COMPLEXITY OF SHORT PRESBURGER ARITHMETIC

DANNY NGUYEN[⋆] AND IGOR PAK[⋆]

Abstract. We study 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 integers involved in the inequalities. We prove that assuming Kannan's partition can be found in polynomial time, the satisfiability of Short-PA sentences can be decided in polynomial time. Furthermore, under the same assumption, we show that the numbers of satisfying assignments of short Presburger sentences can also be computed in polynomial time.

1. Introduction

1.1. The results. We consider *short Presburger sentences* defined as follows:

$$(*) \qquad \exists \mathbf{x}_1\, \forall \mathbf{x}_2\, \exists \mathbf{x}_3\, \ldots\, \forall/\exists \mathbf{x}_k \,:\, \Phi\big(\mathbf{x}_1, \ldots, \mathbf{x}_k\big),$$

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

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

In other words, everything is fixed in $(*)$ except for the entries of the matrices A_i and of the vectors $\overline{b}$ in $(**)$.

Let Short-PA be the satisfiability problem of sentences $(*)$. This is one of the few remaining gaps in complexity of the first order logic problems. If any of the conditions are weakened (unbounded quantifiers, variables, or linear systems), the problem becomes NP-complete or even super-exponential (see below).

The Short-PA generalizes *Integer Linear Programming* in fixed dimension (cf. §4.1), which can be viewed as satisfiability of sentences

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

with $\mathbf{x} \in \mathbb{Z}^n$ for a fixed n. Satisfiability of $(\circ)$ in polynomial time is due to Lenstra [Len83]. Its proof relies on difficult results in geometry of numbers (see the discussion below).

Similarly, Short-PA generalizes *Parametric Integer Linear Programming* in fixed dimension (cf. §4.1), which can be viewed as satisfiability of sentences

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

with $\mathbf{x} \in \mathbb{Z}^n$ and $\mathbf{y} \in \mathbb{Z}^m$ for fixed n and m. Here Q is another rational polyhedron, described by another system $C\mathbf{y} \le \overline{d}$.

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

March 30, 2017.

Satisfiability of ($\circ\circ$) in polynomial time is due to Kannan [Kan90] (Theorem 3.9). His proof crucially relies on *Kannan's partition theorem* (KPT) (Theorem 3.7), which is somewhat technical and can be described as follows. KPT says that there is a partitioning of $\mathbb{Z}^m$ into a polynomially many polyhedral regions P_i, $1 \le i \le r$, such that in order to solve for an $\mathbf{x} \in \mathbb{Z}^n$ satisfying $A\mathbf{x} \le \bar{b}$ with $\bar{b}$ changing, one only need to preprocess the matrix A in polynomial time, and from there get the regions P_i. Then, when queried with $\bar{b} \in P_i$, one only need to check for a finite number (n^{4n}) of candidate solutions $\mathbf{x} \in \mathbb{Z}^n$, which are called *test points*.

In this paper we repeatedly use KPT as a black box, to prove the following general result:

Theorem A. *Assuming KPT, problem* Short-PA *is in* P.

The proof of our Theorem A uses quantifier elimination inductively, with each inductive step applying KPT in the case $m = 1$.

Let us emphasize that even the following special case of ($*$) remained wide open:

$$(\circ\circ\circ) \qquad \exists \mathbf{z} \in R \;\; \forall \mathbf{y} \in Q \;\; \exists \mathbf{x} \, : \, A\mathbf{x} \, + \, B\mathbf{y} \, + \, C\mathbf{z} \, \le \, \bar{b}.$$

This case was singled out by Kannan in [Kan92] as the next challenge.

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

Note that in the above three problems, the restriction in each quantifier can be pushed inward at the cost of introducing extra Boolean operators. For example:

$$\forall \mathbf{y} \in Q \;\; \exists \mathbf{x} \, : \, A\mathbf{x} \, + \, B\mathbf{y} \, \le \, \bar{b} \quad \iff \quad \forall \mathbf{y} \, \exists \mathbf{x} \, : \, (\mathbf{y} \notin Q) \vee (A\mathbf{x} \, + \, B\mathbf{y} \, \le \, \bar{b}).$$

Our next result is a counting analogue of Theorem A. By analogy with ($*$), define a *short Presburger formula* as a set of the form:

$$(*') \qquad \big\{ \mathbf{x}_1 \, : \, \exists \mathbf{x}_2 \, \forall \mathbf{x}_3 \, \ldots \, \exists/\forall \mathbf{x}_k \;\; \Phi\big(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\big) \big\},$$

where the dimensions and the Boolean combinations are fixed as in ($*$). Let #Short-PA be the counting problem of the number of satisfying assignments $\mathbf{x}_1$ of a short Presburger formula ($*'$). The complexity of #Short-PA was stated as an open problem by Barvinok [Bar06, §5], and as a conjecture by Woods [Woo04] (see also [Woo15]).

Theorem B. *Assuming KPT, the counting problem* #Short-PA *is in* FP.

This is an extension of Theorem A, as counting easily implies decision. Following an example above, a special case of Theorem B computes the number of integer points defined in ($\circ\circ\circ$). The proof of Theorem B is inductive and again uses KPT for reduction of the number of quantifiers. We use the Barvinok–Woods theorem (Theorem 3.12) as a base of induction.

1.2. **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 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 proves NP-completeness for two quantifiers $\exists x \forall y : \Phi(x,y)$, where $x, y \in \mathbb{Z}$ and $\Phi(x,y)$ is a quantifier-free Presburger expression. Here the expression $\Phi(x,y)$ has an unbounded number of inequalities and Boolean combinations. This improved on an earlier result by [Grä87], who also established that similar sentences with $k+1$ quantifier alternations and a bounded number of variables are complete for the k-th level in the Polynomial Hierarchy.

In a positive direction, the progress has been slow. The first breakthrough was made by Lenstra [Len83] (see also [Sch86]), who showed that the *integer feasibility problem* ($\circ$) can be solved in polynomial time in a fixed dimension (see also [Eis03, FT87] for better bounds). The next breakthrough was made by Kannan [Kan90] (see also [Kan92]), who showed how to solve *parametric integer linear programs* ($\circ\circ$) in fixed dimensions. This result was further strengthened in [ES08] (see also [Eis10]). All of these greatly contrast with the hardness results from [Sch97] and [Grä87], because here only conjunctions of inequalities are allowed.

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 d. He utilized the *short generating function* approach pioneered by Brion, Vergne and others (see [Bar08] for details and references). Barvinok and Pommersheim [BP99] extend this approach to prove that integers points in a Boolean combination of polytopes can also be counted in polynomial time. This is in contrast with [EH12], which proves that minimizing the number of integer points $\mathbf{x}$ satisfying ($\circ$) over different $\bar{b}$ is NP-hard. Barvinok and Woods showed how to count integer points in projections of (single) polytopes in polynomial time [BW03]. Woods [Woo15] also showed that Presburger formulas can be characterized by having rational generating functions (see also [Woo04]). Theorem B can be viewed as algorithmic version of this result, when the formula is short.

Barvinok's algorithm has been simplified and improved in [DK97, KV08]; it was also extended to various integral sums and valuations over convex polyhedra [B+12, Bar08, BV07]. The algorithm has important applications in a number of areas, ranging from polynomial optimization [D+06a, D+06b] to representation theory [CDW12, PP15], to commutative algebra [D+04, MS05] and to random sampling [Pak02]. Both Barvinok's and Barvinok–Woods' algorithms have been implemented and used for practical computation [DHTY04, Köp07, V+07].

1.3. **Proof features and previous obstacles.** The proofs of theorems A and B have some unusual features when compared to other recent work in the area. First, we use a quantifier elimination technique in the classical style of the formal arithmetic theory. However, we treat Boolean formulas geometrically, in the style of Barvinok et al., to allow the applications of KPT. Let us emphasize that having Boolean formulas is crucial for our proof – without them the inductive argument crumbles, even for sentences like ($\infty\!\infty$) above. We refer to §4.1 for a related phenomenon.

Second, the proof of Theorem B crucially relies on the technology of *short generating functions* (GF)

$$(\circledast) \qquad f(\mathbf{t}) \,=\, \sum_{i=1}^{N} \frac{c_i\, \mathbf{t}^{\overline{a}_i}}{(1-\mathbf{t}^{\overline{b}_{i1}})\cdots(1-\mathbf{t}^{\overline{b}_{ik_i}})},$$

where $c_i \in \mathbb{Q}$, $\overline{a}_i, \overline{b}_{ij} \in \mathbb{Z}^n$ and $\mathbf{t}^{\overline{a}}$ denotes $t_1^{a_1}\cdots t_n^{a_n}$ for $\overline{a} = (a_1,\ldots,a_n) \in \mathbb{Z}^n$. We caution the reader that word "short" in "short GF" only means that the GF is given in the form ($\circledast$).

It does not necessarily mean the GF has polynomial size. As we mentioned earlier, short GFs are a wonderful tool which allows one to take finite unions, intersections, complements and substitutions. Unfortunately, there is no easy way to take projections on the level of short GFs; the hardness result was recently proved in [Woo15] (see also [NP17c]).

