

Il Problema della Raggiungibilita' per gli Automi Ibridi

Tiziano Villa

Universita' di Verona, Gennaio 2014

Sommario

- Il problema della raggiungibilità
- 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*" (in CTL scritto come $A\Box F$) e' soddisfatta da H se lungo tutte le esecuzioni di H lo stato rimane in F .

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

Altre proprieta':

"*eventually F*" se lungo tutte le esecuzioni di H lo stato a un certo punto raggiunge F (*vivacita' semplice, progresso*; in CTL scritto come $A\Diamond F$).

"*always eventually F*" lo stato visita F infinitamente spesso, sempre eventualmente (*rispondenza, vivacita' ripetuta, equita'*; in CTL scritto come $A\Box A\Diamond F$).

"*eventually always F*" a un certo punto lo stato raggiunge F e vi rimane per sempre, eventualmente sempre (*persistenza*; in CTL scritto come $A\Box A\Diamond F$).

$A\Diamond (F \wedge A\Diamond F)$ lungo tutte le esecuzioni di H ci sono almeno due stati dove vale F .

In LTL si omette il quantificatore A sui percorsi.

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 $M = (Q, \Sigma, \Delta, q_0, F)$ 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

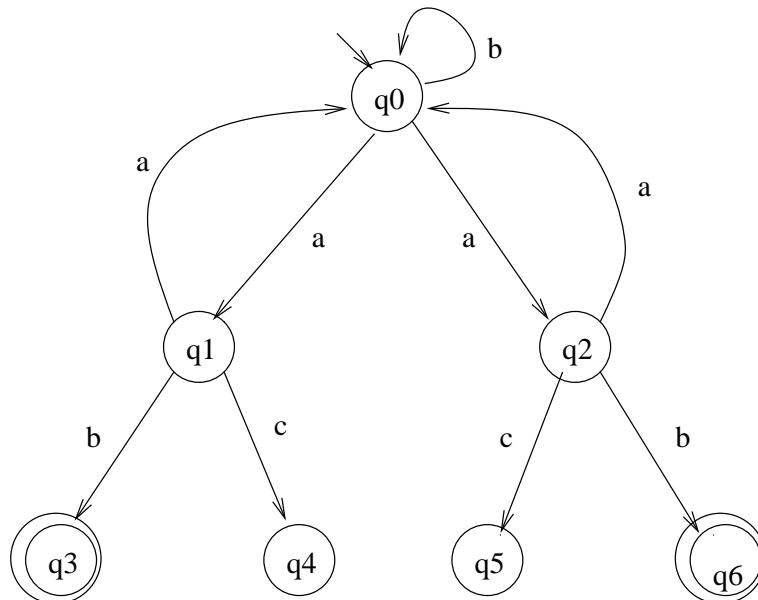
Un automa ibrido $H = (Q, X, Init, f, Inv, E, G, R)$ insieme con una proprietà di sicurezza "always F " è un sistema di transizione dove

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'

```
Raggiungibilita'(T) {  
  Reach0 = S0  
  Reach-1 = ∅  
  i = 0  
  while Reachi ≠ Reachi-1 {  
    Reachi+1 = Reachi ∪  
      {s' ∈ S : ∃s ∈ Reachi, σ ∈ Σ con (s, σ, s') ∈ →}  
    i = i + 1  
  }  
}
```

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 proprietà simili, poiché 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 è una relazione d'equivalenza che preserva la relazione di transizione.

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

1. riflessiva: $(s, s) \in \sim \quad \forall s \in S$
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**, cioè 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** è

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

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

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

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 $T = (S, \Sigma, \rightarrow, S_0, S_F)$, 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 $s_1 \sim s_2$.

Bisimulazione

La precedente definizione di bisimulazione si puo' riscrivere nel seguente modo.

Dati $T = (S, \Sigma, \rightarrow, S_0, S_F)$ e una relazione d'equivalenza \sim su S , \sim e' una **bisimulazione** se per tutte le coppie s_1, s_2 tali che $s_1 \sim s_2$:

1. $s_1 \in S_0 \Rightarrow s_2 \in S_0$
2. $s_1 \in S_F \Rightarrow s_2 \in S_F$
3. $(s_1, \sigma, s'_1) \in \rightarrow \Rightarrow \exists s'_2 [s'_1 \sim s'_2 \wedge (s_2, \sigma, s'_2) \in \rightarrow]$

Si puo' parafrasare il terzo punto dicendo che se sotto σ da uno stato $s_1 \in S_i$ c'e' una transizione in uno stato della classe d'equivalenza S_j , allora da ogni altro stato $s_2 \in S_i$ sotto σ c'e' una transizione in uno stato di S_j .

