On the complexity of quantified integer programming

Dmitry Chistikov[*][1,2] **and Christoph Haase**[3]

1 **Centre for Discrete Mathematics and its Applications (DIMAP) & Department of Computer Science, University of Warwick, UK**
d.chistikov@warwick.ac.uk

2 **Department of Computer Science, University of Oxford, UK**
dmitry.chistikov@cs.ox.ac.uk

3 **Department of Computer Science, University of Oxford, UK**
christoph.haase@cs.ox.ac.uk

Abstract

Quantified integer programming is the problem of deciding assertions of the form $\mathrm{Q}_k \boldsymbol{x}_k \dots \forall \boldsymbol{x}_2\ \exists \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ where vectors of variables $\boldsymbol{x}_k, \dots, \boldsymbol{x}_1$ form the vector $\boldsymbol{x}$, all variables are interpreted over $\mathbb{N}$ (alternatively, over $\mathbb{Z}$), and A and $\boldsymbol{c}$ are a matrix and vector over $\mathbb{Z}$ of appropriate sizes. We show in this paper that quantified integer programming with alternation depth k is complete for the kth level of the polynomial hierarchy.

1998 ACM Subject Classification G.2 Discrete Mathematics

Keywords and phrases integer programming, semi-linear sets, Presburger arithmetic, quantifier elimination

Digital Object Identifier 10.4230/LIPIcs.ICALP.2017.

1 Introduction

The problem of integer programming is, given a system of linear inequalities $A \cdot \boldsymbol{x} \geq \boldsymbol{b}$, to decide whether there exists a solution for $\boldsymbol{x}$ in the non-negative integers. This problem has been studied for decades, and its 0–1 version (in which the components of $\boldsymbol{x}$ are constrained to be either 0 or 1) is one of Karp's seminal 21 NP-complete problems [8]. In this paper, we study quantified integer programming (QIP), an extension of integer programming where some of the variables can be quantified universally—so that its instances have the form

$$\mathrm{Q}_k \boldsymbol{x}_k\ \dots\ \forall \boldsymbol{x}_2.\ \exists \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \geq \boldsymbol{c} \tag{1}$$

where $\mathrm{Q}_i \in \{\exists, \forall\}$ and $\boldsymbol{x}$ consists of all first-order variables appearing in the vectors $\boldsymbol{x}_i$.

Our main contribution is settling the complexity of QIP with k quantifier blocks (as above): we prove this problem complete for the kth level of the polynomial hierarchy, similarly to the quantified version of SAT.[1] We also show that QIP with an unbounded number of quantifier blocks is PSPACE-hard and decidable in $\mathsf{STA}(*, 2^{n^{O(1)}}, n) \subseteq \mathsf{EXPSPACE}$.[2]

[*] Supported by the ERC grant AVS-ISS (648701).

[1] As in the case of quantified CNF SAT, the innermost block of universal quantifiers, if present, is disregarded; e.g., the $\forall^*\exists^*\forall^*$ fragment is complete for Π^{P}_2. So we find fragments of QIP complete for $\Sigma^{\mathsf{P}}_1 = \mathsf{NP}$, Π^{P}_2, Σ^{P}_3, $\dots$, but not for $\mathsf{coNP} = \Pi^{\mathsf{P}}_1$, Σ^{P}_2, $\dots$

[2] The complexity class $\mathsf{STA}(s(n), t(n), a(n))$ was introduced by Berman [1] and contains all decision problems that can be decided by an alternating Turing machine in time $t(n)$ using space at most $s(n)$ and alternating at most $a(n)$ times on every computation branch.

44th International Colloquium on Automata, Languages, and Programming (ICALP 2017).
Editors: Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl;
Article No. ; pp. :1–:21
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Related work and discussion. While the decidability of QIP is immediate—it can be viewed as a syntactic fragment of Presburger arithmetic, the (decidable) first-order theory of the natural numbers with addition and order, in which matrix formulas are constrained to be conjunctions of linear inequalities—its computational complexity has been unknown. It is, of course, not difficult to see that QIP (and in fact Presburger arithmetic) is PSPACE-complete if the interpretation of every first-order variable x_i is restricted to an interval $[l_i, u_i]$ that is given as part of the input: $x_i \in [l_i, u_i]$; see, e.g., [14]. But if $x_i \in \mathbb{N}$, then the best known upper bounds seem to be $\mathsf{STA}(*, 2^{2^{n^{O(1)}}}, O(n)) \subseteq \mathsf{2\text{-}EXPSPACE}$, the generic upper bound for deciding Presburger arithmetic [1], and the $(k-1)$th level of the weak EXP hierarchy for the fragment with k quantifier blocks [6]. The best known lower bound has been Π_2^{P}, established recently by the authors for Π_2-instances of QIP [3, Sec. 4.2].

It may be surprising, and certainly was to the authors, that the complexity of QIP, a natural decision problem, has not yet been established. The main reason is probably that standard quantifier-elimination and automata-based techniques—which are at the core of decision procedures for Presburger arithmetic—fail to yield tight upper bounds for QIP:

- Weispfenning shows that quantifier-elimination procedures for Presburger arithmetic run in time $2^{O(|\Phi|^{(4j)^k})}$ [17, Thm. 2.1], where $|\Phi|$ denotes the size of an input formula Φ with k quantifier blocks and at most j variables in each quantifier block, and that this upper bound is essentially tight [18, Thm. 3.1]. In particular, even the NP upper bound for standard integer programming instances (Σ_1-IP) cannot be obtained by quantifier elimination.
- Automata-based decision procedures for Presburger arithmetic do not suffice either to obtain the bounds for QIP that we establish in this paper. Klaedtke shows [9, Thm. 4.6] that the size of the minimal deterministic finite automaton (DFA) for a formula Φ is upper-bounded by $2^{|\Phi|^{(j+1)^{(k+4)}}}$, which does not give any complexity bounds asymptotically better than those obtained via quantifier elimination.
- Yet another approach to QIP is to construct the semi-linear representation of the set of solutions to the system of linear inequalities of the matrix formula, and then to repeatedly project and complement this set. By an application of [2, Thm. 21], this approach gives a Π_2^{P} upper bound for the Π_2-fragment of QIP; however, as every complementation step increases the number of generators of semi-linear sets by one exponential, this approach would only yield a non-elementary upper bound for general QIP instances and fail to place fragments with bounded alternation depth inside PSPACE.

Our main results are, in short, obtained by means of a new quantifier elimination procedure on *hybrid linear sets*, which are semi-linear sets that represent sets of solutions to systems of linear inequalities. While *existential* projection ($L \mapsto \{x : \exists y.\ (x, y) \in L\}$) is a trivial operation on semi-linear sets (in generator representation), in this paper we define a dual operation, which we call *universal projection* ($L \mapsto \{x : \forall y.\ (x, y) \in L\}$), and show that its application enables us to eliminate blocks of universal quantifiers without resorting to double complementation ($\forall = \neg\exists\neg$; this would lead to a non-elementary blowup). We spell out (these and other) results of the paper in more detail in Section 3 and outline the techniques in Section 4.

Concurrently with our work and building upon a theorem of Kannan [7], Nguyen and Pak [11] have shown that Presburger arithmetic with fixed number of variables *and* fixed Boolean structure of the matrix formula (and, by necessity, where the total number of occurrences of atomic predicates is fixed) can be solved in polynomial time.

2 Preliminaries

By $\mathbb{Z}$ and $\mathbb{N}$ we denote the sets of integers and non-negative integers, respectively. Given sets X and Y, we denote by $X \Rightarrow Y$ the set of all functions with domain X and co-domain Y. Let $\mathcal{X}$ be a countably infinite set of first-order variables, and with no loss of generality assume some total ordering $\prec$ on $\mathcal{X}$. Given a finite set $X \subseteq \mathcal{X}$, an *X-indexed integer vector* is a function $\boldsymbol{v} \in (X \Rightarrow \mathbb{Z})$, and an *$X$-indexed non-negative integer vector* is a function $\boldsymbol{v} \in (X \Rightarrow \mathbb{N})$. We often call $\boldsymbol{v}$ just an *integer vector* respectively a *(non-negative) vector* when X is clear from the context. Due to the total ordering on $\mathcal{X}$, we can interchangeably write $\boldsymbol{v}$ as a tuple $(v_1, \ldots, v_n) \in \mathbb{Z}^n$ such that $n = |X|$. We denote by $\boldsymbol{e}_i$ the ith unit vector (mapping the ith variable to 1 and all other variables to 0). Addition and multiplication of a vector by a scalar value are defined component-wise. Given a set of non-negative vectors $V \subseteq \mathbb{N}^n$, its *complement* is defined as $\overline{V} := \{\boldsymbol{w} \in \mathbb{N}^n : \boldsymbol{w} \notin V\}$.

A *vector of (first-order) variables over* $X \subseteq \mathcal{X}$ is a tuple $\boldsymbol{y} = (y_1, \ldots, y_\ell) \in X^\ell$ such that each $y_i \in X$ and $y_i \prec y_{i+1}$. For $\boldsymbol{v}_i \in (X_i \Rightarrow \mathbb{Z})$, $i \in \{1, 2\}$, with $X_1 \cap X_2 = \emptyset$, by $\boldsymbol{v}_1 \circ \boldsymbol{v}_2$ we denote the vector from $(X_1 \cup X_2) \Rightarrow \mathbb{Z}$ that agrees with $\boldsymbol{v}_i$ on X_i for both $i \in \{1, 2\}$. Given a vector $\boldsymbol{v} \in (X \Rightarrow \mathbb{N})$ and a vector of variables $\boldsymbol{y} = (y_1, \ldots, y_\ell) \in X^\ell$, the *projection of $\boldsymbol{v}$ removing variables $\boldsymbol{y}$* is the vector $\pi_{\boldsymbol{y}}(\boldsymbol{v}) \in ((X \setminus \{y_1, \ldots, y_\ell\}) \Rightarrow \mathbb{N})$ such that $\pi_{\boldsymbol{y}}(\boldsymbol{v})(x) := \boldsymbol{v}(x)$ for all $x \in X \setminus \{y_1, \ldots, y_\ell\}$. This definition of projection naturally extends to sets of vectors:

$$\pi_{\boldsymbol{y}}(V) := \bigcup_{\boldsymbol{v} \in V} \{\pi_{\boldsymbol{y}}(\boldsymbol{v})\} = \{\boldsymbol{v}_1 : \text{there is a } \boldsymbol{v}_2 \in (\{y_1, \ldots, y_\ell\} \Rightarrow \mathbb{N}) \text{ such that } \boldsymbol{v}_1 \circ \boldsymbol{v}_2 \in V\}.$$

For sets of vectors $V \subseteq (X \Rightarrow \mathbb{N})$, we additionally define the *universal projection*

$$\pi^*_{\boldsymbol{y}}(V) := \overline{\pi_{\boldsymbol{y}}(\overline{V})} = \{\boldsymbol{v}_1 : \text{for all } \boldsymbol{v}_2 \in (\{y_1, \ldots, y_\ell\} \Rightarrow \mathbb{N}) \text{ the vector } \boldsymbol{v}_1 \circ \boldsymbol{v}_2 \text{ is in } V\}.$$

For a vector $\boldsymbol{v} \in \mathbb{Z}^n$, we denote by $\|\boldsymbol{v}\| := \max\{\max_{x \in X} |\boldsymbol{v}(x)|, 2\}$ the *maximum norm* of $\boldsymbol{v}$. For $V \subseteq \mathbb{Z}^n$, we define $\|V\| := \max_{\boldsymbol{v} \in V} \|\boldsymbol{v}\|$. For a matrix A, we define $\|A\|$ to be the norm of its set of column vectors.

Quantified integer programming (QIP). Let A be an $n \times m$ integer matrix, $\boldsymbol{x} = (x_1, \ldots, x_m) \in X^m$ a vector of first-order variables for some finite $X \subseteq \mathcal{X}$, and $\boldsymbol{c} \in \mathbb{Z}^n$. We call $\mathfrak{S} \colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ a *system of linear inequalities*. A *solution* to $\mathfrak{S}$ is a vector $\boldsymbol{v} \in (X \Rightarrow \mathbb{Z})$ such that $A \cdot \boldsymbol{v} \geq \boldsymbol{c}$, where "$\geq$" is interpreted component-wise. We denote by $[\![\mathfrak{S}]\!] \subseteq (X \Rightarrow \mathbb{N})$ the set of *all non-negative solutions* to $\mathfrak{S}$.

Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ be vectors of first-order variables over disjoint sets of variables $X_1, \ldots, X_k$, and let $\mathfrak{S} \colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ be a system of linear inequalities. A *formula of* QIP is given by

$$\psi = \mathrm{Q}_k \boldsymbol{x}_k .\ \mathrm{Q}_{k-1} \boldsymbol{x}_{k-1} \ \ldots\ \mathrm{Q}_1 \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \geq \boldsymbol{c},$$

where $\mathfrak{S} \colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ is a system of linear inequalities as above, $Q_i \in \{\exists, \forall\}$, and $Q_i \neq Q_{i+1}$ for all $1 \leq i < k$, i.e., quantifiers alternate between blocks of variables. The *size* $|\psi|$ of ψ is the number of bits required to write down ψ, where we assume binary encoding of numbers, and also that $|\psi| \geq \max\{2, n + m, \log\|A\|, \log\|\boldsymbol{c}\|\}$. The set $[\![\psi]\!] \subseteq (X \setminus (X_1 \cup \cdots \cup X_k) \Rightarrow \mathbb{N})$ of *non-negative solutions* to ψ is inductively defined as follows:

- for $k = 0$, $[\![\psi]\!] := [\![\mathfrak{S}]\!]$;
- for $k > 0$ and $\psi = \exists \boldsymbol{x}_k . \psi_k$, $[\![\psi]\!] := \pi_{\boldsymbol{x}_k} [\![\psi_k]\!]$; and
- for $k > 0$ and $\psi = \forall \boldsymbol{x}_k . \psi_k$, $[\![\psi]\!] := \pi^*_{\boldsymbol{x}_k} [\![\psi_k]\!]$.

A set $M \subseteq (X \Rightarrow \mathbb{N})$ is QIP-*definable* if there is a QIP-formula ψ such that $M = [\![\psi]\!]$. Whenever $X \subseteq X_1 \cup \dots \cup X_k$, we say that ψ is a *sentence*. In this case, ψ is *valid* if $[\![\psi]\!] = \{\top\}$ where $\top$ denotes the unique function from $\emptyset$ to $\mathbb{N}$, and *invalid* if $[\![\psi]\!] = \emptyset$. If $X \setminus (X_1 \cup \dots \cup X_k) = Y = \{y_1, \dots, y_m\}$, we write $\psi(y_1, \dots, y_m)$ to indicate that ψ is *open* in Y. Given $a_1, \dots, a_m \in \mathbb{N}$, we write $\psi[a_1/x_1, \dots, a_m/x_m]$ to denote the instance of QIP obtained from replacing every occurrence of x_i by a_i in $\mathfrak{S}$. We say that two QIP formulas ψ and ϕ are *equivalent* if $[\![\psi]\!] = [\![\phi]\!]$; note that we may always assume with no loss of generality that ψ and ϕ are open in the same set of variables.

A *(valid) instance* of the QIP problem is a (valid) sentence ψ. We call such a ψ an instance of Σ_k-IP if $Q_k = \exists$, and an instance of Π_k-IP if $Q_k = \forall$. The *alternation depth* of ψ is the number k of quantifier blocks.

Hybrid linear and semi-linear sets. Given finite sets $B, P = \{\boldsymbol{p}_1, \dots, \boldsymbol{p}_n\} \subseteq \mathbb{N}^m$ called *base* and *period vectors*, the *hybrid linear set generated by B and P* is the set

$$L(B, P) := \{\boldsymbol{b} + \lambda_1 \cdot \boldsymbol{p}_1 + \dots + \lambda_n \cdot \boldsymbol{p}_n : \boldsymbol{b} \in B, \lambda_i \in \mathbb{N}, 1 \le i \le n\}\,.$$

The representation of $L(B, P)$ as the pair B, P (written explicitly) is called the *generator representation*. If B is singleton then $L(B, P)$ is called a *linear set*; a finite union of (hybrid) linear sets is called a *semi-linear set*. For a hybrid linear set in the generator representation $L = L(B, P)$, we denote $\|L\| := \max(\max\|B\|, \max\|P\|)$.

Hybrid linear sets represent sets of solutions to systems of linear inequalities and equalities. The following bounds on the norm in the generator representation follow from [12, Cor. 1] and [2, Prop. 4].

▶ **Proposition 1.** *Let $\mathfrak{S}\colon A \cdot \boldsymbol{x} \ge \boldsymbol{c}$ be a system of linear inequalities such that A is an $n \times m$ integer matrix. Then $[\![\mathfrak{S}]\!] = L(B, P)$ such that $\|B\|, \|P\| \le (m \cdot \|A\| + \|\boldsymbol{c}\| + 2)^{n+m}$.*

3 Summary

The main result of this paper is the following theorem.

▶ **Theorem 2.** Σ_k-IP *is complete for Σ_k^{P} if k is odd, and* Π_k-IP *is complete for Π_k^{P} if k is even.*

What happens if the parity of k is different? In this case the innermost quantifiers are universal, and it turns out that they can be eliminated in a trivial way.

▶ **Corollary 3.** Σ_{k+1}-IP *is complete for Σ_k^{P} if k is odd, and* Π_{k+1}-IP *is complete for Π_k^{P} if k is even.*

The lower bound of Theorem 2 is proved by a reduction from an alternating version of the subset sum problem, which is essentially shown complete for the respective levels of the polynomial-time hierarchy by Travers [15]. Our reduction and more details are given in Section 7.

The upper bound of Theorem 2 is more challenging. Note that in the well-known case of Σ_1-IP, i.e., of the standard integer programming, in order to prove membership of the problem in NP, one needs to obtain polynomial upper bounds on the bit size of minimal solutions to systems of integer linear inequalities. Such bounds were derived by, e.g., von zur Gathen and Sieveking [16]. In our work, we build upon these bounds and generalize them from Σ_1-IP instances to QIP instances.

▶ **Proposition 4** (small witness property). *For a* QIP *instance ψ of the form* (1) *with k quantifier blocks, the validity of ψ does not change if variables of the vector $\boldsymbol{x}_k$ (bound by the quantifiers of the outermost block) are interpreted over $[0, M-1]$ instead of $\mathbb{N}$, where $\log M = |\psi|^{O(k)}$.*

The domains of other variables can then be bounded in turn as follows—which places QIP with fixed alternation depth into PH.

▶ **Proposition 5** (relativization-type theorem). *For a* QIP *instance ψ of the form* (1) *with k quantifier blocks, the validity of ψ does not change if, for each $i \in [1, k]$, all variables of the vector $\boldsymbol{x}_i$ (bound by the quantifiers of the ith innermost block) are interpreted over $[0, M_i - 1]$ instead of $\mathbb{N}$, where $\log M_i = |\psi|^{O(2k-i)}$ and the constant of $O(\cdot)$ is independent of ψ, k, and i.*

Let us point out that in Proposition 5 it is not possible to substitute $[0, M-1]$ for the range of *all* variables; not only using $M = \max M_i$, but in fact using any finite M. For example, the sentence $\forall x.\ \exists y : y = x + 1$ is true if x and y are interpreted in $\mathbb{N}$, but false if they are interpreted in any finite segment $[0, M-1]$.

▶ Remark 6. The last observation, of course, also holds for Presburger arithmetic in general: any relativization-type theorem (analogous to Proposition 5) must assign different ranges to variables from different quantifier blocks; for instance, this reveals a flaw in the formulation of the relativization-type Theorem 2.2 in [17].

Notice that our small witness property (Proposition 4) is specific to QIP, in the sense that its bound is smaller by one exponential compared to its analogue for general Presburger formulas [17, Thm. 2.2] (the latter is, in fact, tight, as shown implicitly in, e.g., [5, 6]). At the core of our small witness property is a new quantifier elimination procedure for QIP:

▶ **Proposition 7** (quantifier elimination). *Given a* QIP *formula $\phi(\boldsymbol{x})$ with alternation depth k, there exists an equivalent Σ_1-IP formula $\phi'(\boldsymbol{x})$ with at most $2^{|\psi|^{O(k)}}$ existentially quantified variables and numbers of absolute value bounded by $2^{|\psi|^{O(k)}}$.*

The ideas behind Propositions 4 and 7 are outlined in the following Section 4.

Further results. Our results give a uniform upper bound for the general QIP problem, where the number of quantifier blocks can be unbounded. For such a QIP instance, our relativization-type theorem (Proposition 5) suggests doubly exponential ranges for all variables, which places QIP in the complexity class $\mathsf{STA}(*, 2^{n^{O(1)}}, n)$, as $k \le n$. The best lower bound is PSPACE, by the arguments of Section 7.

Another by-product of our techniques is a pseudo-polynomial algorithm for QIP in which the total number of variables is fixed and the matrix formula is $A \cdot \boldsymbol{x} = \boldsymbol{c}$ instead of $A \cdot \boldsymbol{x} \ge \boldsymbol{c}$.

In terms of auxiliary techniques, on the way to our quantifier elimination procedure for QIP we discover (in Sections 5 and 6) some new properties of hybrid linear sets. In particular, these properties enable us to find, as a side result, a polynomial-time algorithm for universality of hybrid linear sets in the generator representation, even if all input numbers are written in binary (Proposition 18 in Section 5).

Finally, our results extend in a natural way to the version of quantified integer programming where all variables are interpreted over $\mathbb{Z}$ instead of over $\mathbb{N}$: the results of Theorem 2 and Corollary 3 still hold.

4 Main ideas

As explained in Section 3, bounding the range of the outermost quantifier is the main technical task in our development. In this section we explain how to do this, thus sketching the ideas behind both the small witness property (Proposition 4) and the quantifier elimination procedure (Proposition 7).

Suppose we start with a QIP instance ψ of the form (1); to find a suitable upper bound M_k for the range of the $\boldsymbol{x}_k$ variables of ψ, we will compute generator representations for the sets of models of formulas

$$\psi_j(\boldsymbol{x}_k, \dots, \boldsymbol{x}_{j+1}) = \mathrm{Q}_j \boldsymbol{x}_j \, \dots \, \forall \boldsymbol{x}_2 . \, \exists \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \geq \boldsymbol{c}$$

for all $j \in [0, k]$, where, as previously, $\boldsymbol{x}$ is the concatenation of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$. For each value of the parameter j, we will find upper bounds on the integers appearing in these representations, starting with $j = 0$ and culminating with $j = k$. The upper bound for the value of parameter $j = k$ will be a valid choice for M_k.

Let us now describe this computation in more detail. Consider a simple abstract example, a Σ_3-IP instance with 3 variables, $\psi \colon \exists x. \, \forall y. \, \exists z : A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ where $\boldsymbol{x} = (x, y, z)$. Let $L_0 \subseteq \mathbb{N}^3$ be the set of all models of $\psi_0 \colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}$; this is a hybrid linear set—denote it $L(C_0, Q_0)$—with $\|C_0\|$, $\|Q_0\|$ upper-bounded by a polynomial in $\|A\|, \|\boldsymbol{c}\|$ with degree at most the size of ψ (see, e.g., Proposition 1). It follows that $\log\|C_0\|$ and $\log\|Q_0\|$ are polynomial in the size of ψ. It is clear that the the set $L_1 = [\![\psi_1]\!] = \{(x, y) \in \mathbb{N}^2 : \text{there exists a } z \in \mathbb{N} \text{ such that } (x, y, z) \in L_0\}$ is simply a projection of $L(C_0, Q_0)$, and in particular $L_1 = L(C, Q)$ where the sets C and Q are obtained by removing z-coordinates from all vectors in C_0 and Q_0, respectively. Hence, $\log\|C\|$ and $\log\|Q\|$ are also polynomial in the size of ψ. (This will, of course, work for all occurrences of the existential quantifier in ψ, including $\exists x$ in our example; but we will need to handle the universal quantifier $\forall y$ before handling $\exists x$.)

The next step is to transform the generator representation $L(C, Q)$ of the set $L_1 = [\![\psi_1]\!]$ into a generator representation of the set

$$L_2 = [\![\psi_2]\!] = \{x \in \mathbb{N} : \text{for all } y \in \mathbb{N} \text{ it holds that } (x, y) \in L_1\}.$$

This set L_2 is the *universal projection* of $L(C, Q)$: $L_2 = \pi^*_y(L(C, Q))$; cf. Section 2. As the main technical contribution of the present paper, we show that, in general, (i) universal projections of hybrid linear sets are hybrid linear sets themselves and that (ii) universal projection as an operation on hybrid linear sets can only lead to a moderate increase in the magnitude of generators. (These results are summarized in Proposition 11 below. For the usual projection, such facts are obvious.)

