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

Eliminazione dei Quantificatori

Definition (Eliminazione dei Quantificatori)

Una teoria al primo-ordine $\mathcal{T}$ ammette l'eliminazione dei quantificatori se per ogni formula ψ di $\mathcal{T}$ esiste una formula $QF(\psi)$ equivalente a ψ e priva di quantificatori

Example

Su $\mathbb{R}$ la formula

$$\forall x(yx^2 + zx + w > 0)$$

È equivalente alla formula

$$z^2 - 4yw < 0$$

Eliminazione dei Quantificatori

Definition (Eliminazione dei Quantificatori)

Una teoria al primo-ordine $\mathcal{T}$ ammette l'eliminazione dei quantificatori se per ogni formula ψ di $\mathcal{T}$ esiste una formula $QF(\psi)$ equivalente a ψ e priva di quantificatori

Example

Su $\mathbb{R}$ la formula

$$\forall x(yx^2 + zx + w > 0)$$

È equivalente alla formula

$$z^2 - 4yw < 0$$

Eliminazione dei Quantificatori

Definition (Eliminazione dei Quantificatori)

Una teoria al primo-ordine $\mathcal{T}$ ammette l'eliminazione dei quantificatori se per ogni formula ψ di $\mathcal{T}$ esiste una formula $QF(\psi)$ equivalente a ψ e priva di quantificatori

Example

Su $\mathbb{R}$ la formula

$$\forall x(yx^2 + zx + w > 0)$$

È equivalente alla formula

$$z^2 - 4yw < 0$$

Eliminazione dei Quantificatori e Decidibilità

Theorem

Se $\mathcal{T}$ ammette l'eliminazione dei quantificatori, $QF(\psi)$ è calcolabile e la validità/soddisfacibilità delle formule senza quantificatori è decidibile, allora $\mathcal{T}$ è decidibile

Example (Aritmetica di Presburger)

Sia $\mathcal{T} = (+, 0, 1)$ la teoria al primo-ordine di $(\mathbb{N}, +, 0, 1)$ ovvero:

- $0 \neq x + 1$
- $x + 0 = x$
- $x + 1 = y + 1 \rightarrow x = y$
- $(x + y) + z = x + (y + z) \wedge x + y = y + x$
- $(P(0) \wedge P(x) \rightarrow P(x + 1)) \rightarrow \forall y(P(y))$

$\mathcal{T}$ ammette l'eliminazione dei quantificatori ed è decidibile

Eliminazione dei Quantificatori e Decidibilità

Theorem

Se $\mathcal{T}$ ammette l'eliminazione dei quantificatori, $QF(\psi)$ è calcolabile e la validità/soddisfacibilità delle formule senza quantificatori è decidibile, allora $\mathcal{T}$ è decidibile

Example (Aritmetica di Presburger)

Sia $\mathcal{T} = (+, 0, 1)$ la teoria al primo-ordine di $(\mathbb{N}, +, 0, 1)$ ovvero:

- $0 \neq x + 1$
- $x + 0 = x$
- $x + 1 = y + 1 \rightarrow x = y$
- $(x + y) + z = x + (y + z) \wedge x + y = y + x$
- $(P(0) \wedge P(x) \rightarrow P(x + 1)) \rightarrow \forall y(P(y))$

$\mathcal{T}$ ammette l'eliminazione dei quantificatori ed è decidibile

O-minimalità

Definition (O-minimalità)

Sia $\mathcal{M} = (M, \ldots, <)$ un modello su cui è definito un ordine totale $<$, $\mathcal{M}$ è o-minimale se ogni insieme $X \subseteq M$ definibile è un unione finita di punti e intervalli
Una teoria $\mathcal{T}$ è o-minimale se ha solo modelli o-minimali

Example

Sia $\mathcal{R}_{sin} = (\mathbb{R}, +, sin(\cdot), 0, 1, <)$

$$sin(x) = 0$$

definisce un insieme infinito di punti, quindi $\mathcal{R}_{sin}$ non è o-minimale

O-minimalità

Definition (O-minimalità)

