Il Problema della Raggiungibilita' per gli Automi Ibridi

Tiziano Villa

Universita' di Verona, Dicembre 2007

Sommario

- Il problema della raggiungibilita'
- Sistemi di transizione
- Relazione di equivalenza
- Bisimulazione
- Simulazione

Il Problema della Raggiungibilita'

Dato un automa ibrido H calcolare $Reach(H) \subset Q \times X$.

Permette di rispondere a domande su proprieta' di *sicurezza*:

dato $F \subseteq Q \times X$, la proprieta' "*always* F" e' soddisfatta da H se lungo tutte le esecuzioni di H lo stato rimane in F.

F e' un insieme "buono" di stati in cui si vuol sempre rimanere o anche F^c e' un insieme "cattivo" di stati da cui si vuole sempre rimanere fuori.

Altre proprieta':

"*eventually* F" *vivacita'* se lungo tutte le esecuzioni di H lo stato a un certo punto raggiunge F.

"*always eventually* F" *rispondenza* sempre eventualmente...

"*eventually always* F" *persistenza* eventualmente sempre...

Sistemi di Transizione

Un **sistema di transizione** e' una collezione

$$T = (S, \Sigma, \rightarrow, S_0, S_F)$$

dove

1. S e' un insieme di stati
2. Σ e' un alfabeto di eventi
3. $\rightarrow \subseteq S \times \Sigma \times S$ e' una relazione di transizione
4. $S_0 \subseteq S$ e' un insieme di stati iniziali
5. $S_F \subseteq S$ e' un insieme di stati finali

Sistemi di Transizione

Un automa finito $M = (Q, \Sigma, \Delta, q_o, F)$ e' un sistema di transizione dove

1. $S = Q$
2. Σ e' lo stesso
3. $\rightarrow = \Delta$
4. $S_0 = q_0$
5. $S_F = F$

Sistemi di Transizione

Un automa ibrido $H = (Q, X, Init, f, Inv, E, G, R)$ insieme con una proprieta' di sicurezza "*always* F" e' un sistema di transizione dove

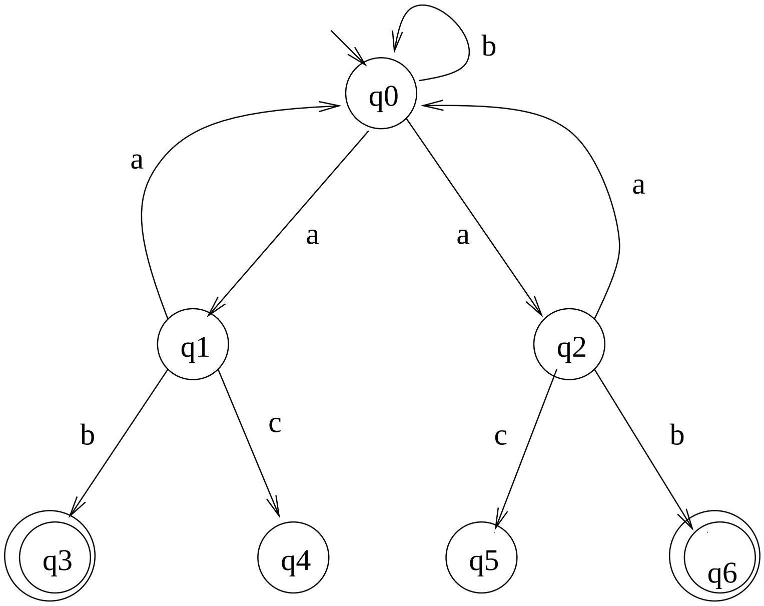
1. $S = Q \times X$
2. $\Sigma = E \cup \{\tau\}$
3. $\rightarrow = \{transizioni\ discrete\} \cup \{evoluzioni\ continue\}$, caratterizzate da Inv, G, R
4. $S_0 = Init$
5. $S_F = F^c$

Sistemi di Transizione

Esempio di problema della **raggiungibilita'**: dato un sistema di transizione T, c'e' uno stato $s_f \in S_F$ raggiungibile da uno stato $s_0 \in S_0$ con una successione di transizioni ?

Per automi finiti si possono sempre risolvere i problemi di raggiungibilita' mediante enumerazione.

Esempio. Automa finito.



Calcolo della Raggiungibilita'

$$
\begin{array}{l}
Raggiungibilita'(T)\ \{ \\
\quad Reach_0 = S_0 \\
\quad Reach_{-1} = \emptyset \\
\quad i = 0 \\
\quad \text{while } Reach_i \neq Reach_{i-1}\ \{ \\
\quad\quad Reach_{i+1} = Reach_i \cup \\
\quad\quad\quad \{s' \in S : \exists s \in Reach_i, \sigma \in \Sigma\ con\ (s, \sigma, s') \in \rightarrow\} \\
\quad\quad i = i + 1 \\
\quad \} \\
\}
\end{array}
$$

Se la procedura puo' essere meccanizzata, ed essa termina, e al termine $Reach_i \cap S_F = \emptyset$ allora la risposta al problema della raggiungibilita' e ' "no".

Per automi finiti la procedura puo' essere meccanizzata e termina sempre.

Nell'esempio $Reach_{-1} = \emptyset$, $Reach_0 = \{q_0\}$, $Reach_1 = \{q_0, q_1, q_2\}$, $Reach_2 = Q$.

Relazione d'Equivalenza

Nell'esempio q_1 e q_2 hanno proprieta' simili, poiche' sono raggiungibili da q_0 mediante a e tutte le esecuzioni successive sono simili. Gli stati q_1 e q_2 sono "equivalenti". La nozione di bisimulazione cattura tale equivalenza.

Una bisimulazione e' una relazione d'equivalenza che preserva la relazione di transizione.

