

# An Efficient Quantifier Elimination Procedure for Presburger Arithmetic

Christoph Haase ✉ 


Department of Computer Science, University of Oxford, UK

Shankara Narayanan Krishna ✉ 

Department of Computer Science & Engineering, IIT Bombay, India

Khushraj Madnani ✉ 

Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern, Germany

Om Swostik Mishra ✉ 

Department of Mathematics, IIT Bombay, India

Georg Zetsche ✉ 

Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern, Germany

---

## Abstract

All known quantifier elimination procedures for Presburger arithmetic require doubly exponential time for eliminating a single block of existentially quantified variables. It has even been claimed in the literature that this upper bound is tight. We observe that this claim is incorrect and develop, as the main result of this paper, a quantifier elimination procedure eliminating a block of existentially quantified variables in singly exponential time. As corollaries, we can establish the precise complexity of numerous problems. Examples include deciding (i) monadic decomposability for existential formulas, (ii) whether an existential formula defines a well-quasi ordering or, more generally, (iii) certain formulas of Presburger arithmetic with Ramsey quantifiers. Moreover, despite the exponential blowup, our procedure shows that under mild assumptions, even NP upper bounds for decision problems about quantifier-free formulas can be transferred to existential formulas. The technical basis of our results is a kind of small model property for parametric integer programming that generalizes the seminal results by von zur Gathen and Sieveking on small integer points in convex polytopes.

**2012 ACM Subject Classification** Theory of computation → Logic

**Keywords and phrases** Presburger arithmetic, quantifier elimination, parametric integer programming, convex geometry

**Digital Object Identifier** 10.4230/LIPIcs.ICALP.2024.142

**Category** Track B: Automata, Logic, Semantics, and Theory of Programming

**Funding** Funded by the European Union (ERC, FINABIS, 101077902). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

*Christoph Haase*: Supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant agreement No. 852769, ARiAT).

*Khushraj Madnani*: Supported in part by the Deutsche Forschungsgemeinschaft (DFG) project 389792660 TRR 248–CPEC.

**Acknowledgements** We are grateful to (i) Pascal Bergsträßer, Moses Ganardi, and Anthony W. Lin for discussions about Weispfenning's lower bound, (ii) Pascal Baumann, Eren Keskin, Roland Meyer for discussions on polyhedra, (iii) Anthony W. Lin and Matthew Hague for explaining some aspects of their results on monadic decomposability, and (iv) Gaëtan Regaud for proofreading.



© Christoph Haase, Shankara Narayanan Krishna, Khushraj Madnani, Om Swostik Mishra, and Georg Zetsche; licensed under Creative Commons License CC-BY 4.0

51st International Colloquium on Automata, Languages, and Programming (ICALP 2024).

Editors: Karl Bringmann, Martin Grohe, Gabriele Puppis, and Ola Svensson;

Article No. 142; pp. 142:1–142:17



Leibniz International Proceedings in Informatics  
LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



## 1 Introduction

Presburger arithmetic is the first-order theory of the integers with addition and order. This theory was shown decidable by Mojżesz Presburger in 1929 [25] by establishing a quantifier elimination procedure in the extended structure additionally consisting of infinitely many predicates  $m \mid \cdot$  for all integers  $m > 0$ , asserting divisibility by a constant. Recall that a logical theory  $T$  admits quantifier elimination whenever for any formula  $\Phi(y_1, \dots, y_k) \equiv \exists x \varphi(x, y_1, \dots, y_k)$  with  $\varphi$  being quantifier free there is a computable quantifier-free formula  $\Psi(y_1, \dots, y_k)$  such that  $\Phi \leftrightarrow \Psi$  is a tautology in  $T$ . Presburger’s quantifier elimination procedure has non-elementary running time. In the early 1970s, Cooper [6] developed an improved version of Presburger’s procedure, which was later shown to run in triply exponential time [23]. Ever since, various other quantifier elimination procedures have been established and analyzed, especially for fragments of Presburger arithmetic with a fixed number of quantifier alternations, see e.g. [26, 32]. Weispfenning [33] analyzed lower bounds for quantifier-elimination procedures and showed that, assuming unary encoding of numbers, *any* quantifier elimination procedure requires triply exponential time. In the same paper, Weispfenning also claims that any algorithm eliminating a single block of existential quantifiers inherently requires *doubly* exponential time [33, p. 50].

The main contribution of this paper is to develop a quantifier elimination procedure for Presburger arithmetic that eliminates a block of existentially quantified variables in *singly* exponential time. This, of course, contradicts Weispfenning’s claim, which actually turns out to be incorrect as we point out in detail in Appendix C. The key technical insight underlying our procedure is a kind of small model property for parametric integer programming. Given an integer matrix  $A \in \mathbb{Z}^{\ell \times n}$  and  $\mathbf{b} \in \mathbb{Z}^\ell$ , recall that integer programming is to decide whether there is some  $\mathbf{x} \in \mathbb{Z}^n$  such that  $A\mathbf{x} \leq \mathbf{b}$ . It is well-known by the work of von zur Gathen and Sieveking [31], and Borosh and Treybig [4], that if such an  $\mathbf{x}$  exists then there is one whose bit length is polynomially bounded in the bit lengths of  $A$  and  $\mathbf{b}$ . In this paper, we refer to the situation in which  $\mathbf{b}$  is not fixed and provided as a parameter as *parametric integer programming*. Our main technical result states that, in this setting, if  $A\mathbf{x} \leq \mathbf{b}$  has a solution for a given  $\mathbf{b} \in \mathbb{Z}^\ell$  then there are  $D \in \mathbb{Q}^{n \times \ell}$  and  $\mathbf{d} \in \mathbb{Q}^n$ , both of bit length polynomial in the bit length of  $A$ , such that  $\mathbf{x} = D\mathbf{b} + \mathbf{d}$  is integral and also a solution. Observe that there is only an exponential number (in the bit length of  $A$ ) of possible choices for  $D$  and  $\mathbf{d}$ . Eliminating a block of variables  $\mathbf{x}$  from a system of linear inequalities thus becomes easy: we have that  $A\mathbf{x} \leq B\mathbf{y} + \mathbf{c}$  is equivalent to the disjunction of systems of the form  $A(D(B\mathbf{y} + \mathbf{c}) + \mathbf{d}) \leq B\mathbf{y} + \mathbf{c}$  for all  $D$  and  $\mathbf{d}$  of bit length polynomial in  $A$ . Using standard arguments, this approach can then be turned into a quantifier elimination procedure that eliminates a block of existentially quantified variables in exponential time.

## 2 Preliminaries

Throughout this paper, all vectors  $\mathbf{z}$  are treated as column vectors unless mentioned otherwise. For a vector  $\mathbf{x} \in \mathbb{Q}^n$ , let  $\|\mathbf{x}\|_\infty$  be the maximal absolute value of all components of  $\mathbf{x}$ . Moreover, let  $\|\mathbf{x}\|_{\text{frac}}$  be the maximal absolute value of all *numerators* and *denominators* of components in  $\mathbf{x}$ . The latter is important for representations: Note that a vector  $\mathbf{x} \in \mathbb{Q}^n$  with  $\|\mathbf{x}\|_{\text{frac}} \leq m$  can be represented using  $O(n \log m)$  bits. We use analogous notations  $\|A\|_\infty$  and  $\|A\|_{\text{frac}}$  for matrices  $A$ . We will sometimes refer to the *Hadamard inequality* [19], which implies that for a square matrix  $A \in \mathbb{Z}^{n \times n}$ , we have  $|\det(A)| \leq n^{n/2} \cdot \|A\|_\infty^n$ . In particular, the determinant of  $A$  is at most exponential in the maximal absolute value of entries of  $A$ .

**Presburger arithmetic.** *Presburger arithmetic* (PA) is the first-order theory of the structure  $\langle \mathbb{Z}; +, <, 0, 1 \rangle$ . In order to enable quantifier elimination, we have to permit modulo constraints. Thus technically, we are working with the structure  $\langle \mathbb{Z}; +, <, (\equiv_m)_{m \in \mathbb{Z}}, 0, 1 \rangle$ , where  $a \equiv_m b$  stands for  $a \equiv b \pmod{m}$ . In our syntax, we allow atomic formulas of the forms  $a_1x_1 + \dots + a_nx_n \leq b$  (called *linear inequalities*) or  $a_1x_1 + \dots + a_nx_n \equiv b \pmod{m}$  (called *modulo* or *divisibility constraints*), where  $x_1, \dots, x_n$  are variables and  $a_1, \dots, a_n, b, m \in \mathbb{Z}$  are constants encoded in binary. A formula is *quantifier-free* if it contains no quantifiers or, equivalently, is a Boolean combination of atomic formulas. Notice that conjunctions of linear inequalities can be written as systems of linear inequalities  $A\mathbf{x} \leq \mathbf{b}$ .

The *size* of a PA Formula  $\varphi$ , denoted  $|\varphi|$ , is the number of letters used to write it down, where we assume all constants to be encoded in binary. (Sometimes, we say that a formula obeys a size bound even if constants are encoded in unary; but this will be stated explicitly).

**Fixed quantifier alternation fragments.** The  $\Sigma_k$  fragment of PA consists of formulas of the form  $\exists \mathbf{u}_1 \forall \mathbf{u}_2 \dots Q_k \mathbf{u}_k : \varphi(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k, \mathbf{z})$  where  $\mathbf{u}_i$  is a vector of quantified variables,  $\mathbf{z}$  is a vector of free variables,  $\varphi(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k, \mathbf{z})$  is a quantifier free PA formula, and  $Q_k$  denotes  $\forall$  or  $\exists$  depending on whether  $k$  is even or odd respectively. Similarly, the  $\Pi_k$  fragment of PA consists of formulas of the form  $\forall \mathbf{u}_1 \exists \mathbf{u}_2 \dots Q_k \mathbf{u}_k : \varphi(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k, \mathbf{z})$  where  $Q_k$  denotes  $\forall$  or  $\exists$  depending on whether  $k$  is odd or even respectively.