Sia $\mathcal{M} = (M, \ldots, <)$ un modello su cui è definito un ordine totale $<$, $\mathcal{M}$ è o-minimale se ogni insieme $X \subseteq M$ definibile è un unione finita di punti e intervalli
Una teoria $\mathcal{T}$ è o-minimale se ha solo modelli o-minimali

Example

Sia $\mathcal{R}_{sin} = (\mathbb{R}, +, sin(\cdot), 0, 1, <)$

$$sin(x) = 0$$

definisce un insieme infinito di punti, quindi $\mathcal{R}_{sin}$ non è o-minimale

O-minimalità

Example

Sia $\mathcal{N} = (\mathbb{N}, +, 0, 1)$ l'aritmetica di Presburger

$$\exists y(x = y + y)$$

È soddisfatta dall'insieme $\mathcal{P}$ dei numeri pari, quindi $\mathcal{N}$ non è o-minimale

Example

Sia $\mathcal{R}_{exp} = (\mathbb{R}, +, *, e^{\cdot}, 0, 1, <)$ è o-minimale

O-minimalità

Example

Sia $\mathcal{N} = (\mathbb{N}, +, 0, 1)$ l'aritmetica di Presburger

$$\exists y(x = y + y)$$

È soddisfatta dall'insieme $\mathcal{P}$ dei numeri pari, quindi $\mathcal{N}$ non è o-minimale

Example

Sia $\mathcal{R}_{exp} = (\mathbb{R}, +, *, e^{\cdot}, 0, 1, <)$ è o-minimale

O-minimalità e Decidibilità

Theorem

Se $\mathcal{T}$ è o-minimale ed ammette l'eliminazione dei quantificatori, allora $\mathcal{T}$ è decidibile

Example

Sia $\mathcal{R} = (\mathbb{R}, +, *, 0, 1, <)$ è o-minimale ed ammette l'eliminazione dei quantificatori [Tarski]
È anche nota come "semi-algebraic theory over the reals"
Gli algoritmi di decisione sono anche noti come Cylindrical Algebraic Decomposition (CAD) (si veda Mathematica, Matlab, ...)

Un caso unidimensionale

Consideriamo un polinomio di grado n in una variabile

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Supponiamo che $lim_{X \to -\infty} p(X) = -\infty$ e $lim_{X \to +\infty} p(X) = +\infty$

La formula $p(X) > 0$ ha almeno una soluzione in $\mathbb{R}$

Un caso unidimensionale

Consideriamo un polinomio di grado n in una variabile

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Supponiamo che $lim_{X \to -\infty} p(X) = -\infty$ e $lim_{X \to +\infty} p(X) = +\infty$

La formula $p(X) > 0$ ha almeno una soluzione in $\mathbb{R}$

Un caso unidimensionale

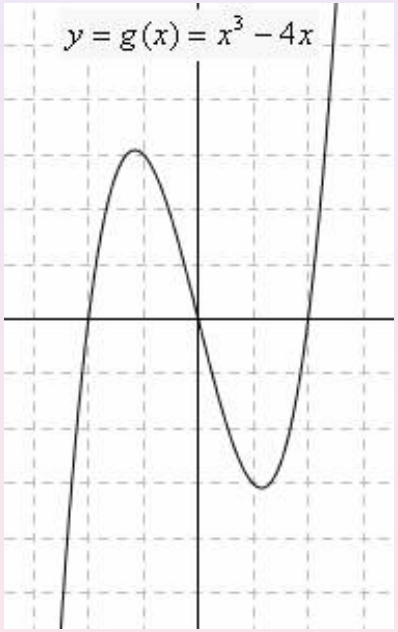
Consideriamo un polinomio di grado n in una variabile

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Supponiamo che $lim_{X \to -\infty} p(X) = -\infty$ e $lim_{X \to +\infty} p(X) = +\infty$

