.

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 projections 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 4.1 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 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 $\ell < \lceil \log_2 r \rceil$ 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 $i \neq j$. 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 position and thus contain no midpoints, a contradiction. □

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 $|\mathrm{E}_1(P)|$ for convex polytopes $P \subset \mathbb{R}^d$. Note, however, that for $X = Q \setminus P$ as in the theorem, the corresponding short GF $f_X(\mathbf{t})$ is simply the difference $f_Q(\mathbf{t}) - f_P(\mathbf{t})$, which can still be computed in polynomial time (see [Bar93]). 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 $|\mathrm{E}_1(Q \setminus P)|$, a contradiction. In other words, Theorem 1.7 is an extension of a result by Woods [Woo04], which shows that projecting short generating functions is 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 $|\mathrm{E}_1(T_1 \cup \cdots \cup T_k)|$ 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 $\mathrm{E}_1(T_i)$. 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 §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 $\#\mathsf{P} \subseteq \mathsf{FP/poly}$.

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 $\mathrm{E}_1(R_i)$ onto the x-axis of each R_i intersects at most one other $\mathrm{E}_1(R_j)$. This can easily be done by drawing vertical lines through vertices of P, which together with ∂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 $\mathrm{E}_1(R_i)$ 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 other in the support. Evaluating $g(1)$, we get the count for $|\mathrm{E}_1(Q \setminus P)|$.

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 NP-complete when some of these dimensions are lowered. Specifically, 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. The second author was partially supported by the NSF.

References

[AB09] S. Arora and B. Barak, *Computational complexity: a modern approach*, Cambridge Univ. Press, Cambridge, 2009.

[Bar93] A. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the fimension is fixed, in *Proc. 34th FOCS*, IEEE, Los Alamitos, CA, 1993, 566–572.

[Bar08] A. Barvinok, *Integer points in polyhedra*, EMS, Zürich, 2008.

[BP99] A. Barvinok and J. E. Pommersheim, An algorithmic theory of lattice points in polyhedra, in *New Perspectives in Algebraic Combinatorics*, Cambridge Univ. Press, Cambridge, 1999, 91–147.

[BW03] A. Barvinok and K. Woods, Short rational generating functions for lattice point problems, *Jour. AMS* **16** (2003), 957–979.

[DRS10] J. A. De Loera, J. Rambau and F. Santos, *Triangulations*, Springer, Berlin, 2010.

[Eis10] F. Eisenbrand, Integer programming and algorithmic geometry of numbers, in *50 years of Integer Programming*, Springer, Berlin, 2010, 505–560.

[EH12] F. Eisenbrand and N. Hähnle, Minimizing the number of lattice points in a translated polygon, in *Proc. 24th SODA*, SIAM, Philadelphia, PA, 2012, 1123–1130.

[ER09] F. Eisenbrand and T. Rothvoß, New hardness results for Diophantine approximation, in *Lecture Notes Comput. Sci.* **5687**, Springer, Berlin, 2009, 98–110.

[Grä87] E. Grädel, *The complexity of subclasses of logical theories*, Dissertation, Universität Basel, 1987.

[Grä88] E. Grädel, Subclasses of Presburger arithmetic and the polynomial-time hierarchy, *Theoret. Comput. Sci.* **56** (1988), no. 3, 289–301.

[GLS89] M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer, Berlin, 1988.

[Kan90] R. Kannan, Test sets for integer programs, $\forall\exists$ sentences, in *Polyhedral Combinatorics*, AMS, Providence, RI, 1990, 39–47

[Kan92] R. Kannan, Lattice translates of a polytope and the Frobenius problem, *Combinatorica* **12** (1992), 161–177.

[Lag85] J. Lagarias, The computational complexity of simultaneous Diophantine approximation problems, *SIAM J. Comput.* **14** (1985), 196–209.

[Len83] H. Lenstra, Integer programming with a fixed number of variables, *Math. Oper. Res.* **8** (1983), 538–548.

[MM11] C. Moore and S. Mertens, *The nature of computation*, Oxford Univ. Press, Oxford, 2011.

[NP17a] D. Nguyen and I. Pak, Complexity of short Presburger arithmetic, in *Proc. STOC 2017*, to appear.

[NP17b] D. Nguyen and I. Pak, Complexity of short generating functions, preprint; `arXiv:1702.08660`.

[Pap94] C. H. Papadimitriou, *Computational complexity*, Addison-Wesley, Reading, MA, 1994.

[Sch86] A. Schrijver, *Theory of linear and integer programming*, John Wiley, Chichester, 1986.

[Sch97] U. Schöning, Complexity of Presburger arithmetic with fixed quantifier dimension, *Theory Comput. Syst.* **30** (1997), 423–428.

[vEB81] P. van Emde Boas, Another NP-complete partition problem and the complexity of computing short vectors in a lattice, *Math. Dept. Report* **81–04**, Univ. Amsterdam, April 1981, 10 pp.

[Woo04] K. Woods, *Rational Generating Functions and Lattice Point Sets*, Ph.D. thesis, University of Michigan, 2004, 112 pp.

[Woo15] K. Woods, Presburger arithmetic, rational generating functions, and quasi-polynomials, *J. Symb. Logic* **80** (2015), 433–449.