Logics and automata on integer and real numbers, with applications in computer-aided verification

Véronique Bruyère

University of Mons - Belgium

8 September 2009

Table of contents

Presburger's arithmetic and its extensions

Presburger's arithmetic

Definition

Presburger's arithmetic

- Structure $\langle \mathbb{N}, =, + \rangle$
- First-order formulae - variables $x, y, z, \dots$ over $\mathbb{N}$
  equality $=$, addition $+$
  connectives $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$
  quantifiers $\exists, \forall$
- Sentences - first-order formulae with each variable under the scope of a quantifier
- $X \subseteq \mathbb{N}^m$ is Presburger-definable if it is definable by a first-order formula $\varphi(x_1, x_2, \dots, x_m)$ of $\langle \mathbb{N}, =, + \rangle$.

Presburger's arithmetic

Structure $\langle \mathbb{N}, =, + \rangle$

Example

- $X = \{x \mid x \text{ is an odd number greater than or equal to } 2\}$
  $\varphi(x) \quad (\exists y)(x = y + y + 1) \wedge (x \geq 2)$
- $X \subseteq \mathbb{N}^2$

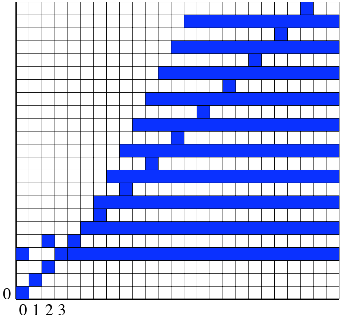
$$
\begin{array}{lcl}
\varphi(x, y) & & (x = 0 \wedge y = 3) \\
 & \vee & (x = 2 \wedge y = 4) \\
 & \vee & (x = y) \\
 & \vee & (\exists z)(\exists t)(x = z + t + 4) \wedge (y = t + t + 3)
\end{array}
$$

Under the hypothesis that $\geq$ and the constants are first-order definable ...

Presburger's arithmetic

$\color{red}{\varphi(x,y)}$

$$
\begin{array}{ll}
 & (x = 0 \wedge y = 3) \\
\vee & (x = 2 \wedge y = 4) \\
\vee & (x = y) \\
\vee & (\exists z)(\exists t)(x = z + t + 4) \wedge (y = t + t + 3)
\end{array}
$$



Intuition for the cone : $(x, y) = z(1,0) + t(1,2) + (4,3)$

Presburger's arithmetic

Proposition

Any arithmetic progression is Presburger-definable

Proof

$x \leq y$	stands for	$(\exists z)\ (x + z = y)$	
$x = 0$		$(\forall y)\ (x \leq y)$	
$x = 1$		$\neg(x = 0) \wedge (\forall y)\ (\neg y = 0) \rightarrow (x \leq y)$	
$x = c$		$(\exists z)\ (z = 1) \wedge (x = z + \cdots + z)$	(c times)
$x = a \cdot y$		$(\exists y)\ (x = y + \cdots + y)$	(a times)

Hence $X = a \cdot \mathbb{N} + c$ is Presburger-definable by the formula

$$\varphi(x) = (\exists y)(\exists z)(\exists t)\ (x = z + t) \wedge (z = a \cdot y) \wedge (t = c).$$

Decidable structures

Definition

The theory of a structure S is decidable is there exists an algorithm which decides whether any sentence of S is true or false.

$$\begin{tikzcd}
 & \text{sentence } \varphi \arrow[d] & \\
 & \boxed{\text{algorithm}} \arrow[dl] \arrow[dr] & \\
\text{true} & & \text{false}
\end{tikzcd}$$

Theorem (Presburger 1929)

The theory of Presburger's arithmetic is decidable

Theorem (Tarski 1936)

The theory of $\langle \mathbb{N}, =, +, \cdot \rangle$ *is not decidable*

Decidable structures

Theorem (Stronger result in [Presburger 1929])

Presburger's arithmetic has an effective quantifier elimination

$$\text{formula } \varphi(x_1, \ldots, x_m)$$
$$\downarrow$$
$$\boxed{\text{algorithm}}$$
$$\downarrow$$
$$\text{equivalent formula } \psi(x_1, \ldots, x_m) \text{ without quantifiers in}$$
$$\langle \mathbb{N}, =, +, \leq, 0, 1, (\mathrm{mod}\, n)_{n\in\mathbb{N}} \rangle$$