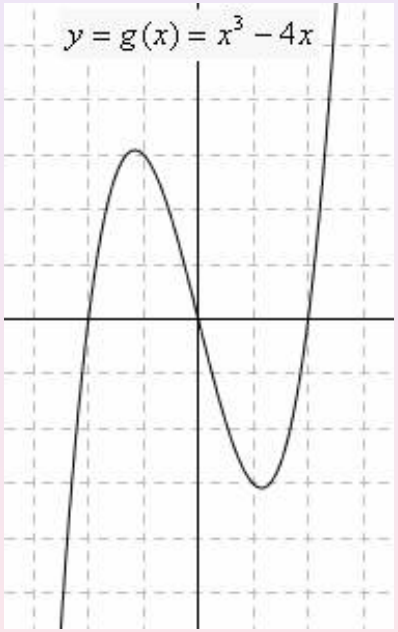
La formula $p(X) > 0$ ha almeno una soluzione in $\mathbb{R}$

Un caso unidimensionale



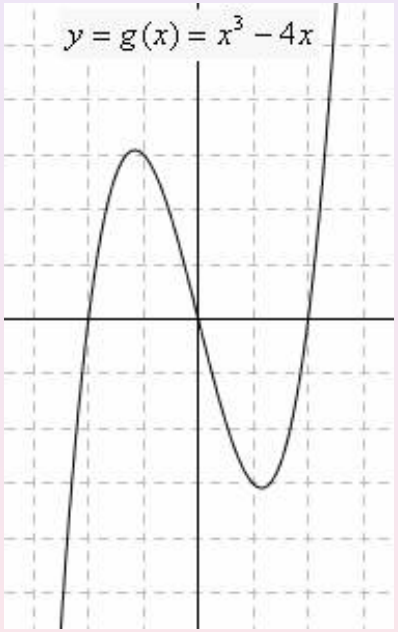
- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- ...
- dopo n passi arrivo ad una costante

Un caso unidimensionale



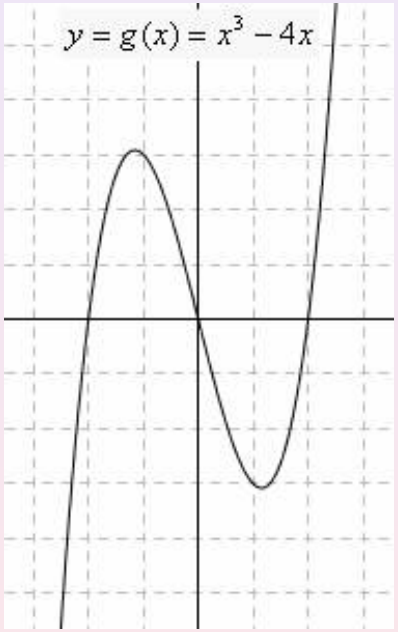
- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- ...
- dopo n passi arrivo ad una costante

Un caso unidimensionale



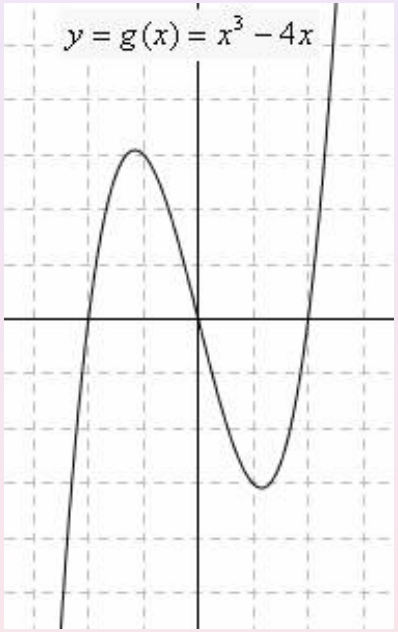
- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- . . .
- dopo n passi arrivo ad una costante

Un caso unidimensionale



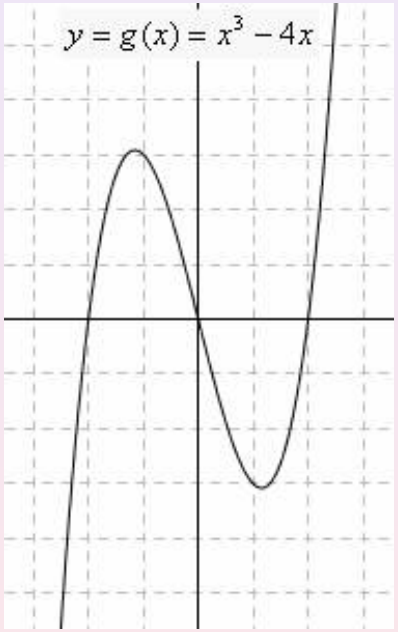
- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- ...
- dopo n passi arrivo ad una costante

