Existential Presburger Arithmetic with Divisibility Constraints: A tour

Alessio Mansutti

IMDEA Software Institute

Trends in Arithmetic Theories – ICALP'24

Presburger arithmetic (PrA)

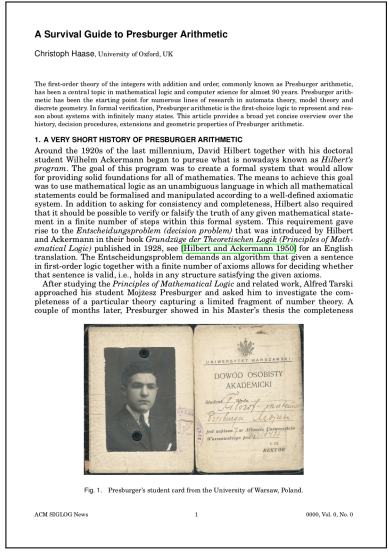
The first-order theory of $\langle \mathbb{Z}; 0, 1, +, \leq \rangle$

"Every integer is either even or odd"

$$\forall x \, \exists y : x = 2y \vee x = 2y + 1$$

Why Presburger arithmetic?
Wide range of applications in verification, program synthesis, compiler optimisation...

- SAT of the existential fragment is in NP
- Full theory is decidable in 2EXPSPACE



A Survival Guide to Presburger Arithmetic

Christoph Haase, University of Oxford, UK

The first-order theory of the integers with addition and order, commonly known as Presburger arithmetic, has been a central topic in mathematical logic and computer science for almost 90 years. Presburger arithmetic has been the starting point for numerous lines of research in automata theory, model theory and discrete geometry. In formal verification, Presburger arithmetic is the first-choice logic to represent and reason about systems with infinitely many states. This article provides a broad yet concise overview over the history, decision procedures, extensions and geometric properties of Presburger arithmetic.

1. A VERY SHORT HISTORY OF PRESBURGER ARITHMETIC

Around the 1920s of the last millennium, David Hilbert together with his doctoral student Wilhelm Ackermann began to pursue what is nowadays known as *Hilbert's program*. The goal of this program was to create a formal system that would allow for providing solid foundations for all of mathematics. The means to achieve this goal was to use mathematical logic as an unambiguous language in which all mathematical statements could be formalised and manipulated according to a well-defined axiomatic system. In addition to asking for consistency and completeness, Hilbert also required that it should be possible to verify or falsify the truth of any given mathematical statement in a finite number of steps within this formal system. This requirement gave rise to the *Entscheidungsproblem (decision problem)* that was introduced by Hilbert and Ackermann in their book *Grundzüge der Theoretischen Logik (Principles of Mathematical Logic)* published in 1928, see [Hilbert and Ackermann 1950] for an English translation. The Entscheidungsproblem demands an algorithm that given a sentence in first-order logic together with a finite number of axioms allows for deciding whether that sentence is valid, i.e., holds in any structure satisfying the given axioms.

After studying the *Principles of Mathematical Logic* and related work, Alfred Tarski approached his student Mojżesz Presburger and asked him to investigate the completeness of a particular theory capturing a limited fragment of number theory. A couple of months later, Presburger showed in his Master's thesis the completeness

Fig. 1. Presburger's student card from the University of Warsaw, Poland.

Existential Presburger Arithmetic with Divisibility constraints (EPAD)

EPAD: existential first-order theory of the structure $\langle \mathbb{Z}; 0, 1, +, \mid, \leq \rangle$.

$$x \mid y \quad \iff \quad \text{there is } k \in \mathbb{Z} \text{ such that } k \cdot x = y$$

A meaningless example: $\varphi(x, y) \coloneqq \exists w : (x + y) \mid w \wedge (2w \leq 5x + y \vee \neg(w \mid (y + 2)))$

Existential Presburger Arithmetic with Divisibility constraints (EPAD)

EPAD: existential first-order theory of the structure $\langle \mathbb{Z}; 0, 1, +, \mid, \leq \rangle$.

$$x \mid y \quad \iff \quad \text{there is } k \in \mathbb{Z} \text{ such that } k \cdot x = y$$

A meaningless example: $\varphi(x, y) \coloneqq \exists w : (x + y) \mid w \wedge (2w \leq 5x + y \vee \neg(w \mid (y + 2)))$

Goals for this tutorial

- Familiarise with EPAD (proof of NP-hardness for fixed number of variables)
- Give an overview on applications of EPAD (automata theory, word equations)
- Present the main technique to decide EPAD (with some new improvement)

Historical remarks

'40s: M. Davis and J. Robinson start working on Hilbert's 10th problem.

1970: Hilbert's 10th problem is proven undecidable (MRDP theorem).

Historical remarks

'40s: M. Davis and J. Robinson start working on Hilbert's 10th problem.

1949: J. Robinson studies the first-order theory of $\langle \mathbb{Z}, 0, 1, +, |, \leq \rangle$, and shows that it is equivalent to Peano arithmetic.

1970: Hilbert's 10th problem is proven undecidable (MRDP theorem).

Historical remarks

'40s: M. Davis and J. Robinson start working on Hilbert's 10th problem.

1949: J. Robinson studies the first-order theory of $\langle \mathbb{Z}, 0, 1, +, |, \leq \rangle$, and shows that it is equivalent to Peano arithmetic.

1970: Hilbert's 10th problem is proven undecidable (MRDP theorem).

1978: L. Lipshitz (and, independently, A. P. Bel'tyukov) shows EPAD decidable...

Historical remarks

'40s: M. Davis and J. Robinson start working on Hilbert's 10th problem.

1949: J. Robinson studies the first-order theory of $\langle \mathbb{Z}, 0, 1, +, |, \leq \rangle$, and shows that it is equivalent to Peano arithmetic.

1970: Hilbert's 10th problem is proven undecidable (MRDP theorem).

1978: L. Lipshitz (and, independently, A. P. Bel'tyukov) shows EPAD decidable...

1981: ...and NP-complete when the number of variables (or divisibilities) is fixed.

Historical remarks

'40s: M. Davis and J. Robinson start working on Hilbert's 10th problem.

1949: J. Robinson studies the first-order theory of $\langle \mathbb{Z}, 0, 1, +, |, \leq \rangle$, and shows that it is equivalent to Peano arithmetic.

1970: Hilbert's 10th problem is proven undecidable (MRDP theorem).

1978: L. Lipshitz (and, independently, A. P. Bel'tyukov) shows EPAD decidable...

1981: ...and NP-complete when the number of variables (or divisibilities) is fixed.

2015: EPAD is shown in NEXP (A. Lechner, J. Ouaknine and J. Worrell).

Historical remarks

'40s: M. Davis and J. Robinson start working on Hilbert's 10th problem.

1949: J. Robinson studies the first-order theory of $\langle \mathbb{Z}, 0, 1, +, |, \leq \rangle$, and shows that it is equivalent to Peano arithmetic.

1970: Hilbert's 10th problem is proven undecidable (MRDP theorem).

1978: L. Lipshitz (and, independently, A. P. Bel'tyukov) shows EPAD decidable...

1981: ...and NP-complete when the number of variables (or divisibilities) is fixed.

2015: EPAD is shown in NEXP (A. Lechner, J. Ouaknine and J. Worrell).

2021: M. Starchak gives a quantifier-elimination-style procedure for EPAD.

Part 1

What can we say and do with EPAD?

A few (meaningful) examples

Modular arithmetic:

$$z \mid x - y \qquad\qquad x \equiv y \mod z$$

$$\exists r : 1 \leq r \leq f(\boldsymbol{x}) - 1 \wedge (g(\boldsymbol{x}) \equiv r \mod f(\boldsymbol{x})) \qquad\qquad \neg(f(\boldsymbol{x}) \mid g(\boldsymbol{x}))$$

A few (meaningful) examples

Modular arithmetic:

$$z \mid x - y \qquad\qquad x \equiv y \mod z$$

$$\exists r : 1 \leq r \leq f(\boldsymbol{x}) - 1 \wedge (g(\boldsymbol{x}) \equiv r \mod f(\boldsymbol{x})) \qquad\qquad \neg(f(\boldsymbol{x}) \mid g(\boldsymbol{x}))$$

Coprimality-related stuff:

$$x \mid x + 1 \qquad\qquad x \in \{-1, 1\}$$

A few (meaningful) examples

Modular arithmetic:

$$z \mid x - y \qquad x \equiv y \mod z$$

$$\exists r : 1 \leq r \leq f(\boldsymbol{x}) - 1 \wedge (g(\boldsymbol{x}) \equiv r \mod f(\boldsymbol{x})) \qquad \neg(f(\boldsymbol{x}) \mid g(\boldsymbol{x}))$$

