Presburger Arithmetic and Semi-Linear Sets: The Past, the Present and the Future

Christoph Haase
University of Oxford, UK

partly based on joint work with Dmitry Chistikov

PUMA Seminar – 9 June 2017

Presburger Arithmetic

First-order theory of $\langle \mathbb{N}, 0, 1, +, = \rangle$

Mojzesz Presburger (1904 – 1943)

Examples

"Every natural number is odd or even":

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

Generalizes Integer Programming:

$$\exists \vec{x} : A \cdot \vec{x} = \vec{b}$$

$$\iff \exists \vec{x} : \vec{a}_1^{\mathsf{T}} \cdot \vec{x} = b_1 \wedge \cdots \wedge \vec{a}_n^{\mathsf{T}} \cdot \vec{x} = b_n$$

Theorem (Presburger, 1929)
Presburger arithmetic admits quantifier elimination.

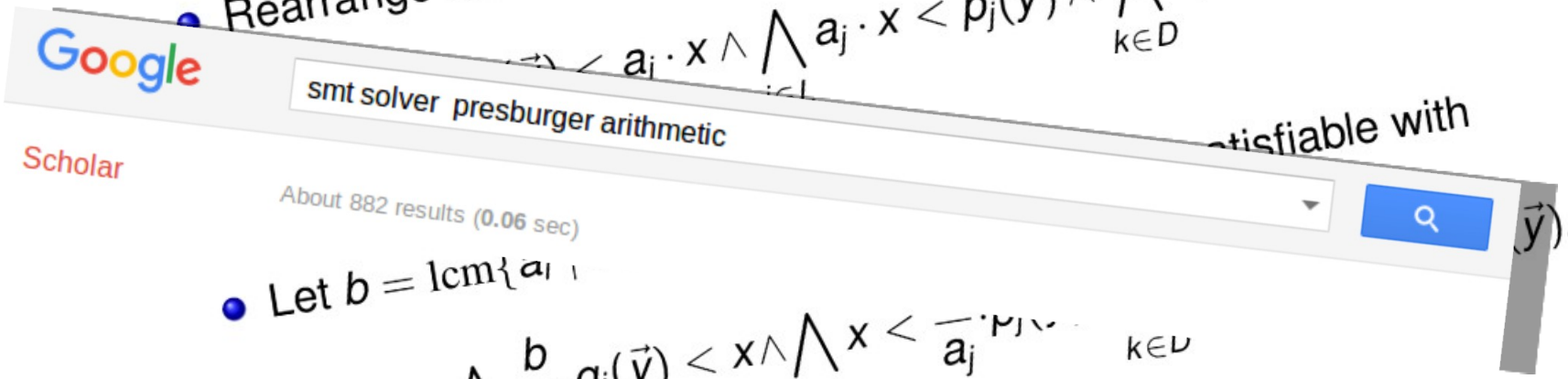
History of Presburger Arithmetic

1929	Presburger: $\mathrm{FO}\langle\mathbb{N}, 0, 1, +, =\rangle$ is decidable
1936	Church: $\mathrm{FO}\langle\mathbb{N}, 0, 1, +, \cdot, =\rangle$ is undecidable
1949	Robinson: $\mathrm{FO}\langle\mathbb{N}, 0, 1, +, \mid, =\rangle$ is undecidable
1960	Büchi gives automata-based decision procedure for PA
1972	Cooper: practically usable quantifier elimination procedure for PA
1974	Fischer and Rabin: 2-EXP lower bound for PA
1978	Oppen: 3-EXP upper bound for PA by QE analysis
1980	Berman: PA is complete for $\mathrm{STA}(*, 2^{2^{n^{O(1)}}}, O(n))$
1997	Weispfenning: blow-up in QE procedure for PA is essentially tight
2008	Klaedtke: 3-EXP upper bound for automata-based approach
around 2010	PA standard theory in SMT solvers such as Z3 or CVC4

Quantifier-elimination for Presburger arithmetic

- Suffices to consider eliminating x from $F = \exists x \bigwedge_{1 \le i \le n} F_i$
- Rearrange matrix formula of F so that x is isolated:

$$\bigwedge_{j \in L} a_j \cdot x < p_j(\vec{y}) \wedge \bigwedge_{k \in D} c_k \mid a_k \cdot x + r_k(\vec{y}).$$