Un caso unidimensionale



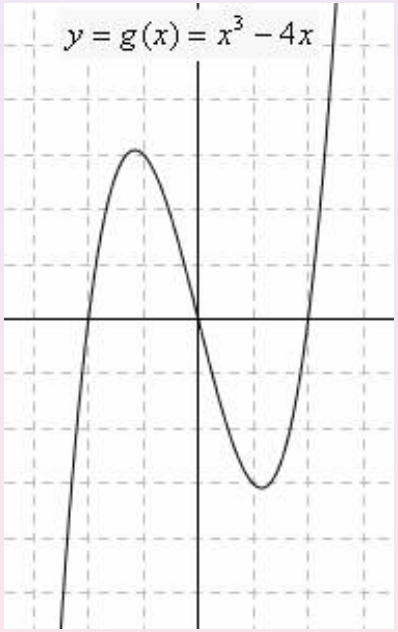
- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- . . .
- dopo n passi arrivo ad una costante

Un caso unidimensionale



- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- ...
- dopo n passi arrivo ad una costante

Un caso unidimensionale



- esiste un intervallo in cui $p(X)$ cresce
- esiste un intervallo in cui $p'(X) > 0$
- $p'(X)$ è di grado $n - 1$
- studio $p'(X) > 0$
- studio $p''(X) > 0$
- ...
- dopo n passi arrivo ad una costante

Radici reali di un polinomio

Theorem (Sturm)

Sia $p(X)$ un polinomio su $\mathbb{R}$, siano $a, b \in \mathbb{R}$ è possibile determinare quante radici di $p(X)$ cadono nell'intervallo (a, b)

Per arrivare al risultato di Tarski su $\mathbb{R}^k$ occorre sfruttare le proiezioni

O-minimal Hybrid Automata

Definition (Lafferriere, Pappas, Sastry 2000)

Un automa $H = \langle Z, Z', \mathcal{V}, \mathcal{E}, \mathit{Inv}, \mathit{Dyn}, \mathit{Act}, \mathit{Reset} \rangle$ è detto o-minimale se

- le formule *Inv*, *Act*, *Reset* sono definite su una teoria o-minimale
- *Dyn* sono campi vettoriali le cui soluzioni sono o-minimali
- *Reset* non dipendono da Z

O-minimal Hybrid Automata

Theorem

Gli automi o-minimali hanno il quoziente per bisimulazione finito

Se costruiti su una teoria o-minimale decidibile, gli automi o-minimali hanno una quoziente per bisimulazione calcolabile

O-minimal Hybrid Automata

Theorem

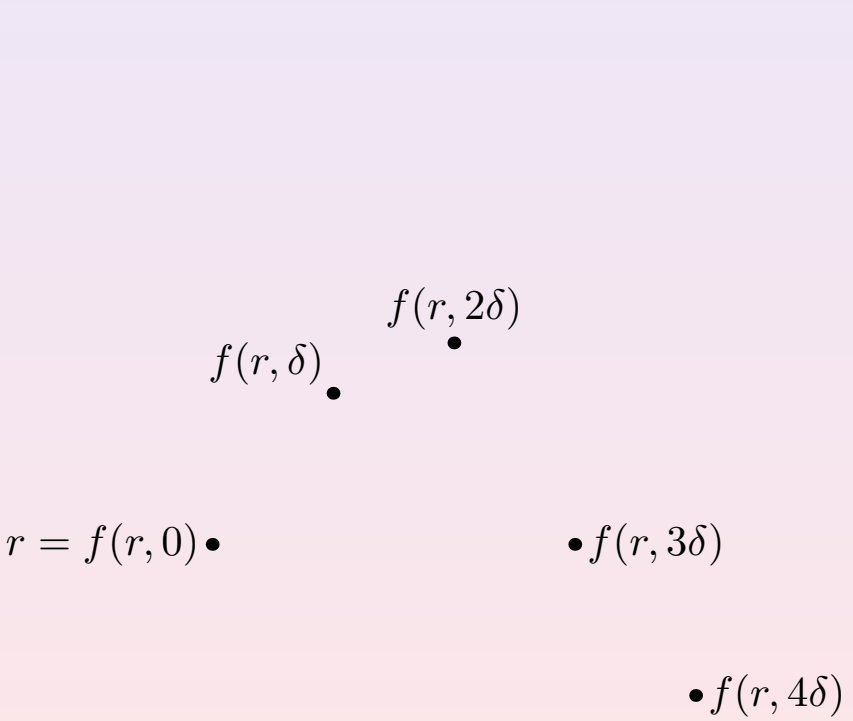
Gli automi o-minimali hanno il quoziente per bisimulazione finito

