Efficient Quantifier Elimination in PA

Christoph Haase [1] Shankara Narayanan Krishna[2] Khushraj Madnani [3] Om Swostik [2] Georg Zetzsche [3]

[1]University of Oxford
[2]IIT Bombay
[3]MPI-SWS

July 12, 2024

Introduction

- Presburger Arithmetic is the first order theory of the structure $(\mathbb{Z}; +, <, 0, 1)$.

Introduction

- Presburger Arithmetic is the first order theory of the structure $(\mathbb{Z}; +, <, 0, 1)$.
- To enable quantifier elimination, we allow modulo constraints in formulas.

Introduction

- Presburger Arithmetic is the first order theory of the structure $(\mathbb{Z}; +, <, 0, 1)$.
- To enable quantifier elimination, we allow modulo constraints in formulas.
- Atomic formulas are of the following form:
  - $a_1x_1 + \cdots + a_nx_n \leq b$
  - $a_1x_1 + \cdots + a_nx_n \equiv b \mod m$

  where $x_1, \ldots, x_n$ are variables and $a_1, \ldots, a_n, b, m \in \mathbb{Z}$ are constants.

Introduction

- Presburger Arithmetic is the first order theory of the structure $(\mathbb{Z}; +, <, 0, 1)$.
- To enable quantifier elimination, we allow modulo constraints in formulas.
- Atomic formulas are of the following form:
  - $a_1x_1 + \cdots + a_nx_n \leq b$
  - $a_1x_1 + \cdots + a_nx_n \equiv b \mod m$

  where $x_1, \ldots, x_n$ are variables and $a_1, \ldots, a_n, b, m \in \mathbb{Z}$ are constants.
- A formula is quantifier-free if it is a Boolean combination of atomic formulas.

An Example

- Given positive integers $m_1, m_2, \ldots m_n$, what is the largest number that cannot be obtained as a non-negative linear combination of those numbers? The answer, if it exists, is the smallest satisfying assignment of the formula:

$$\Phi(x) = \forall y\, (x < y \longrightarrow (\exists z_1, z_2 \ldots z_n(y = z_1 m_1 + \cdots + z_n m_n \\ \wedge z_1 \geq 0 \wedge \cdots \wedge z_n \geq 0)))$$

(For the case $n = 2$, look up Chicken Mcnugget Theorem!)

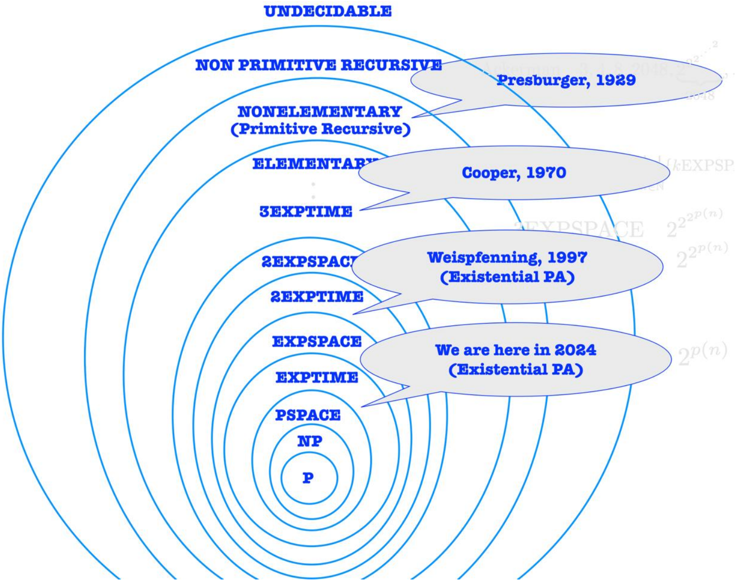
Quantifier Elimination

- In 1929, Mojżesz Presburger formulated the basic principles of PA and showed that it is complete and decidable.

Quantifier Elimination

- In 1929, Mojżesz Presburger formulated the basic principles of PA and showed that it is complete and decidable.
- This result was achieved by using the quantifier elimination method.

Complexity of Quantifier Elimination



Main Result

Theorem

Given a formula φ in existential Presburger arithmetic, we can compute in exponential time an equivalent quantifier-free formula ψ of size exponential in φ. Moreover, all constants in ψ are encoded in unary.

Main Result

Theorem

Given a formula φ in existential Presburger arithmetic, we can compute in exponential time an equivalent quantifier-free formula ψ of size exponential in φ. Moreover, all constants in ψ are encoded in unary.

The main ingredient for proving this is the following proposition,

Main Result

Theorem

Given a formula φ in existential Presburger arithmetic, we can compute in exponential time an equivalent quantifier-free formula ψ of size exponential in φ. Moreover, all constants in ψ are encoded in unary.

The main ingredient for proving this is the following proposition,

Proposition

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

where $||.||_{\mathrm{frac}}$ denotes the maximal absolute value of all numerators and denominators in the representation.

Example for Proposition

Consider the formula $(x_1 - x_2 \leq 3) \wedge (x_1 + 2x_2 \leq 4)$. This formula can be written as the system,

$$\begin{bmatrix} 1 & -1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \leq \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

Let

$$(D, d) = \left(\begin{bmatrix} 2 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$$

Setting $x = Db + d$ gives $(x_1, x_2) = (2, 0)$, which is a satisfying assignment for the formula!

Proof of Proposition

Recall the proposition,

Proof of Proposition

Recall the proposition,

Proposition

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

Proof of Proposition

Recall the proposition,

Proposition

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

- The proposition claims a small model property for parametric integer programming.

