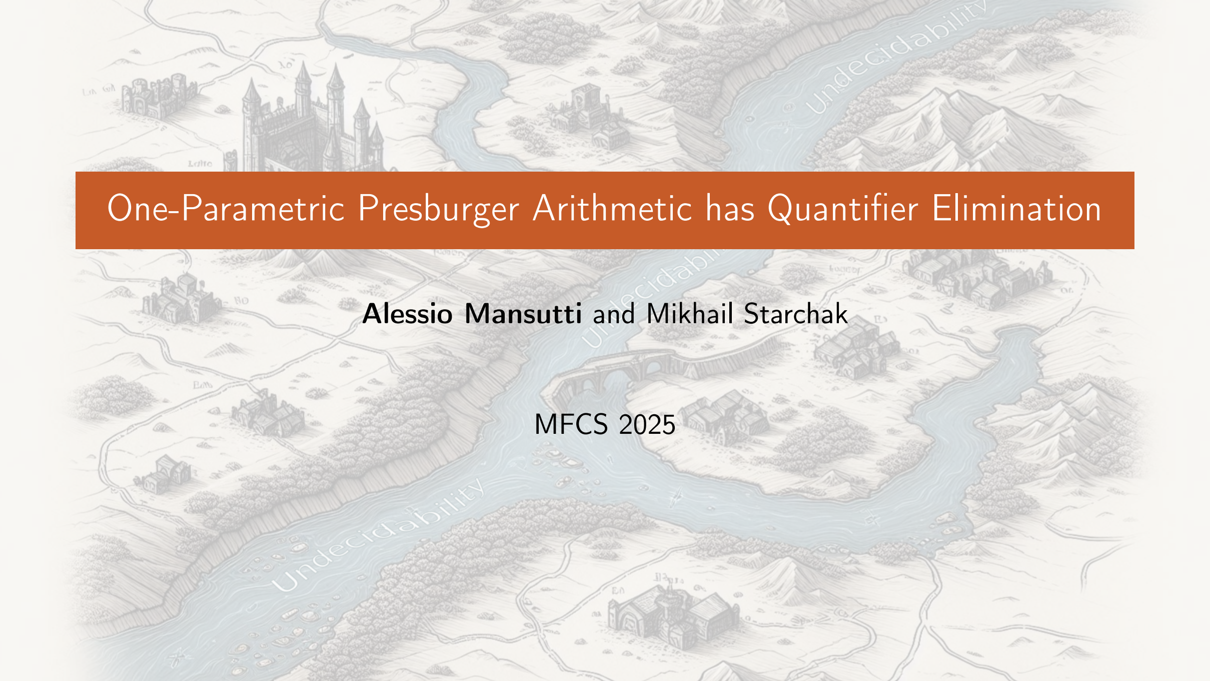


One-Parametric Presburger Arithmetic has Quantifier Elimination

Alessio Mansutti and Mikhail Starchak

MFCS 2025

Undecidability
Undecidability
Undecidability
Undecidability

Peano arithmetic

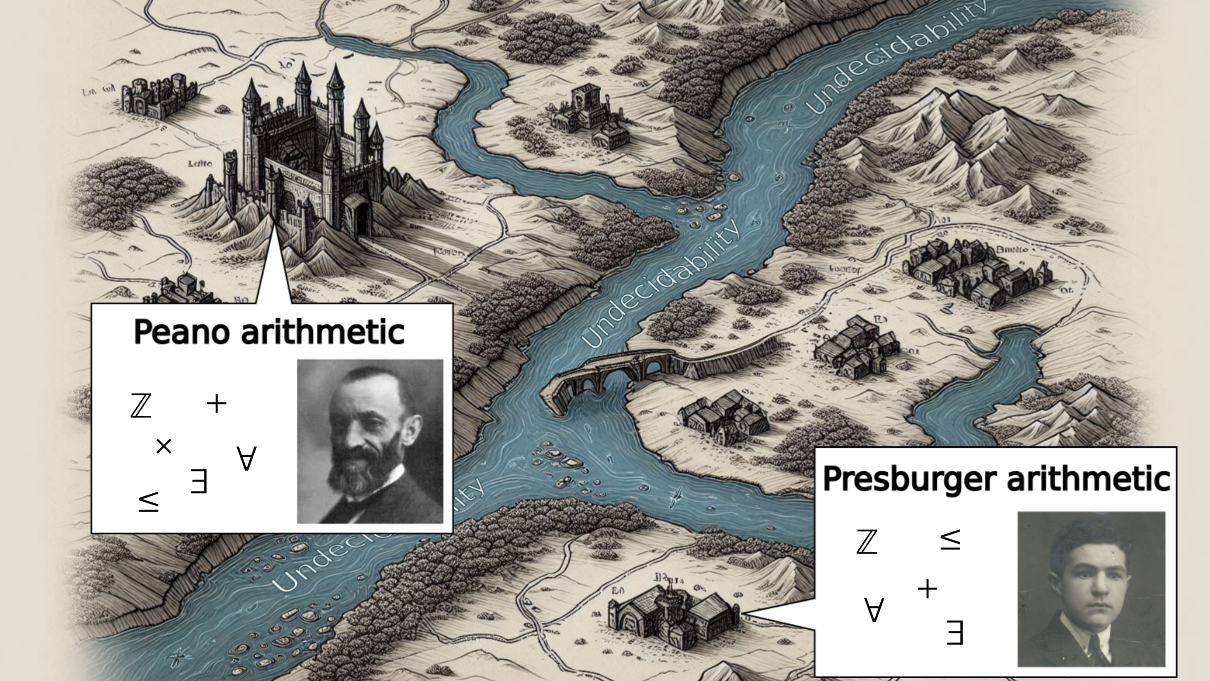
ℤ +

×

∀

∃

≤

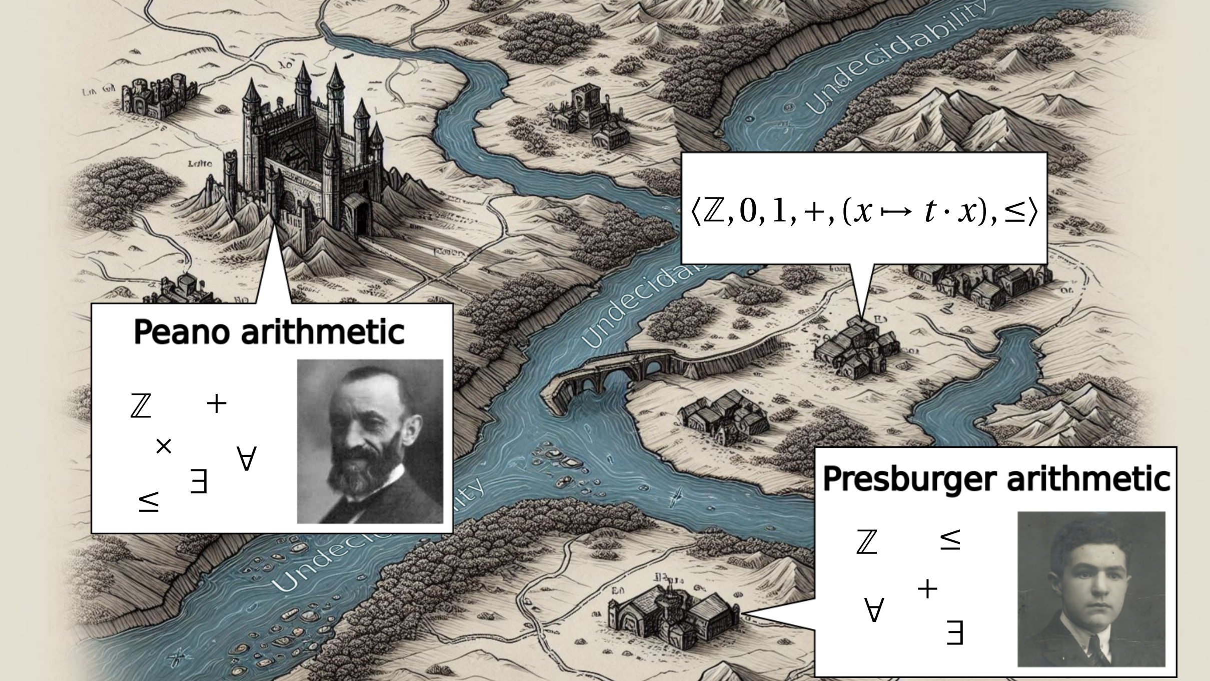


Peano arithmetic

$\mathbb{Z}$ $+$ $\times$ $\forall$ $\exists$ $\leq$

Presburger arithmetic

$\mathbb{Z}$ $\leq$ $+$ $\forall$ $\exists$



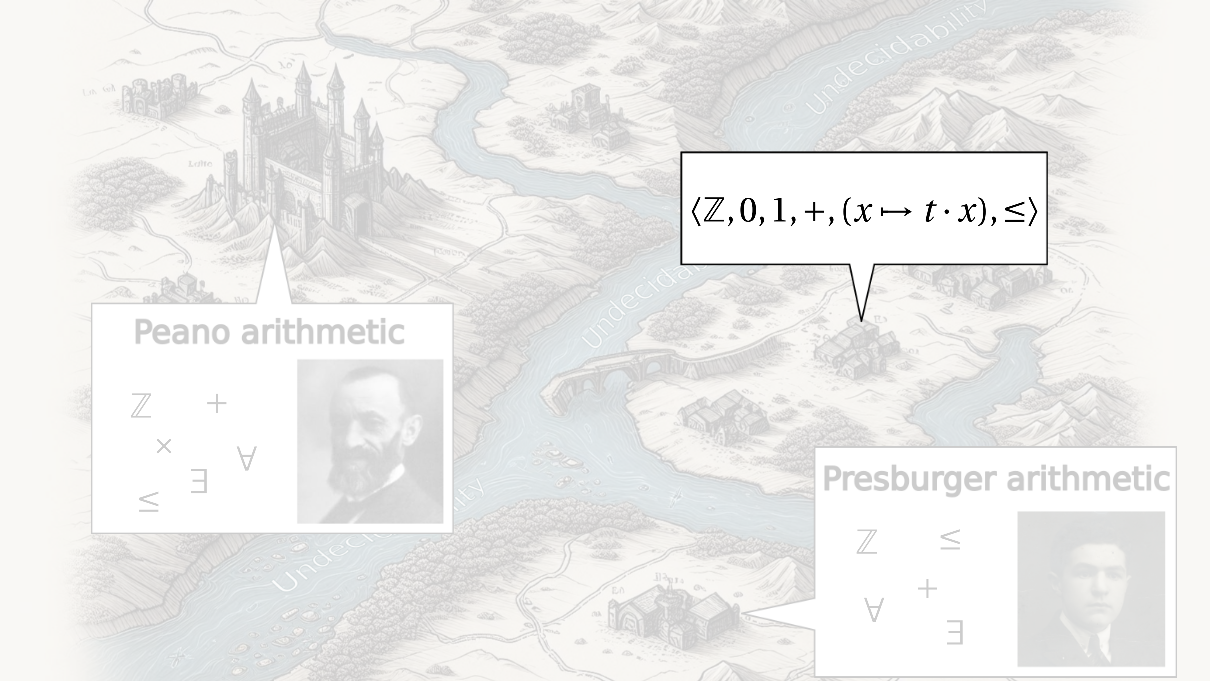
$\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$

Peano arithmetic

$\mathbb{Z}$ $+$ $\times$ $\forall$ $\exists$ $\leq$

Presburger arithmetic

$\mathbb{Z}$ $\leq$ $\forall$ $+$ $\exists$



$\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$

Peano arithmetic

$\mathbb{Z}$ $+$ $\times$ $\forall$ $\exists$ $\leq$

Presburger arithmetic

$\mathbb{Z}$ $\leq$ $+$ $\forall$ $\exists$

One-parametric Presburger arithmetic (1PPA)