Corollary

The theory of Presburger's arithmetic is decidable

Corollary

$X \subseteq \mathbb{N}$ is Presburger-definable iff X is a finite union of constants and arithmetic progressions

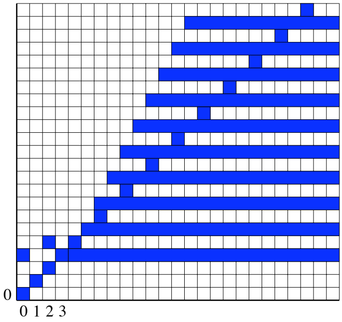
Decidable structures

Example (continued)

- $X = \{x \mid x \text{ is an odd number greater than or equal to } 2\}$
  $\varphi(x)$ $\quad (\exists y)(x = y + y + 1) \wedge (x \geq 2)$
  $\psi(x)$ $\quad (x = 1 \bmod 2) \wedge (x \geq 1 + 1)$

- $\psi(x, y)$

$$
\begin{array}{ll}
 & (x = 0 \wedge y = 3) \\
\vee & (x = 2 \wedge y = 4) \\
\vee & (x = y) \\
\vee & (y \geq 3) \wedge (y + 5 \leq x + x) \\
 & \wedge (y = 1 \bmod 2)
\end{array}
$$



Decidable structures

Corollary

$X \subseteq \mathbb{N}$ is Presburger-definable
iff X is a finite union of constants and arithmetic progressions
iff X is ultimately periodic

Definition

X is ultimately periodic if

$$(\exists l \geq 0)(\exists p \geq 1)(\forall n \geq l)\ (n \in X \Leftrightarrow n + p \in X)$$

Example (continued)

$X = \{x \mid x \text{ is an odd number greater than or equal to } 2\}$ is ultimately periodic with $l = 3$ and $p = 2$

Remark - Several characterizations for Presburger-definable sets $X \subseteq \mathbb{N}^m$ also exist.

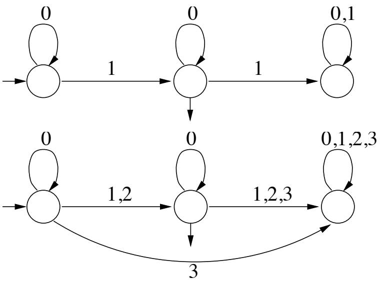
Automata

Definition

Given a base $r \geq 2$, a set $X \subseteq \mathbb{N}^m$ is called *r*-recognizable if X written in base r is recognized by a finite automaton

Example

$X = \{2^n \mid n \geq 0\}$ is 2-recognizable and 4-recognizable



base 2

base 4

Remark - All possible leading 0's are considered

Automata

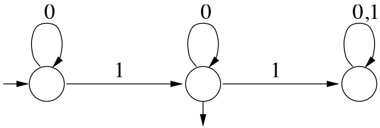
Definition

Automaton $\mathcal{A} = (Q, I, F, T, A)$ with

- a finite set Q of states
- a set $I \subseteq Q$ of initial states
- a set $F \subseteq Q$ of final states
- a set of transitions $T \subseteq Q \times A \times Q$ labeled by a letter of a finite alphabet A

The automaton $\mathcal{A}$ recognizes (or accepts) the set of words, i.e. sequences of letters, which are labels of paths from an initial state to a final state

Example

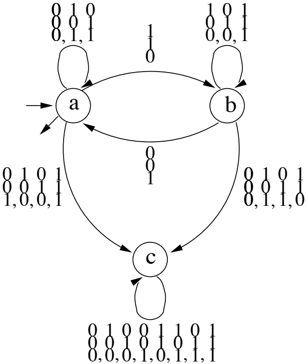


Automata

Example

$X = \{(x,y,z) \mid x+y=z\}$ is 2-recognizable and 10-recognizable

state a :	no carry
state b :	carry
state c :	error



Remark - $\begin{pmatrix}3\\9\end{pmatrix}$ is written as $\begin{pmatrix}0011\\1001\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}$ in base 2.

