SHORT PRESBURGER ARITHMETIC IS HARD[†]

DANNY NGUYEN[⋆] AND IGOR PAK[⋆]

ABSTRACT. We study the computational complexity of short sentences in Presburger arithmetic (SHORT-PA). Here by "short" we mean sentences with a bounded number of variables, quantifiers, inequalities and Boolean operations; the input consists only of the integer coefficients involved in the linear inequalities. We prove that satisfiability of SHORT-PA sentences with $m+2$ alternating quantifiers is Σ_m^{P}-complete or Π_m^{P}-complete, when the first quantifier is $\exists$ or $\forall$, respectively. Counting versions and restricted systems are also analyzed. Further application are given to hardness of two natural problems in Integer Optimization.

1. INTRODUCTION

1.1. **Outline of the results.** We consider *short Presburger sentences*, defined as follows:

$$(\text{Short-PA}_m) \qquad \exists \mathbf{x}_1 \ \forall \mathbf{x}_2 \ \ldots \ \forall/\exists \mathbf{x}_m \ : \ \Phi\big(\mathbf{x}_1, \ldots, \mathbf{x}_m\big),$$

where the quantifiers alternate, the variables $\mathbf{x}_i \in \mathbb{Z}^{n_i}$ have fixed dimensions $\overline{n} = (n_1, \ldots, n_m)$, and $\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_m)$ is a fixed Boolean combination of integer linear systems of fixed lengths (numbers of inequalities):

$$(*) \qquad A_1 \mathbf{x}_1 \ + \ \ldots \ + \ A_k \mathbf{x}_m \ \le \ \overline{b}.$$

In other words, everything is fixed in (Short-PA$_m$), except for the entries of the matrices A_i and of the vectors $\overline{b}$ in $(*)$. We also call Φ a *short Presburger expression*.

The feasibility of short Presburger sentences is a well known open problem which we resolve in this paper. Connected to both Integer Programming and Computational Logic, it was called a "fundamental question" by Barvinok in a recent survey [Bar17]. Many precursors to (Short-PA$_m$) are well known, including *Integer Linear Programming*:

$$(\text{IP}) \qquad \exists \mathbf{x} \ : \ A\mathbf{x} \le \overline{b},$$

and *Parametric Integer Programming*:

$$(\text{PIP}) \qquad \forall \mathbf{y} \in Q \ \ \exists \mathbf{x} \ : \ A\mathbf{x} + B\mathbf{y} \ \le \ \overline{b},$$

where Q is a convex polyhedron given by $K\mathbf{y} \le \overline{u}$. In both cases, the problems were shown to be in P, by Lenstra in 1982 and Kannan in 1990, respectively (Theorem 1.8). Traditionally, the lengths of the systems in both (IP) and (PIP) are not restricted. However, it is known that they both can be reduced to the case of a bounded length system (c.f. Sec. 8.1 [NP17c]).

[†]Extended abstract will appear in *Proceedings of the 58th Annual Symposium on Foundations of Computer Science (FOCS 2017)*.

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

October 19, 2017.

Our main result is a complete solution of the problem. We show that for a fixed $m \geq 3$, deciding (Short-PA$_m$) is $\Sigma^{\mathsf{P}}_{m-2}$-complete (Theorem 1.5). This disproves[1] a conjecture by Woods [Woo04, §5.3] (see also [Woo15]), which claims that decision is in P.

Let us emphasize that until this work even the following special case remained open:

$$\text{(GIP)} \qquad \exists \mathbf{z} \in R \ \forall \mathbf{y} \in Q \ \exists \mathbf{x} : A\mathbf{x} + B\mathbf{y} + C\mathbf{z} \leq \overline{b},$$

where Q and R are convex polyhedra given by $K\mathbf{y} \leq \overline{u}$ and $L\mathbf{z} \leq \overline{v}$, respectively. We also show that (GIP) is NP-complete (Theorem 1.2). This resolves an open problem by Kannan [Kan92].

Our reduction is parsimonious and also proves that the corresponding counting problem is #P-complete:

$$\text{(\#GIP)} \qquad \#\big\{\mathbf{z} \in R \ : \ \forall \mathbf{y} \in Q \ \exists \mathbf{x} \ \ A\mathbf{x} + B\mathbf{y} + C\mathbf{z} \leq \overline{b}\big\}.$$

There is a natural geometric way to view these problems. Problem (IP) asks whether a given rational polyhedron $P \subset \mathbb{R}^d$ contains an integer point. Problem (PIP) asks whether the projection of P contains all integer points in some polyhedron Q. Finally, problem (GIP) asks whether there is an R-slice of a polyhedron P for which the projection contains all integer points in some polyhedron Q.

1.2. **Precise statements.** For $m = 3$ alternating quantifiers, we have the first hard instance of (Short-PA$_m$) :

$$\text{(Short-PA}_3\text{)} \qquad \exists \mathbf{z} \ \forall \mathbf{y} \ \exists \mathbf{x} : \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z}).$$

Here Φ is a short Presburger expression in $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$. We can also define the counting problem

$$\text{(\#Short-PA}_3\text{)} \qquad \#\big\{\mathbf{z} \ : \ \forall \mathbf{y} \ \exists \mathbf{x} \ \ \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z})\big\}.$$

Theorem 1.1. *Deciding* (Short-PA$_3$) *is* NP*-complete, even for a short Presburger expression* Φ *of at most* 10 *inequalities in* 5 *variables* $z \in \mathbb{Z}$, $\mathbf{y} \in \mathbb{Z}^2$, $\mathbf{x} \in \mathbb{Z}^2$. *Similarly, computing* (#Short-PA$_3$) *in this case is* #P*-complete.*

For systems of inequalities, we also get:

Theorem 1.2. *Deciding* (GIP) *is* NP*-complete, even for a system* $A\mathbf{x} + B\mathbf{y} + Cz \leq \overline{b}$ *of at most* 24 *inequalities in* 9 *variables* $z \in \mathbb{Z}$, $\mathbf{y} \in \mathbb{Z}^2$, $\mathbf{x} \in \mathbb{Z}^6$, *when* R *is an interval and* Q *is a triangle. Similarly, computing* (#GIP) *in this case is* #P*-complete.*

The third dimension $\mathbf{x} \in \mathbb{Z}^6$ in the theorem can be lowered to $\mathbf{x} \in \mathbb{Z}^3$ at the cost of increasing the length of the linear system:

Theorem 1.3. *Deciding* (GIP) *is* NP*-complete, even for a system* $A\mathbf{x} + B\mathbf{y} + Cz \leq \overline{b}$ *of at most* 8400 *inequalities in* 6 *variables* $z \in \mathbb{Z}$, $\mathbf{y} \in \mathbb{Z}^2$, $\mathbf{x} \in \mathbb{Z}^3$, *when* R *is an interval and* Q *is a triangle. Similarly, computing* (#GIP) *in this case is* #P*-complete.*

This substantially strengthens our earlier result [NP17c], which considers (GIP) with a "long system", i.e., a system arbitrarily many inequalities:

Theorem 1.4 ([NP17c])**.** *Deciding* (GIP) *is* NP*-complete, for a system* $A\mathbf{x} + B\mathbf{y} + Cz \leq \overline{b}$ *of unbounded length in* 6 *variables* $z \in \mathbb{Z}$, $\mathbf{y} \in \mathbb{Z}^2$, $\mathbf{x} \in \mathbb{Z}^3$.

[1] Assuming the polynomial hierarchy does not collapse.

At the time of proving Theorem 1.4, we thought it would be the strongest negative result (see Section 1.5 below). Nevertheless, the new results in theorems 1.1, 1.2 and 1.3 say that at the level of three quantifiers, both Integer Programming and Presburger Arithmetic quickly saturate to a high level of complexity, even when all parameters are bounded.

The decision part of Theorem 1.1 can naturally be generalized to short Presburger sentences of more than 3 quantifiers:

Theorem 1.5 (Main result)**.** *Fix $m \geq 1$. Let $Q_1, \ldots, Q_{m+2} \in \{\forall, \exists\}$ be $m+2$ alternating quantifiers with $Q_1 = \exists$. Deciding short Presburger sentences of the form*

$$Q_1 \mathbf{z}_1 \ \ \ldots \ \ Q_{m+1}\mathbf{z}_{m+1} \ \ Q_{m+2}\mathbf{z}_{m+2} \ \ : \ \ \Phi(\mathbf{z}_1, \ldots, \mathbf{z}_{m+2})$$

is Σ_m^{P}-complete. Similarly, when $Q_1 = \forall$, deciding short Presburger sentences as above is Π_m^{P}-complete. Here Φ is a short Presburger expression of at most $10m$ inequalities in $4m+1$ variables $\mathbf{z}_1 \in \mathbb{Z}$, $\mathbf{z}_2, \mathbf{z}_{m+2} \in \mathbb{Z}^2$, and $\mathbf{z}_3, \ldots, \mathbf{z}_{m+1} \in \mathbb{Z}^4$.

The proof of the above results uses a chain of reductions. We start with the AP-COVER problem on covering intervals with arithmetic progressions. This problem is NP-compete by a result of Stockmeyer and Meyer [SM73] (see Section 9). The arithmetic progressions are encoded via continued fractions by a single rational number p/q. We use the plane geometry of continued fractions and "lift" the construction to a Boolean combination of polyhedra in dimension 5, proving Theorem 1.1. We then "lift" the construction further to convex polytopes $Q_1 \subset \mathbb{R}^9$ and $Q_2 \subset \mathbb{R}^6$, which give proofs of theorems 1.2 and 1.3, respectively. While both constructions are explicit, the first construction gives a description of Q_1 by its 24 facets, while the second gives a description of Q_2 by its 40 vertices; the bound of 8400 facets then comes from McMullen's Upper bound theorem (Theorem 5.1). Finally, we generalize the problem AP-COVER and the chain of reductions to $m \geq 3$ quantifiers.

1.3. **Applications in integer optimization.** The first application of our construction is the following hardness result on the *bilevel optimization* of a quadratic function over integer points in a polytope.

Theorem 1.6. *Given a rational interval $J \subset \mathbb{R}$, a rational polytope $W \subset \mathbb{R}^5$ and a quadratic rational polynomial $h : \mathbb{R}^6 \to \mathbb{R}$, computing:*

$$\max_{z \in J \cap \mathbb{Z}} \ \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \ h(z, \mathbf{w}) \tag{1.1}$$

is NP-hard. This holds even when W has at most 18 facets.

The polytope W can be given either by its vertices or by its facets, as the theorem holds in both cases.

The second application is to the hardness of the *Pareto optima*. Assume we are given polytope $Q \subset \mathbb{R}^n$, and k functions $f_1, \ldots, f_k : \mathbb{R}^n \to \mathbb{R}$ restricted to the domain $Q \cap \mathbb{Z}^n$. For a point $\mathbf{x} \in Q \cap \mathbb{Z}^n$, the corresponding outcome vector $\mathbf{y} = (f_1(\mathbf{x}), \ldots, f_k(\mathbf{x}))$ is called a *Pareto minimum*, if there is no other point $\widetilde{\mathbf{x}} \in Q \cap \mathbb{Z}^n$ and $\widetilde{\mathbf{y}} = (f_1(\widetilde{\mathbf{x}}), \ldots, f_k(\widetilde{\mathbf{x}}))$, such that $\widetilde{\mathbf{y}} \leq \mathbf{y}$ coordinate-wise and $\widetilde{\mathbf{y}} \neq \mathbf{y}$. The goal is to minimize the value of an *objective function* $g : \mathbb{R}^k \to \mathbb{R}$ over all Pareto minima $\mathbf{y}$ of $(f_1, \ldots, f_k)$ on Q.

Theorem 1.7. *Given a rational polytope $Q \subset \mathbb{R}^6$, two rational linear functions $f_1, f_2 : \mathbb{R}^6 \to \mathbb{R}$, a rational quadratic polynomial $f_3 : \mathbb{R}^6 \to \mathbb{R}$, and rational linear objective function $g : \mathbb{R}^3 \to \mathbb{R}$, computing the minimum of g over the Pareto minima of (f_1, f_2, f_3) on Q is NP-hard. Moreover, the corresponding $1/2$-approximation problem is also NP-hard. This holds even when Q has at most 38 facets.*

Again, the polytope Q can be given either by its vertices or by its facets. Here by ε-approximation we mean approximation up to a multiplicative factor of ε.

We prove both theorems in Section 8. See also §11.6 and §11.7 for some background and open problems.

1.4. **Historical overview.** *Presburger Arithmetic* was introduced by Presburger in [Pre29], where he proved it is a decidable theory. The general theory allows unbounded numbers of quantifiers, variables and Boolean operations. A quantifier elimination (deterministic) algorithm was given by Cooper [Coo72], and was shown to be triply exponential by Oppen [Opp78] (see also [RL78]). A nondeterministic doubly exponential complexity lower bound was obtained by Fischer and Rabin [FR74] for the general theory. This pioneering result was further refined to a triply exponential deterministic lower bound (with unary output) in [Wei97], and a simply exponential nondeterministic lower bound for a bounded number of quantifier alternations [Für82] (see also [Sca84]). Of course, in all these cases the number of variables is unbounded.

In [Sch97], Schöning proved NP-completeness for two quantifiers $\exists y \forall x : \Phi(x, y)$, where $x, y \in \mathbb{Z}$ and $\Phi(x, y)$ is a Presburger expression in 2 variables, i.e., a Boolean combination of arbitrarily many inequalities in x, y. This improved on an earlier result by Grädel, who also established that similar sentences with $m + 1$ alternating quantifiers and a bounded number of variables are complete for the m-th level in the Polynomial Hierarchy [Grä87]. Roughly speaking, one can view our results as variations on Grädel's result, where we trade boundedness of Φ for an extra quantifier.

Let us emphasize that when the number of variables is unbounded, even the most simple systems (IP) become NP-complete. The examples include the KNAPSACK, one of the oldest NP-complete problems [GJ79]. Note also that even when matrix A has at most two nonzero entries in each row, the problem remains NP-complete [Lag85].

In a positive direction, the progress has been limited. The first breakthrough was made by Lenstra [Len83] (see also [Sch86]), who showed that (IP) can be solved in polynomial time in a fixed dimension (see also [Eis03] for better bounds). Combined with a reduction by Scarpellini [Sca84], this implies that deciding (Short-PA_1) is in P.

The next breakthrough was made by Kannan [Kan90] (see also [Kan92]), who showed that (PIP) in fixed dimensions is in P, even if the number s of inequalities is unbounded, i.e. the matrices A and B can be "long". This was a motivation for our earlier Theorem 1.4 from [NP17c], which ruled out "long" systems for (GIP).

Theorem 1.8 (Kannan)**.** *Fix n_1, n_2. The formula* (PIP) *in variables $\mathbf{x} \in \mathbb{Z}^{n_1}$, $\mathbf{y} \in \mathbb{Z}^{n_2}$ with s inequalities can be decided in polynomial time, where s is part of the input.*

Kannan's Theorem was further strengthened by Eisenbrand and Shmonin [ES08] (see §10.2). All of these greatly contrast with the above hardness results by Schöning and Grädel, because here only conjunctions of inequalities are allowed.

