Presburger Arithmetic

A Short Survey

Om Swostik Mishra

IIT Bombay

History and Introduction

- The mathematician Mojżesz Presburger formulated the basic principles of Presburger arithmetic in his 1929 paper "On the completeness of a certain system of arithmetic of whole numbers, in which addition occurs as the only operation".
- In this paper, it was established that Presburger arithmetic is complete and decidable.
- This result was achieved by using the 'quantifier elimination' method.
- Presburger showed the completeness of $Th(\mathbb{Z}, +, 0, 1)$, the first order theory of integers with addition, equality and standard axioms of arithmetic.

An Example

- Even though Presburger arithmetic captures only a fragment of number theory, lots of interesting problems can be expressed using it.
- Given positive integers $m_1, m_2 \dots m_n$, what is the largest number that cannot be obtained as a non-negative linear combination of those numbers? The answer, if it exists, is the smallest satisfying assignment of the formula:

$$\phi(x) = \forall y(x < y \rightarrow (\exists z_1, z_2 \dots z_n(y = z_1 m_1 + \dots z_n m_n \wedge z_1 \geq 0 \wedge \dots \wedge z_n \geq 0)))$$

- Any system of linear inequalities/equations can also be expressed using Presburger arithmetic.

The first approach to deciding PA is the quantifier elimination method [2]. Here's an example to illustrate this idea:
Given $\exists x, y, z \ (2x + 4y - 3z < 7) \wedge (3x - y + 2z < -4)$, we will eliminate the quantifier $\exists z$. Notice,
$\exists x, y, z \ (2x + 4y - 3z < 7) \wedge (3x - y + 2z < -4) \Leftrightarrow$
$\exists x, y, z \ (2x + 4y - 7 < 3z) \wedge (2z < -4 + y - 3x) \Leftrightarrow$
$\exists x, y, z \ (4x + 8y - 14 < 6z) \wedge (6z < -12 + 3y - 9x) \Leftrightarrow$
$\exists x, y \ (13x + 5y - 2 < 0)$
For the above example, we are looking for solutions over the reals. If we want to restrict our solution space to $\mathbb{Z}$, we need to introduce additional constraints:

$$\bigvee_{1 \leq m \leq 6} (6 \mid 4x + 8y - 14 + m) \wedge (13x + 5y - 2 + m < 0)$$

$$\vee \bigvee_{1 \leq m \leq 6} (6 \mid -9x + 3y - 12 - m) \wedge (13x + 5y - 2 + m < 0)$$

We will now describe the general process for eliminating quantifiers from any given formula. Note that $\forall x\ F \equiv \neg\exists x\ \neg F$, hence it suffices to restrict our attention to $\exists$ quantifiers. Given any any formula of the form $\exists\ F$ where F is quantifier-free, we proceed as follows:

- Transform F to disjunctive normal form and distribute $\exists\ x$ over the disjuncts. We will perform elimination separately for each conjunct of relations or negations of relations.
- Eliminate negation by using $\neg(\alpha < \beta) \to \beta < \alpha + 1$ and $\neg(\delta \mid \alpha) \to \vee_{i=1}^{\delta-1} \delta \mid \alpha + i$.
- Simplify each relation by collecting the x terms on one side. If a term doesn't invlove x, take it outside the quantifier. We are left with terms of the form: $\lambda x < \alpha$, $\beta < \mu x$ and $\delta \mid \nu x + \gamma$.

Quantifier elimination (continued)

- Let δ be the LCM of α, ν and β (i.e coefficients of x) over all relations in the conjunct. Multiply both sides of all relations with appropriate constants such that the coefficients of all x's are made δ. Replace $\exists x\, F(\delta x)$ with $\exists x\, (F(x) \wedge \delta \mid x)$. The result will again be a conjunct of relations but the coefficient of x in every term is 1.
- The elimination is performed using the equivalence:

$$\exists x\, (\alpha < x \wedge x < \beta \wedge \delta \mid x) \equiv \bigvee_{j=1}^{\delta} (\alpha + j < \beta \wedge \delta \mid \alpha + j)$$

It has been shown that this algorithm runs in deterministic triply exponential time [8].

- The aim is to construct an automaton whose language encodes all satisfying assignments of the given PA formula.
- Every formula in Presburger arithmetic can be interpreted as a Monadic Second Order formula on the integers with the $<$ relation and a $+$ function.
- Given any MSO formula, there exists a translation to a finite state automaton such that the language accepted by this automaton is exactly the set of satisfying assignments of the formula.
- This approach can lead to high complexity due to the possibility of repeated complementation. However, it has been shown that PA formulas have a special structure that prevents this non-elementary blow-up from happening [3].
- The run-time of this automata-based construction is triply-exponential in the size of the input formula. This is also a optimal bound.

Automata-conversion (Example)

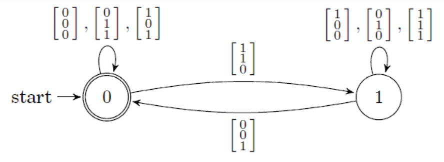

Figure 1: Finite automaton encoding the satisfying assignments of Φ

Let $\Phi(x, y, z) = (+(x, y) = z)$. The above figure represents an automata which accepts a tuple (i, j, k) iff $i + j = k$.