Coprimality-related stuff:

$$x \mid x + 1 \qquad x \in \{-1, 1\}$$

$$\exists w : x \mid w \wedge y \mid (w + 1) \qquad \gcd(x, y) = 1$$

A few (meaningful) examples

Modular arithmetic:

$$z \mid x - y \qquad\qquad x \equiv y \mod z$$

$$\exists r : 1 \leq r \leq f(\boldsymbol{x}) - 1 \wedge (g(\boldsymbol{x}) \equiv r \mod f(\boldsymbol{x})) \qquad\qquad \neg(f(\boldsymbol{x}) \mid g(\boldsymbol{x}))$$

Coprimality-related stuff:

$$x \mid x + 1 \qquad\qquad x \in \{-1, 1\}$$

$$\exists w : x \mid w \wedge y \mid (w + 1) \qquad\qquad \gcd(x, y) = 1$$

$$z \mid x \wedge z \mid y \wedge \exists w : x \mid w \wedge y \mid (w + z) \qquad\qquad \gcd(x, y) = z$$

A few (meaningful) examples

Modular arithmetic:

$$z \mid x - y \qquad x \equiv y \mod z$$

$$\exists r : 1 \leq r \leq f(\boldsymbol{x}) - 1 \wedge (g(\boldsymbol{x}) \equiv r \mod f(\boldsymbol{x})) \qquad \neg(f(\boldsymbol{x}) \mid g(\boldsymbol{x}))$$

Coprimality-related stuff:

$$x \mid x + 1 \qquad x \in \{-1, 1\}$$

$$\exists w : x \mid w \wedge y \mid (w + 1) \qquad \gcd(x, y) = 1$$

$$z \mid x \wedge z \mid y \wedge \exists w : x \mid w \wedge y \mid (w + z) \qquad \gcd(x, y) = z$$

$$x \mid y \wedge x + 1 \mid y \qquad \exists k : y = k(x^2 + x) \wedge k \neq 0$$

A few (meaningful) examples

EPAD does not have a polynomial small-model property

Consider the family of formulae $\{\varphi_n\}_{n\in\mathbb{N}}$ given by

$$\varphi_n(x) \coloneqq \exists x_1, \ldots, x_{n+1} : x \geq x_{n+1} \wedge x_1 \geq 2 \wedge \bigwedge_{i=1}^{n} (\underbrace{x_i \mid x_{i+1} \ \wedge \ x_i + 1 \mid x_{i+1}}_{\text{implies } x_{i+1} > x_i^2}).$$

The smallest x satisfying $\varphi_n(x)$ is bigger than 2^{2^n}.

$z \mid x \wedge z \mid y \wedge \exists w : x \mid w \wedge y \mid (w + z)$

$\gcd(x, y) = z$

$x \mid y \wedge x + 1 \mid y$

$\exists k : y = k(x^2 + x) \wedge k \neq 0$

How to express bounded squaring

How can we characterise $y = x^2 \wedge 1 \leq x \leq b$, where $b \in \mathbb{N}$?

$$1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge b^2 \mid y - x^2$$

How to express bounded squaring

How can we characterise $y = x^2 \wedge 1 \leq x \leq b$, where $b \in \mathbb{N}$?

$$1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge \exists k \in \mathbb{Z} : y = x^2 + k \cdot b^2$$

k forced to be 0

How to express bounded squaring

How can we characterise $y = x^2 \wedge 1 \leq x \leq b$, where $b \in \mathbb{N}$?

$$1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge b^2 \mid y - x^2$$

How to express bounded squaring

How can we characterise $y = x^2 \wedge 1 \leq x \leq b$, where $b \in \mathbb{N}$?

$$1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge b^2 \mid y - x^2$$

Idea: there is nothing special about b^2, we just need $f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

- $f(x, y) \geq b^2$, for every $x \in [1, b]$ and $y \in [1, b^2]$
- $f(x, y) \mid y - x^2$ is expressible in EPAD (intent: cancel x^2 using f)

How to express bounded squaring

How can we characterise $y = x^2 \wedge 1 \leq x \leq b$, where $b \in \mathbb{N}$?

$$1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge b^2 \mid y - x^2$$

Idea: there is nothing special about b^2, we just need $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

- $f(x, y) \geq b^2$, for every $x \in [1, b]$ and $y \in [1, b^2]$
- $f(x, y) \mid y - x^2$ is expressible in EPAD (intent: cancel x^2 using f)

Solution:[1] $f(x, y) \coloneqq x + b^2$

$$x + b^2 \mid y - x^2 \quad \text{iff} \quad x + b^2 \mid y - x^2 + x(x + b^2) \quad \text{iff} \quad x + b^2 \mid y + b^2 x$$

[1] In Lipshitz's '81 paper, $f(x, y) \coloneqq (x + b)(x + b + 1)$ is used instead

How to express bounded squaring

How can we characterise $y = x^2 \wedge 1 \leq x \leq b$, where $b \in \mathbb{N}$?

$$1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge b^2 \mid y - x^2$$

Idea: there is nothing special about b^2, we just need $f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

- $f(x, y) \geq b^2$, for every $x \in [1, b]$ and $y \in [1, b^2]$
- $f(x, y) \mid y - x^2$ is expressible in EPAD (intent: cancel x^2 using f)

Solution:[1] $f(x, y) \coloneqq x + b^2$

$$x + b^2 \mid y - x^2 \quad \text{iff} \quad x + b^2 \mid y - x^2 + x(x + b^2) \quad \text{iff} \quad x + b^2 \mid y + b^2 x$$

Final formula: $1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge x + b^2 \mid y + b^2 x$.

[1] In Lipshitz's '81 paper, $f(x, y) \coloneqq (x + b)(x + b + 1)$ is used instead

How to express bounded squaring

NP-hardness for 2 variables, 4 inequalities, and 2 divisibility constraints

Quadratic residue problem [Manders and Aldeman, STOC'76]

Input: $a, b, m \in \mathbb{N}$ given in binary.
Question: Is there $x \in [1, b]$ such that $x^2 \equiv a \pmod{m}$?

The quadratic residue problem is NP-complete. Reduction to EPAD:

$$\exists x \exists y : \; 1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge x + b^2 \mid y + b^2 x \wedge m \mid y - a \,.$$

Final formula: $1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge x + b^2 \mid y + b^2 x \,.$

[1] In Lipshitz's '81 paper, $f(x, y) \coloneqq (x + b)(x + b + 1)$ is used instead

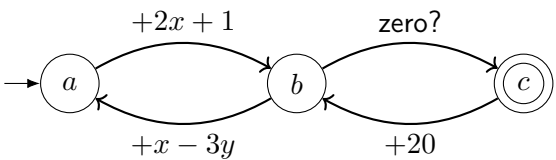
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



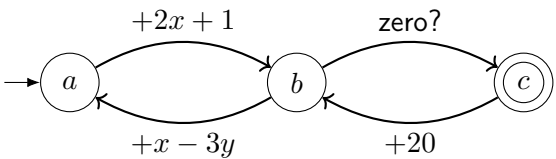
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Parameter synthesis problem:

Input: A POCA $\mathcal{A}$ with initial state a, and an ω-regular property P (e.g. finite reachability, Büchi, coBüchi, LTL languages...).

Question: Is there a valuation of the parameters (e.g. x, y) over $\mathbb{Z}$ such that in **all** runs starting at $(a, 0)$, the property P holds.

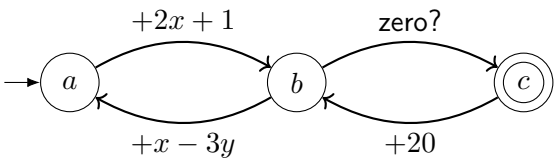
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$\exists K \in \mathbb{N} : 0 + K \cdot (2x + 1 + x - 3y) + 2x + 1 = 0$$

initial value of the counter

final value of the counter

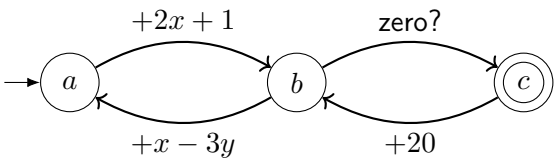
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$\exists K \in \mathbb{N} : K \cdot (2x + 1 + x - 3y) = -2x - 1$$

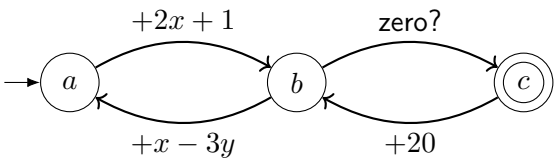
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$\exists K \in \mathbb{Z} : K \cdot (2x+1+x-3y) = -2x-1$$
$$\wedge \big(2x+1=0 \vee (2x+1+x-3y \geq 0 \iff -2x-1 \geq 0)\big)$$

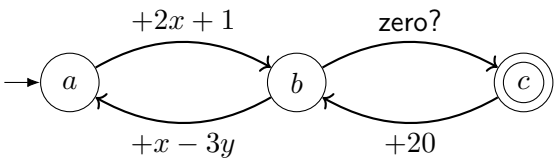
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$(2x+1+x-3y) \mid -2x-1$$
$$\wedge \big(2x+1=0 \vee (2x+1+x-3y \geq 0 \iff -2x-1 \geq 0)\big)$$