The reader can be understandably confused at this point since the ability to take projections is exactly the statement of the Barvinok–Woods theorem. The problem is quite delicate here: having switched from polytopes to short GFs, the Barvinok–Woods technique cannot be iterated. Here is a simple way to think about it. The Barvinok–Woods theorem allows one to efficiently compute short GFs for projections of (single) polytopes $P_1, \ldots, P_r$ in polynomial time. Call these projections $\operatorname{proj}(P_1), \ldots, \operatorname{proj}(P_r)$. Earlier tools by Barvinok and Pommersheim also allow one to compute a short GF for the union $Y = \operatorname{proj}(P_1) \cup \ldots \cup \operatorname{proj}(P_r)$ when r is bounded. However, now that the polytopal structure is lost, there is no easy way to compute in polynomial time another projection of Y when we are given only a short GF for Y. In fact, we recently prove that this is computationally hard in [NP17c].

2. Notations

We use $\mathbb{N} = \{0, 1, 2, \ldots\}$.
Unspecified quantifiers are denoted by Q_1, Q_2, etc.
Unbounded (unrestricted) quantifiers are denoted $\forall$ and $\exists$.
Bounded (restricted) quantifiers are denoted $\forall^{\mathrm{b}}$ and $\exists^{\mathrm{b}}$.
Unquantified Presburger expressions are denoted by Φ, Ψ, Γ, etc.
We use Λ to denote a linear system.
We use $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ to denote a disjunction $(a \vee b)$ and $\left\{\begin{smallmatrix} a \\ b \end{smallmatrix}\right\}$ to denote 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.
The L_1 norm of a vector $\overline{n}$ is denoted by $|\overline{n}|$.
All matrices are denoted A, B, etc.
All integer variables are denoted x, y, z, etc.
All vectors of integer variables are denoted $\mathbf{x}, \mathbf{y}, \mathbf{z}$, etc.
If $x_j \leq y_j$ for every index j in vectors $\mathbf{x}$ and $\mathbf{y}$, we write $\mathbf{x} \leq \mathbf{y}$.
If $x_j \leq c$ for every index j with c a constant, we write $\mathbf{x} \leq c$.
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 $\mathbf{y} = \lfloor \mathbf{x} \rfloor$.
GF is an abbreviation for "*generating function*".
Single-variable GFs are denoted by $f(t), g(u), h(v)$, etc.
Multi-variable GFs are denoted by $A(\mathbf{t}), B(\mathbf{u}), a(\mathbf{v})$, etc.
The function $\phi(\cdot)$ denotes the (binary) length of a formula, GF, matrix, vector, etc.
Half-open intervals are denoted by $[\alpha, \beta)$, etc.
A *polyhedron* is an intersection of finitely many closed half-spaces in some euclidean space $\mathbb{R}^n$.
A *copolyhedron* is a polyhedron with possibly some open facets.
A *polytope* is a bounded polyhedron.

3. Short Presburger sentences

3.1. **Deciding short Presburger sentences.** We consider a fixed class of short Presburger sentences in prenex normal form

$$\mathcal{P}_{k,\overline{n},a} = \Big\{ S = \big[Q_1\mathbf{x}_1 \; Q_2\mathbf{x}_2 \; \ldots \exists\mathbf{x}_k \, : \, \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k) \big] \Big\}. \tag{3.1}$$

Here $Q_1, \ldots, Q_k \in \{\forall, \exists\}$ are k alternating quantifiers with $Q_k = \exists$, each $\mathbf{x}_i \in \mathbb{Z}^{n_i}$ with fixed dimensions $\overline{n} = (n_1, \ldots, n_k)$, and Φ is a Boolean combination of at most a rational inequalities in $\mathbf{x}_i$'s. We can also assume each $\mathbf{x}_i \geq 0$, because every integer variable can be represented as the difference between 2 nonnegative variables, and doing so only increases each n_i by a factor of 2. For a sentence $S \in \mathcal{P}_{k,\overline{n},a}$, we denote by $\phi(S)$ the binary length of S. Now Theorem A can be restated as follows:

Theorem 3.1. *Assuming KPT, every $S \in \mathcal{P}_{k,\overline{n},a}$ can be decided in polynomial time with respect to $\phi(S)$. The polynomial degree depends only on $k, \overline{n}$ and a. In other words, $\mathcal{P}_{k,\overline{n},a} \in$ P for every $k, \overline{n}, a$.*

As we mentioned in the introduction, from Kannan's Theorem 3.2 in [Kan90], every such class $\mathcal{P}_{k,\overline{n},a}$ with $k = 2$ can be decided in polynomial time with respect to $\phi(S)$, with the polynomial degree depending on $\overline{n}$ and a. In the literature, the case $k = 2$ is called Parametric Integer Linear Programming, because every such problem has the form $\forall\mathbf{y} \; \exists\mathbf{x} : \Phi(\mathbf{y}, \mathbf{x})$, where $\mathbf{y}$ varies over the parameter space $\mathbb{Z}^{n_1}$, and for each such $\mathbf{y}$ we need to solve an Integer Linear Programming problem for $\mathbf{x} \in \mathbb{Z}^{n_2}$.

Proposition 3.2. *$\mathcal{P}_{k,\overline{n},a} \in \Sigma^{\mathsf{P}}_{k-2}$ if k is odd and $\mathcal{P}_{k,\overline{n},a} \in \Pi^{\mathsf{P}}_{k-2}$ if k is even.*

Proof of Proposition 3.2. From a general result in [Grä87], we know $\mathcal{P}_{k,\overline{n},a} \in \Sigma^{\mathsf{P}}_{k}/\Pi^{\mathsf{P}}_{k}$ when k is odd/even because there are only a bounded number of quantified variables. In other words, this says that for every $S \in \mathcal{P}_{k,\overline{n},a}$, it suffices to verify S for all $\mathbf{x}_i$ with coordinates $x_{i,j}$ less than 2^{ℓ_i}. Here $\ell_1, \ldots, \ell_k$ are polynomial in $\phi(S)$ and can also be computed in polynomial time from S. Furthermore, given $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-2})$, Theorem 3.9 allows us to check whether $\forall\mathbf{x}_{k-1}\exists\mathbf{x}_k : \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ in polynomial time. Therefore, we get $\mathcal{P}_{k,\overline{n},a} \in \Sigma^{\mathsf{P}}_{k-2}/\Pi^{\mathsf{P}}_{k-2}$ if k is odd/even. □

By the above proposition, to decide a statement $S \in \mathcal{P}_{k,\overline{n},a}$, it is enough restrict the coordinates x_{ij} in $\mathbf{x}_i$ to an interval $[0, 2^{\ell_i})$. Here $\ell_1, \ldots, \ell_k$ are polynomial in $\phi(S)$ and also computable in polynomial time given S. We can change each quantifier $Q_i\mathbf{x}_i$ to $Q_i^{\mathrm{b}}\mathbf{x}_i$, where the superscript "b" means that $\forall/\exists\mathbf{x}_i \in [0, 2^{\ell_i})^{n_i}$. Thus, we can recast each class $\mathcal{P}_{k,\overline{n},a}$ as consisting of polynomial size search problems:

$$\mathcal{P}^{\mathrm{b}}_{k,\overline{n},a} = \Big\{ S = \big[Q_1^{\mathrm{b}}\mathbf{x}_1 \; Q_2^{\mathrm{b}}\mathbf{x}_2 \; \ldots \; \exists^{\mathrm{b}}\mathbf{x}_k \, : \, \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k) \big] \Big\}. \tag{3.2}$$

Lemma 3.3. *For a sentence $S \in \mathcal{P}^{\mathrm{b}}_{k,\overline{n},a}$ as in* (3.2)*, we can convert Φ to a short system* (*conjunction*) *of inequalities at the cost of increasing the length $\phi(S)$ by a polynomial factor, and increasing n_k and a by some constants.*

Proof. First let $n = n_1 + \ldots + n_k$ and $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathbb{Z}^n$, we can rewrite $\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ as a DNF:

$$\Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k) = (A_1\mathbf{x} \leq \overline{b}_1) \vee \cdots \vee (A_t\mathbf{x} \leq \overline{b}_t). \tag{3.3}$$

Here each short system $A_j\mathbf{x} \leq \overline{b}_j$ contains at most a inequalities and defines a polytope $P_j \subset \mathbb{R}^n$ (because each $\mathbf{x}_i$ is bounded). The the total number t of such systems is also at most 2^a. So Φ defines a union of t polytopes (intersecting $\mathbb{Z}^n$). We claim that there exists a polytope $R \subset \mathbb{R}^m$ with $m = t + n$ so that for every $\mathbf{x} \in \mathbb{Z}^n$, we have:

$$\mathbf{x} \in \bigcup_{i=1}^{t} P_j \qquad \Longleftrightarrow \qquad \exists \mathbf{t} \in \mathbb{Z}^t : (\mathbf{t}, \mathbf{x}) \in R. \tag{3.4}$$

To see this, we first define

$$R_j = (0, \ldots, 0, 1_j, 0, \ldots, 0, P_j) \subset \mathbb{R}^m.$$

Explicitly, each R_j is P_j augmented with $t-1$ coordinates 0, and a coordinate 1 in the j-th position. Now we can define

$$R = \operatorname{conv}\{R_1, R_2, \ldots, R_t\}. \tag{3.5}$$

It is easy to see that every integer point $(\mathbf{t}, \mathbf{x})$ in R must be in some R_j, and vice versa. This establishes (3.4).

