

Decidable Fragments of Integer Arithmetic: Beyond Presburger Arithmetic

Marius Bozga & Radu Iosif
Verimag/CNRS (Grenoble, France)

First Order Arithmetic of Natural Numbers

- $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ is **undecidable** [Church '36]
- $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle^{\exists}$ is **undecidable** (Hilbert's 10th Problem) [Matyiasovich '76]
- $\langle \mathbb{N}, +, |, 0, 1 \rangle$ is **undecidable** [Robinson '49]
 - $\langle \mathbb{N}, +, |, 0, 1 \rangle$ is a subtheory of $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$: $f|g \leftrightarrow \exists x f \cdot x = g$
- $\langle \mathbb{N}, +, |, 0, 1 \rangle^{\exists}$ is the *existential* fragment of $\langle \mathbb{N}, +, |, 0, 1 \rangle$
 - shown to be **decidable** [Lipshitz '78]
- $\langle \mathbb{N}, +, 0, 1 \rangle$ is **decidable** [Presburger '29]

Goal: better understand the boundary between decidable and undecidable subtheories of FO arithmetic.

Applications of FO Arithmetic of \mathbb{N}

Automatic verification of systems with infinite state spaces:

- **Automata with Integer Counters**
 - reachability within automata with **flat** control structures and **affine** transition relations is definable in PA [Comon, Yurski '98]
 - reachability within more powerful classes of automata can be defined using more expressive **decidable** theories.
- **Programs with Dynamic Linked Data Structures**
 - verification of *quantitative properties* relative to the size of data structures (e.g., lengths of lists, heights of trees, etc.)
 - PA is too weak even for reasoning about lists [Bozga, Iosif '05]

Outline

- The Left Divides Fragment of $\langle \mathbb{N}, +, |, 0, 1 \rangle$
- Parametric Linear Diophantine Systems $\mathfrak{D}(1)$

The Left-Divides Fragment of $\langle \mathbb{N}, +, |, 0, 1 \rangle$

Syntactic fragment of formulas with following *prenex form*:

$$\mathcal{L}_{|}^{(n)}: \mathbf{Q}_1 \mathbf{z}_1 \dots \mathbf{Q}_n \mathbf{z}_n \mathbf{R}_1 \mathbf{x}_1 \dots \mathbf{R}_m \mathbf{x}_m \varphi(\vec{x}, \vec{z})$$

where each divisibility predicate is of the form:

$$f(\vec{z}) | g(\vec{x}, \vec{z})$$

and there are no linear dependencies between \vec{x} and \vec{z}

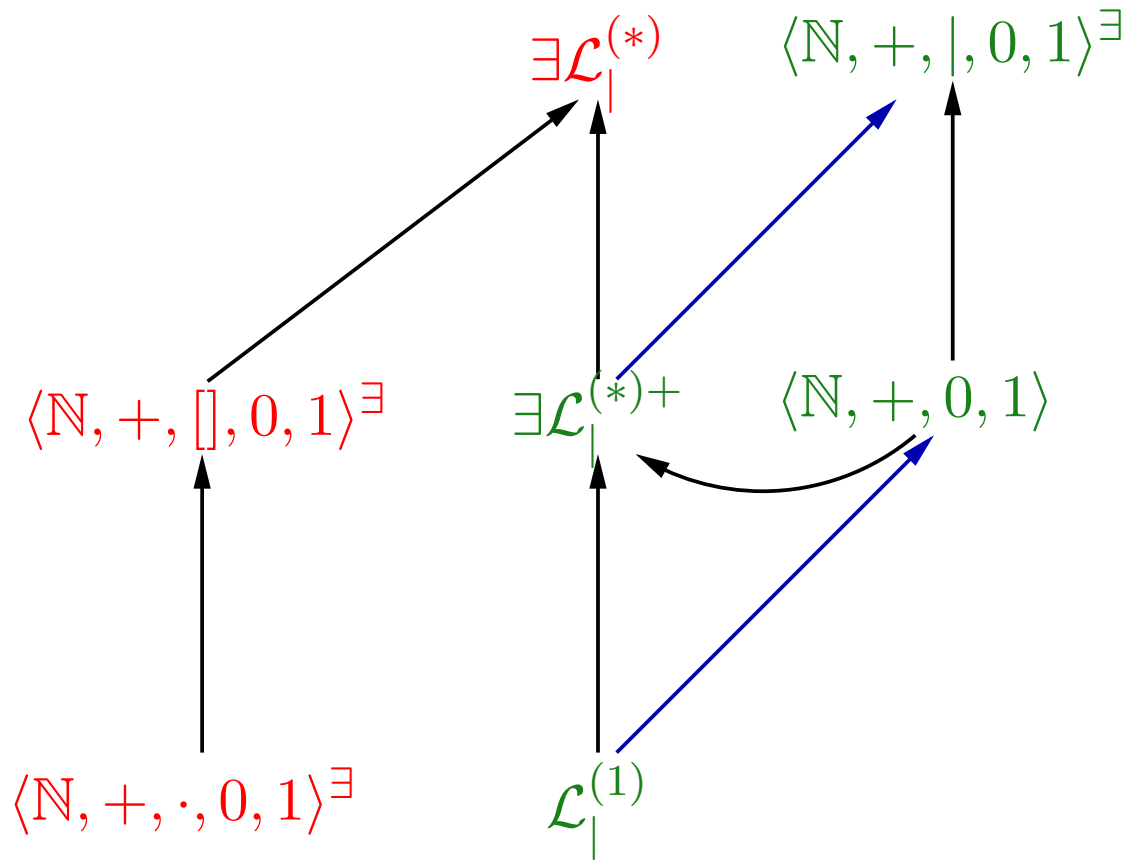
Good subject for research:

- is undecidable but has interesting decidable sub-fragments, which can express queries beyond the scope of known decidable theories:

$$\exists \mathbf{z} \forall \mathbf{x} \forall \mathbf{y} \phi(\mathbf{x}, \mathbf{y}) \wedge \mathbf{z} | \mathbf{x} \wedge \mathbf{z} | \mathbf{y} \wedge \mathbf{z} \neq \mathbf{1}$$

- useful in modeling the semantics of programs handling lists

Context and Contributions



————— "our contribution"
 ————— "definable in"

$$\mathcal{L}_|^{(1)}: \mathbf{QzQ_1x_1 \dots Q_mx_m} \varphi(\vec{x}, z)$$

$$\exists \mathcal{L}_|^{(*)}: \exists \mathbf{z_1 \dots z_n} \mathbf{Q_1x_1 \dots Q_mx_m} \varphi(\vec{x}, \vec{z})$$

TOOLS FOR PROVING DECIDABILITY

The Chinese Remainder Theorem

We use a generalized version of the CRT:

$$\exists x \bigwedge_{i=1}^K m_i | (a_i x - r_i) \iff \bigwedge_{1 \leq i, j \leq K} (a_i m_j, a_j m_i) | (a_i r_j - a_j r_i) \wedge \bigwedge_{i=1}^K (a_i, m_i) | r_i$$

where (A, B) denotes the **greatest common divisor** of A and B

CRT eliminates existential quantifiers introducing g.c.d. subterms.