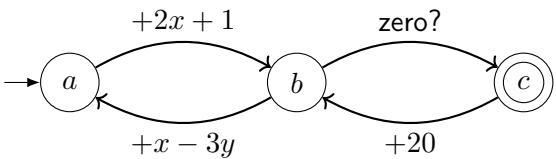
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$x := 2$
$y := 4$

$$(2x+1+x-3y) \mid -2x-1$$
$$\wedge \big(2x+1=0 \vee (2x+1+x-3y \geq 0 \iff -2x-1 \geq 0)\big)$$

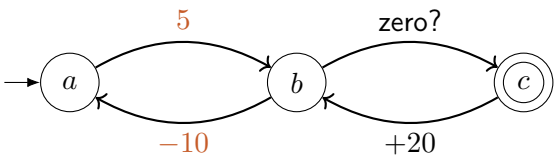
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$x := 2$$
$$y := 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

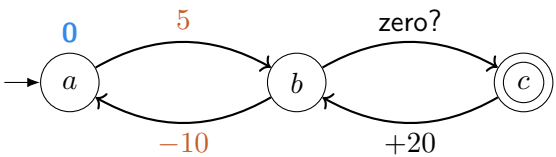
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$x := 2$$
$$y := 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

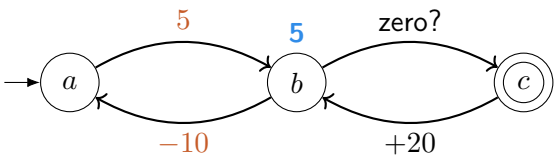
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$x := 2$$
$$y := 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

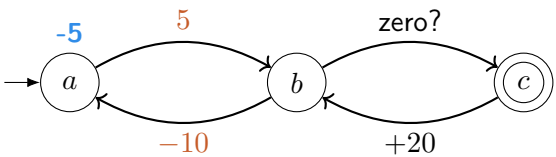
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$x := 2$$
$$y := 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

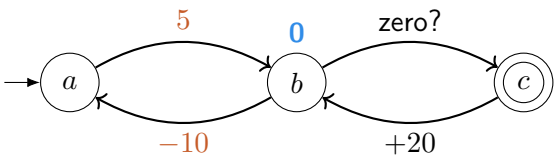
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$x := 2$$
$$y := 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

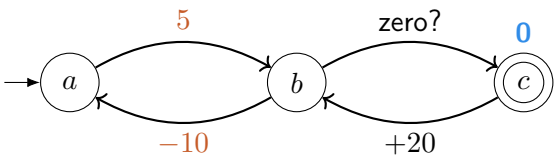
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automaton (POCA):



Let us try to obtain **one** run that reaches c :

$$x := 2$$
$$y := 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

Applying EPAD:

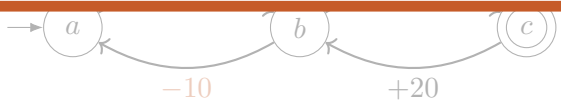
Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Finite reachability of POCAs is expressible in EPAD.

However, synthesis requires to test the given property against **all** runs!



Let us try to obtain **one** run that reaches c :

$$x \coloneqq 2$$
$$y \coloneqq 4$$

$$(2x + 1 + x - 3y) \mid -2x - 1$$
$$\wedge \big(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\big)$$

Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Finite reachability of POCAs is expressible in EPAD.

However, synthesis requires to test the given property against **all** runs!

Translation into BIL, a decidable fragment of ∀∃PAD:

$$\forall \boldsymbol{x} \in \mathbb{N} \bigvee_{i \in I} \Big(\varphi_i(\boldsymbol{x}) \wedge \exists \boldsymbol{y} \in \mathbb{N} \bigwedge_{j \in J_i} (f_j(\boldsymbol{x}) \mid g_j(\boldsymbol{x}, \boldsymbol{y}) \wedge f_j(\boldsymbol{x}) > 0) \Big)$$

where every φ_i is a formula from PrA.

Theorem (Extended Chinese Remainder Theorem (CRT))

For $i \in [1,k]$, *let* $a_i, r_i \in \mathbb{Z}$ *and* $m_i \in \mathbb{Z} \setminus \{0\}$.

The univariate system of divisibilities $\left\{ m_i \mid (a_i \cdot x - r_i) \quad i \in [1,k] \right.$

has a solution iff so does $\begin{cases} \gcd(a_i, m_i) \mid r_i & i \in [1,k] \\ \gcd(a_i \cdot m_j, a_j \cdot m_i) \mid (a_i \cdot r_j - a_j \cdot r_i) & i,j \in [1,k]. \end{cases}$

Theorem (Extended Chinese Remainder Theorem (CRT))

For $i \in [1,k]$, *let* $a_i, r_i \in \mathbb{Z}$ *and* $m_i \in \mathbb{Z} \setminus \{0\}$.

The univariate system of divisibilities $\left\{ m_i \mid (a_i \cdot x - r_i) \quad i \in [1,k] \right.$

has a solution iff so does $\begin{cases} \gcd(a_i, m_i) \mid r_i & i \in [1,k] \\ \gcd(a_i \cdot m_j, a_j \cdot m_i) \mid (a_i \cdot r_j - a_j \cdot r_i) & i,j \in [1,k]. \end{cases}$

Given

$$\forall \boldsymbol{x} \in \mathbb{N} \bigvee_{i \in I} \Big(\varphi_i(\boldsymbol{x}) \wedge \exists \boldsymbol{y} \in \mathbb{N} \bigwedge_{j \in J_i} (f_j(\boldsymbol{x}) \mid g_j(\boldsymbol{x}, \boldsymbol{y}) \wedge f_j(\boldsymbol{x}) > 0) \Big)$$

Theorem (Extended Chinese Remainder Theorem (CRT))

For $i \in [1,k]$, *let* $a_i, r_i \in \mathbb{Z}$ *and* $m_i \in \mathbb{Z} \setminus \{0\}$.

The univariate system of divisibilities $\left\{ m_i \mid (a_i \cdot x - r_i) \quad i \in [1,k] \right.$

has a solution iff so does $\begin{cases} \gcd(a_i, m_i) \mid r_i & i \in [1,k] \\ \gcd(a_i \cdot m_j, a_j \cdot m_i) \mid (a_i \cdot r_j - a_j \cdot r_i) & i,j \in [1,k]. \end{cases}$

Given

$$\forall \boldsymbol{x} \in \mathbb{N} \bigvee_{i \in I} \Big(\varphi_i(\boldsymbol{x}) \wedge \exists \boldsymbol{y} \in \mathbb{N} \bigwedge_{j \in J_i} (f_j(\boldsymbol{x}) \mid g_j(\boldsymbol{x}, \boldsymbol{y}) \wedge f_j(\boldsymbol{x}) > 0) \Big)$$

1. remove $\boldsymbol{y}$ using the CRT. This introduces $\gcd(h_1(\boldsymbol{x}), \ldots, h_m(\boldsymbol{x})) \mid f(\boldsymbol{x})$ ...
2. ...which can be rewritten as $\forall u : \bigwedge_{i=1}^{m} u \mid h_i(\boldsymbol{x}) \implies u \mid f(\boldsymbol{x})$.

Applying EPAD:

QUADRATIC WORD EQUATIONS WITH LENGTH CONSTRAINTS, COUNTER SYSTEMS, AND PRESBURGER ARITHMETIC WITH DIVISIBILITY

ANTHONY W. LIN [a] AND RUPAK MAJUMDAR [b]

Word equations: A word equations problem is a system E

$$w_1 = w_2,\ w_3 = w_4,\ \ldots,\ w_{2k-1} = w_{2k} \qquad \text{(e.g. } x \cdot x \cdot b = y \cdot a \cdot z\text{)}$$

where each w_i is a word in $(\Sigma \cup X)^*$, with Σ finite alphabet and X set of variables.

Applying EPAD:

QUADRATIC WORD EQUATIONS WITH LENGTH CONSTRAINTS, COUNTER SYSTEMS, AND PRESBURGER ARITHMETIC WITH DIVISIBILITY

ANTHONY W. LIN [a] AND RUPAK MAJUMDAR [b]

Word equations: A word equations problem is a system E

$$w_1 = w_2,\ w_3 = w_4,\ \ldots,\ w_{2k-1} = w_{2k} \qquad \text{(e.g. } x \cdot x \cdot b = y \cdot a \cdot z\text{)}$$

where each w_i is a word in $(\Sigma \cup X)^*$, with Σ finite alphabet and X set of variables.

Length constraints: PrA formula φ having as variables the lengths $|x|$ of $x \in X$.