The vertices of each P_j can be computed in polynomial time from its facets. The vertices of R_j come directly from those of P_j. The vertices of R are all vertices of R_j for $1 \le j \le t$. The facets of R can be computed in polynomial time from its vertices because the total dimension $m = n + t$ is bounded. So the polytope R can be presented as

$$A(\mathbf{t}, \mathbf{x}) \le \overline{b}$$

with both A and $\overline{b}$ computable in polynomial time. The original sentence S can now be written in an equivalent form:

$$Q_1^{\mathrm{b}} \mathbf{x}_1 \; Q_2^{\mathrm{b}} \mathbf{x}_2 \; \ldots \; \forall^{\mathrm{b}} \mathbf{x}_{k-1} \; \exists^{\mathrm{b}} \widetilde{\mathbf{x}}_k \; : \; A\widetilde{\mathbf{x}} \le \overline{b}, \tag{3.6}$$

where $\widetilde{\mathbf{x}}_k = (\mathbf{x}_k, \mathbf{t})$ and $\widetilde{\mathbf{x}} = (\mathbf{x}, \mathbf{t})$. By merging $\exists^{\mathrm{b}} \mathbf{x}_k$ and $\exists^{\mathrm{b}} \mathbf{t}$ to form $\exists^{\mathrm{b}} \widetilde{\mathbf{x}}_k$, we get $n_k \leftarrow n_k + t \le n_k + 2^a$.

Note that the system $A\widetilde{\mathbf{x}} \le \overline{b}$ is still short. This can be seen as follows. Each system in (3.3) contains at most a inequalities, so each P_j has at most a^n vertices. Each R_j has the same number of vertices as P_j. Thus, the polytope R in (3.5) has at most $ta^n \le 2^a a^n$ vertices. Therefore, the number of facets of $R \subset \mathbb{R}^m$ is at most

$$(2^a a^n)^m \le (2^a a^n)^{n+2^a},$$

which is a constant. Each facet of R can be computed in polynomial time, so it also has a polynomial length description.

We conclude that both n_k and a are changed by contants depending only on $\overline{n}, a$ and k. The new system of inequalities is short, and has length bounded by a polynomial factor. □

Remark 3.4. The extra dimension for $\mathbf{t}$ in the above proof can actually be lowered to a. Recall that there are at most 2^a polytopes P_i. We can pick 2^a points $\overline{r}_1, \ldots, \overline{r}_{2^a} \in \{0,1\}^a$ and define

$$R_j = (\overline{r}_j, P_j) \subset \mathbb{R}^m,$$

where m is now $a + n$. Notice that $\overline{r}_1, \ldots, \overline{r}_{2^a}$ are vertices of the a-dimensional unit cube, which has no interior integer points. Therefore, the convex hull $R = \operatorname{conv}(R_1, \ldots, R_t)$ still satisfies the property

$$\mathbf{y} \in R \cap \mathbb{Z}^m \qquad \Longleftrightarrow \qquad \mathbf{y} \in R_j \cap \mathbb{Z}^m \text{ for some } j.$$

By the above lemma, at the cost of a polynomial factor, we can restrict our attention to the subclass of $\mathcal{P}^{\mathrm{b}}_{k,\overline{n},a}$ for which the Φ is just a short system of inequalities.

Lemma 3.5. *Every short sentence $S \in \mathcal{P}^{\mathrm{b}}_{k,\overline{n},a}$ of the form*

$$Q^{\mathrm{b}}_1 \mathbf{x}_1 \; Q^{\mathrm{b}}_2 \mathbf{x}_2 \; \ldots \; \forall^{\mathrm{b}} \mathbf{x}_{k-1} \; \exists^{\mathrm{b}} \mathbf{x}_k \; : \; \Phi(\mathbf{x}_1, \ldots, \mathbf{x}_k)$$

is equivalent to a short sentence S' of the form

$$Q^{\mathrm{b}}_1 y_1 \; Q^{\mathrm{b}}_2 y_2 \; \ldots \; \forall^{\mathrm{b}} y_{k-1} \; \exists^{\mathrm{b}} \mathbf{y}_k \; : \; \Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k), \tag{3.7}$$

where $y_1, \ldots, y_{k-1}$ are singletons, $\mathbf{y}_k \in \mathbb{Z}^m$ with $m \leq n_1 + \ldots + n_k$, and Ψ is a short system of length polynomial in $\phi(S)$ that describes a polytope in $\mathbb{R}^{m+k-1}$.

Proof. Since all quantifiers are bounded, we can assume $0 \leq x_{i,j} < 2^{\ell_i}$ for all coordinates $x_{i,j}$ in $\mathbf{x}_i$, where $1 \leq i \leq k, 1 \leq j \leq n_i$. Therefore, we can uniquely represent each vector $\mathbf{x}_i$ by a single integer y_i, where

$$y_i = x_{i,1} + 2^{\ell_i} x_{i,2} + \ldots + 2^{(n_i - 1)\ell_i} x_{i,n_i}.$$

Now each variable y_i is bounded in the range $[0, 2^{n_i \ell_i})$, and we can replace $\mathbf{x}_i$ by y_i for all $1 \leq i \leq k-1$. However, in order to recover all the coordinates $x_{i,j}$ in the system Φ, we need to augment $\mathbf{x}_k$ by $(n_1 + \ldots + n_{k-1})$ extra coordinates. So let $\mathbf{y}_k = (y_{k,1} \; , \ldots , \; y_{k,m})$, where $m = n_1 + \ldots + n_k$. We identify the last n_k coordinates in $\mathbf{y}_k$ with those of $\mathbf{x}_k$. For the first $m - n_k$ coordinates of $\mathbf{y}_k$, we condition

$$\left\{ \begin{aligned} y_1 \quad &= \quad y_{k,1} + 2^{\ell_1} y_{k,2} + \ldots + 2^{(n_1-1)\ell_1} y_{k,n_1} \\ y_2 \quad &= \quad y_{k,n_1+1} + 2^{\ell_2} y_{k,n_1+2} + \ldots + 2^{(n_2-1)\ell_2} y_{k,n_1+n_2} \\ &\;\vdots \\ y_{k-1} \quad &= \quad y_{k,n_1+\ldots+n_{k-2}+1} + \ldots + 2^{(n_{k-1}-1)\ell_{k-1}} y_{k,n_1+\ldots+n_{k-1}} \end{aligned} \right\}.$$

Besides, we require $0 \leq y_{k,j} < 2^{\ell_i}$ for each $y_{k,j}$ in the ith row of the above system. Adding all the above conditions (as linear inequalities) into the new system Φ, where each variable $x_{i,j}$ is substituted by $y_{k,n_1+\ldots+n_{i-1}+j}$, we obtain an equivalent short system $\Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k)$ of length $\mathrm{poly}(\phi(S))$. □

Next, we disassociate $y_1, \ldots, y_{k-2}$ from $\Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k)$ to obtain a system $\Lambda(y_{k-1}, \mathbf{y}_k)$ in only the last two variables y_{k-1} and $\mathbf{y}_k$. The following lemma shows this can be done at a cost of introducing extra relations $R_1(y_1, y_2), \ldots, R_{k-2}(y_{k-2}, y_{k-1})$, which are all short.

Lemma 3.6. *Every short sentence S' of the form*

$$Q^{\mathrm{b}}_1 y_1 \; Q^{\mathrm{b}}_2 y_2 \; \ldots \; \forall^{\mathrm{b}} y_{k-1} \; \exists^{\mathrm{b}} \mathbf{y}_k : \Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k)$$

is equivalent to another short sentence S'' of the form

$$\begin{aligned} &\exists^{\mathrm{b}} z_1 \, \forall^{\mathrm{b}} z_2 \, \neg R_1(z_1, z_2) \vee \Big[\exists^{\mathrm{b}} z_3 \; R_2(z_2, z_3) \wedge \big[\ldots \\ &\qquad \ldots \neg R_{k-2}(z_{k-2}, z_{k-1}) \vee [\exists^{\mathrm{b}} \mathbf{z}_k \; \Lambda(z_{k-1}, \mathbf{z}_k)] \ldots \big] \Big] \end{aligned} \tag{3.8}$$

if k is odd, i.e., $Q^{\mathrm{b}}_k = \exists^{\mathrm{b}}$, or

$$\begin{aligned} &\forall^{\mathrm{b}} z_1 \, \exists^{\mathrm{b}} z_2 \; R_1(z_1, z_2) \wedge \Big[\forall^{\mathrm{b}} z_3 \; \neg R_2(z_2, z_3) \vee \big[\ldots \\ &\qquad \ldots \neg R_{k-2}(z_{k-2}, z_{k-1}) \vee [\exists^{\mathrm{b}} \mathbf{z}_k \; \Lambda(z_{k-1}, \mathbf{z}_k)] \ldots \big] \Big] \end{aligned} \tag{3.9}$$

if k is even, i.e., $Q^{\mathrm{b}}_k = \forall^{\mathrm{b}}$.
Here $R_1, \ldots, R_{k-2}$ and Λ are all short and quantifier free. Also Λ is a short system of inequalities with length $\mathrm{poly}(\phi(S'))$.

