On Presburger Arithmetic with Divisibility Constraints: Applications and Algorithms

Alessio Mansutti

IMDEA Software Institute

Partially based on the paper "Integer Programming with GCD Constraints" (SODA'24)
co-authored with Rémy Défossez, Christoph Haase and Guillermo A. Pérez

Presburger arithmetic (PrA)

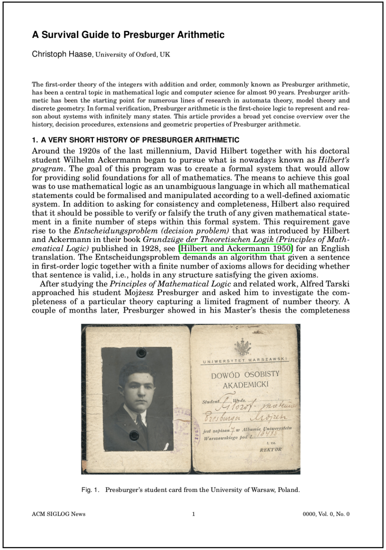
The first-order theory of $\langle \mathbb{Z}, 0, 1, +, \leq \rangle$

"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.

ACM SIGLOG News 1 0000, Vol. 0, No. 0

Existential Presburger Arithmetic with Divisibility constraints (EPAD)

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

$$(\cdot \mid \cdot) := \{(d, n) \in \mathbb{Z}^2 \ : \ c \cdot d = n \text{ for some } c \in \mathbb{Z}\}$$

A meaningless example: $\varphi(x, y) := \exists w : (x + y) \mid w \land (2w \leq 5x + y \lor \neg(w \mid (y + 2)))$

Existential Presburger Arithmetic with Divisibility constraints (EPAD)

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

$$(\cdot \mid \cdot) := \{(d, n) \in \mathbb{Z}^2 \; : \; c \cdot d = n \text{ for some } c \in \mathbb{Z}\}$$

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

Goals for this talk

- Overview a few recent applications of EPAD (automata theory, word equations)
- Discuss algorithmic aspects of EPAD (old and recent results)

Historical remarks

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.

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 $\langle \mathbb{Z}, 0, 1, +, \mid, \leq \rangle$, 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 $\langle \mathbb{Z}, 0, 1, +, \mid, \leq \rangle$, 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 NEXPTIME (Lechner, Ouaknine and Worrell).

2015–2023: various applications of EPAD are discovered.

A few (meaningful) examples

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

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

A few (meaningful) examples

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

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

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

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

A few (meaningful) examples

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

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

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

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

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

A few (meaningful) examples

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

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

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

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

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

Proposition (EPAD does not have a polynomial small-model property)

For $n \geq 1$, the following formula $\varphi_n(x)$ is only satisfied by integers greater than 2^{2^n}.

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

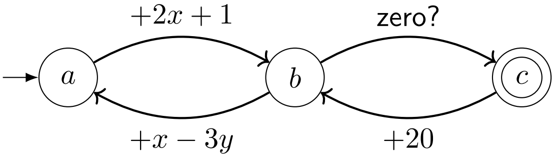
Applying EPAD:

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):



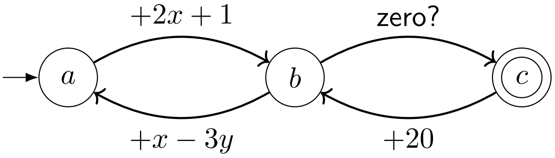
Applying EPAD:

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):



Parameter synthesis problem:

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

Output: A valuation of the parameters (e.g. x, y) over $\mathbb{Z}$ such that P holds in the starting configuration $(a, 0)$.

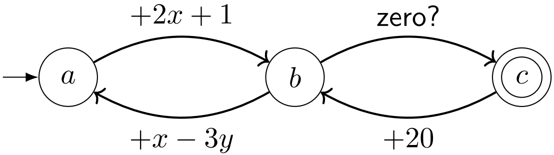
Applying EPAD:

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):



Reaching b with the counter set to 0:

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

initial value
of the counter

final value
of the counter

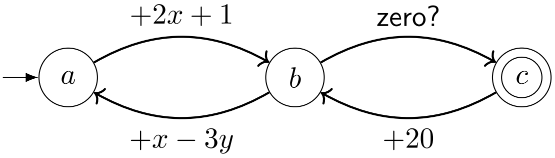
Applying EPAD:

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 automata (POCA):



Reaching b with the counter set to 0:

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

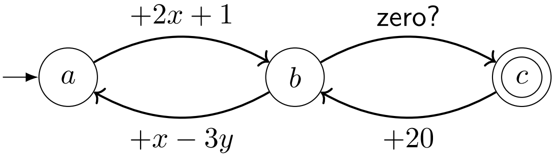
Applying EPAD:

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 automata (POCA):



Reaching b with the counter set to 0:

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

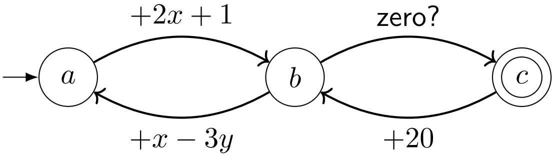
Applying EPAD:

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):



Reaching b with the counter set to 0:

$$
\begin{aligned}
&(2x+1+x-3y) \mid -2x-1 \\
\wedge\ &\big(2x+1=0 \vee (2x+1+x-3y \geq 0 \iff -2x-1 \geq 0)\big)
\end{aligned}
$$

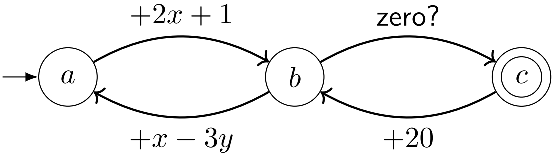
Applying EPAD:

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):



Reaching b with the counter set to 0:

$$\begin{array}{l} x := 2 \\ y := 4 \end{array}$$

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

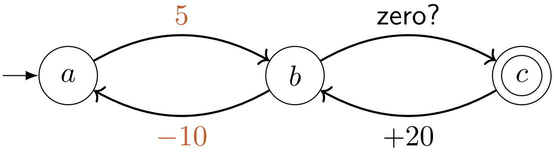
Applying EPAD:

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):



Reaching b with the counter set to 0:

$$\boxed{\begin{aligned} x &:= 2 \\ y &:= 4 \end{aligned}}$$

$$\begin{aligned} &(2x + 1 + x - 3y) \mid -2x - 1 \\ \wedge &\left(2x + 1 = 0 \vee (2x + 1 + x - 3y \geq 0 \iff -2x - 1 \geq 0)\right) \end{aligned}$$

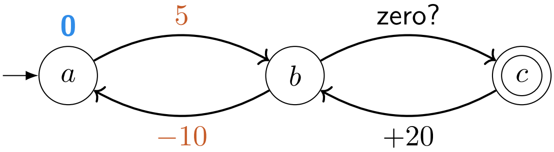
Applying EPAD:

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):



Reaching b with the counter set to 0:

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

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

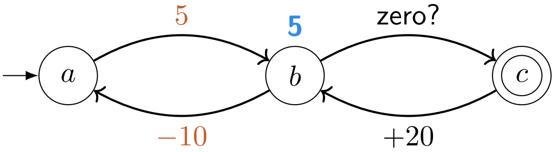
Applying EPAD:

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):



Reaching b with the counter set to 0:

$$x := 2 \qquad y := 4$$

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

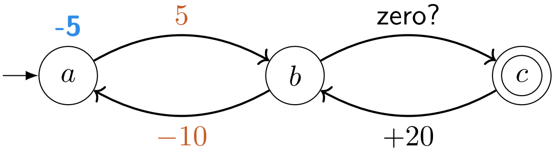
Applying EPAD:

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):



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

Reaching b with the counter set to 0:

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

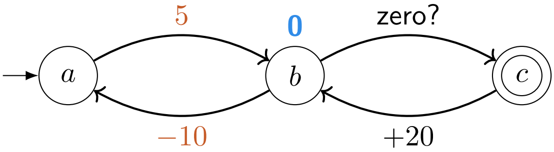
Applying EPAD:

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):



Reaching b with the counter set to 0:

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

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

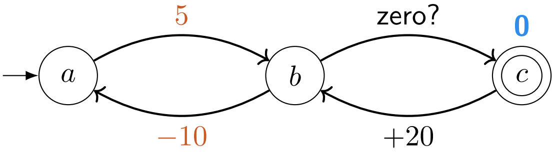
Applying EPAD:

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):



Reaching b with the counter set to 0:

$$\boxed{\begin{array}{l} x := 2 \\ y := 4 \end{array}}$$

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

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 lengths $|x|$ of variables $x \in X$.

