58th Annual IEEE Symposium on Foundations of Computer Science

Short Presburger Arithmetic is hard

Danny Nguyen
Department of Mathematics
University of California, Los Angeles
Los Angeles, California 90095
Email: ldnguyen@math.ucla.edu

Igor Pak
Department of Mathematics
University of California, Los Angeles
Los Angeles, California 90095
Email: pak@math.ucla.edu

***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 $\mathbf{\Sigma}_m^{\mathbf{P}}$-complete or $\mathbf{\Pi}_m^{\mathbf{P}}$-complete, when the first quantifier is $\exists$ or $\forall$, respectively. Counting versions and restricted systems are also analyzed.**

***Keywords*-Presburger arithmetic; computational complexity; completeness;**

I. INTRODUCTION

A. Outline of the results

We consider *short Presburger sentences*, defined as follows:

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

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

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

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 [5]. 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 $\mathbf{P}$, by Lenstra in 1982 and Kannan in 1990, respectively (Theorem 6). 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 [27]).

Our main result is a complete solution of the problem. We show that for a fixed $m \ge 3$, deciding (Short-PA$_m$) is $\mathbf{\Sigma}_{m-2}^{\mathbf{P}}$-complete (Theorem 5). This disproves[1] a conjecture by Woods [39, §5.3] (see also [40]), which claims that decision is in $\mathbf{P}$.

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

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

where Q and R are convex polyhedra given by $K\mathbf{y} \le \overline{u}$ and $L\mathbf{z} \le \overline{v}$, respectively. We also show that (GIP) is $\mathbf{NP}$-complete (Theorem 2). This resolves an open problem by Kannan [18].

Our reduction is parsimonious and also proves that the corresponding counting problem is $\#\mathbf{P}$-complete:

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

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.

B. 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. *Deciding* (Short-PA$_3$) *is* $\mathbf{NP}$*-complete, even for a short Presburger expression* Φ *of at most* 10 *inequalities*

[1] Assuming the polynomial hierarchy does not collapse.

0272-5428/17 $31.00 © 2017 IEEE
DOI 10.1109/FOCS.2017.13

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* $\#\mathbf{P}$*-complete.*

For systems of inequalities, we also get:

Theorem 2. *Deciding* (GIP) *is* $\mathbf{NP}$*-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* $\#\mathbf{P}$*-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 3. *Deciding* (GIP) *is* $\mathbf{NP}$*-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* $\#\mathbf{P}$*-complete.*

This substantially strengthens our earlier result [27], which considers (GIP) with a "long system", i.e., a system arbitrarily many inequalities:

Theorem 4 ([27])**.** *Deciding* (GIP) *is* $\mathbf{NP}$*-complete, for a system* $A\mathbf{x} + B\mathbf{y} + Cz \leq \overline{b}$ *of unbounded length in* 6 *variables* $z \in \mathbb{Z}$, $\mathbf{y} \in \mathbb{Z}^2$, $\mathbf{x} \in \mathbb{Z}^3$.

At the time of proving Theorem 4, we thought it would be the strongest negative result (see Section I-D below). Nevertheless, the new results in theorems 1, 2 and 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 can naturally be generalized to short Presburger sentences of more than 3 quantifiers:

Theorem 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 $\mathbf{\Sigma}_m^{\mathbf{P}}$*-complete. Similarly, when* $Q_1 = \forall$, *deciding short Presburger sentences as above is* $\mathbf{\Pi}_m^{\mathbf{P}}$*-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 $\mathbf{NP}$-compete by a result of Stockmeyer and Meyer [35]. 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. 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 2 and 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 11). Finally, we generalize the problem AP-COVER and the chain of reductions to $m \geq 3$ quantifiers.

C. Historical overview

Presburger Arithmetic was introduced by Presburger in [30], 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 [9], and was shown to be triply exponential by Oppen [28] (see also [31]). A nondeterministic doubly exponential complexity lower bound was obtained by Fischer and Rabin [13] for the general theory. This pioneering result was further refined to a triply exponential deterministic lower bound (with unary output) in [38], and a simply exponential nondeterministic lower bound for a bounded number of quantifier alternations [14] (see also [32]). Of course, in all these cases the number of variables is unbounded.

In [34], Schöning proved $\mathbf{NP}$-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 [16]. 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 $\mathbf{NP}$-complete. The examples include the KNAPSACK, one of the oldest $\mathbf{NP}$-complete problems [15]. Note also that even when matrix A has at most two nonzero entries in each row, the problem remains $\mathbf{NP}$-complete [21].

