Linear arithmetic theories: Theory and applications

Part I: Applications

Christoph Haase
University of Oxford, UK

VTSA, 14 October 2021

Overview

Part I: Applications
- Parikh images and Parikh's theorem
- Petri nets
- Eulerian graphs
- State-space over-approximations for Petri nets definable in linear arithmetic

Part II: Decision procedures
- Satisfiability modulo theories
- Quantifier elimination
- Generator-based procedures
- Automata-based procedures
- The complexity of Presburger arithmetic

Overview

Part III: Lower bounds
- Fischer-Rabin trick
- Gödel encoding
- Diophantine gluing
- Short Presburger arithmetictic

Part IV: Advanced topics
- Presburger arithmetic with divisibility
- Counting in Presburger arithmetic

Parikh images

Given $w \in \Sigma^*$, $\Sigma = \{a_1, \ldots, a_n\}$, the Parikh image of w is the vector $\boldsymbol{v} = (m_1, \ldots, m_n) \in \mathbb{N}^m$ such that every $a_i \in \Sigma$ occurs exactly m_i times in w.

Rohit Parikh
(*1936)

Theorem (Parikh, 1966)
For any context-free language L, there is a regular language M with the same Parikh image.

Even Newton knew about it...

Sir Isaac Newton
(1642 – 1726)

From Newton’s second letter to Leibnitz:

“The foundations of these operations is evident enough, in fact; but because I cannot proceed with the explanation of it now, I have preferred to conceal it thus:

6a cc d æ 13e ff 7i 3l 9n 4o 4q rr 4s 8t 12u x.”

Petri nets

A Petri net is a tuple $\mathcal{N} = (P, T, f)$ consisting of

- A finite set of places P
- A finite set of transitions T
- A flow function $f \colon (P \times T) \cup (T \times P) \to \mathbb{N}$

- Induces infinite transition system whose vertices are functions $m \colon P \to \mathbb{N}$

- Well-suited for modeling systems with unbounded number of components and synthesis tasks

Vector addition systems with states

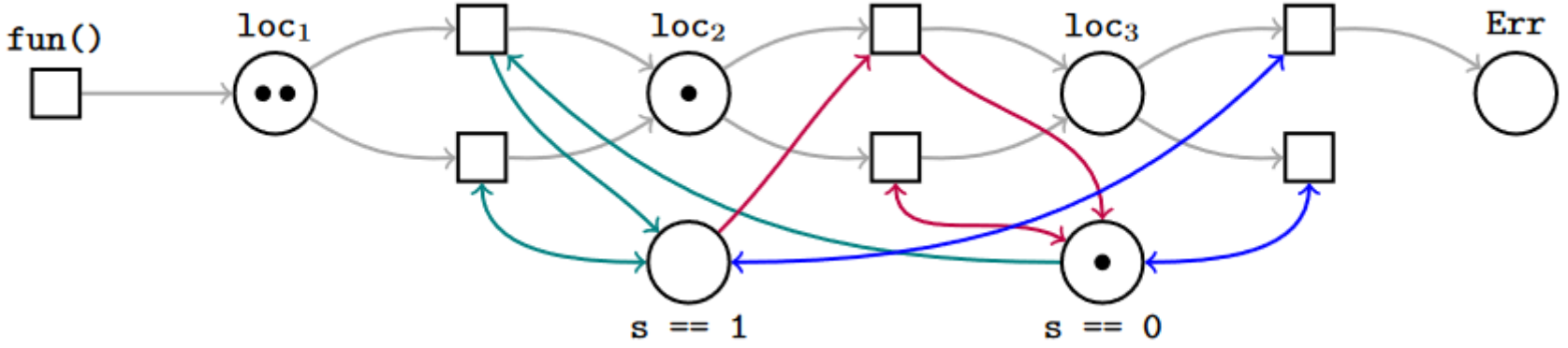
A vector addition system with states is a tuple $\mathcal{A} = (Q, d, \Delta)$ consisting of a

- A finite set of control states Q
- A finite number of d counters over $\mathbb{N}$
- A finite transition relation $\Delta \subseteq Q \times \mathbb{Z}^d \times Q$

- Model equivalent to Petri nets

Modeling concurrent processes

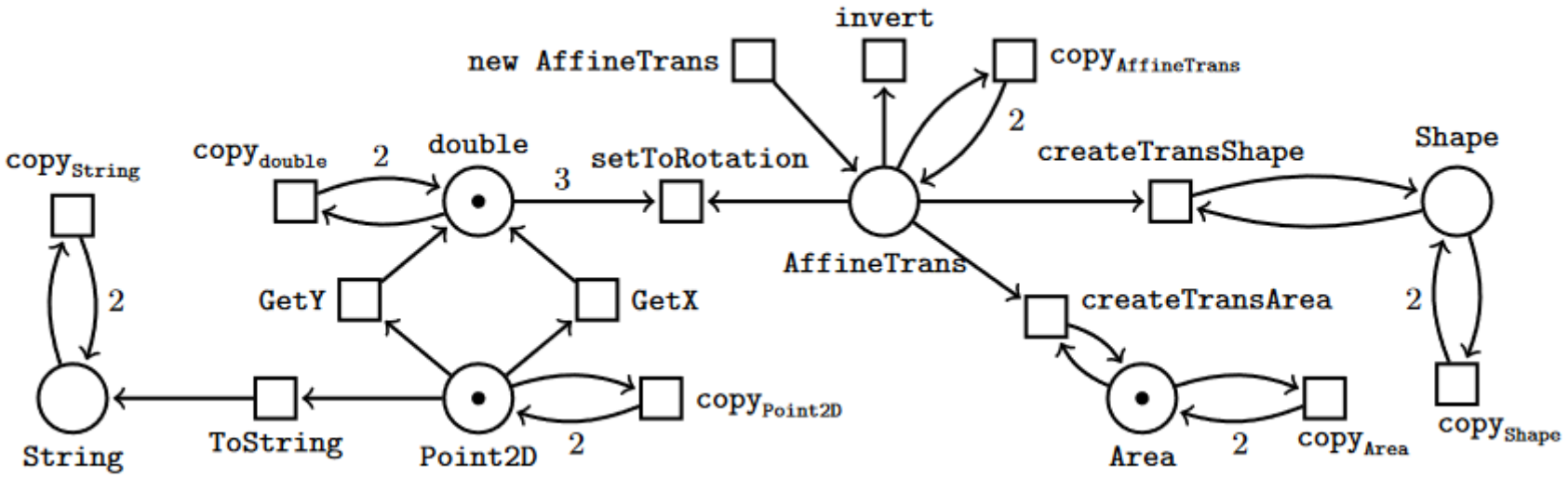
```
0 def fun():
1     s = 1
2     s = 0
3     if s == 1: raise Err()
```



Modeling of APIs

java.awt.geom
`new AffineTransformation()`
`Shape Shape.createTransformedShape(AffineTransformation)`
`String Point2D.ToString()`
`double Point2D.getX()`
`double Point2D.getY()`
`void AffineTransformation.setToRotation(double, double, double)`
`void AffineTransformation.invert()`
`Area Area.createTransformedArea(AffineTransformation)`

Modeling of APIs



Computational complexity

- Deciding whether $\boldsymbol{v} \in \mathbb{N}^n$ is in the Parikh image of some context-free language L is NP-complete
- Deciding coverability for Petri nets is EXPSPACE-complete
- Deciding reachability requires time growing at least as fast as the Ackermann function