Applying EPAD:

QUADRATIC WORD EQUATIONS WITH LENGTH CONSTRAINTS, COUNTER SYSTEMS, AND PRESBURGER ARITHMETIC WITH DIVISIBILITY

ANTHONY W. LIN [a] AND RUPAK MAJUMDAR [b]

Word equations: A word equations problem is a system E

$$w_1 = w_2,\ w_3 = w_4,\ \ldots,\ w_{2k-1} = w_{2k} \qquad \text{(e.g. } x \cdot x \cdot b = y \cdot a \cdot z\text{)}$$

where each w_i is a word in $(\Sigma \cup X)^*$, with Σ finite alphabet and X set of variables.

Length constraints: PrA formula φ having as variables the lengths $|x|$ of $x \in X$.

Problem: Is there a substitution $\sigma\colon X \to \Sigma^*$ satisfying E and φ?

Applying EPAD:

QUADRATIC WORD EQUATIONS WITH LENGTH CONSTRAINTS, COUNTER SYSTEMS, AND PRESBURGER ARITHMETIC WITH DIVISIBILITY

ANTHONY W. LIN [a] AND RUPAK MAJUMDAR [b]

Open problem: Is solving word equations with length constraints decidable?

Quadratic fragment: In the word equations, each variable occur at most twice.

This problem can be solved with EPAD.

- translate the equations in a counter-automata-like device.
- the reachability relation of these devices can be expressed in EPAD.

Problem: Is there a substitution $\sigma : X \to \Sigma^*$ satisfying E and φ?

Problems that are interreducible to EPAD

Reachability in Succinct and Parametric One-Counter Automata

Christoph Haase, Stephan Kreutzer, Joël Ouaknine, and James Worrell
Oxford University Computing Laboratory, UK

Simultaneous Rigid E-Unification and Related Algorithmic Problems

Anatoli Degtyarev
Computing Science Department
Uppsala University

Yuri Matiyasevich
Steklov Institute of Mathematics
St.Petersburg Division

Andrei Voronkov
Computing Science Department
Uppsala University

Part 2

How to solve EPAD.

(plot of $\gcd(x, y) = 1$*)*

Searching solutions – a roadmap

Consider the problem of finding a solution for a system of inequalities with divisibilities:

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$$

Lipshitz's algorithm in a nutshell:

Searching solutions – a roadmap

Consider the problem of finding a solution for a system of inequalities with divisibilities:

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$$

Lipshitz's algorithm in a nutshell:

1. Remove the system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$
   (uses standard results from linear algebra)

Searching solutions – a roadmap

Consider the problem of finding a solution for a system of inequalities with divisibilities:

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$$

Lipshitz's algorithm in a nutshell:

1. Remove the system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$
   (uses standard results from linear algebra)
2. Translate the system of divisibilities into an equisatisfiable increasing system
   (notion inspired by the Chinese Remainder Theorem (CRT); "tautology-driven")

Searching solutions – a roadmap

Consider the problem of finding a solution for a system of inequalities with divisibilities:

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$$

Lipshitz's algorithm in a nutshell:

1. Remove the system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$
   (uses standard results from linear algebra)
2. Translate the system of divisibilities into an equisatisfiable increasing system
   (notion inspired by the Chinese Remainder Theorem (CRT); "tautology-driven")
3. Find local solutions over the (p-adic) integers for a finite set of primes
   (why? Increasing systems enjoy a local-to-global property)

Searching solutions – a roadmap

Consider the problem of finding a solution for a system of inequalities with divisibilities:

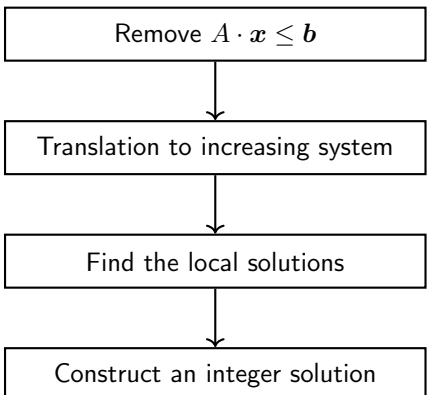
$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$$

Lipshitz's algorithm in a nutshell:

1. Remove the system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$
   (uses standard results from linear algebra)
2. Translate the system of divisibilities into an equisatisfiable increasing system
   (notion inspired by the Chinese Remainder Theorem (CRT); "tautology-driven")
3. Find local solutions over the (p-adic) integers for a finite set of primes
   (why? Increasing systems enjoy a local-to-global property)
4. Construct an integer solution from the local solutions
   (construction of the integer solution uses the CRT)

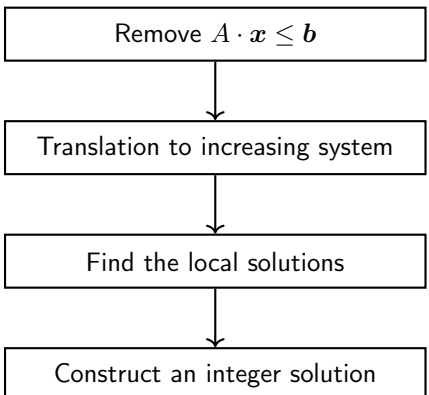
Algorithms for EPAD – search vs. decision

Search algorithm:

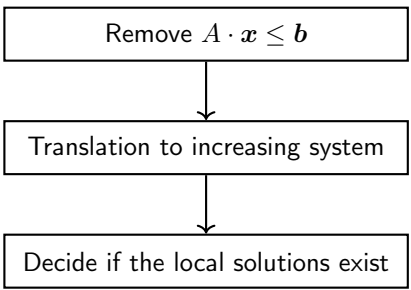


Algorithms for EPAD – search vs. decision

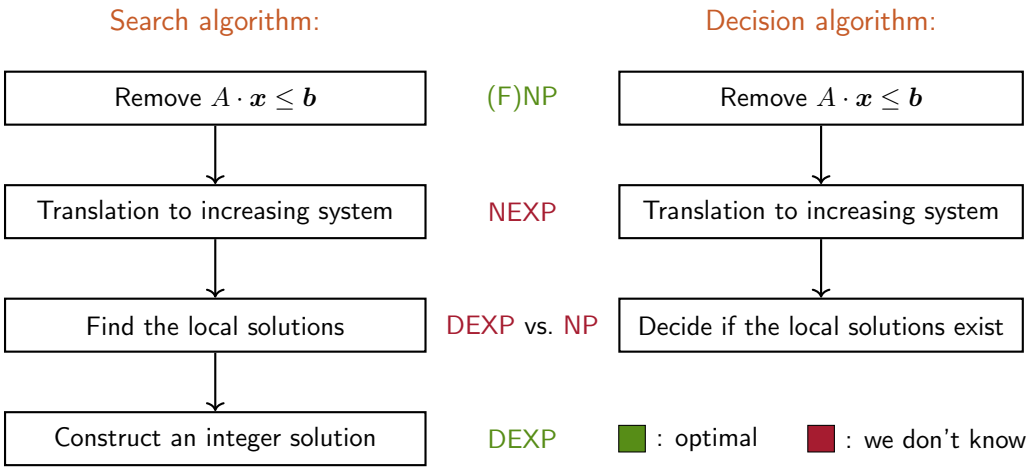
Search algorithm:



Decision algorithm:



Algorithms for EPAD – search vs. decision



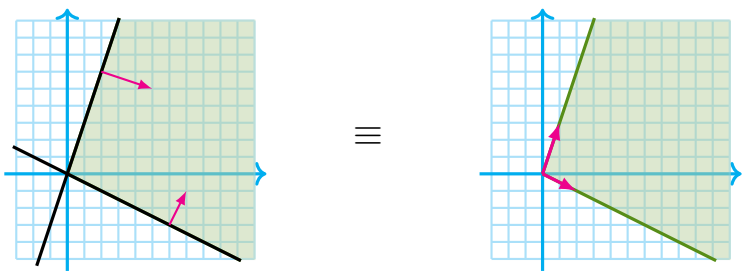
1: Remove the system of inequalities (NP)

Theorem (von zur Gathen and Sieveking, '78)

Let $\Phi(\boldsymbol{x}) \coloneqq A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge C \cdot \boldsymbol{x} = \boldsymbol{d}$, *with* $\boldsymbol{x}$ *vector of* d *variables. Then,*

$$\{\boldsymbol{x} \in \mathbb{Z}^d : \Phi(\boldsymbol{x})\} = \bigcup_{j=1}^{k} \{\boldsymbol{u}_j + E_j \cdot \boldsymbol{y} : \boldsymbol{y} \in \mathbb{N}^{d-r}\},$$

where $r \coloneqq \operatorname{rank}(C)$, $\boldsymbol{u}_j \in \mathbb{Z}^d$ *and* $E_j = [\boldsymbol{p}_{j,1}, \ldots, \boldsymbol{p}_{j,d-r}] \in \mathbb{Z}^{d \times (d-r)}$.