First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

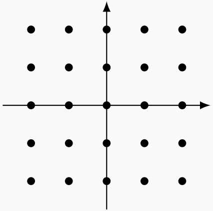
One-parametric Presburger arithmetic (1PPA)

First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

Twisting squares (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

$$|2x + (2t-2)y| \leq t^2 - 2t + 2 \ \wedge \ |(2-2t)x + 2y| \leq t^2 - 2t + 2$$



One-parametric Presburger arithmetic (1PPA)

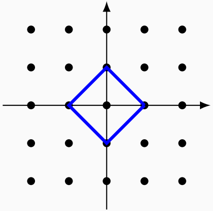
First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

Twisting squares (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

$$|2x + (2t-2)y| \leq t^2 - 2t + 2 \ \wedge \ |(2-2t)x + 2y| \leq t^2 - 2t + 2$$

$t = 0$: $\quad |2x - 2y| \leq 2 \ \wedge \ |2x + 2y| \leq 2$ $\quad$ 5 solutions



One-parametric Presburger arithmetic (1PPA)

First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

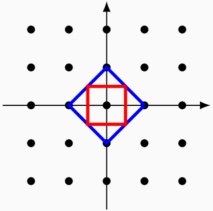
In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

Twisting squares (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

$$|2x + (2t-2)y| \leq t^2 - 2t + 2 \ \wedge \ |(2-2t)x + 2y| \leq t^2 - 2t + 2$$

$t = 0$: $|2x - 2y| \leq 2 \ \wedge \ |2x + 2y| \leq 2$ 5 solutions

$t = 1$: $|2x| \leq 1 \ \wedge \ |2y| \leq 1$ 1 solution



One-parametric Presburger arithmetic (1PPA)

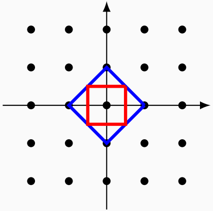
First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

Twisting squares (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

$$|2x + (2t-2)y| \leq t^2 - 2t + 2 \;\wedge\; |(2-2t)x + 2y| \leq t^2 - 2t + 2$$

$t = 0$:	$\lvert 2x - 2y\rvert \leq 2 \;\wedge\; \lvert 2x + 2y\rvert \leq 2$	5 solutions
$t = 1$:	$\lvert 2x\rvert \leq 1 \;\wedge\; \lvert 2y\rvert \leq 1$	1 solution
$t = 2$:	$\lvert 2x + 2y\rvert \leq 2 \;\wedge\; \lvert -2x + 2y\rvert \leq 2$	same as $t = 0$



One-parametric Presburger arithmetic (1PPA)

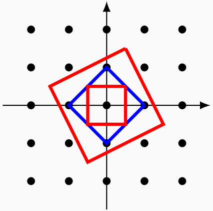
First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

