Decidable Compositions of O-Minimal Automata

Alberto Casagrande[1,2] Pietro Corvaja[1] Carla Piazza[1]
Bud Mishra[3,4]

[1]DIMI, Univ. di Udine, Udine, Italy

[2]Institute of Applied Genomics, Udine, Italy.

[3]Courant Institute, NYU, New York, USA

[4]NYU School of Medicine, New York, USA

Hybrid Systems

Many real systems have a double nature. They:

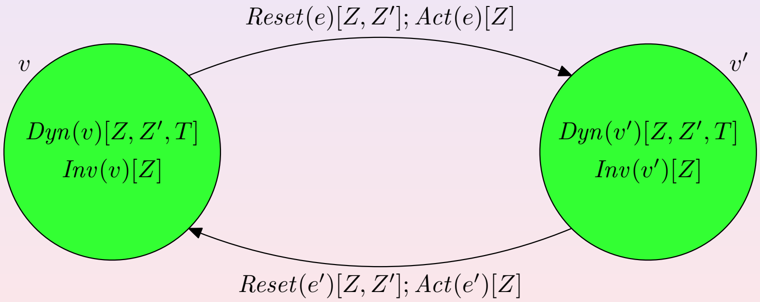
- evolve in a continuous way
- are ruled by a discrete system

We call such systems hybrid systems and we can formalize them using hybrid automata

Hybrid Automata - Intuitively

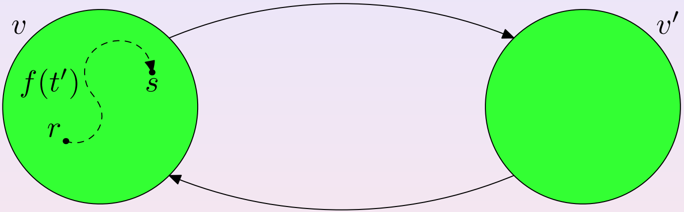
A hybrid automaton *H* is

a finite state automaton with continuous variables *Z*



A state is a pair $\langle v, r \rangle$ where r is an evaluation for Z

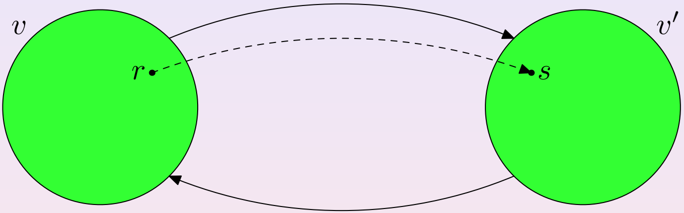
Hybrid Automata - Semantics



Definition (Continuous Transition)

$\langle v, r\rangle \xrightarrow{t}_C \langle v, s\rangle \iff$ there exists a continuous $f : \mathbb{R}^+ \mapsto \mathbb{R}^k$ such that $r = f(0)$, $s = f(t)$, and for each $t' \in [0, t]$ the formulæ $Inv(v)[f(t')]$ and $Dyn(v)[r, f(t'), t']$ hold

Hybrid Automata - Semantics



Definition (Discrete Transition)

$\langle v, r\rangle \xrightarrow{\langle v,\lambda,v'\rangle}_D \langle v', s\rangle \iff$ $\langle v,\lambda,v'\rangle \in \mathcal{E}$ and $Inv(v)[r]$, $Act(\langle v,\lambda,v'\rangle)[r]$, $Reset(\langle v,\lambda,v'\rangle)[r,s]$, and $Inv(v')[s]$ hold

Decidable Classes

Question

Can we automatically verify hybrid automaton properties?

Not even reachability is decidable in general

Many decidable classes have been defined:
Timed automata, Multi-rated automata, Rectangular automata, O-minimal automata, Semi-algebraic Constant Reset automata

Observation

Decidability results are usually obtained by quotients, e.g., Bisimulation and Simulation

Semi-Algebraic O-Minimal Hybrid Automata

Definition (Semi-Algebraic Theory)