In a positive direction, the progress has been limited. The first breakthrough was made by Lenstra [22] (see also [33]), who showed that (IP) can be solved in polynomial time in a fixed dimension (see also [10] for better bounds). Combined with a reduction by Scarpellini [32], this implies that deciding (Short-PA$_1$) is in $\mathbf{P}$.

The next breakthrough was made by Kannan [17] (see also [18]), who showed that (PIP) in fixed dimensions is in $\mathbf{P}$, 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 4 from [27], which ruled out "long" systems for (GIP).

Theorem 6 (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 [12] (see §VIII-B). 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 [2] 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 [3], [6]). He utilized the *short generating function* approach pioneered by Brion, Vergne and others (see [4] for details and references). Woods [39] 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 [7]. Woods [39] extended this approach to general Presburger expressions Φ with a fixed number of inequalities (see also [40] and an alternative proof in [25]). As a consequence, he showed that deciding (Short-PA$_2$) is in $\mathbf{P}$. This represents the most general positive result in this direction:

Theorem 7 (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.

D. Kannan's Partition Theorem

In [17], Kannan introduced the technology of *test sets* for efficient solutions of (PIP). The *Kannan Partition Theorem* (KPT), see Theorem 12 below, claims that one can find in polynomial time a partition of the k-dimensional parameter space W into polynomially many rational (co-)polyhedra

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

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

In [25], 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 4 in [27], we thought that [25] and [27] together would completely characterize the complexity of (GIP), depending on whether the system is restricted or not.

In view of our theorems 1, 2, 3 and 5, it strongly suggests that KPT may actually be erroneous. However, we did not expect this at the time of writing [25]. In fact, the prevailing view was that (Short-PA$_m$) would always be in $\mathbf{P}$, which neatly aligned with the results in [25] (conditional upon KPT). Now that the hardness results are known, we are actually able combine the current techniques with some of those in [25] to obtain the following quantitative result, which strongly contradicts KPT:

Theorem 8. *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 VIII for more on KPT, §IX-A for our point of view, and §IX-B for the gap in the original proof of KPT.

II. 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 $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ for a disjunction $(a \vee b)$ and $\left\{\begin{smallmatrix} a \\ b \end{smallmatrix}\right\}$ 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.

III. 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 $\alpha = [a_0;\ a_1,\ \ldots,\ a_n - 1,\ 1]$, i.e.,:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{(a_n - 1) + \cfrac{1}{1}}}}.$$

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. [19], [20]), 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:

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

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

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 $\overrightarrow{C_iC_{i+1}} = a_i\overrightarrow{OD_i}$.

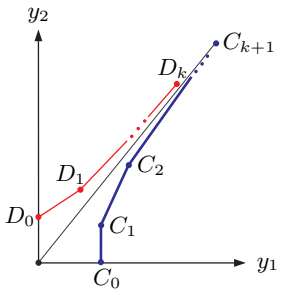

Figure 1. The curves $\mathcal{C}$ (bold) and $\mathcal{D}$.

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 $\overrightarrow{OC_{k+1}}$.

IV. From arithmetic progressions to short Presburger sentences

A. Covering with arithmetic progressions

For a triple $(g, h, e) \in \mathbb{N}^3$, denote by $\text{AP}(g, h, e)$ the arithmetic progression:

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

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 $z \notin \text{AP}_1 \cup \cdots \cup \text{AP}_k$, where $\text{AP}_i = \text{AP}(g_i, h_i, e_i)$?

The problem AP-COVER was shown to be **NP**-complete by Stockmeyer and Meyer. 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:

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

We have:

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

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

$$\gcd(M, g_i) = \gcd(M, g_i + h_i e_i) = 1,\ i = 1, \ldots, k. \quad (2)$$

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 (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 (2). 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_1C_2.

Observation: After these steps, we have h_1+1 integer points on C_1C_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 $\mathcal{A}_1 = \text{AP}_1$. 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 (2). 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_2C_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 (2).

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_3C_4. Reduced mod M, they give $\mathcal{A}_2 = \text{AP}_2$. 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 $\mathcal{A}_{j+1} = \text{AP}_{j+1}$. 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 (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.