Proof of Proposition

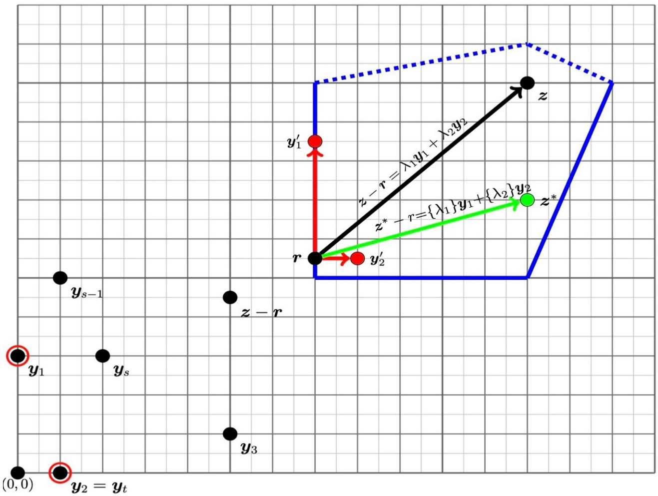
Recall the proposition,

Proposition

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

- The proposition claims a small model property for parametric integer programming.
- If the system $Ax \leq b$ has an integral solution, it has a rational solution of a specific form.

Proof of Proposition



For every rational solution r of $Ax \leq b$, we show that there is a close-by integral solution z^*.

Optimality

- An exponential blowup cannot be avoided when eliminating a block of existential quantifiers.

Optimality

- An exponential blowup cannot be avoided when eliminating a block of existential quantifiers.
- Every PA formula defines an *ultimately periodic* set. We have the following lemma,

Optimality

- An exponential blowup cannot be avoided when eliminating a block of existential quantifiers.
- Every PA formula defines an *ultimately periodic* set. We have the following lemma,

Lemma

Let φ be quantifier-free with one free variable. Then $|\varphi|_{\mathrm{p}} \leq 2^{|\varphi|}$.

where $|\varphi|_{\mathrm{p}}$ denotes the smallest period of the set defined by φ.

Optimality

- An exponential blowup cannot be avoided when eliminating a block of existential quantifiers.
- Every PA formula defines an *ultimately periodic* set. We have the following lemma,

Lemma

Let φ be quantifier-free with one free variable. Then $|\varphi|_{\mathrm{p}} \leq 2^{|\varphi|}$.

where $|\varphi|_{\mathrm{p}}$ denotes the smallest period of the set defined by φ.

- In [Haa14], Haase constructs a sequence $(\Phi_n(x))_{n\geq 0}$ of existential PA formulas of size $O(n^2)$ such that $|\Phi_n|_{\mathrm{p}}$ is at least $2^{2^{\Omega(n)}}$.

Optimality

- An exponential blowup cannot be avoided when eliminating a block of existential quantifiers.
- Every PA formula defines an *ultimately periodic* set. We have the following lemma,

Lemma

Let φ be quantifier-free with one free variable. Then $|\varphi|_\mathrm{p} \leq 2^{|\varphi|}$.

where $|\varphi|_\mathrm{p}$ denotes the smallest period of the set defined by φ.

- In [Haa14], Haase constructs a sequence $(\Phi_n(x))_{n\geq 0}$ of existential PA formulas of size $O(n^2)$ such that $|\Phi_n|_\mathrm{p}$ is at least $2^{2^{\Omega(n)}}$.
- Formulas Φ_n will require exponential sized quantifier equivalents.

An Application

- A *well-quasi-ordering* (WQO) is a reflexive and transitive ordering $(X, \leq)$ such that for every sequence $x_1, x_2, \ldots \in X$, there are $i < j$ with $x_i \leq x_j$.

An Application

- A *well-quasi-ordering* (WQO) is a reflexive and transitive ordering $(X, \leq)$ such that for every sequence $x_1, x_2, \ldots \in X$, there are $i < j$ with $x_i \leq x_j$.
- Given a quantifier-free formula $\varphi(x, y)$, deciding whether the relation $R \subseteq \mathbb{Z}^n \times \mathbb{Z}^n$ defined by φ is a WQO is coNP-complete [BGLZ24].

An Application

- A *well-quasi-ordering* (WQO) is a reflexive and transitive ordering $(X, \leq)$ such that for every sequence $x_1, x_2, \ldots \in X$, there are $i < j$ with $x_i \leq x_j$.
- Given a quantifier-free formula $\varphi(x, y)$, deciding whether the relation $R \subseteq \mathbb{Z}^n \times \mathbb{Z}^n$ defined by φ is a WQO is coNP-complete [BGLZ24].
- Our results allow us to settle the complexity for existential formulas:

Corollary

Given an existential PA formula φ, it is coNEXP*-complete to decide whether φ defines a WQO.*

More Applications

Corollary

The Σ_2-fragment of Presburger Arithmetic is in NEXP.

More Applications

Corollary

The Σ_2-fragment of Presburger Arithmetic is in NEXP*.*

Corollary

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

Conclusion

- Main result establishes a quantifier elimination procedure eliminating a block of existentially quantified variables in singly exponential time.
- All known algorithms before required doubly exponential time.
- The technical basis is a small model property for parametric integer programming.
- Implementing optimizations could lead to a more practical use of the algorithm in SMT solvers.

References I

[BGLZ24] Pascal Bergsträßer, Moses Ganardi, Anthony W. Lin, and Georg Zetzsche. Ramsey quantifiers in linear arithmetics. In *Proc. POPL 2024*, pages 1–32, 2024. doi:10.1145/3632843.

[Grä89] 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.

[Haa14] 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.

[HZ19] Christoph Haase and Georg Zetzsche. 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.

References II

[Sch86] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1986.