1: Remove the system of inequalities (NP)

Theorem (von zur Gathen and Sieveking, '78)

Let $\Phi(\boldsymbol{x}) \coloneqq A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge C \cdot \boldsymbol{x} = \boldsymbol{d}$, *with* $\boldsymbol{x}$ *vector of* d *variables. Then,*

$$\{\boldsymbol{x} \in \mathbb{Z}^d : \Phi(\boldsymbol{x})\} = \bigcup_{j=1}^{k} \{\boldsymbol{u}_j + E_j \cdot \boldsymbol{y} : \boldsymbol{y} \in \mathbb{N}^{d-r}\},$$

where $r \coloneqq \operatorname{rank}(C)$, $\boldsymbol{u}_j \in \mathbb{Z}^d$ *and* $E_j = [\boldsymbol{p}_{j,1}, \ldots, \boldsymbol{p}_{j,d-r}] \in \mathbb{Z}^{d \times (d-r)}$.

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \,|\, g_i(\boldsymbol{x}) \quad \rightsquigarrow \quad \bigvee_{j=1}^{k} \left(\boldsymbol{y} \geq \boldsymbol{0} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{u}_j + E_j \cdot \boldsymbol{y}) \,|\, g_i(\boldsymbol{u}_j + E_j \cdot \boldsymbol{y}) \right)$$

1: Remove the system of inequalities (NP)

Theorem (von zur Gathen and Sieveking, '78)

Let $\Phi(\boldsymbol{x}) \coloneqq A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge C \cdot \boldsymbol{x} = \boldsymbol{d}$, *with* $\boldsymbol{x}$ *vector of* d *variables. Then,*

$$\{\boldsymbol{x} \in \mathbb{Z}^d : \Phi(\boldsymbol{x})\} = \bigcup_{j=1}^{k} \{\boldsymbol{u}_j + E_j \cdot \boldsymbol{y} : \boldsymbol{y} \in \mathbb{N}^{d-r}\},$$

where $r \coloneqq \operatorname{rank}(C)$, $\boldsymbol{u}_j \in \mathbb{Z}^d$ *and* $E_j = [\boldsymbol{p}_{j,1}, \ldots, \boldsymbol{p}_{j,d-r}] \in \mathbb{Z}^{d \times (d-r)}$.

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \,|\, g_i(\boldsymbol{x}) \quad \rightsquigarrow \quad \bigvee_{j=1}^{k} \Big(\boldsymbol{y} \geq \boldsymbol{0} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{u}_j + E_j \cdot \boldsymbol{y}) \,|\, g_i(\boldsymbol{u}_j + E_j \cdot \boldsymbol{y}) \Big)$$

(implicit) equalities in $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$ $\Rightarrow$ number of variables decreases

2: Find an equisatisfiable increasing system – idea

Theorem (Extended Chinese Remainder Theorem (CRT))

For $i \in [1,k]$*, let* $a_i, r_i \in \mathbb{Z}$ *and* $m_i \in \mathbb{Z} \setminus \{0\}$.

The univariate system of divisibilities $\left\{ m_i \mid (a_i \cdot x - r_i) \quad i \in [1,k] \right.$

has a solution iff so does $\begin{cases} \gcd(a_i, m_i) \mid r_i & i \in [1,k] \\ \gcd(a_i \cdot m_j, a_j \cdot m_i) \mid (a_i \cdot r_j - a_j \cdot r_i) & i,j \in [1,k]. \end{cases}$

2: Find an equisatisfiable increasing system – idea

Theorem (Extended Chinese Remainder Theorem (CRT))

For $i \in [1,k]$, *let* $a_i, r_i \in \mathbb{Z}$ *and* $m_i \in \mathbb{Z} \setminus \{0\}$.

The univariate system of divisibilities $\left\{ m_i \mid (a_i \cdot x - r_i) \quad i \in [1,k] \right.$

has a solution iff so does $\begin{cases} \gcd(a_i, m_i) \mid r_i & i \in [1,k] \\ \gcd(a_i \cdot m_j, a_j \cdot m_i) \mid (a_i \cdot r_j - a_j \cdot r_i) & i,j \in [1,k]. \end{cases}$

By iterating the CRT one can decide multivariate system of divisibility constraints $\bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ where the $f_i(\boldsymbol{x})$ are constant polynomials.

We would like to use the CRT for arbitrary systems of divisibilities.
Main problem: a variable can occur in both sides of a divisibility.

2: Find an equisatisfiable increasing system – definition

The system $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ implies further divisibilities following the rules:

$$\frac{}{f \mid f} \qquad \frac{f \mid g \quad a \in \mathbb{Z}}{f \mid a \cdot g} \qquad \frac{f \mid g \quad f \mid h}{f \mid g + h} \qquad \frac{f \mid a \cdot g \quad g \mid h \quad a \in \mathbb{Z}}{f \mid a \cdot h}$$

2: Find an equisatisfiable increasing system – definition

The system $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ implies further divisibilities following the rules:

$$\frac{}{f \mid f} \qquad \frac{f \mid g \quad a \in \mathbb{Z}}{f \mid a \cdot g} \qquad \frac{f \mid g \quad f \mid h}{f \mid g + h} \qquad \frac{f \mid a \cdot g \quad g \mid h \quad a \in \mathbb{Z}}{f \mid a \cdot h}$$

$\Phi(\boldsymbol{x})$ is said to be increasing whenever there is an ordering $x_1 \prec \cdots \prec x_d$ of the variables in $\boldsymbol{x}$ such that, for every $f \mid g$ implied by Φ,

(leading variable of f) $\prec$ (leading variable of g)

or $f \mid g$ is a trivial divisibility of the form $f \mid a \cdot f$.

2: Find an equisatisfiable increasing system – definition

The system $\Phi := \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ implies further divisibilities following the rules:

$$\frac{}{f \mid f} \qquad \frac{f \mid g \quad a \in \mathbb{Z}}{f \mid a \cdot g} \qquad \frac{f \mid g \quad f \mid h}{f \mid g + h} \qquad \frac{f \mid a \cdot g \quad g \mid h \quad a \in \mathbb{Z}}{f \mid a \cdot h}$$

$\Phi(\boldsymbol{x})$ is said to be increasing whenever there is an ordering $x_1 \prec \cdots \prec x_d$ of the variables in $\boldsymbol{x}$ such that, for every $f \mid g$ implied by Φ,

(leading variable of f) $\prec$ (leading variable of g)

or $f \mid g$ is a trivial divisibility of the form $f \mid a \cdot f$.

Examples:

$x + 1 \mid y - 2$	is increasing for $x \prec y$, but not for $y \prec x$
$x + 1 \mid y - 2 \wedge x + 1 \mid x + y$	is not increasing (it implies $x + 1 \mid x + 2$)

2: Find an equisatisfiable increasing system – computation (NEXP)

Input: a system $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$

Output: an increasing system that is equisatisfiable with Φ over $\mathbb{N}$

1. if Φ is increasing, then return a suitable order for the variables
   (check in polynomial time in the size of Φ; based on iterated Kernel computations)
2. if Φ is not increasing,

Proposition

$\Phi \models \bigvee_{i=1}^{n} h_i = 0$ *for some finite set* $\{h_1, \ldots, h_n\}$ *of non-constant linear polynomials.*

2.1 guess $i \in [1, n]$ and apply the Theorem by von zur Gathen and Sieveking

$$\{\boldsymbol{x} \in \mathbb{N}^d : h_i(\boldsymbol{x}) = 0\} \;=\; \bigcup_{j=1}^{k} \{\boldsymbol{u}_j + E_j \cdot \boldsymbol{y} : \boldsymbol{y} \in \mathbb{N}^{d-1}\}$$

2.2 guess $j \in [1, k]$, substitute $\boldsymbol{x}$ by $\boldsymbol{u}_j + E_j \cdot \boldsymbol{y}$ and goto 1. (less variables!)

2: Find an equisatisfiable increasing system – computation (NEXP)

Proposition

$\Phi \models \bigvee_{i=1}^{n} h_i = 0$ *for some non-constant linear polynomials* $h_1, \ldots, h_n$.

Proof by example: The system $2x + 1 \mid -x + 5$ is not increasing.

Assume $x \geq 1$. By definition, we are searching for $c \in \mathbb{Z}$ such that

$$c \cdot (2x + 1) = -x + 5\,.$$

We see that c can be bounded in $[-3, 3]$:

$$|c| \leq \tfrac{|-x+5|}{|2x+1|} \leq \tfrac{6x}{2x} \leq 3\,.$$

Therefore, in this case $\{h_1, \ldots, h_n\} = \{c \cdot (2x + 1) + x - 5 : c \in [-3, 3]\}$.

Searching solutions – what we have seen so far

Consider the problem of finding a solution for a system of inequalities with divisibilities:

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$$

Lipshitz's algorithm in a nutshell:

✓ Remove the system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$

✓ Translate the system of divisibilities into an equisatisfiable increasing system

3. Find solutions over the p-adic integers for a finite set of primes
   (why? Increasing systems enjoy a local-to-global property)
4. Construct an integer solution from the p-adic solutions
   (construction of the integer solution uses the CRT)

3-4: Appeal to the local-to-global property – why?