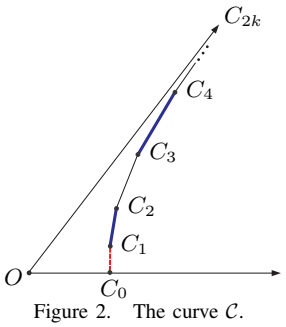

Figure 2. The curve $\mathcal{C}$.

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 $C_{2k} = (q_{2k}, p_{2k}) = (q, p)$.

B. Analysis of the construction

We define:

$$\Delta \;=\; \big\{z \;:\; \exists (y_1, y_2) \in \mathcal{C}' \quad z \equiv y_2 \pmod M\big\}. \tag{3}$$

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, $\ldots$, $C_{2k-1}C_{2k}$. Moreover, by condition (6), for $1 \le i \le k$ we have:

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

Therefore, we have:

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

Recall that AP-COVER asks whether:

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

By (3), 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:

$$\exists z \in J \;\; \forall \mathbf{y} \;\; z \not\equiv y_2 \pmod M \;\vee\; \mathbf{y} \notin \mathcal{C}'. \tag{4}$$

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.,

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

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.,

$$P_\mathbf{y} = \left\{\mathbf{x} \in \mathbb{R}^2 \;:\; \begin{matrix} \mathbf{v}\cdot\mathbf{y} \;\ge\; \mathbf{v}\cdot\mathbf{x} \;\ge\; 0 \\ y_2 \;>\; x_2 \;>\; 0 \end{matrix}\right\}. \tag{5}$$

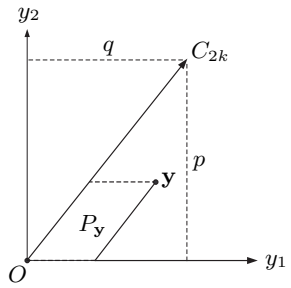

Figure 3. The parallelogram $P_\mathbf{y}$. The upper and lower edges of $P_\mathbf{y}$ are open (dotted). Here we denote $C_{2k} = (q_{2k}, p_{2k}) = (q, p)$.

Lemma 9. *For $\mathbf{y} \in \mathbb{Z}^2$, we have:*

$$\mathbf{y} \in \mathcal{C}' \;\Longleftrightarrow\; \mathbf{v}\cdot\mathbf{y} \ge 0 \;\wedge\; y_2 \ge g_1 \;\wedge\; P_\mathbf{y} \cap \mathbb{Z}^2 = \varnothing. \tag{6}$$

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 $y_2 \ge g_1$. Since $\mathcal{C}$ sits inside θ, we also have $\mathbf{y} \in \theta$, which implies $\mathbf{v}\cdot\mathbf{y} \ge 0$. 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 (5) contains no integer points. We conclude that $\mathbf{y}$ satisfies the RHS in (6).

Conversely, assume $\mathbf{y}$ satisfies the RHS in (6) but $\mathbf{y} \notin \mathcal{C}'$. The following argument is illustrated in Figure 4. First, $\mathbf{v}\cdot\mathbf{y} \ge 0 \wedge y_2 \ge g_1$ 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

[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}.

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 $(G6)$. ■

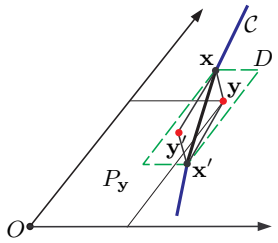

Figure 4. $\mathbf{y}'$ is the reflection of $\mathbf{y}$ across the midpoint of $\mathbf{x}\mathbf{x}'$.

Remark 10. 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.

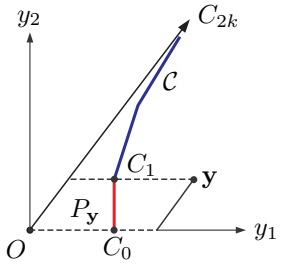

Figure 5. Here $g_1 = 1$, $\mathbf{y} \notin \mathcal{C}$, and yet $P_{\mathbf{y}}$ contains no integer points (dotted edges are open).