The corresponding counting problems have also been studied with great success. First, Barvinok [Bar93] showed that integer points in a convex polytope $P \subset \mathbb{R}^d$ can be counted in polynomial time, for a fixed dimension n (see also [Bar06, BP99]). He utilized the *short generating function* approach pioneered by Brion, Vergne and others (see [Bar08] for details and references). Woods [Woo04] extended this approach to general Boolean formulas.

In the next breakthrough, Barvinok and Woods showed how to count projections of integer points in a (single) polytope in polynomial time [BW03]. Woods [Woo04] extended this approach to general Presburger expressions Φ with a fixed number of inequalities (see

also [Woo15] and an alternative proof in [NP17a]). As a consequence, he showed that deciding (Short-PA_2) is in P. This represents the most general positive result in this direction:

Theorem 1.9 (Woods)**.** *Fix n_1, n_2 and s. Given a short Presburger expression $\Phi(\mathbf{x}, \mathbf{y})$ in variables $\mathbf{x} \in \mathbb{Z}^{n_1}, \mathbf{y} \in \mathbb{Z}^{n_2}$ with at most s inequalities, the sentence*

$$\forall \mathbf{y} \ \exists \mathbf{x} \ : \ \Phi(\mathbf{x}, \mathbf{y})$$

can be decided in polynomial time. Moreover, the number of solutions

$$\#\big\{\mathbf{y} \ : \ \exists \mathbf{x} \ \ \Phi(\mathbf{x}, \mathbf{y})\big\}$$

can be computed in polynomial time.

1.5. **Kannan's Partition Theorem.** In [Kan90], Kannan introduced the technology of *test sets* for efficient solutions of (PIP). The *Kannan Partition Theorem* (KPT), see Theorem 10.1 below, claims that one can find in polynomial time a partition of the k-dimensional parameter space W into polynomially many rational (co-)polyhedra

$$(\circ) \qquad W \ = \ P_1 \sqcup P_2 \sqcup \ldots \sqcup P_r\,,$$

so that only a bounded number of tests need to be performed (see §10.1 for precise statement details).

In [NP17a], we showed that KPT if valid would imply a polynomial time decision algorithm for (Short-PA_m), and in particular (GIP) for a restricted system. Thus, at the time of proving Theorem 1.4 in [NP17c], we thought that [NP17a] and [NP17c] together would completely characterize the complexity of (GIP), depending on whether the system is restricted or not.

In view of our theorems 1.1, 1.2, 1.3 and 1.5, it strongly suggests that KPT may actually be erroneous. However, we did not expect this at the time of writing [NP17a]. In fact, the prevailing view was that (Short-PA_m) would always be in P, which neatly aligned with the results in [NP17a] (conditional upon KPT). Now that the hardness results are known, we are actually able combine the current techniques with some of those in [NP17a] to obtain the following quantitative result, which strongly contradicts KPT:

Theorem 1.10. *Fix m, n and let $k = 1$. Let ϕ be the total bit length of the matrix $A \in \mathbb{Z}^{m\times n}$ in* KPT*. Then for the number r of pieces in Kannan's partition $(\circ)$, we must have $r > \exp(\varepsilon\phi)$ for some constant $\varepsilon = \varepsilon(n, m) > 0$.*

We conclude no polynomial size partition $(\circ)$ exists as claimed by KPT. See Section 10 for a detailed presentation of this result and its implications, §11.1 for our point of view, and §11.2 for the gap in the original proof of KPT.

2. Notations

We use $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$
Universal/existential quantifiers are denoted $\forall/\exists$.
Unspecified quantifiers are denoted by Q_1, Q_2, etc.
Unquantified Presburger expressions are denoted by Φ, Ψ, etc.
We use $[\,{}^{a}_{b}\,]$ for a disjunction $(a \vee b)$ and $\{\,{}^{a}_{b}\,\}$ for a conjunction $(a \wedge b)$.
All constant vectors are denoted $\overline{n}, \overline{b}, \overline{\alpha}, \overline{\nu}$, etc.
We use 0 to denote both zero and the zero vector.
All matrices are denoted A, B, C, etc.
All integer variables are denoted x, y, z, etc.

All vectors of integer variables are denoted $\mathbf{x}, \mathbf{y}, \mathbf{z}$, etc.
In a vector $\mathbf{y} = (y_1, y_2)$, we draw y_2 as a vertical and y_1 as a horizontal coordinate.
We use $\lfloor . \rfloor$ to denote the floor function.
The the vector $\mathbf{y}$ with coordinates $y_i = \lfloor x_i \rfloor$ is denoted by $\mathbf{y} = \lfloor \mathbf{x} \rfloor$.
Half-open intervals are denoted by $[\alpha, \beta)$, $(\alpha, \beta]$, etc.
A *polyhedron* is an intersection of finitely many closed half-spaces in $\mathbb{R}^n$.
A *copolyhedron* is a polyhedron with possibly some open facets.
A *polytope* is a bounded polyhedron.
Subsets of $\mathbb{N}$ are denoted by Γ, Δ, etc.

3. Basic properties of finite continued fractions

Every rational number $\alpha > 1$ can be written in the form:

$$\alpha \ = \ [a_0;\ a_1,\ \ldots,\ a_n] \ = \ a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

where $a_0, \ldots, a_n \in \mathbb{Z}_+$. If $a_n > 1$, we have another representation:

$$\alpha \ = \ [a_0;\ a_1,\ \ldots,\ a_n - 1,\ 1] \ = \ a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{(a_n - 1) + \cfrac{1}{1}}}}.$$

On the other hand, if $a_n = 1$, then we also have:

$$\alpha \ = \ [a_0;\ a_1,\ \ldots,\ a_{n-1},\ 1] \ = \ [a_0;\ a_1,\ \ldots,\ a_{n-1} + 1].$$

It is well known that any rational $\alpha > 1$ can be written as a continued fraction as above in exactly two ways (see e.g. [Kar13, Khi64]), one with an odd number of terms and the other one with an even number of terms.

If a continued fraction $[a_0;\ a_1,\ \ldots,\ a_n]$ evaluates to a rational value p/q, we identify it with the integer point (q, p). We write:

$$(q, p) \ \leftrightarrow \ [a_0;\ a_1,\ \ldots,\ a_n].$$

From now on, we will only consider continued fractions with an odd number of terms:

$$\alpha \ = \ [a_0;\ a_1,\ \ldots,\ a_{2k}].$$

To facilitate later computations, we will relabel these $2k + 1$ terms as:

$$\alpha \ = \ [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_{k-1},\ b_{k-1},\ a_k].$$

The convergents of α are 2-dimensional integer vectors, defined as:

$$\begin{aligned} C_0 = (1, 0)\,, \ D_0 = (0, 1), \\ C_i = a_{i-1} D_{i-1} + C_{i-1}\,, \ \text{for } i = 1, \ldots, k+1, \\ D_i = b_{i-1} C_i + D_{i-1}\,, \ \text{for } i = 1, \ldots, k. \end{aligned} \tag{3.1}$$

We call $C_0, D_0, \ldots, C_k, D_k, C_{k+1}$ the convergents for α. If $C_i = (q_i, p_i)$ and $D_i = (s_i, r_i)$ then we have the properties:

P1) $p_0 = 0,\ q_0 = 1,\ r_0 = 1,\ s_0 = 0$.
P2) $p_i = a_{i-1}r_{i-1} + p_{i-1},\ q_i = a_{i-1}s_{i-1} + q_{i-1}$.
P3) $r_i = b_{i-1}p_i + r_{i-1},\ s_i = b_{i-1}q_i + s_{i-1}$.
P4) $C_{i+1} = (q_{i+1}, p_{i+1}) \leftrightarrow [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ b_{i-1},\ a_i]$.
P5) The quotients p_i/q_i form an increasing sequence, starting with $p_0/q_0 = 0$ and ending with $p_{k+1}/q_{k+1} = \alpha$.
P6) $D_{i+1} = (s_{i+1}, r_{i+1}) \leftrightarrow [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_i,\ b_i]$.
P7) The quotients r_i/s_i form a decreasing sequence, starting with $r_0/s_0 = \infty$, and ending with $r_k/s_k = [a_0;\ b_0,\ a_1,\ b_1,\ \ldots,\ a_{k-1},\ b_{k-1}]$.

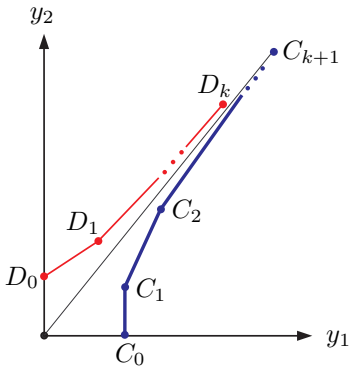

FIGURE 1. The curves $\mathcal{C}$ (bold) and $\mathcal{D}$.

Denote by O the origin in $\mathbb{Z}^2$. The geometric properties of these convergents are:

G1) Each vector $\overrightarrow{OC_i}$ and $\overrightarrow{OD_i}$ is primitive in $\mathbb{Z}^2$, meaning $\gcd(p_i, q_i) = \gcd(r_i, s_i) = 1$.
G2) Each segment C_iC_{i+1} contains exactly $a_i + 1$ integer points, since $\overrightarrow{C_iC_{i+1}} = a_i\overrightarrow{OD_i}$.
G3) Each segment D_iD_{i+1} contains exactly b_i+1 integer points, since $\overrightarrow{D_iD_{i+1}} = b_i\overrightarrow{OC_{i+1}}$.
G4) The curve $\mathcal{C}$ connecting $C_0, C_1, \ldots, C_{k+1}$ is (strictly) convex upward (see Figure 1).
G5) The curve $\mathcal{D}$ connecting $D_0, D_1, \ldots, D_k$ is (strictly) convex downward.
G6) There are no interior integer points above $\mathcal{C}$ and below $\overrightarrow{OC_{k+1}}$. In other words, $\mathcal{C}$ is the upper envelope of all non-zero integer points between $\overrightarrow{OC_0}$ and $\overrightarrow{OC_{k+1}}$.

4. From arithmetic progressions to short Presburger sentences

4.1. **Covering with arithmetic progressions.** For a triple $(g, h, e) \in \mathbb{N}^3$, denote by $\mathrm{AP}(g, h, e)$ the arithmetic progression:

$$\mathrm{AP}(g, h, e) \ = \ \{g + je \ : \ 0 \le j \le h\}.$$

We reduce the following classical NP-complete problem to (Short-PA_3):

AP-COVER
Input: An interval $J = [\mu, \nu] \subset \mathbb{Z}$ and k triples (g_i, h_i, e_i) for $i = 1, \ldots, k$.
Decide: Is there $z \in J$ such that $z \notin \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k$, where $\mathrm{AP}_i = \mathrm{AP}(g_i, h_i, e_i)$?

The problem AP-COVER was shown to be NP-complete by Stockmeyer and Meyer (Theorem 9.1). A short proof of this is included in §9.1 for completeness. We remark that the inputs μ, ν, g_i, h_i, e_i to the problem are in binary. We can assume that each $h_i \ge 1$, i.e.,

each AP_i contains more than 1 integer. This is because we can always increase $\nu \leftarrow \nu + 1$ and add the last integer $\nu + 1$ to any progression AP_i that previously had only a single element. Note that AP-COVER is also invariant under translation, so we can assume that μ, ν and all g_i, h_i, e_i are positive integers.

Next, let:

$$M \;=\; 1 + \nu \prod_{i=1}^{k} g_i(g_i + h_i e_i).$$

We have:

$$M > \nu \quad \text{and} \quad M > \max_i (g_i + h_i e_i).$$

i.e., the interval $[1, M-1]$ contains J and all AP_i. Moreover, we have:

$$\gcd(M, g_i) = \gcd(M, g_i + h_i e_i) = 1, \;\; i = 1, \ldots, k. \tag{4.1}$$

Note that M can be computed in polynomial time from the input of AP-COVER, and

$$\log M \;=\; O\left(\sum_{i=1}^{k} \log g_i + \log h_i + \log e_i \right).$$

Let us construct a continued fraction

$$\alpha \;=\; [a_0;\, b_0,\, a_1,\, b_1,\, \ldots,\, a_{2k-2},\, b_{2k-2},\, a_{2k-1}]$$

with the following properties:

1) All $a_i, b_j \in [1, M]$.
2) For each $1 \le i < k$, we have $a_{2i} = 1$.
3) For each $1 \le i \le k$, we have $a_{2i-1} = h_i$.
4) For each $1 \le i \le k$, if
$$C_{2i-1} := (q_{2i-1}, p_{2i-1}) \leftrightarrow [a_0;\, b_0,\, \ldots,\, a_{2i-2}]$$
then we have $p_{2i-1} \equiv g_i \pmod{M}$.
5) For each $1 \le i \le k$, if
$$C_{2i} := (q_{2i}, p_{2i}) \leftrightarrow [a_0;\, b_0,\, \ldots,\, a_{2i-1}]$$
then we have $p_{2i} \equiv g_i + h_i e_i \pmod{M}$.
6) For each $1 \le i \le k$, the segment $C_{2i-1}C_{2i}$ contains exactly $h_i + 1$ integer points. Moreover, the set
$$\mathcal{A}_i \;:=\; \{y_2 \bmod M \;:\; (y_1, y_2) \in C_{2i-1}C_{2i}\}$$
is exactly AP_i.
7) For each $1 \le i < k$, the segment $C_{2i}C_{2i+1}$ contains no integer points apart from the two end points.

We construct α iteratively as follows. We say an integer vector $Y = (y_1, y_2)$ is congruent to $z \bmod M$, denoted $Y \equiv z \pmod{M}$, if $y_2 \equiv z \pmod{M}$. As in (3.1), let $C_0 = (1, 0)$ and $D_0 = (0, 1)$.

Step 1: Let $a_0 = g_1$. Then

$$C_1 = a_0 D_0 + C_0 = (1, g_1) \;\text{ and }\; C_1 \equiv g_1 \pmod{M}.$$

Step 2: Take b_0 so that

$$D_1 = b_0 C_1 + D_0 = (b_0, b_0 g_1) + (0, 1) \equiv e_1 \pmod{M},$$

i.e.,

$$b_0 g_1 + 1 \equiv e_1 \pmod{M}.$$

We can solve for $b_0 \bmod M$ because $\gcd(M, g_1) = 1$ from (4.1). So there exists $b_0 \in [1, M]$ s.t. $D_1 \equiv e_1 \pmod{M}$.

Step 3: Take $a_1 = h_1$. This implies

$$C_2 = a_1 D_1 + C_1 \equiv h_1 e_1 + g_1 \pmod{M}.$$

By Property (G2), we also have exactly $h_1 + 1$ integer points on $C_1 C_2$.