Input: an increasing system $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ with respect to $x_1 \prec \cdots \prec x_d$

A sketch of the algorithm we want:

1. Take x to be the smallest variable in $\prec$
2. Consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathrm{LV}(g) = x$
   (because of increasingness, f is constant and $g = a \cdot x + r$ with $a, r \in \mathbb{Z}$)
3. Apply the CRT on S, finding a value v for x
4. Replace x with v. If Φ contains further variables, goto 1.

3-4: Appeal to the local-to-global property – why?

Input: an increasing system $\Phi := \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ with respect to $x_1 \prec \cdots \prec x_d$

A sketch of the algorithm we want:

1. Take x to be the smallest variable in $\prec$
2. Consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathrm{LV}(g) = x$
   (because of increasingness, f is constant and $g = a \cdot x + r$ with $a, r \in \mathbb{Z}$)
3. Apply the CRT on S, finding a value v for x
4. Replace x with v. If Φ contains further variables, goto 1.

Problem: Take for instance the following system increasing for $x \prec y$:

$$2 \mid x + 1 \wedge 5 \mid x + 5y$$

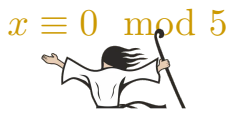
CRT gives $x = 1$, but $5 \mid 1 + 5y$ is unsatisfiable. However, $x = 5$ works!

3-4: Appeal to the local-to-global property – why?

Input: an increasing system $\Phi := \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ with respect to $x_1 \prec \cdots \prec x_d$

We need prophets foretelling us what values we can pick.
These prophets are the local solutions.

- They add congruences for the variable we are eliminating...
- ...so that satisfiability is preserved after variable replacement.
- The local solutions exist if and only if Φ is satisfiable.



Problem: Take for instance the following system increasing for $x \prec y$:

$$2 \mid x + 1 \wedge 5 \mid x + 5y$$

CRT gives $x = 1$, but $5 \mid 1 + 5y$ is unsatisfiable. However, $x = 5$ works!

3-4: Appeal to the local-to-global property – why?

Input: an increasing system $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ with respect to $x_1 \prec \cdots \prec x_d$

A sketch of the algorithm we want:

1. Take x to be the smallest variable in $\prec$
2. Consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathsf{LV}(g) = x$
   (because of increasingness, f is constant and $g = a \cdot x + r$ with $a, r \in \mathbb{Z}$)
3. Add further congruences to S accordingly to the local solutions
4. Apply the CRT on S, finding a value v for x
5. Replace x with v. If Φ contains further variables, goto 1.

3-4: Appeal to the local-to-global property – overview

Let p be a prime number. The p-adic valuation $v_p \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ is defined as

$$v_p(\ell) \coloneqq \begin{cases} \infty & \text{if } \ell = 0 \\ k & \text{unique such that } p^k \mid \ell \text{ and } p^{k+1} \nmid \ell \end{cases}$$

For every $\boldsymbol{x} \in \mathbb{Z}^d$, $f(\boldsymbol{x}) \mid g(\boldsymbol{x})$ if and only if $\forall p \in \mathbb{P} : v_p(f(\boldsymbol{x})) \leq v_p(g(\boldsymbol{x}))$.

3-4: Appeal to the local-to-global property – overview

Let p be a prime number. The p-adic valuation $v_p \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ is defined as

$$v_p(\ell) \coloneqq \begin{cases} \infty & \text{if } \ell = 0 \\ k & \text{unique such that } p^k \mid \ell \text{ and } p^{k+1} \nmid \ell \end{cases}$$

For every $\boldsymbol{x} \in \mathbb{Z}^d$, $f(\boldsymbol{x}) \mid g(\boldsymbol{x})$ if and only if $\forall p \in \mathbb{P} : v_p(f(\boldsymbol{x})) \leq v_p(g(\boldsymbol{x}))$.

Theorem (Local-to-global property – Lipshitz, 1978)

Suppose $\bigwedge_{i=1}^n f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ increasing. There is a finite set of primes P such that

$$\exists \boldsymbol{x} : \textstyle\bigwedge_{i=1}^n f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x}) \quad \textit{if and only if} \quad \forall p \in P \, \exists \boldsymbol{x} : \bigwedge_{i=1}^n v_p(f_i(\boldsymbol{x})) \leq v_p(g_i(\boldsymbol{x})).$$

The right-to-left direction "is" the algorithm in the previous slide!

3: Find the local solutions for a finite set of primes (DEXP, NP)

Given $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$, define $\mathbb{P}(\Phi)$ as the set of primes p such that

$$p \leq k \quad \text{or} \quad p \text{ divides an integer appearing in some } f_i.$$

3: Find the local solutions for a finite set of primes (DEXP, NP)

Given $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$, define $\mathbb{P}(\Phi)$ as the set of primes p such that

$$p \leq k \quad \text{or} \quad p \text{ divides an integer appearing in some } f_i.$$

Lemma (Défossez, Haase, M., Pérez, 2024)

For every prime $p \notin \mathbb{P}(\Phi)$, $\bigwedge_{i=1}^{n} v_p(f_i(\boldsymbol{x})) \leq v_p(g_i(\boldsymbol{x}))$ has a solution $\boldsymbol{x} \mapsto [0, p-1]$.

This means that taking $P \coloneqq \mathbb{P}(\Phi)$ suffices to show Lipshitz's theorem.

3: Find the local solutions for a finite set of primes (DEXP, NP)

Given $\Phi \coloneqq \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$, define $\mathbb{P}(\Phi)$ as the set of primes p such that

$$p \leq k \quad \text{or} \quad p \text{ divides an integer appearing in some } f_i.$$

Lemma (Défossez, Haase, M., Pérez, 2024)

For every prime $p \notin \mathbb{P}(\Phi)$, $\bigwedge_{i=1}^{n} v_p(f_i(\boldsymbol{x})) \leq v_p(g_i(\boldsymbol{x}))$ has a solution $\boldsymbol{x} \mapsto [0, p-1]$.

This means that taking $P \coloneqq \mathbb{P}(\Phi)$ suffices to show Lipshitz's theorem.

The complexity of building $\mathbb{P}(\Phi)$ and the local solutions:

- $\mathbb{P}(\Phi)$ can be built in polynomial time with an oracle for factoring.
- Given $p \in \mathbb{P}(\Phi)$, $\exists \boldsymbol{x} \bigwedge_{i=1}^{n} v_p(f_i(\boldsymbol{x})) \leq v_p(g_i(\boldsymbol{x}))$ can be solved in NP...
- ...but the certificate represents a solution succinctly. Decompression in DEXP.

3: Find the local solutions for a finite set of primes (DEXP, NP)

Given $\Phi := \bigwedge_{i=1}^{k} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$, define $\mathbb{P}(\Phi)$ as the set of primes p such that

Lem

For e

]*.*

This

The

- $\mathbb{P}(\Phi)$ can be built in polynomial time with an oracle for factoring.
- Given $p \in \mathbb{P}(\Phi)$, $\exists \boldsymbol{x} \bigwedge_{i=1}^{n} v_p(f_i(\boldsymbol{x})) \leq v_p(g_i(\boldsymbol{x}))$ can be solved in NP...
- ...but the certificate represents a solution succinctly. Decompression in DEXP.

This concludes the algorithm for the **decision** problem!

1. eliminate the system of inequalities
2. put the system of divisibilities in increasing form
3. decide the existence of a local solution for every prime in $\mathbb{P}(\Phi)$

Overall complexity: NEXP

4: Construct an integer solution (DEXP)

Theorem (Lechner, Ouaknine, Worrell, 2015)

Consider an increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{\mathrm{poly}(d)}$.

4: Construct an integer solution (DEXP)

Theorem (Lechner, Ouaknine, Worrell, 2015)

Consider an increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{\mathrm{poly}(d)}$.

1. Take x to be the smallest variable in $\prec$
2. Consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathrm{LV}(g) = x$
3. Add further congruences to S accordingly to the local solutions
4. Apply the CRT on S, finding a value v for x
5. Replace x with v. If Φ contains further variables, goto 1.

4: Construct an integer solution (DEXP)

Theorem (Lechner, Ouaknine, Worrell, 2015)

Consider an increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{\mathrm{poly}(d)}$.

1. Take x to be the smallest variable in $\prec$
2. Consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathrm{LV}(g) = x$
3. Add further congruences to S accordingly to the local solutions
4. Apply the CRT on S, finding a value v for x
5. Replace x with v. If Φ contains further variables, goto 1.

Disclaimer: This is not the full picture!

- During the procedure further primes needs to be added to $\mathbb{P}(\Phi)$.
- Key: after replacing x, the new system satisfies the hypothesis of the theorem.