Taming the Greatest Common Divisor

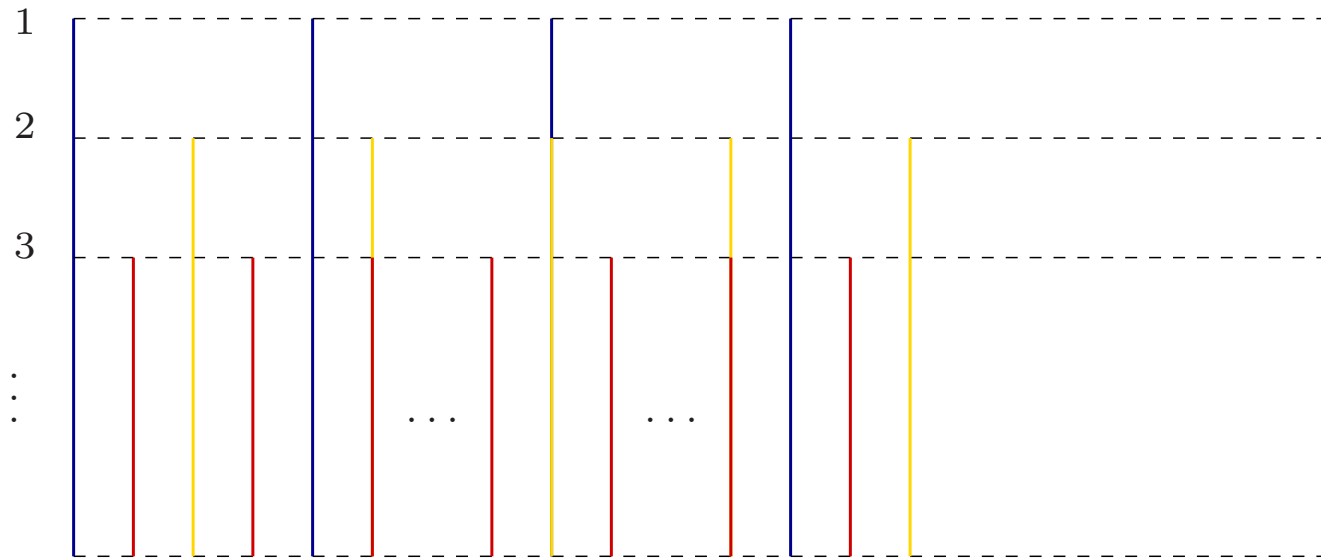
$$A(x) = ax + b, B(x) = cx + d$$

$$\exists p, q, r \in \mathbb{Z} \forall x . pA(x) = qB(x) + r$$

$$\forall x \left[(A(x), B(x)) = (A(x), r) \right]$$

$$\forall x \left[(A(x), r) \mid F \iff \bigvee_{i=0}^{r-1} A(x) \equiv i \pmod{r} \wedge (i, r) \mid F \right]$$

A 25\$ Conjecture of Erdős



N arithmetic progressions $\{a_i + b_i\mathbb{N}\}_{i=1}^N$ cover \mathbb{N} \iff they cover the set $1, 2, 3, \dots, 2^N$. [R. Crittenden and C. Vanden Eynden '69]

Elimination of universal quantifiers:

$$\forall x \bigvee_{i=1}^N b_i | x - a_i \iff \bigwedge_{t=1}^{2^N} \bigvee_{i=1}^N b_i | t - a_i$$

A Generalized Version of Erdős' Lemma

N progressions $\{a_i + b_i\mathbb{N}\}_{i=1}^N$ **cover a progression $a + b\mathbb{N}$** \iff they cover the set **$\{a, a + b, \dots, a + b \cdot (2^N - 1)\}$** .

Elimination of universal quantifiers in presence of negation:

$$\forall x \bigvee_{i=1}^N b_i | x - a_i \quad \vee \quad \bigvee_{j=1}^M c_j \nmid x - d_j \iff$$

$$\forall x \bigwedge_{j=1}^M c_j | x - d_j \quad \rightarrow \quad \bigvee_{i=1}^N b_i | x - a_i \iff$$

$$\underbrace{\neg \exists y \bigwedge_{j=1}^M c_j | y - d_j}_{\text{vacuity}} \vee \underbrace{\exists y \bigwedge_{j=1}^M c_j | y - d_j}_{\text{non-vacuity}} \wedge \underbrace{\bigwedge_{t=1}^{2^N} \bigvee_{i=1}^N b_i | [c_j]_{j=1}^M \cdot t + y - a}_{\text{coverage}}$$

DECIDABILITY OF $\mathcal{L}_|^{(1)}$

$$\mathcal{L}_|^{(1)} : \mathbf{QzR}_1\mathbf{x}_1 \dots \mathbf{R}_m\mathbf{x}_m \varphi(\vec{x}, z)$$

