Automi Ibridi

Carla Piazza[1]

[1] Dipartimento di Matematica ed Informatica
Università di Udine
carla.piazza@dimi.uniud.it

Indice del Corso (Dis)Ordinato

- Automi Ibridi: Sintassi e Semantica
- Sistemi a stati finiti (breve ripasso)
- Il problema della Raggiungibilità
- Risultati di Indecidibilità
- Classi notevoli di Automi Ibridi: timed, rectangular, o-minimal, ...
- Tecniche di Decisione: (Bi)Simulazione, Cylindric Algebraic Decomposition, Teoremi di Selezione, Semantiche approssimate
- Equazioni Differenziali
- ... e tanto altro:
  - Logiche temporali
  - Composizione di Automi
  - Il caso Stocastico
  - Stabilità, Osservabilità, Controllabilità
  - Strumenti Software
  - Applicazioni

Nella lezione precedente . . .

. . . abbiamo visto che:

Se H è definito con formule su $(\mathbb{R}, +, *, <, 0, 1)$, allora

Path Reachability	$\Leftrightarrow$	Formula Satisfiability
Reachability	$\Leftrightarrow$	Infinite Formula Satisfiability

Inoltre si possono usare le formule per definire modelli astratti

- Casagrande et al. *Inclusion dynamics hybrid automata.* I.&C., 2008
- Tiwari et al. *Series of Abstractions for Hybrid Automata.* HSCC, 2002

Warning!

- i risultati relativi alla Path Reachability presuppongono almeno la transitività delle dinamiche
- con le formule siamo passati da semantica operazionale a denotazionale
- anche nei modelli astratti abbiamo mantenuto precisione infinita

Proviamo a passare a precisione finita

Warning!

- i risultati relativi alla Path Reachability presuppongono almeno la transitività delle dinamiche
- con le formule siamo passati da semantica operazionale a denotazionale
- anche nei modelli astratti abbiamo mantenuto precisione infinita

Proviamo a passare a precisione finita

Warning!

- i risultati relativi alla Path Reachability presuppongono almeno la transitività delle dinamiche
- con le formule siamo passati da semantica operazionale a denotazionale
- anche nei modelli astratti abbiamo mantenuto precisione infinita

Proviamo a passare a precisione finita

Warning!

- i risultati relativi alla Path Reachability presuppongono almeno la transitività delle dinamiche
- con le formule siamo passati da semantica operazionale a denotazionale
- anche nei modelli astratti abbiamo mantenuto precisione infinita

Proviamo a passare a precisione finita

Which is Your Point of View?

- The world is dense
- The world is discrete

Which is Your Point of View?

- The world is dense

  $(\mathbb{R}, +, *, <, 0, 1)$ first-order theory is decidable

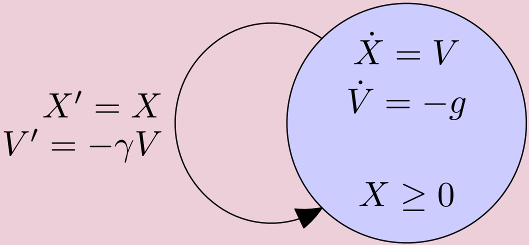
- The world is discrete

  Diophantine equations are undecidable

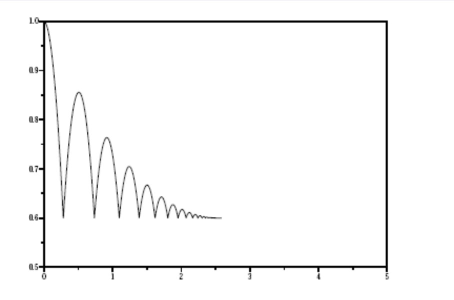
What about their interplay?

Example

Bouncing Ball

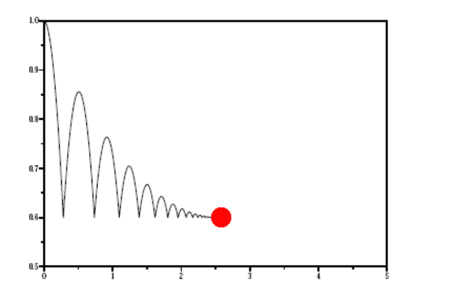


Example



Zeno Behavior The automaton avoids time elapsing by crossing edges infinitely often

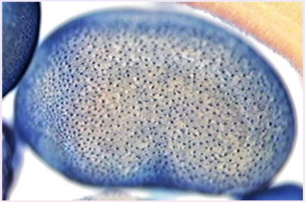
Example



Zeno Point The limit point of a Zeno behavior

Delta-Notch

Delta and Notch are proteins involved in cell differentiation (see, e.g., Collier et al., Ghosh et al.)