Observation: After these steps, we have $h_1 + 1$ integer points on $C_1 C_2$. Every two such consecutive points differ by $\overrightarrow{OD_1}$. Reduced mod M, they give:

$$C_1 \equiv g_1,\ g_1 + e_1,\ \ldots,\ g_1 + h_1 e_1 \equiv C_2 \pmod{M}.$$

Thus, we have $\mathcal{A}_1 = \mathrm{AP}_1$. Conditions (1)–(7) hold so far.

Step 4: Take b_1 so that $D_2 \equiv g_2 - (g_1 + h_1 e_1) \pmod{M}$. Since we have the recurrence

$$D_2 = b_1 C_2 + D_1 \equiv b_1 (g_1 + h_1 e_1) + e_1 \pmod{M}$$

this is equivalent to solving

$$b_1 (g_1 + h_1 e_1) + e_1 \equiv g_2 - (g_1 + h_1 e_1) \pmod{M}.$$

Again we can solve for $b_1 \bmod M$ because $\gcd(M, g_1 + h_1 e_1) = 1$ from (4.1). So there exists $b_1 \in [1, M]$ s.t. $D_2 \equiv g_2 - (g_1 + h_1 e_1) \pmod{M}$.

Step 5: Take $a_2 = 1$. This implies

$$\begin{aligned} C_3 = a_2 D_2 + C_2 &\equiv g_2 - (g_1 + h_1 e_1) + g_1 + h_1 e_1 \\ &\equiv g_2 \pmod{M}. \end{aligned}$$

This satisfies condition (4) for $i = 2$. Now we can start encoding AP_2 with $C_3 \pmod{M}$.

Observation: One can see that b_1 in Step 4 was appropriately set up to facilitate Step 5. It is conceptually easier to start with Step 5 and retrace to get the appropriate condition for b_1. Taking $a_2 = 1$ also implies that there are no other integer points on $C_2 C_3$ apart from the two endpoints.

Step 6: Take b_2 so that $D_3 = b_2 C_3 + D_2 \equiv e_2 \pmod{M}$. This is similar to Step 2. Again we use condition (4.1).

Step 7: Take $a_3 = h_2$, which implies

$$C_4 = a_3 D_3 + C_3 \equiv g_2 + h_2 e_2 \pmod{M}.$$

After this, we again get exactly $h_2 + 1$ integer points on $C_3 C_4$. Reduced mod M, they give $\mathcal{A}_2 = \mathrm{AP}_2$. Note that conditions (1)–(7) still hold.

The rest proceeds similarly to Steps 4–7, for $2 \le j \le k - 1$:

Step 4j: Take b_{2j-1} so that

$$D_{2j} \equiv g_{j+1} - (g_j + h_j e_j) \pmod{M}.$$

Step 4j+1: Take $a_{2j} = 1$, which implies

$$C_{2j+1} = D_{2j} + C_{2j} \equiv g_{j+1} \pmod{M}.$$

Step 4j+2: Take b_{2j} so that $D_{2j+1} \equiv e_{j+1} \pmod{M}$.

Step 4j+3: Take $a_{2j+1} = h_{j+1}$, which implies

$$C_{2j+2} \equiv g_{j+1} + h_{j+1}e_{j+1} \pmod{M}.$$

The segment $C_{2j+1}C_{2j+2}$ contains exactly $h_{j+1} + 1$ integer points.

Observation: After these four steps, we get $\mathcal{A}_{j+1} = \mathrm{AP}_{j+1}$. Conditions (1)–(7) hold throughout.

All modular arithmetic mod M in the above procedure can be performed in polynomial time. The last **Step** $4k-1$ gives:

$$C_{2k} \;=\; (q_{2k}, p_{2k}) \;\leftrightarrow\; [a_0;\, b_0,\, a_1,\, b_1,\, \ldots,\, a_{2k-1}].$$

All terms a_i and b_j are in the range $[1, M]$, so the final quotient p_{2k}/q_{2k} can be computed in polynomial time using the recurrence (3.1). This implies that p_{2k} and q_{2k} have polynomial binary lengths compared to the input μ, ν, g_i, h_i, e_i of AP-COVER. The curve $\mathcal{C}$ connecting $C_0, C_1, \ldots, C_{2k}$ is shown in Figure 2.

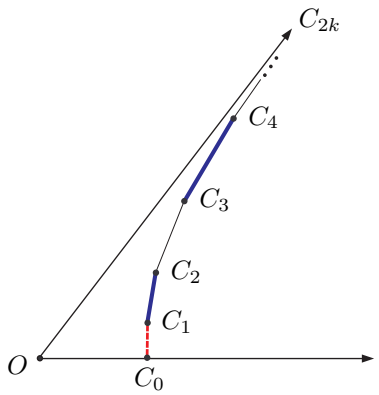

FIGURE 2. The curve $\mathcal{C}$.

Here each bold segment $C_{2i-1}C_{2i}$ contains $h_i + 1$ integer points. Each thin black segment $C_{2i}C_{2i+1}$ contains no interior integer points. The dotted segment C_0C_1 contains $g_1 + 1$ integer points, the first g_1 of which we will not need. Let $\mathcal{C}'$ be $\mathcal{C}$ minus the first g_1 integer points on C_0C_1. For brevity, we also denote $C_{2k} = (q_{2k}, p_{2k}) = (q, p)$.

4.2. **Analysis of the construction.** We define:

$$\Delta \;=\; \big\{ z \;:\; \exists (y_1, y_2) \in \mathcal{C}' \quad z \equiv y_2 \pmod{M} \big\}. \tag{4.2}$$

By condition (7), every integer point $\mathbf{y} = (y_1, y_2) \in \mathcal{C}'$ lies on one of the segments C_1C_2, C_3C_4, …, $C_{2k-1}C_{2k}$. Moreover, by condition (6), for $1 \le i \le k$ we have:

$$\mathrm{AP}_i \;=\; \mathcal{A}_i \;=\; \big\{ z \,:\, \exists \mathbf{y} \in C_{2i-1}C_{2i} \;\; z \equiv y_2 \pmod{M} \big\}$$

Therefore, we have:

$$\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k \;=\; \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_k \;=\; \Delta.$$

Recall that AP-COVER asks whether:

$$\exists z \in J \;\; z \notin \mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k \quad \Longleftrightarrow \quad \exists z \in J \;\; z \notin \Delta.$$

By (4.2), this is equivalent to:

$$\exists z \in J \quad \forall \mathbf{y} \in \mathcal{C}' \quad z \not\equiv y_2 \pmod{M},$$

which can be rewritten as:

$$\exists z \in J \ \ \forall \mathbf{y} \ \ z \not\equiv y_2 \pmod{M} \ \vee \ \mathbf{y} \notin \mathcal{C}'. \tag{4.3}$$

Next, we express the condition $\mathbf{y} = (y_1, y_2) \in \mathcal{C}'$ in short Presburger arithmetic. Let $\mathbf{v} = (p, -q)$ and θ be the cone between $\overrightarrow{OC_0}$ and $\overrightarrow{OC_{2k}}$, i.e.,

$$\theta \ = \ \big\{\mathbf{y} \in \mathbb{R}^2 \ : \ y_2 \geq 0, \ \mathbf{v} \cdot \mathbf{y} \geq 0\big\}.$$

For each $\mathbf{y} = (y_1, y_2) \in \theta$, denote by $P_{\mathbf{y}}$ the parallelogram with two opposite vertices O and $\mathbf{y}$ and sides parallel to $\overrightarrow{OC_0}$ and $\overrightarrow{OC_{2k}}$ (see Figure 3). We also require that horizontal edges in $P_{\mathbf{y}}$ are open, i.e.,

$$P_{\mathbf{y}} = \left\{\mathbf{x} \in \mathbb{R}^2 \ : \ \begin{array}{c} \mathbf{v}\cdot\mathbf{y} \ \geq \ \mathbf{v}\cdot\mathbf{x} \ \geq \ 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{array} \right\}. \tag{4.4}$$

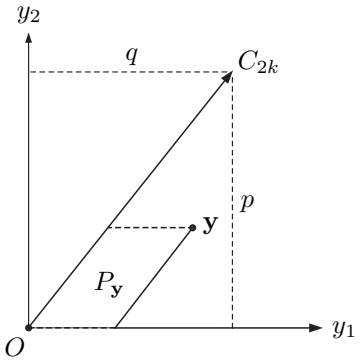

FIGURE 3. The parallelogram $P_{\mathbf{y}}$. The upper and lower edges of $P_{\mathbf{y}}$ are open (dotted). Here we denote $C_{2k} = (q_{2k}, p_{2k}) = (q, p)$.

Lemma 4.1. *For $\mathbf{y} \in \mathbb{Z}^2$, we have:*

$$\mathbf{y} \in \mathcal{C}' \iff \mathbf{v} \cdot \mathbf{y} \geq 0 \ \wedge \ y_2 \geq g_1 \ \wedge \ P_{\mathbf{y}} \cap \mathbb{Z}^2 = \varnothing. \tag{4.5}$$

Proof. First, assume $\mathbf{y} := (y_1, y_2) \in \mathcal{C}'$. Recall that $\mathcal{C}'$ is $\mathcal{C}$ minus the first g_1 integer points on C_0C_1. Therefore, we have $y_2 \geq g_1$. Since $\mathcal{C}$ sits inside θ, we also have $\mathbf{y} \in \theta$, which implies $\mathbf{v} \cdot \mathbf{y} \geq 0$. Let $\mathcal{R}$ be the concave region above $\mathcal{C}$ and below $\overrightarrow{OC_{2k}}$. By property (G6), $\mathcal{R}$ contains no interior integer points. Since $\mathbf{y} \in \mathcal{C}$, we have $P_{\mathbf{y}} \subset \mathcal{R}$. Therefore, the parallelogram $P_{\mathbf{y}}$ in (4.4) contains no integer points. We conclude that $\mathbf{y}$ satisfies the RHS in (4.5).

Conversely, assume $\mathbf{y}$ satisfies the RHS in (4.5) but $\mathbf{y} \notin \mathcal{C}'$. The following argument is illustrated in Figure 4. First, $\mathbf{v} \cdot \mathbf{y} \geq 0 \wedge y_2 \geq g_1$ implies $\mathbf{y} \in \theta$. Also, the parallelogram $P_{\mathbf{y}}$ contains no integer points. By property (G6), if $\mathbf{y} \notin \mathcal{C}'$, it must lie strictly below $\mathcal{C}'$. Let $\mathbf{x}$ and $\mathbf{x}'$ be the integer points on $\mathcal{C}$ that are immediately above and below $\mathbf{y}$ (see Figure 4). In other words, $\mathbf{x} \in \mathcal{C}$ is the integer point immediately above the intersection of $\mathcal{C}$ with the upper edge of $P_{\mathbf{y}}$, and $\mathbf{x}' \in \mathcal{C}$ is the integer point immediately below the intersection of $\mathcal{C}$ with the right edge of $P_{\mathbf{y}}$. Since $P_{\mathbf{y}}$ contains no integer points, particularly those on $\mathcal{C}$,

the points $\mathbf{x}$ and $\mathbf{x}'$ must be adjacent on $\mathcal{C}$, i.e., they form a segment on $\mathcal{C}$.[2] Now we draw a parallelogram D with two opposite vertices $\mathbf{x}, \mathbf{x}'$ and edges parallel to those of $P_{\mathbf{y}}$ (the dashed bold parallelogram in Figure 4). It is clear that D lies inside θ and also contains $\mathbf{y}$. Take $\mathbf{y}'$ to be the reflection of $\mathbf{y}$ across the midpoint of $\mathbf{x}\mathbf{x}'$. Since $\mathbf{x}, \mathbf{x}'$ and $\mathbf{y}$ are integer points, so is $\mathbf{y}'$. We also have $\mathbf{y}' \in D \subset \theta$. Note also that $\mathbf{y}'$ lies on the opposite side of $\mathcal{C}$ compared to $\mathbf{y}$. Therefore, we have $\mathbf{y}' \in \mathcal{R}$, contradicting property $(G6)$. □

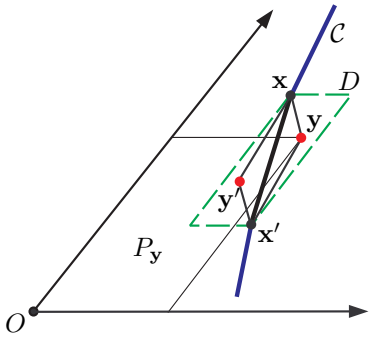

FIGURE 4. $\mathbf{y}'$ is the reflection of $\mathbf{y}$ across the midpoint of $\mathbf{x}\mathbf{x}'$.

Remark 4.2. There is a subtle point about the existence of $\mathbf{x}'$ in the above proof. It is clear that $\mathbf{x}$ exists because $\mathbf{y}$ lies below $\mathcal{C}$. However, if $\mathbf{y}$ lies too low, the right edge $P_{\mathbf{y}}$ might not intersect $\mathcal{C}$. For example, in Figure 5, we have $g_1 = 1$ and $\mathbf{y}$ lies on the line $y_2 = 1$. This this case, $P_{\mathbf{y}}$ contains no integer points and its right edge does not intersect $\mathcal{C}$. Thus, we have no $\mathbf{x}'$ and the geometric argument in Figure 4 does not work. However, this can be easily fixed by requiring $a_0 = g_1 \geq 2$, noting that AP-COVER is invariant under a simultaneous translation of J and all AP_i.

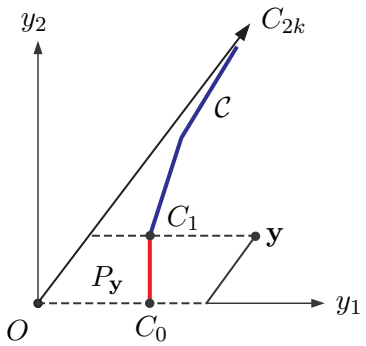

FIGURE 5. Here $g_1 = 1$, $\mathbf{y} \notin \mathcal{C}$, and yet $P_{\mathbf{y}}$ contains no integer points (dotted edges are open).

[2]Note that $\mathbf{x}$ and $\mathbf{x}'$ are not necessarily two consecutive vertices C_i and C_{i+1} of $\mathcal{C}$. They could be two consecutive points on some segment C_iC_{i+1}.