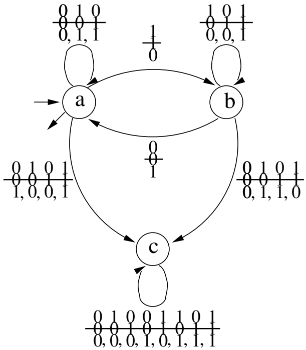
Automata

Example

$X = \{(x, z) \mid x \leq z\}$ is 2-recognizable and 10-recognizable

Recall that $x \leq z$ is first-order definable by $(\exists y)\ (x + y = z)$

Take the automaton for $\{(x, y, z) \mid x + y = z\}$ and erase the second component of the letters



Automata

Theorem

The theory of Presburger's arithmetic is decidable

Proof (Hodgson 83)

- Show that any Presburger-definable set $X \subseteq \mathbb{N}^m$ is 2-recognizable, by induction on the formulae.
  - Atomic formulae : The sets $\{(x, y) \mid x = y\}$ and $\{(x, y, z) \mid x + y = z\}$ are 2-recognizable.
  - Connectives $\vee$, $\neg$: The class of 2-recognizable sets is closed under boolean operations.
  - Quantifier $\exists$: Erase the related component of the alphabet.
- Given a sentence φ, the related automaton $\mathcal{A}$ has no letter on its transitions. This sentence is true iff there is a path in $\mathcal{A}$ from an initial state to a final state.
- Each step is effective.

Additional results

Example

$X = \{2^n \mid n \geq 0\}$ is 2-recognizable, but not Presburger-definable (Recall the structure of Presburger-definable sets $X \subseteq \mathbb{N}$)

Theorem (Büchi 60)

Let $r \geq 2$ be a base. A set $X \subseteq \mathbb{N}^m$ is r-recognizable iff X is definable by a first-order formula $\varphi(x_1, \ldots, x_m)$ of $\langle \mathbb{N}, =, +, V_r \rangle$.

Definition

$V_r(x) = y$ means that y is the greatest power of r dividing x.

$V_2(20) = 4$	20	1	0	1	0	0
	4			1	0	0

Example

$X = \{2^n \mid n \geq 0\}$ is first-order definable by the formula $V_2(x) = x$

Additional results

Theorem (Büchi 60)

Let $r \geq 2$ be a base. A set $X \subseteq \mathbb{N}^m$ is r-recognizable iff X is definable by a first-order formula $\varphi(x_1, \ldots, x_m)$ of $\langle \mathbb{N}, =, +, V_r \rangle$.

Proof

$\boxed{\Leftarrow}$ (Hodgson 83) Same approach as for Presburger's arithmetic, with an automaton in base r for the atomic formula $V_r(x) = y$.

Corollary

The theory of $\langle \mathbb{N}, =, +, V_r \rangle$ is decidable

Corollary

Any Presburger-definable set is r-recognizable, for each base $r \geq 2$

Corollary (Several references)

There exists an algorithm which tests whether a r-recognizable set $X \subseteq \mathbb{N}^m$ is Presburger-definable or not.

Additional results

Corollary

There exists an algorithm which tests whether a r-recognizable set $X \subseteq \mathbb{N}^m$ is Presburger-definable or not.

Proof ($m = 1$)

Let $X \subseteq \mathbb{N}$ be a r-recognizable set.
Then X is definable by a first-order formula $\varphi(x)$ of $\langle \mathbb{N}, =, +, V_r \rangle$.
The set X is ultimately periodic
iff

$$(\exists l \geq 0)(\exists p \geq 1)(\forall n \geq l)\ (n \in X \Leftrightarrow n + p \in X)$$

iff the following sentence of Presburger's arithmetic is true

$$(\exists l \geq 0)(\exists p \geq 1)(\forall n \geq l)\ (\varphi(n) \leftrightarrow \varphi(n + p)).$$

Recall that the theory of $\langle \mathbb{N}, =, +, V_r \rangle$ is decidable.

Dependence on the base

Example (continued)

$X = \{2^n \mid n \geq 0\}$ is 2-recognizable and 4-recognizable
Is it 3-recognizable ? (1, 2, 11, 22, 121, 1012, 2101, . . .)