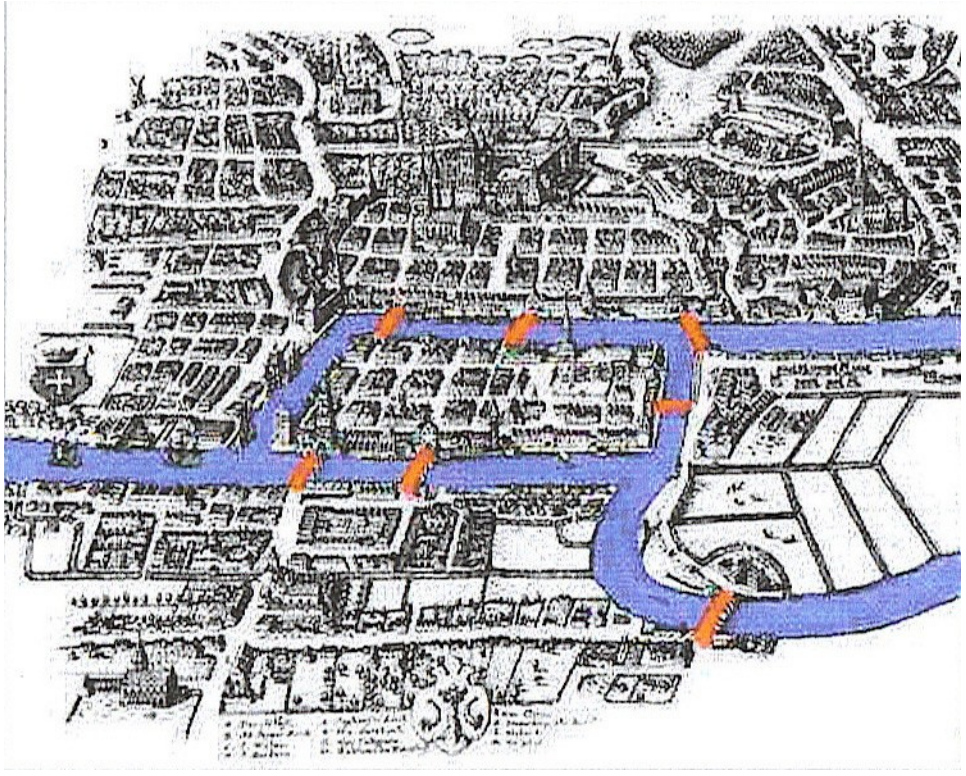
Linear arithmetic theories

Quantified Boolean combinations of linear inequalities

$$a_1 \cdot x_1 + \cdots + a_n \cdot x_n \geq b$$

- Variables range over reals (linear real arithmetic) or integers (linear integer arithmetic, aka Presburger arithmetic)
- Satisfiability: Does $\Phi(x_1, \ldots, x_n)$ have a solution?
- Optimal satisfiability: Find a solution of $\Phi(x_1, \ldots, x_n)$ that minimizes a linear objective function f

Seven bridges of Königsberg



Leonhard Euler
(1707 – 1783)

Eulerian graphs

An directed graph is Eulerian if

- The in-degree of every vertex equals its out-degree
- All vertices lie in a single strongly connected component

Theorem (Euler)
A directed graph has a circuit visiting every edge exactly once if and only if it is Eulerian.

Walks on graphs

Euler's criteria allow to characterize walks in a graph

- Every vertex in the graph is entered as often as it is left (except for starting and final vertex)

- Undirected graph induced by walk is connected

First condition readily expressible in linear arithmetic. Given $G = (V, E)$, if x_e records number of times edge $e \in E$ is traversed require

$$\bigwedge_{v \in V} \sum_{e=(w,v) \in E} x_e = \sum_{e=(v,w) \in E} x_e$$

Graph connectivity

- Simulate a breadth-first search
- Label all vertices with discovery times y_v
- For all but the initial vertex v^*, require that there is a predecessor discovered before:

$$y_{v^*} = 1 \wedge \bigwedge_{v \in V \setminus \{v^*\}} (y_v > 1 \wedge \bigvee_{\{v,w\} \in E} y_w < y_v)$$

Parikh images via linear arithmetic

Theorem (Seidl, Schwentick, Muscholl, Habermehl, 2004)
For any regular language $L \subseteq \Sigma^*$, $\Sigma = \{a_1, \ldots, a_n\}$, there is a formula $\Phi(x_1, \ldots, x_n)$ of linear integer arithmetic such that $\Phi(m_1, \ldots, m_n)$ holds whenever $(m_1, \ldots, m_n)$ is the Parikh image of some $w \in L$.

Moreover, $\Phi(x_1, \ldots, x_n)$ can be constructed in linear time from a finite-state automaton defining L.

Parikh images of context-free grammars

Approach can be lifted to Parikh images of context-free grammars:

- In- and out-flow conditions need to be adapted
- Graph connectivity needs to be suitably defined

Showing that any set definable in linear integer arithmetic is the Parikh image of some regular language gives Parikh’s theorem for free… more tomorrow

What about Petri nets and VASS?

Reachability sets of Petri nets and VASS not definable in linear integer arithmetic:

$$\left\{(x, y, n) \in \mathbb{N}^3 : x + y \leq 2^n\right\}$$

Relaxations of Petri nets and VASS have reachability sets definable in linear arithmetic:

- Petri nets whose places can “carry” negative number of tokens
- Continuous Petri nets in which transitions can be fired fractional number of times

State-space over-approximations

Petri net relaxations over-approximate state space of original Petri net:

- Any marking reachable in original net remains reachable
- Length of path in relaxation reaching a marking lower bounds length of path reaching the marking in original Petri net

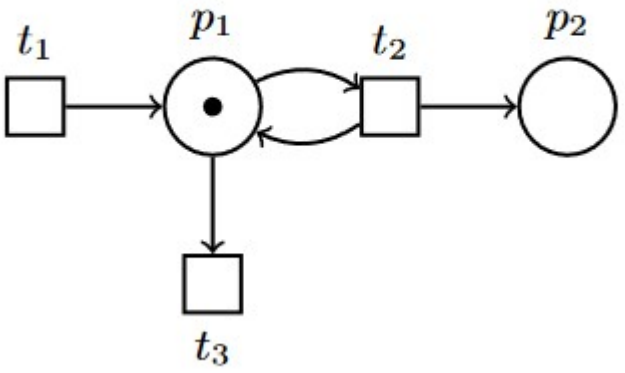
Graph traversal heuristics

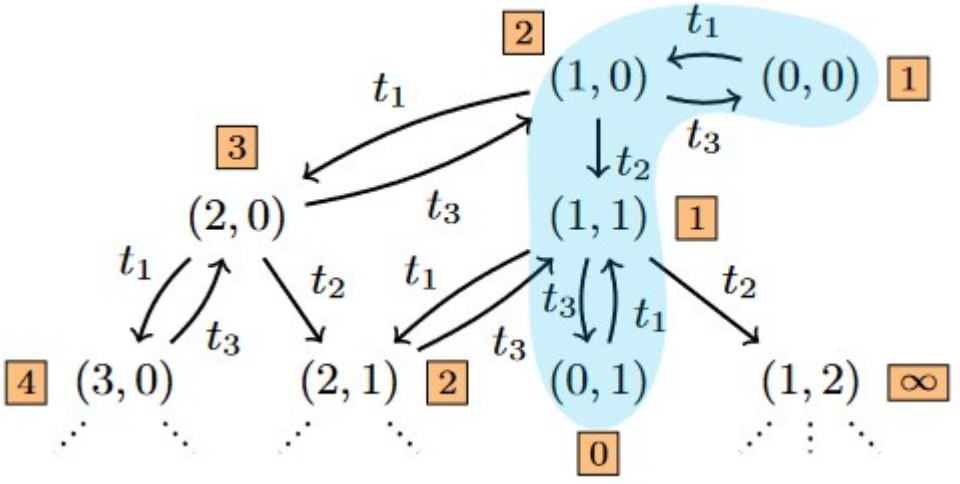
Relaxations enable graph traversal heuristics in infinite transition graph:

- A* and greedy best-first search (GBFS) two well-known graph traversal algorithms
- Both algorithms keep set of active nodes that are expanded according to heuristic function estimating distance to target
- A* finds shortest path if heuristic function always under-approximates actual distance

A* example for Petri nets

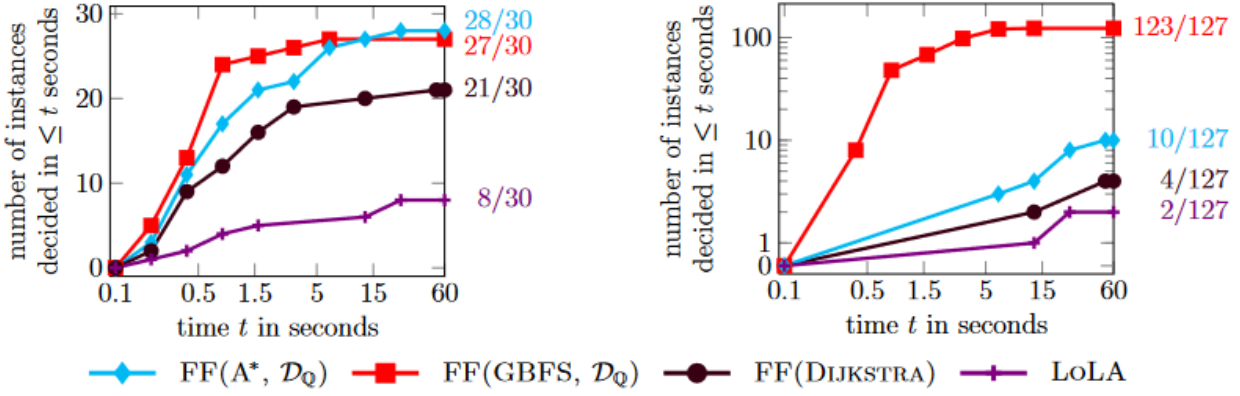
Relaxations dramatically shrink search space:





Benchmarks for large-scale instances

Suite	Size	Number of places				Number of transitions			
		min.	med.	mean	max.	min.	med.	mean	max.
COVERABILITY	61	16	87	226	2826	14	181	1519	27370
SYPET	30	65	251	320	1199	537	2307	2646	8340
RANDOM WALKS	127	52	306	531	2826	60	3137	5885	27370



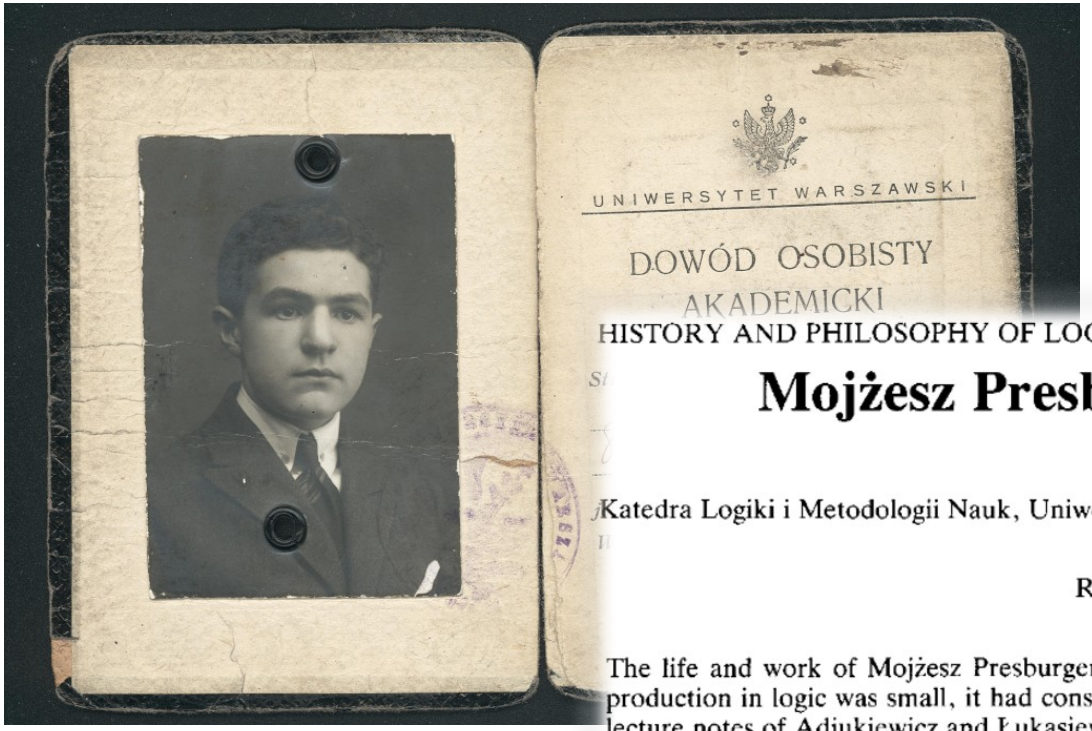
Linear arithmetic theories: Theory and applications

Part II: Decision procedures

Christoph Haase
University of Oxford, UK

VTSA, 14 October 2021

Presburger arithmetic



HISTORY AND PHILOSOPHY OF LOGIC, **12** (1991), 211–223

Mojżesz Presburger: Life and Work

JAN ZYGMUNT

Katedra Logiki i Metodologii Nauk, Uniwersytet Wrocławski, 50-139 Wrocław, ul.Szewska 36, Poland

Received 13 July 1990

The life and work of Mojżesz Presburger (1904–1943?) are summarised in this article. Although his production in logic was small, it had considerable impact, both his own researches and his editions of lecture notes of Adjukiewicz and Łukasiewicz. In addition, the surviving records of his student time at Warsaw University provide information on a little-studied topic.

Mojżesz Presburger (1904 – c. 1943)

Presburger arithmetic

Presburger arithmetic is first-order theory of the structure $(\mathbb{N}, +, 0, 1, =)$ (alternatively $(\mathbb{Z}, +, 0, 1, <)$)

Examples

"Every integer is odd or even": $\forall x \, \exists y \, x = 2y \vee x = 2y + 1$

Frobenius problem:
Given co-prime $a_1, \ldots, a_n \in \mathbb{N}$, is the largest $c \in \mathbb{N}$ not representable as their linear combination at least k?

$$\exists c \, \forall x \, y_1 \ldots y_n \, x = a_1 \cdot y_1 + \cdots + a_n \cdot y_n \rightarrow x \neq c \wedge c \geq k$$

Why Presburger arithmetic?

- Number theory is (highly) undecidable
- Starting point of algorithmic paradigms: quantifier elimination, automata-based methods, methods based on generating functions, generator-based methods
- Beautiful geometry: semi-linear sets
- Wide range of further applications: automated verification, program synthesis, compiler optimisation

Satisfiability Modulo Theories

- Decides existential fragment of Presburger arithmetic
- Most widely used in practice
- Leverages strength of SAT solvers

Systems of linear inequalities

Simplest formula of existential Presburger arithmetic is a system of linear inequalities:

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

- Efficiently solvable over the reals using simplex algorithm
- Cutting plane method uses simplex algorithm to find (optimal) solutions over integers

General existential formulas

Can assume formula in conjunctive normal form:

$$\bigwedge_{1 \leq i \leq n} \bigvee_{1 \leq j \leq m_i} \boldsymbol{a}_{i,j} \cdot \boldsymbol{x} \leq b_{i,j}$$

- Introduce propositional variables $P_{i,j}$ for every inequality
- Satisfying assignment to $P_{i,j}$ induces system of linear inequalities
- Give system to theory solver that propagates back conflict information if induced system is unsatisfiable