C. Proof of Theorem 1 (decision part)

Combining (4), (5) and (6), the negation of AP-COVER is equivalent to:

$$\exists z \in J \quad \forall \mathbf{y} \quad \left[z \not\equiv y_2 \pmod{M} \ \vee \ \mathbf{v}\cdot\mathbf{y} < 0 \right. \\ \left. \vee \ y_2 < g_1 \ \vee \ \exists \mathbf{x} \begin{Bmatrix} \mathbf{v}\cdot\mathbf{y} \geq \mathbf{v}\cdot\mathbf{x} \geq 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{Bmatrix} \right]. \tag{7}$$

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 (7) in prenex normal form:

$$\exists z \ \forall \mathbf{y} \ \exists \mathbf{x} \ \ \mu \leq z \leq \nu \ \wedge \ \left[0 < z - y_2 - Mx_1 < M \right. \\ \left. \vee \ \mathbf{v}\cdot\mathbf{y} < 0 \ \vee \ y_2 < g_1 \ \vee \ \begin{Bmatrix} \mathbf{v}\cdot\mathbf{y} \geq \mathbf{v}\cdot\mathbf{x} \geq 0 \\ y_2 \ > \ x_2 \ > \ 0 \end{Bmatrix} \right]. \tag{8}$$

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 (8). This shows that (8) is **NP**-hard, and so is (Short-PA_3). For **NP**-completeness, by Theorem 3.8 in [16], 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 7, 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. □

V. Proof of Theorems 2 and 3 (decision part)

We will recast (8) into the form (GIP). For the polytopes R and Q in (GIP), let $R = J = [\mu, \nu]$ and

$$Q = \left\{ \mathbf{y} \in \mathbb{R}^2 \ : \ y_2 \geq g_1, \ y_1 \leq q, \ \mathbf{v}\cdot\mathbf{y} \geq 0 \right\}, \tag{9}$$

see Figure 6.

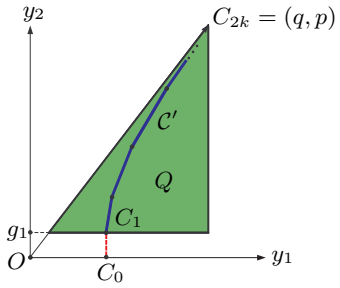

Figure 6. The triangle Q (shaded).

Since $R \supset \mathcal{C}'$, (4) 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 (6), for $\mathbf{y} \in Q$, we have

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

Thus, the sentence (8) is equivalent to:

$$\exists z \in R \quad \forall \mathbf{y} \in Q \quad \exists \mathbf{x} \\ 0 < z - y_2 - Mx_1 < M \quad \vee \quad \mathbf{x} \in P_{\mathbf{y}}. \tag{10}$$

The remaining step is to covert the expression

$$1 \le z - y_2 - Mx_1 \le M-1 \ \vee \ \begin{Bmatrix} \mathbf{v}\cdot\mathbf{y} \ge \mathbf{v}\cdot\mathbf{x} \ge 0 \\ y_2 - 1 \ge x_2 \ge 1 \end{Bmatrix} \quad (11)$$

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 (11) if and only if there exists such an $\mathbf{x}$ within some bounded range. Indeed, both R and Q are bounded, and (11) imply boundedness for $\mathbf{x}$. Therefore, we can take an N large enough so that

$$-N \le z,\, y_1,\, y_2,\, x_1,\, x_2 \le N. \quad (12)$$

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

Now we convert (11) into a single system. This can be done in two slightly different ways, leading to theorems 2 and 3.

A. Proof of Theorem 2 (decision part)

Applying the distributive law on (11), we get an equivalent expression:

$$\begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M-1 \\ \mathbf{v}\cdot\mathbf{x} \le \mathbf{v}\cdot\mathbf{y} \end{bmatrix} \ \wedge \ \begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M-1 \\ 0 \le \mathbf{v}\cdot\mathbf{x} \end{bmatrix} \ \wedge \ \dots \quad (13)$$

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 (13). By the bounds (12), it is equivalent to:

$$\begin{bmatrix} 1 \le z - y_2 - Mx_1 \le M-1 \\ 0 \le \mathbf{v}\cdot\mathbf{y} - \mathbf{v}\cdot\mathbf{x} \le 2N(p+q) \end{bmatrix}. \quad (14)$$

Let $t_1 = z - y_2 - Mx_1$ and $t_2 = \mathbf{v}\cdot\mathbf{y} - \mathbf{v}\cdot\mathbf{x}$. By (12), we always have

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

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

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

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

Then (14) can be rewritten as:

$$(t_1, t_2) \ \in \ P_1 \ \cup \ P_2\,. \quad (15)$$

Next, define:

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

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:

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

From this, we have:

$$(t_1, t_2) \ \in \ P_1 \ \cup \ P_2 \iff \exists t_3 \ : \ (t_1, t_2, t_3) \ \in \ P. \quad (16)$$

Combined with (15), it implies that (14) 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 (13), we get four new variables $\mathbf{t} \in \mathbb{Z}^4$ and a combined system of 24 inequalities. Thus, the original disjunction (11) 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 (10), we obtain the decision part of Theorem 2. □

B. Proof of Theorem 3 (decision part)

Another way to convert (11) into a system is to directly interpret its two clauses and two separate polytopes. The same bounds (12) 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 [41]).