**Bounded existential Presburger arithmetic.** In addition to our quantifier elimination result, we shall prove a somewhat stronger version, which states that one can compute a compact representation of a quantifier-free formula in polynomial time. As compact representations, we introduce a syntactic variant of existential Presburger arithmetic, which we call *bounded existential Presburger arithmetic*, short  $\exists^{\leq} \text{PA}$ . Essentially,  $\exists^{\leq} \text{PA}$  requires all quantifiers to be restricted to bounded intervals, but also permits polynomials over the quantified variables. Using standard methods, one can translate every formula in  $\exists^{\leq} \text{PA}$  in polynomial time into an  $\exists \text{PA}$  formula. However, the converse is not obvious, and our main results states that this is possible. Syntactically, an  $\exists^{\leq} \text{PA}$  formula over free variables  $y_1, \dots, y_m$  is of the form

$$\exists^{\leq k_1} x_1 \dots \exists^{\leq k_n} x_n : \varphi,$$

where  $x_1, \dots, x_n$  are variables, each  $k_i \in \mathbb{N}$  is a number given in binary, and  $\varphi$  is a quantifier-free formula where every atom is of one of the forms:

$$\sum_{i=1}^m p_i y_i \leq q \quad \text{or} \quad \sum_{i=1}^m p_i y_i \equiv r \pmod{q}, \quad (1)$$

where  $p_1, \dots, p_m, q, r \in \mathbb{Z}[x_1, \dots, x_n]$  are polynomials over the variables  $x_1, \dots, x_n$ . Thus, where  $\exists \text{PA}$  allows constant integral coefficients,  $\exists^{\leq} \text{PA}$  allows polynomials from  $\mathbb{Z}[x_1, \dots, x_n]$ . The quantifiers  $\exists^{\leq k_i} x_i$  are interpreted as “there exists  $x_i \in \mathbb{Z}$  with  $|x_i| \leq k_i$ ”.

► **Remark 2.1.** Now indeed, a  $\exists^{\leq} \text{PA}$  formula can be converted in polynomial time into an  $\exists \text{PA}$  formula: The bounded quantification is clearly expressible in  $\exists \text{PA}$ . The terms  $p_i y_i$  and  $q$  in (1) (recall  $p_i$  and  $q$  are polynomials are from  $\mathbb{Z}[x_1, \dots, x_n]$ ) are also expressible, because multiplication with exponentially bounded variables can be expressed using polynomial-size  $\exists \text{PA}$  formulas. This is because given a polynomial  $p \in \mathbb{Z}[x_1, \dots, x_n]$  and a variable  $y$ , we can construct a polynomial-size existential formula  $\pi(x_1, \dots, x_n, y, z)$  expressing  $z = p(x_1, \dots, x_n) \cdot y \wedge |x_1| \leq k_1 \wedge \dots \wedge |x_n| \leq k_n$ . This, in turn, follows from the fact that given  $\ell$  in unary, we can construct an existential formula  $\mu_\ell(x, y, z)$ , of size linear in  $\ell$ , expressing  $z = x \cdot y \wedge |x| \leq 2^\ell$  (see [17, Sec. 3.1] or [18, p. 7]). Thus, we can construct  $\pi$  in  $\exists \text{PA}$  by introducing a variable for each subterm of  $p$  (which can clearly all be bounded exponentially).

**Making  $\exists^{\leq}\text{PA}$  formulas quantifier-free.** Moreover, a  $\exists^{\leq}\text{PA}$  formula can easily be converted (in exponential time) into an exponential-size quantifier-free formula: Just take an exponential disjunction over all assignments of the existentially bounded variables  $x_1, \dots, x_n$  and replace the variables by their values in all the atoms. Thus,  $\exists^{\leq}\text{PA}$  formulas can be regarded as compact representations of quantifier-free formulas.

### 3 Main results

Here, we state and discuss implications of the main result of this paper:

► **Theorem 3.1.** *Given a formula of  $\exists\text{PA}$ , we can construct in polynomial time an equivalent formula in  $\exists^{\leq}\text{PA}$ .*

From Theorem 3.1, we can deduce the following, since by the remark Remark 2.1 in Section 2, one can easily convert a  $\exists^{\leq}\text{PA}$  formula into an exponential-sized quantifier-free formula.

► **Corollary 3.2.** *Given a formula  $\varphi$  in existential Presburger arithmetic, we can compute in exponential time an equivalent quantifier-free formula  $\psi$  of size exponential in  $\varphi$ . Moreover, all constants in  $\psi$  are encoded in unary.*

In Section 6, we will see that an exponential blowup cannot be avoided when eliminating a block of existential quantifiers, even if we allow constants to be encoded in binary in the quantifier-free formula.

There are several applications of Theorem 3.1 and Corollary 3.2. The most obvious type of applications are those, where, for every problem<sup>1</sup> that is in NP (resp. coNP) for quantifier-free formulas, the same problem belongs to NEXP (resp. coNEXP) for existential formulas. Oftentimes, this yields optimal complexity. We mention some examples.

A direct consequence of Corollary 3.2 (and the NP membership of the quantifier free fragment of PA) is the following.

► **Corollary 3.3.** *The  $\Sigma_2$ -fragment of Presburger arithmetic belongs to NEXP.*

The NEXP upper bound is known and was shown by Haase [17, Thm. 1]. In fact, the  $\Sigma_2$ -fragment is known to be NEXP-complete: An NEXP lower bound was shown much earlier by Grädel [14], already for the  $\exists\forall^*$ -fragment.

**Ramsey quantifiers.** In fact, combining Corollary 3.2 with the results from [2], we can strengthen Corollary 3.3. The *Ramsey quantifier*  $\exists^{\text{ram}}$  states the existence of infinite (directed) cliques. More precisely, if  $\varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is a Presburger formula where  $\mathbf{x}$  and  $\mathbf{y}$  are vectors of  $n$  variables each, then  $\exists^{\text{ram}}(\mathbf{x}, \mathbf{y}): \varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is satisfied for  $\mathbf{z}$  if and only if there exists an infinite sequence  $\mathbf{a}_1, \mathbf{a}_2, \dots \in \mathbb{Z}^n$  of pairwise distinct vectors with  $\varphi(\mathbf{a}_i, \mathbf{a}_j, \mathbf{z})$  for every  $i < j$ . As mentioned in [2], Ramsey quantifiers can be applied to deciding liveness properties, deciding monadic decomposability (see below), and deciding whether a formula defines a well-quasi-ordering (see below).

In [2, Thm. 5.1], it is shown that if  $\varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is an  $\exists\text{PA}$  formula, then one can compute in polynomial time an  $\exists\text{PA}$  formula  $\varphi'(\mathbf{z})$  equivalent to  $\exists^{\text{ram}}(\mathbf{x}, \mathbf{y}, \mathbf{z}): \varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ .

<sup>1</sup> To be precise: Every *semantic* problem, meaning one that only depends on the set defined by the input formula.

► **Corollary 3.4.** *Given a  $\Sigma_2$ -formula  $\varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ , we can construct an exponential-size  $\exists$ PA formula equivalent to  $\exists^{\text{ram}}(\mathbf{x}, \mathbf{y}): \varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$ . In particular, deciding the truth of  $\exists^{\text{ram}}(\mathbf{x}, \mathbf{y}): \psi$  for  $\Sigma_2$ -formulas  $\psi(\mathbf{x}, \mathbf{y})$  is NEXP-complete.*

Indeed, Corollary 3.2 lets us convert  $\varphi(\mathbf{x}, \mathbf{y}, \mathbf{z})$  into an exponential-size existential formula  $\varphi'$ , so that we can apply the above result of [2] to the formula  $\exists^{\text{ram}}(\mathbf{x}, \mathbf{y}): \varphi'(\mathbf{x}, \mathbf{y}, \mathbf{z})$ , which results in an equivalent exponential  $\exists$ PA formula. The NEXP lower bound in the second statement follows from NEXP-hardness of the  $\Sigma_2$ -fragment and the fact that for a given  $\Sigma_2$ -formula  $\chi$  without free variables, the statement  $\exists^{\text{ram}}(\mathbf{x}, \mathbf{y}): \chi \wedge \mathbf{x} < \mathbf{y}$  is equivalent to  $\chi$ .

**Detecting WQOs.** A *well-quasi-ordering* (WQO) is a reflexive and transitive ordering  $(X, \leq)$  such that for every sequence  $x_1, x_2, \dots \in X$ , there are  $i < j$  with  $x_i \leq x_j$ . Well-quasi-orderings are of paramount importance in the widely applied theory of well-structured transition systems [7, 1, 10]. The problem of deciding whether a given Presburger formula  $\varphi(\mathbf{x}, \mathbf{y})$  defines a WQO was recently raised by Finkel and Gupta [8], with the hope of establishing automatically that certain systems are well-structured. As observed in [9, Prop. 12], this problem reduces to evaluating Ramsey quantifiers, which is decidable by [28]. Based on an NP algorithm for Ramsey quantifiers, it is shown in [2, Sec. 8.3] that given a quantifier-free formula  $\varphi(\mathbf{x}, \mathbf{y})$ , where  $\mathbf{x}$  and  $\mathbf{y}$  are vectors of  $n$  variables each, it is coNP-complete whether the relation  $R \subseteq \mathbb{Z}^n \times \mathbb{Z}^n$  defined by  $\varphi$  is a WQO. Our results allow us to settle the complexity for existential formulas:

► **Corollary 3.5.** *Given an  $\exists$ PA formula  $\varphi$ , it is coNEXP-complete to decide whether  $\varphi$  defines a WQO.*

The upper bound follows directly from Corollary 3.2 and the fact that it is coNP-complete to decide whether a given quantifier-free formula defines a well-quasi-ordering [2, Sec. 8.3]. This yields a coNEXP procedure overall. It should be noted that Corollary 3.5 can also be deduced from Corollary 3.4 (using the same idea as in [2, Sec. 8.3]). However, we find it instructive to demonstrate how quantifier elimination permits a direct transfer of the coNP algorithm as a black box. We show the coNEXP lower bound in Section 5.