First-order polynomial formulæ over the reals $(\mathbb{R}, 0, 1, *, +, >)$

Example

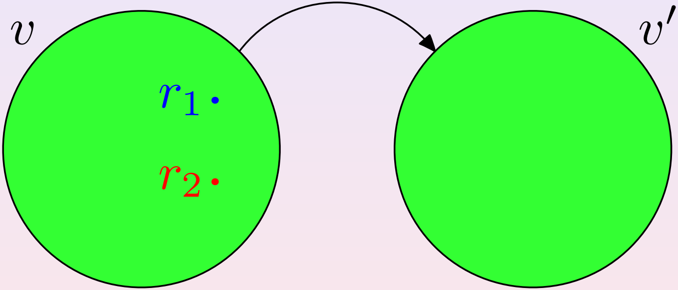
$$\exists T \geq 0 (Z' = T^2 - T + Z \wedge 1 \leq Z \leq 2)$$

Definition

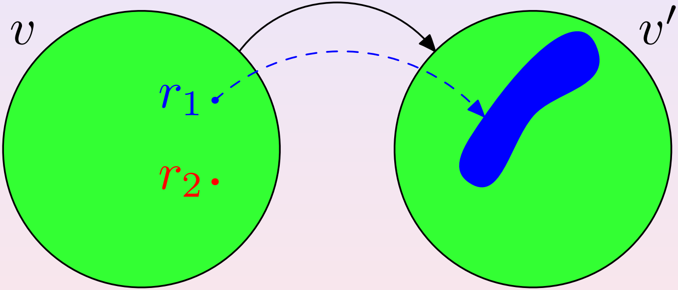
An hybrid automaton H is semi-algebraic o-minimal if:

- H is o-minimal (mainly means constant resets)
- *Dyn*, *Inv*, *Reset*, and *Act* are semi-algebraic

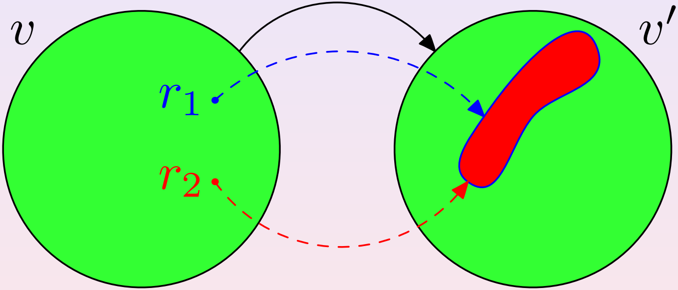
Constant Resets



Constant Resets



Constant Resets

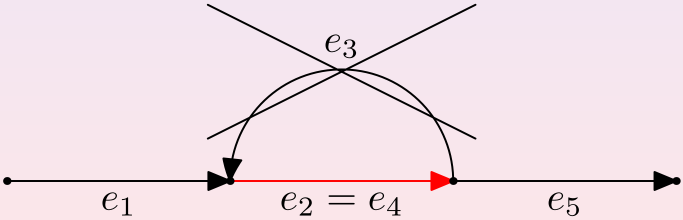


$$\forall Z' \, (\mathit{Reset}(e)[r_1, Z'] \leftrightarrow \mathit{Reset}(e)[r_2, Z'])$$

Semi-Algebraic O-Minimal Automata Properties - I

Constant resets imply that:

Acyclic paths are enough for reachability



Semi-Algebraic O-Minimal Automata Properties - II

Constant resets and semi-algebraic formulæ allow us to reduce reachability to satisfiability of first-order formulæ over $(\mathbb{R}, 0, 1, *, +, >)$

$$Reachable[Z, Z'] \equiv \bigvee_{ph \in Ph} \exists T \geq 0 (Reach_{ph}[Z, Z', T])$$

where Ph is the set of all acyclic paths and $Reach_{ph}[Z, Z', T]$ means that Z reaches Z' in time T through ph

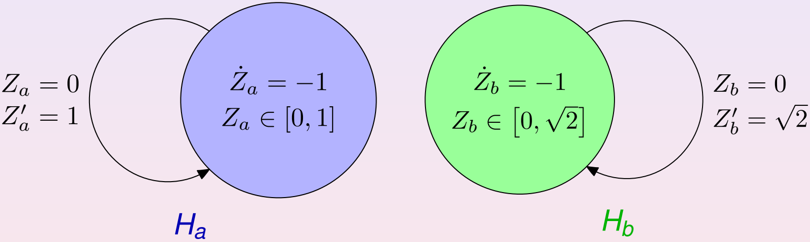
First-order formulæ over $(\mathbb{R}, 0, 1, *, +, >)$ are decidable [Tarski]

How to Increase Expressivity?