Theorem 11 (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:

$$\big\{ (x_1, y_2, z) \ : \ 1 \le z - y_2 - Mx_1 \le M-1, \\ -N \le x_1, y_2, z \le N \big\}.$$

This is a 3-dimensional polytope with 8 facets. Applying Theorem 11, 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:

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

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 (16) 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 11, 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 (11) is equivalent to a system:

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

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 (10), we obtain the decision part of Theorem 3. $\square$

VI. Proof of theorems 1, 2 and 3 (counting part)

Notice that the above reduction from AP-COVER to (8) is parsimonious, i.e., z lies in $J \setminus (\mathrm{AP}_1 \cup \cdots \cup \mathrm{AP}_k)$ if and only if $\mu \leq z \leq \nu$ and

$$\forall \mathbf{y} \quad \exists \mathbf{x} \quad \left[0 < z - y_2 - Mx_1 < M \ \vee \ \mathbf{v} \cdot \mathbf{y} < 0 \right. \\ \left. \vee \ y_2 < g_1 \ \vee \left\{ \begin{matrix} \mathbf{v} \cdot \mathbf{y} \geq \mathbf{v} \cdot \mathbf{x} \geq 0 \\ y_2 > x_2 > 0 \end{matrix} \right\} \right]. \tag{17}$$

At the same time, the reduction from 3SAT to AP-COVER given in [35]. Since #3SAT is $\#\mathbf{P}$-complete (see e.g. [1], [24], [29]), so is counting the number of z satisfying (17). This proves the second part of Theorem 1.

The counting parts of theorems 2 and 3 can be proved with a similar argument to Section V. $\square$

VII. Proof of Theorem 5

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

m-AP-COVER

Input: The following elements:
- m intervals $J_1 = [\mu_1, \nu_1], \ldots, J_m = [\mu_m, \nu_m]$,
- k_1 triples (g_{1i}, h_{1i}, e_{1i}), with $1 \leq i \leq k_1$,
- $\ldots$
- k_m triples (g_{mi}, h_{mi}, e_{mi}), with $1 \leq i \leq k_m$,
- 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:

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

where

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

By a similar argument to [35], it is not hard to show that m-AP-COVER is $\mathbf{\Sigma}_m^{\mathbf{P}}/\mathbf{\Pi}_m^{\mathbf{P}}$-complete, depending on the parity of m. We prove Theorem 5 by reducing m-AP-COVER to short Presburger arithmetic. Theorem 1 is the special case when $m = 1$ ($\mathbf{\Sigma}_1^{\mathbf{P}} \equiv \mathbf{NP}$). For simplicity, we show the reduction for the case $m = 2$. The same argument works for $m > 2$.

Consider 2-AP-COVER, which is $\mathbf{\Pi}_2^{\mathbf{P}}$-complete. We can rewrite 2-AP-COVER as:

$$\forall z_2 \in J_2 \quad \big[z_2 \in \Delta_2 \ \vee \\ \vee \ \ \exists z_1 \in J_1 \ \ \tau_1 z_1 + \tau_2 z_2 \notin \Delta_1 \big]. \tag{18}$$

Replacing z with $\tau_1 z_1 + \tau_2 z_2$ in (17), 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, (18) is equivalent to:

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

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 $\mathbf{w}$).

The same reduction works for $m > 2$. We omit the details. □

VIII. On Kannan's Partition Theorem (KPT)

A. 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:

$$\forall\, \overline{b} \in W \quad \exists \mathbf{x} \in \mathbb{Z}^n \;\; : \;\; A\mathbf{x} \leq \overline{b}. \tag{19}$$

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 [17, Theorem 3.1], Kannan claimed the following result, which implies a polynomial time algorithm to decide (19). From here on, we use RA to denote *rational affine transformations*. Also let $K_{\overline{b}} := \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leq \overline{b}\}$ for every $\overline{b} \in W$.

Theorem 12 (Kannan's Partition Theorem)**.** *Fix n and k. Given a* PIP *problem, we can find in polynomial time a partition*

$$W = P_1 \sqcup P_2 \sqcup \cdots \sqcup P_r, \tag{20}$$

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).