Twisting squares (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

$$|2x + (2t-2)y| \leq t^2 - 2t + 2 \;\wedge\; |(2-2t)x + 2y| \leq t^2 - 2t + 2$$

$t = 0$:	$\|2x - 2y\| \leq 2 \;\wedge\; \|2x + 2y\| \leq 2$	5 solutions
$t = 1$:	$\|2x\| \leq 1 \;\wedge\; \|2y\| \leq 1$	1 solution
$t = 2$:	$\|2x + 2y\| \leq 2 \;\wedge\; \|-2x + 2y\| \leq 2$	same as $t = 0$
$t = 3$:	$\|2x + 4y\| \leq 5 \;\wedge\; \|-4x + 2y\| \leq 5$	5 solutions



One-parametric Presburger arithmetic (1PPA)

First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

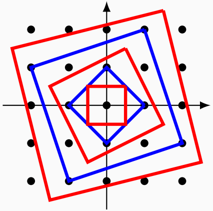
In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

Twisting squares (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

$$|2x + (2t-2)y| \leq t^2 - 2t + 2 \ \wedge \ |(2-2t)x + 2y| \leq t^2 - 2t + 2$$

For a fixed $t \geq 0$, this formula:

- has $t^2 - 2t + 2$ solutions when t is odd
- has $t^2 - 2t + 5$ solutions when t is even



One-parametric Presburger arithmetic (1PPA)

First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

"Chinese Remainder Theorem"

Let $f, g \in \mathbb{Z}[t]$. The following formula is valid:

$$\underbrace{\big(f \geq 1 \land g \geq 1 \land \exists u, v : f \cdot u + g \cdot v = 1\big)}_{f(t) \text{ and } g(t) \text{ are positive and coprime}} \implies \underbrace{\forall a \forall b \exists x : \quad \begin{aligned} & 0 \leq x < f \cdot g \\ & \land f \mid x - a \\ & \land g \mid x - b \end{aligned}}_{\text{CRT}}$$

where $(f \mid \tau) := \exists w\, (w \cdot f = \tau)$.

One-parametric Presburger arithmetic (1PPA)

First-order theory of the structure $\langle \mathbb{Z}, 0, 1, +, (x \mapsto t \cdot x), \leq \rangle$.

In the multiplication function $x \mapsto t \cdot x$, the parameter t is a fixed free variable.

A formula $\varphi(\boldsymbol{x})$ of 1PPA defines a parametric Presburger family $\{[\![\varphi]\!]_k : k \in \mathbb{Z}\}$, where

$$[\![\varphi]\!]_k : \text{set of solutions to } \varphi \text{ after replacing } t \text{ with } k$$

We can ask several questions about φ:

- satisfiability: is $[\![\varphi]\!]_k$ non-empty for some k?
- universality: is $[\![\varphi]\!]_k$ non-empty for every k?
- finiteness: is $[\![\varphi]\!]_k$ non-empty only for finitely many k?

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ be a 1PPA *formula. The counting function $f(k) := \#[\![\varphi]\!]_k$ is an EQP.*

A function $f : \mathbb{N} \to \mathbb{N}$ is an eventual quasi-polynomial (EQP) whenever there are

- a threshold T and a period P, and
- a family of univariate polynomials $f_0, \dots, f_{P-1}$

such that for every $n \geq T$, $f(n) = f_{(n \bmod P)}(n)$.

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ be a 1PPA *formula. The counting function $f(k) := \#[\![\varphi]\!]_k$ is an EQP.*

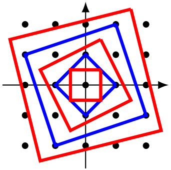
A function $f : \mathbb{N} \to \mathbb{N}$ is an eventual quasi-polynomial (EQP) whenever there are

- a threshold T and a period P, and
- a family of univariate polynomials $f_0, \ldots, f_{P-1}$

such that for every $n \geq T$, $f(n) = f_{(n \bmod P)}(n)$.

Examples:

$$\left\lfloor \frac{x}{2} \right\rfloor = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x-1}{2} & \text{if } x \text{ is odd} \end{cases}$$



Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ be a 1PPA *formula. The counting function $f(k) := \#[\![\varphi]\!]_k$ is an EQP.*

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ be a 1PPA *formula. The counting function $f(k) := \#[\![\varphi]\!]_k$ is an EQP.*

Proof idea: Show the result for quantifier-free formulae. Then,

$$\varphi \; = \; \exists x_1 \; \forall x_2 \; \ldots : \psi$$

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ be a 1PPA *formula. The counting function $f(k) := \#[\![\varphi]\!]_k$ is an EQP.*

Proof idea: Show the result for quantifier-free formulae. Then,

$$\varphi \; = \; \exists x_1 \; \forall x_2 \; \ldots : \psi$$

$$\Big\downarrow$$

bounded quantifier elimination (Weispfenning. *ISSAC 1997*)

"$\exists y \leq p(t)$" constrains y in $[0..p(t)]$

$$\varphi \; \equiv \; \exists y_1 \leq p_1(t) \; \forall y_2 \leq p_2(t) \; \ldots : \gamma$$