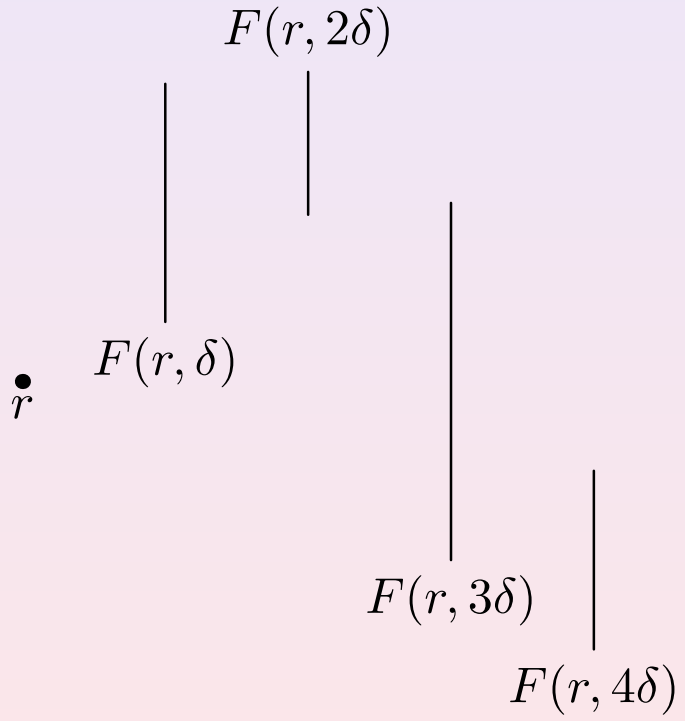
Se costruiti su una teoria o-minimale decidibile, gli automi o-minimali hanno una quoziente per bisimulazione calcolabile

- come possiamo estenderli? (FOCoRe, IDA, Prodotto Cartesiano)
- come altro possiamo sfruttare il risultato di Tarski? (Tiwari, Ratschan)