**Monadic decomposability.** A Presburger formula is *monadic* if each of its atoms contains at most one variable. Moreover, we say that a Presburger formula  $\varphi$  is *monadically decomposable* if  $\varphi$  is equivalent to a monadic Presburger formula. Motivated by the role monadic formulas play in constraint databases [15, 21], Veanes, Bjørner, and Nachmanson, and Berge recently raised the question of how to decide whether a given formula is monadically decomposable [30]. For Presburger arithmetic, decidability follows from [13, p. 1048] and for quantifier-free formulas, monadic decomposability was shown coNP-complete in [20, Thm. 1] (in [2, Cor. 8.1], the coNP upper bound is shown via Ramsey quantifiers). Corollary 3.2 allows us to settle the case of  $\exists$ PA formulas.

► **Corollary 3.6.** *Monadic decomposability of  $\exists$ PA formulas is coNEXP-complete.*

This is because given an  $\exists$ PA formula, we can compute an exponential-sized quantifier-free formula and apply the existing coNP procedure, yielding a coNEXP upper bound overall. Again, the coNEXP upper bound could also be deduced from Corollary 3.4 (but this proof shows again how to transfer algorithms using quantifier elimination). The coNEXP lower bound follows the same idea as the coNP lower bound in [2], see Section 5.

**NP upper bounds.** In addition to new NEXP and coNEXP upper bounds, Theorem 3.1 can also be used to obtain NP upper bounds. Suppose we have a predicate  $\mathbf{p}$  on sets of integral vectors. That is, for each  $S \subseteq \mathbb{Z}^m$  for some  $m \in \mathbb{N}$ , either  $\mathbf{p}(S)$  is true or not. We call this predicate *admissible* if for any  $m \in \mathbb{N}$ ,  $S_1, S_2 \subseteq \mathbb{Z}^m$ , we have that  $\mathbf{p}(S_1 \cup S_2)$  implies  $\mathbf{p}(S_1)$  or  $\mathbf{p}(S_2)$ . Let us see some examples:

- (i) The predicate  $\mathbf{p}$  with  $\mathbf{p}(S)$  if and only if  $S \neq \emptyset$ .
- (ii) The predicate  $\mathbf{p}$  with  $\mathbf{p}(S)$  if and only if  $S$  is infinite.
- (iii) The predicate  $\mathbf{p}$  with  $\mathbf{p}(S)$  if and only if  $S \subseteq \mathbb{Z}$  and  $S$  contains a power of 2.
- (iv) The predicate  $\mathbf{p}$  with  $\mathbf{p}(S)$  if and only if  $S \subseteq \mathbb{Z}^{2k}$  and viewed as a relation  $S \subseteq \mathbb{Z}^k \times \mathbb{Z}^k$ ,  $S$  has an infinite clique.
- (v) The predicate  $\mathbf{p}$  with  $\mathbf{p}(S)$  if and only if  $S \subseteq \mathbb{Z}$  and  $S$  contains infinitely many primes.
- (vi) The predicate  $\mathbf{p}$  with  $\mathbf{p}(S)$  if and only if  $S \subseteq \mathbb{Z}^2$  and  $S$  contains a pair  $(x, 2^x)$ .

For each such predicate, we consider the problem  $\mathbf{p}(\exists\text{PA})$ :

**Input** An  $\exists\text{PA}$  formula  $\varphi$  with  $m$  free variables for some  $m \in \mathbb{N}$ .

**Question** Does  $\mathbf{p}(S)$  hold, where  $S \subseteq \mathbb{Z}^m$  is the set defined by  $\varphi$ ?

Moreover,  $\mathbf{p}(\text{QF})$  is the restriction of the problem where the input formula  $\varphi$  is quantifier-free.

For several of the examples above, it is known that  $\mathbf{p}(\exists\text{PA})$  is in NP: For (i) and (ii), these are standard facts, and for (iii), this follows from NP-completeness of existential Büchi arithmetic [16, Thm. 1]. For (iv), this follows from the fact that Ramsey quantifiers can be evaluated in NP [2, Thm 5.1]. Our results imply that for proving NP upper bounds, we may always assume a quantifier-free input formula. This is perhaps surprising, because one might expect that for non-linear predicates, it is difficult to bound the quantified variables.

► **Corollary 3.7.** *For every admissible predicate  $\mathbf{p}$ , the problem  $\mathbf{p}(\exists\text{PA})$  is in NP if and only if  $\mathbf{p}(\text{QF})$  is in NP.*

Here, the “only if” direction is trivial, and the “if” direction follows from Theorem 3.1. This is because Theorem 3.1 allows us to assume that  $\varphi$  is given as a  $\exists^{\leq}\text{PA}$  formula  $\exists^{\leq k_1} x_1 \cdots \exists^{\leq k_n} x_n: \psi(x_1, \dots, x_n, y_1, \dots, y_m)$ . Moreover, admissibility of  $\mathbf{p}$  implies that  $\mathbf{p}$  is satisfied for  $\varphi$  if and only if there exists an assignment  $(a_1, \dots, a_n)$  for the bounded variables such that the quantifier-free formula  $\psi(a_1, \dots, a_n, y_1, \dots, y_m)$  satisfies  $\mathbf{p}$ . Thus, we can guess the assignment (which occupies polynomially many bits) and run the NP algorithm for quantifier-free formulas.

## 4 Quantifier elimination

In this section, we prove Theorem 3.1. The following is our main geometric ingredient.

► **Proposition 4.1.** *Let  $A \in \mathbb{Z}^{\ell \times n}$  and  $\mathbf{b} \in \mathbb{Z}^{\ell}$ , and let  $\Delta$  be an upper bound on all absolute values of the subdeterminants of  $A$ . If the system  $A\mathbf{x} \leq \mathbf{b}$  has an integral solution, then it has an integral solution of the form  $D\mathbf{b} + \mathbf{d}$ , where  $D \in \mathbb{Q}^{n \times \ell}$  and  $\mathbf{d} \in \mathbb{Q}^n$  with  $\|D\|_{\text{frac}} \leq \Delta$  and  $\|\mathbf{d}\|_{\text{frac}} \leq n\Delta^2$ .*

Before we prove Proposition 4.1, let us see how it implies Theorem 3.1 and Corollary 3.2.

**Proof of Corollary 3.2.** While Corollary 3.2 follows from Theorem 3.1, it follows very directly from Proposition 4.1 and the proof is a good warm-up for the proof of Theorem 3.1. Therefore, we first derive Corollary 3.2 from Proposition 4.1. Suppose we are given a Presburger formula  $\exists \mathbf{x}: \varphi(\mathbf{x}, \mathbf{y})$ , where  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_m)$  are variables and  $\varphi$  is quantifier-free.

It is well-known that divisibility constraints can be eliminated in favor of existentially quantified variables, since  $a \equiv b \pmod m$  if and only if  $\exists x: a - b = mx$ . Thus, we may assume that  $\varphi$  contains no divisibility constraints. Then, by moving all negations inwards and using the standard equivalence  $\neg(r \leq t) \iff t + 1 \leq r$ , we may assume that  $\varphi$  is a positive Boolean combination of atoms  $\mathbf{a}^\top \mathbf{x} \leq \mathbf{b}^\top \mathbf{y} + c$ , where  $\mathbf{a} \in \mathbb{Z}^n$ ,  $\mathbf{b} \in \mathbb{Z}^m$ , and  $c \in \mathbb{Z}$ .

By bringing  $\varphi$  into DNF, we can write it as a disjunction of exponentially many systems of inequalities of the form  $A\mathbf{x} \leq B\mathbf{y} + \mathbf{c}$ , where  $A \in \mathbb{Z}^{\ell \times n}$ ,  $B \in \mathbb{Z}^{\ell \times m}$ , and  $\mathbf{c} \in \mathbb{Z}^\ell$ . Thus, it suffices to construct a quantifier-free formula for  $\exists \mathbf{x}: A\mathbf{x} \leq B\mathbf{y} + \mathbf{c}$ . Let  $\Delta$  be an upper bound for all absolute values of subdeterminants of  $A$ . Since the transformation into DNF does not change the appearing constants, we have that  $\Delta \leq n^{n/2} \|A\|_\infty^n$  is at most exponential in the size of the input formula.

According to Proposition 4.1, a vector  $\mathbf{x}$  with  $\varphi(\mathbf{x}, \mathbf{y})$  exists if and only if there exists a matrix  $D \in \mathbb{Q}^{n \times \ell}$  and  $\mathbf{d} \in \mathbb{Q}^n$  with  $\|D\|_{\text{frac}} \leq \Delta$  and  $\|\mathbf{d}\|_{\text{frac}} \leq n\Delta^2$  such that (i) substituting  $D(B\mathbf{y} + \mathbf{c}) + \mathbf{d}$  for  $\mathbf{x}$  satisfies  $A\mathbf{x} \leq B\mathbf{y} + \mathbf{c}$  and also (ii) the vector  $D(B\mathbf{y} + \mathbf{c}) + \mathbf{d}$  is integral. Therefore, the formula  $\exists \mathbf{x}: A\mathbf{x} \leq B\mathbf{y} + \mathbf{c}$  is equivalent to

$$\bigvee_{(D, \mathbf{d}) \in P} A(D(B\mathbf{y} + \mathbf{c}) + \mathbf{d}) \leq B\mathbf{y} + \mathbf{c} \wedge D(B\mathbf{y} + \mathbf{c}) + \mathbf{d} \in \mathbb{Z}^n$$

where  $P$  is the set of all pairs  $(D, \mathbf{d})$  with  $D \in \mathbb{Q}^{n \times \ell}$ ,  $\mathbf{d} \in \mathbb{Q}^n$ ,  $\|D\|_{\text{frac}} \leq \Delta$ , and  $\|\mathbf{d}\|_{\text{frac}} \leq n\Delta^2$ . Clearly,  $P$  contains at most exponentially many elements. Moreover, note that the condition  $D(B\mathbf{y} + \mathbf{c}) + \mathbf{d} \in \mathbb{Z}^n$  is a set of  $n$  modulo constraints.  $\blacktriangleleft$

**Proof of Theorem 3.1.** The proof of Theorem 3.1 is similar to the above construction – we just need to circumvent the exponential conversion into DNF. We proceed as follows.