Bisimulazione

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

Compito: Dimostrare la proposizione.

Bisimulazione

Alcuni fatti per aiutare l'intuizione:

- Se \sim e' una bisimulazione, T e T/\sim si dicono bisimili.
- La relazione d'uguaglianza e' una bisimulazione.
- Sistemi di transizione bisimili generano le stesse successioni di transizioni, cioe' gli stessi linguaggi.
- Se \sim e' una bisimulazione, non distinguiamo tra gli elementi di una classe d'equivalenza.
- Se uno stato in S_F e' raggiungibile da uno stato in S_0 , uno stato in S_F/\sim e' raggiungibile da uno stato in S_0/\sim .

Bisimulazione

Svolgimento del compito precedente.

Data la definizione:

Una relazione d'equivalenza \sim e' una **bisimulazione** se e solo se per tutte le coppie s_1, s_2 tali che $s_1 \sim s_2$:

1. $s_1 \in S_0 \Rightarrow s_2 \in S_0$
2. $s_1 \in S_F \Rightarrow s_2 \in S_F$
3. $(s_1, \sigma, s'_1) \in \rightarrow \Rightarrow \exists s'_2 [s'_1 \sim s'_2 \wedge (s_2, \sigma, s'_2) \in \rightarrow]$

dimostrare la proposizione precedente:

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

Bisimulazione

Dimostrazione di \Rightarrow 1.

- Dato che S_0 e' un'unione di classi d'equivalenza, se $s_1 \in S_0$ e $s_1 \sim s_2$ si ha che anche $s_2 \in S_0$, perche' S_0 contiene l'intera classe d'equivalenza di s_1

Dimostrazione di \Rightarrow 2.

Come nel caso precedente.

Dimostrazione di \Rightarrow 3.

- Data la coppia $s_1 \sim s_2$ sia $(s_1, \sigma, s'_1) \in \rightarrow$, vogliamo mostrare che $\exists s'_2$ tale che $s'_1 \sim s'_2$ e $(s_2, \sigma, s'_2) \in \rightarrow$
- Sia $C_{s'_1}$ la classe di equivalenza di s'_1 e poniamo $P = C_{s'_1}$
- Siccome $P = C_{s'_1}$ e' una classe di equivalenza (caso speciale di un'unione di classi di equivalenza), $Pre_\sigma(P)$ e' un'unione di classi di equivalenza, e in particolare $s_2 \in Pre_\sigma(C_{s'_1})$ (da $s_1 \in Pre_\sigma(C_{s'_1})$ e $s_1 \sim s_2$)
- $s_2 \in Pre_\sigma(C_{s'_1})$ vuol dire che $\exists s'_2 \in C_{s'_1}$ tale che sia $(s_2, \sigma, s'_2) \in \rightarrow$, e inoltre $s'_1 \sim s'_2$ dato che per costruzione $P = C_{s'_1}$ coincide con la classe di equivalenza di s'_1

Bisimulazione

Dimostrazione di $\Leftarrow 1$.

- Sia $s_1 \in S_0$, poiché S_0 è un'unione di classi di equivalenza, in particolare S_0 contiene la classe d'equivalenza di s_1 e perciò se $s_1 \sim s_2$ si ha che $s_2 \in S_0$

Dimostrazione di $\Leftarrow 1$.
Come nel caso precedente.

Dimostrazione di $\Leftarrow 3$.

- Sia P un'unione di classi d'equivalenza. $s_1 \in Pre_\sigma(P) \Rightarrow \exists s'_1 \in P : (s_1, \sigma, s'_1) \in \rightarrow$
- $(s_1, \sigma, s'_1) \in \rightarrow \wedge s_1 \sim s_2 \Rightarrow \exists s'_2 : s'_1 \sim s'_2 \wedge (s_2, \sigma, s'_2) \in \rightarrow$
- $s'_1 \sim s'_2$ e P unione di classi d'equivalenza $\Rightarrow s'_2 \in P$
- $s'_2 \in P \wedge (s_2, \sigma, s'_2) \in \rightarrow \Rightarrow s_2 \in Pre_\sigma(P)$
- Poiché $\forall s_2 : s_1 \sim s_2$ vale $s_2 \in Pre_\sigma(P)$, $Pre_\sigma(P)$ è un'unione di classi d'equivalenza.