4.3. **Proof of Theorem 1.1 (decision part).** Combining (4.3), (4.4) and (4.5), the negation of AP-COVER is equivalent to:

$$\exists z \in J \quad \forall \mathbf{y} \quad \left[z \not\equiv y_2 \pmod{M} \ \vee \ \mathbf{v}\cdot\mathbf{y} < 0 \ \vee \ y_2 < g_1 \ \vee \ \exists \mathbf{x} \begin{Bmatrix} \mathbf{v}\cdot\mathbf{y} \geq \mathbf{v}\cdot\mathbf{x} \geq 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{Bmatrix} \right]. \tag{4.6}$$

The condition $z \not\equiv y_2 \pmod{M}$ can be expressed as:

$$\exists t \quad 0 < z - y_2 - Mt < M.$$

This existential quantifier $\exists t$ can be absorbed into $\exists \mathbf{x}$ because they are connected by a disjunction. The restricted quantifier $\exists z \in J$ with $J = [\mu, \nu]$ is just

$$\exists z \quad \mu \leq z \leq \nu.$$

Overall, we can rewrite (4.6) in prenex normal form:

$$\begin{aligned} \exists z \ \forall \mathbf{y} \ \exists \mathbf{x} \ \ \mu \leq z \leq \nu \ \wedge \ \Bigg[& 0 < z - y_2 - Mx_1 < M \ \vee \\ & \vee \ \mathbf{v}\cdot\mathbf{y} < 0 \ \vee \ y_2 < g_1 \ \vee \ \begin{Bmatrix} \mathbf{v}\cdot\mathbf{y} \geq \mathbf{v}\cdot\mathbf{x} \geq 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{Bmatrix} \Bigg]. \end{aligned} \tag{4.7}$$

All strict inequalities with integer variables can be sharpened. For example $y_2 > x_2$ is equivalent to $y_2 - 1 \geq x_2$. This final form contains 5 variables and 10 inequalities.

In summary, we have reduced (the negation of) AP-COVER to (4.7). This shows that (4.7) is NP-hard, and so is (Short-PA_3). For NP-completeness, by Theorem 3.8 in [Grä87], if (Short-PA_3) is true, there must be a satisfying $\mathbf{z}$ with binary length bounded polynomially in the binary length of Φ. Given such a polynomial length certificate $\mathbf{z}$, one can substitute it into (Short-PA_3) and verify the rest of the sentence, which has the form $\forall \mathbf{y} \ \exists \mathbf{x} \ \Psi(\mathbf{x}, \mathbf{y})$. Here Ψ is again a short Presburger expression. By Corollary 1.9, this can be checked in polynomial time. Thus, the whole sentence (Short-PA_3) is in NP. This concludes the proof of the decision part of Theorem 1.1. □

5. Proof of theorems 1.2 and 1.3 (decision part)

We will recast (4.7) into the form (GIP). For the polytopes R and Q in (GIP), let $R = J = [\mu, \nu]$ and

$$Q = \left\{ \mathbf{y} \in \mathbb{R}^2 \ : \ y_2 \geq g_1, \ y_1 \leq q, \ \mathbf{v}\cdot\mathbf{y} \geq 0 \right\}, \tag{5.1}$$

see Figure 6.

Since $R \supset \mathcal{C}'$, (4.3) is equivalent to:

$$\exists z \in R \quad \forall \mathbf{y} \in Q \quad z \not\equiv y_2 \pmod{M} \ \ \vee \ \ \mathbf{y} \notin \mathcal{C}'.$$

By condition (4.5), for $\mathbf{y} \in Q$, we have

$$\mathbf{y} \notin \mathcal{C}' \quad \iff \quad \exists \mathbf{x} \in P_{\mathbf{y}}.$$

Thus, the sentence (4.7) is equivalent to:

$$\begin{aligned} \exists z \in R \quad & \forall \mathbf{y} \in Q \quad \exists \mathbf{x} \\ & 0 < z - y_2 - Mx_1 < M \quad \vee \quad \mathbf{x} \in P_{\mathbf{y}}. \end{aligned} \tag{5.2}$$

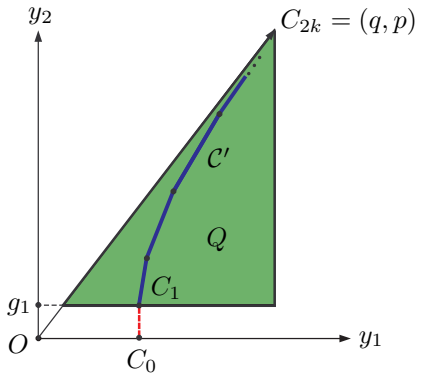

FIGURE 6. The triangle Q (shaded).

The remaining step is to covert the expression

$$1 \le z - y_2 - Mx_1 \le M - 1 \ \vee \ \begin{Bmatrix} \mathbf{v}\cdot\mathbf{y} \ge \mathbf{v}\cdot\mathbf{x} \ge 0 \\ y_2 - 1 \ge x_2 \ge 1 \end{Bmatrix} \tag{5.3}$$

into a single system. Here we expanded $\mathbf{x} \in P_{\mathbf{y}}$ and also sharpened all inequalities.

First, observe that for $z \in R$ and $\mathbf{y} \in Q$, there exists $\mathbf{x}$ satisfying (5.3) if and only if there exists such an $\mathbf{x}$ within some bounded range. Indeed, both R and Q are bounded, and (5.3) imply boundedness for $\mathbf{x}$. Therefore, we can take an N large enough so that

$$-N \le z,\, y_1,\, y_2,\, x_1,\, x_2 \le N. \tag{5.4}$$

For instance, $N = (M + p + q)^3$ suffices.

Now we convert (5.3) into a single system. This can be done in two slightly different ways, leading to theorems 1.2 and 1.3.

5.1. **Proof of Theorem 1.2 (decision part).** Applying the distributive law on (5.3), we get an equivalent expression:

$$\begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M - 1 \\ \mathbf{v}\cdot\mathbf{x} \le \mathbf{v}\cdot\mathbf{y} \end{bmatrix} \ \wedge \ \begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M - 1 \\ 0 \le \mathbf{v}\cdot\mathbf{x} \end{bmatrix} \ \wedge \ \dots \tag{5.5}$$

Here each $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ stands for a disjunction $a \vee b$ of two terms. In total, there are four such disjunctions.

Now we convert each of the above disjunctions into a conjunction. WLOG, consider the first one in (5.5). By the bounds (5.4), it is equivalent to:

$$\begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M - 1 \\ 0 \le \mathbf{v}\cdot\mathbf{y} - \mathbf{v}\cdot\mathbf{x} \le 2N(p+q) \end{bmatrix}. \tag{5.6}$$

Let $t_1 = z - y_2 - Mx_1$ and $t_2 = \mathbf{v}\cdot\mathbf{y} - \mathbf{v}\cdot\mathbf{x}$. By (5.4), we always have

$$|t_1| \le 2N + MN, \quad |t_2| \le 2N(p+q).$$

Define two polygons in $\mathbb{R}^2$:

$$P_1 \ = \ \big\{(t_1,t_2) \in \mathbb{R}^2 \ : \ 1 \le t_1 \le M-1, |t_2| \le 2N(p+q)\big\},$$

$$P_2 \ = \ \big\{(t_1,t_2) \in \mathbb{R}^2 \ : \ |t_1| \le 2N + MN, \ 0 \le t_2 \le 2N(p+1)\big\}.$$

Then (5.6) can be rewritten as:

$$(t_1,t_2) \ \in \ P_1 \ \cup \ P_2\,. \tag{5.7}$$

Next, define:

$$P_1' = (P_1, 0), \quad P_2' = (P_2, 1) \quad \text{and} \quad P = \operatorname{conv}(P_1', P_2').$$

In other words, we embed P_1 into the plane $t_3 = 0$ and P_2 into the plane $t_3 = 1$, all inside $\mathbb{R}^3$. As 3-dimensional polytopes, the convex hull of P_1' and P_2' is another polytope $P \subset \mathbb{R}^3$. It is easy to see that P has 6 facets, whose equations can be found from the vertices of P_1 and P_2. Also observe that for $(t_1, t_2, t_3) \in \mathbb{Z}^3$, we have:

$$(t_1, t_2, t_3) \ \in \ P \iff \begin{array}{l} (t_1, t_2) \ \in \ P_1, \ t_3 = 0, \ \text{or} \\ (t_1, t_2) \ \in \ P_2, \ t_3 = 1. \end{array}$$

From this, we have:

$$(t_1, t_2) \ \in \ P_1 \cup P_2 \iff \exists t_3 \ : \ (t_1, t_2, t_3) \ \in \ P. \tag{5.8}$$

Combined with (5.7), it implies that (5.6) is equivalent to:

$$\exists t \ : \ (z - y_2 - Mx_1, \, py_1 - qy_2 - px_1 + qx_2, \, t) \ \in \ P.$$

The above condition is a linear system with 6 equations. Doing this for each disjunction in (5.5), we get four new variables $\mathbf{t} \in \mathbb{Z}^4$ and a combined system of 24 inequalities. Thus, the original disjunction (5.3) is equivalent to a system:

$$\exists \mathbf{t} \in \mathbb{Z}^4 \ : \ A\mathbf{x} + B\mathbf{y} + Cz + D\mathbf{t} \ \le \ \overline{b}.$$

The inner existential quantifiers $\exists \mathbf{x} \in \mathbb{Z}^2$ and $\exists \mathbf{t} \in \mathbb{Z}^4$ can be combined into $\exists \mathbf{x} \in \mathbb{Z}^6$. Substituting everything into (5.2), we obtain the decision part of Theorem 1.2. □

5.2. **Proof of Theorem 1.3 (decision part).** Another way to convert (5.3) into a system is to directly interpret its two clauses and two separate polytopes. The same bounds (5.4) still apply. We will need the following special case of the *Upper Bound Theorem* (see e.g. Theorem 8.23 and Exercise 0.9 in [Zie95]).

Theorem 5.1 (McMullen)**.** *A polytope $P \subset \mathbb{R}^d$ with n vertices has at most*

$$f(d,n) \ := \ \binom{n - \lceil d/2 \rceil}{n-d} + \binom{n - \lfloor d/2 \rfloor - 1}{n-d} \quad \textit{facets.}$$

Similarly, a polytope $Q \subset \mathbb{R}^d$ with n facets has at most $f(d,n)$ vertices.

The first polytope we consider is given by:

$$\big\{(x_1, y_2, z) \in \mathbb{R}^3 \ : \ 1 \ \le \ z - y_2 - Mx_1 \ \le \ M - 1, \ -N \le x_1, y_2, z \le N\big\}.$$

This is a 3-dimensional polytope with 8 facets. Applying Theorem 5.1, we see that it has at most 12 vertices. To interpret it as a polytope in $z, \mathbf{y}$ and $\mathbf{x}$ we need to form its direct product with the interval $-N \le y_2 \le N$ also embed it in the hyperplane $x_2 = 0$. This produces a polytope $P_1 \subset \mathbb{R}^5$ with 24 vertices.

The second polytope we consider is given by:

$$\big\{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^4 \ : \ \mathbf{v} \cdot \mathbf{y} \ \ge \ \mathbf{v} \cdot \mathbf{x} \ \ge \ 0, \ y_2 - 1 \ \ge \ x_2 \ \ge \ 1, \ y \in Q\big\}.$$

As a 4-dimensional polytope it has only 8 vertices. These 8 vertices correspond to the cases when $\mathbf{y}$ lies at one of the three vertices of Q. Two of these vertices give two degenerate parallelograms $P_{\mathbf{y}}$, each of which is a segment with 2 vertices. The lower right vertex of Q gives a non-degenerate parallelogram $P_{\mathbf{y}}$ with 4 vertices. To interpret this as a 5-dimensional polytope in $z, \mathbf{y}$ and $\mathbf{x}$, we need to form its direct product with the polytope $R = [\mu, \nu]$ for z. This results in a polytope $P_2 \subset \mathbb{R}^5$ with 16 vertices.

Altogether, we have two polytopes $P_1, P_2 \subset \mathbb{R}^5$ with 40 vertices in total. We reapply the "lifting" trick in (5.8) to produce another polytope $P \subset \mathbb{R}^6$ with 40 vertices so that:

$$(z, \mathbf{y}, \mathbf{x}) \ \in \ P_1 \ \cup \ P_2 \ \iff \ \exists t \ : \ (z, \mathbf{y}, \mathbf{x}, t) \ \in \ P.$$

By Theorem 5.1, the resulting polytope P has at most

$$f(6, 40) \ = \ \binom{37}{34} \ + \ \binom{36}{34} \ = \ 8400$$

facets, which can all be found in polynomial time from the vertices. Therefore, the disjunction (5.3) is equivalent to a system:

$$\exists t \ : \ A\mathbf{x} + B\mathbf{y} + Cz + Dt \ \le \ \overline{b}$$

with at most 8400 inequalities. The existential quantifiers $\exists t$ and $\exists \mathbf{x} \in \mathbb{Z}^2$ can be combined into $\exists \mathbf{x} \in \mathbb{Z}^3$. Substituting all into (5.2), we obtain the decision part of Theorem 1.3. □

6. Proof of theorems 1.1, 1.2 and 1.3 (counting part)

Notice that the above reduction from AP-COVER to (4.7) is parsimonious, i.e., z lies in $J \setminus (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k)$ if and only if $\mu \le z \le \nu$ and

$$(6.1) \quad \forall \mathbf{y} \ \exists \mathbf{x} \ \left[0 < z - y_2 - Mx_1 < M \ \vee \ \mathbf{v} \cdot \mathbf{y} < 0 \ \vee \ y_2 < g_1 \ \vee \left\{ \begin{array}{c} \mathbf{v} \cdot \mathbf{y} \ge \mathbf{v} \cdot \mathbf{x} \ge 0 \\ y_2 > x_2 > 0 \end{array} \right\} \right].$$

At the same time, the reduction from 3SAT to AP-COVER given in §9.1 is also parsimonious, i.e., every satisfying assignment $\mathbf{u}$ for (9.1) corresponds to a unique $z \in J$ not covered by the arithmetic progressions and vice versa. This is due the uniqueness part of the Chinese Remainder Theorem used in (9.2). Since #3SAT is #P-complete (see e.g. [AB, MM11, Pap94]), so is counting the number of z satisfying (6.1). This proves the second part of Theorem 1.1.

The counting parts of theorems 1.2 and 1.3 can be proved with a similar argument to Section 5. □

7. Proof of Theorem 1.5

Consider the following m-generalization of the problem AP-COVER:

m-AP-COVER

Input: The following elements:
- m intervals $J_1 = [\mu_1, \nu_1]$, ... , $J_m = [\mu_m, \nu_m]$,
- k_1 triples (g_{1i}, h_{1i}, e_{1i}), with $1 \le i \le k_1$,
- ...
- k_m triples (g_{mi}, h_{mi}, e_{mi}), with $1 \le i \le k_m$,
- m integers $\tau_1, \ldots, \tau_m \in \mathbb{Z}$.

Decide:

$$Q_1(z_1 \in J_1 \setminus \Delta_1) \ \ldots \ Q_{m-1}(z_{m-1} \in J_{m-1} \setminus \Delta_{m-1}) \\ \ldots \ Q_m(z_m \in J_m) \ : \ \tau_1 z_1 + \ldots + \tau_m z_m \notin \Delta_m.$$

Here $Q_1, \ldots, Q_m \in \{\forall, \exists\}$ are m alternating quantifiers with $Q_m = \exists$. The sets $\Delta_1, \ldots, \Delta_m$ are defined as:

$$\Delta_t = \mathrm{AP}_{t1} \cup \cdots \cup \mathrm{AP}_{tk_t}, \ 1 \le t \le m$$

where

$$\mathrm{AP}_{ti} = \mathrm{AP}(g_{ti}, h_{ti}, e_{ti}), \ 1 \le i \le k_t.$$

Using Theorem 9.3, we prove Theorem 1.5 by reducing m-AP-COVER to short Presburger arithmetic. Theorem 1.1 is the special case when $m = 1$ ($\Sigma_1^{\mathsf{P}} \equiv \mathsf{NP}$). For simplicity, we show the reduction for the case $m = 2$. The same argument works for $m > 2$.