As above, we are given a Presburger formula  $\exists \mathbf{x}: \varphi(\mathbf{x}, \mathbf{y})$ , where  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_m)$  are variables and  $\varphi$  is quantifier-free. Moreover, we may assume that  $\varphi$  contains no divisibility constraints and is a positive Boolean combination of atoms  $\mathbf{a}^\top \mathbf{x} \leq \mathbf{b}^\top \mathbf{y} + c$ , where  $\mathbf{a} \in \mathbb{Z}^n$ ,  $\mathbf{b} \in \mathbb{Z}^m$ , and  $c \in \mathbb{Z}$ .

Let  $\mathbf{a}_i^\top \mathbf{x} \leq \mathbf{b}_i^\top \mathbf{y} + c_i$  for  $i = 1, \dots, \ell$  be the set of all atoms occurring in  $\varphi$  and let  $A \in \mathbb{Z}^{\ell \times n}$  be the matrix with rows  $\mathbf{a}_i^\top$  and  $B \in \mathbb{Z}^{\ell \times m}$  be the matrix of rows  $\mathbf{b}_i^\top$ , and let  $\mathbf{c} \in \mathbb{Z}^\ell$  be the (column) vector with entries  $c_1, \dots, c_\ell$ . Thus, our formula  $\varphi$  consists of  $\ell$  atoms, each of which is a row in the system of linear inequalities  $A\mathbf{x} \leq B\mathbf{y} + \mathbf{c}$ . Let  $\varphi'$  be the formula obtained from  $\varphi$  by replacing the atom  $\mathbf{a}_i^\top \mathbf{x} \leq \mathbf{b}_i^\top \mathbf{y} + c_i$  by  $z_i = 1$ , where  $z_i$ ,  $i \in \{1, \dots, \ell\}$ , is a fresh variable for each of the  $\ell$  atoms. Now let  $\Delta$  be an upper bound on all absolute values of the subdeterminants of  $A$ . Then  $\Delta \leq n^{n/2} \|A\|_\infty^n$  is at most exponential in the size of the input formula. Consider the formula

$$\begin{aligned} \exists z_1, \dots, z_\ell \in \{0, 1\}: \quad & \exists D \in \mathbb{Q}^{n \times \ell}, \|D\|_{\text{frac}} \leq \Delta: \\ \exists \mathbf{d} \in \mathbb{Q}^n, \|\mathbf{d}\|_{\text{frac}} \leq n\Delta^2: \quad & \varphi' \wedge D(B\mathbf{y} + \mathbf{c}) + \mathbf{d} \in \mathbb{Z}^n \wedge \bigwedge_{i=1}^{\ell} (z_i = 1 \rightarrow \psi_i), \quad (2) \end{aligned}$$

where  $\psi_i$  is the formula  $\mathbf{a}_i^\top (D(B\mathbf{y} + \mathbf{c}) + \mathbf{d}) \leq \mathbf{b}_i^\top \mathbf{y} + c_i$ . Note that (2) is expressible in  $\exists \leq \text{PA}$ : We introduce (i) one variable for each  $z_i$ , (ii) two variables for each entry of  $D$  (one for the numerator, and one for the denominator), and (iii) two variables for each entry of  $\mathbf{d}$ .

Each of the  $n$  divisibility constraints of  $D(B\mathbf{y} + \mathbf{c}) + \mathbf{d} \in \mathbb{Z}^n$  and each of the atoms  $\psi_i$  can be written in the forms (1). To see this, let  $u_1, \dots, u_k$  be the bounded variables used for the numerators or denominators in  $D$  and  $\mathbf{d}$ . Observe that the vector  $B\mathbf{y}$  is a linear combination of  $\mathbf{y}$  with integer coefficients. The matrix  $D$  and the vector  $\mathbf{d}$  consist

of quotients of bounded variables, hence rational functions in  $\mathbb{Z}[u_1, \dots, u_k]$ . Thus, the vector  $D(\mathbf{B}\mathbf{y} + \mathbf{c}) + \mathbf{d}$  has in each entry an expression  $s + \sum_{i=1}^m r_i y_i$ , where  $r_1, \dots, r_m, s \in \mathbb{Z}[u_1, \dots, u_k]$ . Hence, by multiplying with the product of all denominators, we can write each inequality  $\mathbf{a}_i^\top (D(\mathbf{B}\mathbf{y} + \mathbf{c}) + \mathbf{d}) \leq \mathbf{b}_i^\top \mathbf{y} + c_i$  in the form of (1). Moreover, for the requirement  $D(\mathbf{B}\mathbf{y} + \mathbf{c}) + \mathbf{d} \in \mathbb{Z}^n$ , we can write each row of  $D(\mathbf{B}\mathbf{y} + \mathbf{c}) + \mathbf{d}$  as a quotient  $\frac{1}{q}(r + \sum_{i=1}^m p_i y_i)$ , where  $q, r, p_1, \dots, p_m \in \mathbb{Z}[u_1, \dots, u_k]$ , so that membership in  $\mathbb{Z}$  is equivalent to  $\sum_{i=1}^m p_i y_i \equiv -r \pmod{q}$ .

Let us argue why (2) is equivalent to  $\exists \mathbf{x}: \varphi(\mathbf{x}, \mathbf{y})$ . Clearly, if (2) is satisfied, then  $\mathbf{z} = (z_1, \dots, z_\ell)$  yields a set of atoms that, if satisfied, makes  $\varphi$  true. Moreover, the vector  $D(\mathbf{B}\mathbf{y} + \mathbf{c}) + \mathbf{d}$  is an integer vector that satisfies all the atoms specified by  $\mathbf{z}$ .

Conversely, suppose  $\varphi(\mathbf{x}, \mathbf{y})$  holds for some  $\mathbf{x} \in \mathbb{Z}^n$  and  $\mathbf{y} \in \mathbb{Z}^m$ . First, we set exactly those  $z_i$  to 1 for which the  $i$ -th atom in  $\varphi$  is satisfied by  $\mathbf{x}, \mathbf{y}$ . Recall that each row of  $A$  (and each row of  $B$ , and of  $\mathbf{c}$ ) corresponds to an atom in  $\varphi$ . Let  $A'$  be the matrix obtained from  $A$  by selecting those rows that correspond to atoms that are satisfied by our  $\mathbf{x}$  and  $\mathbf{y}$ . Define  $B'$  similarly from  $B$ , and  $\mathbf{c}'$  from  $\mathbf{c}$ . Then we have  $A'\mathbf{x} \leq B'\mathbf{y} + \mathbf{c}'$ . Now Proposition 4.1 yields a matrix  $D'$  and a vector  $\mathbf{d}$  (each with  $n$  rows) with  $A'(D'(B'\mathbf{y} + \mathbf{c}') + \mathbf{d}) \leq B'\mathbf{y} + \mathbf{c}'$ . Now the set of rows of  $B'\mathbf{y} + \mathbf{c}'$  is a subset of the rows of  $B\mathbf{y} + \mathbf{c}$ , so by inserting zero-columns into  $D'$ , we can construct a matrix  $D$  with  $D(\mathbf{B}\mathbf{y} + \mathbf{c}) = D'(B'\mathbf{y} + \mathbf{c}')$ . Hence, we have  $A'(D(\mathbf{B}\mathbf{y} + \mathbf{c}) + \mathbf{d}) \leq B'\mathbf{y} + \mathbf{c}'$ . The latter means exactly that  $\psi_i$  is satisfied for every  $i$  with  $z_i = 1$ . Thus, this choice of  $z_1, \dots, z_\ell, D$ , and  $\mathbf{d}$  satisfies (2). ◀

## 4.1 Constructing solutions as affine transformations

### 4.1.1 Convex geometry

Before we start with the proof of Proposition 4.1, we recall some standard definitions from convex geometry from Schrijver's book [29]. Below, we let  $\mathbb{R}_+ = \{r \in \mathbb{R} \mid r \geq 0\}$ . A *polyhedron* is a set  $P = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{b}\}$ , where  $A$  is an  $\ell \times n$  integer matrix and  $\mathbf{b} \in \mathbb{Z}^\ell$ . Let  $C \subseteq \mathbb{R}^\ell$ , then  $C$  is a *convex cone* if  $\lambda\mathbf{x} + \mu\mathbf{y} \in C$  for all  $\mathbf{x}, \mathbf{y} \in C$  and  $\lambda, \mu \in \mathbb{R}_+$ . Given a set  $X \subseteq \mathbb{R}^\ell$ ,

$$\text{cone}(X) = \{\lambda_1 \mathbf{x}_1 + \dots + \lambda_t \mathbf{x}_t \mid t \geq 0, \mathbf{x}_1, \dots, \mathbf{x}_t \in X, \lambda_1, \dots, \lambda_t \in \mathbb{R}_+\}.$$

The *convex hull* of a set  $X \subseteq \mathbb{R}^\ell$  is the smallest convex set containing that set, i.e.,

$$\text{conv.hull}(X) = \{\lambda_1 \mathbf{x}_1 + \dots + \lambda_t \mathbf{x}_t \mid t \geq 1, \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_t \in X, \lambda_1, \dots, \lambda_t \in \mathbb{R}_+, \lambda_1 + \dots + \lambda_t = 1\}.$$

Next, we recall some terminology concerning the structure of polyhedra. The *characteristic cone* of a polyhedron  $P = \{\mathbf{x} \mid A\mathbf{x} \leq \mathbf{b}\} \subseteq \mathbb{R}^n$  is the set  $\text{char.cone}(P) := \{\mathbf{y} \in \mathbb{R}^n \mid A\mathbf{y} \leq 0\}$ . The *lineality space* of polyhedron  $P$  is the set  $\text{lin.space}(P) := \{\mathbf{y} \in \mathbb{R}^n \mid A\mathbf{y} = 0\}$ .

► **Definition 4.2 (Faces).** *Given a polyhedron  $P \subseteq \mathbb{R}^n$ ,  $F \subseteq P$  is a face of  $P$  if and only if  $F$  is non-empty and*

$$F = \{\mathbf{x} \in P \mid A'\mathbf{x} = \mathbf{b}'\}$$

*for some subsystem  $A'\mathbf{x} \leq \mathbf{b}'$  of  $A\mathbf{x} \leq \mathbf{b}$ . We call  $F \subseteq P$  a proper face of  $P$  if  $F \neq \emptyset$  and  $F \neq P$ .*

It follows that  $P$  has only finitely many faces. A *minimal face* of  $P$  is a face not containing any other face. We have the following characterization of minimal faces [29, Thm 8.4],



► **Proposition 4.3.** *A set  $F$  is a minimal face of a polyhedron  $P \subseteq \mathbb{R}^n$  if and only if  $\emptyset \neq F \subseteq P$  and*

$$F = \{\mathbf{x} \in \mathbb{R}^n \mid A'\mathbf{x} = \mathbf{b}'\}$$

for some subsystem  $A'\mathbf{x} \leq \mathbf{b}'$  of  $A\mathbf{x} \leq \mathbf{b}$ , such that the matrix  $A'$  has the same rank as  $A$ .