Una **relazione d'equivalenza** $\sim \subseteq S \times S$ e' una relazione:

1. riflessiva: $(s, s) \in \sim \;\; \forall s \in S$
2. simmetrica: $(s, s') \in \sim \; \Rightarrow \; (s', s) \in \sim$
3. transitiva: $(s, s') \in \sim \; \wedge \; (s', s'') \in \sim \; \Rightarrow \; (s, s'') \in \sim$

Una relazione d'equivalenza partiziona S in un numero di classi d'equivalenza S_i: $S = \bigcup_i S_i$ tali che $\forall s, s' \in S, \;\; s, s' \in S_i$ *se e solo se* $s \sim s'$.

Relazione d'Equivalenza

Data una relazione d'equivalenza $\sim$, $S/\sim = \{S_i\}$ denota lo **spazio quoziente**, cioe' l'insieme delle classi d'equivalenza.

Dato un insieme $P \subseteq S$, $P/\sim$ rappresenta la parte dello spazio quoziente in comune con P:

$$P/\sim = \{S_i : S_i \cap P \neq \emptyset\} \subseteq S/\sim$$

Dato un sistema di transizione $T = (S, \Sigma, \rightarrow, S_0, S_F)$, il **sistema di transizione quoziente** e'

$$T/\sim = \{S/\sim, \Sigma, \rightarrow_\sim, S_0/\sim, S_F/\sim\}$$

dove per $S_1, S_2 \in S/\sim, (S_1, \sigma, S_2) \in \rightarrow_\sim$ se e solo se ci sono $s_1 \in S_1$ e $s_2 \in S_2$ tali che $(s_1, \sigma, s_2) \in \rightarrow$.

Per $\sigma \in \Sigma$, $Pre_\sigma : 2^S \rightarrow 2^S$ e' l'insieme degli stati che raggiungono P con una transizione in σ

$$Pre_\sigma(P) = \{s \in S : \exists s' \in P \ con \ (s, \sigma, s') \in \rightarrow\}$$

Nell'esempio, se $P = \{q_3, q_4, q_5, q_6\}$, allora $Pre_b(P) = Pre_c(P) = \{q_1, q_2\}$.

Bisimulazione

Dato $T = (S, \Sigma, \rightarrow, S_0, S_F)$ e una relazione d'equivalenza $\sim$ su S, $\sim$ si dice una **bisimulazione** se

1. S_0 e' un'unione di classi d'equivalenza

2. S_F e' un'unione di classi d'equivalenza

3. $\forall \sigma \in \Sigma$, se P e' un'unione di classi d'equivalenza, anche $Pre_\sigma(P)$ e' un'unione di classi d'equivalenza.

Se $\sim$ e' una bisimulazione, T e $T/\sim$ si dicono bisimili.

$\Rightarrow$ Date le classi d'equivalenza P, Q e $\sigma \in \Sigma$, dev'essere $Pre_\sigma(P) \cap Q = \emptyset$ o $Pre_\sigma(P) \cap Q = Q$.

Proposizione. Se $T = (S, \Sigma, \rightarrow, S_0, S_F)$ e $T/\sim = \{S/\sim, \Sigma, \rightarrow_\sim, S_0/\sim, S_F/\sim\}$ sono sistemi di transizione bisimili, i problemi di raggiungibilita' di T e $T/\sim$ sono equivalenti.

Bisimulazione

Dato $T = (S, \Sigma, \rightarrow, S_0, S_F)$, una **bisimulazione** e' una relazione binaria $\sim \subseteq S \times S$ tale che $\forall \sigma \in \Sigma$:

1. $s_1 \sim s_2 \;\wedge\; s_1 \in S_0 \;\Rightarrow\; s_2 \in S_0$
2. $s_1 \sim s_2 \;\wedge\; s_2 \in S_0 \;\Rightarrow\; s_1 \in S_0$
3. $s_1 \sim s_2 \;\wedge\; s_1 \in S_F \;\Rightarrow\; s_2 \in S_F$
4. $s_1 \sim s_2 \;\wedge\; s_2 \in S_F \;\Rightarrow\; s_1 \in S_F$
5. $s_1 \sim s_2 \wedge (s_1, \sigma, s_1') \in \rightarrow \;\Rightarrow\; \exists s_2' \; [s_1' \sim s_2' \;\wedge\; (s_2, \sigma, s_2') \in \rightarrow]$
6. $s_1 \sim s_2 \wedge (s_2, \sigma, s_2') \in \rightarrow \;\Rightarrow\; \exists s_1' \; [s_1' \sim s_2' \;\wedge\; (s_1, \sigma, s_1') \in \rightarrow]$

Gli stati s_1 e s_2 sono **equivalenti rispetto alla bisimulazione** o **bisimili** se c'e' una bisimulazione $\sim$ tale che $s_1 \sim s_2$.

Compito: Dimostrare l'equivalenza delle due definizioni di bisimulazione.

Bisimulazione

Due sistemi di transizione $T = (S, \Sigma, \rightarrow, S_0, S_F)$ e $T' = (S', \Sigma, \rightarrow', S'_0, S'_F)$ si dicono **bisimili** se esiste una relazione binaria $\sim \subseteq S \times S'$ tale che $\forall \sigma \in \Sigma$:

1. $s_1 \sim s_2 \;\wedge\; s_1 \in S_0 \;\Rightarrow\; s_2 \in S'_0$
2. $s_1 \sim s_2 \;\wedge\; s_2 \in S'_0 \;\Rightarrow\; s_1 \in S_0$
3. $s_1 \sim s_2 \;\wedge\; s_1 \in S_F \;\Rightarrow\; s_2 \in S'_F$
4. $s_1 \sim s_2 \;\wedge\; s_2 \in S'_F \;\Rightarrow\; s_1 \in S_F$
5. $s_1 \sim s_2 \wedge (s_1, \sigma, s'_1) \in\rightarrow \;\Rightarrow\; \exists s'_2\; [s'_1 \sim s'_2 \wedge (s_2, \sigma, s'_2) \in\rightarrow']$
6. $s_1 \sim s_2 \wedge (s_2, \sigma, s'_2) \in\rightarrow' \;\Rightarrow\; \exists s'_1\; [s'_1 \sim s'_2 \wedge (s_1, \sigma, s'_1) \in\rightarrow]$