Proof. By the bounded quantifiers, we have $y_i \in [0, 2^{\ell_i})$ for $1 \le i \le k-1$ and $y_{k,j} \in [0, 2^{\ell_k})$ for $1 \le j \le n_k$. We will make new variables $z_1, \ldots, z_{k-1}$ and condition them so that each z_i express $y_1, \ldots, y_i$ concatenated in binary. We identify z_1 with y_1. For z_2, we concatenate y_1 and y_2. This just means that z_2 has $\ell_1 + \ell_2$ binary digits, with the first (most significant) ℓ_1 digits from y_1 (now z_1), and the last (least significant) ℓ_2 digits from y_2. In other words, we have $z_1 = \lfloor z_2/2^{\ell_2} \rfloor$. So the first condition $R_1(z_1, z_2)$ is:

$$R_1(z_1, z_2) : z_1 = \lfloor z_2/2^{\ell_2} \rfloor \quad \Longleftrightarrow \quad \begin{cases} z_1 \le z_2/2^{\ell_2} \\ z_1 > z_2/2^{\ell_2} - 1 \end{cases}.$$

In general, if $t_j = \ell_1 + \cdots + \ell_j$, then for any $1 \le j \le k-2$, the variable z_{j+1} has its first t_j binary digits from z_j, and an extra ℓ_{j+1} last digits. This is again guaranteed by enforcing:

$$R_j(z_j, z_{j+1}) : z_j = \lfloor z_{j+1}/2^{\ell_{j+1}} \rfloor \quad \Longleftrightarrow \quad \begin{cases} z_j \le z_{j+1}/2^{\ell_{j+1}} \\ z_j > z_{j+1}/2^{\ell_{j+1}} - 1 \end{cases}.$$

So now, if $R_1(z_1, z_2), \ldots, R_{k-2}(z_{k-2}, z_{k-1})$ are all satisfied, then z_{k-1} has t_{k-1} digits corresponding to all digits from $y_1, \ldots, y_{k-1}$ concatenated. If $\mathbf{y}_k$ has n_k coordinates, we let $\mathbf{z}_k$ have $(k-1) + n_k$ coordinates. The last n_k coordinates in $\mathbf{z}_k$ correspond to those in $\mathbf{y}_k$. The first $k-1$ coordinates in $\mathbf{z}_k$ are needed to recover $y_1, \ldots, y_{k-1}$ from z_{k-1}. This is achieved by conditioning:

$$z_{k-1} = 2^{\ell_2 + \cdots + \ell_{k-1}} z_{k,1} + 2^{\ell_3 + \cdots + \ell_{k-1}} z_{k,2} + \ldots\ldots + 2^{\ell_{k-1}} z_{k,k-2} + z_{k,k-1}, \tag{3.10}$$

and

$$\begin{gathered} 0 \le z_{k,1} < 2^{\ell_1}, \ \ldots, \ 0 \le z_{k,k-1} < 2^{\ell_{k-1}}, \\ 0 \le z_{k,k} \ , \ \ldots, \ z_{k,k-1+n_k} < 2^{\ell_k}. \end{gathered} \tag{3.11}$$

The whole system $\Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k)$ can now be expressed in z_{k-1} and $\mathbf{z}_k$. Indeed, we first rewrite the system $\Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k)$ with

$$z_{k,1} \ , \ldots, \ z_{k,k-1}, \ z_{k,k}, \ \ldots, \ z_{k,k-1+n_k}$$

in place of

$$y_1, \ \ldots, \ y_{k-1}, \ y_{k,1}, \ \ldots, \ y_{k,n_k} \, .$$

Now we let $\Lambda(z_{k-1}, \mathbf{z}_k)$ be a new system including (3.10), (3.11) and Ψ. It is clear that $\Psi(y_1, \ldots, y_{k-1}, \mathbf{y}_k)$ holds if and only if $\Lambda(z_{k-1}, \mathbf{z}_k)$ holds. It is also clear that the new sentence S'' as in (3.8) or (3.9) has length $\text{poly}(\phi(S'))$ and is equivalent to the original sentence S'. Note that $z_1, \ldots, z_{k-1}$ now have length bounds $t_1 < \cdots < t_{k-1}$, i.e., we require $0 \le z_j < 2^{t_j}$ for each of the first $k-1$ quantifier. □

Combining lemmas 3.3, 3.5, and 3.6, we conclude that every sentence $S \in \mathcal{P}^{\text{b}}_{k,\overline{n},a}$ is equivalent to a sentence S'' of the form (3.8) or (3.9) in some other class $\mathcal{P}^{\text{b}}_{k,\overline{n}',a'}$. The first $k-1$ variables in S'' are now singletons and the system $\Lambda(z_{k-1}, \mathbf{z}_k)$ involves only the last two variables z_{k-1} and $\mathbf{z}_k$. We say that such short Presburger sentences S'' are in *disassociated form.*

In order to prove Theorem 3.1, we need the following special case of Kannan's partition theorem (KPT), tailored to suit our situation with short Presburger sentences (see §4.3). We refer to Theorem 3.1 in [Kan90] for the original version. Adopting the terminology in [Kan90], we call a polyhedron with possibly some open facets a *copolyhedron.*

Theorem 3.7 (Kannan's partition theorem)**.** *Let A be an integer matrix of fixed dimensions $m \times n$ and binary length ϕ. For every $\overline{b} \in \mathbb{R}^m$, let $K_{\overline{b}} = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \le \overline{b}\}$. Assume that $K_{\overline{b}}$ is bounded for all $\overline{b} \in \mathbb{R}^m$. Then one can find in polynomial time a partition*

$$\mathbb{R}^m \, = \, P_1 \sqcup P_2 \sqcup \cdots \sqcup P_r,$$

where $r \le (mn\phi)^{mn^{dn}}$, ϕ is the binary length of A, d is a universal constant, and each P_i is a rational copolyhedron with the following properties. For each P_i, $1 \le i \le r$, one can find in polynomial time a finite set $\mathcal{T}_i = \big\{(T_{ij}, T'_{ij})\big\}$ of pairs of rational affine transformations $T_{ij} : \mathbb{R}^m \to \mathbb{R}^n$ and $T'_{ij} : \mathbb{Z}^n \to \mathbb{Z}^n$, such that for every $\overline{b} \in P_i$, we have:

$$K_{\overline{b}} \cap \mathbb{Z}^n \neq \varnothing \quad \Longleftrightarrow \quad \exists (T_{ij}, T'_{ij}) \in \mathcal{T}_i \; : \; T'_{ij} \lfloor T_{ij} \overline{b} \rfloor \in K_{\overline{b}}. \tag{3.12}$$

Furthermore, the size $\big|\mathcal{T}_i\big| \le n^{4n}$, for all $1 \le i \le r$.

Remark 3.8. Since the dimensions of A are fixed, each condition $T'_{ij}\lfloor T_{ij}\overline{b}\rfloor \in K_{\overline{b}}$ 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, the condition $\frac{1}{2} + \lfloor b/5 \rfloor \le 3$ for $b \in \mathbb{R}$ can be expressed as either

$$\exists t \left\{ \begin{array}{ccc} t & \le & b/5 \\ t & > & b/5 - 1 \\ \frac{1}{2} + t & \le & 3 \end{array} \right\} \quad \text{or} \quad \forall t \left[\begin{array}{ccc} t & > & b/5 \\ t & \le & b/5 - 1 \\ \frac{1}{2} + t & \le & 3 \end{array} \right]. \tag{3.13}$$

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

Theorem 3.9 (Kannan)**.** *Short sentences $\forall \mathbf{y} \, \exists \mathbf{x} \; \Phi(\mathbf{x}, \mathbf{y})$ in every fixed class $\mathcal{P}_{2,\overline{n},a}$ can be decided in polynomial time.*

Remark 3.10. The idea of Theorem 3.9's proof is to first partition the parameter space $\mathbb{R}^{n_1}$ for $\mathbf{y}$ into polynomially many copolyhedra using Theorem 3.7. For each copolyhedron, we have a finite set of candidates for $\mathbf{x}$, expressible using an extra quantifier $\forall \mathbf{t}$ as in (3.13), which is then combined with the outer $\forall \mathbf{y}$ quantifier. For the full proof, see [Kan90]. See also §4.1 for a related remark.