Consider 2-AP-COVER in (9.6), which is Π_2^{P}-complete. We can rewrite it as:

$$\forall z_2 \in J_2 \quad \big[z_2 \in \Delta_2 \ \vee \ \exists z_1 \in J_1 \ \ \tau_1 z_1 + \tau_2 z_2 \notin \Delta_1 \big]. \tag{7.1}$$

Replacing z with $\tau_1 z_1 + \tau_2 z_2$ in (6.1), we can express the condition $\tau_1 z_1 + \tau_2 z_2 \notin \Delta_1$ by a short formula $\forall \mathbf{y} \ \exists \mathbf{x} \ \Phi_1(\mathbf{x}, \mathbf{y}, \tau_1 z_1 + \tau_2 z_2)$ with 4 extra variables $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$ and 8 linear inequalities. Similarly, the condition $z_2 \in \Delta_2$ can be expressed as $\exists \mathbf{w} \ \forall \mathbf{t} \ \Phi_2(\mathbf{t}, \mathbf{w}, z_2)$ with another 4 variables $\mathbf{w}, \mathbf{t} \in \mathbb{Z}^2$ and also 8 inequalities.

Overall, (7.1) is equivalent to:

$$\forall z_2 \in J_2 \quad \Big[\exists \mathbf{w} \ \ \forall \mathbf{t} \ \ \Phi_2(\mathbf{t}, \mathbf{w}, z_2) \ \ \vee \ \ \exists z_1 \in J_1 \ \ \forall \mathbf{y} \ \ \exists \mathbf{x} \ \ \Phi_1(\mathbf{x}, \mathbf{y}, \tau_1 z_1 + \tau_2 z_2) \Big].$$

Each of the restricted quantifiers $\forall z_2 \in J_2$ and $\exists z_1 \in J_1$ contributes 2 more inequalities. Note that the two quantifier groups $\exists \mathbf{w} \ \forall \mathbf{t}$ and $\exists z_1 \ \forall \mathbf{y} \ \exists \mathbf{x}$ can be merged through the disjunction into $\exists \mathbf{w} \ \forall \mathbf{y}' \ \exists \mathbf{x}$. This results in new variables $\mathbf{w} \in \mathbb{Z}^2$, $\mathbf{y}' = (\mathbf{t}, \mathbf{y}) \in \mathbb{Z}^4$ and $\mathbf{x} \in \mathbb{Z}^2$. The final sentence takes the form

$$\forall z_2 \quad \exists \mathbf{w} \quad \forall \mathbf{y}' \quad \exists \mathbf{x} \quad \Phi(\mathbf{x}, \mathbf{y}', \mathbf{w}, z_2)$$

with 20 inequalities and 9 variables (z_1 has been absorbed into $\mathbf{w}$). □

8. Bilevel optimization and Pareto optima

8.1. **Proof of Theorem 1.6.** First, we characterize the convex chains $\mathcal{C}$ and $\mathcal{D}$ from Figure 1 using a quadratic function:

Lemma 8.1. *Let $\alpha = p/q \in \mathbb{Q}_+$. If $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^2$ satisfy $\frac{u_2}{u_1} < \alpha < \frac{v_2}{v_1}$ and $v_2 u_1 - v_1 u_2 = 1$ then both $\frac{u_2}{u_1}$ and $\frac{v_2}{v_1}$ are "weak" convergents of α, i.e., $\mathbf{u} \in \mathcal{C}$ and $\mathbf{v} \in \mathcal{D}$.*

Proof. Assume $\mathbf{u} \notin \mathcal{C}$, then $\mathbf{u} = (u_1, u_2)$ lies stricly below $\mathcal{C}$. By the argument from Lemma 4.1, the parallelogram $P_{\mathbf{u}}$ contains another point $\mathbf{u}' = (u_1', u_2') \in \mathbb{Z}^2$ with $\frac{u_2'}{u_1'} < \alpha$. Draw a line ℓ parallel to $\vec{\mathbf{v}}$ and passing through $\mathbf{u}$. Since $\frac{v_2}{v_1} > \alpha$, $P_{\mathbf{u}}$ lies completely to the left of ℓ (See Figure 7). From this, we conclude that $1 = v_2u_1 - v_1u_2 > v_2u_1' - v_1u_2' > 0$. In other words, the triangle $O\mathbf{uv}$ has larger area than that of $O\mathbf{u}'\mathbf{v}$. This is impossible, because $v_2u_1' - v_1u_2' \in \mathbb{Z}$. Therefore, we must have $\mathbf{u} \in \mathcal{C}$. By the same argument, we have $\mathbf{v} \in \mathcal{D}$. □

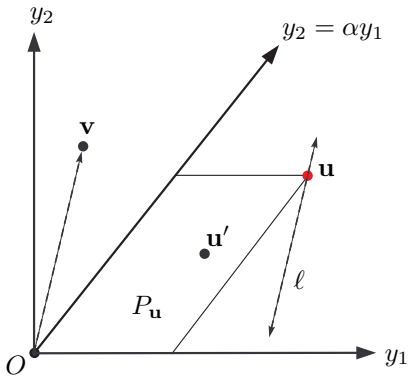

FIGURE 7. $\mathbf{u}$ and $\mathbf{v}$.

Conversely, for any weak convergent $\mathbf{u} \in \mathcal{C}$, we can find $\mathbf{v} \in \mathcal{D}$ with $v_2u_1 - v_1u_2 = 1$. This comes from the fact that any two consecutive convegents $\frac{p_i}{q_i}$ and $\frac{p_{i+1}}{q_{i+1}}$ of α satisfy $p_{i+1}q_i - p_iq_{i+1} = (-1)^i$.

Proof of Theorem 1.6. We use the same reduction from AP-COVER as in Sections 4 and 5. With the same rational number $\alpha = p/q$, let

$$Q = \big\{(u_1, u_2) \in \mathbb{R}^2 \ : \ u_2 \geq g_1, \ u_1 \leq q, \ pu_1 - qu_2 \geq 0\big\},$$

and

$$P = \big\{(v_1, v_2) \in \mathbb{R}^2 \ : \ v_2 \leq p - 1, \ v_1 \geq 0, \ pv_1 - qv_2 \leq 0\big\}.$$

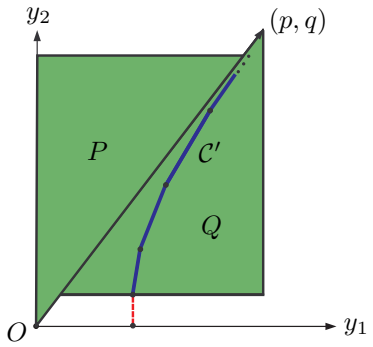

FIGURE 8. P and Q.

Recall from (4.3) that the NP-complete problem AP-COVER asks if there exists some $z \in J \subset [0, M]$ for which no $\mathbf{y} \in \mathcal{C}'$ satisfies $z \equiv y_2 \pmod{M}$. Here $\mathcal{C}'$ is the part of the

convex chain $\mathcal{C}$ lying inside Q. Now let $\mathbf{w} = (\mathbf{u}, \mathbf{v}, t)$, $W = Q \times P \times [0, T]$ and

$$h(z, \mathbf{w}) \quad = \quad K(v_2u_1 - v_1u_2 - 1) \quad + \quad (u_2 - z - tM)^2.$$

Here T and K are two appropriately chosen constants. Specifically, let $T = p/M$ so that if $z \equiv u_2 \pmod M$ then there always exists $t \in [0, T]$ with $t = \frac{u_2 - z}{M}$. For K, we pick it sufficiently large so that $K \gg (u_2 - z - tM)^2$ for every $\mathbf{u} \in Q$, $z \in J$ and $t \in [0, T]$. Clearly $K = (2TM + p)^3$ suffices.

With $\mathbf{u} \in Q \cap \mathbb{Z}^2$ and $\mathbf{v} \in P \cap \mathbb{Z}^2$, we have $v_2u_1 - v_1u_2 \geq 1$. Furthermore, by Lemma 8.1, equality happens if and only if $\mathbf{u} \in \mathcal{C}'$ and $\mathbf{v} \in \mathcal{D}$. For a fixed $z \in J$ consider the $\mathbf{w} \in W$ that minimizes $h(z, \mathbf{w})$. Since $K \gg (z - tM - u_2)^2$, the first term in h always dominate the second one. So we must have $v_2u_1 - v_1u_2 = 1$ when h is minimized, which implies $\mathbf{u} \in \mathcal{C}'$. Furthermore, among all $\mathbf{y} \in \mathcal{C}'$, $\mathbf{u}$ must be the one for which $u_2 \bmod M$ is closest to z, so that the second term in h is minimized. Thus,

$$\min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \quad h(z, \mathbf{w}) \quad \geq \quad 0,$$

and equality holds if and only if there is some $\mathbf{y} \in \mathcal{C}'$ with $z \equiv y_2 \pmod M$. Therefore,

$$\max_{z \in J \cap \mathbb{Z}} \quad \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \quad h(z, \mathbf{w}) \quad > \quad 0$$

if and only if there exists some $z \in J$ for which no $\mathbf{y} \in \mathcal{C}'$ satisfies $z \equiv y_2 \pmod M$. We conclude that computing (1.1) is NP-hard, as it implies AP-COVER. □

8.2. **Proof of Theorem 1.7.** First recall the definition of Pareto optima defined in Section 1.3. To summarize Section 8.1, we showed that computing

$$\max_{z \in J \cap \mathbb{Z}} \quad \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} \quad h(z, \mathbf{w}) \tag{8.1}$$

is NP-hard for $I \subset \mathbb{R}^1$ an interval, $W \subset \mathbb{R}^5$ a polytope with 18 facets and $h : \mathbb{R}^6 \to \mathbb{R}$ a quadratic function. Let $Q = I \times W \subset \mathbb{R}^6$, which has 38 facets. For $\mathbf{x} = (z, \mathbf{w}) \in Q \cap \mathbb{Z}^6$, let

$$f_1(\mathbf{x}) = z, \quad f_2(\mathbf{x}) = -z \quad \text{and} \quad f_3(\mathbf{x}) = h(z, \mathbf{w}).$$

Consider the set of Pareto minima of (f_1, f_2, f_3) on Q. For convenience, we denote an outcome vector $\mathbf{y} = \big(f_1(\mathbf{x}), f_2(\mathbf{x}), f_3(\mathbf{x})\big)$ by $\mathbf{y} = f(\mathbf{x})$. Consider two points $\mathbf{x} = (z, \mathbf{w})$ and $\mathbf{x}' = (z, \mathbf{w}')$ in $Q \cap \mathbb{Z}^6$. If $h(z, \mathbf{w}) < h(z, \mathbf{w}')$ then $f_1(\mathbf{x}) = f_1(\mathbf{x}')$, $f_2(\mathbf{x}) = f_2(\mathbf{x}')$, and $f_3(\mathbf{x}) < f_3(\mathbf{x}')$. Then $\mathbf{y}' = f(\mathbf{x}')$ is not a Pareto minimum in this case. Therefore, all Pareto minima must be of the form $\mathbf{y} = f(\mathbf{x})$, where $\mathbf{x} = (z, \mathbf{w}_{\min})$ with $h(z, \mathbf{w}_{\min}) = \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} h(z, \mathbf{w})$. Furthermore, if $\mathbf{x} = (z, \mathbf{w}_{\min})$ and $\mathbf{x}' = (z', \mathbf{w}'_{\min})$ are two such points with $z \neq z'$, then the outcome vectors $\mathbf{y} = f(\mathbf{x})$ and $\mathbf{y}' = f(\mathbf{x}')$ are incomparable, simply because either $f_1(\mathbf{x}) < f_1(\mathbf{x}')$ and $f_2(\mathbf{x}) > f_2(\mathbf{x}')$, or the other way around.

We conclude that the set Pareto minima of (f_1, f_2, f_3) on Q is given as:

$$\mathcal{P} \ = \ \Big\{ \mathbf{y} = \big(z, -z, h(z, \mathbf{w}_{\min})\big) \ : \ z \in J \cap \mathbb{Z}, \ h(z, \mathbf{w}_{\min}) = \min_{\mathbf{w} \in W \cap \mathbb{Z}^5} h(z, \mathbf{w}) \Big\}.$$

For $\mathbf{y} \in \mathbb{R}^3$, let $g(\mathbf{y}) = -y_3$. Then minimizing $g(\mathbf{y})$ over $\mathbf{y} \in \mathcal{P}$ is the same as computing the negated value of (8.1). This proves the first part of Theorem 1.7.

To show the hardness of approximating $\min_{\mathbf{y} \in \mathcal{P}} g(\mathbf{y})$ within a multiplicative factor of $1/2$, recall from Section 8.1 that the value of (8.1) determines the AP-COVER. To be precise, (8.1) is equal to the largest squared distance of an integer $z \in J$ from the union $\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k$, which is 0 if and only if $J \cap \mathbb{Z}$ is entirely covered by these APs.

Recall the part of the proof of Theorem 9.1, where we reduce 3SAT to AP-COVER. There, we pick the first ℓ primes $p_1 = 2, p_2, \ldots, p_\ell$. The reduction would work verbatim

if we picked $p_2 = 3, \ldots, p_{\ell+1}$ instead. The advantage of this small change is that now we can exclude the arithmetic progression $z \equiv 0 \pmod 2$ from J. In other words, we require $z \equiv 1 \pmod 2$ and the Chinese Remainder Theorem still works. Then the final union $\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k$ which we exclude from J must contain all even numbers. This implies that the largest squared distance of an integer $z \in J$ to $\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k$ is at most 1. Therefore, the value of (8.1) is either 1 or 0. So getting a 1/2-approximation is equivalent to deciding AP-COVER, and thus NP-hard.

9. Covering with arithmetic progressions

9.1. **NP-completeness of AP-COVER.** Recall the following problem from §4.1.

AP-COVER
Input: An interval $J = [\mu, \nu] \subset \mathbb{Z}$ and k triples (g_i, h_i, e_i) for $i = 1, \ldots, k$.
Decide: Is there $z \in I$ such that $z \notin (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k)$, where $\mathrm{AP}_i = \mathrm{AP}(g_i, h_i, e_i)$?

In this section, we reproduce (in a somewhat different language) the original proof from [SM73], see also Remark 9.2 below. The reduction in the proof will later be extended to work with more quantifiers.