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ be a 1PPA *formula. The counting function $f(k) := \#[\![\varphi]\!]_k$ is an EQP.*

Proof idea: Show the result for quantifier-free formulae. Then,

$$\varphi \;=\; \exists x_1 \; \forall x_2 \; \dots : \psi$$

↓ *bounded quantifier elimination* (Weispfenning. *ISSAC 1997*)

"$\exists y \leq p(t)$" constrains y in $[0..p(t)]$

$$\varphi \;\equiv\; \exists y_1 \leq p_1(t) \; \forall y_2 \leq p_2(t) \; \dots : \gamma$$

↓ *parsimonious transformation* (Chen, Li, Sam. *Trans. Amer. Math. Soc. 2012*)

$\#[\![\varphi]\!]_k = \#[\![\varphi']\!]_k$ for every k

φ' quantifier-free

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ

Proof

In *Discrete Analysis 2017*, Bogart, Goodrick and Woods ask whether the parsimonious transformation can be replaced with quantifier elimination.

$$\varphi \;=\; \exists x_1 \; \forall x_2 \; \ldots : \psi$$

↓ *bounded quantifier elimination* (Weispfenning. *ISSAC 1997*)

"$\exists y \leq p(t)$" constrains y in $[0..p(t)]$

$$\varphi \;\equiv\; \exists y_1 \leq p_1(t) \; \forall y_2 \leq p_2(t) \; \ldots : \gamma$$

↓ *parsimonious transformation* (Chen, Li, Sam. *Trans. Amer. Math. Soc. 2012*)

$\#[\![\varphi]\!]_k = \#[\![\varphi']\!]_k$ for every k

φ' quantifier-free

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods. *Discrete Analysis 2017*)

Let φ

In *Discrete Analysis 2017*, Bogart, Goodrick and Woods ask whether the parsimonious transformation can be replaced with quantifier elimination.

Proof

$\varphi \equiv \exists x \; \forall x \; \dots : \gamma$

In *Arch. Math. Logic 2018*, Goodrick conjectures that extending 1PPA with a function $x \mapsto \left\lfloor \frac{x}{p(t)} \right\rfloor$ for every polynomial p suffices.

$$\varphi \;\equiv\; \exists y_1 \le p_1(t) \; \forall y_2 \le p_2(t) \; \dots : \gamma$$

parsimonious transformation (Chen, Li, Sam. *Trans. Amer. Math. Soc. 2012*)

$\#[\![\varphi]\!]_k = \#[\![\varphi']\!]_k$ for every k

φ' quantifier-free

Eventual quasi-polynomials and 1PPA

Theorem (Bogart, Goodrick, Woods, *Discrete Analysis 2017*)

Let φ

Proof

In *Discrete Analysis 2017*, Bogart, Goodrick and Woods ask whether the parsimonious transformation can be replaced with quantifier elimination.

$\varphi \equiv \exists y_1 \forall y_2 \dots : \gamma$

In *Arch. Math. Logic 2018*, Goodrick conjectures that extending 1PPA with a function $x \mapsto \left\lfloor \frac{x}{p(t)} \right\rfloor$ for every polynomial p suffices.

$\varphi \equiv \exists y_1 \leq p_1(t) \; \forall y_2 \leq p_2(t) \; \dots : \gamma$

parsi

ns. Amer. Math. Soc. 2012)

We prove Goodrick's conjecture.

$\#[\![\varphi]\!]_k$

φ' quantifier-free

Our results

Theorem

There is a quantifier elimination procedure for the extension of $1\mathsf{PPA}$ *with the functions:*

- *integer division:* $x \mapsto \left\lfloor \frac{x}{t^d} \right\rfloor$ *one function for each* $d \in \mathbb{N}$*, assuming* $t \neq 0$
- *integer remainder function:* $x \mapsto (x \bmod p)$ *for each* $p \in \mathbb{Z}[t]$
- *divisibility relation:* $p \mid x$ *for each* $p \in \mathbb{Z}[t]$

(The functions $x \mapsto \left\lfloor \frac{x}{p(t)} \right\rfloor$ capture all these functions and relations.)

Our results

Theorem

There is a quantifier elimination procedure for the extension of 1PPA *with the functions:*

- *integer division:* $x \mapsto \left\lfloor \frac{x}{t^d} \right\rfloor$ *one function for each* $d \in \mathbb{N}$*, assuming* $t \neq 0$
- *integer remainder function:* $x \mapsto (x \bmod p)$ *for each* $p \in \mathbb{Z}[t]$
- *divisibility relation:* $p \mid x$ *for each* $p \in \mathbb{Z}[t]$

(The functions $x \mapsto \left\lfloor \frac{x}{p(t)} \right\rfloor$ capture all these functions and relations.)

Theorem

For the class of all existential formulae of 1PPA*, the following holds:*

Satisfiability:	*Universality:*	*Finiteness:*
NP-*complete*	**coNEXP**-*complete*	**coNP**-*complete*

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA ($1\mathsf{PPA}^+$).
Output: A quantifier-free formula $\psi(\boldsymbol{z})$ from $1\mathsf{PPA}^+$ that is equivalent to $\exists \boldsymbol{x} \, \varphi$.