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 $\forall \sigma \in \Sigma$:

$$1. s_1 \sim s_2 \wedge s_1 \in S_0 \Rightarrow s_2 \in S'_0$$

$$2. s_1 \sim s_2 \wedge s_2 \in S'_0 \Rightarrow s_1 \in S_0$$

$$3. s_1 \sim s_2 \wedge s_1 \in S_F \Rightarrow s_2 \in S'_F$$

$$4. s_1 \sim s_2 \wedge s_2 \in S'_F \Rightarrow s_1 \in S_F$$

$$5. s_1 \sim s_2 \wedge (s_1, \sigma, s'_1) \in \rightarrow \Rightarrow \exists s'_2 [s'_1 \sim s'_2 \wedge (s_2, \sigma, s'_2) \in \rightarrow']$$

$$6. s_1 \sim s_2 \wedge (s_2, \sigma, s'_2) \in \rightarrow' \Rightarrow \exists s'_1 [s'_1 \sim s'_2 \wedge (s_1, \sigma, s'_1) \in \rightarrow]$$

Bisimulazione

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.

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 $s_2 \sim s_1$.

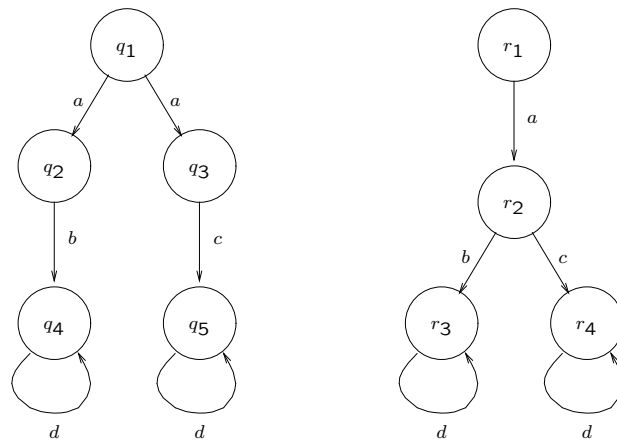
Per avere una bisimulazione bisogna che $\sim' \equiv \sim^{-1}$, cioe' \sim dev'essere una simulazione in entrambe le direzioni.

Simulazione

Bisimulazione \implies Simulazione \implies 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 \sim su T con $q \sim r$.

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'

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

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 $S/ \sim = \{S_0 \setminus S_F, S_F \setminus S_0, S_0 \cap S_F, S \setminus (S_0 \cup S_F)\}$.

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 $\forall \sigma \in \Sigma$, $P \cap \text{Pre}_\sigma(P')$ e' uguale a P o a $\emptyset \Rightarrow \text{Pre}_\sigma(P')$ e' un'unione di classi d'equivalenza

4. Anche se P e' una classe d'equivalenza singola, $Pre_\sigma(P)$ potrebbe essere l'unione di piu' classi d'equivalenza, ad es. ci potrebbero essere P' e γ tali che $Pre_\gamma(P') \cap Pre_\sigma(P) = Pre_\gamma(P')$ cosi' da partizionare $Pre_\sigma(P)$ in $Pre_\gamma(P')$ e $Pre_\sigma(P) \setminus Pre_\gamma(P')$.

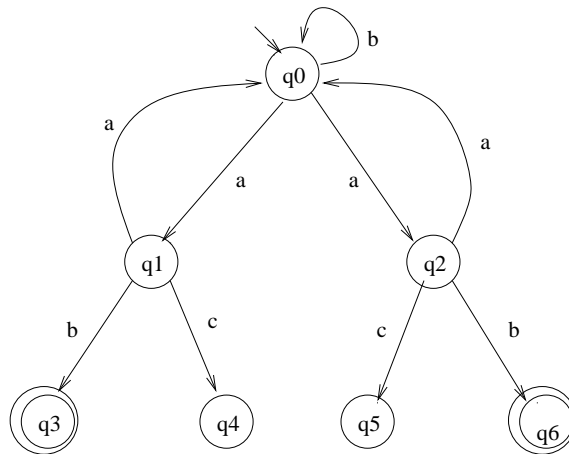
Calcolo del Quoziente di Bisimilarita'

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'.