As mentioned in Section I-D, combining the current techniques with those in [25], we obtained Theorem 8. This strongly contradicts KPT, even for the case $k = 1$ ($\overline{b}$ is 1-dimensional). The proof of Theorem 8 is omitted here due to its length. It can be found in full journal version of the paper.

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

B. Implications

To summarize, Theorem 8 shows that a polynomial size decomposition into polyhedral pieces as in (20) does not exist. If one is willing to sacrifice the polyhedral structure of the pieces, then a polynomial size partition similar to (20) does in fact exist [12] (see also [11]):

Theorem 13 (Eisenbrand and Shmonin)**.** *Fix n and k. Let $A\mathbf{x} \leq \overline{b}$ be a* PIP *problem with a k-dimensional parameter space W. Then we can find in polynomial time a partition*

$$W = S_1 \sqcup S_2 \sqcup \cdots \sqcup S_r, \tag{21}$$

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

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

Here $\ell = \ell(n)$ is a constant that depends only on n. All polyhedra S'_i can be found in polynomial time. The partition (21) *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 14. Consider the polytope $S' = \left\{(y_1, y_2) \in \mathbb{R}^2 \;:\; 0 \leq y_2 \leq 1,\; 0 \leq y_1 - 3y_2 \leq 2\right\}$. The integer projection of S' on the coordinate y_1 is $S = [0, 2] \cup [3, 4]$ (see Figure 7).

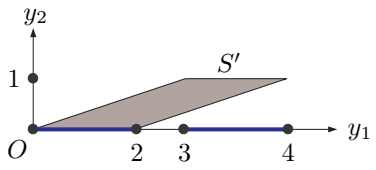

Figure 7. A polytope S' (shaded) and is integer projection (bold).

We emphasize that the proofs of theorems 6 and 7 still hold if KPT is substituted by Theorem 13 (see [12]). Overall, the only discrepancy between KPT and Theorem 13 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 [7] on counting integer points in the integer projection of a single polytope. This algorithm uses a weaker (valid) partitioning procedure also due to Kannan [18, Lemma 3.1]. However, as we pointed out in Section I-D, for three quantifiers or more, this structural discrepancy between KPT and Theorem 13 is of crucial importance.

IX. Final remarks and open problems

A. 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 13). In fact, for many applications, including Kannan's Theorem 6 and Barvinok–Woods algorithm [7], Kannan's weaker result in [18] 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.

B. The gap in the proof of KPT (Theorem 3.1 in [17]) 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 [18]. In equation (4.5) of [18], 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 [17] and [18].

C. There is a delicate difference between the treatment of (PIP) in Section VIII-A versus that in the integer programming literature (see e.g. [8], [36], [37]). 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 [26] that there are strong obstacles in using (short) generating functions to decide feasibility of Presburger sentences.

D. Now that we have Theorem 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 8, KPT actually holds for a PIP problem $ax \le f(y,z)$ with a single variable x, i.e., when $n = 1$. Therefore, this sentence can be decided by the approach in [25]. 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 3 can be lowered. We believe it can be, at least for the counting part (cf. [27]).

E. Motivated in part by the *Hilbert's tenth problem*, Manders and Adleman [23] (see also [15, §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 2 as a related result, where a single quadratic equation and two linear inequalities $x, y \ge 0$ (over $\mathbb{Z}$) are replaced with a system of 24 linear inequalities.

Acknowledgment

We are greatly indebted to Sasha Barvinok for many fruitful discussions and encouragement. We are also thankful to Iskander Aliev, Matthias Aschenbrenner, Artëm Chernikov, Jesús De Loera, Fritz Eisenbrand, Lenny Fukshansky, Oleg Karpenkov, Rafi Ostrovsky and Kevin Woods for interesting conversations and helpful remarks. The second author was partially supported by the NSF.

References

[1] S. Arora and B. Barak, *Computational complexity. A modern approach*, Cambridge Univ. Press, Cambridge, UK, 2009.

[2] 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.

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

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

[5] 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.

[6] 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.

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

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

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

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

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

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

[13] 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.

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

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

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

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

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

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

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

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

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

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

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

[25] D. Nguyen and I. Pak, Complexity of short Presburger arithmetic, *Proc. 49th STOC*, ACM, 2017; `arXiv:1704.00249`.

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

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

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

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

[30] 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.

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

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

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

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

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

[36] 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.

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

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

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

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

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