- The automata reads the binary representation of the numbers, adds digit by digit and accepts at 0 as long as a carry doesn't occur.
- When a carry does occur, the automata switches to state 1 and stays there until the carry has been resolved.
- Once the carry is resolved, the automata switches back to state 0 and accepts.

Semi-Linear sets

- Given a base vector $b \in \mathbb{Z}^d$ and a finite set of period vectors $P = \{p_1, \ldots, p_n\} \subseteq \mathbb{Z}^d$, the linear set $L(b, P)$ is defined as

$$L(b, P) = b + \{\lambda_1 p_1 + \cdots + \lambda_n p_n \;:\; \lambda_1 \geq 0 \wedge \cdots \wedge \lambda_n \geq 0\}$$

- A semi-linear set is a finite union of linear sets.
- Semi-linear sets are trivially closed under projection.

Semi-Linear sets (continued)

- Every linear set is definable in Presburger arithmetic. Let $v(i)$ denote the i-th component of vector v. $x \in L(b, P)$ iff x is a solution of

$$\Phi(x) = \exists \lambda_1 \dots \lambda_n \bigwedge_{1 \leq x \leq d} x(i) = b(i) + \lambda_1 p_1(i) + \cdots + \lambda_n p_n(i)$$

- Since a semi-linear set is a finite union of linear sets, it is also definable in PA.
- The reverse also holds i.e. every set of integer tuples definable in PA forms a semi-linear set.
- Since PA admits quantifier elimination, it suffices to show that the set of solutions to a system of linear inequalities and a system of linear congruences is semi-linear and that semi-linear sets are closed under intersection.

- Given a $d \times n$ matrix A, we will show that the set $S \subseteq \mathbb{N}_0^n$ consisting of non-negative integer solutions to $Ax = 0$ is semi-linear.
- S is a commutative monoid with respect to addition.
- Given vectors $v, w \in S$ with non-negative entries, we define a partial ordering $<$ such that $v \leq w$ if $v(i) \leq w(i), \forall i$.
- With respect to the ordering $<$, the set S has finitely many minimal elements (follows from Dickson's lemma).
- Let $P \subset S$ be the set of all minimal elements. It can be shown (by induction) that P generates every element of S.
- We can conclude that $S = L(0, P)$, which is a linear set.

Linear equations (continued)

- Consider the non-homogenous case i.e. let $S \subseteq \mathbb{N}_0^n$ be the set of all solutions of the equation $Ax = b$.
- If S is empty i.e. the equation has no solution, then semi-linearity of S trivially follows.
- If S is non-empty, consider the set B consisting of all minimal elements of S. Finiteness of B follows from Dickson's lemma.
- Let P be the finite set of minimal vectors which generates all solutions of the homogenous equation $Ax = 0$.
- Using the same argument as for the homogenous case, it follows,

$$S = L(B, P) = \bigcup_{b \in B} L(b, P)$$

- Given a system of linear inequalities $Ax \geq b$, let $S \subseteq \mathbb{N}_0^n$ denote the set of solutions, which we will show to be semi-linear.
- Let $B \subset S$ denote the set consisting of minimal elements of S. Finiteness of B follows from Dickson's lemma.
- Let P denote the finite set of minimal vectors satisfying the inequality $Ax \geq 0$. As before, we can show that, the set of vectors in P generate all solutions of the system $Ax \geq 0$.
- Using the same argument as was done for the case of linear equations, we have,

$$S = L(B, P) = \bigcup_{b \in B} L(b, P)$$

- Given a system of divisibility constraints, the set of solutions $S \subseteq \mathbb{N}_0^n$ forms a semi-linear set.
- Consider the system

$$\Phi(x) = \bigwedge_{1 \leq i \leq d} c_i \mid p_i(x)$$

  where $x = (x_1, \ldots, x_n)$ and each $p_i(x)$ is a linear expression in $x_1, \ldots, x_n$.
- Let $c = lcm(c_1, \ldots, c_n)$ and $B = \{v \in \{0, 1 \ldots, c-1\}^n \mid \Phi(v/x) \text{ is true}\}$.
- Now, let $P = \{c.e_i \mid 1 \leq i \leq n\}$, where e_i is the i-th unit vector.
- $S = L(B, P)$ is the set of non-negative integer solutions of $\Phi(x)$.

Closure under intersection

- Semi-linear sets are closed under intersection.
- Due to distributivity of union and intersection, it suffices to show intersection of two linear sets is semi-linear.
- Let $L(c, Q)$ and $L(d, R)$ be linear sets.
  $v \in L(c, Q) \cap L(d, R)$ iff there exists $\lambda, \gamma \geq 0$ such that,

$$\begin{aligned} & v = c + Q\lambda \text{ and } v = d + R\gamma \\ \Leftrightarrow \ & c + Q\lambda = d + R\gamma \\ \Leftrightarrow \ & (Q \mid -R) \begin{bmatrix} \lambda \\ \gamma \end{bmatrix} = d - c \end{aligned}$$

- The last condition reduces to a system of linear equations which we have shown to be semi-linear. Let $L(E, S)$ be the semi-linear set obtained after projecting the solution set to the λ-coordinates.