We now briefly introduce the techniques that we develop for handling the universal projection. Define for each $y \in \mathbb{N}$ the cross section $S(y) = \{x \in \mathbb{N} : (x, y) \in L_1\}$, then

$$L_2 = \bigcap_{y \in \mathbb{N}} S(y) \tag{2}$$

by definition. Each set $S(y)$ is a semi-linear set (and, in fact, a hybrid linear set—because it is essentially the intersection of two hybrid linear sets, see Lemma 15, and such intersections are hybrid linear sets themselves, see, e.g., [2, Theorem 6]), but the intersection in (2) is infinite, and, in general, an infinite intersection of semi-linear sets does not have to be semi-linear.[3] However, we prove (in Section 5) the following lemma, which is our first and key insight:

[3] For every $n \geq 1$, consider the hybrid linear set $L_n = \mathbb{N} \setminus \{0, n\} = L([1, n-1] \cup \{2n\}, \{n\})$. Given any $A \subseteq \mathbb{N}$, the intersection $\bigcap_{n \in A} L_n = \mathbb{N} \setminus (\{0\} \cup A)$ is only semi-linear (i.e., ultimately periodic) if so is A.

▶ **Lemma 8.** *Let $L = L(C, Q) \subseteq \mathbb{N}^m$ be a hybrid linear set with $C, Q \subseteq \mathbb{N}^m$. Let the components of vectors be indexed by m variables X, let $U \subseteq X$, $|U| = s$, and suppose $\boldsymbol{u}$ is the corresponding vector of variables. Then the following statements hold:*

- *If, for some variable $u_i \in U$, the set Q contains no multiple of the unit vector $\boldsymbol{e}_i$ associated with u_i, then $\pi^*_{\boldsymbol{u}}(L) = \emptyset$.*
- *Otherwise, denote $a_i = \min\{a : a \cdot \boldsymbol{e}_i \in Q\}$ and $H = \{\boldsymbol{b} \in \mathbb{N}^s : 0 \leq \boldsymbol{b}(u_i) \leq a_i - 1$ for all $u_i \in U\}$. Then*

$$\pi^*_{\boldsymbol{u}}(L) = \bigcap_{\boldsymbol{b} \in H} \pi_{\boldsymbol{u}}\big(L(C, Q) \cap \{\boldsymbol{u} = \boldsymbol{b}\}\big)$$

where $\{\boldsymbol{u} = \boldsymbol{b}\}$ denotes the hybrid linear set $\{\boldsymbol{c} \in \mathbb{N}^m : \boldsymbol{c}(u_i) = \boldsymbol{b}(u_i)$ for all $u_i \in U\}$.

In other words, unless $L_2 = \emptyset$, the intersection in (2) can be made finite without changing its result: $\bigcap_{y \in \mathbb{N}} S(y) = \bigcap_{y < N} S(y)$, where $\log N$ is polynomial in the size of ψ. Since, as we have just mentioned, hybrid linear sets are closed under finite intersections, this shows that the set L_2 is hybrid linear, and, in fact, the following general result follows:

▶ **Proposition 9.** *A set in $\mathbb{N}^m$ is* QIP*-definable iff it is hybrid linear.*

Furthermore, the set L_2 turns out to have a small generator representation as well. Indeed, we first observe that all sets $S(y)$ have representations $L(B_y, P)$ with a common set of periods P and with $\|B_y\|$, $\|P\|$ small if so is $\|y\|$ (Lemma 15 in Section 5). We then prove (in Section 6) the following lemma, which is our second insight:

▶ **Lemma 10.** *Let $L_i = L(C_i, Q)$, $i \in [1, n]$, be hybrid linear sets with $C_i, Q \subseteq \mathbb{N}^m$. The set $S = \bigcap_{i=1}^n L_i$ has a representation $S = L(B, Q)$ where $\|B\| \leq \max_{i \in [1,n]} \|L_i\|^{O(m^3)}$ independently of n.*

In other words, long intersections of hybrid linear sets with a common set of periods preserve small representations, regardless of the number of sets in the intersection. Combining Lemmas 8 and 10, we obtain the following statement:

▶ **Proposition 11.** *Let $L = L(C, Q) \subseteq \mathbb{N}^m$ be a hybrid linear set with $C, Q \subseteq \mathbb{N}^m$. Let the components of vectors be indexed by m variables $\boldsymbol{u}, \boldsymbol{v}$, and suppose the vector $\boldsymbol{u}$ has s variables. Then the universal projection $\pi^*_{\boldsymbol{u}}(L)$ has a representation $L(B, P)$ where $P = \pi_{\boldsymbol{u}}(\{\boldsymbol{q} \in Q : q_1 = \ldots = q_s = 0\})$ and $\|B\| \leq \|L\|^{O(m^5)}$.*

In particular, we conclude that the set $L_2 = \bigcap_{y<N} L(B_y, P)$ has a representation $L(B, P)$ with $\|B\| < M$ where $\log M$ is polynomial in the size of ψ. But note that $\psi = \psi_3$ is true iff $L_2 = [\![\psi_2]\!]$ is non-empty; therefore, the validity of ψ is unchanged if the range of $\exists x$ is changed from $\mathbb{N}$ to $[0, M - 1]$. Thus, in our example the bound M_3 can be chosen as M; it can hence be deduced that a Σ_3^{P} algorithm can handle such instances. The argument for the general case follows the same lines.

5 Universal projection and universality

A semi-linear set in $\mathbb{N}^d$ is called *universal* if it is equal to $\mathbb{N}^d$.

▶ **Example 12.** A one-dimensional hybrid linear set $L = L(B, P) \subseteq \mathbb{N}$ with $B, P \subseteq \mathbb{N}$ is universal iff $P \setminus \{0\} \neq \emptyset$ and L contains the integer segment $[0, k - 1]$ where $k = \min P \setminus \{0\}$. Indeed, the right-to-left direction is immediate: if L satisfies the conditions above, then $\mathbb{N} = L([0, k - 1], \{k\}) \subseteq L$. For the left-to-right direction, suppose $L = \mathbb{N}$. First observe that the set $P \setminus \{0\}$ is non-empty because L is infinite. Therefore, $k > 0$ is well-defined. Second, as $L = \mathbb{N}$, the set L contains all natural numbers, in particular those in $[0, k - 1]$.

The following lemma generalizes Example 12; recall that $\boldsymbol{e}_i$ denotes the ith unit vector.

▶ **Lemma 13.** *A hybrid linear set $L = L(B, P) \subseteq \mathbb{N}^m$ with $B, P \subseteq \mathbb{N}^m$ is universal iff P contains vectors $a_i \cdot \boldsymbol{e}_i$ for some $a_i > 0$, for every $i \in [1, m]$, and L contains the box $H = [0, a_1 - 1] \times \ldots \times [0, a_m - 1]$.*

Proof. The right-to-left direction is immediate: if L satisfies the conditions of the lemma, then $\mathbb{N}^m = L(H, \{a_1 \cdot \boldsymbol{e}_1, \ldots, a_m \cdot \boldsymbol{e}_m\}) \subseteq L$. For the left-to-right direction, suppose $L = \mathbb{N}^m$. We first prove that, for each $i \in [1, m]$, the set of periods P contains a vector $a_i \cdot \boldsymbol{e}_i$ with $a_i > 0$. Assume without loss of generality that $i = 1$ and denote $N = \mathbb{N} \times \boldsymbol{0} \subseteq \mathbb{N}^m$. Since L is universal (and $\mathbb{Q}_{\geq 0} \times \boldsymbol{0}$ is a face of $\mathbb{Q}^m_{\geq 0}$), $N = L(B, P) \cap N \subseteq L(B \cap N, P \cap N)$. Therefore, the set $P \cap N$ contains at least one vector $a_1 \cdot \boldsymbol{e}_1$ with $a_1 > 0$, otherwise the set N would be finite. Hence, P contains $a_1 \cdot \boldsymbol{e}_1, \ldots, a_m \cdot \boldsymbol{e}_m$ with all $a_i > 0$. It now remains to note that, as $L = \mathbb{N}^m$, the set L contains all nonnegative integer vectors, in particular those in H. This completes the proof. ◀

▶ Remark 14. If $m = 1$, then in the statement of Lemma 13, the condition $H \subseteq L(B, P)$ is equivalent to the condition $H \subseteq B$, as long as H is defined using the *shortest* vector $a_1 \cdot \boldsymbol{e}_1$ in $P \setminus \{\boldsymbol{0}\}$. For $m \geq 2$, this is no longer the case.

▶ **Lemma 15.** *Suppose $L = L(C, Q) \subseteq \mathbb{N}^m$ and $M = L(D, E) \subseteq \mathbb{N}^m$ where $E = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_s\}$. Then the set $L \cap M$ has a representation $L(B, P)$ where $P = \{\boldsymbol{q} \in Q : q_{s+1} = \ldots = q_m = 0\}$ and $\|B\| \leq \|L\|^{O(m^2)} \cdot \|M\|^{O(m)}$.*

We can now restate and prove Lemma 8, which appeared previously in Section 4.

▶ **Lemma 8.** *Let $L = L(C, Q) \subseteq \mathbb{N}^m$ be a hybrid linear set with $C, Q \subseteq \mathbb{N}^m$. Let the components of vectors be indexed by m variables X, let $U \subseteq X$, $|U| = s$, and suppose $\boldsymbol{u}$ is the corresponding vector of variables. Then the following statements hold:*

- *If, for some variable $u_i \in U$, the set Q contains no multiple of the unit vector $\boldsymbol{e}_i$ associated with u_i, then $\pi^*_{\boldsymbol{u}}(L) = \emptyset$.*
- *Otherwise, denote $a_i = \min\{a : a \cdot \boldsymbol{e}_i \in Q\}$ and $H = \{\boldsymbol{b} \in \mathbb{N}^s : 0 \leq \boldsymbol{b}(u_i) \leq a_i - 1$ for all $u_i \in U\}$. Then*

  $$\pi^*_{\boldsymbol{u}}(L) = \bigcap_{\boldsymbol{b} \in H} \pi_{\boldsymbol{u}}\big(L(C, Q) \cap \{\boldsymbol{u} = \boldsymbol{b}\}\big)$$

  where $\{\boldsymbol{u} = \boldsymbol{b}\}$ denotes the hybrid linear set $\{\boldsymbol{c} \in \mathbb{N}^m : \boldsymbol{c}(u_i) = \boldsymbol{b}(u_i)$ for all $u_i \in U\}$.