Inclusion Dynamics

Passiamo da funzioni ad inclusioni per definire il flusso

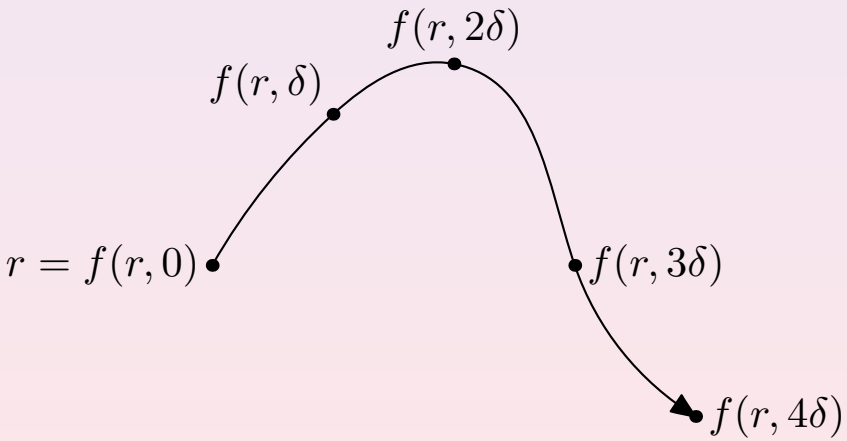


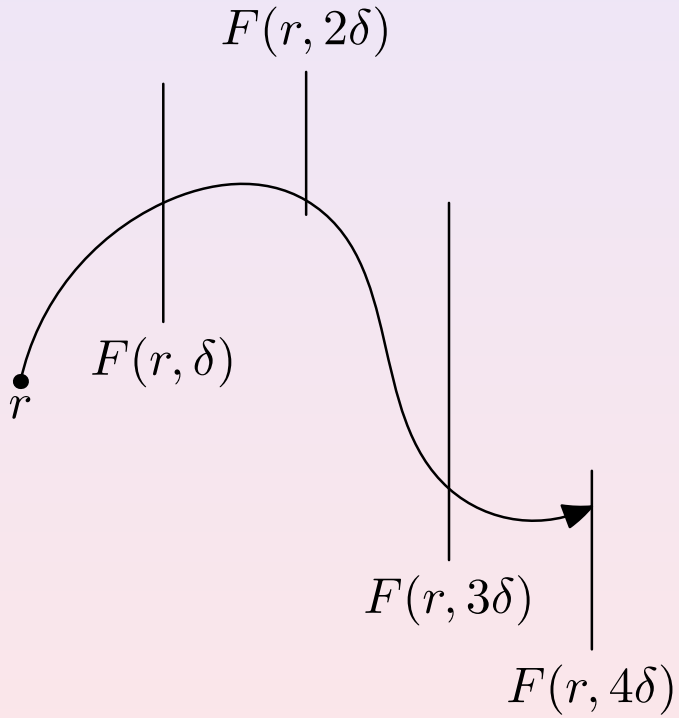


$Dyn[Z, Z', T] \equiv Z' = f(Z, T)$ $\quad$ $Dyn[Z, Z', T] \equiv Z' \in F(Z, T)$

Inclusion Dynamics

Passiamo da funzioni ad inclusioni per definire il flusso





$Dyn[Z, Z', T] \equiv Z' = f(Z, T)$

$Dyn[Z, Z', T] \equiv Z' \in F(Z, T)$

Perché Inclusion Dynamics?

Possiamo usarle per:

- approssimare soluzioni di equazioni differenziali
- stimare parametri non noti coinvolti nelle dinamiche

Problemi

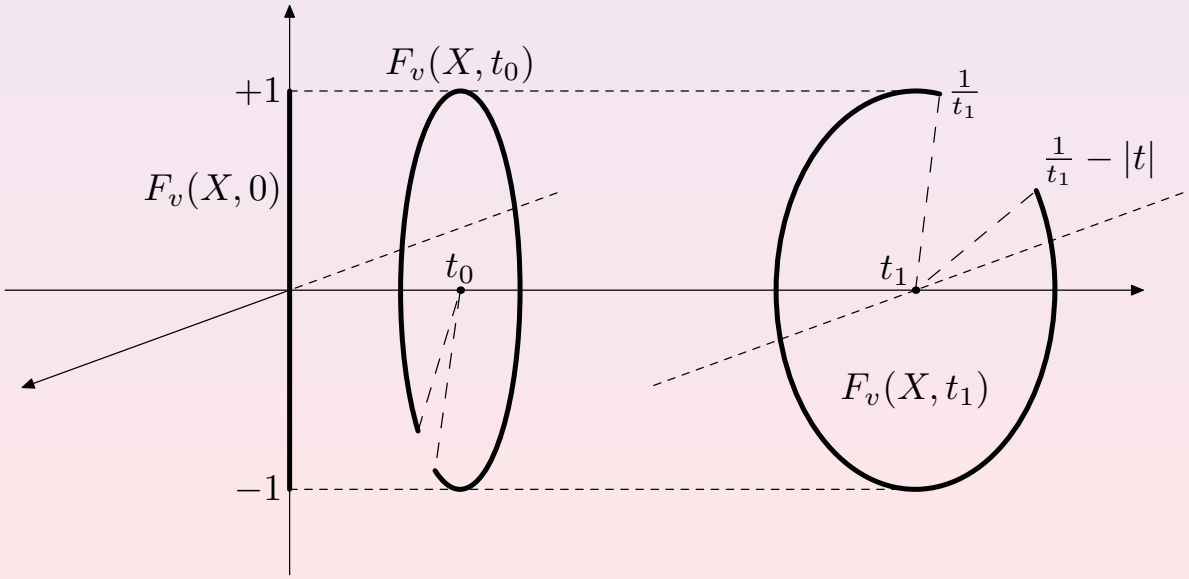
Dobbiamo garantire che se $Dyn(v)[Z, Z', T]$ vale, allora esiste un flusso continuo che soddisfa la dinamica