Part 3

Some recent improvements

(plot of $x \mid y \wedge x+1 \mid y$)

r-increasing systems: grouping "independent variables"

$$f_1(\boldsymbol{z}) \mid g_1(\boldsymbol{z}) + a \cdot x$$
$$f_2(\boldsymbol{z}) \mid g_2(\boldsymbol{z}) + b \cdot y$$

Lipshitz's procedure requires ordering x and y. What happens if we relax this condition?

r-increasing systems: grouping "independent variables"

$$f_1(\boldsymbol{z}) \mid g_1(\boldsymbol{z}) + a \cdot x$$
$$f_2(\boldsymbol{z}) \mid g_2(\boldsymbol{z}) + b \cdot y$$

Lipshitz's procedure requires ordering x and y. What happens if we relax this condition?

Definition (r-increasingness)

A system of divisibilities Φ is said to be r-increasing whenever there is a partition $(X_1, \ldots, X_r)$ of its variables such that Φ is increasing for every total order $\prec$ having the property that given $x \prec y$, we have $x \in X_i$ and $y \in X_j$ for some $1 \leq i \leq j \leq r$.

r-increasing systems: grouping "independent variables"

$$f_1(\boldsymbol{z}) \mid g_1(\boldsymbol{z}) + a \cdot x$$
$$f_2(\boldsymbol{z}) \mid g_2(\boldsymbol{z}) + b \cdot y$$

Lipshitz's procedure requires ordering x and y. What happens if we relax this condition?

Definition (r-increasingness)

A system of divisibilities Φ is said to be r-increasing whenever there is a partition $(X_1, \ldots, X_r)$ of its variables such that Φ is increasing for every total order $\prec$ having the property that given $x \prec y$, we have $x \in X_i$ and $y \in X_j$ for some $1 \leq i \leq j \leq r$.

Theorem (Défossez, Haase, M., Pérez, 2024)

Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

r-increasing systems: grouping "independent variables"

EPAD does not have a polynomial small-model property

Consider the family of formulae $\{\varphi_n\}_{n\in\mathbb{N}}$ given by

$$\varphi_n(x) \coloneqq \exists x_1, \dots, x_{n+1} : x \geq x_{n+1} \wedge x_1 \geq 2 \wedge \bigwedge_{i=1}^{n} (\underbrace{x_i \mid x_{i+1} \ \wedge \ x_i + 1 \mid x_{i+1}}_{\text{implies } x_{i+1} > x_i^2}).$$

The smallest x satisfying $\varphi_n(x)$ is bigger than 2^{2^n}.

$\varphi_n(x)$ is $(n+2)$-increasing.

Theorem (Défossez, Haase, M., Pérez, 2024)

Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

A closer look to the local-to-global property of r-increasing systems

Theorem (Défossez, Haase, M., Pérez, 2024)

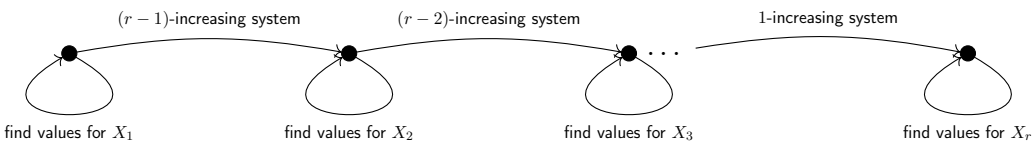
Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

A closer look to the local-to-global property of r-increasing systems

Theorem (Défossez, Haase, M., Pérez, 2024)

Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

Suppose Φ r-increasing with respect to the partition $(X_1, \ldots, X_r)$.

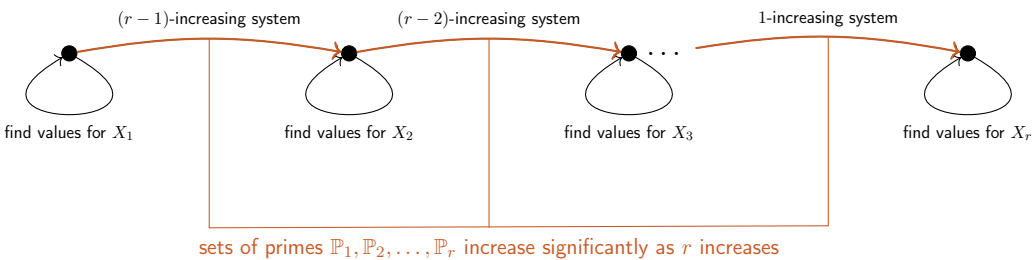


A closer look to the local-to-global property of r-increasing systems

Theorem (Défossez, Haase, M., Pérez, 2024)

Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

Suppose Φ r-increasing with respect to the partition $(X_1, \ldots, X_r)$.

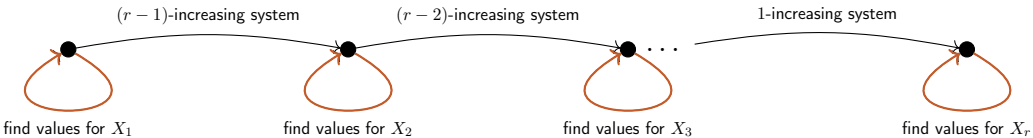


A closer look to the local-to-global property of r-increasing systems

Theorem (Défossez, Haase, M., Pérez, 2024)

Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

Suppose Φ r-increasing with respect to the partition $(X_1, \ldots, X_r)$.



$$\begin{cases} x \equiv a_p & \mod p^{k_p} \quad p \in \mathbb{P}_i \\ x \not\equiv b_{q,h} & \mod q \quad q \in Q_i, \quad h \in H_i \end{cases}$$

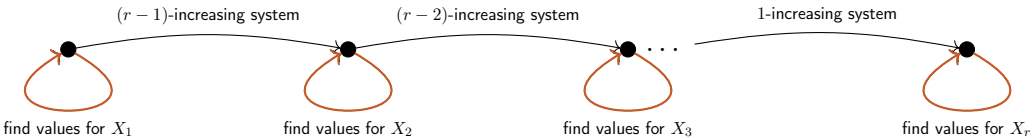
where $\mathbf{P}_i \cap Q_i = \varnothing$, Q_i increases as we assign values to variables in X_i, and H_i is of cardinality $< \min Q_i$

A closer look to the local-to-global property of r-increasing systems

Theorem (Défossez, Haase, M., Pérez, 2024)

Consider an r-increasing system Φ having a local solution $\boldsymbol{b}_p$ for every $p \in \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{a}$ over $\mathbb{N}$ of bit size $\langle \boldsymbol{a} \rangle \leq (\langle \Phi \rangle + \max\{\langle \boldsymbol{b}_p \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.

Suppose Φ r-increasing with respect to the partition $(X_1, \dots, X_r)$.



$$\begin{cases} x \equiv a_p & \mod p^{k_p} & p \in \mathbb{P}_i \\ x \not\equiv b_{q,h} & \mod q & q \in Q_i, \quad h \in H_i \end{cases}$$

where $\mathbf{P}_i \cap Q_i = \varnothing$, Q_i increases as we assign values to variables in X_i, and H_i is of cardinality $< \min Q_i$

A CRT for simultaneous congruences and non-congruences

Theorem (Défossez, Haase, M., Pérez, 2024)

Let $d \in \mathbb{N}$ and consider a finite set of coprime positive integers $M \cup Q$ such that $M \cap Q = \varnothing$, Q set of primes, and $d < \min(Q)$. the system of constraints

$$\begin{cases} x \equiv a_m & \mod m \qquad m \in M \\ x \not\equiv b_{q,i} & \mod q \qquad q \in Q, \;\; 1 \leq i \leq d \end{cases}$$

has a solution in every interval of size $((d+1) \cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$.

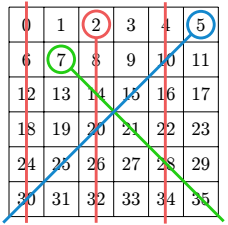
A CRT for simultaneous congruences and non-congruences

Theorem (Défossez, Haase, M., Pérez, 2024)

Let $d \in \mathbb{N}$ and consider a finite set of coprime positive integers $M \cup Q$ such that $M \cap Q = \varnothing$, Q set of primes, and $d < \min(Q)$. the system of constraints

$$\begin{cases} x \equiv a_m & \bmod m \qquad m \in M \\ x \not\equiv b_{q,i} & \bmod q \qquad q \in Q, \;\; 1 \le i \le d \end{cases}$$

has a solution in every interval of size $((d+1)\cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$.



Idea: This looks like a sieve problem!

$x \not\equiv 0 \mod 2, \quad x \not\equiv 0 \mod 5, \quad x \not\equiv 0 \mod 7$

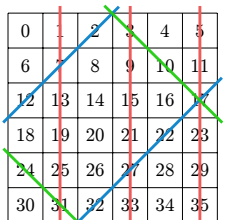
A CRT for simultaneous congruences and non-congruences

Theorem (Défossez, Haase, M., Pérez, 2024)

Let $d \in \mathbb{N}$ and consider a finite set of coprime positive integers $M \cup Q$ such that $M \cap Q = \varnothing$, Q set of primes, and $d < \min(Q)$. the system of constraints

$$\begin{cases} x \equiv a_m & \bmod m \qquad m \in M \\ x \not\equiv b_{q,i} & \bmod q \qquad q \in Q, \;\; 1 \le i \le d \end{cases}$$

has a solution in every interval of size $((d+1)\cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$.