Proof. Denote $V = X \setminus U$; we will abuse notation and let symbols $\boldsymbol{u}$ and $\boldsymbol{v}$ refer to U- and V-indexed integer vectors (wherever this creates no confusion). By definition, a vector $\boldsymbol{v}^*$ belongs to $\pi^*_{\boldsymbol{u}}(L)$ if and only if for all $\boldsymbol{u}$ the vector $(\boldsymbol{u}, \boldsymbol{v}^*)$ belongs to L. This condition is equivalent to the requirement that

$$L \cap \{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{N}^m : \boldsymbol{v} = \boldsymbol{v}^*\} = \{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{N}^m : \boldsymbol{v} = \boldsymbol{v}^*\}. \tag{3}$$

Note that $\{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{N}^m : \boldsymbol{v} = \boldsymbol{v}^*\} = L((\boldsymbol{0}, \boldsymbol{v}^*), E)$ where E is the set of all unit vectors associated with variables $\boldsymbol{u}$. We now apply Lemma 15: $L \cap L((\boldsymbol{0}, \boldsymbol{v}^*), E) = L(D_{\boldsymbol{v}^*}, R)$ where $R = \{\boldsymbol{q} = (\boldsymbol{u}, \boldsymbol{v}) \in Q : \boldsymbol{v} = \boldsymbol{0}\}$. Now the requirement (3) has the form $L(D_{\boldsymbol{v}^*}, R) = \{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{N}^m : \boldsymbol{v} = \boldsymbol{v}^*\}$ and, by Lemma 13, is equivalent to the requirement that, first, the set R contains some multiple of the unit vector, $a_i \cdot \boldsymbol{e}_i$ for some $a_i > 0$, associated with each variable $u_i \in U$, and, second, the set $L(D_{\boldsymbol{v}^*}, R)$ contains the box

$$H(\boldsymbol{v}^*) = \{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{N}^m : \boldsymbol{v} = \boldsymbol{v}^*, 0 \leq u_i \leq a_i - 1 \text{ for all variables } u_i \in U\}.$$

Note that in the statement of Lemma 13 we can always choose $a_i \cdot \boldsymbol{e}_i$ to be the shortest vectors of the required form in R; expanding the definition of R then gives

$$a_i = \min\{a : a \cdot \boldsymbol{e}_i \in Q\} \qquad \text{for each variable } u_i \in U. \tag{4}$$

We now make the following observations. First, the set R does not depend on the vector $\boldsymbol{v}^*$, but only on Q and on the way the variables are split into $\boldsymbol{u}$ and $\boldsymbol{v}$. Therefore, the condition that R contains $a_i \cdot \boldsymbol{e}_i$ for some $a_i > 0$ is either satisfied or not satisfied for all $\boldsymbol{v}^*$ simultaneously. In the former case, $\pi^*_{\boldsymbol{u}}(L) = \emptyset$; so it suffices to consider the latter case. We have the following equivalence:

$$\boldsymbol{v}^* \in \pi^*_{\boldsymbol{u}}(L) \quad \text{iff} \quad (\boldsymbol{u}, \boldsymbol{v}^*) \in L(D_{\boldsymbol{v}^*}, R) \text{ for all } \boldsymbol{u} \in H$$

where $H = \{\boldsymbol{u} : 0 \le u_i \le a_i - 1 \text{ for all variables } u_i \in U\}$ and a_i are as defined in (4). Since $L(D_{\boldsymbol{v}^*}, R)$ was chosen as $L \cap \{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{N}^m : \boldsymbol{v} = \boldsymbol{v}^*\}$, this is the same as

$$\boldsymbol{v}^* \in \pi^*_{\boldsymbol{u}}(L) \quad \text{iff} \quad (\boldsymbol{u}, \boldsymbol{v}^*) \in L \text{ for all } \boldsymbol{u} \in H,$$

and the equation of the lemma follows. ◀

▶ **Example 16.** Consider any set $L = L(C, \{3\,\boldsymbol{e}_2\}) \subseteq \mathbb{N}^2$ with a finite $C \subseteq \mathbb{N}^2$. Its universal projection $L' = \pi^*_y(L) = \{x : (x, y) \in L \text{ for all } y \in \mathbb{N}\}$ can be obtained by taking cross sections $S_b = \{x : (x, b) \in L\}$ for $b = 0, 1, 2$, removing the y coordinate, and intersecting the results: $L' = \pi_y(S_0) \cap \pi_y(S_1) \cap \pi_y(S_2)$ where the projection $\pi_y \colon \mathbb{N}^2 \to \mathbb{N}$ removes the y coordinate. So whether or not a specific $a \in \mathbb{N}$ belongs to L' is fully determined by whether the vectors $(a, 0)$, $(a, 1)$, and $(a, 2)$ belong to L. In fact, this conclusion will also hold if instead of L we consider any set $M = L(C, \{3\,\boldsymbol{e}_2\} \cup Q)$ where Q contains no vectors of the form $a \cdot \boldsymbol{e}_2$.

Intermezzo: Deciding universality of hybrid linear sets

The technique developed above, in fact, enables us to show that universality of hybrid linear sets (given in generator representation) can be decided in polynomial time, even if all numbers are written in binary. Consider the following lemma, which is a more general version of Example 12 and Lemma 13.

▶ **Lemma 17.** *Let $L = L(B, P) \subseteq \mathbb{N}^m$ be a hybrid linear set with $B, P \subseteq \mathbb{N}^m$. Define the set of* shallow points,

$$W = \big\{\, \boldsymbol{w} \in \mathbb{N}^m : \textit{there is no } \boldsymbol{p} \in P \setminus \{\boldsymbol{0}\} \textit{ with } \boldsymbol{w} \ge \boldsymbol{p} \,\big\} = \mathbb{N}^m \setminus \bigcup_{\boldsymbol{p} \in P \setminus \{\boldsymbol{0}\}} (\boldsymbol{p} + \mathbb{N}^m).$$

Then L is universal iff $W \subseteq B$.

Indeed, for Example 12, observe that for $m = 1$ the set W is the integer segment $[0, k-1]$ where $k = \min P \setminus \{0\}$; cf. Remark 14.

For Lemma 13, note that $W \subseteq B$ is only possible if W is finite, which implies that for each $i \in [1, m]$ there is a vector $a_i \cdot \boldsymbol{e}_i \in P$ with $a_i > 0$ (otherwise all such vectors for some given i are in W, and there are infinitely many of them). But then $W \subseteq H = [0, a_1 - 1] \times \ldots \times [0, a_m - 1]$.

▶ **Proposition 18.** *There is a polynomial-time algorithm that takes a hybrid linear set $L(B, P) \subseteq \mathbb{N}^m$, presented as $B, P \subseteq \mathbb{N}^m$ with numbers written in binary, and decides if $L(B, P)$ is universal.*

Proof. By the characterization of Lemma 17, it is sufficient to check if $W \subseteq B$. First check that the necessary condition of Lemma 13 is satisfied: if for some i there is no $a_i \cdot \boldsymbol{e}_i \in P$ with $a_i > 0$, then $L(B, P)$ is not universal. Otherwise consider the Hasse diagram of the partial order $(H, \leq)$, i.e., the directed acyclic graph with vertex set H and all edges $(\boldsymbol{x}, \boldsymbol{y})$ where $\boldsymbol{x} < \boldsymbol{y}$ and there is no $\boldsymbol{z}$ with $\boldsymbol{x} < \boldsymbol{z} < \boldsymbol{y}$. Notice that this graph does not have to be of polynomial size with respect to the input.

Run the depth-first search (DFS) procedure on (a part of) this graph, starting from $\mathbf{0}$ and for each $\boldsymbol{x} \in H$ ordering the outgoing edges $(\boldsymbol{x}, \boldsymbol{y})$ according to the (unique) index $i \in [1, m]$ for which $x_i < y_i$. Whenever the current node is outside W, the algorithm backtracks (observe that the set W is always downward closed, i.e., whenever $\boldsymbol{w} \in W$ and $\boldsymbol{w}' \leq \boldsymbol{w}$, then also $\boldsymbol{w}' \in W$); if it is in W but not in B, the algorithm terminates immediately, reporting that $L(B, P)$ is not universal. If the search finishes, the algorithm concludes that $W \subseteq B$ and reports that $L(B, P)$ is universal. All visited nodes are marked and not re-entered, ensuring that no node is ever visited twice. As all visited notes are checked for inclusion in B, which is given as part of the input, it follows that the running time of the search is proportional to the size of the input, and the entire procedure works in polynomial time. ◀

6 Long intersections

▶ **Lemma 19.** *Let $L_i = L(C_i, Q)$, $i \in [1, n]$, be hybrid linear sets with $C_i, Q \subseteq \mathbb{N}^m$. Suppose the vectors of Q are linearly independent. Then the set $S = \bigcap_{i=1}^n L_i$ has a representation $S = L(B, Q)$ where $\|B\| \leq 2^{O(m \log m)} \cdot \max_{i \in [1,n]} \|L_i\| \cdot \|Q\|^m$ independently of n.*

Proof (sketch). Note that $\bigcap_{i=1}^n L(C_i, Q)$ is the union over all $\boldsymbol{c}_1 \in C_1, \ldots, \boldsymbol{c}_n \in C_n$ of $\bigcap_{i=1}^n L(\boldsymbol{c}_i, Q)$, so we shall assume with no loss of generality that $C_i = \{\boldsymbol{c}_i\}$ for all i.

Define a point lattice $\mathcal{L} = Q \cdot \mathbb{Z}^r = \{Q \cdot \boldsymbol{u} : \boldsymbol{u} \in \mathbb{Z}^r\}$ where $r = |Q|$; see, e.g., [10, Chapter 2]. Vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^m$ are called *congruent* modulo $\mathcal{L}$, written $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{\mathcal{L}}$, if and only if $\boldsymbol{x} - \boldsymbol{y} \in \mathcal{L}$. This congruence splits $\mathbb{Z}^m$ into a disjoint union of equivalence classes, which have the form $\boldsymbol{x} + \mathcal{L}$ where $\boldsymbol{x} \in \mathbb{Z}^m$. Note that the relation $\equiv$ is compatible with addition and subtraction of elements of Q, in the sense that vectors $\boldsymbol{x} \pm \boldsymbol{q}$, $q \in Q$, belong to the same equivalence class as $\boldsymbol{x}$; therefore, $L_i = \boldsymbol{c}_i + Q \cdot \mathbb{N}^r \equiv \boldsymbol{c}_i \pmod{\mathcal{L}}$. Hence, unless the intersection $\bigcap_{i=1}^n L_i$ is empty, it must be the case that $\boldsymbol{c}_i \equiv \boldsymbol{c}_j \pmod{\mathcal{L}}$ for all i, j. We assume in the sequel that this is indeed the case, i.e., all sets L_i are contained in the same equivalence class $\boldsymbol{c}_1 + \mathcal{L}$.

Let us now define the coordinates in $\boldsymbol{c}_1 + \mathcal{L}$ in a natural way. Consider the mapping $\psi \colon \boldsymbol{c}_1 + \mathcal{L} \to \mathbb{Z}^r$ that maps each $\boldsymbol{x}$ into a vector $\boldsymbol{u} = \psi(\boldsymbol{x})$ such that $\boldsymbol{x} = \boldsymbol{c}_1 + Q \cdot \boldsymbol{u}$; note that $\boldsymbol{u}$ exists as long as $\boldsymbol{x} \in \boldsymbol{c}_1 + \mathcal{L}$ and is determined uniquely because the vectors in Q are linearly independent. The mapping ψ is, in fact, a bijection between $\boldsymbol{c}_1 + \mathcal{L}$ and $\mathbb{Z}^r$, so $L_1 \cap \ldots \cap L_n = \psi^{-1}(\psi(L_1) \cap \ldots \psi(L_n))$. Denote $\boldsymbol{f}_i = \psi(\boldsymbol{c}_i)$ and observe that $\psi(L_i) = \psi(\boldsymbol{c}_i) + \mathbb{N}^r$. So a vector $\boldsymbol{v} \in \mathbb{Z}^r$ belongs to the intersection of all $\psi(L_i)$ if and only if $\boldsymbol{v} \geq \boldsymbol{f}_i$ for all $i \in [1, n]$. This condition is satisfied if and only if $\boldsymbol{v} \geq \boldsymbol{f}$ where $\boldsymbol{f}$ is the component-wise maximum of vectors $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$; in other words, $\bigcap_{i=1}^n \psi(L_i) = \boldsymbol{f} + \mathbb{N}^r$ and $L_1 \cap \ldots \cap L_n = L(\psi^{-1}(\boldsymbol{f}), Q)$.

It remains to find an upper bound on $\|\psi^{-1}(\boldsymbol{f})\|$. Note that $\psi^{-1}(\boldsymbol{f}) = \boldsymbol{c}_1 + Q \cdot \boldsymbol{f}$, so $\|\psi^{-1}(\boldsymbol{f})\| \leq \|\boldsymbol{c}_1\| + \|Q \cdot \boldsymbol{f}\|$. Suppose $\boldsymbol{f} = (f^1, \ldots, f^r)$ and $Q = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_r\}$, then $Q \cdot \boldsymbol{f} = f^1 \cdot \boldsymbol{q}_1 + \ldots + f^r \cdot \boldsymbol{q}_r$. Recall that each f^j is, in fact, a component of some $\boldsymbol{f}_i = \psi(\boldsymbol{c}_i)$.

For this $i = i(j)$ it holds that $\boldsymbol{c}_i = \boldsymbol{c}_1 + Q \cdot \boldsymbol{f}_i$, and by [2, Proposition 3] we have

$$|f^j| \le 2^{O(m \log m)} \cdot \max\left(\|\boldsymbol{c}_i - \boldsymbol{c}_1\|, \|Q\|\right) \cdot \|Q\|^{m-1} \quad \text{and}$$
$$\|\psi^{-1}(\boldsymbol{f})\| \le \|C_1\| + m \cdot \max_{j\in[1,r]} \|f^j \cdot \boldsymbol{q}_j\| \le 2^{O(m \log m)} \cdot \max_{i\in[1,n]} \|L_i\| \cdot \|Q\|^m. \qquad ◀$$

We can now restate and prove Lemma 10, which appeared previously in Section 4.