The following is shown in [29, Sec. 8.8]:

► **Proposition 4.4.** *Let  $C$  be the cone  $\{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{0}\}$ . There is a finite collection  $G_1, G_2, \dots, G_s$  of subsets, which are of the form  $G_i = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{a}_i^\top \mathbf{x} \leq 0, A'\mathbf{x} = \mathbf{0}\}$ , where  $\begin{bmatrix} A' \\ \mathbf{a}_i^\top \end{bmatrix}$  is a subset of the rows of  $A$ , such that the following holds. If we choose for each  $i = 1, \dots, s$  a vector  $\mathbf{y}_i$  from  $G_i \setminus \text{lin.space}(C)$  and choose  $\mathbf{z}_0, \dots, \mathbf{z}_t$  in  $\text{lin.space}(C)$  such that  $\text{lin.space}(C) = \text{cone}(\mathbf{z}_0, \dots, \mathbf{z}_t)$ , then*

$$C = \text{cone}(\mathbf{y}_1, \dots, \mathbf{y}_s, \mathbf{z}_0, \dots, \mathbf{z}_t).$$

Here, the sets  $G_i$  are also called minimal proper faces (but Proposition 4.4 is not a characterization of those).

### 4.1.2 Proof of Proposition 4.1

We now prove Proposition 4.1. For the remainder of the section, let  $A \in \mathbb{Z}^{\ell \times n}$  and  $\mathbf{b} \in \mathbb{Z}^\ell$ . Moreover, let  $\Delta$  be an upper bound on all absolute values of the sub-determinants of  $A$ . Our first step is a simple application of standard facts about polyhedra.

► **Lemma 4.5.** *If the system  $A\mathbf{x} \leq \mathbf{b}$  has a solution in  $\mathbb{Q}^n$ , then it has one of the form  $\frac{1}{a}E\mathbf{b}$ , where  $E \in \mathbb{Z}^{n \times \ell}$ ,  $a \in \mathbb{Z} \setminus \{0\}$ ,  $|a| \leq \Delta$ , and  $\|E\|_\infty \leq \Delta$ .*

**Proof.** It is well-known that if  $A\mathbf{x} \leq \mathbf{b}$  has a rational solution, then there is a solution inside a minimal face of the polyhedron  $P = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{b}\}$  defined by the system of linear inequalities  $A\mathbf{x} \leq \mathbf{b}$  [29, Thm. 8.5]. Recall that a *minimal face* is a non-empty subset  $F \subseteq P$  of the form

$$F = \{\mathbf{x} \in \mathbb{R}^n \mid A'\mathbf{x} = \mathbf{b}'\}, \tag{3}$$

where  $A'\mathbf{x} \leq \mathbf{b}'$  is a subset of the inequalities in  $A\mathbf{x} \leq \mathbf{b}$  such that the matrix  $A'$  has the same rank as  $A$  (see Proposition 4.3 or [29, Thm. 8.4]). Suppose  $F$  is a non-empty minimal face and satisfies (3). Here, we may assume that the rows of  $A'$  are linearly independent (otherwise, we can remove redundant rows without changing  $F$ ). This means,  $A'$  can be written as  $A' = (B \ C)$  such that  $B$  is invertible. Then the vector  $\mathbf{x}^* := (B^{-1}\mathbf{b}' \ \mathbf{0})^\top$  belongs to  $F$ . Since  $F \subseteq P$ , we know that  $A\mathbf{x}^* \leq \mathbf{b}$ . By Cramer's rule, the entry  $(j, i)$  of  $B^{-1}$  is  $\frac{(-1)^{i+j} \det(B_{ij})}{\det(B)}$ , where  $B_{ij}$  is the matrix obtained from  $B$  by removing the  $i$ -th row and  $j$ -th column. Note that  $|\det(B_{ij})| \leq \Delta$  and  $|\det(B)| \leq \Delta$ . In particular,  $\mathbf{x}^*$  can be written as  $\frac{1}{a}E\mathbf{b}$ , where  $a = \det(B)$  and  $\|E\|_\infty \leq \Delta$ . ◀

We also employ the following well-known fact, which again uses standard arguments.

► **Lemma 4.6.** *There are integral vectors  $\mathbf{y}_1, \dots, \mathbf{y}_s$  with each component being at most  $\Delta$  in absolute value, such that  $\{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{0}\} = \text{cone}(\mathbf{y}_1, \dots, \mathbf{y}_s)$ .*

## 142:10 An Efficient Quantifier Elimination Procedure for Presburger Arithmetic

**Proof.** Let  $C = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{0}\}$ . The lemma follows from Proposition 4.4. First, it is a consequence of Cramer's rule that we can choose  $\mathbf{z}_0, \dots, \mathbf{z}_t$  as a basis of  $\text{lin.space}(C) = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} = \mathbf{0}\}$  so that all  $\mathbf{z}_0, \dots, \mathbf{z}_t$  are integral and have absolute values at most  $\Delta$  in all components. For example, see [29, Cor. 3.1c]. It remains to pick from each set

$$G_i \setminus \text{lin.space}(C) = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{a}_i^\top \mathbf{x} < 0, A'\mathbf{x} = \mathbf{0}\}$$

an integral vector with all components bounded by  $\Delta$ . For this, we can proceed similarly to Lemma 4.5. As a subset of rows of  $A$ , the matrix  $B = \begin{bmatrix} A' \\ \mathbf{a}_i^\top \end{bmatrix}$  has rank at most  $n$ , and we may assume  $\mathbf{a}_i \neq \mathbf{0}$  (otherwise  $G_i \setminus \text{lin.space}(C)$  would be empty). Moreover, we may assume that the rows of  $B$  are linearly independent, as otherwise we can remove rows from  $A'$  without changing  $G_i$ . We can thus write  $B = (E \ F)$ , where  $E$  is invertible. By Cramer's rule (see, e.g. [29, Sec. 3.2]), the  $j$ -th component of the vector  $\mathbf{y} = E^{-1}(0, \dots, 0, -1)$  can be written as  $\frac{1}{\det(E)} \det(\tilde{E})$ , where  $\tilde{E}$  is obtained from  $E$  by replacing the  $j$ -th column by  $(0, \dots, 0, -1)$ . This means, the vector  $|\det(E)| \cdot \mathbf{y}$  has only integer components and all of them have absolute value at most  $\Delta$ . Now let  $\mathbf{y}^*$  be the vector obtained from  $|\det(E)| \cdot \mathbf{y}$  adding as many 0's as  $F$  has columns. Then we have  $B\mathbf{y}^* = E(|\det(E)| \cdot \mathbf{y}) = (0, \dots, 0, -|\det(E)|)$  and thus  $\mathbf{y}^* \in G_i \setminus \text{lin.space}(C)$ .  $\blacktriangleleft$

We also rely on the well-known theorem of Carathéodory [29, Cor. 7.1(i)].

► **Theorem 4.7** (Carathéodory's theorem). *If  $X \subseteq \mathbb{R}^n$  is some subset and  $\mathbf{x} \in \text{cone}(X)$ , then there are linearly independent  $\mathbf{x}_1, \dots, \mathbf{x}_m \in X$  with  $\mathbf{x} \in \text{cone}(\mathbf{x}_1, \dots, \mathbf{x}_m)$ .*

The following lemma is the key ingredient for proving Proposition 4.1. Its proof closely follows the ideas of [29, Thm. 17.2], which Schrijver attributes to Cook, Gerards, Schrijver, and Tardos [5]. The latter shows that for every rational  $\mathbf{x}$  that maximizes an expression  $\mathbf{c}^\top \mathbf{x}$  among the solutions of  $A\mathbf{x} \leq \mathbf{b}$ , there is a close-by integral vector that maximizes this expression among all integral vectors.

► **Lemma 4.8.** *Suppose the system  $A\mathbf{x} \leq \mathbf{b}$  has an integral solution, and let  $\mathbf{r} \in \mathbb{Q}^n$  be a rational solution. Then there is an integral solution  $\mathbf{z}^* \in \mathbb{Z}^n$  with  $\|\mathbf{z}^* - \mathbf{r}\|_\infty \leq n\Delta$ .*

**Proof.** An illustration of the proof is given in Figure 1. Let  $\mathbf{z}$  be an integral solution to  $A\mathbf{x} \leq \mathbf{b}$ . Split the equations  $A\mathbf{x} \leq \mathbf{b}$  into  $A_1\mathbf{x} \leq \mathbf{b}_1$  and  $A_2\mathbf{x} \leq \mathbf{b}_2$  such that  $A_1\mathbf{r} \leq A_1\mathbf{z}$  and  $A_2\mathbf{r} \geq A_2\mathbf{z}$ . In other words, we split  $A, \mathbf{b}$  into two sets of rows, depending on in which coordinates  $\mathbf{r}$  resp.  $\mathbf{z}$  is larger. Now consider the cone  $C = \{\mathbf{x} \in \mathbb{R}^n \mid A_1\mathbf{x} \geq \mathbf{0}, A_2\mathbf{x} \leq \mathbf{0}\}$ . Then, by the choice of  $A_1$  and  $A_2$ , we have  $\mathbf{z} - \mathbf{r} \in C$  and therefore

$$\mathbf{z} - \mathbf{r} = \lambda_1 \mathbf{y}_1 + \dots + \lambda_t \mathbf{y}_t,$$

where  $\lambda_1, \dots, \lambda_t \geq 0$  are real numbers and  $\mathbf{y}_1, \dots, \mathbf{y}_t$  are some linearly independent vectors chosen from the set of integer vectors  $\{\mathbf{y}_1, \dots, \mathbf{y}_s\}$  provided by Lemma 4.6 satisfying  $C = \text{cone}(\mathbf{y}_1, \dots, \mathbf{y}_s)$ . The choice of linearly independent vectors is possible due to Carathéodory's theorem. In particular, each  $\mathbf{y}_i$  has maximal absolute value at most  $\Delta$  and we have  $t \leq n$ .