Simulazione

Dato $T = (S, \Sigma, \rightarrow, S_0, S_F)$, una **simulazione** e' una relazione binaria $\sim \subseteq S \times S$ tale che $\forall \sigma \in \Sigma$:

1. $s_1 \sim s_2 \ \wedge \ s_1 \in S_0 \ \Rightarrow \ s_2 \in S_0$
2. $s_1 \sim s_2 \ \wedge \ s_1 \in S_F \ \Rightarrow \ s_2 \in S_F$
3. $s_1 \sim s_2 \wedge (s_1, \sigma, s_1') \in \rightarrow \Rightarrow \ \exists s_2' \ [s_1' \sim s_2' \wedge (s_2, \sigma, s_2') \in \rightarrow]$

Gli stati s_1 e s_2 sono **equivalenti rispetto alla simulazione** se c'e' una simulazione $\sim$ tale che $s_1 \sim s_2$ e una simulazione $\sim'$ tale che $s_2 \sim s_1$.

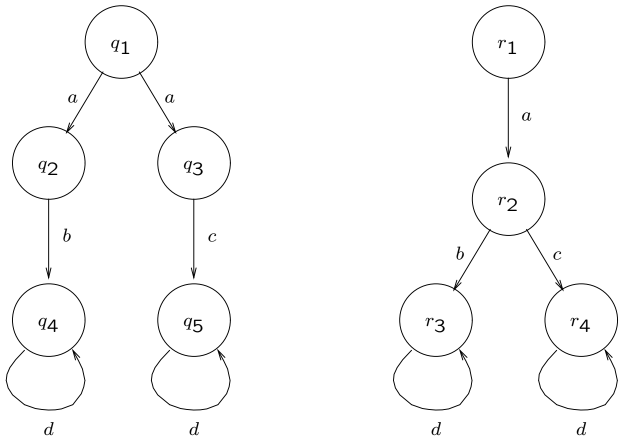
Per avere una bisimulazione bisogna che $\sim' \equiv \sim^{-1}$, cioe' $\sim$ dev'essere una simulazione in entrambe le direzioni.

Simulazione

Bisimulazione $\Longrightarrow$ Simulazione $\Longrightarrow$ Linguaggio.

Un'equivalenza piu' fine di un'altra identifica meno stati come equivalenti. Dalla piu' fine alla meno fine:
Bisimulazione $\longrightarrow$ Simulazione $\longrightarrow$ Linguaggio.

Esempio. Gli stati q_1 e r_1 sono equivalenti rispetto al linguaggio, ma non simili, perche' nessun a-successore di q_1 simula l'a-successore r_2 di r_1.



Compito: Esibire dei sistemi di transizione T e T' tali che lo stato iniziale s_0 di T e' equivalente allo stato iniziale s'_0 di T' rispetto a simulazione e linguaggio, ma non rispetto a bisimulazione.

Calcolo del Quoziente di Bisimilarita'

Se T e' un sistema di transizione, la relazione binaria $\equiv_T^{bis} \subseteq S \times S$ e' definita da $q \equiv_T^{bis} r$ se e solo se c'e una bisimulazione $\preceq$ su T con $q \preceq r$.

La relazione $\equiv_T^{bis}$ e' l'unione di tutte le bisimulazioni su T.

Compito: La relazione $\equiv_T^{bis}$ e' una bisimulazione su T.

La relazione $\equiv_T^{bis}$ si dice **bisimilarita'**.

Il quoziente $T/_{\equiv_T^{bis}}$ e' il **quoziente di bisimilarita'** di T.

Calcolo del Quoziente di Bisimilarita'

$$
\begin{array}{l}
Bisimilarita'(T) \ \{ \\
\quad S/\sim = \{S_0, S_F, S \setminus (S_0 \cup S_F)\} \\
\quad \text{while } \exists P, P' \in S/\sim,\ \sigma \in \Sigma\text{: } P \cap Pre_\sigma(P') \neq P \quad \wedge \\
\qquad\qquad P \cap Pre_\sigma(P') \neq \emptyset \ \{ \\
\qquad P_1 = P \cap Pre_\sigma(P') \\
\qquad P_2 = P \setminus Pre_\sigma(P') \\
\qquad S/\sim = (S/\sim \setminus \{P\}) \cup \{P_1, P_2\} \\
\quad \} \\
\}
\end{array}
$$

Si suppone $S_0 \neq \emptyset$, $S_F \neq \emptyset$, $S_0 \cap S_F = \emptyset$. Se $S_0 \cap S_F \neq \emptyset$, si pone $S/\sim = \{S_0 \setminus S_F, S_F \setminus S_O, S_0 \cap S_F, S \setminus (S_0 \cup S_F)\}$.

Se l'algoritmo termina $\sim$ e' una bisimulazione:

1. S_0 e' un'unione di classi d'equivalenza: inizialmente $S_0 \in S/\sim$ e poi l'unica operazione e' la suddivisione di una classe in piu' classi

2. S_F e' un'unione di classi d'equivalenza: inizialmente $S_F \in S/\sim$ e poi l'unica operazione e' la suddivisione di una classe in piu' classi

3. Se termina $\forall P, P' \in S/\sim$ e $\forall \sigma \in \Sigma$, $P \cap Pre_\sigma(P')$ e' uguale a P o a $\emptyset \Rightarrow Pre_\sigma(P')$ e' un'unione di classi d'equivalenza.

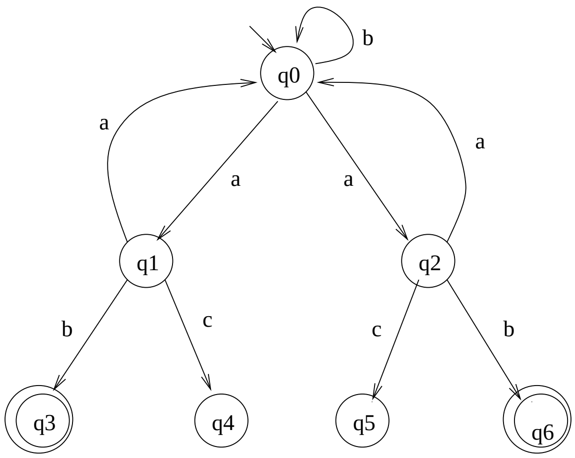
Calcolo del Quoziente di Bisimilarita'

T e $T/\sim$ hanno problemi di raggiungibilita' equivalenti.