Reduction of $\mathcal{L}_|^{(1)}$ to Presburger Arithmetic

$$Q_1 x_1 \dots Q_n x_n \bigvee_{i=1}^N \left(\bigwedge_{j=1}^{M_i} f_{ij}(z) \mid f'_{ij}(\vec{x}, z) \wedge \bigwedge_{j=1}^{P_i} g_{ij}(z) \ \not\mid g'_{ij}(\vec{x}, z) \wedge \varphi_i(\vec{x}) \wedge \psi_i(z) \right)$$

where $f_{ij}, f'_{ij}, g_{ij}, g'_{ij}$ are linear functions and φ_i, ψ_i are PA formulas

- eliminate \vec{x} from φ_i (e.g. using the semilinear form of φ_i)
- eliminate quantified variables x_n, x_{n-1}, \dots, x_1
- translate the solved form into Presburger Arithmetic

An Example

Define the set of all z that satisfy:

$$\forall x \forall y \ z | 12x + 4y \rightarrow z | 3x + 12y$$

An Example

Define the set of all z that satisfy:

$$\forall x \quad \underbrace{\forall y \ z|12x + 4y \rightarrow z|3x + 12y}_{\left[\neg \exists y \ z|12x+4y \vee \exists y \ z|12x+4y \wedge z|3x+12y \wedge z|3x+12\left(y + \frac{z}{4}\right) \right]}$$

An Example

Define the set of all z that satisfy:

$$\forall x \quad \underbrace{\forall y \ z|12x + 4y \rightarrow z|3x + 12y}_{\left[\neg \underbrace{\exists y \ z|12x + 4y}_{(z,4)|12x} \vee \exists y \ z|12x+4y \wedge z|3x+12y \wedge z|3x+12\left(y + \frac{z}{(z,4)}\right) \right]}$$

An Example

Define the set of all z that satisfy:

$$\forall x \exists y \ z | 12x + 4y \wedge z | 3x + 12y \wedge z | 3x + 12y + \frac{12z}{(z, 4)}$$

Note: $(z | 3x + 12y)$ **implies** $(z | 3x + 12y + \frac{12z}{(z, 4)} \iff z | \frac{12z}{(z, 4)} \iff \top)$

An Example

Define the set of all z that satisfy:

$$\forall x \exists y \underbrace{z | 12x + 4y \wedge z | 3x + 12y}_{z | 33x \wedge (z, 4) | 12x \wedge (z, 12) | 3x}$$

Solution: $z \in \{1, 3, 11, 33\}$

DECIDABILITY OF $\exists\mathcal{L}_1^{(*)}$

$$\exists\mathcal{L}_1^{(*)} : \exists\mathbf{z}_1 \dots \exists\mathbf{z}_n \mathbf{R}_1\mathbf{x}_1 \dots \mathbf{R}_m\mathbf{x}_m \varphi(\vec{x}, \vec{z})$$

Negation leads to Undecidability

- $\langle \mathbb{N}, +, [], 0, 1 \rangle^{\exists}$ can be defined in $\exists \mathcal{L}_1^{(*)}$:

$$[x, y] = z \iff \forall t \ x|t \wedge y|t \leftrightarrow z|t$$

- the **perfect square** relation can be defined in $\langle \mathbb{N}, +, [], 0, 1 \rangle$:

$$x^2 = y \iff y + x = [x, x + 1]$$

- **multiplication** is defined using the following:

$$(x + y)^2 - (x - y)^2 = 4xy$$

- we have reduced **Hilbert's Tenth Problem** to the satisfiability of $\exists \mathcal{L}_1^{(*)}$

The Positive Fragment is Decidable

We apply the same quantifier elimination as for $\mathcal{L}_|^{(1)}$:

- the solved form involves terms of the form:

$$(f_1(\vec{z}), f_2(\vec{z}), \dots, f_n(\vec{z})) | h(\vec{z})$$

- define $\exists \mathcal{L}_|^{(*)+}$ into $\langle \mathbb{N}, +, |, 0, 1 \rangle^\exists$ [Lipshitz '78]:

$$(f_1, (f_2, \dots, f_n) \dots) | h$$

CRT
 \Leftrightarrow

$$\exists y_1 \ f_1 | y_1 - h \wedge (f_2, \dots, f_n) | y_1$$

CRT
 \Leftrightarrow

...

$$\exists y_1 \exists y_2 \dots \exists y_{n-1} \ f_1 | y_1 - h \wedge \bigwedge_{i=2}^{n-1} f_i | y_i - y_{i-1} \wedge f_n | y_{n-1}$$

Outline

- The Left Divides Fragment of $\langle \mathbb{N}, +, |, 0, 1 \rangle$
- Parametric Linear Diophantine Systems $\mathfrak{D}(1)$

The Problem

$$\left\{ \begin{array}{l} a_{11}(m) \cdot x_1 + a_{12}(m) \cdot x_2 + \dots + a_{1k}(m) \cdot x_k = b_1(m) \\ a_{21}(m) \cdot x_1 + a_{22}(m) \cdot x_2 + \dots + a_{2k}(m) \cdot x_k = b_2(m) \\ \dots \\ a_{r1}(m) \cdot x_1 + a_{r2}(m) \cdot x_2 + \dots + a_{rk}(m) \cdot x_k = b_r(m) \end{array} \right.$$

where $a_{ij}(m), b_i(m)$ are polynomials in m .

Are there positive integers m, x_1, \dots, x_k that satisfy all of the equations?

Minimal Solutions of Linear Systems

- Reduce to **homogeneous** systems:

$$A(m)\vec{x} = B(m) \iff A(m)\vec{x} = B(m)x_{n+1} \wedge x_{n+1} = 1$$

- Bound the minimal solutions [Pottier '90]:

$$x_i \leq (n - r_0) \left(\frac{\sum_{i,j} |a_{ij}|}{r_0} \right)^{r_0} \leq m^{(K+3)r+1}$$

where $r_0 = \text{rank}(A)$, K is the maximum degree of $a_{ij}(m)$, and m sufficiently large.

The m -base representation of minimal solutions is bounded by $(K + 3)r + 1$

- The m -base representation of minimal solutions can be expressed by linear systems

Solving Systems of m -base Equations

Example

$$1 \cdot x_1 + m \cdot x_2 = m^2 + 2$$

$$\text{For } m \geq 3: \quad (1)_m \cdot x_1 + (10)_m \cdot x_2 = (102)_m$$

Minimal solutions are of the form $x_1 = (a_2 a_1 a_0)_m$ and $x_2 = (b_1 b_0)_m$

$$(1)_m \cdot (a_2 a_1 a_0)_m + (10)_m \cdot (b_1 b_0)_m = (102)_m$$

$$\left\{ \begin{array}{l} a_0 = 2 \\ a_1 + b_0 = 0 \\ a_2 + b_1 = 1 \end{array} \right. \quad \left\{ \begin{array}{l} a_0 = 2 \\ a_1 + b_0 = m \\ a_2 + b_1 + 1 = 1 \end{array} \right.$$

$$(x_1, x_2) = \{((102)_m, (0)_m), ((2)_m, (10)_m)\} \cup \{((c \ 2)_m, (m-c \ 0)_m) \mid 1 < c < m\}$$

Conclusions

- Syntactic fragment of $\langle \mathbb{N}, +, |, 0, 1 \rangle$ based on a separation of variables on the left of $|$ from the variables on the right.
- $\mathcal{L}_|^{(1)}$ with one variable on the left is reducible to Presburger Arithmetic.
- $\exists \mathcal{L}_|^{(*)}$ where all variables on the left are existentially quantified, is undecidable.
- $\exists \mathcal{L}_|^{(*)+}$ where all divisibility propositions occur under an even number of negations, is decidable, by reduction to $\langle \mathbb{N}, +, |, 0, 1 \rangle^{\exists}$.
- Satisfiability of $\mathcal{D}(1)$ systems is decidable