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula $\psi(\boldsymbol{z})$ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x} \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions

$$\cdots + \left\lfloor \frac{\tau}{t^d} \right\rfloor + \cdots \leq 0 \quad \to \quad \exists x \left(\cdots + x + \cdots \leq 0 \land \left(t^d x \leq \tau < t^d (x+1) \right) \right)$$

$$\cdots + (\tau \bmod p) + \cdots \leq 0 \quad \to \quad \exists x \left(\cdots + x + \cdots \leq 0 \land \left(0 \leq x < p - 1 \right) \land \left(p \mid \tau - x \right) \right)$$

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula $\psi(\boldsymbol{z})$ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x} \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions

$$\cdots + \left\lfloor \frac{\tau}{t^d} \right\rfloor + \cdots \leq 0 \quad \to \quad \exists x \big(\cdots + x + \cdots \leq 0 \land \big(t^d x \leq \tau < t^d (x+1) \big) \big)$$

$$\cdots + (\tau \bmod p) + \cdots \leq 0 \quad \to \quad \exists x \big(\cdots + x + \cdots \leq 0 \land \big(0 \leq x < p - 1 \big) \land \big(p \mid \tau - x \big) \big)$$

Step II. Bounded quantifier elimination:

$$\exists \boldsymbol{x}' : \varphi'(\boldsymbol{x}', \boldsymbol{z}) \quad \to \quad \exists \boldsymbol{w} \leq B \bigvee_i \gamma_i(\boldsymbol{w}, \boldsymbol{z})$$

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x},\boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
O

Before 2024: Quantifier elimination procedures for Presburger arithmetic required **2EXPTIME / NEXPTIME** to remove one block of existential quantifiers.

St

$$\cdots + \left\lfloor \frac{\tau}{t^d} \right\rfloor + \cdots \le 0 \quad \to \quad \exists x \left(\cdots + x + \cdots \le 0 \land \left(t^d x \le \tau < t^d (x+1) \right) \right)$$

$$\cdots + (\tau \bmod p) + \cdots \le 0 \quad \to \quad \exists x \left(\cdots + x + \cdots \le 0 \land \left(0 \le x < p-1 \right) \land \left(p \mid \tau - x \right) \right)$$

Step II. Bounded quantifier elimination:

$$\exists \boldsymbol{x}' : \varphi'(\boldsymbol{x}',\boldsymbol{z}) \quad \to \quad \exists \boldsymbol{w} \le B \bigvee_i \gamma_i(\boldsymbol{w},\boldsymbol{z})$$

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).

Before 2024: Quantifier elimination procedures for Presburger arithmetic required **2EXPTIME** / **NEXPTIME** to remove one block of existential quantifiers.

In ICALP'24: Two different procedures running in **EXPTIME** / **NP** were found, by [Chistikov, M., Starchak] and [Haase, Krishna, Madnani, Mishra, Zetzsche].

Step II. Bounded quantifier elimination:

We extend the quantifier elimination procedure from [Chistikov, M., Starchak] from Presburger arithmetic to one-parametric Presburger arithmetic.

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula ψ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x}\, \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions.

Step II. Bounded quantifier elimination: compute $\exists \boldsymbol{w} \leq B : \bigvee_i \gamma_i(\boldsymbol{w}, \boldsymbol{z})$.

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula ψ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x}\, \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions.

Step II. Bounded quantifier elimination: compute $\exists \boldsymbol{w} \leq B : \bigvee_i \gamma_i(\boldsymbol{w}, \boldsymbol{z})$.

Step III. Remove the divisibility relations:

$$f \mid \tau(\boldsymbol{w}) + \sigma(\boldsymbol{z}) \quad \to \quad f \mid \tau(\boldsymbol{w}) + (\sigma(\boldsymbol{z}) \bmod f)$$

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula ψ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x}\, \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions.

Step II. Bounded quantifier elimination: compute $\exists \boldsymbol{w} \leq B : \bigvee_i \gamma_i(\boldsymbol{w}, \boldsymbol{z})$.

Step III. Remove the divisibility relations:

$$f \mid \tau(\boldsymbol{w}) + \sigma(\boldsymbol{z}) \quad \to \quad f \mid \tau(\boldsymbol{w}) + (\sigma(\boldsymbol{z}) \bmod f)$$

Bounded!

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula ψ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x}\, \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions.

Step II. Bounded quantifier elimination: compute $\exists \boldsymbol{w} \leq B : \bigvee_i \gamma_i(\boldsymbol{w}, \boldsymbol{z})$.