Theorem 9.1 (Stockmeyer and Meyer)**.** AP-COVER *is* NP*-complete.*

Proof. We reduce 3SAT to AP-COVER. Consider a 3-CNF Boolean expression:

$$\Psi(\mathbf{u}) \ = \ \bigwedge_{i=1}^{n} C_i(\mathbf{u}), \tag{9.1}$$

where $\mathbf{u} = u_1 \ldots u_\ell \in \{\text{true}, \text{false}\}^\ell$ are Boolean variables, and each clause $C_i(\mathbf{u})$ is a disjunction of three literals from the set

$$\{u_j, \neg u_j \ : \ 1 \le j \le \ell\}.$$

Let $p_1, \ldots, p_\ell$ be the first ℓ primes. We have $p_\ell = O(\ell \log \ell)$ by the Prime Number Theorem. So $p_1, \ldots, p_\ell$ can be found in time $\mathrm{poly}(\ell)$. We restrict z to the interval $J = [0, p)$, where $p = p_1 \cdots p_\ell$. For each assignment of $\mathbf{u} = u_1 \ldots u_\ell \in \{\text{true}, \text{false}\}^\ell$, we shall associate a unique integer $z \in J$ that satisfies:

$$u_j = \text{true} \iff z \equiv 1 \pmod{p_j} \quad ; \quad u_j = \text{false} \iff z \equiv 0 \pmod{p_j}. \tag{9.2}$$

First, for each j, we exclude all moduli mod p_j that are not 0 or 1. In other words, we exclude the arithmetic progressions:

$$\mathrm{AP}_{jt} \ = \ \big\{z \in J \ : \ z \equiv t \pmod{p_j}\big\} \quad \text{for} \quad 1 \le j \le \ell, \ 2 \le t < p_j\,. \tag{9.3}$$

If $z \notin \bigcup_{jt} \mathrm{AP}_{jt}$ then z is equal to 0 or 1 mod every p_j. Now consider each clause $C_i(\mathbf{u})$. For example, assume $C_1(\mathbf{u}) = u_1 \vee \neg u_2 \vee u_3$. The negation $\neg C_1(\mathbf{u})$ is $\neg u_1 \wedge u_2 \wedge \neg u_3$. To this, we associate an arithmetic progression:

$$\mathrm{AP}_1 \ = \ \big\{z \in J \ : \ z \equiv 0 \pmod{p_1} \ \wedge \ z \equiv 1 \pmod{p_2} \ \wedge \ z \equiv 0 \pmod{p_3}\big\}. \tag{9.4}$$

By the Chinese remainder theorem, we can write:

$$\mathrm{AP}_1 \ = \ \big\{z \in J \ : \ z \equiv e \pmod{p_1 p_2 p_3}\big\},$$

where e is unique mod $p_1 p_2 p_3$ and also computable in polynomial time. Then we have:

$$C_1(\mathbf{u}) = \text{true} \quad \iff \quad z \notin \mathrm{AP}_1. \tag{9.5}$$

Doing this for all clauses $C_1, \ldots, C_n$, we get n arithmetic progressions $\mathrm{AP}_1, \ldots, \mathrm{AP}_n$. From (9.1), (9.3) and (9.5), we conclude that:

$$\Psi(\mathbf{u}) \;=\; \bigwedge_{i=1}^{n} C_i(\mathbf{u}) = \text{true} \quad \iff \quad z \notin \bigcup_{1\le i\le n} \mathrm{AP}_i \bigcup_{\substack{1\le j\le \ell \\ 2\le t<p_j}} \mathrm{AP}_{jt}\,.$$

Therefore,

$$\exists \mathbf{u} \quad \Psi(\mathbf{u}) = \text{true} \quad \iff \quad \exists z \in J \;:\; z \notin \bigcup_{1\le i\le n} \mathrm{AP}_i \bigcup_{\substack{1\le j\le \ell \\ 2\le t<p_j}} \mathrm{AP}_{jt}\,.$$

The above LHS is a 3SAT sentence, which is NP-complete to decide. Thus, the RHS, which is AP-COVER, is also NP-complete. In total, we have $k := n + \sum_{j=1}^{\ell}(p_j - 1)$ arithmetic progressions, each of which can be given as a triple (g_i, h_i, e_i). □

Remark 9.2. In [GJ79, §A7], the problem AP-COVER is phrased differently under the name SIMULTANEOUS INCONGRUENCES problem.

9.2. **Generalization of AP-COVER to m quantifiers.** We consider the following m-generalization of the problem AP-COVER.

m-AP-COVER

Input: The following elements:
- m intervals $J_1 = [\mu_1, \nu_1]$, ... , $J_m = [\mu_m, \nu_m]$,
- k_1 triples (g_{1i}, h_{1i}, e_{1i}), with $1 \le i \le k_1$,
- ...
- k_m triples (g_{mi}, h_{mi}, e_{mi}), with $1 \le i \le k_m$,
- m integers $\tau_1, \ldots, \tau_m \in \mathbb{Z}$.

Decide: The truth of the sentence:

$$Q_1(z_1 \in J_1 \setminus \Delta_1) \;\; \ldots \;\; Q_{m-1}(z_{m-1} \in J_{m-1} \setminus \Delta_{m-1}) \\ \ldots \;\; Q_m(z_m \in J_m) \;\; : \;\; \tau_1 z_1 + \ldots + \tau_m z_m \notin \Delta_m.$$

Here $Q_1, \ldots, Q_m \in \{\forall, \exists\}$ are m alternating quantifiers with $Q_m = \exists$. The sets $\Delta_1, \ldots, \Delta_m$ are defined as:

$$\Delta_t = \mathrm{AP}_{t1} \cup \cdots \cup \mathrm{AP}_{tk_t},\; 1 \le t \le m$$

where

$$\mathrm{AP}_{ti} = \mathrm{AP}(g_{ti}, h_{ti}, e_{ti}),\; 1 \le i \le k_t.$$

For example, 2-AP-COVER asks whether

$$\forall (z_2 \in J_2 \setminus \Delta_2) \quad \exists z_1 \in J_1 \quad \tau_1 z_1 + \tau_2 z_2 \notin \Delta_1, \tag{9.6}$$

i.e., for all $z_2 \in J_2$ either z_2 is covered by some AP in the first group, or there is some $z_1 \in J_1$ so that their linear combination $\tau_1 z_1 + \tau_2 z_2$ is not covered by any AP in the second group.

Theorem 9.3. *m-AP-COVER is Σ_m^{P}-complete for m odd and Π_m^{P}-complete for m even.*

Proof. For simplicity, we show that 2-AP-COVER is Π_2^{P}-complete. The proof for general m-AP-COVER is analogous.

This is similar to Theorem 9.1's proof, but instead of 3SAT we decide:

$$\forall \mathbf{v} \quad \exists \mathbf{u} \quad \Psi(\mathbf{u}, \mathbf{v}) = \text{true}, \tag{9.7}$$

where $\mathbf{u}, \mathbf{v} \in \{\text{true}, \text{false}\}^{\ell}$, and $\Psi(\mathbf{u}, \mathbf{v}) = \bigwedge_{i=1}^{n} C_i(\mathbf{u}, \mathbf{v})$, with each clause $C_i(\mathbf{u}, \mathbf{v})$ a disjunction of three literals from the set

$$\{u_j, \neg u_j, v_j, \neg v_j \ : \ 1 \le j \le \ell\}.$$

Deciding (9.7) is Π_2^{P}-complete (see e.g. [GJ79, Pap94]). To reduce (9.7) to (9.6), we again take the first 2ℓ primes $p_1, \ldots, p_\ell, q_1, \ldots, q_\ell$. Let $p = p_1 \cdots p_\ell$, $q = q_1 \cdots q_\ell$ and:

$$J_1 \ := \ [0, \ p) \quad \text{and} \quad J_2 \ := \ [0, \ q).$$

Since $\gcd(p, q) = 1$, we can also find in polynomial time $\tau_1, \tau_2 \in \mathbb{Z}$ so that:

$$\tau_1 \equiv 1 \pmod{p}, \ q \,|\, \tau_1 \quad \text{and} \quad \tau_2 \equiv 1 \pmod{q}, \ p \,|\, \tau_2. \tag{9.8}$$

Next, we require that $z_2 \equiv 0$ or $1 \pmod{q_j}$ for $i = 1, \ldots, \ell$. This can be expressed as $z_2 \in J_2 \setminus \Delta_2$, where Δ_2 is a union of some arithmetic progressions similar to those in (9.3). These are the k_2 progressions $\text{AP}_{21}, \ldots, \text{AP}_{2k_2}$.

We also require $z_1 \equiv 0$ or $1 \pmod{p_j}$ for $j = 1, \ldots, \ell$. By (9.8), this is equivalent to $\tau_1 z_1 + \tau_2 z_2 \equiv 0$ or $1 \pmod{p_j}$. Again, this condition can be expressed as:

$$\tau_1 z_1 + \tau_2 z_2 \ \notin \ \Gamma_1 \tag{9.9}$$

for Γ_1 a union of some arithmetic progressions.

Analogous to (9.2), the variables z_1 and z_2 correspond to $\mathbf{u}$ and $\mathbf{v}$, respectively. By the Chinese remainder theorem (see (9.4) and (9.5)), we can express each clause $C_i(\mathbf{u}, \mathbf{v})$ as:

$$C_1(\mathbf{u}, \mathbf{v}) = \text{true} \quad \iff \quad \tau_1 z_1 + \tau_2 z_2 \ \notin \ \text{AP}_i$$

for some arithmetic progression AP_i with $i = 1, \ldots, n$. Let Δ_1 be the union of Γ_1 in (9.9) with $\text{AP}_1, \ldots, \text{AP}_n$.

Overall, we have $k_1 + k_2$ finite arithmetic progressions from Δ_1 and Δ_2. Note that $k_1 + k_2$ is still polynomial compared to ℓ and the length of Ψ. It is straightforward that (9.6) and (9.7) are equivalent. Therefore, deciding (9.6) is Π_2^{P}-complete. □

10. On Kannan's Partition Theorem

10.1. **Validity of KPT.** By *Parametric Integer Programming* (PIP), we mean the following problem. Given an integer matrix $A \in \mathbb{Z}^{m \times n}$ and a k-dimensional polyhedron $W \subset \mathbb{R}^m$, is the following sentence true:

$$\forall\, \overline{b} \in W \quad \exists \mathbf{x} \in \mathbb{Z}^n \quad : \quad A\mathbf{x} \le \overline{b}. \tag{10.1}$$

We think of $\overline{b}$ as a parameter varying over W. For every fixed $\overline{b}$, this gives an Integer Programming problem in fixed dimension n. In [Kan90, Theorem 3.1], Kannan claimed the following result, which implies a polynomial time algorithm to decide (10.1). From here on, we use RA to denote *rational affine transformations*. Also let $K_{\overline{b}} := \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \le \overline{b}\}$ for every $\overline{b} \in W$.

Theorem 10.1 (Kannan's Partition Theorem)**.** *Fix n and k. Given a* PIP *problem, we can find in polynomial time a partition*

$$W = P_1 \sqcup P_2 \sqcup \cdots \sqcup P_r, \tag{10.2}$$

where each P_i is a rational copolyhedron[3]*, so that the partition satisfies the following properties. For each P_i, we can find in polynomial time a finite set $\mathcal{T}_i = \{(S_{ij}, T_{ij})\}$ of pairs of RAs $T_{ij} : \mathbb{R}^m \to \mathbb{R}^n$ and $S_{ij} : \mathbb{Z}^n \to \mathbb{Z}^n$, so that for every $\overline{b} \in P_i$ we have:*

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \iff \exists (S_{ij}, T_{ij}) \in \mathcal{T}_i \ : \ S_{ij}\lfloor T_{ij}\overline{b}\rfloor \in K_{\overline{b}}.$$

Furthermore, for each P_i, the set $\mathcal{T}_i$ contains at most n^{4n} pairs (S_{ij}, T_{ij}). The number of all P_i is $r \leq (mn\phi)^{kn^{\delta n}}$, where ϕ is the binary length of A and δ is a universal constant.

KPT claims that in order to solve for an $\mathbf{x} \in \mathbb{Z}^n$ satisfying $A\mathbf{x} \leq \overline{b}$ with $\overline{b}$ varying over W, we only need to preprocess the matrix A in polynomial time and obtain a polynomial number of regions P_i. When queried with $\overline{b} \in P_i$, we only need to check for a fixed number (n^{4n}) of candidates of the form $\mathbf{x} = S_{ij}\lfloor T_{ij}\overline{b}\rfloor$ to get an integer solution in $K_{\overline{b}}$ (if any exists).

Let us prove that KPT, if true, would imply far stronger statements for a PIP problems that involves only a matrix of fixed length m. From now on, fix m, n and k. By KPT and the observation $mn \leq \phi$, the number of regions P_i in (10.2) can be bounded as:

$$r \ \leq \ (mn\phi)^{kn^{\delta n}} \ \leq \ \phi^{\gamma(n,k)}. \tag{10.3}$$

Here $\gamma(n, k)$ is a constant which depends only on n and k. The following structural result is an implication of KPT when the parameter space W is 1-dimensional, i.e. when $k = 1$:

$$W \ = \ \{f(y) \in \mathbb{R}^m \ : \ y \in I\} \tag{10.4}$$

where $f : \mathbb{R}^1 \to \mathbb{R}^m$ is a RA, and $I \subset \mathbb{R}$ a bounded interval.

Lemma 10.2. *Assume* (10.3) *holds. Given a* PIP *problem with a 1-dimensional parameter space W* (10.4)*, there exists a finite set $\mathcal{T} = \{(S_j, T_j)\}$ of pairs of RAs $T_j : \mathbb{R}^1 \to \mathbb{R}^n$ and $S_j : \mathbb{Z}^n \to \mathbb{Z}^n$ so that the following hold. For every $y \in I \cap \mathbb{Z}$ and $\overline{b} = f(y) \in \mathbb{R}^m$, we have:*

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \quad \iff \quad \exists (S_j, T_j) \in \mathcal{T} \ : \ S_j\lfloor T_j y\rfloor \in K_{\overline{b}}.$$

Furthermore, the set $\mathcal{T}$ contains at most $c(n)$ pairs (S_j, T_j), where $c(n)$ is a constant which depends only on n.

Remark 10.3. The above lemma says that the bound (10.3) as implied by KPT would guarantee a small set of candidates for any "short" PIP problem $A\mathbf{x} \leq f(y)$ with 1-dimensional parameters y. The number of candidates $c(n)$ depends only on the dimension n.