Optimal solutions

Given an optimization problem:

$$\max \boldsymbol{c} \cdot \boldsymbol{x} \text{ s.t. } \bigwedge_{1 \leq i \leq n} \bigvee_{1 \leq j \leq m_i} \boldsymbol{a}_{i,j} \cdot \boldsymbol{x} \leq b_{i,j}$$

- Find satisfying assignment $\boldsymbol{x}^*$ giving value $\boldsymbol{c} \cdot \boldsymbol{x}^*$, then add $\boldsymbol{c} \cdot \boldsymbol{x} < \boldsymbol{c} \cdot \boldsymbol{x}^*$ and repeat until unsatisfiable
- Alternatively: binary search
- Implemented in e.g. Z3 and OptiMathSAT

Quantifier elimination

- First algorithm to establish decidability
- Syntactic decision procedure working on formulas
- Complementation easy, but projection difficult
- Derives many upper bounds
- Decidability of extension with unary counting quantifier

Quantifier elimination

Given a quantifier-free conjunction of atomic formulas $\Phi(x, \boldsymbol{y})$, compute quantifier-free $\Psi(\boldsymbol{y})$ such that

$$(\exists x\, \Phi(x, \boldsymbol{y})) \leftrightarrow \Psi(\boldsymbol{y})$$

Fact
Presburger arithmetic does not have quantifier elimination:

$$\Phi(y) \equiv \exists x\, y = 2 \cdot x$$

Solution: Extend structure with predicates $\{c \mid \cdot\}_{c>1}$

Fourier-Motzkin quantifier elimination

Given a system of linear inequalities
$A \cdot \boldsymbol{y} + \boldsymbol{b} \cdot x < \boldsymbol{c}$ over the reals, eliminate x

Joseph Fourier
1768 – 1830

Step 1: Isolate x

$$\bigwedge_{i \in G} \boldsymbol{a}_i \cdot \boldsymbol{y} + c_i < b_i \cdot x \wedge \bigwedge_{j \in L} b_j \cdot x < \boldsymbol{a}_j \cdot \boldsymbol{y} + c_j$$

Step 2: Normalise x

$$\bigwedge_{i \in G} \frac{1}{b_i}(\boldsymbol{a}_i \cdot \boldsymbol{y} + c_i) < x \wedge \bigwedge_{j \in L} x < \frac{1}{b_j}(\boldsymbol{a}_j \cdot \boldsymbol{y} + c_j)$$

Step 3: Eliminate x

$$\bigwedge_{i \in G, j \in L} \frac{1}{b_i}(\boldsymbol{a}_i \cdot \boldsymbol{y} + c_i) < \frac{1}{b_j}(\boldsymbol{a}_j \cdot \boldsymbol{y} + c_j)$$

Presburger quantifier elimination

Step 1: Isolate x

$$\bigwedge_{i \in G} \boldsymbol{a}_i \cdot \boldsymbol{y} + c_i < b_i \cdot x \wedge \bigwedge_{j \in L} b_j \cdot x < \boldsymbol{a}_j \cdot \boldsymbol{y} + c_j$$

Step 2: Normalise x, where $b = \operatorname{lcm}\{b_i, b_j : i \in G \cup L\}$

$$\Psi(\vec{y}, z) \equiv \bigwedge_{i \in G} \frac{b}{b_i}(\boldsymbol{a}_i \cdot \boldsymbol{y} + c_i) < z \wedge \bigwedge_{j \in L} z < \frac{b}{b_j}(\boldsymbol{a}_j \cdot \boldsymbol{y} + c_j) \wedge b \mid z$$

Step 3: Eliminate z

$$\bigvee_{k \in G} \bigvee_{1 \le m \le b} \Psi \left[\frac{b}{b_i}(\boldsymbol{a}_k \cdot \boldsymbol{y} + c_k) + m \;/\; z \right]$$

Growth of the procedure

- Translations into DNF cause non-elementary blow-up, but blow-up in every clause manageable

- After quantifier elimination, many inequalities with same linear part, and moreover

$$\exists x \bigvee_{i \in I} \Phi_i(x, \boldsymbol{y}) \equiv \bigvee_{i \in I} \exists x \, \Phi_i(x, \boldsymbol{y})$$

- Bit-length of smallest solution of $\Phi(x)$ with a quantifier alternations and at most b variables in every quantifier block bounded by $O(|\Phi|^{(3b)^a})$

- 3-EXP decision procedure

Geometry of unary relations

- Quantifier elimination shows that quantifier-free $\Phi(x)$ is a Boolean combination of atomic formulas

$$a \cdot x > b \qquad\qquad c \mid a \cdot x + b$$

- Every atomic formula defines an ultimately periodic set: there are p, t such that for all $x > t$

$$\Phi(x) \leftrightarrow \Phi(x + p)$$

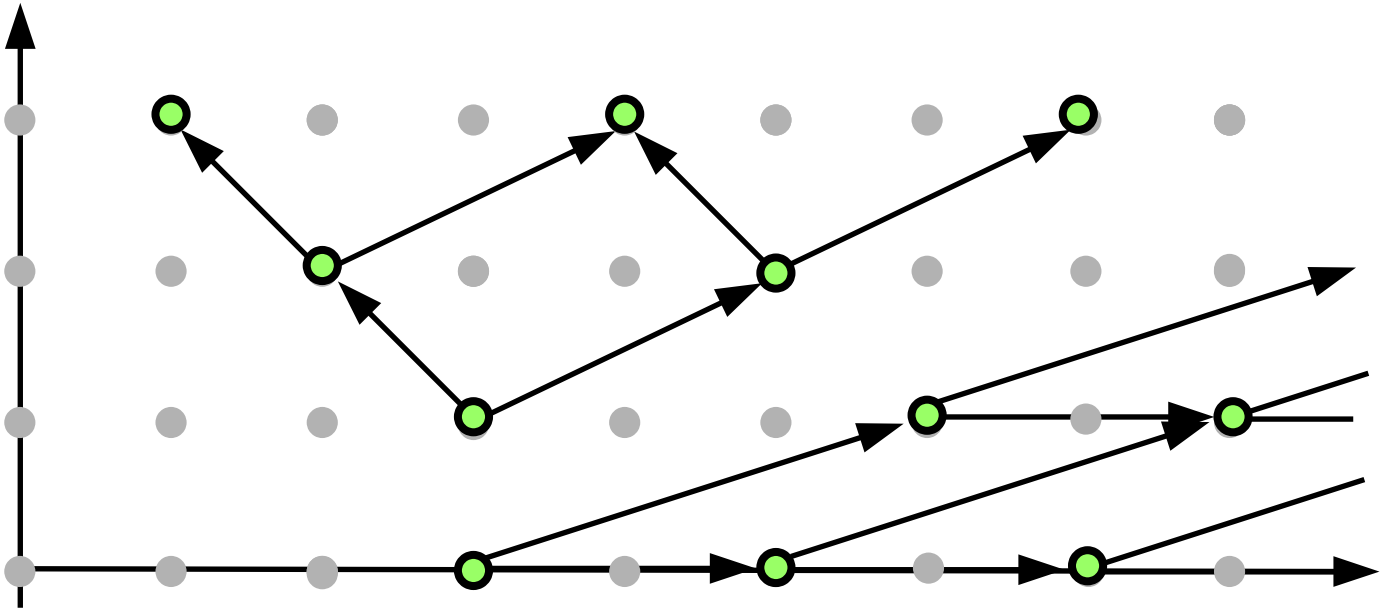
A unary counting quantifier

- Unary counting quantifier $\exists^{=x} y\, \Phi(x, y, \boldsymbol{z})$ such that there are x many different y making $\Phi(x, y, \boldsymbol{z})$ true
- Consider conjunction of atomic formulas
  $p(x, \boldsymbol{z}) < y,\ y < p(x, \boldsymbol{z}), c \mid y + p(x, \boldsymbol{z})$

Generator-based decision procedures

- Decision procedure based on semi-linear sets
- Semantic decision procedure
- Projection easy, but complementation difficult
- Decidability of extension with Kleene star

Semi-linear sets



Given $\boldsymbol{b} \in \mathbb{Z}^d, P = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n\} \subseteq \mathbb{Z}^d$, generated linear set is

$$L(\boldsymbol{b}, P) = \left\{ \boldsymbol{b} + \sum_{i=1}^{n} \lambda_i \cdot \boldsymbol{p}_i : \lambda_i \in \mathbb{N} \right\}$$

A semi-linear set is a finite union of linear sets.