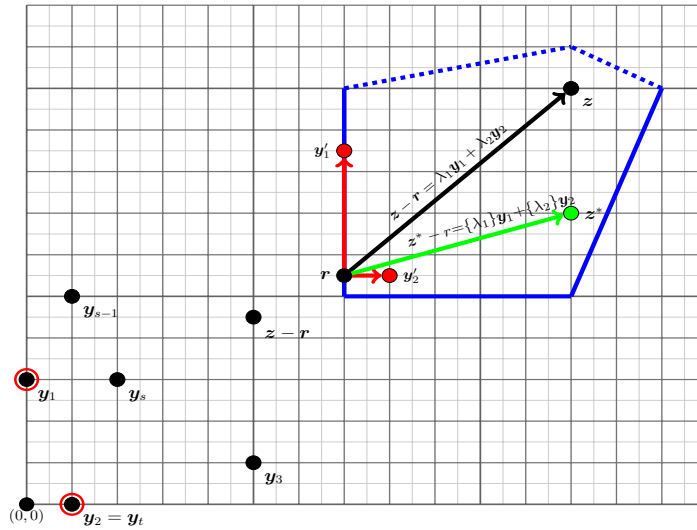
Observe that for any  $\mu_1, \dots, \mu_t$  with  $0 \leq \mu_i \leq \lambda_i$  for  $i \in [1, t]$ , the vector

$$\mathbf{r} + \mu_1 \mathbf{y}_1 + \dots + \mu_t \mathbf{y}_t$$

is still a solution to  $A\mathbf{x} \leq \mathbf{b}$ . Indeed,  $A_1 \mathbf{y}_i \geq \mathbf{0}$  and  $A_2 \mathbf{y}_i \leq \mathbf{0}$  implies

$$A_1(\mathbf{r} + \mu_1 \mathbf{y}_1 + \dots + \mu_t \mathbf{y}_t) \leq A_1 \mathbf{z} \leq \mathbf{b}_1, \text{ and}$$

$$A_2(\mathbf{r} + \mu_1 \mathbf{y}_1 + \dots + \mu_t \mathbf{y}_t) \leq A_2 \mathbf{r} \leq \mathbf{b}_2,$$



**Figure 1** The main idea behind Lemma 4.8. The region enclosed by blue lines depicts the solution space of the given system of linear inequalities. As mentioned in the lemma,  $r$  and  $z$  are respectively the given rational and integral solutions. Due to Lemma 4.6, we know that  $C$  (containing  $z - r$ ) can be obtained as a cone of integer vectors  $y_1, \dots, y_s$ . Moreover, by Carathéodory's theorem, we know that there are  $t$  linearly independent ( $t = 2$  in this case) vectors whose cone contains  $z - r$ . Intuitively, these vectors  $(y_1, y_2)$  form a coordinate system for searching the required  $z^*$ . For  $i \in \{1, 2\}$ ,  $y'_i = y_i + r$ ,  $\{\lambda_i\} = \lambda_i - \lfloor \lambda_i \rfloor$ .

and thus  $A(r + \mu_1 y_1 + \dots + \mu_t y_t) \leq b$ . In particular, the vector

$$z^* = r + (\lambda_1 - \lfloor \lambda_1 \rfloor) y_1 + \dots + (\lambda_t - \lfloor \lambda_t \rfloor) y_t$$

is a solution to  $Ax \leq b$ . Moreover,  $z^*$  is obtained from  $z$  by subtracting integer multiples of the integer vectors  $y_1, \dots, y_t$ , and thus  $z^*$  is integral as well. Finally, we have

$$\|z^* - r\|_\infty = \|(\lambda_1 - \lfloor \lambda_1 \rfloor) y_1 + \dots + (\lambda_t - \lfloor \lambda_t \rfloor) y_t\|_\infty \leq \sum_{i=1}^t \|y_i\|_\infty \leq n\Delta. \quad \blacktriangleleft$$

**Proof of Proposition 4.1.** According to Lemma 4.5, there is a rational solution  $\frac{1}{a}Eb$  to  $Ax \leq b$ , where  $E \in \mathbb{Z}^{n \times \ell}$ ,  $a \in \mathbb{Z} \setminus \{0\}$ ,  $|a| \leq \Delta$ , and  $\|E\|_\infty \leq \Delta$ . We set  $D := \frac{1}{a}E$ . Now since  $Ax \leq b$  has an integral solution, Lemma 4.8 yields an integral solution  $z^*$  close to  $D\mathbf{b}$ , meaning  $\|z^* - D\mathbf{b}\|_\infty \leq n\Delta$ . We set  $\mathbf{d} := z^* - D\mathbf{b}$ . Then of course  $D\mathbf{b} + \mathbf{d} = z^*$  is an integral solution to  $Ax \leq b$ . Moreover, we clearly have  $\|\mathbf{d}\|_\infty \leq n\Delta$ . It remains to show that even  $\|\mathbf{d}\|_{\text{frac}} \leq n\Delta^2$ . Indeed, since  $z^*$  is integral,  $\mathbf{b}$  is integral, and  $D = \frac{1}{a}E$  with integral  $E$ , we know that in  $\mathbf{d} = z^* - D\mathbf{b}$ , every entry can be written with  $a$  as its denominator. As this fraction has absolute value at most  $n\Delta$  and  $|a| \leq \Delta$ , both numerator and denominator have absolute value at most  $n\Delta^2$ .  $\blacktriangleleft$

## 5 Matching complexity lower bounds

In this section we prove the lower bounds for Corollaries 3.5 and 3.6.

**Detecting WQOs.** We begin with the lower bound for Corollary 3.5. That is, we show that deciding whether an existential Presburger formula defines a WQO is coNEXP hard. The idea is essentially the same as the coNP lower bound for detecting WQOs for quantifier-free

## 142:12 An Efficient Quantifier Elimination Procedure for Presburger Arithmetic

formulas in [3, Sec. 8]. The proof follows from reducing the satisfiability problem for  $\Pi_2$  sentences to WQO-definability of existential Presburger formulas. Given an instance  $\gamma$  of a  $\Pi_2$  sentence, we synthesize an existential Presburger formula  $\varphi$  and show that  $\varphi$  defines a WQO iff  $\gamma$  is satisfiable. The **coNEXP**-completeness of  $\Pi_2$  sentences follows from the **NEXP**-completeness of  $\Sigma_2$  sentences [17].

Consider an instance of a  $\Pi_2$  sentence

$$\gamma := \forall \mathbf{y}: \exists \mathbf{x}: \psi(\mathbf{x}, \mathbf{y})$$

where  $\psi$  is quantifier-free,  $\mathbf{x}$  ranges over  $\mathbb{Z}^n$ , and  $\mathbf{y}$  ranges over  $\mathbb{Z}^m$ . The goal is to construct an existential PA formula  $\varphi$  such that  $\varphi$  defines a WQO iff  $\gamma$  is true. First we define the formula

$$\Gamma(\mathbf{y}) := \exists \mathbf{x} \psi(\mathbf{x}, \mathbf{y})$$

Now, define the existential Presburger formula  $\varphi$  as follows.

$$\begin{aligned} \varphi((x, \mathbf{x}), (\mathbf{y}, \mathbf{y})) := & (x < 0 \wedge \mathbf{y} < 0) \vee (x > 0 \wedge \mathbf{y} > 0) \vee (x < 0 \wedge \mathbf{y} = 0) \\ & \vee (x = 0 \wedge \mathbf{y} > 0) \vee (x = 0 \wedge \mathbf{y} = 0) \\ & \vee (x < 0 \wedge \mathbf{y} > 0 \wedge \Gamma(\mathbf{y})). \end{aligned}$$

Here, both  $\mathbf{x}$  and  $\mathbf{y}$  range over  $\mathbb{Z}^m$ , hence  $\varphi$  defines a relation in  $\mathbb{Z}^{1+m} \times \mathbb{Z}^{1+m}$ . Since the existential quantifiers of  $\Gamma$  can be moved in front of  $\varphi$ ,  $\varphi$  is an existential Presburger instance.

► **Lemma 5.1.**  *$\varphi$  defines a WQO if and only if  $\gamma$  is true i.e.  $\Gamma(\mathbf{w})$  is true  $\forall \mathbf{w} \in \mathbb{Z}^m$ .*

**Proof.** ( $\Rightarrow$ ) Let  $\varphi$  define a WQO. Assume for contradiction there exists  $\mathbf{w} \in \mathbb{Z}^m$  such that  $\Gamma(\mathbf{w})$  is false. Notice that, by definition,  $\varphi((-1, \mathbf{w}), (0, \mathbf{w}))$  and  $\varphi((0, \mathbf{w}), (1, \mathbf{w}))$  are true. By transitivity, we must have that  $\varphi((-1, \mathbf{w}), (1, \mathbf{w}))$  is true. Therefore,  $\Gamma(\mathbf{w})$  must be true. This is a contradiction.

( $\Leftarrow$ ) Let  $\Gamma(\mathbf{w})$  be true for all  $\mathbf{w} \in \mathbb{Z}^m$ . Let  $A, B$  and  $C$  be sets of all vectors over  $\mathbb{Z}^{1+m}$  with negative, zero and positive first component, respectively. It is easy to see that  $\varphi$  relates all vectors within each of  $A, B$  and  $C$ . Further,  $\varphi(\mathbf{u}, \mathbf{v})$  is true if

- $\mathbf{u} \in A$  and  $\mathbf{v} \in B$ , or
- $\mathbf{u} \in B$  and  $\mathbf{v} \in C$ , or
- $\mathbf{u} \in A$  and  $\mathbf{v} \in C$ .