▶ **Lemma 10.** *Let $L_i = L(C_i, Q)$, $i \in [1, n]$, be hybrid linear sets with $C_i, Q \subseteq \mathbb{N}^m$. The set $S = \bigcap_{i=1}^n L_i$ has a representation $S = L(B, Q)$ where $\|B\| \le \max_{i\in[1,n]} \|L_i\|^{O(m^3)}$ independently of n.*

Proof (sketch). We first apply a discrete version of the Carathéodory theorem [2, Proposition 5] to the set L_1, decomposing it into a union of hybrid linear sets with linearly independent periods:

$$L_1 = \bigcup_j M_j \quad \text{where} \quad M_j = L(D_j, Q_j) \quad \text{and} \quad \|D_j\| \le \|C_1\| + (\#Q \cdot \|Q\|)^{O(m)},$$

with each $Q_j \subseteq Q$ a set of linear independent vectors (here and below # denotes the cardinality of a set). The intent is to make it possible to invoke Lemma 19.

Notice that, whereas intersecting two hybrid linear sets L and L' with sets of periods P and $P' \subseteq P$, respectively, will always give a hybrid linear set with the set of periods P' (see, e.g., [2, Theorem 6] and, transitively, Theorem 5.6.1 of [4, p. 180]), this observation would not suffice for our purposes. Indeed, the magnitude of the base vectors in the hybrid linear representation of $L \cap L'$ can still increase compared to the magnitude of the base vectors of L and L'; and so $n - 1$ consecutive applications of this operation would lead to a blowup in the representation size if n grows. Instead of using this observation, we will rely on Lemma 19 to defeat the effect of large n, and will use another trick to make its application possible.

Indeed, observe that

$$L_1 \cap L_2 \cap \ldots \cap L_n = \bigcup_j M_j \cap L_2 \cap \ldots \cap L_n = \bigcup_j (M_j \cap L_2) \cap \ldots \cap (M_j \cap L_n).$$

Since the sets of periods of M_j and L_i are Q_j and Q, respectively, it follows by [2, Theorem 6] that each $M_j \cap L_i$ is a hybrid linear set with representation $L(B_{i,j}, Q_j)$, where

$$\|B_{i,j}\| \le ((\#Q_j + \#Q) \cdot \max(\|M_j\|, \|L_i\|))^{O(m)} \le \max\left(\|C_1\| + (\#Q \cdot \|Q\|)^{O(m)}, \|L_i\|\right)^{O(m)}.$$

But now, for each j, the intersection of $L(B_{i,j}, Q_j)$, $i \in [2, n]$, satisfies the conditions of Lemma 19, and thus can be written as $L(B_j, Q_j)$ with $\|B_j\|$ small with respect to $\|B_{i,j}\|$ and $\|Q_j\|$ (estimations to follow). Now $S = \bigcup_j L(B_j, Q_j)$, and it remains to note that, as $L_i + L(\boldsymbol{0}, Q) = L_i$ for all i, it also holds that $S + L(\boldsymbol{0}, Q) = S$ and hence

$$S = \bigcup_j L(B_j, Q_j) + L(\boldsymbol{0}, Q) = \bigcup_j L(B_j, Q) = L\left(\bigcup_j B_j,\ Q\right), \quad \text{with}$$
$$\|B_j\| \le 2^{O(m \log m)} \cdot \max\left(\max_{i\in[2,n]} \|B_{i,j}\|, \|Q_j\|\right) \cdot \|Q_j\|^m \le \max_{i\in[1,n]} \|L_i\|^{O(m^3)}. \qquad ◀$$

7 Lower bounds

We show lower bounds for QIP and Σ_k-IP via a reduction from a generalisation of the classical SubsetSum problem. For odd k, let $\boldsymbol{a}_k \in \mathbb{N}^{m_k}, \ldots, \boldsymbol{a}_1 \in \mathbb{N}^{m_1}$ be vectors of natural numbers, and let $t \in \mathbb{N}$ be a target. An instance of Σ_k-SubsetSum is a tuple $(\boldsymbol{a}_k, \ldots, \boldsymbol{a}_1, t)$. This instance is a valid instance whenever the following holds:

$$\exists \boldsymbol{x}_k \in \{0,1\}^{m_k}.\ \forall \boldsymbol{x}_{k-1} \in \{0,1\}^{m_{k-1}} \ldots \exists \boldsymbol{x}_1 \in \{0,1\}^{m_1} : \sum_{i=1}^{k} \boldsymbol{a}_i \cdot \boldsymbol{x}_i = t. \tag{5}$$

Thus, Σ_k-SubsetSum can be viewed as the 0–1 variant of Σ_k-IP, i.e., variables are only interpreted over $\{0,1\}$. For even k, Π_k-SubsetSum is defined analogously. When we take the union of Σ_k-SubsetSum for all $k > 0$, we obtain QSubsetSum.

▶ **Proposition 20.** *For every fixed $k > 0$, for odd k Σ_k-SubsetSum is Σ_k^{P}-complete, and for even k Π_k-SubsetSum is Π_k^{P}-complete. QSubsetSum is PSPACE-complete.*

Upper bounds for Σ_k-SubsetSum and QSubsetSum can be obtained trivially. The PSPACE lower bound for QSubsetSum was established by Travers in [15, Lem. 4]. Unfortunately, the construction given in [15] does not directly yield Σ_k^{P} hardness for Σ_k-SubsetSum, as the lower bound for QSubsetSum is shown in [15] by a reduction from 3-CNF QBF in which the alternating quantifiers range over *single* variables, and Σ_k^{P} hardness for 3-CNF k-QBF requires an unbounded number of variables in every quantifier block [13]. It is not difficult to show that the construction from [15] can indeed be adapted in order to yield Σ_k^{P} hardness for Σ_k-SubsetSum for odd k, and likewise for even k.

Proof of lower bounds in Theorem 2

We reduce from Σ_k-SubsetSum and show how to transform an instance given as (5) into an equivalent instance of Σ_k-IP. Note that the existentially quantified variables do not present an issue, since, for instance, $\boldsymbol{x}_1 \in \{0,1\}^{m_1}$ iff $\boldsymbol{x}_1 \leq \boldsymbol{1}$, i.e., (5) is equivalent to

$$\exists \boldsymbol{x}_k \in \{0,1\}^{m_k}.\ \forall \boldsymbol{x}_{k-1} \in \{0,1\}^{m_{k-1}} \ldots \forall \boldsymbol{x}_2 \in \{0,1\}^{m_2}.\ \exists \boldsymbol{x}_1 : \sum_{i=1}^{k} \boldsymbol{a}_i \cdot \boldsymbol{x}_i = t \wedge \boldsymbol{x}_1 \leq \boldsymbol{1}. \tag{6}$$

The key insight is that, for universally quantified variables, conjunctions of linear integer constraints can express division with remainder using any fixed divisor. In particular, consider

$$\exists \boldsymbol{x}_k \in \{0,1\}^{m_k}.\ \forall \boldsymbol{x}_{k-1} \in \{0,1\}^{m_{k-1}} \ldots \forall \boldsymbol{x}_2.\ \exists \boldsymbol{x}_1.\ \exists \boldsymbol{\lambda} :$$
$$\sum_{i=3}^{k} \boldsymbol{a}_i \cdot \boldsymbol{x}_i + \boldsymbol{a}_2 \cdot (\boldsymbol{x}_2 - 2 \cdot \boldsymbol{\lambda}) + \boldsymbol{a}_1 \cdot \boldsymbol{x}_1 = t \wedge \boldsymbol{x}_1 \leq \boldsymbol{1} \wedge \boldsymbol{0} \leq \boldsymbol{x}_2 - 2 \cdot \boldsymbol{\lambda} \leq \boldsymbol{1}. \tag{7}$$

We claim that the sentences (6) and (7) are equivalent. First, no matter what $\boldsymbol{x}_2$ is, $\boldsymbol{\lambda}$ has to be $\lfloor \boldsymbol{x}_2/2 \rfloor$ in order to satisfy the last constraint of (7). If sentence (6) is true, then (7) is also true. Indeed, if $\boldsymbol{x}_2 \in \{0,1\}^{m_2}$, then we can choose $\boldsymbol{\lambda} = \boldsymbol{0}$ and the inequalities become the same as before (and thus, for instance, there is an appropriate $\boldsymbol{x}_1$). Analogously, if $\boldsymbol{x}_2$ is outside $\{0,1\}^m$, then it is the vector $\boldsymbol{x}_2 - 2 \cdot \boldsymbol{\lambda}$ that is in $\{0,1\}^{m_2}$, and for this vector we already know the appropriate $\boldsymbol{x}_1$ from the previous formula. Conversely, suppose the sentence (7) is true, then it is in particular true for all choices $\boldsymbol{x}_2 \in \{0,1\}^{m_2}$ in which case $\boldsymbol{\lambda} = \lfloor \boldsymbol{x}_2/2 \rfloor = \boldsymbol{0}$. Hence, the assignment for $\boldsymbol{x}_1$ chosen in (7) given $\boldsymbol{x}_2$ will also work for (6). This proves the claim.

In fact, the trick above works regardless of how many universal variables we have and at which positions they occur in the quantifier prefix. So we can handle both existential and universal variables and can transform any instance of Σ_k-SubsetSum respectively Π_k-SubsetSum into an equivalent instance of Σ_k-IP respectively Π_k-IP, which yields the desired lower bounds, when variables are interpreted over the natural numbers.

References

1 Leonard Berman. The complexitiy of logical theories. *Theor. Comput. Sci.*, 11:71–77, 1980. doi:10.1016/0304-3975(80)90037-7.

2 Dmitry Chistikov and Christoph Haase. The taming of the semi-linear set. In *Automata, Languages, and Programming, ICALP*, volume 55 of *LIPIcs*, pages 128:1–128:13. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPIcs.ICALP.2016.128.

3 Dmitry Chistikov, Christoph Haase, and Simon Halfon. Context-free commutative grammars with integer counters and resets. *Theor. Comput. Sci.*, pages –, 2017. To appear. doi:10.1016/j.tcs.2016.06.017.

4 Seymour Ginsburg. *The mathematical theory of context-free languages*. McGraw-Hill, 1966.

5 Erich Grädel. Dominoes and the complexity of subclasses of logical theories. *Ann. Pure Appl. Logic*, 43(1):1–30, 1989. doi:10.1016/0168-0072(89)90023-7.

6 Christoph Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *Computer Science Logic and Logic in Computer Science, CSL-LICS*, pages 47:1–47:10. ACM, 2014. doi:10.1145/2603088.2603092.

7 Ravi Kannan. Test sets for integer programs, ∀∃ sentences. In *Polyhedral Combinatorics, Proceedings of a DIMACS Workshop, Morristown, New Jersey, USA, June 12-16, 1989*, pages 39–48, 1990.

8 Richard M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, The IBM Research Symposia Series, pages 85–103. Plenum Press, New York, 1972.

9 Felix Klaedtke. Bounds on the automata size for Presburger arithmetic. *ACM Trans. Comput. Log.*, 9(2):11:1–11:34, 2008. doi:10.1145/1342991.1342995.

10 Jiri Matoušek. *Lectures on discrete geometry*. Graduate texts in mathematics. Springer, 2002. doi:10.1007/978-1-4613-0039-7.

11 Danny Nguyen and Igor Pak. Complexity of short Presburger arithmetic. In *Symposium on the Theory of Computing, STOC*, 2017. To appear. URL: https://arxiv.org/abs/1704.00249.

12 Loïc Pottier. Minimal solutions of linear Diophantine systems: Bounds and algorithms. In *Rewriting Techniques and Applications, RTA*, volume 488 of *Lect. Notes Comp. Sci.*, pages 162–173. Springer, 1991. doi:10.1007/3-540-53904-2_94.

13 Larry J. Stockmeyer. The polynomial-time hierarchy. *Theor. Comput. Sci.*, 3(1):1–22, 1976. doi:10.1016/0304-3975(76)90061-X.

14 K. Subramani. Tractable fragments of Presburger arithmetic. *Theory Comput. Syst.*, 38(5):647–668, 2005. doi:10.1007/s00224-004-1220-0.