Closure under intersection (continued)

- Let $B = c + QE$ and $P = QS$. Recall that $v = c + Q\lambda$, where $\lambda \geq 0$.

$$\begin{aligned} L(c,Q) \cap L(d,R) &= c + \{Qw \mid w \in L(E,S)\} \\ &= c + Q.L(E,S) \\ &= c + Q.\{E + S\zeta \mid \zeta \geq 0\} \\ &= L(c + Q.E, P = Q.S) \\ &= L(B,P) \end{aligned}$$

- It follows that semi-linear sets are closed under intersection.
- We can conclude, given any PA formula, its set of solutions forms a semi-linear set.

- A linear set $L(b, P)$ decomposes as

$$L(b, P) = \bigcup_{i \in I} L(b_i, P_i)$$

where $P_i \subseteq P$ are linearly independent [5].

- We have an even stronger property [7]. Every semi-linear set M is equivalent to a semi-linear set

$$M = \bigcup_{i \in I} L(b_i, P_i)$$

such that all P_i are linearly independent and $L(b_i, P_i) \cap L(b_j, P_j) = \emptyset, \forall\, i \neq j$.

Complementation

- Complement of a semi-linear set also forms a semi-linear set.
- This follows from the equivalence between semi-linear and Presburger definable sets.
- Alternatively, we can give a direct proof of this result.
- Due to closure under union and intersection, it suffices to show complementation of a linear set is semi-linear.
- Let $M = L(b, P)$ be a linear set and WLOG assume P is linearly independent.
- Let $\widetilde{M}$ denote the convex hull of M.
- By Minkowski-Weyl's theorem, there is a system of linear inequalities $Ax \leq c$ defining $\widetilde{M}$.
- Then the set $\mathbb{R}^d \setminus \widetilde{M}$ can be obtained as the set of all solutions of the system $Ax > c$.

- For every $v \in M$, there exists unique $\lambda \in \mathbb{N}^n$ such that $v = b + P\lambda$.
- Any $w \in \widetilde{M} \setminus M$ can be obtained as $w = b + P\gamma$ with the exception that some component of γ is not integral.
- Define $C = b + (\{v \in P\lambda \cap \mathbb{Z}^d \ : \ \lambda \in [0,1)^n\} \setminus \{0\})$ which gives, $\widetilde{M} \setminus M = L(C, P)$.
- We can now realize,

$$\mathbb{Z}^d \setminus M = ((\mathbb{R}^d \setminus \widetilde{M}) \cap \mathbb{Z}^d) \cup L(C, P)$$

as a semi-linear set.

- The aim is to keep track of the constants and the size of the generator set while describing a semi-linear set.
- Let $Ax = 0$ be a homogenous system and consider the set of its non-negative integer solutions, with the generator set P.
- If $\|P\|$ denotes the largest absolute value in P,

$$\|P\| \leq (1 + \|A\|_{1,\infty})^r$$

- This bound was obtained by analyzing minimal solutions of linear diophantine systems [9].

Computational Complexity

- Cooper's quantifier elimination algorithm runs in deterministic triply exponential time [8].
- In 1974, a non-deterministic doubly exponential time lower bound was shown for full Presburger arithmetic [4]. This was the first hardness result for PA.
- In 1980, Berman [1] showed that Presburger arithmetic is complete for $STA(*, 2^{2^{p(n)}}, O(n))$, where p is a fixed polynomial.
- The above result yields a doubly exponential space upper bound.
- The high lower bounds for Presburger arithmetic require formulas with an unbounded number of alternations. Fixing the number of quantifiers/alternations lowers the complexity.

Leonard Berman.
The complexity of logical theories.
Theoretical Computer Science, 11(1):71–77, 1980.

David C Cooper.
Theorem proving in arithmetic without multiplication.
Machine intelligence, 7(91-99):300, 1972.

Antoine Durand-Gasselin and Peter Habermehl.
On the use of non-deterministic automata for presburger arithmetic.
In *International Conference on Concurrency Theory*, pages 373–387. Springer, 2010.

Michael J Fischer and Michael O Rabin.
Super-exponential complexity of presburger arithmetic.
In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 122–135. Springer, 1998.

Seymour Ginsburg and Edwin H Spanier.
Bounded ALGOL-like languages.
SDC, 1963.

Christoph Haase.
A survival guide to presburger arithmetic.
ACM SIGLOG News, 5(3):67–82, 2018.

Ryuichi Ito.
Every semilinear set is a finite union of disjoint linear sets.
J. Comput. Syst. Sci., 3(2):221–231, 1969.

Derek C Oppen.
A 222pn upper bound on the complexity of presburger arithmetic.
Journal of Computer and System Sciences, 16(3):323–332, 1978.

Loic Pottier.
Minimal solutions of linear diophantine systems: bounds and algorithms.
In *International Conference on Rewriting Techniques and Applications*, pages 162–173. Springer, 1991.

Conclusion

THANK YOU!