Idea: This looks like a sieve problem!
But with shifts.

$x \not\equiv 1 \mod 2, \quad x \not\equiv 2 \mod 5, \quad x \not\equiv 3 \mod 7$

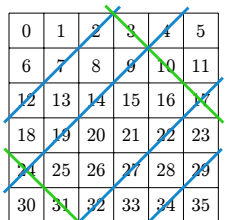
A CRT for simultaneous congruences and non-congruences

Theorem (Défossez, Haase, M., Pérez, 2024)

Let $d \in \mathbb{N}$ and consider a finite set of coprime positive integers $M \cup Q$ such that $M \cap Q = \varnothing$, Q set of primes, and $d < \min(Q)$. the system of constraints

$$\begin{cases} x \equiv a_m & \bmod m \qquad m \in M \\ x \not\equiv b_{q,i} & \bmod q \qquad q \in Q, \;\; 1 \le i \le d \end{cases}$$

has a solution in every interval of size $((d+1)\cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$.



Idea: This looks like a sieve problem!
But with shifts. Multiple non-congruences.

$x \not\equiv 4 \mod 5, \quad x \not\equiv 2 \mod 5, \quad x \not\equiv 3 \mod 7$

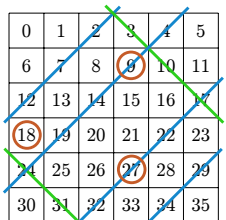
A CRT for simultaneous congruences and non-congruences

Theorem (Défossez, Haase, M., Pérez, 2024)

Let $d \in \mathbb{N}$ and consider a finite set of coprime positive integers $M \cup Q$ such that $M \cap Q = \varnothing$, Q set of primes, and $d < \min(Q)$. the system of constraints

$$\begin{cases} x \equiv a_m & \bmod m \qquad m \in M \\ x \not\equiv b_{q,i} & \bmod q \qquad q \in Q, \;\; 1 \leq i \leq d \end{cases}$$

has a solution in every interval of size $((d+1) \cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$.



Idea: This looks like a sieve problem!
But with shifts. Multiple non-congruences.
And inside some arithmetic progression.

$x \not\equiv 4 \mod 5, \quad x \not\equiv 2 \mod 5, \quad x \not\equiv 3 \mod 7$

A CRT for simultaneous congruences and non-congruences

Theorem (Défossez, Haase, M., Pérez, 2024)

Let $d \in \mathbb{N}$ and consider a finite set of coprime positive integers $M \cup Q$ such that $M \cap Q = \varnothing$, Q set of primes, and $d < \min(Q)$. the system of constraints

$$\begin{cases} x \equiv a_m & \mod m \qquad m \in M \\ x \not\equiv b_{q,i} & \mod q \qquad q \in Q, \;\; 1 \leq i \leq d \end{cases}$$

has a solution in every interval of size $((d+1) \cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$.

Conclusion: We can rely on an abstract version of Brun's pure sieve in order to prove our theorem. Off-the-shelf, this sieve already establishes that the system

$$x \not\equiv 0 \qquad \mod p \qquad p \in P,$$

with P set of primes, admits a solution of size at most $\#P^{7 \cdot \ln\ln(\#P+1)}$.

A corollary: IP-GCD has a polynomial small-model property

minimise $\boldsymbol{c}^{\mathsf{T}} \cdot \boldsymbol{x}$ (or maximise; variables over $\mathbb{Z}$)

subject to $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$

$$\gcd(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) \sim_i d_i \quad i \in [1, k], \quad \text{where } \sim_i \in \{=, \neq, \leq, \geq\},\ d_i \in \mathbb{N}$$

A corollary: IP-GCD has a polynomial small-model property

minimise $\boldsymbol{c}^{\mathsf{T}} \cdot \boldsymbol{x}$ (or maximise; variables over $\mathbb{Z}$)

subject to $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$

$$\gcd(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) \sim_i d_i \quad i \in [1,k], \quad \text{where } \sim_i \in \{=, \neq, \leq, \geq\},\ d_i \in \mathbb{N}$$

Theorem (Défossez, Haase, M., Pérez, 2024)

If an instance of IP-GCD is feasible then it has a solution (and an optimal solution, if one exists) of polynomial bit length. Hence, IP-GCD feasibility is NP-complete.

- polynomial-time translation into EPAD
- ad-hoc way to construct a polynomial-size 3-increasing system
- ad-hoc way for constructing polynomial-size local solutions

Bits to take away

On expressiveness...

EPAD does not have a polynomial small-model property

Consider the family of formulae $\{\varphi_n\}_{n\in\mathbb{N}}$ given by

$$\varphi_n(x) \coloneqq \exists x_1, \ldots, x_{n+1} : x \geq x_{n+1} \wedge x_1 \geq 2 \wedge \bigwedge_{i=1}^{n} \underbrace{(x_i \mid x_{i+1} \wedge x_i + 1 \mid x_{i+1})}_{\text{implies } x_{i+1} > x_i^2}.$$

The smallest x satisfying $\varphi_n(x)$ is bigger than 2^{2^n}.

Bits to take away

On expressiveness...

EPAD does not have a polynomial small-model property

Consi

$\varphi_n($

The s

NP-hardness for 2 variables, 4 inequalities, and 2 divisibility constraints

Quadratic residue problem [Manders and Aldeman, STOC'76]

Input: $a, b, m \in \mathbb{N}$ given in binary.
Question: Is there $x \in [1, b]$ such that $x^2 \equiv a \pmod{m}$?

The quadratic residue problem is NP-complete. Reduction to EPAD:

$$\exists x \exists y : \ 1 \leq x \leq b \wedge 1 \leq y \leq b^2 \wedge x + b^2 \mid y + b^2 x \wedge m \mid y - a \, .$$

Bits to take away

On applications...

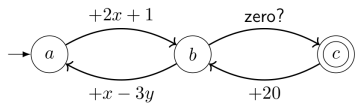
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

Parametric one-counter automata (POCA):



Bits to take away

On applications...

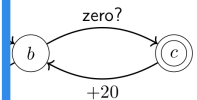
Applying EPAD:

Revisiting Parameter Synthesis for One-Counter Automata

Guillermo A. Pérez
University of Antwerp – Flanders Make, Belgium

Ritam Raha
University of Antwerp, Belgium
LaBRI, University of Bordeaux, France

CA):



QUADRATIC WORD EQUATIONS WITH LENGTH CONSTRAINTS, COUNTER SYSTEMS, AND PRESBURGER ARITHMETIC WITH DIVISIBILITY

ANTHONY W. LIN[a] AND RUPAK MAJUMDAR[b]

Reachability in Succinct and Parametric One-Counter Automata

Christoph Haase, Stephan Kreutzer, Joël Ouaknine, and James Worrell
Oxford University Computing Laboratory, UK

Simultaneous Rigid *E*-Unification and Related Algorithmic Problems

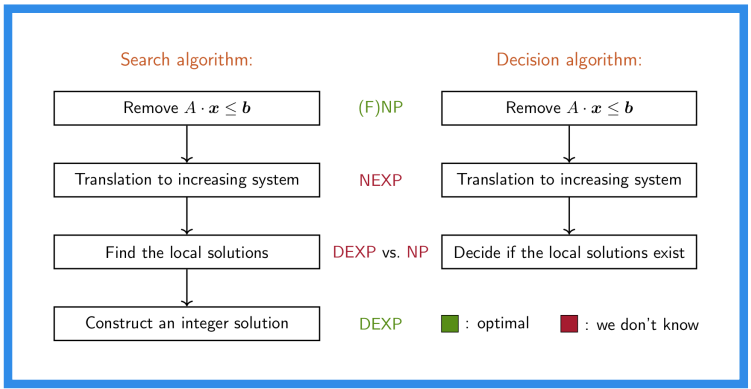
Anatoli Degtyarev
Computing Science Department
Uppsala University

Yuri Matiyasevich
Steklov Institute of Mathematics
St.Petersburg Division

Andrei Voronkov
Computing Science Department
Uppsala University

Bits to take away

On procedures...



Bits to take away

On procedures...

Search algorithm:

Remove $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$

Translation to increasing system

Find the local solutions

Construct an integer solution

(F)NP

NL

DEXP

DL

Decision algorithm:

Remove $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$

$$\begin{cases} x \equiv a_m \mod m & m \in M \\ x \not\equiv b_{q,i} \mod q & q \in Q, \quad 1 \leq i \leq d \end{cases}$$

has a solution in every interval of size $((d+1) \cdot \#Q)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M.$

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29
30	31	32	33	34	35

Idea: This looks like a sieve problem!
But with shifts. Multiple non-congruences.
And inside some arithmetic progression.

$x \not\equiv 4 \mod 5, \quad x \not\equiv 2 \mod 5, \quad x \not\equiv 3 \mod 7$