15 Stephen D. Travers. The complexity of membership problems for circuits over sets of integers. *Theor. Comput. Sci.*, 369(1-3):211–229, 2006. doi:10.1016/j.tcs.2006.08.017.

16 Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *P. Am. Math. Soc.*, 72(1):155–158, 1978. doi:10.1090/S0002-9939-1978-0500555-0.

17 Volker Weispfenning. The complexity of almost linear Diophantine problems. *J. Symb. Comp.*, 10(5):395–403, 1990. doi:10.1016/S0747-7171(08)80051-X.

18 Volker Weispfenning. Complexity and uniformity of elimination in Presburger arithmetic. In *Symbolic and Algebraic Computation, ISSAC*, pages 48–53. ACM, 1997. doi:10.1145/258726.258746.

A The case of universal innermost quantifier block

▶ **Lemma 21.** *Suppose $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$. Consider a system of linear inequalities $\mathfrak{S}\colon B \cdot \boldsymbol{y} \geq \boldsymbol{c}$ where B and $\boldsymbol{c}$ are a matrix and vector over $\mathbb{K}$ of appropriate sizes, and let Y be the set of variables of $\boldsymbol{y}$. The system $\mathfrak{S}$ is satisfied by all $\boldsymbol{b} \in (Y \Rightarrow \mathbb{K}_{\geq 0})$ if and only if all entries of B are nonnegative and $\mathfrak{S}$ is satisfied by $\boldsymbol{y} = \boldsymbol{0}$, i.e., $\boldsymbol{0} \geq \boldsymbol{c}$.*

Proof. If the matrix B has a negative entry in position (i, j), then by assigning an appropriately large number from $\mathbb{K}_{\geq 0}$ to the corresponding variable $y_j \in Y$, we can falsify the ith inequality, thus transforming any solution to $\mathfrak{S}$ into a non-solution. Therefore, if $\mathfrak{S}$ is satisfied by all $\boldsymbol{b} \in (Y \Rightarrow \mathbb{K}_{\geq 0})$, then all entries of B are nonnegative. But in this case $B \cdot \boldsymbol{b} \geq B \cdot \boldsymbol{0}$, i.e., it is sufficient to check the condition for $\boldsymbol{b} = \boldsymbol{0}$. ◀

Proof of Corollary 3. Any QIP-instance with the innermost universal quantifier block may be reduced to another instance with a decreased alternation depth as follows. Rewrite the quantifier-free part of the instance as the system of inequalities $\mathfrak{S}\colon A \cdot \boldsymbol{x} + B \cdot \boldsymbol{y} \geq \boldsymbol{c}$, where $\boldsymbol{y}$ is the vector of variables bound by the innermost universal quantifiers, and $\boldsymbol{x}$ is the vector of all other variables. Now if B has a negative entry, then the instance is a no-instance of QIP; otherwise replace $\mathfrak{S}$ with $\mathfrak{S}'\colon A \cdot \boldsymbol{x} \geq \boldsymbol{c}$ and remove all variables $\boldsymbol{y}$. The correctness of this transformation follows from Lemma 21. ◀

B Proof of upper bounds in Theorem 2

The overall strategy is simple. We will start with a QIP instance

$$\psi = \mathrm{Q}_k \boldsymbol{x}_k \ \ldots\ \forall \boldsymbol{x}_2.\ \exists \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \geq \boldsymbol{c}$$

where all variables of the vectors $\boldsymbol{x}_k, \ldots, \boldsymbol{x}_1$ are interpreted over $\mathbb{N}$ and $\mathrm{Q}_k = \exists$ if k is odd and $\mathrm{Q}_k = \forall$ if k is even. Our argument will proceed in two steps.

1. *Bounding the range of the outermost quantifier:* We will find an integer M_k such that the validity of ψ does not change if variables of the vector $\boldsymbol{x}_k$ are interpreted over $[0, M_k - 1]$ instead of $\mathbb{N}$.
2. *Propagating bounds inwards:* For each $i = k-1, \ldots, 1$, we will find an integer M_i based on $M_k, \ldots, M_{i+1}$, such that the validity of ψ does not change if variables of the vector $\boldsymbol{x}_k, \ldots, \boldsymbol{x}_i$ are interpreted over $[0, M_k - 1], \ldots, [0, M_i - 1]$ instead of $\mathbb{N}$.

In fact, the bit size of M_k will be upper-bounded by a polynomial in the size of ψ, and so will be the bit size of M_i in the bit sizes of ψ and M_{i+1}. This will imply that the validity of ψ can be decided by an alternating polynomial-time Turing machine that models the game encoded in ψ: it will guess an assignment of a value from $[0, M_i - 1]$ to each variable of $\boldsymbol{x}_i$ for $i = k, \ldots, 1$, alternating between existential and universal modes according to ψ. It will then accept if and only if the combined assignment to $\boldsymbol{x}$ satisfies the quantifier-free formula $A \cdot \boldsymbol{x} \geq \boldsymbol{c}$. This will be a Σ_k^{P} respectively Π_k^{P} algorithm for QIP, depending on the parity of k.

B.1 Proof of Lemma 15

Clearly, $L(C, Q) \cap L(D, E) = \bigcup_{\boldsymbol{c} \in C, \boldsymbol{d} \in D} L(\boldsymbol{c}, Q) \cap L(\boldsymbol{d}, E)$. For fixed $\boldsymbol{c} \in C$ and $\boldsymbol{d} \in D$, consider the systems of equations

$$\mathfrak{S}\colon \boldsymbol{c} + P \cdot \boldsymbol{\lambda} + (Q \setminus P) \cdot \boldsymbol{\mu} = \boldsymbol{d} + E \cdot \boldsymbol{\nu} \quad \text{and}$$
$$\mathfrak{S}_0\colon P \cdot \boldsymbol{\lambda} + (Q \setminus P) \cdot \boldsymbol{\mu} = E \cdot \boldsymbol{\nu}.$$

Let $S = [\![\mathfrak{S}]\!]$ and $S_0 = [\![\mathfrak{S}_0]\!]$. By [2, Prop. 4], $S = L(F, R) = F + L(\mathbf{0}, R)$ and $S_0 = L(\mathbf{0}, R)$ for some F, R; here

$$\|F\| \le ((\#Q + s + 1) \cdot \|Q\| + \|C\| + \|D\| + 1)^m.$$

Suppose that $P = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_t\}$. Denote by π the projection from $\mathbb{N}^m$ to $\mathbb{N}^s$ that removes the coordinates $s+1, \ldots, m$. Let us prove that we can choose $R = \{(\boldsymbol{e}_i, \mathbf{0}, \pi(\boldsymbol{p}_i)) : i \in [1, t]\}$. Indeed, it is easily checked that $L(\mathbf{0}, R) \subseteq S_0$. Conversely, consider an arbitrary solution $(\boldsymbol{\lambda}, \boldsymbol{\mu}, \boldsymbol{\nu})$ to $\mathfrak{S}_0$. Since all vectors of E have zero in components $s+1, \ldots, m$, it is necessary that $\boldsymbol{\mu} = 0$, because each $\boldsymbol{q} \in Q \setminus P$ has at least one non-zero component among $s+1, \ldots, m$. (Note that this argument crucially depends on the non-negativity of the involved vectors and matrices.) But for any given $\boldsymbol{\lambda}$ there is a unique choice of $\boldsymbol{\nu}$ such that $P \cdot \boldsymbol{\lambda} = E \cdot \boldsymbol{\nu}$; in particular, if $\boldsymbol{\lambda} = \sum_{i \in [1,s]} \lambda_i \cdot \boldsymbol{e}_i$, then $\boldsymbol{\nu} = \sum_{i \in [1,s]} \lambda_i \cdot \pi(\boldsymbol{p}_i)$, and therefore $S_0 \subseteq L(\mathbf{0}, R)$.

Now

$$L(\boldsymbol{c}, Q) \cap L(\boldsymbol{d}, E) = \{\boldsymbol{c} + P \cdot \boldsymbol{\lambda} + (Q \setminus P) \cdot \boldsymbol{\mu} : \text{there exists } \boldsymbol{\nu} \text{ such that } (\boldsymbol{\lambda}, \boldsymbol{\mu}, \boldsymbol{\nu}) \in L(F, R)\}.$$

Note that $(\boldsymbol{\lambda}, \boldsymbol{\mu}, \boldsymbol{\nu}) \in L(F, R)$ if and only if

$$(\boldsymbol{\lambda}, \boldsymbol{\mu}, \boldsymbol{\nu}) = (\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3) + \sum_{i \in [1,t]} \alpha_i \cdot (\boldsymbol{e}_i, \mathbf{0}, \pi(\boldsymbol{p}_i))$$

for some $(\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3) \in F$ and $\alpha_i \in \mathbb{N}$. Thus,

$$\begin{aligned} \boldsymbol{c} + P \cdot \boldsymbol{\lambda} + (Q \setminus P) \cdot \boldsymbol{\mu} &= \boldsymbol{c} + P \cdot (\boldsymbol{f}_1 + \sum_{i \in [1,t]} \alpha_i \cdot \boldsymbol{e}_i) + (Q \setminus P) \cdot \boldsymbol{f}_2 \\ &= (\boldsymbol{c} + P \cdot \boldsymbol{f}_1 + (Q \setminus P) \cdot \boldsymbol{f}_2) + P \cdot (\alpha_1, \ldots, \alpha_t)^\top. \end{aligned}$$

This means that $L(\boldsymbol{c}, Q) \cap L(\boldsymbol{d}, E) = L(G, P)$ where

$$G = G(\boldsymbol{c}, \boldsymbol{d}) = \{\boldsymbol{c} + P \cdot \boldsymbol{f}_1 + (Q \setminus P) \cdot \boldsymbol{f}_2 : \text{ there exists } \boldsymbol{f}_3 \text{ such that } (\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3) \in F\}.$$

It remains to note that

$$\begin{aligned} \|G\| &\le \|C\| + \#Q \cdot \|Q\| \cdot \|F\| \\ &\le \|C\| + \#Q \cdot \|Q\| \cdot ((\#Q + s + 1) \cdot \|Q\| + \|C\| + \|D\| + 1)^m \\ &\le \|L\|^{O(m^2)} \cdot \|N\|^{O(m)}. \end{aligned}$$

This implies the required upper bound on $\|B\|$.

B.2 Detailed derivations of bounds from Section 6

For Lemma 19:

The upper bounds on $\|\psi^{-1}(\boldsymbol{f})\|$ are as follows:

$$\begin{aligned} \|\psi^{-1}(\boldsymbol{f})\| &\le \|C_1\| + m \cdot \|f^j \cdot \boldsymbol{q}_j\| \\ &\le \|C_1\| + m \cdot 2^{O(m \log m)} \cdot \max\left(\max_{i \in [1,n]} 2\,\|\boldsymbol{c}_i\|, \|Q\|\right) \cdot \|Q\|^m \\ &\le 2^{O(m \log m)} \cdot \max\left(\max_{i \in [1,n]} \|C_i\|, \|Q\|\right) \cdot \|Q\|^m \\ &\le 2^{O(m \log m)} \cdot \max_{i \in [1,n]} \|L_i\| \cdot \|Q\|^m. \end{aligned}$$

For Lemma 10:

The upper bounds on $\|B_{i,j}\|$ are as follows:

$$\begin{aligned}\|B_{i,j}\| &\le ((\#Q_j + \#Q) \cdot \max(\|M_j\|, \|L_i\|))^{O(m)}\\ &\le (\#Q)^{O(m)} \cdot \max\left(\|C_1\| + (\#Q \cdot \|Q\|)^{O(m)}, \|L_i\|\right)^{O(m)}\\ &\le \max\left(\|C_1\| + (\#Q \cdot \|Q\|)^{O(m)}, \|L_i\|\right)^{O(m)}.\end{aligned}$$

The upper bounds on $\|B_j\|$ are as follows:

$$\begin{aligned}\|B_j\| &\le 2^{O(m \log m)} \cdot \max\left(\max_{i\in[2,n]} \|B_{i,j}\|, \|Q_j\|\right) \cdot \|Q_j\|^m\\ &\le 2^{O(m \log m)} \cdot \max_{i\in[2,n]} \max\left(\|C_1\| + (\#Q \cdot \|Q\|)^{O(m)}, \|L_i\|\right)^{O(m)} \cdot \|Q_j\|^m\\ &\le \max\left(\|C_1\| + (\#Q \cdot \|Q\|)^{O(m)}, \max_{i\in[2,n]} \|L_i\|\right)^{O(m)}\\ &\le \max_{i\in[1,n]} \|L_i\|^{O(m^3)}.\end{aligned}$$