- We need to relax constant resets
- We could try to define ad-hoc conditions
(e.g., at least one constant reset along each cycle)
- What if we compose semi-algebraic o-minimal automata?
Compositionality is important both in modeling and in verification

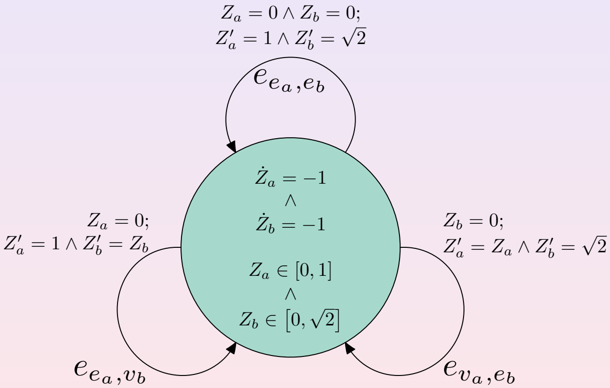
Is reachability still decidable?

Example



To formalize the overall system, we may perform parallel composition of components

Example



$H_a \times H_b$

Decidability is not preserved by composition [Miller]

Parallel Composition of Hybrid Automata

Definition

Let H_a and H_b be two hybrid automata over distinct variables. The *parallel composition* of H_a and H_b is the hybrid automaton $H_a \otimes H_b$, where:

- we consider all the variables of H_a and H_b
- the locations are the cartesian product of the locations
- each edge represents either one edge in one of the two components or one edge in each component
- *Dyn*, *Inv*, and *Act* are trivially defined as conjunctions
- *Reset* are conjunctions of either one reset and one identity or two resets

Composition of Semi-Algebraic O-Minimal Automata

The product of semi-algebraic o-minimal automata:

- is not a semi-algebraic o-minimal automata
  also identity resets are involved
- may have infinite simulation quotient
  we cannot use quotients for reachability

Reachability in Parallel Composition

Let us consider $H_a \times H_b$, i.e., two automata

(s_a, s_b) reaches (f_a, f_b) iff there exists a time t such that:

- s_a reaches f_a in time t in H_a and
- s_b reaches f_b in the same time in H_b

Reachability in Parallel Composition

Let us consider $H_a \times H_b$, i.e., two automata

(s_a, s_b) reaches (f_a, f_b) iff there exists a time t such that:

- s_a reaches f_a in time t in H_a and
- s_b reaches f_b in the same time in H_b

We can reduce reachability on the composition to:

1. study timed reachability on each component
2. intersect the results

Reachability in Parallel Composition

Let us consider $H_a \times H_b$, i.e., two automata

(s_a, s_b) reaches (f_a, f_b) iff there exists a time t such that:

- s_a reaches f_a in time t in H_a and
- s_b reaches f_b in the same time in H_b

We can reduce reachability on the composition to:

1. study timed reachability on each component
2. intersect the results

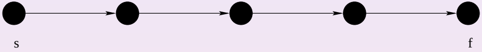
We already know that we cannot use quotients

Let us try with first-order formulæ

Timed Reachability on Semi-Algebraic O-Minimal

s reaches *f* from in time *t* in *H* iff

- there exists an acyclic path *ph* leading from *f* to *s* in time *tp*



- there are cycles which can be added to *ph*

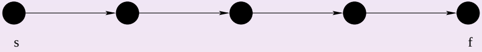
  which can be covered once in time ct_1, ct_2, . . .

- $t = th + n_1 * ct_1 + n_2 * ct_2 + \ldots$, with $n_1, n_2, \ldots$ natural

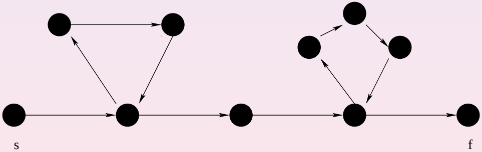
Timed Reachability on Semi-Algebraic O-Minimal

s reaches *f* from in time *t* in *H* iff

- there exists an acyclic path *ph* leading from *f* to *s* in time *tp*



- there are cycles which can be added to *ph*



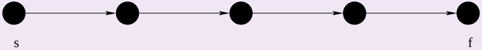
which can be covered once in time $ct_1, ct_2, \ldots$