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 lengths $|x|$ of variables $x \in X$.

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

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: Only look at systems of word equations where each variable occur at most twice. This problem can be solved with EPAD:

- translate the equations in a particular counter automata
- express the reachability relation of these counter automata into EPAD
- add the length constraints to the EPAD formula and check satisfiability.

EPAD satisfiability: complete problems

Reachability problem for parametric one-counter automata

Input: A parametric one-counter automata $\mathcal{A}$, and two configurations $(s_i, c_i), (s_f, c_f)$.

Question: Can the parameter be set over $\mathbb{Z}$ in a way such that $(s_i, c_i) \to_{\mathcal{A}}^{*} (s_f, c_f)$.

EPAD satisfiability: complete problems

Reachability problem for parametric one-counter automata

Input: A parametric one-counter automata $\mathcal{A}$, and two configurations $(s_i, c_i), (s_f, c_f)$.

Question: Can the parameter be set over $\mathbb{Z}$ in a way such that $(s_i, c_i) \to_{\mathcal{A}}^{*} (s_f, c_f)$.

Simultaneous rigid E-unification with one unary function symbol

Input: A set S of terms $\{\boldsymbol{s}_i = \boldsymbol{t}_i : i \in I\} \models \boldsymbol{s} = \boldsymbol{t}$ (I finite), where each equation is a word equation enriched with a single (uninterpreted) unary function symbol f.

Question: Is there a substitution $\sigma \colon X \to \{$words built from Σ and $f\}$ making all terms in S valid, i.e., $s\sigma = \boldsymbol{t}\sigma$ is derivable in the equational theory $\{\boldsymbol{s}_i\sigma = \boldsymbol{t}_i\sigma : i \in I\}$?

Deciding EPAD: roadmap

Consider the satisfiability problem 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. Appeal to a local-to-global property of increasing systems to find a solution in $\mathbb{Z}$
   (a.k.a. an Hasse principle: (1) find solutions over the p-adic integers for a finite set of primes; (2) glue these solutions using the CRT to find a solution over $\mathbb{Z}$)

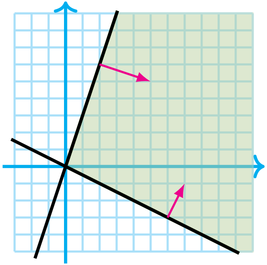
1: Remove the system of inequalities

Theorem (von zur Gathen and Sieveking, '78)

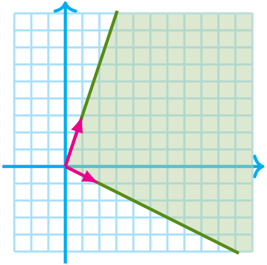
Let $\Phi(\boldsymbol{x}) := A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge C \cdot \boldsymbol{x} = \boldsymbol{d}$, *with* $\boldsymbol{x}$ *vector of* d *variables. Then,*

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

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



$\equiv$



1: Remove the system of inequalities

Theorem (von zur Gathen and Sieveking, '78)

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

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

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

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

1: Remove the system of inequalities

Theorem (von zur Gathen and Sieveking, '78)

Let $\Phi(\boldsymbol{x}) := A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge C \cdot \boldsymbol{x} = \boldsymbol{d}$, *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 $r := \operatorname{rank}(C)$, $\boldsymbol{u}_j \in \mathbb{Z}^d$ *and* $E_j = [\boldsymbol{p}_{j,1}, \dots, \boldsymbol{p}_{j,d-r}] \in \mathbb{Z}^{d \times (d-r)}$.

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

(implicit) equalities in $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$ $\Rightarrow$ some variables are "eliminated"

2: Find an equisatisfiable increasing system – idea

Theorem (Extended Chinese Remainder Theorem (CRT))

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

The univariate system of divisibilities $\begin{cases} m_i \mid (a_i \cdot x - r_i) & i \in [1,k] \end{cases}$

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 and $m_i \in \mathbb{Z}$.