Proof of Theorem 3.1. Consider a short disassociated Presburger sentence S with variables $z_1, \ldots, z_{k-1}, \mathbf{z}_k$ of the form (3.8) or (3.9). We induct on k, with the base case $k = 2$ being Theorem 3.9. Now assume that for a fixed k and every $\overline{n}', a'$, sentences in $\mathcal{P}_{k-1,\overline{n}',a'}$ are decidable in polynomial time. For convenience, we assume k is odd; the case k even is analogous. Then S has the form:

$$\begin{aligned} &\exists^{\mathrm{b}} z_1 \, \forall^{\mathrm{b}} z_2 \; \neg R_1(z_1, z_2) \vee \Big[\exists^{\mathrm{b}} z_3 \; R_2(z_2, z_3) \wedge \big[\ldots \\ &\qquad \ldots \forall^{\mathrm{b}} z_{k-1} \; \neg R_{k-2}(z_{k-2}, z_{k-1}) \vee \big[\exists^{\mathrm{b}} \mathbf{z}_k \; \Lambda(z_{k-1}, \mathbf{z}_k) \big] \ldots \big] \Big]. \end{aligned} \tag{3.14}$$

Notice that the last system $\exists^{\mathrm{b}} \mathbf{z}_k \Lambda(z_{k-1}, \mathbf{z}_k)$ has fixed dimensions. If the system has m inequalities, which is at most a constant, we can rewrite it as

$$\exists^{\mathrm{b}} \mathbf{z}_k : A\mathbf{z}_k \le \overline{\alpha} z_{k-1} + \overline{\nu} \quad \text{with} \quad \overline{\alpha}, \overline{\nu} \in \mathbb{Z}^m, A \in \mathbb{Z}^{m \times n_k}.$$

So we can treat $\mathbf{z}_k$ as $\mathbf{x}$ and $(\overline{\alpha} z_{k-1} + \overline{\nu})$ as $\overline{b}$ in Theorem 3.7. For convenience, we denote n_k by n. For each z_{k-1}, define a set $K_{z_{k-1}} \coloneqq \{\mathbf{z}_k : \Lambda(z_{k-1}, \mathbf{z}_k)\}$. Theorem 3.7 gives a polynomial size partition $\mathbb{R}^m = P_1 \sqcup \cdots \sqcup P_r$. This in turn induces a partition of $\mathbb{R}$, as the parameter space for z_{k-1}, into

$$\mathbb{R} = R_1 \sqcup \cdots \sqcup R_r, \tag{3.15}$$

where every R_i is a rational interval.[1] Since $\overline{b} = \overline{\alpha} z_{k-1} + \overline{\nu}$ depends affinely on z_{k-1}, by (3.12), we have for each interval R_i a constant size collection $\mathcal{T}_i = \{(T_{ij}, T'_{ij})\}$ of pairs of rational affine maps $T_{ij} : \mathbb{R} \to \mathbb{R}^n$ and $T'_{ij} : \mathbb{Z}^n \to \mathbb{Z}^n$, so that for every $z_{k-1} \in R_i$ we have:

$$\begin{aligned} \exists^{\mathrm{b}} \mathbf{z}_k \, \Lambda(z_{k-1}, \mathbf{z}_k) \iff & \exists (T_{ij}, T'_{ij}) \in \mathcal{T}_i \, : \, T'_{ij} \lfloor T_{ij}(z_{k-1}) \rfloor \in K_{z_{k-1}} \\ \iff & \bigvee_j A \, T'_{ij} \lfloor T_{ij}(\overline{\alpha} z_{k-1} + \overline{\nu}) \rfloor \le \overline{\alpha} z_{k-1} + \overline{\nu} \\ \iff & \bigvee_j \forall \mathbf{t}_j \begin{bmatrix} \mathbf{t}_j \neq \lfloor T_{ij}(\overline{\alpha} z_{k-1} + \overline{\nu}) \rfloor \\ \\ A \, T'_{ij} \mathbf{t}_j \le \overline{\alpha} z_{k-1} + \overline{\nu} \end{bmatrix}, \end{aligned} \tag{3.16}$$

where the disjunction is over all j such that $(T_{ij}, T'_{ij}) \in \mathcal{T}_i$.

Here we are expressing the condition $\mathbf{t}_j \neq \lfloor T_{ij}(\overline{\alpha} z_{k-1} + \overline{\nu}) \rfloor$ using a short disjunction after $\forall t$ as in (3.13). We have to do this for all coordinates $t_{j,1}, \ldots, t_{j,n}$. The next step is to bring all the quantifiers $\forall \mathbf{t}_j$ outside of the short disjunction $\bigvee_j$ in (3.16). We can concatenate all $\mathbf{t}_j$'s into another vector $\mathbf{u}$. Thus, for every $z_{k-1} \in R_i$, we have:

$$\exists^{\mathrm{b}} \mathbf{z}_k \; \Lambda(z_{k-1}, \mathbf{z}_k) \iff \forall \mathbf{u} \bigvee_j \begin{bmatrix} \mathbf{u}_j \neq \lfloor T_{ij}(\overline{\alpha} z_{k-1} + \overline{\nu}) \rfloor \\ \\ A \, T'_{ij} \mathbf{u}_j \le \overline{\alpha} z_{k-1} + \overline{\nu} \end{bmatrix}. \tag{3.17}$$

Notice that $\mathbf{u}$ still has bounded dimension, because the number of pairs $(T_{ij}, T'_{ij}) \in \mathcal{T}_i$ is at most n^{4n}. Also, the whole expression after $\forall \mathbf{u}$ is still short.

Now comes the benefit of having $z_1, \ldots, z_{k-2}$ disassociated from $\Lambda(z_{k-1}, \mathbf{z}_k)$. Let us recall the proof of Lemma 3.6. In there, the variables $z_1, \ldots, z_{k-1}$ have length bounds $t_1 < \cdots < t_{k-1}$. For every $1 \le j \le k-2$, the relation $R_j(z_j, z_{j+1})$ forces z_{j+1} to carry all the binary digits of z_j as its first (most significant) t_j binary digits. So if all $R_1(z_1, z_2), \ldots, R_{k-2}(z_{k-2}, z_{k-1})$ are all satisfied, then out of the t_{k-1} digits of z_{k-1}, the first t_1 digits are from z_1. For particular value of z_1 in the range $[0, 2^{t_1})$, every such z_{k-1} lies in a contiguous segment of length $2^{t_{k-1} - t_1}$. To be precise, for every $z_1 \in [0, 2^{t_1})$, we have

$$z_{k-1} \in I_{z_1} \coloneqq \big[z_1 2^{t_{k-1} - t_1}, \; (z_1 + 1) 2^{t_{k-1} - t_1} \big).$$

There are 2^{t_1} such segments I_{z_1}, one for each $z_1 \in [0, 2^{t_1})$. However, by (3.15), the domain $\mathbb{R}$ for z_{k-1} was partitioned into r (rational) segments $R_1 \sqcup \cdots \sqcup R_r$, where r is polynomial in $\phi(S)$. Therefore, at most a polynomial number of intervals I_{z_1} overlap with more than one interval R_i. We partition the interval $[0, 2^{t_1})$ of all possible z_1 values into two subsets:

$$\begin{aligned} & \mathcal{F}_1 = \big\{ z_1 \in [0, 2^{t_1}) : I_{z_1} \subseteq R_i \text{ for some } 1 \le i \le r \big\} \quad \text{and} \\ & \mathcal{F}_2 = \big\{ z_1 \in [0, 2^{t_1}) : I_{z_1} \text{ intersects both } R_i \text{ and } R_{i+1} \text{ for some } i \big\}. \end{aligned} \tag{3.18}$$

In other words, $\mathcal{F}_1$ contains every interval I_{z_1} that lies completely inside some interval R_i, and $\mathcal{F}_2$ contains the rest. Observe that $|\mathcal{F}_2| \le r = \mathrm{poly}(\phi(S))$. This is because the intervals I_{z_1} are disjoint for different values of z_1, and if $z_1 \in \mathcal{F}_2$ then I_{z_1} must contain the common end point of R_i and R_{i+1} for some $1 \le i \le r$.

The original sentence S begins with $\exists^{\mathrm{b}} z_1$. First, we check over all values $z_1 \in \mathcal{F}_2$. Substituting any such z_1 value into S, we get another short sentence with ***one quantifier less***,

[1] Each R_i can be half open with rational end points. Even though this forms a partition of $\mathbb{R}$, we only consider integer values in each R_i for z_{k-1}.

i.e., a sentence in some class $\mathcal{P}^{\mathrm{b}}_{k-1,\overline{n}',a'}$. By induction, each such sentence is polynomial time decidable. In summary, we can check whether any $z_1 \in \mathcal{F}_2$ satisfies S, in time poly$(\phi(S))$.