- $t = th + n_1 * ct_1 + n_2 * ct_2 + \ldots$, with $n_1, n_2, \ldots$ natural

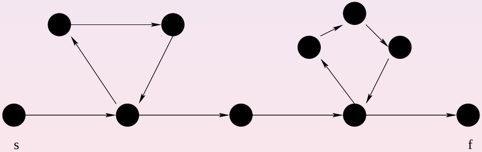
Timed Reachability on Semi-Algebraic O-Minimal

s reaches *f* from in time *t* in *H* iff

- there exists an acyclic path *ph* leading from *f* to *s* in time *tp*



- there are cycles which can be added to *ph*

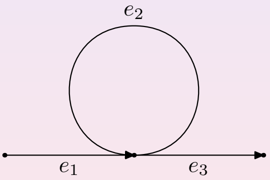


  which can be covered once in time ct_1, ct_2, ...

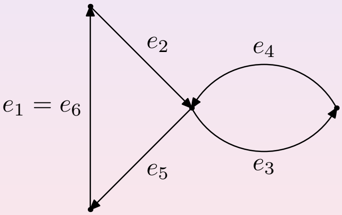
- $t = th + n_1 * ct_1 + n_2 * ct_2 + \ldots$, with n_1, n_2, ... natural

Technicalities - Cycles

We have a cycle only when we cross twice the same edge, since we need to use twice the same reset



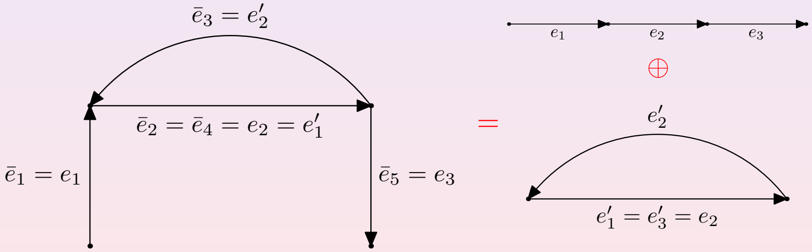
An acyclic path



A simple cycle

Technicalities - Path Decomposition

Each path is a composition of an acyclic path and a finite set of simple cycles



Back to Timed Reachability

If s reaches f in H through an acyclic path ph and $\{cy_1, cy_2, \ldots, cy_k\}$ are the simple cycles augmentable to ph, then s can reach f in H in time $t \in \mathrm{Time}(ph)$ with

$$\mathrm{Time}(ph) = \{t \mid t = tp + n_1 * tc_1 + \cdots + n_k * tc_k\}$$

where $tp \in T(ph)$, $tc_i \in T(cy_i)$, and $n_i \in \mathbb{N}$

This is a linear formula involving both semi-algebraic (roots of polynomials) and integer variables

Intersection, i.e., Reachability on the Composition

Let us consider again $H_a \times H_b$

We have to impose that they "spend time together", i.e.,

$$\mathrm{Time}(ph_a) \cap \mathrm{Time}(ph_b) \neq \emptyset$$

From timed reachability results, this is equivalent to

$$tpa + n_1 * tca_1 + \cdots + n_k * tca_k = tpb + m_1 * tcb_1 + \cdots + m_h * tcb_h$$

where there are natural and semi-algebraic variables

We have reduced our problem to . . .

. . . a Problem in Computational Number Theory

We have to solve a "system of linear Diophantine equations" with semi-algebraic coefficients:

$$tpa + n_1 * tca_1 + \cdots + n_k * tca_k = tpb + m_1 * tcb_1 + \cdots + m_h * tcb_h$$

The semi-algebraic coefficients are not fixed, but are solutions of first-order formulæ over the reals

We proved that this problem is decidable
The proof suggests us the easy case

Easy Case

In the easy case: semi-algebraic coefficients are not punctual

Example

$$\begin{cases} tpa + n * tca = tpb + m * tcb \\ tpa^2 - 2 \geq 0 \\ 0 \leq tpb \leq 1 \\ tca^5 - 2tca + 1 \geq 0 \\ tcb^3 + tcb - 10 \geq 0 \end{cases}$$

This means that in this case

Reachability on product is reachability on components

Conclusions

- We studied parallel composition of k semi-algebraic o-minimal hybrid automata
- They have identity resets and infinite quotients
- We decided reachability through an algebraic translation

From an high level perspective:

- Reals are “highly” decidable [Tarski]
- Integers are “highly” undecidable [10th Hilbert Pb]
- What is in the middle?