Presburger sets are semi-linear

Theorem (Ginsburg and Spanier, 1964)
The sets of integers definable in Presburger arithmetic are precisely the semi-linear sets.

- Obviously a linear set $L(\boldsymbol{b}, P) \subseteq \mathbb{Z}^d$ is definable via

$$\Phi(x_1, \ldots, x_d) \equiv \exists y_1 \ldots y_n \, \boldsymbol{x} = \boldsymbol{b} + \boldsymbol{p}_1 \cdot y_1 + \cdots + \boldsymbol{p}_n \cdot y_n$$

- Converse direction obtained from showing closure properties of semi-linear sets and semi-linearity of

$$\boldsymbol{a} \cdot \boldsymbol{x} \geq c \qquad\qquad c \mid \boldsymbol{a} \cdot \boldsymbol{x} + b$$

Homogeneous systems of equations

Given $A \cdot \boldsymbol{x} = \mathbf{0}$, the solutions over $\mathbb{N}^d$ form a finitely generated monoid

Dickson's lemma (Dickson, 1913)
For any infinite sequence $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots \in \mathbb{N}^d$ there are $i < j$ such that $\boldsymbol{x}_i \leq \boldsymbol{x}_j$.

- If the minimal set P generating all solutions of $A \cdot \boldsymbol{x} = \mathbf{0}$ was infinite there would be $\boldsymbol{x} \neq \boldsymbol{y}$ in P such that $\boldsymbol{x} \leq \boldsymbol{y}$
- Hence $\boldsymbol{z} = \boldsymbol{y} - \boldsymbol{x} \geq \mathbf{0}$ and $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z}$, contradicting minimality of P

Linear inequalities and congruences

- Semi-linearity of $A \cdot \boldsymbol{x} = \mathbf{0}$ easily implies semi-linearity of $A \cdot \boldsymbol{x} = \boldsymbol{c}$ and then $A \cdot \boldsymbol{x} \geq \boldsymbol{c}$

- Linear congruences $c \mid \boldsymbol{a} \cdot \boldsymbol{x} + b$ are easily semi-linear

Intersection and projection

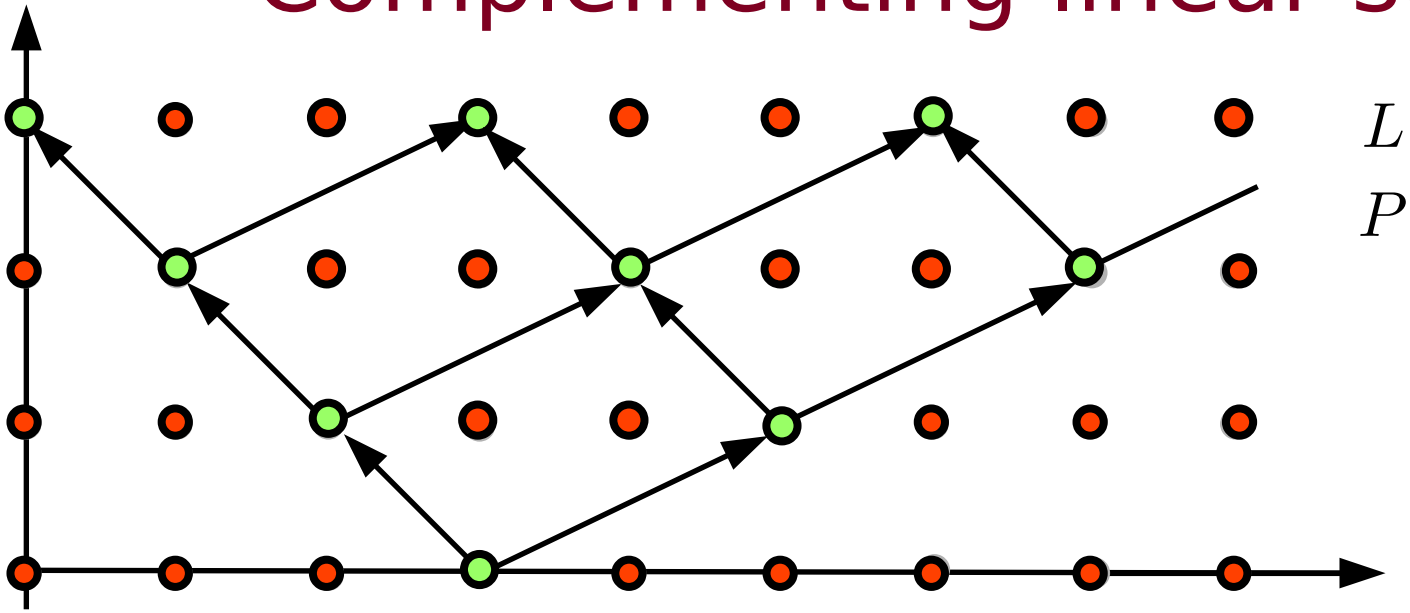
- Intersection of $L(\boldsymbol{b}, P)$ and $L(\boldsymbol{c}, Q)$ is semi-linear:

$$\boldsymbol{v} \in L(\boldsymbol{b}, P) \cap L(\boldsymbol{c}, Q) \iff \boldsymbol{v} = \boldsymbol{b} + P \cdot \boldsymbol{x} = \boldsymbol{c} + Q \cdot \boldsymbol{y}$$

$$\rightsquigarrow \begin{bmatrix} P & -Q \end{bmatrix} \cdot \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix} = \boldsymbol{c} - \boldsymbol{b}$$

- Projection of a semi-linear set is trivial

Complementing linear sets



$$L(\boldsymbol{b}, P) \subseteq \mathbb{Z}^d$$
$$P = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n\}$$

- All points lie in a polytope $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$, so each point outside satisfies $\boldsymbol{a} \cdot \boldsymbol{x} > b$ for some row of $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$

- If P has full rank, "inner complement" is $L(C, P)$ for
$$C = \boldsymbol{b} + (\{\lambda_1 \cdot \boldsymbol{p}_1 + \cdots + \lambda_n \cdot \boldsymbol{p}_n : \lambda_i \in [0, 1)\} \cap \mathbb{Z}^d) \setminus \mathbf{0}$$

Carathéodory-type theorems

Theorem (Carathéodory, 1907)
If $\boldsymbol{v} \in \mathbb{R}^d$ is in the cone generated by P then there is a linearly independent $P' \subseteq P$ whose cone contains $\boldsymbol{v}$.