B.3 Proof of Proposition 11

Apply Lemma 8: the set $\pi^*_{\boldsymbol{u}}(L)$, unless it is empty, is an intersection of a finite number of sets of the form $\pi_{\boldsymbol{u}}\big(L(C,Q) \cap \{\boldsymbol{u} = \boldsymbol{b}\}\big)$ where $\boldsymbol{b} \in H = \{\boldsymbol{u} : 0 \le u_i \le a_i - 1$ for all variables u_i among $\boldsymbol{u}\}$ and $a_i = \min\{a : a \cdot \boldsymbol{e}_i \in Q\}$. Notice that the hybrid linear set $\{\boldsymbol{u} = \boldsymbol{b}\}$ has a generator representation with norm $\|\boldsymbol{b}\| \le \|H\| \le \|Q\| \le \|L\|$. By Lemma 15, each set $L(C,Q) \cap \{\boldsymbol{u} = \boldsymbol{b}\}$ has a representation $L(B(\boldsymbol{b}), P)$ where

$$\begin{aligned}&P = \{\boldsymbol{q} = (\boldsymbol{u}, \boldsymbol{v}) \in Q : \boldsymbol{u} = \boldsymbol{0}\} = \{\boldsymbol{q} \in Q : q_1 = \ldots = q_s = 0\} \quad \text{and}\\ &\|B(\boldsymbol{b})\| \le \|L\|^{O(m^2)} \cdot \|\boldsymbol{b}\|^{O(m)} \le \|L\|^{O(m^2)} \cdot \|L\|^{O(m)} \le \|L\|^{O(m^2)}.\end{aligned}$$

As the standard projection cannot increase the norm of a hybrid linear set, the intersection $\pi^*_{\boldsymbol{u}}(L)$ is now an intersection of a finite number of hybrid linear sets with periods $\pi_{\boldsymbol{u}}(P)$ and with norm at most $\|L\|^{O(m^2)}$. But by Lemma 10 such an intersection is a hybrid linear set with the same set of periods and with norm at most

$$\left(\|L\|^{O(m^2)}\right)^{O(m^3)} = \|L\|^{O(m^5)},$$

because the projected sets are in dimension at most m. This completes the proof.

B.4 Proofs of Proposition 4 and 7

The argument follows the plan outlined in Section 4. Start with a QIP instance ψ of the form (1) with k quantifier blocks. To find a suitable upper bound M_k for the range of $\boldsymbol{x}_k$ variables of ψ, we will compute generator representations for the sets of models of formulas

$$\psi_j(\boldsymbol{x}_k, \ldots, \boldsymbol{x}_{j+1}) = \mathrm{Q}_j \boldsymbol{x}_j \ \ldots \ \forall \boldsymbol{x}_2.\ \exists \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \ge \boldsymbol{c}$$

for all $j \in [0,k]$, where, as previously, $\boldsymbol{x}$ is the concatenation of $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$. For each value of the parameter j, we will find upper bounds on the integers appearing in these representations, starting with $j = 0$ and culminating with $j = k$. The upper bound for the value of parameter $j = k$ will be a valid choice for M_k.

By Proposition 1, $[\![\psi_0]\!]$ is a hybrid linear set L with

$$\|L\| \le (m \cdot \|A\| + \|\boldsymbol{c}\| + 2)^{n+m} \le (|\psi| \cdot 2^{|\psi|})^{|\psi|} \le 2^{O(|\psi|^2)}.$$

We now perform a sequence of projections and universal projections on L. It is easy to see that the usual projection cannot increase the norm of a set, and by Proposition 11 the universal projection of a hybrid linear set $N \subseteq \mathbb{N}^\ell$ is a hybrid linear set with norm at most $\|N\|^{O(\ell^5)}$. For the proof of Proposition 4, note that the innermost quantifier is existential, and we apply projections and universal projections following all quantifier blocks except the outermost one. So among the k operations the universal projection is only performed on steps $2, \ldots, 2 \cdot \lfloor (k-1)/2 \rfloor$, i.e., $c = \lfloor (k-1)/2 \rfloor$ many times in total. Suppose ψ has m variables; then as the result of all these consecutive operations we obtain a hybrid linear representation of the set $[\![\psi_{k-1}]\!]$, with norm bounded by

$$\|L\|^{(O(m^5))^c} = \|L\|^{m^{O(c)}} \le 2^{O(|\psi|^2) \cdot m^{O(c)}} \le 2^{|\psi|^{O(k)}}$$

Now, if the outermost quantifier block is existential, then the QIP instance ψ is true iff the hybrid linear set has at least one base vector—and therefore the validity of ψ is unchanged if the variables bound by this quantifier block are interpreted over $[0, M_k - 1]$ where $M_k - 1$ is the norm of the hybrid linear set $[\![\psi_{k-1}]\!]$. Similarly, if the outermost quantifier block is universal, then by Lemma 13 the set $[\![\psi_{k-1}]\!]$ is universal iff it contains all vectors whose norm is bounded by $\|[\![\psi_{k-1}]\!]\|$. Therefore, in both cases all quantifiers of the outermost block can be replaced by bounded quantifiers with range $[0, M_k - 1]$ where $M_k \le 2^{|\psi|^{O(k)}}$.

For the proof of Proposition 7, if the outermost quantifier block is existential, then we perform exactly the same sequence of projections and universal projections as described above (stopping before the outermost block), otherwise we also need to perform the ultimate universal projection—which may increase the norm one more time, so the constant c in the exponent is replaced with $c' = \lfloor k/2 \rfloor$, which is again $O(k)$. The existential quantification of the resulting formula comes from the logical representation of the hybrid linear set—recall that

$$L(B, P) = \{\boldsymbol{x} : \exists \boldsymbol{\lambda}.\ \exists \boldsymbol{\mu}.\ \boldsymbol{x} = B \cdot \boldsymbol{\lambda} + P \cdot \boldsymbol{\mu} \text{ and } \boldsymbol{\lambda} \cdot \boldsymbol{1} = 1\}$$

—and potentially from the outermost block of existential quantifiers in the original formula. It is easily seen that the total number of the existentially quantified variables in the obtained formula will be bounded from above by $|\psi| + \#B + \#P$ where $L(B, P)$ is the representation of the last obtained hybrid linear set. This bound will never exceed

$$\max(\|B\|, \|P\|)^{O(m)} \le 2^{|\psi|^{O(k)}}.$$

B.5 Proof of Proposition 5

Define a sequence of numbers M_i, $i \in [1, k]$, by

$$\log M_i = |\psi|^{\alpha \cdot (2k-i)+\beta} \tag{8}$$

where α and β are positive constants to be fixed later. We will show that these numbers can be used as upper bounds for the ranges of quantifiers depending on i, the index of the quantifier block. Define as previously

$$\psi_j(\boldsymbol{x}_k, \ldots, \boldsymbol{x}_{i+1}) = \mathrm{Q}_j \boldsymbol{x}_j\ \ldots\ \forall \boldsymbol{x}_2.\ \exists \boldsymbol{x}_1 : A \cdot \boldsymbol{x} \ge \boldsymbol{c}$$

for all $i \in [0, k]$, where $\boldsymbol{x}$ is the concatenation of $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$.

We prove the following statement by induction. For every $i \in [1, k]$ and for every tuple of vectors $\boldsymbol{a}_k, \ldots, \boldsymbol{a}_{i+1}$ such that $\|\boldsymbol{a}_j\| < M_j$, $j \in [i+1, k]$, the validity of the closed formula $\psi_i[\boldsymbol{a}_k/\boldsymbol{x}_k, \ldots, \boldsymbol{a}_{i+1}/\boldsymbol{x}_{i+1}]$ does not change if variables bound by the outermost quantifier block of ψ_i (i.e., the variables $\boldsymbol{x}_i$) are interpreted over $[0, M_i - 1]$ instead of $\mathbb{N}$.

The base of the induction is $i = k$. In this case, the statement follows from Proposition 4 if α and β are chosen appropriately. To prove the inductive step, consider the following scenario. In the standard Prover–Refuter game associated with ψ, suppose the variables $\boldsymbol{x}_k, \ldots, \boldsymbol{x}_{i+1}$ have been assigned values $\boldsymbol{a}_k, \ldots, \boldsymbol{a}_{i+1}$. How does the player associated with the ith quantifier block choose the values for $\boldsymbol{x}_i$? Consider the formula $\chi(\boldsymbol{x}_i) = \psi_{i-1}[\boldsymbol{a}_k/\boldsymbol{x}_k, \ldots, \boldsymbol{a}_{i+1}/\boldsymbol{x}_{i+1}]$. Without loss of generality, we may assume that the player picks the assignment for $\boldsymbol{x}_i$ that satisfies χ (respectively does not satisfy χ) and has the smallest possible norm. Recall that by Proposition 9 the set $[\![\psi_{i-1}]\!]$ is hybrid linear, and so is the set

$$A = \{\boldsymbol{x} = (\boldsymbol{x}_k, \ldots, \boldsymbol{x}_1) : \boldsymbol{x}_k = \boldsymbol{a}_k, \ldots, \boldsymbol{x}_{i+1} = \boldsymbol{a}_{i+1}\} = L(\{\boldsymbol{a}\}, E),$$

where $\boldsymbol{a} = (\boldsymbol{a}_k, \ldots, \boldsymbol{a}_{i+1}, \boldsymbol{0})$ and E is the appropriate set of unit vectors. The set $[\![\chi]\!]$ is in fact the projection of the set $[\![\psi_{i-1}]\!] \cap A$, so its norm can be bounded using Lemma 15. The norm of $[\![\psi_{i-1}]\!]$ is essentially bounded in Proposition 4 and does not exceed $2^{|\psi|^{O(k)}}$, and the norm of A is at most M_i by the induction hypothesis. Let m be the total number of variables; then by Lemma 15

$$\begin{aligned}\log\|[\![\chi]\!]\| &\leq O(m^2) \cdot |\psi|^{O(k)} + O(m) \cdot |\psi|^{\alpha \cdot (2k-i)+\beta} \\ &\leq |\psi|^{2+O(1)+O(k)} + |\psi|^{1+O(1)+\alpha \cdot (2k-i)+\beta}.\end{aligned}$$

As $\xi + \eta \leq 2 \max\{\xi, \eta\}$ for any real ξ, η, and since $2 \leq |\psi|$ by our definition of the formula size, it remains to pick α and β such that the following conditions:

$$\begin{aligned}&2 + O(1) + O(k) \leq \alpha \cdot (2k - i + 1) + \beta \quad \text{and} \\ &1 + O(1) + \alpha \cdot (2k - i) + \beta \leq \alpha \cdot (2k - i + 1) + \beta\end{aligned}$$

are satisfied for all k and all $i \in [1, k]$. This will ensure that $\log\|[\![\chi]\!]\|$ is at most $\log M_{i-1} = |\psi|^{\alpha \cdot (2k-i+1)+\beta}$. It is easy to see that such α and β indeed exist. This completes the proof.

C Proof of Lemma 17

We first prove the right-to-left direction. Suppose $W \subseteq B$ and let $\boldsymbol{w}$ be any vector in $\mathbb{N}^m$; we will show that $\boldsymbol{w} \in L$. If $\boldsymbol{w} \in W$, then $\boldsymbol{w} \in B \subseteq L(B, P)$; so we can assume $\boldsymbol{w} \notin W$. In this case there is a $\boldsymbol{p} \in P \setminus \{\boldsymbol{0}\}$ such that $\boldsymbol{w}_0 := \boldsymbol{w} \geq \boldsymbol{p}$; that is, $\boldsymbol{w}_1 := \boldsymbol{w}_0 - \boldsymbol{p} \in \mathbb{N}^m$. Note that $\boldsymbol{w}_0 \in L$ if $\boldsymbol{w}_1 \in L$, and also that $\|\boldsymbol{w}_0\| > \|\boldsymbol{w}_1\|$. Now consider $\boldsymbol{w}_1$: if $\boldsymbol{w}_1 \in W$, then $\boldsymbol{w}_1 \in B \subseteq L$ and we are done, otherwise $\boldsymbol{w}_1 \notin W$ and there is a $\boldsymbol{q} \in P \setminus \{\boldsymbol{0}\}$ such that $\boldsymbol{w}_1 \geq \boldsymbol{q}$; that is, $\boldsymbol{w}_2 := \boldsymbol{w}_1 - \boldsymbol{q} \in \mathbb{N}^m$. Since there can be no infinitely descending chain of numbers in $\mathbb{N}$, $\|\boldsymbol{w}_0\| > \|\boldsymbol{w}_1\| > \ldots > \|\boldsymbol{w}_n\| > \ldots$, this process will terminate with some $\boldsymbol{w}_n \in W$. But then $\boldsymbol{w}_i \in L$ for all $i \leq n$, and in particular $\boldsymbol{w} = \boldsymbol{w}_0 \in L$.