Proof of Lemma 10.2. WLOG, assume $I = [0, N)$ and $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$. Let

$$M \ = \ N \prod_{ij}(|a_{ij}| + 1) \prod_{k}(|p_k q_k| + 1), \tag{10.5}$$

where p_k/q_k runs over all rational coefficients in f. Let $J = [0, MN)$. Consider the following PIP problem with one parameter $y' \in J$ and $n + 2$ integer variables $\mathbf{x} \in \mathbb{Z}^n$, $y_1, y_2 \in \mathbb{Z}$:

$$Ny_1 + y_2 = y', \quad 0 \leq y_1 < M, \quad 0 \leq y_2 < N, \quad A\mathbf{x} - f(y_2) \leq 0. \tag{10.6}$$

Observe that when (10.6) is feasible, the values of y_1 and y_2 are uniquely determined. Indeed, we should have $y_1 = \lfloor y'/N\rfloor$ and $y_2 = y' - Ny_1$. So as y' varies over $J \cap \mathbb{Z}$, the solutions of (10.6) correspond bijectively with the solutions of the original PIP problem $A\mathbf{x} \leq f(y)$ where $y = \lfloor y'/N\rfloor \in I$.

Clearly, (10.6) can be put into the form $B\mathbf{z} \leq g(y')$ where $\mathbf{z} = (\mathbf{x}, y_1, y_2) \in \mathbb{Z}^{n+2}$ are variables and g is an RA. Let $\overline{b}' = g(y')$, then the problem takes the form $B\mathbf{z} \leq \overline{b}'$. Also let

[3]A copolyhedron is a convex polyhedron with possibly some open facets.

$W' = \{\overline{b}' = g(y') : y' \in J\}$. Applying KPT to the PIP problem $B\mathbf{z} \le \overline{b}'$ with a 1-dimensional parameter space W', we have a partition of W' into polynomially many intervals. Since $\overline{b}' = g(y')$ and g is an RA, this partition induces another partition on J (the space for y') into intervals:

$$J \;=\; J_1 \sqcup \cdots \sqcup J_r\,. \tag{10.7}$$

By (10.3), the number r of all intervals in this partition is polynomial in the binary length of the matrix B. From (10.5) and (10.6), it is clear that B has no more than $2mn$ entries, each bounded by M. Therefore, we have:

$$r \;\le\; \left(\sum_{ij} \lceil \log b_{ij} \rceil\right)^{\gamma} \;\le\; (2mn \log M)^{\gamma} \;\ll\; M. \tag{10.8}$$

Here $\gamma = \gamma(n,k)$ is some constant degree guaranteed by KPT. Since $r \ll M$, some interval J_i from (10.7) must contain an entire subinterval $I' = [kN, (k+1)N)$ for some $0 \le k < M$. For simplicity, assume $I' = [kN, (k+1)N] \subseteq J_1$.

Also by KPT, for the interval J_1, there is a set of candidates $\mathcal{T}_1 = \{(S_{1j}, T_{1j})\}$ of size at most $c(n) := (n+2)^{4(n+2)}$ for the PIP problem $B\mathbf{z} \le \overline{b}'$. For every $y' \in I' \subseteq J_1$, each solution of (10.6) should have $y_1 = k$ and $y_2 = y' - Nk$. By a translation $y = y' - Nk$, we can map I' back to I. Accordingly, we can modify each candidate $(S_{ij}, T_{ij}) \in \mathcal{T}_i$ to be a pair of RAs in y. Clearly, they serve as candidates for the original PIP problem $A\mathbf{x} \le f(y)$ with $y \in I$. □

Lemma 10.2 can be easily boosted to a k-dimensional parameter space W for a fixed k:

$$W \;=\; \{f(\mathbf{y}) \in \mathbb{R}^m \;:\; \mathbf{y} \in R\} \tag{10.9}$$

with $f : \mathbb{R}^k \to \mathbb{R}^m$ an RA and $R \subset \mathbb{R}^k$ a rectangular box.

Lemma 10.4. *Assume* (10.3) *holds. Given a* PIP *problem with a k-dimensional parameter space W* (10.9)*, there exists a finite set $\mathcal{T} = \{(S_j, T_j)\}$ of pairs of RAs $T_j : \mathbb{R}^k \to \mathbb{R}^n$ and $S_j : \mathbb{Z}^n \to \mathbb{Z}^n$ so that the following hold. For every $\mathbf{y} \in R \cap \mathbb{Z}^k$ and $\overline{b} = f(\mathbf{y}) \in \mathbb{R}^m$, we have:*

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \quad \iff \quad \exists (S_j, T_j) \in \mathcal{T} \;:\; S_j\lfloor T_j \mathbf{y} \rfloor \in K_{\overline{b}}.$$

Furthermore, the set $\mathcal{T}$ contains at most $c(n,k)$ pairs (S_j, T_j), where $c(n,k)$ is a constant which depends only on n and k.

Proof. WLOG, assume $R = [0, r_1) \times \ldots \times [0, r_k)$. We "flatten" the k-dimensional parameter $\mathbf{y}$. For every $\mathbf{y} = (y_1, \ldots, y_k) \in R$, let:

$$y' \;=\; y_1 + y_2 r_1 + y_3 (r_1 r_2) + \ldots + y_k (r_1 \cdots r_{k-1}) \;\in\; [0,\, r_1 \cdots r_k). \tag{10.10}$$

This RA maps the integer points in R bijectively to those in $I = [0,\, r_1 \cdots r_k)$. We rewrite $A\mathbf{x} \le f(\mathbf{y})$ as another PIP problem with a 1-dimensional parameter $y' \in I$ and $n+k$ variables $\mathbf{x} \in \mathbb{Z}^n$, $\mathbf{y} \in \mathbb{Z}^k$:

$$\begin{aligned} y' \;&=\; y_1 + y_2 r_1 + y_3 (r_1 r_2) + \ldots + y_k (r_1 \cdots r_{k-1}), \\ 0 \le y_i < r_i \;&\text{ for }\; 1 \le i \le k, \quad A\mathbf{x} - f(\mathbf{y}) \le 0. \end{aligned} \tag{10.11}$$

Note that (10.11) has a solution if and only if the original PIP problem $A\mathbf{x} \le f(\mathbf{y})$ has a solution. Furthermore, in every solution of (10.11), the variables $\mathbf{y}$ are uniquely determined by y' via the RA (10.10). Applying Lemma 10.2, we get a set $\mathcal{T}' = \{(S'_j, T'_j)\}$ of at most $c(n,k) := (n+k+2)^{4(n+k+2)}$ candidates for (10.11), where $T'_j : \mathbb{R}^1 \to \mathbb{R}^{n+k}$ and

$S'_j : \mathbb{Z}^{n+k} \to \mathbb{Z}^{n+k}$ are pairs of RAs. Using (10.10), we can re-express each pair (S'_j, T'_j) as a pair (S_j, T_j) with $T_j : \mathbb{R}^k \to \mathbb{R}^n$ and $S_j : \mathbb{Z}^n \to \mathbb{Z}^n$ so that (10.11) has a solution if and only if $\mathbf{x} = S_j\lfloor T_j\mathbf{y}\rfloor$ satisfies $A\mathbf{x} \le f(\mathbf{y})$ for some j. In other words, $\mathcal{T} = \{(S_j, T_j)\}$ is a finite set of at most $c(n,k)$ candidates for the original PIP problem $A\mathbf{x} \le f(\mathbf{y})$. □

Remark 10.5. Since the dimensions of A are fixed, each condition $S_{ij}\lfloor T_{ij}\mathbf{y}\rfloor \in K_{\overline{b}}$ can be expressed as a short Boolean combination of linear inequalities, at the cost of introducing a few extra $\exists$ or $\forall$ quantifiers. For example, a condition $\frac{1}{2} + \lfloor y/5\rfloor \le 3$ for $y \in \mathbb{Z}$ can be expressed as either

$$\exists t \left\{ \begin{array}{ccc} t & \le & y/5 \\ t & > & y/5 - 1 \\ \frac{1}{2} + t & \le & 3 \end{array} \right\} \quad \text{or} \quad \forall t \left[\begin{array}{ccc} t & > & y/5 \\ t & \le & y/5 - 1 \\ \frac{1}{2} + t & \le & 3 \end{array} \right]. \tag{10.12}$$

Here $\{\cdot\}$ is a conjunction and $[\cdot]$ is a disjunction.

Now we relax the parameter space W to an arbitrary k-dimensional polyhedron, i.e.,

$$W \;=\; \{f(\mathbf{y}) \in \mathbb{R}^m \;:\; \mathbf{y} \in Q\} \tag{10.13}$$

with $f : \mathbb{R}^k \to \mathbb{R}^m$ an RA and $Q \subset \mathbb{R}^k$ a polyhedron.

Corollary 10.6. *Assume* (10.3) *holds. Then for every fixed m, n and k, there is a constant $d(m,n,k)$ so that the following holds. For a* PIP *problem with a k-dimensional parameter space W* (10.13)*, let:*

$$Q' \;=\; \big\{\mathbf{y} \in Q \cap \mathbb{Z}^k \;:\; A\mathbf{x} \le f(\mathbf{y}) \;\textit{ has no solutions }\; \mathbf{x} \in \mathbb{Z}^n\big\}.$$

If $|Q'| > d(m,n,k)$, then it contains three distinct points $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3$ with $\mathbf{y}_3 = (\mathbf{y}_1 + \mathbf{y}_2)/2$.

Proof. Let R be a large enough box that contains Q. Applying Lemma 10.4 to the PIP problem $A\mathbf{x} \le f(\mathbf{y})$ with $\mathbf{y} \in R$, we get a set of candidates $\mathcal{T} = \{(S_j, T_j)\}$ of size at most $c(n,k)$ so that:

$$A\mathbf{x} \le f(\mathbf{y}) \text{ has no solutions} \quad \Longleftrightarrow \quad \forall (S_j, T_j) \in \mathcal{T} \;:\; S_j\lfloor T_j\mathbf{y}\rfloor \not\le f(\mathbf{y}).$$

By the argument in Remark 10.5, each condition $S_j\lfloor T_j\mathbf{y}\rfloor \not\le f(\mathbf{y})$ can be expressed by a short Presburger formula $\exists \mathbf{t}\; \Phi_j(\mathbf{y}, \mathbf{t})$ with length bounded in m (fixed). Taking conjunction over all such formulas for $1 \le j \le c(n,k)$, we have:

$$A\mathbf{x} \le f(\mathbf{y}) \text{ has no solutions} \quad \Longleftrightarrow \quad \exists \widetilde{\mathbf{t}} \quad \Phi(\mathbf{y}, \widetilde{\mathbf{t}}).^4 \tag{10.14}$$

Here Φ is still a short Presburger expression in a bounded number of variables. Denote by λ and μ the total number of variables and inequalities in Φ, respectively. Both of these are constants in m, n and k. Let $d = d(m,n,k) = 2^{\lambda+\mu}$. The μ inequalities in Φ determine μ hyperplanes in $\mathbb{R}^\lambda$. These hyperplanes partition $\mathbb{R}^\lambda$ into polyhedral regions:

$$\mathbb{R}^\lambda \;=\; W_1 \sqcup \cdots \sqcup W_\eta,$$

with $\eta \le 2^\mu$. Observe that as $(\mathbf{y}, \widetilde{\mathbf{t}})$ varies over a single region W_j, the value of $\Phi(\mathbf{y}, \widetilde{\mathbf{t}})$ is always true or always false. Since $|Q'| > d$, we have at least $d+1$ distinct pairs $(\mathbf{y}_1, \widetilde{\mathbf{t}}_1), \ldots, (\mathbf{y}_{d+1}, \widetilde{\mathbf{t}}_{d+1})$ for each of which $\Phi(\mathbf{y}_i, \widetilde{\mathbf{t}}_i) =$ true. By the pigeon hole principle, some region W_j contains at least $2^\lambda + 1$ of these pairs. Each such pair is a point in $\mathbb{Z}^\lambda$, so at least two of them must have coordinates equal mod 2 pairwise. Assume $(\mathbf{y}_1, \widetilde{\mathbf{t}}_1)$ and $(\mathbf{y}_2, \widetilde{\mathbf{t}}_2)$ are two such two pairs. By convexity, $(\mathbf{y}_1 + \mathbf{y}_2, \widetilde{\mathbf{t}}_1 + \widetilde{\mathbf{t}}_2)/2$ is another integer

[4] Separate variables $\mathbf{t}$ for different Φ_j must be concatenated into $\widetilde{\mathbf{t}}$.

point in W_j. Since Φ is always true over W_j, this pair also satisfies Φ. By (10.14), the point $\mathbf{y}_3 = (\mathbf{y}_1 + \mathbf{y}_2)/2$ also lies in Q'. We conclude that $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \in Q'$. □

Theorem 10.7. *The bound* (10.3) *as claimed by* KPT *does not hold in full generality. In other words, even for $k = 1$ and fixed m, n, the number of pieces r in the partition* (10.2) *must be at least* $\exp(\varepsilon\phi)$ *for some constant $\varepsilon = \varepsilon(m, n) > 0$.*

Proof. Assume (10.3) holds. Consider the following continued fraction of length $(2s + 1)$:

$$\alpha_s \ = \ [2;\ 1,\ \ldots,\ 1] \ = \ p/q,$$

where $p = F_{2s+3}$, $q = F_{2s+1}$ are the Fibonacci numbers. From Properties (G1)–(G6) in Section 3, we see that the lower convex curve $\mathcal{C}$ for α connects $s + 2$ integer points:

$$C_0 = (0, 1),\ C_1 = (2, 1),\ C_2 = (5, 2),\ \ldots,\ C_{s+1} = (p, q).^5$$

Here $C_i = (F_{2i+1}, F_{2i-1})$ for $1 \le i \le s + 1$. Let $\mathcal{C}'$ be the convex curve connecting $C_1, \ldots, C_{s+1}$ (see Figure 1). Property (G2), for every $1 \le i \le s$, the segment C_iC_{i+1} has exactly 2 integer points, C_i and C_{i+1}. In other words, we have $\mathcal{C}' \cap \mathbb{Z}^2 = \{C_1, \ldots, C_{s+1}\}$.

Let Q be the triangle defined in (5.1). By Lemma 4.1, an integer point $\mathbf{y} = (y_2, y_1) \in Q$ lies on $\mathcal{C}'$ if and only if $P_{\mathbf{y}}$ is integer point free, where $P_{\mathbf{y}}$ was defined in (4.4).[6] In other words, we have:

$$\begin{aligned} Q' \ &= \ \left\{ \mathbf{y} \in Q \cap \mathbb{Z}^2 \ : \ \begin{Bmatrix} py_1 - qy_2 & \ge & px_1 - qx_2 & \ge & 0 \\ y_2 - 1 & \ge & x_2 & \ge & 1 \end{Bmatrix} \text{ has no solutions } (x_2, x_1) \in \mathbb{Z}^2 \right\} \\ &= \ \mathcal{C}' \cap \mathbb{Z}^2. \end{aligned}$$

The above is a PIP problem with parameters $\mathbf{y} \in Q$ and variables $\mathbf{x} = (x_2, x_1) \in \mathbb{Z}^2$. Note that the system has fixed length $m = 4$. By Corollary 10.6, there exists a constant d, so that if $|\mathcal{C}' \cap \mathbb{Z}^2| = s + 1 > d$ then there are 3 distinct points $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \in \mathcal{C}' \cap \mathbb{Z}^2$ with $\mathbf{y}_3 = (\mathbf{y}_1 + \mathbf{y}_2)/2$. However, by the previous paragraph, the only integer points on $\mathcal{C}'$ are $C_1, \ldots, C_{s+1}$, which are in convex position, see Property (G4). Thus, none among them can be the midpoint of two others. We get a contradiction. Therefore, (10.3) cannot hold in general.