If $\boldsymbol{v} \in L(\boldsymbol{b}, P)$ then

- $\boldsymbol{v} \in L(\boldsymbol{c}, P')$ for linearly independent $P' \subseteq P$ and $\log ||\boldsymbol{c}||$ polynomial in $\log ||P||$
- $\boldsymbol{v} \in L(\boldsymbol{b}, P')$ for $P' \subseteq P$ and $\#P' \leq 2d \log(4d||P||)$

A decision procedure

- Given $\Psi \equiv \forall \boldsymbol{x}_1 \exists \boldsymbol{x}_2 \cdots \exists \boldsymbol{x}_k \, \Phi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k)$, to decide Ψ compute semi-linear representation of $\Phi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k)$ and then repeatedly project and complement

- Runs in non-elementary time, though gives strong upper bounds for one quantifier alternation

Kleene stars

The semi-linear set approach yields a straight-forward decision procedure for an extension with a Kleene star:

- Given $M \subseteq \mathbb{Z}^d$, let $M^* = \{\boldsymbol{v}_1 + \boldsymbol{v}_2 + \cdots + \boldsymbol{v}_m : \boldsymbol{v}_i \in M\}$
- For $M = \bigcup_{j \in J} L(\boldsymbol{c}_j, Q_j)$, have $M^* = \bigcup_{K \subseteq J} L(\boldsymbol{b}_K, P_K)$ with

$$\boldsymbol{b}_K = \sum_{k \in K} \boldsymbol{c}_k \qquad P_K = \bigcup_{k \in K} \{\boldsymbol{c}_k\} \cup \bigcup_{k \in K} Q_k$$

Automata-based decision procedures

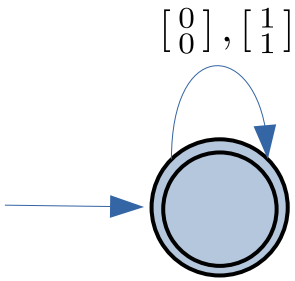
- Decision procedure based on finite-state automata
- Language-theoretic decision procedure
- Both projection and complementation easy
- Decidability of Büchi arithmetic

Automata-based decision procedure

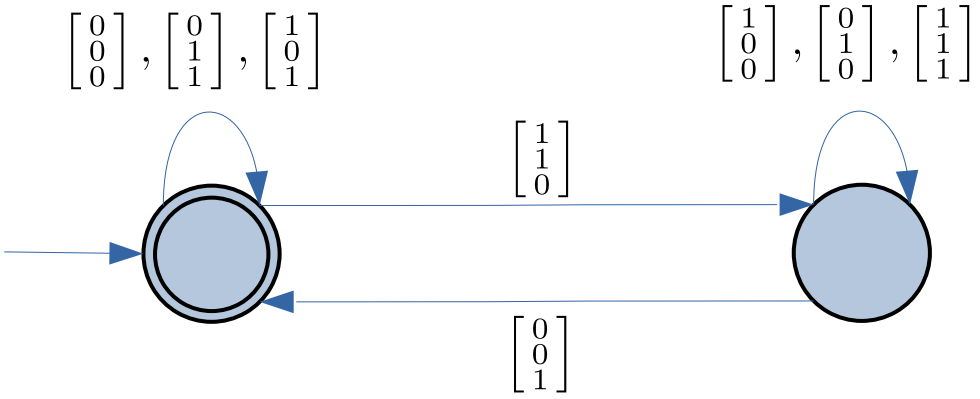
Represent $\boldsymbol{x} \in \mathbb{N}^d$ as strings over the alphabet

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

Gadget for $x = y$:



Gadget for $x + y = z$:



Automata-based decision procedure

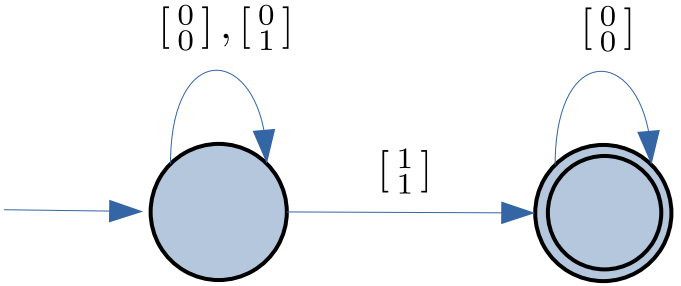
- Closure of regular languages under union, intersection, complement, homomorphism and inverse homomorphism yields decision procedure
- A priori non-elementary growth can be controlled to give 3-EXP decision procedure

Büchi arithmetic

First-order theory of $\langle \mathbb{N}, 0, 1, +, V_p, = \rangle$ for fixed $p > 1$:

$V_p(x, y) \Leftrightarrow$ x is the largest power of p dividing y without remainder

Gadget for $V_2(x, y)$:



Theorem
Büchi arithmetic is TOWER-complete.

Definability in Büchi arithmetic

"x is a power of p": $P_p(x) := V_p(x, x)$

"p generates a multiplicative subgroup modulo q ":

$$\Phi(x) \equiv x > 1 \wedge P_p(x) \wedge x \equiv 1 \bmod q$$

Theorem (Cobham-Semenov)
If $M \subseteq \mathbb{N}^d$ is definable in Büchi arithmetic of two multiplicatively independent bases then M is definable in Presburger arithmetic.

p-universality

Is a formula of Büchi arithmetic satisfiable in all bases?

Theorem (H., Mansutti)
For existential Büchi arithmetic, p-universality is decidable in co-NEXP.

Given $A \cdot \boldsymbol{x} = \boldsymbol{c}$, $A \in \mathbb{Z}^{m \times d}$ a DFA generating all solutions is $M = (Q, \Sigma, \delta, q_0, F)$ with

- $Q = \mathbb{Z}^m$
- $\Sigma = \{0, \ldots, p-1\}^d$
- $\delta = (\boldsymbol{q}, \boldsymbol{v}) \mapsto p \cdot \boldsymbol{q} + A \cdot \boldsymbol{v}$
- $q_0 = \mathbf{0}$ and $F = \{\boldsymbol{c}\}$

p-automata

For $A \cdot \boldsymbol{x} = \boldsymbol{c}$, only states $\boldsymbol{q}$ with $||\boldsymbol{q}|| \leq ||A||, ||\boldsymbol{c}||$ are live in any p-automaton, i.e., independent of p

- Recall $\delta = (\boldsymbol{q}, \boldsymbol{v}) \mapsto p \cdot \boldsymbol{q} + A \cdot \boldsymbol{v}$, so