Theorem (Cobham 1969)

If a set $X \subseteq \mathbb{N}$ is r-recognizable for every base $r \geq 2$, then X is ultimately periodic.
More precisely, it suffices that X is r- and s-recognizable, with r, s being two multiplicatively independent bases.

- Two bases $r, s \geq 2$ are multiplicatively dependent if $r^k = s^l$ for some $k, l \in \mathbb{N} \setminus \{0\}$.

Example (continued)

Bases $2, 4$ are multiplicatively dependent. Bases $2, 3$ are not.
$X = \{2^n \mid n \geq 0\}$ is exactly 2^k-recognizable for every $k \geq 1$.

Dependence on the base

Cobham's theorem : one of the jewels in the theory of formal languages

Simpler proofs and numerous generalizations
(see my survey "On Cobham's theorem", 2001,
`http ://staff.umh.ac.be/Bruyere.Veronique/slides.html`)

- Dimension 1 (Cobham 1969, Hansel 1982, Michaux-Villemaire 1993, Durand 2008)
- Higher dimensions (Semenov 1977, Muchnik 1991, Michaux-Villemaire 1996, Durand 2008)
- Non classical bases (Fabre 1994, Point-Bruyère 1997, Fagnot 1998, Hansel 1998, Bès 2000)
- Equality of factors (Fagnot 1997)
- θ-substitutions (Durand 1998, Durand 2001)
- Substitution tiling systems (Holton-Radin-Sadun 2005)
- Regular sequences (Bell 2006)

Extension to the integers

Summary (See (Bruyère-Hansel-Michaux-Villemaire 1994))

- *The theory of Presburger's arithmetic and the theory of* $\langle \mathbb{N}, =, +, V_r \rangle$ *are decidable*
- *A set* $X \subseteq \mathbb{N}^m$ *is* r*-recognizable iff* X *is definable by a first-order formula* $\varphi(x_1, \ldots, x_m)$ *of* $\langle \mathbb{N}, =, +, V_r \rangle$
- *Characterizations of Presburger-definable sets* $X \subseteq \mathbb{N}$
- *Cobham's theorem*

Extension to the integers

- Structures $\langle \mathbb{Z}, =, + \rangle$ and $\langle \mathbb{Z}, =, +, V_r \rangle$
- Automata for integers : in base r, a positive (resp. negative) number always begins with 0 (resp. $r - 1$).

Example

In base 2, $-6 = -8 + 2$ is written as 1010, and 10 as 01010

Extension to the integer and real numbers

Definition

Arithmetic of the integer and real numbers

- Structure $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$
- First-order formulae -
  Variables $x, y, z, \ldots$ over $\mathbb{R}$
  Predicate $\mathbb{Z}(x)$ means that x is an integer variable
- Subsets X of $\mathbb{R}^m$ definable by a first-order formula $\varphi(x_1, x_2, \ldots, x_m)$ of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$

Example

$X = \left\{ 2n + \left]0, \frac{4}{3}\right[\;\middle|\; n \in \mathbb{Z} \right\}$ is definable by the formula $\varphi(x)$:

$$\exists y \exists z : \quad \mathbb{Z}(y) \wedge (x = y + y + z) \wedge (0 < z < \frac{4}{3})$$

Exercise - Any rational constant is first-order definable.

Extension to the integer and real numbers

Theorem (Weispfenning 1999)

$\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ *has an effective quantifier elimination.*

Corollary

The theory of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ *is decidable.*

Corollary

$X \subseteq \mathbb{R}$ *is first-order definable in* $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ *iff* X *is ultimately periodically simple.*

- X is a finite union of sets of the form $Y_i + Z_i$ where
- each Y_i is either an integer constant, or an arithmetic progression, or its opposite
- each Z_i is an interval of $[0, 1[$ for rational endpoints

Example

$X = \left\{ 2n + \left]0, \frac{4}{3}\right[\;\middle|\; n \in \mathbb{Z} \right\}$ is ultimately periodically simple

Extension to the integer and real numbers

Definition

Given a base $r \geq 0$, real numbers are positionally encoded as infinite words over $\{0, 1, \ldots, r-1, \star\}$