Se S e' finito, l'algoritmo termina sempre e riduce la complessita' del calcolo della raggiungibilita'.

Esempio. Quoziente di bisimilarita' del precedente automa finito: $\sim = \{\{q_0\}, \{q_1, q_2\}, \{q_3, q_6\}, \{q_4, q_5\}\}$.

[Da $P = \{q_1, q_2, q_4, q_5\}$, $P' = \{q_0\}$, $Pre_a(P') = \{q_1, q_2\}$, $P \cap Pre_a(P') = \{q_1, q_2\}$, $P \setminus Pre_a(P') = \{q_4, q_5\}$.]



Calcolo del Quoziente di Bisimilarita'

T e $T/\sim$ hanno problemi di raggiungibilita' equivalenti.

Se S e' infinito, il calcolo della raggiungibilita' non e' detto termini. Se pero' l'algoritmo della bisimulazione termina producendo un quoziente $T/\sim$ finito, si possono risolvere su $T/\sim$ i problemi di raggiungibilita'.

Se T ha una bisimulazione finita, e' garantito che su $T/\sim$ sia la raggiungibilita' in avanti che all'indietro terminano.

Ma c'e' di piu'...
Se T ha una bisimulazione finita, o la raggiungibilita' in avanti o quella all'indietro terminano su T.

Il quoziente rispetto alla bisimilarita' serve soprattutto a stabilire la decidibilita' del problema, poi si calcola la raggiungibilita' in avanti o all'indietro.

Calcolo del Quoziente di Bisimilarita'

Problema: per quale classe di sistemi di transizione infiniti, c'e' una bisimulazione finita ?

La decidibilita' richiede non solo la terminazione della procedura, ma anche la calcolabilita' di ogni passo:

- rappresentare simbolicamente gl'insiemi
- eseguire intersezione e complementazione d'insiemi
- calcolare se un insieme e' vuoto
- calcolare $Pre_\sigma(Y)$ di un insieme Y

Sommario

- Automi temporizzati
- Bisimulazione di automi temporizzati

Automa Temporizzato

Predicati di orologio

L'insieme $\Phi(X)$ di predicati di orologio di X e' un insieme di espressioni logiche finite definite induttivamente da $\delta \in \Phi(X)$ se:

$$\delta := (x_i \leq c) \mid (x_i \geq c) \mid \neg\delta_1 \mid \delta_1 \wedge \delta_2$$

dove $\delta_1, \delta_2 \in \Phi(X), x_i \in X$ e $c \geq 0$ e' un razionale.

A ogni $\delta \in \Phi$ si associa un insieme

$$\widehat{\delta} = \{x \in \boldsymbol{X} : \delta(x) = True\}$$

Esempi

- $(x_1 \leq 1) \in \Phi(X)$
- $(0 \leq x_1 \leq 1) \in \Phi(X)$ $(\equiv (x_1 \geq 0) \wedge (x_1 \leq 1))$
- $(x_1 = 1) \in \Phi(X)$ $(\equiv (x_1 \geq 1) \wedge (x_1 \leq 1))$
- $(x_1 < 1) \in \Phi(X)$ $(\equiv \neg(x_1 \geq 1))$
- $True \in \Phi(X)$ $(\equiv \neg((x_1 \leq 0) \wedge (x_1 \geq 1)))$
- $(x_1 \leq x_2) \notin \Phi(X)$

Automa Temporizzato

Un automa temporizzato e' un automa ibrido

$H = (Q, X, Init, f, Inv, E, G, R)$ dove

- Q e' l'insieme dei modi (stati discreti), $\boldsymbol{Q} = \{q_1, \dots, q_m\}$
- $X = \{x_1, \dots, x_n\}$, $\boldsymbol{X} = R^n$
- $Init = \{\{q_i\} \times \widehat{Init_{q_i}(x)}\}_{i=1}^{m}$, dove $Init_{q_i}(x) \in \Phi(X)$
- $f(q, x) = (1, \dots, 1)$, $\forall (q, x)$
- $Inv(q, x) = \widehat{Inv_q(x)}$, dove $Inv_q(x) \in \Phi(X)$, $\forall q \in \boldsymbol{Q}$
- $E \subseteq \boldsymbol{Q} \times \boldsymbol{Q}$
- $G(e, x) = \widehat{G_e(x)}$, dove $G_e(x) \in \Phi(X)$, $\forall e = (q, q') \in E$
- $R(e, x)$ o lascia x_i invariato o lo azzera, $\forall e \in E$

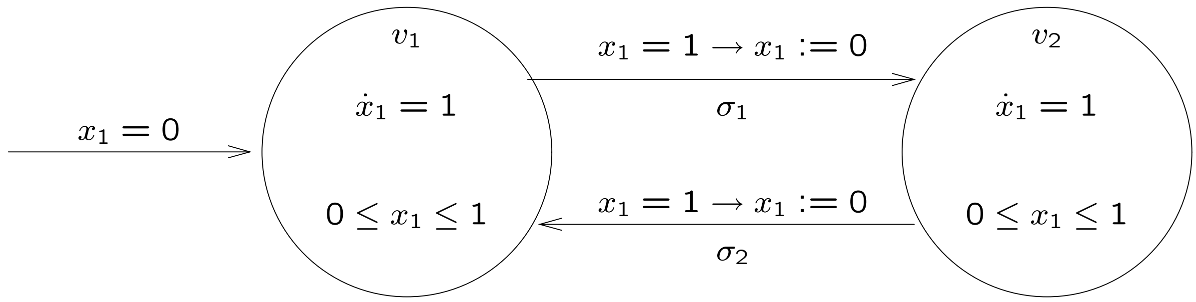
Per semplicita' nel costruire la bisimulazione si assumera'