Se $Dyn(v)[Z, Z', T] \equiv Z' = f_v(Z, T)$, è sufficiente richiedere che f_v sia continua

Se $Dyn(v)[Z, Z', T] \equiv Z' \in F_v(Z, T)$, la Hausdorff continuità di F_v non basta

Esempio

$$F_v(X,t) = \begin{cases} \{\langle t\cos\theta, \sin\theta\rangle \mid \theta \in [\frac{1}{t}, \frac{1}{t} + 2\pi - |t|]\} & \text{if } t \neq 0 \\ \{\langle x, y\rangle \mid y \in [-1,1] \wedge x = 0\} & \text{otherwise} \end{cases}$$



Hybrid Automata with Inclusion Dynamics

Definition (Michael's Form)

Sia $F_Z^v(T) \stackrel{\text{def}}{=} \{Z' \mid Dyn(v)[Z, Z', T] \wedge Inv(v)[Z']\}$. Un automa è in Michael's form se

1. F_Z^v è lower semi-continua
2. per ogni $t \in I_Z^v$ l'insieme $F_Z^v(t)$ è chiuso e convesso

dove I_Z^v è il più grande intervallo $[0, t')$ tale che $F_Z^v(t) \neq \emptyset$ per ogni $t \in [0, t')$

Hybrid Automata with Inclusion Dynamics

Definition (Michael's Form)

Sia $F_Z^v(T) \stackrel{\text{def}}{=} \{Z' \mid Dyn(v)[Z, Z', T] \wedge Inv(v)[Z']\}$. Un automa è in Michael's form se

1. F_Z^v è lower semi-continua
2. per ogni $t \in I_Z^v$ l'insieme $F_Z^v(t)$ è chiuso e convesso

dove I_Z^v è il più grande intervallo $[0, t')$ tale che $F_Z^v(t) \neq \emptyset$ per ogni $t \in [0, t')$

Theorem

Se H è in Michael's form, allora $s \in F_r^v(t)$ sse $\langle v, r \rangle \xrightarrow{t}_C \langle v, s \rangle$.

Michael's Form e Raggiungibilità

Per ogni automa in Michael's form, possiamo scrivere una formula $Reach(H, ph)[Z, Z', T]$, dove $ph = v_0, \ldots, v_n$ è un cammino in $\langle \mathcal{V}, \mathcal{E} \rangle$, tale che

$Reach(H, ph)[Z, Z', T]$ vale $\iff$ H raggiunge $\langle v_n, Z' \rangle$ da $\langle v_0, Z \rangle$ con una traiettoria corrispondente a ph

Michael's Form e Raggiungibilità

Per ogni automa in Michael's form, possiamo scrivere una formula $Reach(H, ph)[Z, Z', T]$, dove $ph = v_0, \ldots, v_n$ è un cammino in $\langle \mathcal{V}, \mathcal{E} \rangle$, tale che

$Reach(H, ph)[Z, Z', T]$ vale $\iff$ H raggiunge $\langle v_n, Z' \rangle$ da $\langle v_0, Z \rangle$ con una traiettoria corrispondente a ph

Problema

Sfortunatamente, esistono automi con cammini discreti di lunghezza infinita

FOCoRe e IDA

FOCoRe (First Order Constant Reset hybrid automata) sono first-order hybrid automata:

- in Michael's form
- con constant resets (i.e., $Reset(e)[Z, Z']$ non dipende da Z)

IDA (Independent Dynamics hybrid Automata) consentono identity resets tra locazioni che hanno la stessa dinamica

FOCoRe e IDA

FOCoRe (First Order Constant Reset hybrid automata) sono first-order hybrid automata:

- in Michael's form
- con constant resets (i.e., $Reset(e)[Z, Z']$ non dipende da Z)

IDA (Independent Dynamics hybrid Automata) consentono identity resets tra locazioni che hanno la stessa dinamica