The univariate system of divisibilities $\begin{cases} m_i \mid (a_i \cdot x - r_i) & i \in [1,k] \end{cases}$

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 $x_1 \prec \dots \prec x_d$ of the variables in $\boldsymbol{x}$ such that, for every $f \mid g$ implied by Φ,

$$\begin{aligned} & (\text{leading variable of } f) \prec (\text{leading variable of } g) \\ \text{or} \quad & f \mid g \text{ is a trivial divisibility of the form } f \mid a \cdot f. \end{aligned}$$

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 $x_1 \prec \dots \prec x_d$ 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 $\quad f \mid g$ 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

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

Output: an equisatisfiable increasing system

1. if Φ is increasing, then return it
   (in polynomial time. The algorithm is based on finding the Kernel of a matrix.
   If Φ is increasing, the algorithm returns an order on the variables)
2. if Φ is not increasing,

Proposition

$\Phi \models \bigvee_{i=1}^{n} h_i = 0$ *for some finite set* $\{h_1, \dots, h_n\}$ *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

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

Output: an equisatisfiable increasing system

1. if Φ is increasing, then return it

ix.

2.

omials.

Example: The system $2x + 1 \mid -x + 5$ is not increasing. We have:

$$\bigvee_{c \in \mathbb{Z}} c \cdot (2x + 1) = -x + 5\,.$$

However, c can be bounded in $[-3, 3]$:

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

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

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

Deciding EPAD: what we have seen so far

Consider the satisfiability problem 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. Appeal to a local-to-global property of increasing systems to find a solution in $\mathbb{Z}$ (a.k.a. an Hasse principle: (1) find solutions over the p-adic integers for a finite set of primes; (2) glue these solutions using the CRT to find a solution over $\mathbb{Z}$)

3: 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 $x_1 \prec \cdots \prec x_d$

The algorithm we would like (but it is incorrect):

For i from 1 to d

(from previous iterations, we have evaluated all variables x_j with $j < i$)

1. consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathsf{LV}(g) = x_i$
   (because of increasingness, f is constant and $g = a \cdot x_i + r$ with $a, r \in \mathbb{Z}$)
2. apply the CRT on S, finding a solution for x_i

3: 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 $x_1 \prec \dots \prec x_d$

The algorithm we would like (but it is incorrect):

For i from 1 to d

(from previous iterations, we have evaluated all variables x_j with $j < i$)

1. consider the set S of all non-trivial divisibilities $f \mid g$ in Φ with $\mathrm{LV}(g) = x_i$
   (because of increasingness, f is constant and $g = a \cdot x_i + r$ with $a, r \in \mathbb{Z}$)
2. apply the CRT on S, finding a solution for x_i

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: 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 $x_1 \prec \cdots \prec x_d$

The algorithm we would like (but it is incorrect):

We need prophets foretelling us what values we can pick.
These prophets are the local solutions.
They give additional congruences for the CRT.

$x \equiv 0 \mod 5$

(because of increasingness, f is constant and $g = a \cdot x_i + r$ with $a, r \in \mathbb{Z}$)

2. apply the CRT on S, finding a solution for x_i

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: 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: 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

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

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

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

The right-to-left direction is algorithmic; it uses the CRT to construct the solution.

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.
2. **Find an equisatisfiable increasing system:**
   in NEXPTIME. The size of the output is exponential in the number of variables.

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.
2. **Find an equisatisfiable increasing system:**
   in NEXPTIME. The size of the output is exponential in the number of variables.
3. **Appeal to a local-to-global property of increasing systems:**

   Computing the primes in P:

   Finding a certificate for a local solution:

   Compute a local solution:

   Construct the integer solution:

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.
2. **Find an equisatisfiable increasing system:**
   in NEXPTIME. The size of the output is exponential in the number of variables.
3. **Appeal to a local-to-global property of increasing systems:**

   Computing the primes in P: reduces to an instance of integer factoring; P has polynomially many primes of polynomial size (Défossez, Haase, M., Pérez, '23).

   Finding a certificate for a local solution:

   Compute a local solution:

   Construct the integer solution:

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.
2. **Find an equisatisfiable increasing system:**
   in NEXPTIME. The size of the output is exponential in the number of variables.
3. **Appeal to a local-to-global property of increasing systems:**

   Computing the primes in P: reduces to an instance of integer factoring; P has polynomially many primes of polynomial size (Défossez, Haase, M., Pérez, '23).

   Finding a certificate for a local solution: in NP (Guépin, Haase, Worrell, '19).