Example

3.5 is encoded in base 2 as $011 \star 10^\omega$ or $011 \star 01^\omega$

Remark

- positive (resp. negative) numbers begin with 0 (resp. $r - 1$)
- some numbers have dual writings
- integer numbers correspond to infinite words $u \star 0^\omega$ and $u \star (r-1)^\omega$
- rational numbers correspond to infinite words $u \star vw^\omega$

Extension to the integer and real numbers

Definition

Given a base $r \geq 2$, a set $X \subseteq \mathbb{R}^m$ is r-recognizable if X written in base r is recognized by a Büchi automaton.

Definition

A Büchi automaton is an automaton $\mathcal{A} = (Q, I, F, T, A)$ as before, with an adapted acceptance condition :
It recognizes (or accepts) the set of infinite words which are labels of paths from an initial state and going through a final state infinitely many times

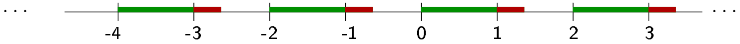
Example

$X = \{2^n \mid n \in \mathbb{Z}\}$ is 2-recognizable

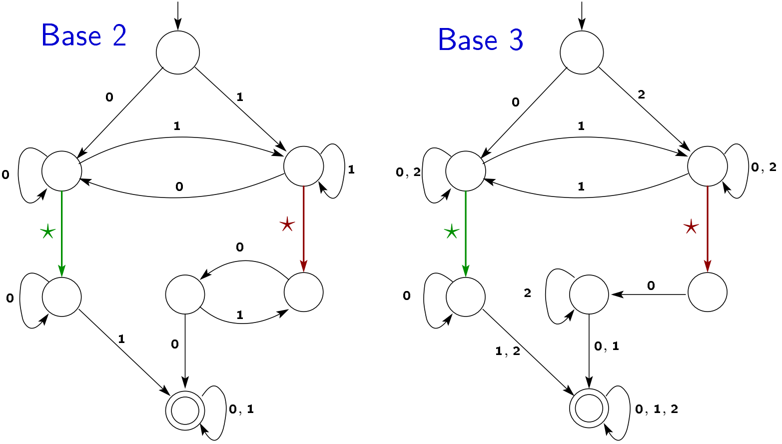
Exercise - Construct a Büchi automaton recognizing all encodings of X in base 2

Extension to the integer and real numbers

Example



$$\left\{ 2n + \left]0, \tfrac{4}{3}\right[\;\middle|\; n \in \mathbb{Z} \right\}$$



Extension to the integer and real numbers

Theorem (Boigelot-Rassart-Wolper 1998)

$X \subseteq \mathbb{R}^m$ is r-recognizable iff X is first-order definable in $\langle \mathbb{R}, =, +, \leq, \mathbb{Z}, V_r \rangle$.

- $V_r(x) = y$ means y is the greatest power of r dividing x as follows : $x = ky$ with $k \in \mathbb{Z}$

Example

$X = \{2^n \mid n \in \mathbb{Z}\}$ is definable by the formula $\varphi(x) : V_2(x) = x$

Proof

Same approach as for $\langle \mathbb{N}, =, +, V_r \rangle$ (Hodgson 83)

Corollary

The theory of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z}, V_r \rangle$ is decidable

Extension to the integer and real numbers

Corollary

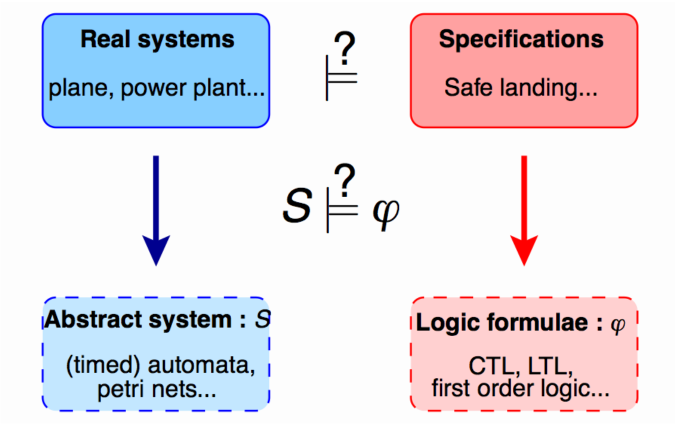
Any set $X \subseteq \mathbb{R}^m$ that is first-order definable in $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ is r-recognizable, for each base $r \geq 2$

Recent research works by S. Jodogne, J. Leroux, B. Boigelot, J. Brusten, V. Bruyère, P. Wolper, ...