Recall the PIP problem (10.6) with a 1-dimensional parameter y', i.e., $k = 1$. From (10.3), we deduced $r \ll M$ in (10.8). This led to the observation that at least one interval I' must lie in a single piece J_i. The chain of deductions continued from there through Lemma 10.4 and Corollary 10.6 and led to the above contradiction. Therefore, we must have $r > M$, which implies $r \ge 2^{\varepsilon\phi}$ for some constant $\varepsilon = \varepsilon(m, n) > 0$. □

10.2. **Implications.** To summarize, Theorem 10.7 shows that a polynomial size decomposition into polyhedral pieces as in (10.2) does not exist. If one is willing to sacrifice the polyhedral structure of the pieces, then a polynomial size partition similar to (10.2) does in fact exist [ES08] (see also [Eis10]):

Theorem 10.8 (Eisenbrand and Shmonin)**.** *Fix n and k. Let $A\mathbf{x} \le \overline{b}$ be a* PIP *problem with a k-dimensional parameter space W. Then we can find in polynomial time a partition*

$$W \ = \ S_1 \sqcup S_2 \sqcup \ldots \sqcup S_r, \tag{10.15}$$

[5] Recall that the vertical coordinate is put in the first position.

[6] We take the first term in α to be 2 because of Remark 4.2

where each S_i is an integer projection *of another polyhedron $S'_i \subseteq \mathbb{R}^{m+\ell}$, defined as:*

$$S_i \;=\; \big\{\overline{b} \in \mathbb{R}^m \;:\; \exists \mathbf{t} \in \mathbb{Z}^\ell \;\; (\overline{b}, \mathbf{t}) \in S'_i\big\}.$$

Here $\ell = \ell(n)$ is a constant that depends only on n. All polyhedra S'_i can be found in polynomial time. The partition (10.15) *satisfies all other properties as claimed in* KPT.

Note that the integer projection of a polyhedron defined in the theorem is not necessarily a polyhedron as the following example shows.

Example 10.9. Consider the polytope $S' = \big\{(y_2, y_1) \in \mathbb{R}^2 \;:\; 0 \le y_2 \le 1,\; 0 \le y_1 - 3y_2 \le 2\big\}$. The integer projection of S' on the coordinate y_1 is $S = [0,2] \cup [3,4]$ (see Figure 9).

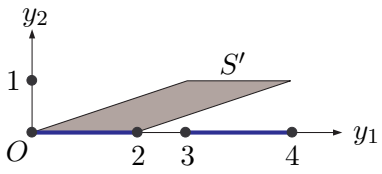

FIGURE 9. A polytope S' (shaded) and is integer projection (bold).

We emphasize that the proofs of Theorem 1.8 and Corollary 1.9 still hold if KPT is substituted by Theorem 10.8 (see [ES08]). Overall, the only discrepancy between KPT and Theorem 10.8 is about the structures of the pieces in the partition. This does not at all affect all known results about decision with 2 quantifiers or less. Worth mentioning is the polynomial time algorithm by Barvinok and Woods [BW03] on counting integer points in the integer projection of a polytope. This algorithm uses a weaker (valid) partitioning procedure also due to Kannan [Kan92, Lemma 3.1]. However, as we pointed out in Section 1.5, for 3 quantifiers or more, this structural discrepancy between KPT and Theorem 10.8 is of crucial importance.

11. Final remarks and open problems

11.1. Niels Bohr, the inventor of quantum theory, is quoted saying:

> "It is the hallmark of any deep truth that its negation is also a deep truth."

This roughly reflects our attitude towards KPT. A pioneer result at the time, it only slightly overstated the truth compared to the Eisenbrand–Shmonin theorem (Theorem 10.8). In fact, for many applications, including Kannan's Theorem 1.8 and Barvinok–Woods algorithm [BW03], Kannan's weaker result in [Kan92] is sufficient.

Let us emphasize that, of course, it would be natural to have a partition into convex (co-)polyhedra rather than general semilinear sets, since convex polyhedra are much easier to work with. The fact that it took nearly 30 years until KPT was disproved, shows both the delicacy and the technical difficulty of the issue.

11.2. The gap in the proof of KPT (Theorem 3.1 in [Kan90]) could be traced to the following lines:

> "... for each $(b, x) \in S_i$ (with $b \in P$, $x \in \mathbb{Z}^n$), there is a unique $y \in \mathbb{Z}^\ell$ so that (b, x, y) belongs to S'_i. In fact, each component of y is of the form $F'\lfloor Fx \rfloor$, where F', F are affine transformations. This is easily proved by induction on n, noting that (4.5) of [8], the z is in fact forced to be $\lfloor \alpha + 1 - \beta \rfloor$."

Here [8] refers to the conference proceedings version of paper [Kan92]. In equation (4.5) of [Kan92], variable z is in fact forced to be $\lfloor \alpha + 1 - \beta \rfloor$. However, the quantity α in (4.5) actually depends on b, which makes $\lfloor \alpha + 1 - \beta \rfloor$ a function of b instead of a constant. This implies that y in the above quoted paragraph could also depend on b. This technical error was perhaps due to the unclear notation α, which does not reflect its dependence on b, or due to the complicated cross referencing between [Kan90] and [Kan92].

11.3. There is a delicate difference between the treatment of (PIP) in Section 10.1 versus that in the integer programming literature (see e.g. [CL98, V+07, VW08]). In the latter, the parameter space W is also partitioned into convex polyhedra P_i, and over each P_i the number of solutions $\mathbf{x}$ is given by a quasi-polynomial $p_i(\overline{b})$ in $\overline{b}$. However, since there are no test sets, this does not allow us to solve (PIP) for *all* $\overline{b}$. In other words, even though a quasi-polynomial $p_i(\overline{b})$ is obtained, which evaluates to $|K_{\overline{b}} \cap \mathbb{Z}^n|$, there is no easy way to test whether $p_i(\overline{b}) \neq 0$ for all $\overline{b}$ within P_i. In general, we prove in [NP17b] that there are strong obstacles in using (short) generating functions to decide feasibility of Presburger sentences.

11.4. Now that we have Theorem 1.1, one can ask if the dimension 5 is tight. Observe that for three variables and three quantifiers, there is essentially a unique form of short Presburger sentence:

$$\exists z \ \forall y \ \exists x \ : \ \Phi(x, y, z).$$

Despite Theorem 1.10, KPT actually holds for a PIP problem $ax \leq f(y, z)$ with a single variable x, i.e., when $n = 1$. Therefore, this sentence can be decided by the approach in [NP17a]. The only remaining special case of (Short-PA_3) is

$$\exists z \ \forall y \ \exists \mathbf{x} \ : \ \Phi(\mathbf{x}, y, z), \quad \text{where } \mathbf{x} \in \mathbb{Z}^2.$$

It would be interesting to see if this case is also NP-complete.

Similarly, for sentences (GIP), one can ask if dimension 6 in Theorem 1.3 can be lowered. We believe it can be, at least for the counting part (cf. [NP17c]).

11.5. Motivated in part by the *Hilbert's tenth problem*, Manders and Adleman [MA] (see also [GJ79, §A7.2]) proved the following classical result: feasibility over $\mathbb{N}$ of

$$ax^2 + by = c$$

is NP-complete, given $a, b, c \in \mathbb{Z}$. One can view our Theorem 1.2 as a related result, where a single quadratic equation and two linear inequalities $x, y \geq 0$ (over $\mathbb{Z}$) are replaced with a system of 24 linear inequalities.

11.6. Minimizing polynomial functions over integer points in a convex polytope is an interesting problem of Integer Programming. Already for polynomials of degree 4 in two variables this is known to be NP-hard [DHKW06], but for lower degree polynomials some such problems can be solved in polynomial time [DHWZ16]. The survey paper [Kop12] contains extensive background on various related problems. Curiously, the following natural problem remains open:

Question 11.1. *Let n be fixed. Given a polytope $P \subset \mathbb{R}^n$ and a rational quadratic function $f : \mathbb{R}^n \to \mathbb{R}$, can the optimization problem $\min_{\mathbf{x}\in P\cap\mathbb{Z}^n} f(\mathbf{x})$ be solved in polynomial time?*

The case $n = 2$ was resolved positively in [DeW14]. Note that the case $n = 3$ with f homogeneous is known to have an FPTAS [HWZ17].

11.7. Our Theorem 1.7 strongly contrasts with the positive results in [DHK09], which require that all f_i's are linear. There, it is proved that optimizing over the Pareto minima can be done in polynomial time when g is linear. Furthermore, if g is non-linear then an FPTAS also exists. Here, we say that having even one f_i quadratic is enough to make the problem hard.

Note that in Theorem 1.7 we use three polynomial functions, two or which are linear. It would be interesting to see if just two polynomial functions suffice for the hardness.

Acknowledgements. We are greatly indebted to Sasha Barvinok for many fruitful discussions and encouragement. We are also grateful to Iskander Aliev, Matthias Aschenbrenner, Artëm Chernikov, Fritz Eisenbrand, Lenny Fukshansky, Robert Hildebrand, Ravi Kannan, Oleg Karpenkov, Matthias Köppe, Rafi Ostrovsky and Kevin Woods for interesting conversations and helpful remarks. Special thanks to Jesús De Loera for suggesting hardness of Pareto optima as a possible application of our main results. This work was finished while both authors were in residence of the MSRI long term Combinatorics program in the Fall of 2017; we thank MSRI for the hospitality. The first author was partially supported by the UCLA Dissertation Year Fellowship. The second author was partially supported by the NSF.

References

[AB] S. Arora and B. Barak, *Computational complexity. A modern approach*, Cambridge Univ. Press, Cambridge, UK, 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.

[Bar06] A. Barvinok, The complexity of generating functions for integer points in polyhedra and beyond, in *Proc. ICM*, Vol. 3, EMS, Zürich, 2006, 763–787.

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

[Bar17] A. Barvinok, Lattice points and lattice polytopes, to appear in *Handbook of Discrete and Computational Geometry* (third edition), CRC Press, Boca Raton, FL, 2017, 26 pp.

[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.

[CL98] P. Clauss and V. Loechner, Parametric analysis of polyhedral iteration spaces, *J. VLSI Signal Process.* **19** (1998), 179–194.

[Coo72] D. C. Cooper, Theorem proving in arithmetic without multiplication, in *Machine Intelligence* (B. Meltzer and D. Michie, eds.), Edinburgh Univ. Press, 1972, 91–99.

[DHK09] J. A. De Loera, R. Hemmecke, M. Köppe, Pareto optima of multicriteria integer linear programs, *INFORMS J. Comput.* **21** (2009), 39–48.

[DHKW06] J. A. De Loera, R. Hemmecke, M. Köppe and R. Weismantel, Integer Polynomial Optimization in Fixed Dimension, *Math. Oper. Research* **31** (2006), 147–153.

[DeW14] A. Del Pia and R. Weismantel, Integer quadratic programming in the plane, in *Proc. 25th SODA*, ACM, New York, 2014, 840–846.

[DHWZ16] A. Del Pia, R. Hildebrand, R. Weismantel and K. Zemmer, Minimizing cubic and homogeneous polynomials over integers in the plane, *Math. Oper. Res.* **41** (2016), 511–530.

[Eis03] F. Eisenbrand, Fast integer programming in fixed dimension, in *Proc. 11th ESA*, Springer, Berlin, 2003, 196–207.

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

[ES08] F. Eisenbrand and G. Shmonin, Parametric integer programming in fixed dimension, *Math. Oper. Res.* **33** (2008), 839–850.

[FR74] M. J. Fischer and M. O. Rabin, Super-Exponential Complexity of Presburger Arithmetic, in *Proc. SIAM-AMS Symposium in Applied Mathematics*, AMS, Providence, RI, 1974, 27–41.

[Für82] M. Fürer, The complexity of Presburger arithmetic with bounded quantifier alternation depth, *Theoret. Comput. Sci.* **18** (1982), 105–111.

[GJ79] M. R. Garey and D. S. Johnson, *Computers and intractability. A guide to the theory of NP-completeness*, Freeman, San Francisco, CA, 1979.

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

[HWZ17] R. Hildebrand, R. Weismantel and K. Zemmer, An FPTAS for minimizing indefinite quadratic forms over integers in polyhedra, in *Proc. 27th SODA*, ACM, New York, 2016, 1715–1723.

[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.

[Kar13] O. Karpenkov, *Geometry of continued fractions*, Springer, Heidelberg, 2013.

[Khi64] A. Ya. Khinchin, *Continued fractions*, Univ. of Chicago Press, Chicago, IL, 1964.

[Kop12] M. Köppe, On the complexity of nonlinear mixed-integer optimization, *Mixed integer nonlinear programming*, 533–557, IMA Vol. Math. Appl., 154, Springer, New York, 2012.

[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.

[MA] K. Manders and L. Adleman, NP-complete decision problems for binary quadratics, *J. Comput. System Sci.* **16** (1978), 168–184.

[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, *Proc. 49th STOC*, ACM, 2017; `arXiv:1704.00249`.

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

[NP17c] D. Nguyen and I. Pak, The computational complexity of integer programming with alternations, *Proc. 32nd CCC*, 2017; `arXiv:1702.08662`.

[Opp78] D. C. Oppen, A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic, *J. Comput. System Sci.* **16** (1978), 323–332.

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

[Pre29] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt (in German), in *Comptes Rendus du I congrès de Mathématiciens des Pays Slaves*, Warszawa, 1929, 92–101.

[RL78] C. R. Reddy and D. W. Loveland, Presburger arithmetic with bounded quantifier alternation, in *Proc. 10th STOC*, ACM, 1978, 320-325.

[Sca84] B. Scarpellini, Complexity of subcases of Presburger arithmetic, *Trans. AMS* **284** (1984), 203–218.

[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.

[SM73] L. J. Stockmeyer and A. R. Meyer, Word problems requiring exponential time: preliminary report, in *Proc. Fifth STOC*, ACM, New York, 1973, 1–9.

[V+07] S. Verdoolaege, R. Seghir, K. Beyls, V. Loechner and M. Bruynooghe, Counting integer points in parametric polytopes using Barvinok's rational functions, *Algorithmica* **48** (2007), 37–66.

[VW08] S. Verdoolaege and K. Woods, Counting with rational generating functions, *J. Symbolic Comput.* **43** (2008), 75–91.

[Wei97] V. D. Weispfenning, Complexity and uniformity of elimination in Presburger arithmetic, in *Proc. 1997 ISSAC*, ACM, New York, 1997, 48–53.

[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. Log.* **80** (2015), 433–449.

[Zie95] G. Ziegler, *Lectures on polytopes*, Springer, New York, 1995.