- $Inv(q, x) = \boldsymbol{X}$, $\forall q \in \boldsymbol{Q}$

Automi Temporizzati

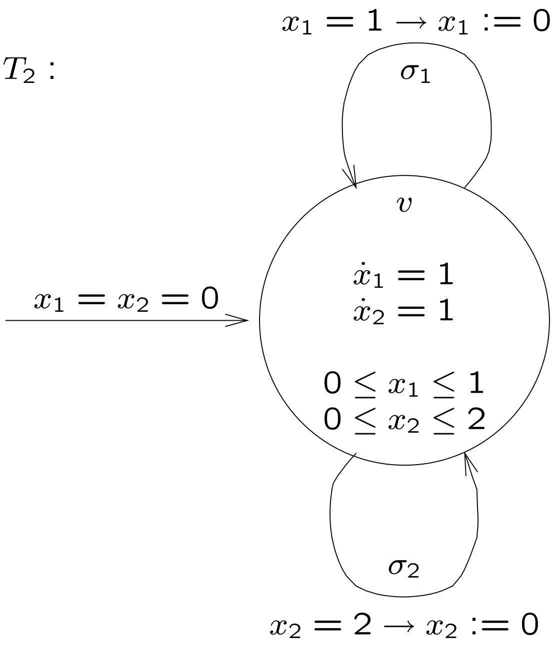
Esempio di automa a tempo con 1 orologio.

T_1 :



Esempio di automa a tempo con 2 orologi.

T_2 :



Automi Temporizzati

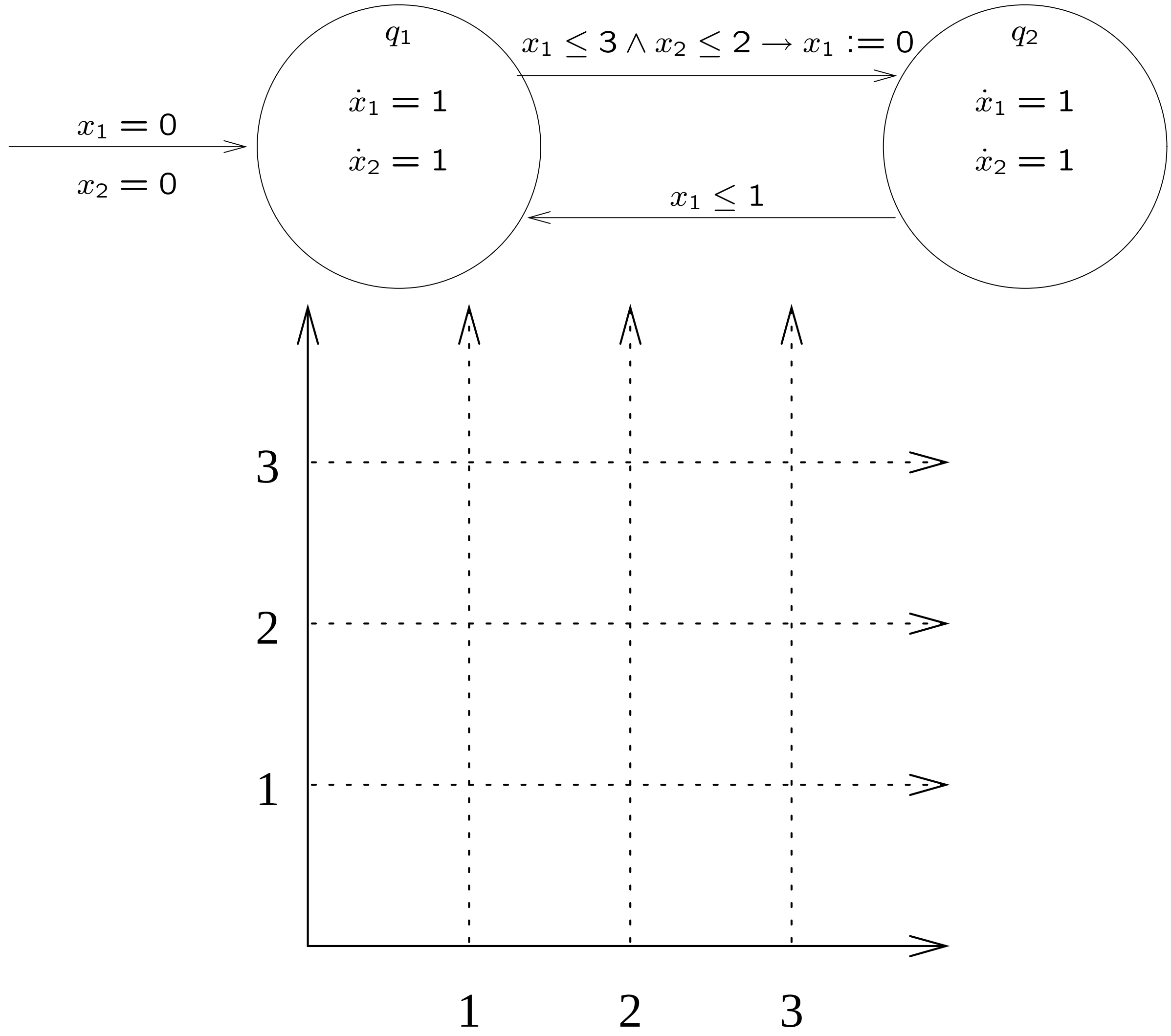
Un automa temporizzato, con un insieme di stati finali $F = \{\{q_i\} \times \widehat{F_{q_i}}\}_{i=1}^{m}$, dove $F_{q_i} \in \Phi(X)$ si puo' vedere come un sistema di transizione $T = (S, \Sigma, \rightarrow, S_0, S_F)$ dove

1. $S = \boldsymbol{Q} \times \boldsymbol{X}$
2. $\Sigma = E \cup \{\tau\}$, τ e' un simbolo che denota il passaggio del tempo
3. $((q, x), e, (q', x')) \in\rightarrow$ if $e = (q, q') \in E$, $G_e(x) = True$ e $x' \in R(e, x)$
4. $((q, x), \tau, (q', x')) \in\rightarrow$ if $q = q'$, $\exists t \geq 0 : x' = x + t(1, \ldots, 1)$
5. $S_0 = Init$
6. $S_F = F$

Automi Temporizzati

Esempio di automa a tempo.