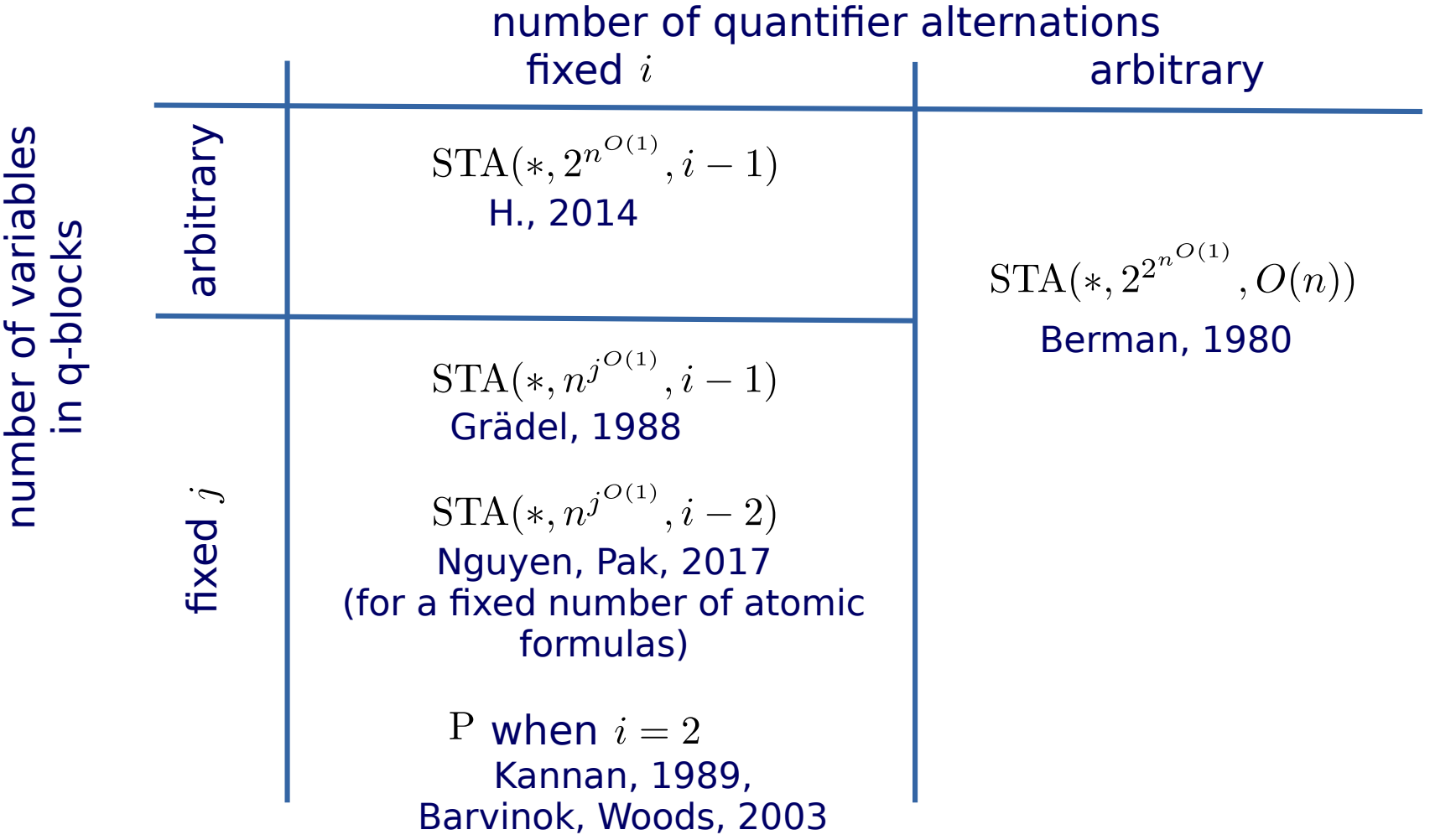
$$\boldsymbol{q} \to \boldsymbol{r} \iff \boldsymbol{r} = p \cdot \boldsymbol{q} + A \cdot \boldsymbol{x}, ||\boldsymbol{x}|| < p$$

- Yields ultimately periodic presentation of all bases in which a transition is present:

$$\Phi(y) \equiv \exists \boldsymbol{x}\, \boldsymbol{r} = y \cdot \boldsymbol{q} + A \cdot \boldsymbol{x} \wedge ||\boldsymbol{x}|| < y$$

- Can also be used to show NP upper bound for existential Büchi arithmetic

Complexity of Presburger arithmetic



Linear arithmetic theories: Theory and applications

Part III: Lower bounds

Christoph Haase
University of Oxford, UK

VTSA, 15 October 2021

Constructing large numbers

- Constructing 2^n:

$$\Phi_0(x) \equiv x = 1 \qquad \Phi_{n+1}(x) \equiv \exists y\, \Phi_n(y) \wedge x = y + y$$

- An n-bit number x divides y:

$$\Psi_n(x, y) \equiv \exists x_1\, y_1 \cdots x_n\, y_n\, \exists k$$
$$\bigwedge_{1 \le i \le n} ((x_i = 0 \wedge y_i = 0) \vee (x_i = 1 \wedge y_i = k)) \wedge$$
$$x = \sum_{1 \le i \le n} 2^{i-1} \cdot x_i \wedge y = \sum_{1 \le i \le n} 2^{i-1} \cdot y_i$$

- The number y is divided by all n-bit numbers, so $y \ge \mathrm{lcm}\{1, \ldots, 2^n\} \ge 2^{2^n}$:

$$\Theta(y) \equiv \forall x\, 1 \le x < 2^n \to \Psi_n(x, y)$$

Constructing large numbers

- Fischer-Rabin trick for $x = 2^{2^n} \cdot z$:

$$\Phi_0(x, z) \equiv z + z$$

$$\begin{aligned}\Phi_{n+1}(x, z) &\equiv \exists y\, \Phi_n(x, y) \wedge \Phi_n(y, z) \\ &\equiv \exists y\, \forall u\, \forall v\, ((u = x \wedge v = y) \vee (u = y \wedge v = z)) \\ &\qquad \rightarrow \Phi_n(u, v)\end{aligned}$$

- Constructing 2^{2^n} using the Kleene star:

$$\Psi_1(x) \equiv x = 2$$

$$\begin{aligned}\Psi_{n+1}(x) \equiv \exists x'\, y\, y'\, z\, \Big(&\Psi_n(x') \wedge y + z = 1 \wedge y' + x = x' \wedge \\ &y = 1 \rightarrow y' = x' \wedge z = 1 \rightarrow x = x'\Big)^* \wedge \\ &y = 1 \wedge z = y'\end{aligned}$$

Exceptions to the rule

- Existential Büchi arithmetic NP-complete despite:

$$\Phi_q(x) \equiv x > 1 \wedge P_2(x) \wedge x \equiv 1 \bmod q$$

- Existential Presburger arithmetic with divisibility:

$$\Phi(x_n) \equiv \exists x_1 \cdots x_{n-1}\, x_1 = 2 \wedge \bigwedge_{1 \leq i \leq n} x_i \mid x_{i+1} \wedge x_i + 1 \mid x_{i+1}$$

Gödel encodings

- Given co-prime $n_1, \ldots, n_k \in \mathbb{N}$, the Chinese remainder theorem gives an ismorphism:

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \quad \simeq \quad \mathbb{Z}/n_1 \cdots n_k\mathbb{Z}$$

- By prime number theorem $\pi(n) \sim n/\log n$, so $n_i = p_i$ good choice, but may require to compute i-th prime

Theorem (Ingham, 1940)
For sufficiently large i, there is a prime in $[i^3, (i+1)^3)$.

Diophantine gluing

Recall SubsetSum problem:
Given $S = \{s_1, \ldots, s_n\},\ t \in \mathbb{N}$, find $S' \subseteq S$ such that $\sum_{s \in S'} s = t$

Suppose we forgot SubsetSum is NP-hard, attempt reduction from 1-in-3-SAT:

$$\Phi(x_1, \ldots, x_m) = \bigwedge_{1 \le i \le k} \ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3}$$

$$\begin{array}{lll} x_1 + \overline{x_1} = 1 & h(\ell_{1,1}) + h(\ell_{1,2}) + h(\ell_{1,3}) = 1 & h(x_i) = x_i \\ & & h(\neg x_i) = \overline{x_i} \\ \vdots & \vdots & \\ x_n + \overline{x_n} = 1 & h(\ell_{k,1}) + h(\ell_{k,2}) + h(\ell_{k,3}) = 1 & \end{array}$$

Diophantine gluing

Theorem (Glover, Woolsey, 1972)
Given Diophantine equations $\boldsymbol{c} \cdot \boldsymbol{x} = a$, $\boldsymbol{d} \cdot \boldsymbol{x} = b$ with $\boldsymbol{c}, \boldsymbol{d} \in \mathbb{N}^d$, $a, b > 0$, there are polynomial-time computable $\alpha, \beta \in \mathbb{N}$ s.t. $(\alpha \boldsymbol{c} + \beta \boldsymbol{d}) \cdot \boldsymbol{x} = \alpha a + \beta b$ has the solution set.