- Let $b = \mathrm{lcm}\{a_i \mid$ ... $\}$

$$G = \exists x \bigwedge_{i \in G} \frac{b}{a_i} \cdot q_i(\vec{y}) < x \wedge \bigwedge_{j \in L} x < \frac{\cdot p_j(\vec{y}) + b \mid x}{a_j} \quad k \in D$$

- Now G is equivalent to

$$\begin{cases} \bigvee_{0 \le m < c} G[m/x] & \text{if } G = \emptyset \\ \bigvee_{j \in G} \bigvee_{1 \le m \le c} G[((b/a_j) \cdot q_j(\vec{y}) + m)/x] & \text{otherwise} \end{cases}$$

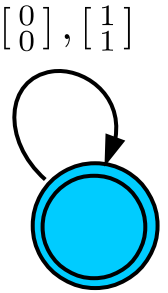
7 / 12

Automata-Based Decision Procedure

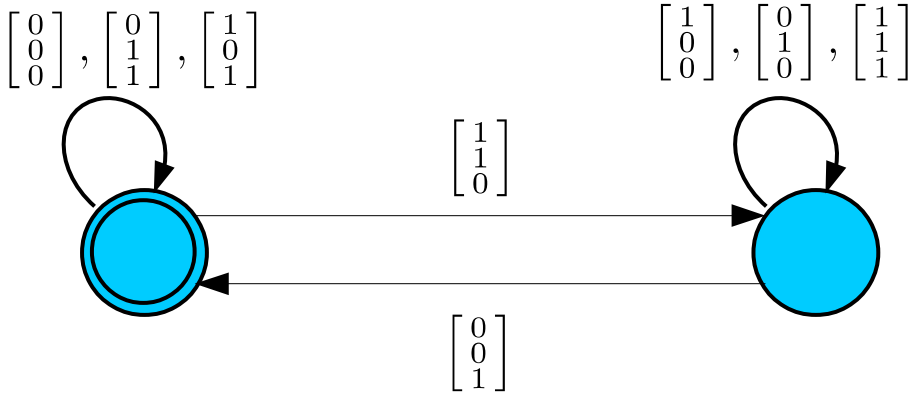
Encode valuations as paired bit-strings over alphabet

$$\Sigma_n = \left\{ \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \right\}$$

Gadget for $x_1 = x_2$:



Gadget for $x_1 + x_2 = x_3$:



...then apply closure under union intersection, complement, homomorphism and inverse homomorphism

Complexity of Presburger Arithmetic

number of variables in q-blocks \ number of quantifier alternations	arbitrary	fixed i
arbitrary	$\mathrm{STA}(*, 2^{2^{n^{O(1)}}}, O(n))$ Berman, 1980	$\mathrm{STA}(*, 2^{n^{O(1)}}, i)$ H., 2014
fixed j	$?$	$\mathrm{STA}(*, n^{O(j)}, i)$ Grädel, 1988

...if everything and even the structure is fixed then Presburger arithmetic is decidable in P [Nguyen, Pak, 2017]

Sets Definable in Presburger Arithmetic

Bringing a quantifier-free formula into DNF yields

$$\psi(\vec{x}) = \bigvee_{i \in I} A_i \cdot \vec{x} = \vec{b}_i$$

Non-negative solutions to $A \cdot \vec{x} = \vec{0}$ form a monoid:

if $A \cdot \vec{x} = \vec{0}$ and $A \cdot \vec{y} = \vec{0}$ then $A \cdot (\vec{x} + \vec{y}) = \vec{0}$

This monoid is finitely generated:

- Suppose the set of minimal solutions $P = \{\vec{x} : A \cdot \vec{x} = \vec{0}\}$ is infinite
- By Dickson's lemma, there are $\vec{x}, \vec{y} \in P$ such that $\vec{x} \leq \vec{y}$
- But then $\vec{z} := \vec{y} - \vec{x} \in M$ and $\vec{y} = \vec{x} + \vec{z}$, contradicting minimality of P

Sets Definable in Presburger Arithmetic

All solutions of $A \cdot \vec{x} = \vec{0}$ lie in the cone generated by P:

$$\text{cone}(P) := \{\lambda_1 \cdot \vec{p}_1 + \cdots + \lambda_n \cdot \vec{p}_n : \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}$$

What about solutions M of general $A \cdot \vec{x} = \vec{b}$?

$$M = B + \text{cone}(P)$$

minimal solutions of $(A - \vec{b}) \cdot (\vec{x}, y) = \vec{0}$ with y component equal to 1

minimal solutions of $A \cdot \vec{x} = \vec{0}$

both finite

Semi-Linear Sets

A set $M \subseteq \mathbb{N}^d$ is a *hybrid linear set* if there are $B, P \subseteq \mathbb{N}^d$ such that $M = L(B, P) := B + \text{cone}(P)$. A set $M \subseteq \mathbb{N}^d$ is *semi-linear* if it is a finite union of hybrid linear sets.