For $z_1 \in \mathcal{F}_1$, recall by Theorem 3.7 that one can find $R_1, \dots, R_r$ in polynomial time. Thus, we can subpartition $\mathcal{F}_1$ into r parts:

$$\mathcal{F}_1 = \bigsqcup_{i=1}^{r} \mathcal{F}_{1,i} \quad \text{where} \quad \mathcal{F}_{1,i} = \big\{ z_1 \in \mathcal{F}_1 : I_{z_1} \subseteq R_i \big\},\ 1 \le i \le r. \tag{3.19}$$

Note that each $\mathcal{F}_{1,i}$ is a contiguous subinterval in $[0, 2^{t_1})$. For each $\mathcal{F}_{1,i}$, we can iteratively check if any $z_1 \in \mathcal{F}_{1,i}$ satisfies S as follows. For a fixed i and all $z_1 \in \mathcal{F}_{1,i}$, we have $z_{k-1} \in I_{z_1} \subseteq R_i$. Therefore, by (3.17), the final quantifier $\exists^{\mathrm{b}} \mathbf{z}_k\ \Lambda(z_{k-1}, \mathbf{z}_k)$ can be replaced by $\forall^{\mathrm{b}} \mathbf{u}\ \Gamma_i(z_{k-1}, \mathbf{u})$. Here Γ_i as given by the RHS in (3.17) depends on i but is still short. So now in (3.14) we can combine $\forall z_{k-1}$ and $\forall \mathbf{u}$ together and get

$$\begin{aligned} &\exists^{\mathrm{b}}(z_1 \in \mathcal{F}_{1,i})\ \forall^{\mathrm{b}} z_2\ \neg R_1(z_1, z_2) \vee \Big[\exists^{\mathrm{b}} z_3\ R_2(z_2, z_3) \wedge \big[\dots \\ &\dots \forall^{\mathrm{b}} z_{k-1} \forall^{\mathrm{b}} \mathbf{u}\ \ \neg R_{k-2}(z_{k-2}, z_{k-1})\ \vee\ \Gamma_i(z_{k-1}, \mathbf{u}) \dots \big] \Big]. \end{aligned} \tag{3.20}$$

The quantifiers $\forall^{\mathrm{b}} z_{k-1}$ and $\forall^{\mathrm{b}} \mathbf{u}$ can be combined as $\forall^{\mathrm{b}}(\mathbf{z}_{k-1}, \mathbf{u})$. This results in a short sentence in some class $\neg\mathcal{P}^{\mathrm{b}}_{k-1,\overline{n}'',a''}$ (negated because the last quantifier is $\forall^{\mathrm{b}}$). By the inductive assumption, we can check this sentence in polynomial time. In summary, we can check the sentence (3.20) in polynomial time for each $1 \le i \le r$. Since r is polynomial in $\phi(S)$, we can check the whole set $\mathcal{F}_1$ in time poly$(\phi(S))$.

The case of even k follows verbatim, with $\mathcal{F}_2$ consisting of subproblems in some class $\mathcal{P}^{\mathrm{b}}_{k-1,\overline{n}',a'}$ and $\mathcal{F}_1$ consisting of subproblems in some other class $\neg\mathcal{P}^{\mathrm{b}}_{k-1,\overline{n}'',a''}$. □

3.2. **Finding short generating functions for short Presburger formulas.** A short Presburger formula is defined as a short Presburger sentence with the first variable $\mathbf{x}_1$ unquantified. We again group these formulas into families:

$$\mathcal{PF}_{k,\overline{n},a} = \Big\{ F = \big[\mathbf{x}_1 : Q_2 \mathbf{x}_2\ Q_3 \mathbf{x}_3\ \dots\ \exists \mathbf{x}_k\ \ \Phi(\mathbf{x}_1, \dots, \mathbf{x}_k) \big] \Big\}.$$

Here $k, \overline{n}, a$ have the same meanings as in (3.1). The $k-1$ quantifiers $Q_2, \dots, Q_k \in \{\exists, \forall\}$ alternate, with $Q_k = \exists$. First, we prove a restricted version of Theorem B:

Theorem 3.11. *Assuming KPT, given a short formula $F \in \mathcal{PF}_{k,\overline{n},a}$ and a number N in binary, one can find a short GF for*

$$\big\{ \mathbf{x}_1 \in \mathbb{Z}^{n_1} \cap [-N, N]^{n_1} : F(\mathbf{x}_1) = \text{true} \big\}$$

in time polynomial in $\phi(F)$ and $\log N$.

As we mentioned in the introduction, the special case $k = 2$ of the above theorem follows from Theorem 1.7 in [BW03] on projection of integer points in a finite dimensional polytope, which we restate below for convenience.

Theorem 3.12 (Barvinok and Woods)**.** *Fix m. Given a rational polytope $P \subset \mathbb{R}^m$ described by $A\mathbf{x} \le \overline{b}$, and a linear transformation $T : \mathbb{Z}^m \to \mathbb{Z}^n$ represented by a matrix $T \in \mathbb{Z}^{n \times m}$, there is a polynomial time algorithm that computes a short GF for $T(P \cap \mathbb{Z}^m)$ as:*

$$g(\mathbf{t}) = \sum_{\mathbf{z} \in T(P \cap \mathbb{Z}^m)} \mathbf{t}^{\mathbf{z}} = \sum_{i=1}^{M} \frac{c_i\, \mathbf{t}^{\overline{a}_i}}{(1 - \mathbf{t}^{\overline{b}_{i1}}) \dots (1 - \mathbf{t}^{\overline{b}_{is}})}\,,$$

where $c_i = p_i/q_i \in \mathbb{Q}$, $\overline{a}_i, \overline{b}_{ij} \in \mathbb{Z}^n$, $\overline{b}_{ij} \neq 0$ for all i,j, and $s = s(m)$ is a constant depending only on m.

Define the *length* of the short GF $g(\mathbf{t})$ as in Theorem 3.12 as

$$\phi(g) \, = \, \sum_i \lceil \log_2 |p_i\, q_i| + 1 \rceil \, + \sum_{i,j} \lceil \log_2 a_{ij} + 1 \rceil + + \sum_{i,j,r} \lceil \log_2 b_{ijr} + 1 \rceil , \tag{3.21}$$

where $\overline{a}_i = (a_{i1}, \ldots, a_{in})$ and $\overline{b}_{ij} = (b_{ij1}, \ldots, b_{ijn})$.

Referring back to the proof of Theorem 3.1, we see that Theorem 3.11 can be proved following the same vein if we assume $n_1 = 1$, i.e., $\mathbf{x}_1$ is a singleton x_1. If $n_1 > 1$, we can first convert $\mathbf{x}_1$ into a singleton by concatenating its (bounded) coordinates into a single number x_1 as in Lemma 3.5. The cases corresponding to positive and negative coordinates $x_{1,j}$ can be treated separately. However, doing so would affect the multi-variable generating function for $\mathbf{x}_1$. The following technical result is a GF analogue of Lemma 3.5, which allows one to convert between multi-variable and single-variable short generating functions.

Lemma 3.13. *Fix n. Assume $F \subseteq [0, 2^\ell)^n$ has a short GF $f(\mathbf{t})$ which expands into $\sum_{\mathbf{x}\in F} \mathbf{t}^{\mathbf{x}}$. Let $G \subseteq \big[0, 2^{n\ell}\big)$ be defined as*

$$G := \big\{ x_1 + 2^\ell x_2 + \cdots + 2^{(n-1)\ell} x_n : (x_1, \ldots, x_n) \in F \big\}.$$

Then G has a short GF $g(t)$ of length $\operatorname{poly}(\phi(f) + \ell)$ *which expands into $\sum_{x\in G} t^x$. Conversely, if G has a short GF $g(t)$, then F also has a short GF $f(\mathbf{t})$ of length* $\operatorname{poly}(\phi(g) + \ell)$.

Proof of Lemma 3.13. Let $N = 2^\ell$. Assume the formula F has a short GF $f(\mathbf{t})$ that satisfies

$$f(\mathbf{t}) = \sum_{\mathbf{x}\in F} \mathbf{t}^{\mathbf{x}} = \sum_{\mathbf{x}\in F} t_1^{x_1} \ldots t_n^{x_n}.$$

Let $g(t)$ be the evaluation of $f(\mathbf{t})$ under the following substitutions:

$$t_1 \leftarrow t, \; t_2 \leftarrow t^N, \ldots, \; t_n \leftarrow t^{N^{n-1}},$$

so that

$$\mathbf{t}^{\mathbf{x}} \, = \, t^{x_1 + N x_2 + \ldots + N^{n-1} x_{n-1}}.$$

Clearly, GF $g(t)$ expands into $\sum_{x\in G} t^x$. Thus it is a short generating function for G. By Theorem 2.6 in [BW03], the above monomial substitutions on $f(\mathbf{t})$ can be performed in polynomial time, giving $g(t)$ of polynomial length.

For the other direction, assume G has a short GF $g(t)$. Consider the following multi-variable short GF $a(\mathbf{t})$:

$$a(\mathbf{t}) \, = \sum_{\mathbf{x}\in[0,N)^n} \mathbf{t}^{\mathbf{x}} \, = \, \frac{1 - t_1^N}{1 - t_1} \cdots \frac{1 - t_n^N}{1 - t_n}.$$

Since n is fixed, after expanding product in the numerators, we have $a(\mathbf{t})$ a short GF of length $\operatorname{poly}(\log N)$.