- Used to show Π_2^{P}-lower bound for linear set inclusion in dimension one
- Can be further generalised to show Π_2^{P}-lower bound for universality of semi-linear sets in dimension one

Short Presburger arithmetic

Frobenius problem:
Given co-prime $a_1, \ldots, a_n \in \mathbb{N}$, is the largest $c \in \mathbb{N}$ not representable as their linear combination at least k ?

$$\exists c \, \forall x \, y_1 \ldots y_n \, x = a_1 \cdot y_1 + \cdots + a_n \cdot y_n \to x \neq c \, \wedge \, c \geq k$$

- For fixed n, Frobenius number computable in polynomial time [Kannan, 1992]
- The $\exists\forall$-fragment of short Presburger arithmetic is in P [Kannan, 1989; Barvinok, Woods, 2003]
- Assuming Kannan's partition theorem, short Presburger arithmetic is in P [Nguyen, Pak, 2017]

Short Presburger arithmetic

Theorem (Nguyen, Pak, 2017)
The $\exists\forall\exists$-fragment of short Presburger arithmetic is NP-complete, even in the presence of at most 10 inequalities and 5 variables.

- Reduction from AP-Cover: cover an interval with a finite union of arithmetic progressions
- Encode AP-Cover instance into convergents of a rational number $p/q = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$
- Use PA formula to check validity of AP-Cover instance

Linear arithmetic theories: Theory and applications

Part IV: Advanced Topics

Christoph Haase
University of Oxford, UK

VTSA, 15 October 2021

Presburger arithmetic with divisibility

Presburger arithmetic with divisibility

First-order theory of $(\mathbb{N}, +, 0, 1, |, =)$:

- Undecidable first-order theory:

$$\mathrm{lcm}(x, y, z) \equiv \forall t \ (y \mid t \vee z \mid t) \leftrightarrow x \mid t$$

- So $x^2 = \mathrm{lcm}(x, x+1) - 2x - 1$ and $2xy = (x+y)^2 - x^2 - y^2$

Julia Robinson
1919 – 1985

Theorem (Bel'tyukov 1976; Lipshitz, 1978; Lechner, Ouaknine, Worrell 2015)
The existential theory of Presburger arithmetic with divisibility is decidable in NEXP, and NP-complete in fixed dimension.

Local-to-global principle

Theorem (Hasse-Minkowski)
A quadratic form has a root in the rationals if and only if it has a root in the reals and the p-adic numbers for all primes p.

Every polynomial $f(x_1, \ldots, x_n)$ has a root modulo all m iff it has a solution modulo all prime powers p^k.

Proof
Let $m = p_1^{t_1} \cdots p_r^{t_r}$, have $f(x_1^{(i)}, \ldots, x_n^{(i)}) \equiv 0 \bmod p_i^{t_i}$. By the Chinese remainder theorem, there are $x_1^*, \ldots, x_n^* \in \mathbb{N}$ such that $x_j^* \equiv x_j^{(i)} \bmod p_i^{t_i}$. Thus $f(x_1^*, \ldots, x_n^*) \equiv 0 \bmod p_i^{t_i}$ and so $f(x_1^*, \ldots, x_n^*) \equiv 0 \bmod m$.

Presburger arithmetic with divisibility

Existential Presburger arithmetic fails the "Chinese remainder local-to-global principle":

$x+2 \mid x+1 \iff k \cdot (x+2) = x+1$ has no solution in $\mathbb{N}$, but has a solution modulo all p^t with $x+2 \not\equiv 0 \bmod p^t$

Consider $a_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n \mid b_0 + b_1 \cdot x_1 + \cdots + b_n \cdot x_n$ and assume $a_i, b_i > 0$ and $x_1 < x_2 < \cdots < x_n$, then

$$(\sum_{i=1}^{n} b_i \cdot x_i + b_0)/(\sum_{i=1}^{n} a_i \cdot x_i + a_0) \leq \sum_{i=1}^{m} b_i + d$$

Can thus assume "increasing normal form":

$$(a_0 + \sum_{i=1}^{k} a_i \cdot x_i) \mid (b_0 + \sum_{i=1}^{k} b_i \cdot x_i + \sum_{i=k+1}^{n} b_i \cdot x_i)$$

Presburger arithmetic with divisibility

Theorem (Lipshitz 1978)
A formula in increasing normal form is satisfiable iff it is satisfiable in the p-adic integers for all primes p.

- Restricted fragments allow for quantification; here each f_i positive and Φ_i quantifier-free PA formula:

$$\forall \boldsymbol{x}\, \exists \boldsymbol{y} \bigvee \bigwedge (f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x}, \boldsymbol{y})) \wedge \Phi_i(\boldsymbol{x})$$

- Decidability of $\sum_{i,j=1}^{n} a_{i,j} \cdot x_i x_j + \sum_{j=1}^{n} b_j \cdot x_j + c = 0 \wedge \Phi(\boldsymbol{x})$

Counting solutions of Presburger formulas

Rational generating functions

For $S \subseteq \mathbb{N}^d$, associate the generating function

$$f(S, \boldsymbol{x}) = \sum_{(s_1,\ldots,s_d)\in S} x_1^{s_1} \cdots x_d^{s_d}$$

Example

For $S = \{3, 5, 7 \ldots\}$, have $f(S, x) = x^3 + x^5 + \cdots = \dfrac{x^3}{1 - x^2}$.

Rational generating function:

$$f(S, \boldsymbol{x}) = \frac{q(\boldsymbol{x})}{(1 - \boldsymbol{x}^{\boldsymbol{b}_1}) \cdots (1 - \boldsymbol{x}^{\boldsymbol{b}_k})}$$

Theorem (Woods 2015)

A set $S \subseteq \mathbb{N}^d$ is Presburger-definable if and only if its associated generating function is rational.

Parametric counting problems

Given $\Phi(\boldsymbol{x};\boldsymbol{y})$, associate the counting function

$$\#\Phi(\boldsymbol{y}) = \#\{\boldsymbol{x} \in \mathbb{N}^d : \Phi(\boldsymbol{x};\boldsymbol{y}) \text{ is true}\}$$

Example

For $\Phi(x,y,p) \equiv 2x + 2y \leq p$, we have

$$\#\Phi(p) = \frac{1}{2}\left(\left\lfloor\frac{p}{2}\right\rfloor + 1\right)\cdot\left(\left\lfloor\frac{p}{2}\right\rfloor + 2\right)$$

$$= \begin{cases} \frac{1}{8}p^2 + \frac{3}{4}p + 1 & \text{if } p \text{ is odd} \\ \frac{1}{8}p^2 + \frac{1}{2}p + \frac{3}{8} & \text{if } p \text{ is odd} \end{cases}$$

Parametric counting problems

Theorem (Woods 2015)
The counting function $\#\Phi(\boldsymbol{y})$ associated to $\Phi(\boldsymbol{x};\boldsymbol{y})$ is a piecewise quasi-polynomial.

A quasi-polynomial is a function $f\colon \mathbb{N}^d \to \mathbb{Q}$ such that there is a d-dimensional lattice $\Lambda \subseteq \mathbb{Z}^d$ and polynomials $p_{\boldsymbol{\lambda}}\colon \mathbb{N}^d \to \mathbb{Q}$ for every $\boldsymbol{\lambda} \in \mathbb{Z}^n/\Lambda$ such that

$$f(\boldsymbol{y}) = p_{\boldsymbol{\lambda}}(\boldsymbol{y}) \text{ when } \boldsymbol{y} \in \boldsymbol{\lambda}$$

A piecewise quasi-polynomial is a function $f\colon \mathbb{N}^d \to \mathbb{Q}$ s.t. there is a partition $\mathbb{N}^d = \bigcup_{i\in I}(P_i \cap \mathbb{N}^d)$ and for $i \in I$ a quasi-polynomial f_i s.t.

$$f(\boldsymbol{y}) = f_i(\boldsymbol{y}) \text{ when } \boldsymbol{y} \in P_i$$

Applications

Theorem (H., Różycki, 2021)
Existential Büchi arithmetic is not expressively complete.

In compiler optimisation:

```
for i:=0 to N do:
    for j:=0 to M do:
        f()
```

Number of times `f()` is called can be rephrased as a parametric counting problem