T_1 :



Automi Temporizzati

- $Q = \{q\}$, $\boldsymbol{Q} = \{q_1, q_2\}$
- $X = \{x_1, x_2\}$, $\boldsymbol{X} = R^2$
- $Init = \{(q_1, 0, 0)\}$
- $f(q, x) = (1, 1)$, $\forall (q, x)$
- $Inv(q) = R^2$, $\forall q \in \boldsymbol{Q}$
- $E = \{(q_1, q_2), (q_2, q_1)\}$
- $G((q_1, q_2)) = \{x \in R^2 : (x_1 \leq 3) \wedge (x_2 \leq 2)\}$, $G((q_2, q_1)) = \{x \in R^2 : (x_1 \leq 1)\}$
- $R((q_1, q_2), x) = \{(0, x_2)\}$, $R((q_2, q_1), x) = \{(x_1, x_2)\}$

Bisimulazione di Automi Temporizzati

Obiettivo: mostrare che gli automi temporizzati hanno una bisimulazione finita.

Senza perdita di generalita' si possono considerare tutte le costanti come intere. Sia T un sistema di transizione definito da un automa temporizzato H e $\lambda > 0$ un razionale. Sia H_λ l'automa temporizzato ottenuto sostituendo tutte le costanti c in H con λc. Sia T_λ il sistema di transizione associato con H_λ.

Proposizione. T e T_λ sono bisimili.

Compito. Dimostrarlo.

Percio' consideriamo il sistema bisimile T_λ, dove λ e' il multiplo comune di tutti i denominatori delle costanti non intere.

Bisimulazione di Automi Temporizzati

Sia c_i la costante maggiore con cui si confronta x_i. Nell'es. $c_1 = 3, c_2 = 2$.

Sia $\lfloor x_i \rfloor$ la parte intera di x_i e $\langle x_i \rangle$ la parte frazionaria di x_i: $x_i = \lfloor x_i \rfloor + \langle x_i \rangle$, $\lfloor x_i \rfloor \in Z$, $\langle x_i \rangle \in [0, 1)$.

Si consideri la relazione binaria $\sim \subseteq \boldsymbol{Q} \times \boldsymbol{Q}$, dove $(q, x) \sim (q', x')$ se

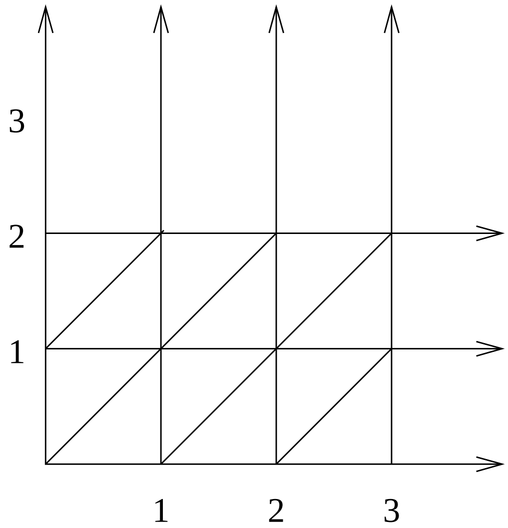
1. $q = q'$
2. $\forall x_i, \lfloor x_i \rfloor = \lfloor x'_i \rfloor$ oppure $(x_i > c_i) \wedge (x'_i > c_i)$
3. $\forall x_i, x_j$ con $x_i \leq c_i$ e $x_j \leq c_j$
$$(\langle x_i \rangle \leq \langle x_j \rangle) \Leftrightarrow (\langle x'_i \rangle \leq \langle x'_j \rangle)$$
4. $\forall x_i$ con $x_i \leq c_i$
$$(\langle x_i \rangle = 0) \Leftrightarrow (\langle x'_i \rangle = 0)$$

Proposizione. $\sim$ e' una relazione d'equivalenza.

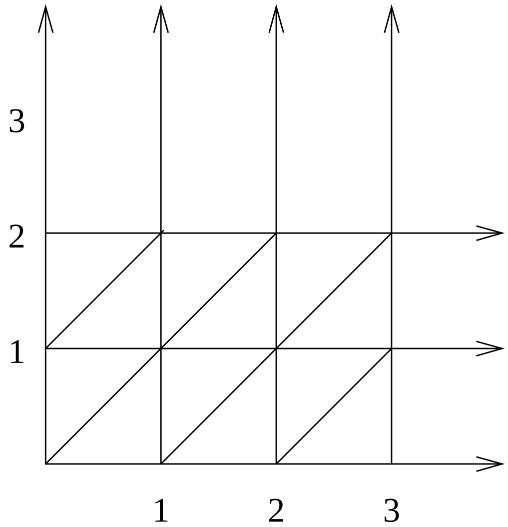
Compito. Dimostrarlo.

Bisimulazione di Automi Temporizzati

Classi di equivalenza per q_1:



Classi di equivalenza per q_2:



Bisimulazione di Automi Temporizzati

Le classi di equivalenza sono

- triangoli aperti
- segmenti o semirette aperti
- rettangoli aperti
- punti

Nell'esempio il numero di classi d'equivalenza e': $2 \times$ (12 punti + 30 linee + 18 regioni) = 120.

Bisimulazione di Automi Temporizzati

Teorema. $\sim$ e' una bisimulazione.