Step III. Remove the divisibility relations:

$$\begin{aligned} f \mid \tau(\boldsymbol{w}) + \sigma(\boldsymbol{z}) \quad &\to \quad f \mid \tau(\boldsymbol{w}) + (\sigma(\boldsymbol{z}) \bmod f) \\ &\to \quad \exists w \leq p(t) : f \cdot w = \tau(\boldsymbol{w}) + (\sigma(\boldsymbol{z}) \bmod f) \end{aligned}$$

Overview of our procedure

Input: A quantifier-free formula $\varphi(\boldsymbol{x}, \boldsymbol{z})$ from the extended language of 1PPA (1PPA$^+$).
Output: A quantifier-free formula ψ from 1PPA$^+$ that is equivalent to $\exists \boldsymbol{x} \varphi$.

Step I. Preprocessing: Remove divisions and remainder functions.

Step II. Bounded quantifier elimination: compute $\exists \boldsymbol{w} \le B : \bigvee_i \gamma_i(\boldsymbol{w}, \boldsymbol{z})$.

Step III. Remove the divisibility relations:

$$\begin{aligned} f \mid \tau(\boldsymbol{w}) + \sigma(\boldsymbol{z}) \quad &\to \quad f \mid \tau(\boldsymbol{w}) + (\sigma(\boldsymbol{z}) \bmod f) \\ &\to \quad \exists w \le p(t) \colon f \cdot w = \tau(\boldsymbol{w}) + (\sigma(\boldsymbol{z}) \bmod f) \end{aligned}$$

Step IV. Elimination of bounded quantifiers by "bit blasting".

Step IV: Elimination of bounded quantifiers

$$\exists x \leq t^2 + t - 1 \ \exists z \leq t + 2 \ : \ (t+1) \cdot z = x + (-b \bmod t+1)$$

Assume $t \geq 2$.

Step IV: Elimination of bounded quantifiers

$$\exists x \leq t^2 + t - 1 \ \exists z \leq t + 2 \ : \ (t+1) \cdot z = x + (-b \bmod t + 1)$$

Assume $t \geq 2$. Bit blast:

$$\exists z \leq t + 2 \colon \varphi \quad \to \quad \exists z_0, z_1, z_2 \leq t - 1 \colon \quad 0 \leq z_2 \cdot t^2 + z_1 \cdot t + z_0 \leq t + 2$$

$$\wedge \, \varphi[z_2 \cdot t^2 + z_1 \cdot t + z_0 \, / \, z]$$

Step IV: Elimination of bounded quantifiers

$$\exists x \leq t^2 + t - 1 \ \exists z \leq t + 2 \ : \ (t+1) \cdot z = x + (-b \bmod t+1)$$

Assume $t \geq 2$. Bit blast:

$$\exists z \leq t+2 : \varphi \quad \rightarrow \quad \exists z_0, z_1, z_2 \leq t-1 : \quad \begin{aligned} & 0 \leq z_2 \cdot t^2 + z_1 \cdot t + z_0 \leq t+2 \\ & \wedge \varphi[z_2 \cdot t^2 + z_1 \cdot t + z_0 \, / \, z] \end{aligned}$$

The equality $(t+1) \cdot z = x - (b \bmod t+1)$ becomes:

$$(t+1) \cdot (z_2 \cdot t^2 + z_1 \cdot t + z_0) = (x_2 \cdot t^2 + x_1 \cdot t + x_0) + (-b \bmod t+1).$$

Step IV: Elimination of bounded quantifiers

$$\exists x \leq t^2 + t - 1 \ \exists z \leq t + 2 \ : \ (t+1) \cdot z = x + (-b \bmod t+1)$$

Assume $t \geq 2$. Bit blast:

$$\exists z \leq t + 2 \colon \varphi \quad \rightarrow \quad \exists z_0, z_1, z_2 \leq t - 1 \colon \quad 0 \leq z_2 \cdot t^2 + z_1 \cdot t + z_0 \leq t + 2$$
$$\land\, \varphi[z_2 \cdot t^2 + z_1 \cdot t + z_0 \,/\, z]$$

The equality $(t+1) \cdot z = x - (b \bmod t+1)$ becomes:

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + (x_1 - z_0 - z_1) \cdot t + (x_0 - z_0) + (-b \bmod t+1) = 0.$$

Step IV: Elimination of bounded quantifiers

$$\exists x \leq t^2 + t - 1 \; \exists z \leq t + 2 \; : \; (t+1) \cdot z = x + (-b \bmod t+1)$$

Assume $t \geq 2$. Bit blast:

$$\exists z \leq t + 2 \colon \varphi \quad \to \quad \exists z_0, z_1, z_2 \leq t - 1 \colon \quad 0 \leq z_2 \cdot t^2 + z_1 \cdot t + z_0 \leq t + 2$$
$$\land \, \varphi[z_2 \cdot t^2 + z_1 \cdot t + z_0 \, / \, z]$$

The equality $(t+1) \cdot z = x - (b \bmod t+1)$ becomes:

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + (x_1 - z_0 - z_1) \cdot t + (x_0 - z_0) + (-b \bmod t+1) = 0.$$

Divide by t the maximal subterm with no quantified variables:

$$(-b \bmod t+1) \quad \to \quad \left\lfloor \tfrac{-b \bmod t+1}{t} \right\rfloor \cdot t + \big((-b \bmod t+1) \bmod t\big)$$

Step IV: Elimination of bounded quantifiers

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) \cdot t$$
$$+ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = 0$$

Step IV: Elimination of bounded quantifiers

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) \cdot t \\ + (x_0 - z_0) + \big((-b \bmod t + 1) \bmod t\big) = 0$$

- $(x_0 - z_0) + \big((-b \bmod t + 1) \bmod t\big)$ belongs to $[-t..2 \cdot t]$...
- ...and must be divisible by t. (This only applies to equalities.)