   Compute a local solution:

   Construct the integer solution:

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.
2. **Find an equisatisfiable increasing system:**
   in NEXPTIME. The size of the output is exponential in the number of variables.
3. **Appeal to a local-to-global property of increasing systems:**

   Computing the primes in P: reduces to an instance of integer factoring; P has polynomially many primes of polynomial size (Défossez, Haase, M., Pérez, '23).

   Finding a certificate for a local solution: in NP (Guépin, Haase, Worrell, '19).

   Compute a local solution: in EXPTIME (direct argument in Lipshitz'78).

   Construct the integer solution:

Deciding EPAD: complexity remarks

1. **Remove the system of inequalities:**
   in (F)NP thanks to the bounds obtained by von zur Gathen and Sieveking.
2. **Find an equisatisfiable increasing system:**
   in NEXPTIME. The size of the output is exponential in the number of variables.
3. **Appeal to a local-to-global property of increasing systems:**

   Computing the primes in P: reduces to an instance of integer factoring; P has polynomially many primes of polynomial size (Défossez, Haase, M., Pérez, '23).

   Finding a certificate for a local solution: in NP (Guépin, Haase, Worrell, '19).

   Compute a local solution: in EXPTIME (direct argument in Lipshitz'78).

   Construct the integer solution: in EXPTIME (Lipshitz) in a parameter $\mathcal{R} \in \mathbb{N}$ that is bounded by the number of variables (Défossez, Haase, M., Pérez, '23).

EPAD in NP ? Local-to-global property is unproblematic

Appeal to a local-to-global property of increasing systems:

Computing the primes in P: reduces to integer factoring

Finding a certificate for a local solution: in NP

Corollary

The satisfiability problem for increasing systems of divisibility constraints is in NP.

EPAD in NP ? Local-to-global property is unproblematic

Appeal to a local-to-global property of increasing systems:

Computing the primes in P: reduces to integer factoring

Finding a certificate for a local solution: in NP

Corollary

The satisfiability problem for increasing systems of divisibility constraints is in NP.

Observation: known exponential small-models are unproblematic

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

can be easily rewritten in increasing form.

EPAD in NP ? Making the system increasing is problematic

Find an equisatisfiable increasing system:
in NEXPTIME. The size of the output is exponential in the number of variables.

- Best algorithm for this problem is still Lipshitz's one from 1978.
- Recent results by M. Starchak's PhD thesis might shed new lights on this issue.

EPAD in NP ? Making the system increasing is problematic

Find an equisatisfiable increasing system:
in NEXPTIME. The size of the output is exponential in the number of variables.

- Best algorithm for this problem is still Lipshitz's one from 1978.
- Recent results by M. Starchak's PhD thesis might shed new lights on this issue.

While we wait for a better algorithm...

Consider a fragment F of EPAD.

- If for every Φ in F we can compute an equisatisfiable increasing formula in non-deterministic polynomial time, then the satisfiability problem for F is in NP,
- and if local solutions have polynomial size and the parameter $\mathcal{R} \in \mathbb{N}$ is bounded by a fixed number for every Φ in F, then F has a polynomial small-model property.

IP-GCD feasibility is in NP

$$\begin{aligned} \text{minimize} \quad & \boldsymbol{c}^\intercal \cdot \boldsymbol{x} \\ \text{subject to} \quad & A \cdot \boldsymbol{x} \leq \boldsymbol{b} \\ & \gcd(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) \sim_i d_i \quad i \in [1,k], \quad \text{where } \sim_i \in \{=, \neq, \leq, \geq\},\ d_i \in \mathbb{N} \end{aligned}$$

Theorem (Défossez, Haase, M., Pérez, '23)

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.

For feasibility:

- polynomial translation into EPAD
- ad-hoc ways for translation into increasing system and finding local solutions
- parameter $\mathcal{R}$ always bounded by 3

Recap

The satisfiability problem for the existential fragment of $\langle \mathbb{Z}, 0, 1, +, |, \leq \rangle$ ...

- ...is NP-hard (even when the number of variables is fixed)
- ...is in NEXPTIME
- ...has applications in automata theory and for solving word equations
- ...inter-reduces to, e.g., reachability in parametric one-counter automata.

Could it be in NP ? Bottleneck is the transformation to increasing systems.

Could it be outside NP ? Hard to say: there are open problems in word equations that (1) capture EPAD, (2) are not known to be decidable, (3) best lower bound is NP.