Dobbiamo dimostrare che:

1. $Init$ e' un'unione di classi d'equivalenza

2. F e' un'unione di classi d'equivalenza

3. Se P e' un'unione di classi d'equivalenza e $e \in E$, $Pre_e(P)$ e' un'unione di classi d'equivalenza.

4. Se P e' un'unione di classi d'equivalenza, $Pre_\tau(P)$ e' un'unione di classi d'equivalenza.

Bisimulazione di Automi Temporizzati

$Init$ e F sono unioni di classi d'equivalenza..

Se $\delta \in \Phi(X)$, $\widehat{\delta} = \{x \in \boldsymbol{X}\colon \delta(x) = True\}$ e' un'unione di classi d'equivalenza (solo sulle variabili X), poiche' $\widehat{\delta}$ puo' scriversi come unione e intersezione d'insiemi della forma $\{x_i \geq c\}$, $\{x_i \leq c\}$, $\{x_i < c\}$, $\{x_i > c\}$, $\{x_i = c\}$.

Tutti questi insiemi sono unioni di classi d'equivalenza sulle variabili in X.

Bisimulazione di Automi Temporizzati

Lemma. Se P e' un'unione di classi d'equivalenza

$$R^{-1}(e,P) = \{(q,x) \in \mathbf{Q} \times \mathbf{X} : \exists (q',x') \in P, e = (q,q'), x' \in R(e,x)\}$$

e' un'unione di classi d'equivalenza.

Proposizione. Se P e' un'unione di classi d'equivalenza,

$$Pre_{(q,q')}(P) = R^{-1}((q,q'),P) \cap (\{q\} \times G((q,q')))$$

e' un'unione di classi d'equivalenza.

Proposizione. Se P e' un'unione di classi d'equivalenza,

$$\begin{aligned} Pre_\tau(P) \;=\; & \{(q,x) \in \mathbf{Q} \times \mathbf{X} : \\ & \exists (q',x') \in P, t \geq 0, q = q', x' = x + t(1,\ldots,1)\} \end{aligned}$$

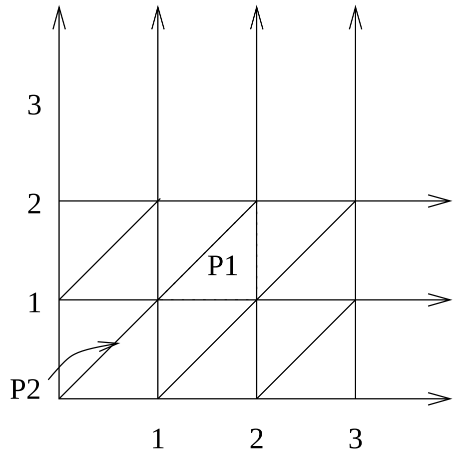
e' un'unione di classi d'equivalenza.

Bisimulazione di Automi Temporizzati

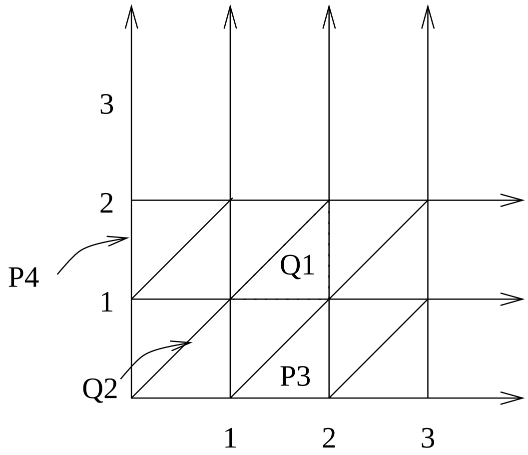
Dimostrazione per esempio :-)

Siano $P_1, P_2, P_3, P_4, Q_1, Q_2$ come in figura:

Classi di equivalenza per q_1:



Classi di equivalenza per q_2:



Bisimulazione di Automi Temporizzati

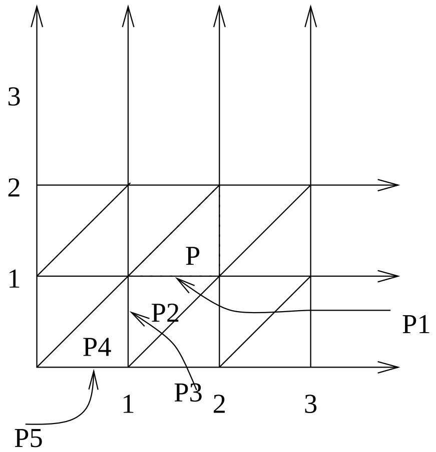
$e_1 = (q_1, q_2)$, $e_2 = (q_2, q_1)$

$$
\begin{array}{rcl}
Pre_{e_1}(P_1) & = & \emptyset \\
Pre_{e_2}(P_1) & = & Q_1 \cap (\{q_2\} \times \{x_1 \leq 1\}) \\
 & = & \emptyset \\
Pre_{e_1}(P_2) & = & \emptyset \\
Pre_{e_2}(P_2) & = & Q_2 \cap (\{q_2\} \times \{x_1 \leq 1\}) \\
 & = & Q_2 \\
Pre_{e_1}(P_3) & = & R^{-1}((q_1, q_2), P_3) \cap (\{q_1\} \times G((q_1, q_2))) \\
 & = & \emptyset \cap (\{q_1\} \times \{x_1 \leq 3 \wedge x_2 \leq 2\}) \\
 & = & \emptyset \\
Pre_{e_2}(P_3) & = & \emptyset \\
Pre_{e_1}(P_4) & = & \{q_1\} \times (\{x_1 \geq 0 \wedge 1 < x_2 < 2\} \cap \{x_1 \leq 3 \wedge x_2 \leq 2\}) \\
 & = & \{q_1\} \times \{0 \leq x_1 \leq 3 \wedge 1 < x_2 < 2\} \\
Pre_{e_2}(P_4) & = & \emptyset
\end{array}
$$