Step IV: Elimination of bounded quantifiers

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) \cdot t$$
$$+ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = 0$$

- $(x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big)$ belongs to $[-t..2 \cdot t]$...
- ...and must be divisible by t. (This only applies to equalities.)

Guess $r_0 \in \{-1, 0, 1, 2\}$ and rewrite the equality as

$$-z_2 \cdot t^2 + (x_2 - z_1 - z_2) \cdot t + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) + r_0 = 0$$
$$\land \ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = r_0 \cdot t$$

Important: z_0, x_0 and x_1 now only have integer coefficients!

Step IV: Elimination of bounded quantifiers

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) \cdot t$$
$$+ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = 0$$

- $(x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big)$ belongs to $[-t..2 \cdot t]$...
- ...and must be divisible by t. (This only applies to equalities.)

Guess $r_0 \in \{-1, 0, 1, 2\}$ and rewrite the equality as

$$-z_2 \cdot t^2 + (x_2 - z_1 - z_2) \cdot t + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) + r_0 = 0$$
$$\land \ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = r_0 \cdot t$$

Important: z_0, x_0 and x_1 now only have integer coefficients!

Step IV: Elimination of bounded quantifiers

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) \cdot t$$
$$+ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = 0$$

- $(x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big)$ belongs to $[-t..2 \cdot t]$...
- ...and must be divisible by t. (This only applies to equalities.)

Guess $r_0 \in \{-1, 0, 1, 2\}$ and rewrite the equality as

$$-z_2 \cdot t^2 + (x_2 - z_1 - z_2) \cdot t + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) + r_0 = 0$$
$$\land \ (x_0 - z_0) + \big((-b \bmod t+1) \bmod t\big) = r_0 \cdot t$$

Important: z_0, x_0 and x_1 now only have integer coefficients!

Step IV: Elimination of bounded quantifiers

$$-z_2 \cdot t^3 + (x_2 - z_1 - z_2) \cdot t^2 + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) \cdot t$$

$= 0$

2nd iteration: Also z_1 and x_2 will have integer coefficients.
3rd iteration: All variables will have integer coefficients.

We can then call a quantifier elimination procedure for Presburger arithmetic!

- ...and must be divisible by t. (This only applies to equalities.)

Guess $r_0 \in \{-1, 0, 1, 2\}$ and rewrite the equality as

$$-z_2 \cdot t^2 + (x_2 - z_1 - z_2) \cdot t + \left(x_1 - z_0 - z_1 + \left\lfloor \frac{-b \bmod t+1}{t} \right\rfloor\right) + r_0 = 0$$

$$\land \ (x_0 - z_0) + \big((-b \bmod t + 1) \bmod t\big) = r_0 \cdot t$$

Important: z_0, x_0 and x_1 now only have integer coefficients!

Our results

Theorem

There is a quantifier elimination procedure for the extension of 1PPA *with the functions:*

- *integer division:* $x \mapsto \left\lfloor \frac{x}{t^d} \right\rfloor$ *one function for each* $d \in \mathbb{N}$, *assuming* $t \neq 0$
- *integer remainder function:* $x \mapsto (x \bmod p)$ *for each* $p \in \mathbb{Z}[t]$
- *divisibility relation:* $p \mid x$ *for each* $p \in \mathbb{Z}[t]$

Theorem

For the class of all existential formulae of 1PPA, *the following holds:*

Satisfiability: **NP**-*complete*	*Universality:* **coNEXP**-*complete*	*Finiteness:* **coNP**-*complete*

How does the following picture change for 1PPA?

Quantifier elimination

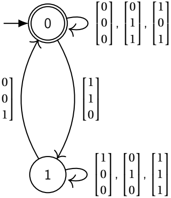
[Presburger, ‘29]

$$\begin{tikzcd}
\exists x : \varphi(x, \boldsymbol{y}) \arrow[d, squiggly, "\equiv"] \\
\psi(\boldsymbol{y})
\end{tikzcd}$$

3EXPTIME

Automata

[Büchi, ‘60]

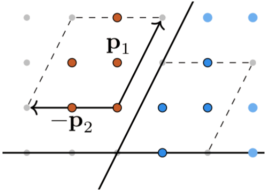


0
$\begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}$
$\begin{bmatrix}0\\0\\1\end{bmatrix}$
$\begin{bmatrix}1\\1\\0\end{bmatrix}$
1
$\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}$

3EXPTIME

Geometry

[Ginsburg and Spanier, ‘66]



3EXPTIME