- For sets $X \subseteq \mathbb{R}^m$ definable in $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$, weak Büchi automata are sufficient and are more efficient
- Generalization of Cobham's theorem in one and several dimensions

Some applications in computer-aided verification

Model-checking



In 2007, Turing award given to E. M. Clarke, E. A. Emerson and J. Sifakis for their roles "*in developing Model-Checking into a highly effective verification technology, widely adopted in the hardware and software industries*"

Model-checking

Actual issue of verification : to identify

- classes of systems $\mathcal{S}$
- sets of formulae Φ

such that there exists an efficient algorithm which given $S \in \mathcal{S}$ and $\varphi \in \Phi$ decides whether $S \models \varphi$.
Model-checking problem is decidable when such an algorithm exists. Implementation in a model-checker.

Example

- Classes of models : Kripke structures, Petri nets, pushdown automata, timed automata, hybrid automata
- formulae of temporal logics (LTL, CTL, ...), first-order logics (Presburger's arithmetics, ...)

Model-checking

A system S has a finite or infinite number of configurations. An execution of S is a sequence of configurations.

Basic problem in verification is reachability (resp. safety) :
Is a given configuration reachable (resp. avoidable) from an initial configuration ?

Example (safety)

Absence of deadlock, capacity overflow, division by zero.

Approaches :

- easy if finite number of configurations : compute one by one the reachable configurations from the initial configuration
- difficult and even not decidable for systems with an infinite number of configurations
- acceleration techniques in a way to compute in one step an infinite number of reachable configurations

Counter systems

Definition

Counter system $S = (Q, X, T)$ with

- Q finite set of states
- X finite set of counters $x_1, \ldots, x_n$ (integer variables)
- $T \subseteq Q \times \mathit{Presb}(X, X') \times Q$ finite set of transitions, labeled by a formula $\varphi(x_1, \ldots, x_n, x'_1, \ldots, x'_n)$ of $\langle \mathbb{Z}, =, +, \leq \rangle$ (X' copy of X)

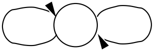
Definition

- Configuration $(q, \overline{v}) = (q, (v_1, \ldots, v_n))$ with q a state, and each v_i an integer value of x_i
- Successive configurations $(q, \overline{v}) \rightarrow_e (q', \overline{v}')$ with $e = (q, \varphi, q')$ a transition and $\varphi(\overline{v}, \overline{v}')$ satisfied
- Reachable configuration

Counter systems

Example (Syracuse problem)

$$(\exists y)(x_1 = 2y) \wedge (x_1' = y)$$



$$\neg((\exists y)(x_1 = 2y)) \wedge (x_1' = 3x_1 + 1)$$

Problem : for every initial value of x_1, the system always reaches a configuration with the value of x_1 equal to 0. Open problem

Counter systems :

- Rich class allowing the modeling of communication protocols, multi-thread programs, programs with pointers, ...
- Too rich class with reachability and safety problems being not decidable
- identification of decidable subclasses

Reachability of counter systems

Logical approach to the reachability problem :

- Composition of two successive transitions

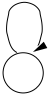
  $$q \xrightarrow{\varphi(\overline{x},\overline{x}')} q' \xrightarrow{\varphi'(\overline{x},\overline{x}')} q''$$

  equivalent to a transition

  $$q \xrightarrow{\phi(\overline{x},\overline{x}')} q'' \qquad \text{with } \phi(\overline{x},\overline{x}') = (\exists \overline{y})(\varphi(\overline{x},\overline{y}) \wedge \varphi'(\overline{y},\overline{x}'))$$

  Formula $\phi(\overline{x},\overline{x}')$ of $\langle \mathbb{Z}, =, +, \leq \rangle$

- Acceleration of a loop

  $\varphi(\overline{x},\overline{x}')$

  formula expressing all iterations k, $k \geq 0$, of the cycle.
  Effective expressivity in $\langle \mathbb{Z}, =, +, \leq \rangle$?