This means that  $\varphi$  must be a transitive, reflexive relation. Hence,  $\varphi$  trivially defines a WQO: in any infinite sequence  $\mathbf{u}_1, \mathbf{u}_2, \dots$  of vectors over  $\mathbb{Z}^{1+m}$ , we can always find  $\mathbf{u}_i, \mathbf{u}_j$  with  $i < j$  such that both  $\mathbf{u}_i, \mathbf{u}_j$  belong to either  $A$  or  $B$  or  $C$ . Since  $\varphi$  relates all vectors within each of these, the lemma follows. ◀

**Monadic decomposability.** Let us now show the lower bound for Corollary 3.6, i.e., that monadic decomposability for  $\exists$ PA formulas is **coNEXP**-hard. The idea is the same as the **coNP**-hardness for quantifier-free formulas in [2]<sup>2</sup>. We reduce from the  $\Pi_2$ -fragment of Presburger arithmetic, which is known to be **coNEXP**-complete (see the discussion around Corollary 3.3). Suppose we are given a  $\Pi_2$ -formula  $\varphi = \forall \mathbf{x} \exists \mathbf{y}: \psi(\mathbf{x}, \mathbf{y})$ , where  $\mathbf{x}$  contains  $n$  variables, and  $\mathbf{y}$  contains  $m$  variables. We claim that the existential formula  $\kappa = \exists \mathbf{y}: \psi(\mathbf{x}, \mathbf{y}) \vee z_1 = z_2$  (which has free variables  $\mathbf{x}, z_1, z_2$ ) is monadically decomposable if and only if  $\varphi$  holds (see Section 5), which would clearly complete the reduction.

<sup>2</sup> As Anthony W. Lin and Matthew Hague explained to us, it would also not be difficult to adapt the idea of the **coNP** lower bound in [20, Lem. 2].

Indeed, if  $\varphi$  holds, then  $\kappa$  is satisfied for every vector in  $\mathbb{Z}^{n+2}$  and is thus clearly monadically decomposable. Conversely, if  $\varphi$  does not hold, then there is some  $\mathbf{a} \in \mathbb{Z}^n$  so that  $\exists \mathbf{y}: \psi(\mathbf{a}, \mathbf{y})$  fails to hold. If  $\kappa$  were monadically decomposable, then so would the formula  $\kappa \wedge \mathbf{x} = \mathbf{a}$ , but this is equivalent to  $z_1 = z_2$ , which is clearly not monadically decomposable. This establishes the claim and hence coNEXP-hardness.

## 6 An exponential lower bound for quantifier elimination

Our main results show that one can eliminate a block of existential quantifiers with only an exponential blow-up. Using an example from [17, Thm. 2], we will now prove an exponential lower bound, even if constants are encoded in binary.

In the presence of binary encoded constants, we cannot use Weispfenning's lower bound argument [33, Thm. 3.1] (even for a singly exponential lower bound), which compares norms of vectors in finite sets defined by  $\exists$ PA vs. quantifier-free formulas. Indeed, it is a simple consequence of Pottier's bounds on Hilbert bases [24] that finite sets defined by  $\exists$ PA formulas consist of at most exponentially large vectors. With binary encoded constants, one easily constructs quantifier-free formulas defining finite sets of exponentially large vectors.

Instead, we measure the periodicity of infinite sets. Recall that every Presburger formula with one free variable defines an *ultimately periodic* set  $S \subseteq \mathbb{Z}$ , meaning that there are  $n_0, p \in \mathbb{N}$ ,  $p \geq 1$ , such that for every  $n \in \mathbb{Z}$ ,  $|n| \geq n_0$ , we have  $n + p \in S$  if and only if  $n \in S$ . Such a  $p$  is called a *period* of  $S$ . For a formula  $\varphi$  with one free variable, we denote by  $|\varphi|_p$  the *smallest* period of the set defined by  $\varphi$ . In [17, Thm. 2], Haase constructs<sup>3</sup> a sequence  $(\Phi_n(x))_{n \geq 0}$  of  $\exists$ PA formulas of size  $O(n^2)$  such that  $|\Phi_n|_p$  is at least  $2^{2^{\Omega(n)}}$ . The following will imply that the formulas  $\Phi_n$  require exponential-sized quantifier-free equivalents:

► **Lemma 6.1.** *Let  $\varphi$  be quantifier-free with one free variable. Then  $|\varphi|_p \leq 2^{|\varphi|}$ .*

**Proof.** We prove this by structural induction. If  $\varphi$  is an atom  $ax \leq b$ , then  $|\varphi|_p = 1$ . If  $\varphi$  is an atom  $ax \equiv b \pmod{c}$  with constants  $a, b, c$  written in binary, then  $|\varphi|_p \leq |c| \leq 2^{|\varphi|}$ . Moreover,  $|\neg\varphi|_p = |\varphi|_p$ . Now observe that if  $S_1, S_2 \subseteq \mathbb{Z}$  are ultimately periodic sets, then we have  $|S_1 \cup S_2|_p \leq |S_1|_p \cdot |S_2|_p$  and  $|S_1 \cap S_2|_p \leq |S_1|_p \cdot |S_2|_p$ . This implies  $|\varphi_1 \vee \varphi_2|_p \leq |\varphi_1|_p \cdot |\varphi_2|_p \leq 2^{|\varphi_1| + |\varphi_2|} \leq 2^{|\varphi|}$  and similarly  $|\varphi_1 \wedge \varphi_2|_p \leq |\varphi_1|_p \cdot |\varphi_2|_p \leq 2^{|\varphi_1| + |\varphi_2|} \leq 2^{|\varphi|}$ . ◀

Now indeed, if  $(\varphi_n)_{n \geq 0}$  is a sequence of quantifier-free equivalents of  $(\Phi_n)_{n \geq 0}$ , then for some constant  $c > 0$  and large  $n$ , we have  $2^{|\varphi_n|} \geq |\varphi_n|_p = |\Phi_n|_p \geq 2^{2^{cn}}$  and hence  $|\varphi_n| \geq 2^{cn}$ .

## References

- 1 Parosh A. Abdulla, Karlis Čerāns, Bengt Jonsson, and Yih-Kuen Tsay. Algorithmic analysis of programs with well quasi-ordered domains. *Inform. and Comput.*, 160(1–2):109–127, 2000. doi:10.1006/inco.1999.2843.
- 2 Pascal Bergsträßer, Moses Ganardi, Anthony W. Lin, and Georg Zetsche. Ramsey quantifiers in linear arithmetics. In *Proc. POPL 2024*, pages 1–32, 2024. doi:10.1145/3632843.
- 3 Pascal Bergsträßer, Moses Ganardi, Anthony W. Lin, and Georg Zetsche. Ramsey quantifiers in linear arithmetics, 2023. doi:10.48550/arXiv.2311.04031.
- 4 Itshak Borosh and Leon B. Treybig. Bounds on positive integral solutions of linear Diophantine equations. *P. Am. Math. Soc.*, 55:299–304, 1976. doi:10.1090/S0002-9939-1976-0396605-3.

<sup>3</sup> See also Appendix B.

- 5 W. Cook, A. M. H. Gerards, A. Schrijver, and É. Tardos. Sensitivity theorems in integer linear programming. *Math. Program.*, 34:251–264, 1986. doi:10.1007/BF01582230.
- 6 D. C. Cooper. Theorem proving in arithmetic without multiplication. In Bernard Meltzer and Donald Michie, editors, *Proceedings of the Seventh Annual Machine Intelligence Workshop, Edinburgh, 1971*, volume 7, pages 91–99. Edinburgh University Press, 1972.
- 7 Alain Finkel. A generalization of the procedure of Karp and Miller to well structured transition systems. In *Proc. ICALP 1987*, volume 267 of *Lecture Notes in Computer Science*, pages 499–508. Springer, 1987. doi:10.1007/3-540-18088-5\_43.
- 8 Alain Finkel and Ekanshdeep Gupta. The well structured problem for Presburger counter machines. In *Proc. FSTTCS 2019*, volume 150 of *LIPICs*, pages 41:1–41:15. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPICs.FSTTCS.2019.41.
- 9 Alain Finkel and Ekanshdeep Gupta. The well structured problem for Presburger counter machines. *CoRR*, abs/1910.02736, 2019. doi:10.48550/arXiv.1910.02736.
- 10 Alain Finkel and Philippe Schnoebelen. Well-structured transition systems everywhere! *Theor. Comput. Sci.*, 256(1–2):63–92, 2001. doi:10.1016/S0304-3975(00)00102-X.
- 11 Michael J. Fischer and Michael O. Rabin. Super-exponential complexity of Presburger arithmetic. In Bob F. Caviness and Jeremy R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 122–135, Vienna, 1998. Springer Vienna. doi:10.1007/978-3-7091-9459-1\_5.
- 12 Martin Fürer. The complexity of Presburger arithmetic with bounded quantifier alternation depth. *Theor. Comput. Sci.*, 18:105–111, 1982. doi:10.1016/0304-3975(82)90115-3.
- 13 Seymour Ginsburg and Edwin H Spanier. Bounded regular sets. *P. Am. Math. Soc.*, 17(5):1043–1049, 1966. doi:10.1090/S0002-9939-1966-0201310-3.
- 14 Erich Grädel. Dominoes and the complexity of subclasses of logical theories. *Ann. Pure Appl. Log.*, 43(1):1–30, 1989. doi:10.1016/0168-0072(89)90023-7.
- 15 Stéphane Grumbach, Philippe Rigaux, and Luc Segoufin. Spatio-temporal data handling with constraints. *GeoInformatica*, 5(1):95–115, 2001. doi:10.1023/A:1011464022461.
- 16 Florent Guépin, Christoph Haase, and James Worrell. On the existential theories of Büchi arithmetic and linear  $p$ -adic fields. In *Proc. LICS 2019*, pages 1–10. IEEE, 2019. doi:10.1109/LICS.2019.8785681.
- 17 Christoph Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *Proc. CSL-LICS 2014*, pages 47:1–47:10. ACM, 2014. doi:10.1145/2603088.2603092.
- 18 Christoph Haase and Georg Zetsche. Presburger arithmetic with stars, rational subsets of graph groups, and nested zero tests. In *Proc. LICS 2019*, pages 1–14. IEEE, 2019. doi:10.1109/LICS.2019.8785850.
- 19 Jacques Hadamard. Résolution d’une question relative aux déterminants. *B. Sci. Math.*, 2(17):240–246, 1893.
- 20 Matthew Hague, Anthony W. Lin, Philipp Rümmer, and Zhilin Wu. Monadic decomposition in integer linear arithmetic. In *Proc. IJCAR 2020*, volume 12166 of *Lecture Notes in Computer Science*, pages 122–140. Springer, 2020. doi:10.1007/978-3-030-51074-9\_8.
- 21 Gabriel Kuper, Leonid Libkin, and Jan Paredaens. *Constraint Databases*. Springer, 2000.
- 22 Mohan Nair. On Chebyshev-type inequalities for primes. *Am. Math. Mon.*, 89(2):126–129, 1982. doi:10.2307/2320934.
- 23 Derek C. Oppen. A  $2^{2^{2^{p^n}}}$  upper bound on the complexity of Presburger arithmetic. *J. Comput. Syst. Sci.*, 16(3):323–332, 1978. doi:10.1016/0022-0000(78)90021-1.
- 24 Loïc Pottier. Minimal solutions of linear diophantine systems: Bounds and algorithms. In *Proc. RTA 1991*, volume 488 of *Lecture Notes in Computer Science*, pages 162–173. Springer, 1991. doi:10.1007/3-540-53904-2\_94.
- 25 Mojżesz Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du I congrès de Mathématiciens des Pays Slaves*, pages 92–101. Ksiaznica Atlas, 1929.