Define a linear map $\tau : \mathbb{Z}^n \to \mathbb{Z}$ as:

$$\tau(\mathbf{x}) \, = \, x_1 + N x_2 + \ldots + N^{n-1} x_n.$$

Given $A(\mathbf{t}) = \sum \alpha_{\mathbf{x}} \mathbf{t}^{\mathbf{x}}$ a multi-variable short GF and $B(t) = \sum \beta_x t^x$ a single-variable short GF, we define their *τ-Hadamard product* $C(\mathbf{t}) = A(\mathbf{t}) \star_\tau B(t)$ as follows:

$$A(\mathbf{t}) \star_\tau B(t) := \sum \alpha_{\mathbf{x}} \beta_{\tau(\mathbf{x})} \mathbf{t}^{\mathbf{x}}. \tag{3.22}$$

From this definition, it is clear that our original set $F \in [0, N)^n$ has a GF given by:

$$f(\mathbf{t}) = a(\mathbf{t}) \star_\tau g(t).$$

We prove the following claim: The τ-Hadamard product of two short GFs is again a short GF of polynomial length. The proof is an analogue of Barvinok's argument in [Bar06] (see also lemmas 3.4 and 3.6 in [BW03]). First, notice that the τ-Hadamard product is bilinear in $A(\mathbf{t})$ and $B(t)$. Therefore, it suffices to prove the claim when $A(\mathbf{t})$ and $B(\mathbf{t})$ each has only one term, i.e.,

$$A(\mathbf{t}) = \frac{\mathbf{t}^{\overline{a}}}{\prod_{i=1}^{p}(1 - \mathbf{t}^{\overline{b}_i})} \quad \text{and} \quad B(t) = \frac{t^c}{\prod_{j=1}^{q}(1 - t^{d_j})}. \tag{3.23}$$

Consider an (unbounded) polyhedron $P \subset \mathbb{R}^{p+q}$ with coordinates $(\zeta_1, \ldots, \zeta_p, \xi_1, \ldots, \xi_q)$, defined as:

$$P := \left\{ \begin{array}{ccc} \zeta_1, \ldots, \zeta_p, \xi_1, \ldots, \xi_q & \geq & 0 \\ \tau(\overline{a} + \zeta_1 \overline{b}_1 + \cdots + \zeta_p \overline{b}_p) & = & c + \xi_1 d_1 + \cdots + \xi_q d_q \end{array} \right\}. \tag{3.24}$$

By Theorem 2.2 from [Bar93], we can write a short GF for $P \cap \mathbb{Z}^{p+q}$:

$$D(\mathbf{u}, \mathbf{v}) := \sum_{(\boldsymbol{\zeta}, \boldsymbol{\xi}) \in P} \mathbf{u}^{\boldsymbol{\zeta}} \mathbf{v}^{\boldsymbol{\xi}} = \sum_{(\boldsymbol{\zeta}, \boldsymbol{\xi}) \in P} u_1^{\zeta_1} \ldots u_p^{\zeta_p} \, v_1^{\xi_1} \ldots v_q^{\xi_q}. \tag{3.25}$$

By (3.23), the expansions of $A(\mathbf{t})$ and $B(t)$ are:

$$A(\mathbf{t}) = \sum_{\boldsymbol{\zeta} \geq 0} \mathbf{t}^{\overline{a} + \zeta_1 \overline{b}_1 + \cdots + \zeta_p \overline{b}_p}, \; B(t) = \sum_{\boldsymbol{\xi} \geq 0} t^{c + \xi_1 d_1 + \cdots + \xi_q d_q}. \tag{3.26}$$

We substitute

$$u_1 \leftarrow \mathbf{t}^{\overline{b}_1}, \ldots, u_p \leftarrow \mathbf{t}^{\overline{b}_p} \quad \text{and} \quad v_1 \leftarrow 1, \ldots, v_q \leftarrow 1.$$

By (3.24), (3.25) and (3.26), we get

$$\mathbf{t}^{\overline{a}} D(\mathbf{t}^{b_1}, \ldots, \mathbf{t}^{b_p}, 1, \ldots, 1) = A(\mathbf{t}) \star_\tau B(t) = C(\mathbf{t}).$$

Since substitutions can be done in polynomial time, we obtain a short GF $C(\mathbf{t})$ of polynomial length. This completes the proof. □

Proof of Theorem 3.11. First, we make a change of variables from $\mathbf{x}_1$ to $\mathbf{x}_1' = \mathbf{x}_1 + N$, i.e., $x_{1,j}' = x_{1,j} + N$. So counting the number of $\mathbf{x}_1 \in [-N, N]^{n_1}$ is equivalent to counting the number of $\mathbf{x}_1' \in [0, 2N]^{n_1}$. Therefore, we can assume that all coordinates of $\mathbf{x}_1$ are non-negative.

Given a formula in $\mathcal{PF}_{k,\overline{n},a}$, we can apply Lemmas 3.3, 3.5 and 3.6 to convert it into an equivalent formula F in disassociated form as in (3.14) (with $\exists^{\mathrm{b}} z_1$ replaced by "z_1 :"). The vector $\mathbf{x}_1$ is now a singleton z_1 bounded in some interval $[0, 2^{t_1})$. Applying Lemma 3.13, it is equivalent to show that the GF $f(t) = \sum_{z_1} t^{z_1}$ is short. We prove the result by induction on k. The case $k = 2$ follows from Theorem 3.12.

Assume that for fixed k and all $\overline{n}'$ and a', every formula in $\mathcal{PF}_{k-1,\overline{n}',a'}$ has a short GF of polynomial length in every finite interval $[0, N)$. Applying the same reasoning as in the proof of Theorem 3.1, we get a partition for $[0, 2^{t_1})$ into $\mathcal{F}_1$ and $\mathcal{F}_2$, see (3.18). Recall that $|\mathcal{F}_2|$ is polynomial in $\phi(F)$. Substituting each value $z \in \mathcal{F}_2$ into F for z_1, we get a fully quantified short Presburger statement S_z in some class $\mathcal{P}^{\mathrm{b}}_{k-1,\overline{n}',a'}$, with $\phi(S_z) = \mathrm{poly}(\phi(F))$.

Each such statement S_z can be checked in time $\operatorname{poly}(\phi(S_z))$ by Theorem 3.1. Therefore, in time $\operatorname{poly}(\phi(F))$, we obtain a short GF $g(t)$:

$$g(t) = \sum_{z \in \mathcal{F}_2 \, : \, S_z = \text{true}} t^z.$$

By (3.19), we have a refinement of $\mathcal{F}_1$ into polynomially many intervals $\mathcal{F}_{1,i}$, where $1 \le i \le r$. By (3.20), for $z_1 \in \mathcal{F}_{1,i}$, the formula F is equivalent to another formula F_i in some class $\neg\mathcal{PF}_{k-1,\overline{n}'',a''}$, with $\phi(F_i) = \operatorname{poly}(\phi(F))$. The GF $f_i(t)$ for F_i can be found in time $\operatorname{poly}(\phi(F_i))$ by induction.

In summary, we obtain in time $\operatorname{poly}(\phi(F))$, the GF

$$f(t) = \sum_{i=1}^{r} f_i(t) + g(t),$$

which completes the proof. □

We can actually remove the coordinate bounds in Theorem 3.11:

Theorem 3.14. *Assuming KPT, given a short formula $F \in \mathcal{PF}_{k,\overline{n},a}$, we can find a short GF for*

$$\big\{\mathbf{x}_1 \in \mathbb{Z}^{n_1} \, : \, F(\mathbf{x}_1) = \text{true}\big\}$$

in time polynomial in $\phi(F)$.

Proof. By Theorem 5.3 in [NP17a], given a Presburger formula F, the full generating function $f(\mathbf{t})$ for all satisfying $\mathbf{x}_1$ can be computed in polynomial time given a partial generating function $f_N(\mathbf{t})$ for satisfying $\mathbf{x}_1$ in a large enough box $[-N, N]^{n_1}$. This result also allows us to compute N in polynomial time given F. With such an N, we can appeal to Theorem 3.11 to compute $f_N(\mathbf{t})$ so that $\phi(f_N)$ is polynomial in $\log N$ and $\phi(F)$. Since $\log N = \operatorname{poly}(\phi(F))$, we also have $\phi(f_N) = \operatorname{poly}(\phi(F))$. By an application of Theorem 5.3 in [NP17a], we recover the full generating function f, which satisfies $\phi(f) = \operatorname{poly}(\phi(f_N)) = \operatorname{poly}(\phi(F))$.[2] □

Remark 3.15. Here we treat the full generating function of $\mathbf{x}_1$ as formal power series which can also be represented as a rational function $f(\mathbf{t})$. In some cases, the power series might not converge under numerical substitution. For example, if F is a trivial formula then every $\mathbf{x}_1 \in \mathbb{Z}^{n_1}$ satisfies F. So the power series for $\mathbf{x}_1$ is $\sum_{\mathbf{x}_1 \in \mathbb{Z}^{n_1}} \mathbf{t}^{\mathbf{x}_1}$, which is not convergent for any non-zero $\mathbf{t}$. However, if $\mathbf{x}_1$ is restricted to lie in a pointed cone, for example $\mathbf{x}_1 \in \mathbb{N}^{n_1}$, then the power series converges on a non-empty open domain. For any $\mathbf{t}$ in that domain, the power series converges to the computed rational function $f(\mathbf{t})$.