Reachability of counter systems

- Composition of two successive transitions
- Acceleration of a loop

Example

cycle label $\varphi(\overline{x}, \overline{x}')$

- $x_1' = x_1 + 1$
  accelerated as $(\exists y \geq 0)(x_1' = x_1 + y)$, formula of $\langle \mathbb{Z}, =, +, \leq \rangle$
- $x_1' = 2x_1$
  accelerated as $(\exists y \geq 0)(x_1' = 2^y \cdot x_1)$ not definable in $\langle \mathbb{Z}, =, +, \leq \rangle$

- Flattening of the system
  - A flat system is a system with no nested loops
  - Is there a flattening of the system with the same set of reachable configurations ?

Reachability of counter systems

- Composition of two successive transitions
- Acceleration of a loop
- Flattening of the system

Theorem

If a counter system has a flattening such that each of its loops can be accelerated as a formula of $\langle \mathbb{Z}, =, +, \leq \rangle$*, then its set of reachable configurations is first-order definable in* $\langle \mathbb{Z}, =, +, \leq \rangle$

Corollary

For these systems, the reachability and safety problems are decidable

Effective constructions required !

Reachability of counter systems

Many research works by S. Bardin, B. Boigelot, H. Comon, A. Finkel, Y. Jurski, J. Leroux, A. Sangnier, G. Sutre, P. Wolper, ...

Theorem (2002,2005)

The loops of a linear counter system with a finite monoid can be effectively accelerated as a formula of $\langle \mathbb{Z}, =, +, \leq \rangle$

- A counter system is linear if the label $\varphi(\overline{x}, \overline{x}')$ of each transition is of the form $\phi(\overline{x}) \rightarrow (\overline{x}' = A\overline{x} + \overline{b})$ with A an integer matrix and $\overline{b}$ an integer vector

Many well-known systems of counter systems are linear counter systems with a finite monoid, with many interesting subclasses being flattable.

Linear hybrid automata

Definition

Linear hybrid automaton $H = (Q, X, T, s_0)$ with

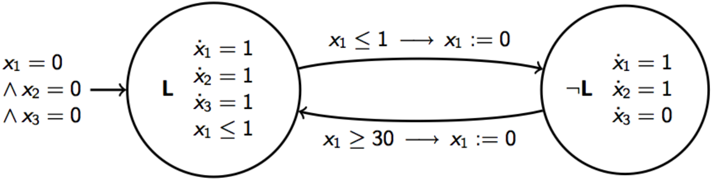
- Q finite set of states with an initial state s_0
- X finite set of real variables
- T finite set of transitions
- an initial guard $P_0\overline{x} \leq \overline{q}_0$
- for each transition e
  - a guard $P_e\overline{x} \leq \overline{q}_e$
  - an assignement $\overline{x} := A_e\overline{x} + \overline{b}_e$
- for each state s
  - a invariant $P_s\overline{x} \leq \overline{q}_s$
  - a continuous activity $A_s\dot{\overline{x}} \leq \overline{b}_s$

with all matrices and vectors being integer.

Linear hybrid automata

Example (Leaking gas burner)

"Whenever the gas burner is used for at least 60s. and provided that it leaks for at most 1s. every 30s., then the accumulated leaking time does not exceed 1/20th of total elapsed time"

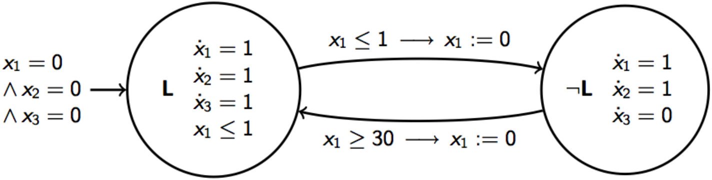


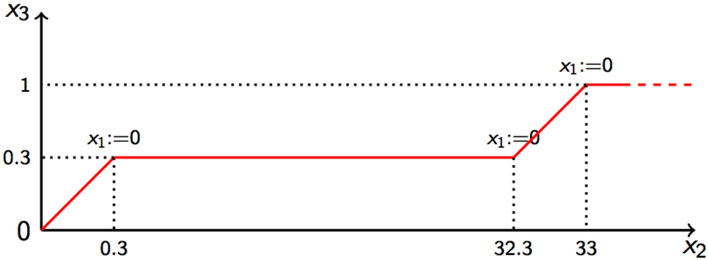
- x_2 total time
- x_3 leaking time
- x_1 clock used for "every 30s."