- 26 C. R. Reddy and Donald W. Loveland. Presburger arithmetic with bounded quantifier alternation. In *Proc. STOC 1978*, pages 320–325, New York, NY, USA, 1978. ACM. doi:10.1145/800133.804361.
- 27 J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(1):64–94, 1962. doi:10.1215/ijm/1255631807.
- 28 Sasha Rubin. Automata presenting structures: A survey of the finite string case. *Bull. Symb. Log.*, 14(2):169–209, 2008. doi:10.2178/BSL/1208442827.
- 29 Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1986.
- 30 Margus Veanes, Nikolaj S. Bjørner, Lev Nachmanson, and Sergey Bereg. Monadic decomposition. *J. ACM*, 64(2):14:1–14:28, 2017. doi:10.1145/3040488.
- 31 Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72(1):155–158, 1978. doi:10.1090/S0002-9939-1978-0500555-0.
- 32 Volker Weispfenning. The complexity of almost linear Diophantine problems. *J. Symb. Comput.*, 10(5):395–403, 1990. doi:10.1016/S0747-7171(08)80051-X.
- 33 Volker Weispfenning. Complexity and uniformity of elimination in Presburger arithmetic. In *Proc. ISSAC 1997*, pages 48–53. ACM, 1997. doi:10.1145/258726.258746.

## A More Details for Lemma 4.6

We recall Cramer’s rule which has been used in the proof.

► **Proposition A.1** (Cramer’s rule). *Let a system of  $n$  linear equations for  $n$  unknowns be represented as*

$$Ax = b,$$

where  $A$  is an invertible  $(n \times n)$  matrix. This system has as unique solution given by  $x = (x_1, x_2, \dots, x_n)$  where,

$$x_i = \frac{\det(A_i)}{\det(A)}$$

$A_i$  is the matrix formed by replacing the  $i$ th column of  $A$  by  $b$ .

## B Sets with large periods

The formula  $\Phi_n$  constructed by Haase in [17, Thm. 2] defines the set

$$S_n = \{a \in \mathbb{N} \mid \exists b: 1 < b < 2^n, b \text{ divides } a\}.$$

and Haase argues that the smallest period of  $S_n$  is  $2^{2^{\Omega(n)}}$ . While the latter is true, the argument in [17] does not quite show this. The proof of [17, Thm. 2] argues that the smallest period of  $S_n$  is the least common multiple of the numbers  $\{1, \dots, 2^n - 1\}$ , which is lower bounded by  $2^{2^{\Omega(n)}}$  according to Nair [22]. However, as we will see, the smallest period of  $S_n$  is in fact a slightly smaller number. It is still lower bounded  $2^{2^{\Omega(n)}}$ , but this requires a different argument. We present a correction.

An easy fix for the result would be to instead define the set

$$\begin{aligned} S'_n &= \{a \in \mathbb{N} \mid \exists b: 1 < b < 2^n, b \text{ does not divide } a\} \\ &= \{a \in \mathbb{N} \mid \exists b, c: 1 < b < 2^n, 1 \leq c < 2^n, b \text{ divides } a + c\}, \end{aligned}$$

## 142:16 An Efficient Quantifier Elimination Procedure for Presburger Arithmetic

for which a simple modification of the formulas  $\Phi_n$  in [17] yields a polynomial-sized  $\exists$ PA formula  $\Phi'_n$ . Moreover, the smallest period of  $S'_n$  is indeed the least common multiple of  $\{1, \dots, 2^n - 1\}$ , and so Nair's bound would apply.

However, one can show that the smallest period of  $S_n$  is indeed lower bounded by  $2^{2^{\Omega(n)}}$ , just not by the least common multiple of  $\{1, \dots, 2^n - 1\}$ . For any natural  $n \in \mathbb{N}$ , define the *primorial* of  $n$ , in symbols  $n\#$ , as the product of all primes  $\leq n$ . Thus, if  $p_1, p_2, \dots$  is the sequence of all primes in ascending order and  $\pi(n)$  is the number of all prime numbers  $\leq n$ , then

$$n\# = \prod_{i=1}^{\pi(n)} p_i.$$

▷ **Claim B.1.** The smallest period of  $S_n$  is  $2^n\#$ .

*Proof.* Clearly,  $2^n\#$  is a period of  $S_n$ :  $S_n$  is the set of all numbers that have a prime divisor among  $\{2, \dots, 2^n - 1\}$ , and adding or subtracting the product of all these primes does not change that.

It remains to show that  $2^n\#$  is the smallest period of  $S_n$ . Suppose  $k$  is a period of  $S_n$ . We will show that every prime  $p$  with  $1 < p < 2^n$  is a divisor of  $k$ , which will clearly establish the claim. Let  $\{p_1, \dots, p_\ell\}$  be the primes in  $\{2, \dots, 2^n - 1\}$ . Towards a contradiction, suppose there is a prime  $p_j$ ,  $1 \leq j \leq \ell$ , that does not divide  $k$ . By the Chinese Remainder Theorem, the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{p_i} && \text{for each } i \in \{1, \dots, \ell\}, i \neq j, \\ x &\equiv -k \pmod{p_j} \end{aligned}$$

has infinitely many solutions  $a \in \mathbb{N}$ . For each such  $a$ , we have  $a \notin S_n$ , because  $a$  is not divisible by any  $p_i$ ,  $1 \leq i \leq \ell$ . However,  $a + k$  is divisible by  $p_j$ , and thus  $a + k \in S_n$ . Therefore,  $k$  cannot be a period of  $S_n$ . ◁

Using Claim B.1, we can now obtain the  $2^{2^{\Omega(n)}}$  lower bound for the smallest period of  $S_n$ . This is because equation (3.14) of [27] implies that for every  $m \geq 563$ , we have  $m\# \geq 2^{m-1}$ . In particular, for  $n \geq 10$ , we have  $2^n\# \geq 2^{2^n-1}$ . This proves that  $|\Phi_n|_p$  is lower bounded by  $2^{2^{\Omega(n)}}$ .

### **C** Incorrect lower bounds on eliminating a block of existential quantifiers

We elaborate on a flaw in Weispfenning's paper [33] which is a consequence of misinterpreting results from the literature, from which he incorrectly concludes that the elimination of a block of existential quantifiers from a formula of Presburger arithmetic results in an inherent doubly exponential blow-up.

The main result of Section 3 of [33] is Theorem 3.1, which states that performing quantifier elimination on *arbitrary* formulas of Presburger arithmetic results in an inherent triply exponential blow-up, assuming unary encoding of numbers. To this end, Weispfenning invokes a result by Fischer and Rabin [11] who showed that there exists a function  $g: \mathbb{N} \rightarrow \mathbb{N}$  such that for almost all  $n$ ,

$$g(n) \geq 2^{2^{2^{n+1}}},$$



and who gave a family of formulas  $\Phi_n(x, y, z)$  of Presburger arithmetic of size linear in  $n$  such that  $\Phi_n(x, y, z)$  holds if and only if  $0 \leq x, y, z < g(n)$  and  $x \cdot y = z$ . He then goes on concluding that the smallest quantifier-free formula defining the set  $\{z \in \mathbb{Z} \mid \Phi_n(1, z, z)\}$  requires a formula of size at least  $g(n)$ , assuming unary encoding of numbers.

Weispfenning then continues sketching how to adapt this approach in the presence of a bounded number of quantifier alternations. To this end, he appeals to a result by Fürer [12], which states that for some constant  $r > 0$ , one can define multiplication up to

$$2^{2^{(n/a)^{ra}}} \tag{4}$$

using a formula of length  $n$  and  $a$  quantifier alternations. Adapting his line of reasoning from the general case, Weispfenning applies this to  $a = 1$  and concludes that eliminating a block of existential quantifiers yields an inherent doubly exponential blow up. Fürer does indeed claim the existence of such a family in the third paragraph in [12, p. 108]. However, a close inspection of Fürer's proof reveals that these formulas are not constructed *for every  $a$  and  $n$* , but only *for infinitely many  $a$  and  $n$* . More specifically, Fürer supposes some given  $k, m \in \mathbb{N}$  and constructs a formula of length  $c(mk \log k + 1)$  and  $2m + d$  quantifier alternations (see the seventh paragraph in [12, p. 108]). Here,  $c$  and  $d$  appear to be unspecified constants. By choosing  $a = 2m + d$  and  $n = c(mk \log k + 1)$ , Fürer's claims then yield multiplication up to (4) for a suitable  $r > 0$ . In particular, Fürer's construction does not yield the existence of such formulas for *every*  $a \in \mathbb{N}$ .

Of course, from the fact that existential Presburger arithmetic allows for defining ultimately periodic sets with a doubly exponential period, cf. Appendix B, it is not unreasonable to believe that this could somehow be turned into a lower bound similar to the one claimed by Weispfenning. However, such large periods can already be produced by an exponential intersection of divisibility constraints and thus do not imply a doubly exponential lower bound on the formula size after eliminating a block of existentially quantified variables.