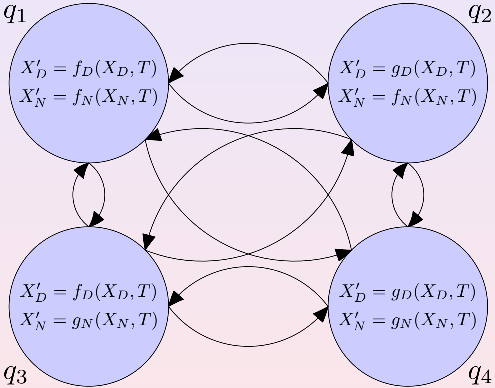


Notch production is triggered by high Delta levels in neighboring cells

Delta production is triggered by low Notch concentrations in the same cell

High Delta levels lead to differentiation

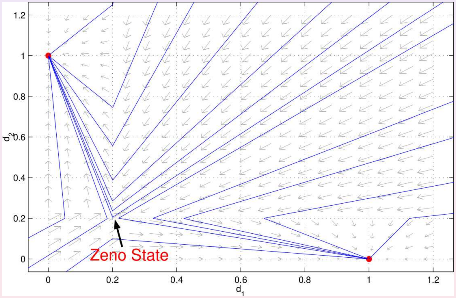
Delta-Notch: Single Cell Automaton



f_D and f_N increase Delta and Notch, g_D and g_N decrease Delta and Notch, respectively

Delta-Notch: Two Cells Automaton

It is the Cartesian product of two “single cell” automata



The Zeno state can occur only in the case of two cells with identical initial concentrations

Verification

Question

Can we automatically verify hybrid automata?

Let us start from the basic case of Reachability

Verification

Question

Can we automatically verify hybrid automata?

Let us start from the basic case of Reachability

$Naive\_Reachability(H, Initial\_set)$

$Old \leftarrow \emptyset$

$New \leftarrow Initial\_set$

while $New \neq Old$ **do**

  $Old \leftarrow New$
  $New \leftarrow Discrete\_Reach(H, Continuous\_Reach(H, Old))$

return Old

Bounded Sets and Undecidability

Even if the invariants are bounded, reachability is undecidable

Proof sketch

Encode two-counter machine by exploiting density:

- each counter value, n, is represented in a continuous variable by the value 2^{-n}
- each control function is mimed by a particular location

Where is the Problem?

Keeping in mind our examples:

Question "Meaning"

What is the meaning of these undecidability results?

Question "Decidability"

Can we avoid undecidability by adding some *natural* hypothesis to the semantics?

Undecidability in Real Systems

Undecidability in our models comes from . . .

- infinite domains: unbounded invariants
- dense domains: the “trick” n as 2^{-n}

Undecidability in Real Systems

Undecidability in our models comes from ...

- infinite domains: unbounded invariants
- dense domains: the "trick" n as 2^{-n}

But which real system does involve ...

- unbounded quantities?
- infinite precision?

Unboundedness and density abstract discrete large quantities

Dense vs Discrete - Intuition

We do not really want to completely abandon dense domains

We need to introduce a finite level of precision in bounded dense domains, we can distinguish two sets only if they differ of “at least ϵ”

Intuitively, we can see that something new has been reached only if a reasonable large set of new points has been discovered, i.e., we are myope

Dense vs Discrete

Lemma (Convergence)

Let $S \subseteq \mathbb{R}^k$ be a bounded set such that $S = \cup_{i \in \mathbb{N}} D_i$, with either $D_i = D_j$ or $D_i \cap D_j = \emptyset$
If there exists $\epsilon > 0$ such that for each $i \in \mathbb{N}$ there exists a_i such that $B(\{a_i\}, \epsilon) \subseteq D_i$, then there exists $j \in \mathbb{N}$ such that $S = \cup_{i \leq j} D_i$

This is a trivial compactness-like result

Finite Precision Semantics

Definition (ϵ-Semantics)

Let $\epsilon > 0$. For each formula ψ:

(ϵ) either $\{\!|\psi|\!\}_\epsilon = \emptyset$ or $\{\!|\psi|\!\}_\epsilon$ contains an ϵ-ball

($\cap$) $\{\!|\psi_1 \wedge \psi_2|\!\}_\epsilon \subseteq \{\!|\psi_1|\!\}_\epsilon \cap \{\!|\psi_2|\!\}_\epsilon$

($\cup$) $\{\!|\psi_1 \vee \psi_2|\!\}_\epsilon = \{\!|\psi_1|\!\}_\epsilon \cup \{\!|\psi_2|\!\}_\epsilon$

($\neg$) $\{\!|\psi|\!\}_\epsilon \cap \{\!|\neg\psi|\!\}_\epsilon = \emptyset$

It is a general framework: there exist many different ϵ-semantics

Reachability

Eps-Reachability($H, \psi[Z], \{\!|\cdot|\!\}_\epsilon$)