Check property $(x_2 \geq 60) \rightarrow (20x_3 \leq x_2)$

Linear hybrid automata

Example (continued)





Linear hybrid automata

Subclasses of Linear Hybrid automata :

- Timed-automata
  set X of clocks, with continuous activity $\dot{x} = 1$, and additional restrictions on guards, assignments and invariants
- Stopwatch automata
  like timed automata, with activity $\dot{x} = 1$ or $\dot{x} = 0$
- Rectangular initialized hybrid automata

Theorem

The reachability problem is decidable for timed automata and rectangular initialized hybrid automata, and is not decidable for linear hybrid automata and stopwatch automata

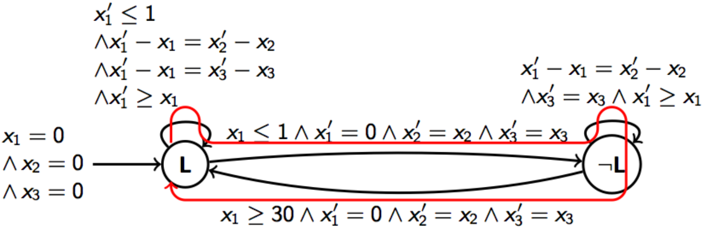
(Alur-Dill 91) (Henzinger et al. 95)

Reachability of linear hybrid automata

Logical approach to the reachability problem :

- Symbolic and effective semantics for linear hybrid automata in $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$
- Composition and acceleration of formulae $\varphi(\overline{x}, \overline{x}')$ of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ of the form $P(\overline{x}\ \overline{x}') \leq \overline{q}$

Example



Acceleration of the red cycle as

$$(\exists k \in \mathbb{N})(x_1' = 0) \wedge (x_3' - x_3 \leq k + 1 - x_1) \wedge (x_3 \leq x_3') \\ \wedge((x_2' - x_2) - (x_3' - x_3) \geq 30(k+1))$$

Reachability of linear hybrid automata

Many research works by B. Boigelot, H. Comon, F. Herbreteau Y. Jurski, P. Wolper, ...

Theorem (2006)

If a loop has a label $\varphi(\overline{x}, \overline{x}')$ of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ of the form $P(\overline{x}\ \overline{x}') \leq \overline{q}$ which is periodic, then it can be accelerated as a formula of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$

Theorem (1998, 1999)

The loops in a timed automaton and in a multicounter automaton can be accelerated as a formula of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$.

Theorem (1999)

The binary reachability relation of a timed automaton can be defined as a formula $\phi_{s,s'}(\overline{x}, \overline{x}')$ of $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$ (thanks to a flattening).

Software tools

- Manipulation of sets that are first-order definable in $\langle \mathbb{Z}, =, +, \leq \rangle$ or in $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$

  Differents tools :

  - OMEGA. Manipulation of formulae of $\langle \mathbb{N}, =, +, \leq \rangle$
  - BRAIN. Manipulation of semi-linear sets
  - MONA. Manipulation of automata for $\langle \mathbb{N}, =, +, \leq \rangle$
  - FAST. Manipulation of automata for $\langle \mathbb{Z}, =, +, \leq \rangle$
  - LASH. Manipulation of automata for $\langle \mathbb{Z}, =, +, \leq \rangle$ and $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$
  - LIRA. Manipulation of automata for $\langle \mathbb{R}, =, +, \leq, \mathbb{Z} \rangle$

- Reachability of linear counter systems

  Differents tools :

  - LASH. Loop aceleration
  - FAST. Loop acceleration, flattening
  - Alv. Checking of CTL formulae on counter systems
  - TReX. manipulation of clock and counter systems, with some restrictions

Thank you !