Possiamo ridurre il problema della raggiungibilità per FOCoRe e IDA $\mathcal{T}$-automata al problema della soddifacibilità di formule in $\mathcal{T}$

Raggiungibilità e Bisimulazione

Theorem

Sia $\mathcal{T}$ una teoria al primo-ordine decidibile. Il problema della raggiungibilità per FOCoRe e IDA $\mathcal{T}$-automata è decidibile

Theorem

Esistono FOCoRe e IDA con quozienti per (bi)simulazione infiniti

Predicate Abstraction

A. Tiwari and G. Khanna *Series of Abstractions for Hybrid Automata*, HSCC 2002

Consideriamo un'automa H in cui:

- le dinamiche sono definite con equazioni differenziali della forma

$$\dot{Z} = p(Z)$$

  con p polinomio
- invarianti, activation e reset sono disequazioni tra polinomi

In generale, su questi automi la raggiungibilità è indecidibile

Prediacate Abstraction - Intuitivamente

Consideriamo il caso di una sola locazione in cui

$$\dot{Z} = p(Z)$$

Divido lo spazio in un numero finito di regioni a seconda che

- $p(Z) > 0$
- $p(Z) = 0$
- $p(Z) < 0$

Predicate Abstraction - Intuitivamente

$p(Z)$ è continua, quindi per passare da $p(Z) > 0$ a $p(Z) < 0$ occorre passare attraverso $p(Z) = 0$

inoltre per passare da $p(Z) > 0$ a $p(Z) = 0$ deve essere $Z'' < 0$

- calcolo $Z'' = p'(Z) * Z' = p'(Z) * p(Z)$
- risuddivido lo spazio ...

itero il ragionamento

Predicate Abstraction - Intuitivamente

$p(Z)$ è continua, quindi per passare da $p(Z) > 0$ a $p(Z) < 0$ occorre passare attraverso $p(Z) = 0$

inoltre per passare da $p(Z) > 0$ a $p(Z) = 0$ deve essere $Z'' < 0$

- calcolo $Z'' = p'(Z) * Z' = p'(Z) * p(Z)$
- risuddivido lo spazio ...

itero il ragionamento

Predicate Abstraction - Intuitivamente

$p(Z)$ è continua, quindi per passare da $p(Z) > 0$ a $p(Z) < 0$ occorre passare attraverso $p(Z) = 0$

inoltre per passare da $p(Z) > 0$ a $p(Z) = 0$ deve essere $Z'' < 0$

- calcolo $Z'' = p'(Z) * Z' = p'(Z) * p(Z)$
- risuddivido lo spazio ...

itero il ragionamento

Predicate Abstraction - Intuitivamente

$p(Z)$ è continua, quindi per passare da $p(Z) > 0$ a $p(Z) < 0$ occorre passare attraverso $p(Z) = 0$

inoltre per passare da $p(Z) > 0$ a $p(Z) = 0$ deve essere $Z'' < 0$

- calcolo $Z'' = p'(Z) * Z' = p'(Z) * p(Z)$
- risuddivido lo spazio ...

itero il ragionamento

Predicate Abstraction - Stati e Transizioni

Intendo astrarre H con $(Q, \rightarrow)$

Come costruisco Q?

- considero l'insieme P_0 dei polinomi che occorrono in H
- saturo P_0 chiudendolo per "derivazione" (ottengo P)
- per ogni polinomio $p \in P$ considero una variabile x_p che varia in $\{-, +, 0\}$
- considero l'insieme $Q = \{-, +, 0\}^{|P|}$ delle possibili combinazioni di valori assunti dalle varibili

Predicate Abstraction - Stati e Transizioni

Intendo astrarre H con $(Q, \rightarrow)$

Come costruisco $\rightarrow$? se $q_1 \rightarrow q_2$, allora devono valere le

seguenti condizioni:

- se $x_p = +$ in q_1 e $x_p = 0$ in q_2, allora deve essere $x_{p'} = -$ in q_1
- ...

Constraint Interval Arithmetics

S. Ratschan and Z. She *Safety Verification of Hybrid Systems by Constraint Propagation Based Abstraction Refinement*, HSCC 2005