Hybrid Linear Sets as the Discrete Minkowski-Weyl Representation

Theorem (Minkowski-Weyl)
A set $M \subseteq \mathbb{R}^n$ is a polyhedron $A \cdot \vec{x} \geq \vec{c}$ if and only if there are finite $V, W \subseteq \mathbb{R}^n$ such that

$$M = \left\{ \sum_i \gamma_i \cdot \vec{v}_i : \gamma_i \in \mathbb{R}_{\geq 0}, \sum_i \gamma_i = 1, \vec{v}_i \in V \right\} + \left\{ \sum_i \lambda_i \cdot \vec{w}_i : \lambda_i \in \mathbb{R}_{\geq 0}, \vec{w}_i \in W \right\}$$

replace $\mathbb{R}_{\geq 0}$ by $\mathbb{N}$ to see relationship to hybrid linear representation

Semi-Linear Sets

Corollary

Presburger-definable sets are semi-linear. Conversely,

$$\vec{x} \in L(B, P)$$

$$\iff \exists \lambda_1 \ldots \lambda_n : \bigvee_{\vec{b} \in B} \vec{b} + \lambda_1 \cdot \vec{p}_1 + \cdots + \lambda_n \cdot \vec{p}_n \,.$$

In particular, semi-linear sets are closed under all Boolean operations.

Theorem (Pottier, 1991)

The set of solutions of $A \cdot \vec{x} = \vec{c}$ is a semi-linear set $L(B, P)$ s.t.

$$||B||, ||P|| \leq (n \cdot ||A|| + ||\vec{c}|| + 2)^{m+1}$$

largest absolute value

$m \times n$ matrix

History of Semi-Linear Sets

1961 — Parikh introduces semi-linear sets, shows that Parikh image of CFGs are semi-linear

1964 — Ginsburg and Spanier show that semi-linear sets coincide with Presburger-definable sets

1969 — Eilenberg and Schützenberger, and Ito show independently that semi-linear sets can be made unambiguous

1982 — Huynh gives bounds on descriptive complexity of complement and

1986 — norm of smallest vector in complement, proves that inclusion is Π_2^{P}-complete

2016 — Chistikov and H. give bounds on descriptive complexity of all Boolean operations for implicitly represented semi-linear sets

only largest absolute value is known

Complementing Semi-Linear Sets

Theorem (Chistikov, H., 2016)
Given a semi-linear set $M = \bigcup_{j \in J} L(C_j, Q_j) \subseteq \mathbb{N}^n$. Then

$$\overline{M} = \bigcup_{i \in I} L(B_i, P_i) \subseteq \mathbb{N}^n$$

such that

$$||B_i||, ||P_i|| \leq ||M||^{\#J \cdot O(n^4)}.$$

Corollary
The equivalence for exponent-sensitive commutative grammars is in coNEXP, improving a 2-EXPSpace upper bound of Mayr and Weihmann (2013).

Drawback
Blows-up non-elementary for repeated complementing.

Deciding Presburger Arithmetic via Semi-Linear Sets

Given $\phi = \exists \vec{x}_1 \, \forall \vec{x}_2 \ldots \exists \vec{x}_k : \psi(\vec{x}_1, \ldots, \vec{x}_k)$, obtain semi-linear representation $\bigcup_{i \in I} L(B_i, P_i)$ of $\psi(x_1, \ldots, \vec{x}_n)$.

Decide ϕ via repeated projection and complementation.

trivial

bad

Theorem (Chistikov, H., 2017)
Given a hybrid linear set $L(C, Q)$ then its universal projection is again a hybrid linear set $L(B, P)$ such that

$$||B|| \leq (||C|| + ||Q||)^{O(m^5)} \text{ and } ||P|| \leq ||Q||$$

Corollary
Quantified Integer Programming with fixed quantifier alternations is complete for every level of the poly. hierarchy.