4. Final remarks

4.1. **Long systems.** Recall that both Lenstra and Kannan's results on deciding sentences of types (∘) and (∘∘) as in the introduction allow for *long systems of inequalities.* However, we can reduce each case to deciding a polynomial numbers of short sentences. Indeed, let n be fixed and $m \ge 2^n$ be arbitrary. The *Doignon–Bell–Scarf theorem* [Sch86, §16.5] (see also [ABDL]) implies that a system $A\mathbf{x} \le \overline{b}$ with $A \in \mathbb{Z}^{m \times n}$ has an integer solution $\mathbf{x} \in \mathbb{Z}^n$

[2] Generally speaking, one needs to be careful taking evaluations and Hadamard products for bi-infinite Laurent power series, to avoid summations of the type $\sum_{n \in \mathbb{Z}} t^n$. Paper [NP17a] sidesteps this problem by explicitly disallowing such summations. We refer to [Bar08, BP99] for the theory of valuations in this context, which allows one to get around this issue.

if and only if every short subsystem $A'\mathbf{x} \leq \overline{b'}$ has a solution $\mathbf{x} \in \mathbb{Z}^n$. Here A' is a submatrix with 2^n rows from A, and $\overline{b'}$ is the corresponding subvector from $\overline{b}$.

For one quantifier $\exists$, by the Doignon–Bell–Scarf theorem, we have:

$$\exists \mathbf{x} \, : \, A\mathbf{x} \leq \overline{b} \quad \Longleftrightarrow \quad \bigwedge_{(A',\overline{b'})} \exists \mathbf{x} \, : \, A'\mathbf{x} \leq \overline{b'}.$$

So it is equivalent to decide each of the $\binom{m}{2^n}$ short sentences individually. This number clearly polynomial in m if n is fixed.

For two quantifiers $\forall\exists$, in the system $A'\mathbf{x} + B'\mathbf{y} \leq \overline{c'}$ we can proceed in a similar manner, see [NP17b, §7.1]. However, already for three quantifiers as in ($\circ\circ\circ$) this approach provably fails. Roughly, this is because the long conjunction over $(A', B', \overline{c'})$ no longer commutes with the outer existential quantifier $\exists \mathbf{z} \in R$.

In fact, our most recent result [NP17b] proves that for long systems as in ($\circ\circ\circ$), the problems becomes NP-complete, already for $\overline{n} = (1, 2, 3)$. This negatively resolves an open problem in [Kan92] and underscores the contrast with Theorem A.

4.2. **Bounded affine dimension.** In [ES08], Eisenbrand and Shmonin strengthened Kannan's Theorem 3.9 by completely removing the condition that P has a bounded affine dimension N. However, their version of KPT weakens the conclusion by partitioning the parameter space P into $Q_1 \sqcup \cdots \sqcup Q_r$, where each $Q_i \subset \mathbb{R}^m$ is no longer a copolyhedron. Instead, each Q_i is now the *integer projection* of some higher dimensional rational copolyhedron $Q'_i \subset \mathbb{R}^{m+k}$, defined as:

$$Q_i = \{\mathbf{x} \in \mathbb{R}^m \, : \, \exists \mathbf{y} \in \mathbb{Z}^k \;\; (\mathbf{x}, \mathbf{y}) \in Q'_i\}.$$

For $m = 1$, such sets are called *semilinear* and are of independent interest (see [CH16, NP17a]).

Note that having each piece P_i as an actual copolyhedron (interval for $m = 1$), is crucial for our proof of Theorem 3.1. For this, see the partition into intervals R_i in (3.15), and a discussion that follows.

4.3. **Kannan's partition theorem.** Kannan originally proved Kannan's partition theorem (Theorem 3.7) in greater generality, see Theorem 3.1 in [Kan90]. In his version, the number of inequalities n is allowed to vary, but the parameters $\overline{b}$ are constrained to lie in a polyhedron $P \subset \mathbb{R}^m$ of a *fixed* affine dimension N. The algorithm finds a partition $P = P_1 \sqcup \cdots \sqcup P_r$ of P into r rational copolyhedra. The rest of the statement is the same as in Theorem 3.7. As we mentioned above, we only need $m = 1$ case.

Now, the proof of KPT given in [Kan90] is quite technical and relies on an earlier conference paper which was later revised and published separately [Kan92], which in turn uses the *flatness theorem* (as did [BW03, ES08]), and other earlier work. While we have no doubt in the validity of Kannan's Theorem 3.9, in part due to its self-contained presentation and generalization in [ES08] (see also [Eis10]), we were unable to piece together all the details which go into the proof of KPT. However, at this time we are not ready to establish a clear gap in the proof of KPT, which would revert its status to a conjecture. We are simply being cautious in citing a theorem whose proof we do not fully understand, and which is crucially used as a black box in the proof of both theorems A and B.

In the near future, we intend to bring more clarity into validity of KPT, at least in the $m = 1$ case which is used in the paper. In the meantime we intend to treat KPT as an oracle, a time honored tradition in both computational logic and computational complexity.

We hope this clarifies the reasoning behind our somewhat nonstandard use of KPT as an assumption in the statements of the results.

Acknowledgements. We are greatly indebted to Sasha Barvinok for his eternal optimism, many fruitful discussions and encouragement. We are also thankful to Iskander Aliev, Matthias Aschenbrenner, Artëm Chernikov, Jesús De Loera, Lenny Fukshansky, Oleg Karpenkov and Sinai Robins for interesting conversations and helpful remarks. We are very grateful to Rafi Ostrovsky and Vijay Vazirani for kindly advising us on the structure of the paper, and to anonymous referees for their comments. The second author was partially supported by the NSF.

References

[ABDL] I. Aliev, R. Bassett, J. A. De Loera, and Q. Louveaux, A Quantitative Doignon–Bell–Scarf Theorem, to appear in *Combinatorica*; `arXiv:1405.2480`.

[B+12] V. Baldoni, N. Berline, J. A. De Loera, M. Köppe and M. Vergne, Computation of the highest coefficients of weighted Ehrhart quasi-polynomials of rational polyhedra, *Found. Comput. Math.* **12** (2012), 435–469.

[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.

[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.

[BV07] N. Berline and M. Vergne, Local Euler–Maclaurin formula for polytopes, *Mosc. Math. J.* **7** (2007), 355–386.

[CH16] D. Chistikov and C. Haase, The taming of the semi-linear set, in *Proc. ICALP 2016*, 127:1–127:13.

[CDW12] M. Christandl, B. Doran and M. Walter, Computing multiplicities of Lie group representations, in *Proc. 53rd FOCS*, IEEE, Los Alamitos, CA, 2012, 639–648

[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.

[D+04] J. A. De Loera, D. Haws, R. Hemmecke, P. Huggins, B. Sturmfels and R. Yoshida, Short rational functions for toric algebra and applications, *J. Symbolic Comput.* **38** (2004), 959–973.

[D+06a] J. A. De Loera, R. Hemmecke, M. Köppe and R. Weismantel, Integer polynomial optimization in fixed dimension, *Math. Oper. Res.* **31** (2006), 147–153.

[D+06b] J. A. De Loera, R. Hemmecke, M. Köppe and R. Weismantel, FPTAS for mixed-integer polynomial optimization with a fixed number of variables, in *Proc. 17th SODA*, ACM Press, 2006, 743–748.

[DHTY04] J. A. De Loera, R. Hemmecke, J. Tauzer and R. Yoshida, Effective lattice point counting in rational convex polytopes, *J. Symbolic Comput.* **38** (2004), 1273–1302.

[DK97] M. Dyer and R. Kannan, On Barvinok's algorithm for counting lattice points in fixed dimension, *Math. Oper. Res.* **22** (1997), 545–549.

[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.

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

[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.

[FT87] A. Frank and É. Tardos, An application of simultaneous Diophantine approximation in combinatorial optimization, *Combinatorica* **7** (1987), 49–65.

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

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

[Kan90] R. Kannan, Test sets for integer programs, ∀∃ 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.

[Köp07] M. Köppe, A primal Barvinok algorithm based on irrational decompositions, *SIAM J. Discrete Math.* **21** (2007), 220–236.

[KV08] M. Köppe and S. Verdoolaege, Computing parametric rational generating functions with a primal Barvinok algorithm, *Electron. J. Combin.* **15** (2008), no. 1, RP 16, 19 pp.

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

[MS05] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Springer, New York, 2005.

[NP17a] D. Nguyen and I. Pak, Enumeration of integer points in projections of unbounded polyhedra, extended abstract to appear in *Proc. IPCO 2017*; `arXiv:1612.08030`.

[NP17b] D. Nguyen and I. Pak, The computational complexity of integer programming with alternations; `arXiv:1702.08662`.

[NP17c] D. Nguyen and I. Pak, Complexity of short generating functions; `arXiv:1702.08660`.

[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.

[Pak02] I. Pak, On sampling integer points in polyhedra, in *Foundations of Computational Mathematics*, World Sci., River Edge, NJ, 2002, 319–324.

[PP15] I. Pak and G. Panova, On the complexity of computing Kronecker coefficients, to appear in *Computational Complexity*; `arXiv:1404.0653`.

[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; English transltion in *Hist. Philos. Logic* **12** (1991), 225–233.

[RL78] C. R. Reddy and D. W. Loveland, Presburger arithmetic with bounded quantifier alternation, *Proc. 10th STOC* (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.

[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.

[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.

[WV08] K. Woods and S. Verdoolaege, Counting with rational generating functions, *J. Symbolic Comput.* **43** (2008), 75–91.