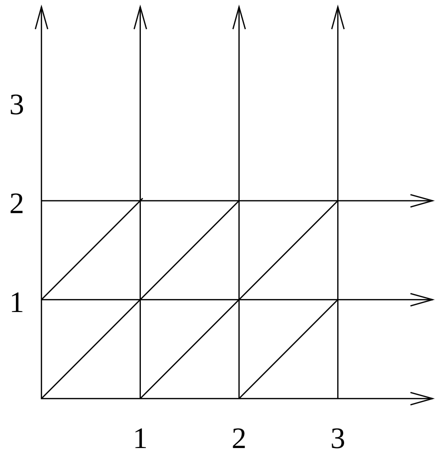
Bisimulazione di Automi Temporizzati

Siano $P, P_1, P_2, P_3, P_4, P_5$ come in figura:

Classi d'equivalenza per q_1:



Classi d'equivalenza per q_2:



$$Pre_\tau(P) = P \cup P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_5$$

Bisimulazione di Automi Temporizzati

Conclusione: i problemi di raggiungibilita' su automi temporizzati possono essere risolti su un insieme di transizione finito, **grafo delle regioni**, con un numero di stati discreti limitato da

$$m(n!)2^n \Pi_{i=1}^{n}(2c_i + 2)$$

(m modi, n orologi).

In generale invece di costruire il grafo delle regioni si puo':

- o calcolare al volo la raggiungibilita' - spesso termina senza aver costruito l'intero grafo delle ragioni

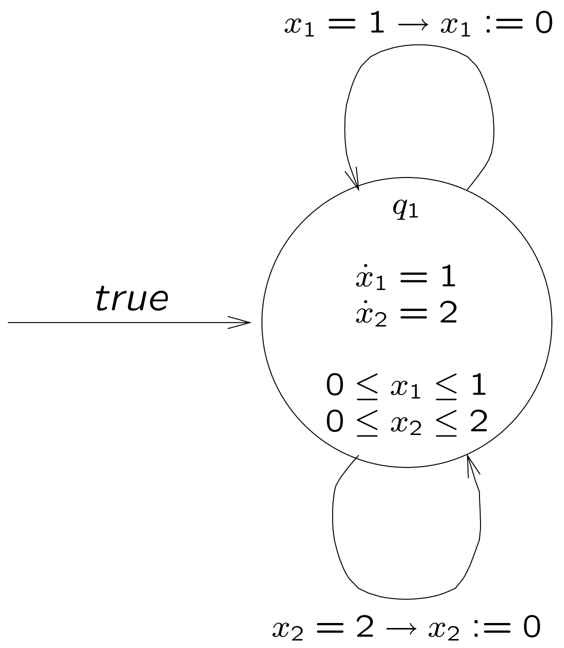
- o calcolare una bisimulazione piu' grezza, ad esempio il quoziente di bisimilarita' che spesso genera meno classi di equivalenza del grafo delle regioni

Ma il problema e' PSPAZIO-completo !

Automi a Pendenza Fissa

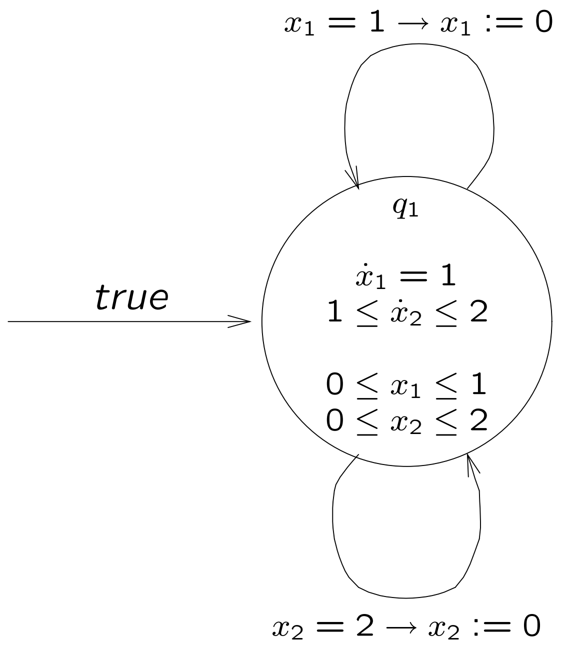
Gli automi a pendenza fissa generalizzano gli automi temporizzati ammettendo orologi del tipo $\dot{x}_i = a_i$, dove a_i e' una costante intera che non varia da modo a modo.

Compito. Esibire una bisimulazione finita per gli automi a pendenza fissa. Calcolare la relazione di bisimilarita' sull'esempio seguente.



Un Automa Rettangolare

Compito. Applicare l'algoritmo di bisimilarita' al seguente automa rettangolare. Che cosa si puo' dedurre circa l'esistenza di uno spazio quoziente finito ?



Bibliografia

1. R. Alur, D. Dill, "A theory of timed automata", Theoretical Computer Science, Vol. 126, 1994, pages 183-235.

2. R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, "The algorithmic analysis of hybrid systems", Theoretical Computer Science, Vol. 138, 1995, pages 3-34.

3. T.A. Henzinger, "The theory of hybrid automata", Proceedings of the 11th Annual Symposium on Logic in Computer Science, IEEE Computer Society Press, 1996, pages 278-292.

4. T.A. Henzinger, P.-H. Ho, H. Wong-Toi, "HyTech: a model checker for hybrid systems", Software Tools for Technology Transfer, Vol. 1, 1997, pages 110-122.

5. R. Alur, T.A. Henzinger, P.-H. Ho, "Automatic symbolic verification of embedded systems", IEEE Transactions on Software Engineering, Vol. 22, 1996, pages 181-201.

6. T.A. Henzinger, P.-H. Ho, H. Wong-Toi, "Algorithmic analysis of nonlinear hybrid systems", IEEE Transactions on Automatic Control, Vol. 43, 1998, pages 540-554.

7. T.A. Henzinger, P.W. Kopke, A. Puri, P. Varaiya, "What's decidable about hybrid automata ?", Journal of Computer and System Sciences, Vol. 57, 1998, pages 94-124.