For the left-to-right direction, assume the set L is universal. Consider any vector $\boldsymbol{w} \in W$; as $L = \mathbb{N}^m$, it must be the case that $\boldsymbol{w} \in L$. However, by the definition of W, there is no $\boldsymbol{p} \in P \setminus \{\boldsymbol{0}\}$ with $\boldsymbol{w} \geq \boldsymbol{p}$; therefore, whenever $\boldsymbol{w} = \boldsymbol{b} + \sum \lambda_i \boldsymbol{p}_i$ with $\boldsymbol{b} \in B$, $\lambda_i \in \mathbb{N}$, and $\boldsymbol{p}_i \in P \setminus \{\boldsymbol{0}\}$ for all i, it is necessary that $\lambda_i = 0$ for all i and $\boldsymbol{w} = \boldsymbol{b}$. But then $\boldsymbol{w} \in B$. As this must be true for all $\boldsymbol{w} \in W$, the proof is complete.

D Bounding the ranges of variables in Presburger arithmetic: the general case

Theorem 2.2 in [17] states that, for any prenex sentence in Presburger arithmetic with at most a quantifier blocks, each of length at most b, there exists a constant $c > 0$ such that ϕ is equivalent to the the sentence obtained from ϕ by replacing for the range of every quantifier with

$$[0, M-1] \text{ where } \log M \leq c \cdot |\phi|^{(3b)^a}. \tag{9}$$

As we argued in Section 3, such a uniform M does not exist in general. Here we indicate a way to rectify the ranges given by (9).

The argument given in the proof (p. 400) proceeds via induction on a. In the induction step, the induction hypothesis is invoked on a formula different from the ϕ—which changes its size and thus makes the actual bounds different from the stated ones.

By inspecting the argument carefully, it is not difficult to see that the proof can in fact proceed as given, except that the derived bounds on the ranges of variables would be different for different quantifier blocks. Among the total of a quantifier blocks, the variables of the outermost one can take values from the range $[0, M_k - 1]$ where $\log M_k \leq c \cdot |\phi|^{(3b)^a}$ as above. In general, however, the range changes to

$$[0, M_i - 1] \text{ where } \log M_i \leq |\phi|^{(3b)^{O((a-i+1)\cdot a)}}, \text{ for all variables of the } i\text{th innermost block.} \tag{10}$$

The ranges given by (10) can in fact be used instead of (9) for all $i \in [1, a]$.

E An adaptation of Travers' lower bound

Let

$$\phi = \exists y_1^k \dots y_{n_k}^k . \forall y_1^{k-1} \dots y_{n_{k-1}}^{k-1} \cdots \exists y_1^1 \dots \exists y_{n_1}^1 : F$$

be an instance of Σ_k-QBF, where $F = \bigwedge_{1 \leq i \leq m} L_{i_1} \vee L_{i_2} \vee L_{i_3}$ is a formula in 3-CNF. By introducing slack variables z_j^i, we obtain an equivalent 3-CNF QBF instance with strict alternation:

$$\phi' = \exists y_1^k . \forall z_1^k \dots \forall z_{n_k - 1}^k . \exists z_{n_k}^k . \forall y_1^{k-1} . \exists z_1^{k-1} \cdots \forall z_{n_1 - 1}^1 . \exists z_{n_1}^1 : F$$

Note that no z_j^i appear in F. Let p be the number of all variables appearing in ϕ', and let f be a bijection between $[1, p]$ such that $f(\ell)$ uniquely identifies the ℓ-th variable. Travers shows in [15, Lem. 4] how to compute from ϕ' in logarithmic space an equi-satisfiable instance ψ' of QSubsetSum of the following form:

$$\begin{aligned}
&\psi' = \exists x_1^k . \forall w_1^k \dots \forall w_{n_k - 1}^k . \exists x_{n_k}^k . \forall x_1^{k-1} . \exists w_1^{k-1} \cdots \forall w_{n_1 - 1}^1 . \exists x_{n_1}^1 . \\
&\forall v_1 . \exists u_1 \cdots \forall v_p . \exists u_p . \forall t_1 . \exists s_1 \cdots \forall t_{2m} \exists s_{2m} : \\
&\qquad\qquad \sum_{1 \leq i \leq k} \sum_{1 \leq j \leq n_i} (a_j^i \cdot x_j^i + b_j^i \cdot w_j^i) + \sum_{1 \leq i \leq p} (c_i \cdot u_i) + \sum_{1 \leq i \leq 2m} (d_i \cdot s_i) = T.
\end{aligned}$$

First observe that the variables $v_1, \dots, v_p$ and $t_1, \dots, t_{2m}$ do not occur at all in the matrix formula of ψ'. Moreover, since z_j^i does not occur in F, the construction in [15, Lem. 4] has the property that for all $1 \leq i \leq k$, $1 \leq j \leq n_i$ and ℓ such that $f(\ell) = z^i_j$, $b^i_j = c_\ell$ and in the decimal expansion of b^i_j and c_ℓ all digits are set to 0, except a unique digit that is set to 1 and also set to 1 in T, and that is set to 0 in all other constants appearing in the matrix formula. Consequently, we can drop all variables not occurring in the matrix formula and all variables w^i_j while preserving equi-satisfiability, and obtain:

$$\psi = \exists x^k_1 \ldots \exists x^k_{n_k}.\forall x^{k-1}_1 \ldots \forall x^{k-1}_{n_{k-1}} \cdots \exists x^1_1 \ldots \exists x^1_{n_1}.\exists u_1 \ldots \exists u_p.\exists s_1 \ldots \exists s_{2m} : \\ \sum_{1 \leq i \leq k} \sum_{1 \leq j \leq n_i} (a^i_j \cdot x^i_j) + \sum_{1 \leq i \leq p} (c_i \cdot u_i) + \sum_{1 \leq i \leq 2m} (d_i \cdot s_i) = T,$$

which is an instance of Σ_k-SubsetSum equi-satisfiable with ϕ.

F Quantified integer programming over $\mathbb{Z}$

Here we consider $\mathbb{Z}$-QIP, the version of quantified integer programming where all variables are interpreted over $\mathbb{Z}$. The fragments of $\mathbb{Z}$-QIP are denoted analogously to the fragments of QIP (cf. p. 4).

▶ **Theorem 22.** *Σ_k-$\mathbb{Z}$-IP is complete for Σ^{P}_k if k is odd, and Π_k-$\mathbb{Z}$-IP is complete for Π^{P}_k if k is even. Σ_{k+1}-$\mathbb{Z}$-IP is complete for Σ^{P}_k if k is odd, and Π_{k+1}-$\mathbb{Z}$-IP is complete for Π^{P}_k if k is even.*

Proof. From our PH upper bounds for QIP over $\mathbb{N}$ (Theorem 2 and Corollary 3), one can derive matching PH upper bounds for $\mathbb{Z}$-QIP. Indeed, consider the following embedding of $\mathbb{Z}$-QIP into QIP. Take a $\mathbb{Z}$-QIP instance with variables $x_i \in \mathbb{Z}$ and replace each x_i with $y_i - z_i$ where y_i and z_i are interpreted over $\mathbb{N}$. This gives (syntactically) a QIP instance with the same alternation depth, and it is easy to show that the obtained QIP instance is a yes-instance iff the original $\mathbb{Z}$-QIP instance is a yes-instance.

For the lower bounds, let us now extend the argument from Section 7. We claim that the sentence (7) on p. 12 is equivalent to the following sentence in which the unconstrained variables in $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are interpreted over $\mathbb{Z}$, and which differs from (7) by the additional $\boldsymbol{x}_1 \geq 0$ constraint:

$$\exists \boldsymbol{x}_k \in \{0,1\}^{m_k}.\ \forall \boldsymbol{x}_{k-1} \in \{0,1\}^{m_{k-1}} \ \ldots\ \forall \boldsymbol{x}_2.\ \exists \boldsymbol{x}_1.\ \exists \boldsymbol{\lambda} : \\ \sum_{i=3}^{k} \boldsymbol{a}_i \cdot \boldsymbol{x}_i + \boldsymbol{a}_2 \cdot (\boldsymbol{x}_2 - 2 \cdot \boldsymbol{\lambda}) + \boldsymbol{a}_1 \cdot \boldsymbol{x}_1 = t \wedge \boldsymbol{x}_1 \leq \mathbf{1} \wedge \mathbf{0} \leq \boldsymbol{x}_2 - 2 \cdot \boldsymbol{\lambda} \leq \mathbf{1} \wedge \boldsymbol{x}_1 \geq \mathbf{0}. \tag{11}$$

Suppose the sentence (7) evaluates to true (over $\mathbb{N}$), then the sentence (11) over $\mathbb{Z}$ obviously holds whenever $\boldsymbol{x}_2 \geq \mathbf{0}$. Now if $x < 0$ for some component x of $\boldsymbol{x}_2$, then note that the corresponding component λ of $\boldsymbol{\lambda}$ has to be an integer (from $\mathbb{Z}$) such that $x - 2\lambda \in \{0,1\}$. Therefore, $\boldsymbol{x}_2 - 2 \cdot \boldsymbol{\lambda} \in \{0,1\}^{m_2}$, and an appropriate $\boldsymbol{x}_1$ (which is necessarily in $\{0,1\}^{m_1}$) exists because the sentence (7) holds over $\mathbb{N}$. Conversely, if the sentence (11) holds over $\mathbb{Z}$, then it holds in particular for all choices of $\boldsymbol{x}_2 \geq \mathbf{0}$; now again $\boldsymbol{\lambda} = \lfloor \boldsymbol{x}_2/2 \rfloor$, and the sentence will assert the existence of an appropriate $\boldsymbol{x}_1$, which (by virtue of the added constraint) will be nonnegative. But then this $\boldsymbol{x}_1$ will work for the sentence (7) as well. This shows that Σ_k-$\mathbb{Z}$-IP is Σ^{P}_k-complete, and the proof for the dual case is analogous. ◀

G Pseudo-polynomial algorithm

We explain here how, using our techniques, to obtain a pseudo-polynomial algorithm for the fragment of QIP where the total number of variables is fixed and the matrix formula is $A \cdot \boldsymbol{x} = \boldsymbol{c}$ instead of $A \cdot \boldsymbol{x} \geq \boldsymbol{c}$. Assume in this section that the matrix formula has m equations and that the total number of variables is $n = O(1)$.

First observe that the sets of nonnegative integer solutions to systems of linear equations are hybrid linear sets with norm at most $(n \cdot \|A\| + \|\boldsymbol{c}\| + 1)^{r+1}$ where r is the rank of A; this follows from [12, Thm. 1]. This bound is similar to the one of Proposition 1, but the crucial difference is that here the norm is bounded by a polynomial in the size of the input, because $r \leq n = O(1)$ and because $\|A\|, \|\boldsymbol{c}\|$ do not exceed the input size (recall that we aim to describe a *pseudo-polynomial* algorithm, i.e., in the setting at hand all numbers in the input are written in unary). Let the input QIP instance be ψ, then the norm of the set L of solutions to $A \cdot \boldsymbol{x} = \boldsymbol{c}$ is at most $p(|\psi|)$ where $p(\cdot)$ is a fixed polynomial.

We can now apply the scheme of Proposition 4 (small witness property) and Proposition 5 (relativization-like theorem). We first perform a sequence of at most $n = O(1)$ projections and universal projections on the set L; the norm will grow to at most $M = (p(|\psi|))^{n^{O(n)}}$, which is again polynomial in $|\psi|$. This number will correspond to the range of the outermost quantifier block, and the other quantifiers will then be dealt using the technique of Proposition 5 or by substituting the witness and following the same process again, repeatedly. So the ranges for all variables will be of the form $[0, M_i - 1]$ where all M_i are polynomial in $|\psi|$. After this, the existence of a polynomial algorithm is immediate.