$R[Z] \leftarrow \psi[Z]$

$May\_New\_R[Z'] \leftarrow \exists Z(\widehat{Reach}^{1}(Z, Z') \wedge R[Z])$

$New\_R[Z] \leftarrow May\_New\_R[Z] \wedge \neg R[Z]$

while($\{\!|New\_R[Z]|\!\}_\epsilon \neq \emptyset$)

$\quad R[Z] \leftarrow R[Z] \vee New\_R[Z]$

$\quad May\_New\_R[Z'] \leftarrow \exists Z(\widehat{Reach}^{1}(Z, Z') \wedge R[Z])$

$\quad New\_R[Z] \leftarrow May\_New\_R[Z] \wedge \neg R[Z]$

return $R[Z]$

A Decidability Result

Theorem (Reachability Problem)

Using ϵ-semantics and assuming both bounded invariants and decidability for specification language, we have decidability of reachability problem for hybrid automata

A Decidability Result

Theorem (Reachability Problem)

Using ϵ-semantics and assuming both bounded invariants and decidability for specification language, we have decidability of reachability problem for hybrid automata

Proof Sketch

Because of condition (ϵ) of ϵ-semantics, continuous steps can either:

- increase the reached set by at least ϵ
- do not increase the reach set

($\cap$), ($\cup$), and ($\neg$) ensure that the sets *New_R* are disjoint

An Instance of ϵ-semantics

Definition

Let $\epsilon > 0$. We define $[\![\psi]\!]_\epsilon$ by structural induction on ψ as follows:

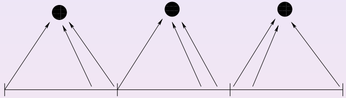
- $[\![t_1 \circ t_2]\!]_\epsilon = B([\![t_1 \circ t_2]\!], \epsilon)$, for $\circ \in \{=, <\}$
- $[\![\psi_1 \vee \psi_2]\!]_\epsilon = [\![\psi_1]\!]_\epsilon \cup [\![\psi_2]\!]_\epsilon$
- $[\![\psi_1 \wedge \psi_2]\!]_\epsilon = \cup_{B(\{p\},\epsilon) \subseteq [\![\psi_1]\!]_\epsilon \cap [\![\psi_2]\!]_\epsilon} B(\{p\}, \epsilon)$
- $[\![\exists Z \psi[Z, X]]\!]_\epsilon = \cup_{p \in \mathbb{R}} [\![\psi[p, X]]\!]_\epsilon$
- $[\![\forall Z \psi[Z, X]]\!]_\epsilon = \cup_{B(\{p\},\epsilon) \subseteq \cap_{Z \in \mathbb{R}} [\![\psi[Z,X]]\!]_\epsilon} B(\{p\}, \epsilon)$
- $[\![\neg \psi]\!]_\epsilon = \cup_{B(\{p\},\epsilon) \cap [\![\psi]\!]_\epsilon = \emptyset} B(\{p\}, \epsilon)$

Conclusions

- Hybrid automata are both powerful and natural in the modeling of hybrid systems
- May be a little bit too expressive ...
- Real systems always have finite precision
- ϵ-semantics introduce a finite precision ingredient in hybrid automata
- Using ϵ-semantics we do not have Zeno behaviors

Why not. . .

. . . modeling systems over discrete latices?



No, because three main reasons:

- modeling would became harder
- we would increase computational complexity
- we would still assume infinite precision!!! (e.g., $0,999\ldots9 \neq 1$)

. . . using only $<$ and $>$ instead of $=$?
No, because reachability is still undecidable.

Under, Over and Demorgan

Example

Consider the formula $1 < X < 5$ and $\epsilon = 0.1$
We have that $[\![1 < X < 5]\!]_\epsilon = [\![1 < X \wedge X < 5]\!]_\epsilon = (0.9, 5.1)$,

Consider the formula $\neg(1 < X < 5)$
We get that $[\![\neg(1 < X < 5)]\!]_\epsilon = (-\infty, 0.9) \cup (5.1, +\infty)$

Notice that this last formula is not equivalent to $X \leq 1 \vee X \geq 5$
whose semantics is $[\![X \leq 1 \vee X \geq 5]\!]_\epsilon = (-\infty, 1.1) \cup (4.9, +\infty)$

References

- Casagrande et al., “Discrete Semantics for Hybrid Automata” Discrete Event Dynamic Systems 2009
- A. Girard and G. J. Pappas, “Approximation metrics for discrete and continuous systems”, IEEE TAC 2007
- M. Fränzle, “Analysis of hybrid systems: An ounce of realism can save an infinity of states”, CSL 99