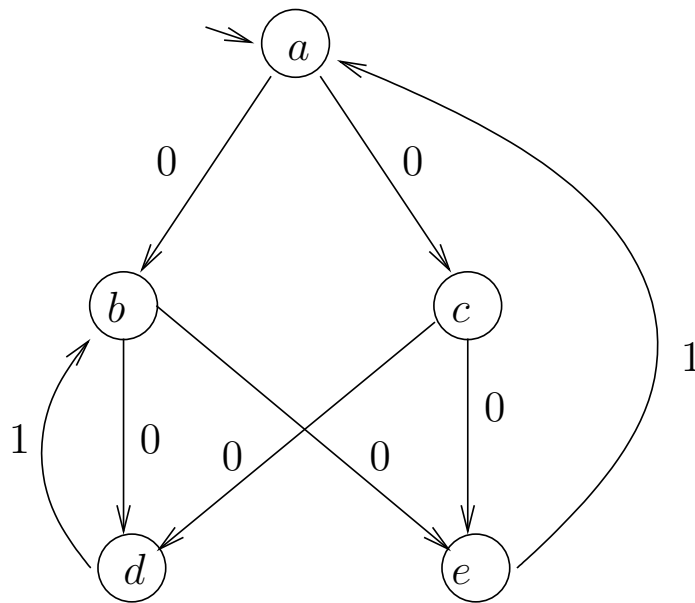
Esempio. Quoziente di bisimilarita' del precedente automa finito: $\sim = \{\{q_0\}, \{q_1, q_2\}, \{q_3, q_6\}, \{q_4, q_5\}\}$.

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



Quoziente di Bisimilarita': T e T/R

Problema: si consideri il seguente sistema di transizione T :



- stati: a, b, c, d, e ; a stato iniziale e tutti gli stati finali;
- transizione da a a b : con evento 0,
transizione da a a c : con evento 0,
transizione da b a d : con evento 0,
transizione da b a e : con evento 0,
transizione da c a d : con evento 0,
transizione da c a e : con evento 0,
transizione da d a b : con evento 1,
transizione da e a a : con evento 1.

1. Data la relazione d'equivalenza $R_0 = \{\{a, b, c, d, e\}\}$, si mostri il grafo di T/R_0 .

Si verifichi se T simula T/R_0 e viceversa se T/R_0 simula T (esibendo la relazione di simulazione se esiste, o la ragione per cui non esiste).

Traccia.

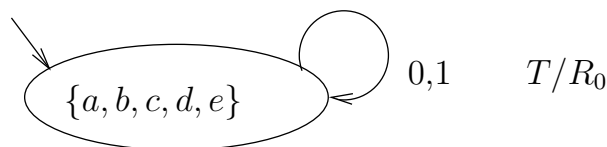
Dati $T_1 = (S_1, \Sigma, \rightarrow_1, S_{0_1}, S_{F_1})$ e $T_2 = (S_2, \Sigma, \rightarrow_2, S_{0_2}, S_{F_2})$, una **simulazione** di T_1 da parte di T_2 e' una relazione binaria $\sim \subseteq S_1 \times S_2$ tale che $\forall \sigma \in \Sigma$:

- (a) $\forall s_{0_1} \in S_{0_1} \exists s_{0_2} \in S_{0_2}$ tale che $s_{0_1} \sim s_{0_2}$
- (b) $s_1 \sim s_2 \wedge (s_1, \sigma, s'_1) \in \rightarrow_1 \Rightarrow \exists s'_2 [s'_1 \sim s'_2 \wedge (s_2, \sigma, s'_2) \in \rightarrow_2]$

(definizione adattata da quella della bisimulazione di sistemi di transizione)

Si noti che:

- T/R_i simula T , per $i = 0, \dots, 4$, come spiegato nel punto finale. Ogni stato s in T e' simulato dallo stato B in T/R_i tale che $s \in B$.

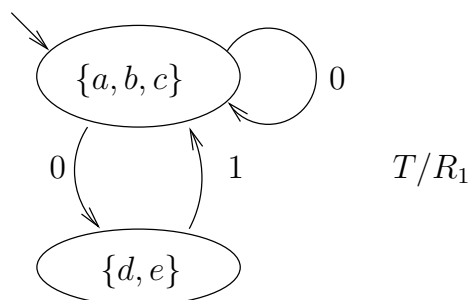


- T non simula T/R_0 ; ad es. non c'e' una transizione sotto 1 dallo stato iniziale a di T , mentre c'e' una transizione sotto 1 dallo stato iniziale $\{a, b, c, d, e\}$ di T/R_0 .

2. Data la relazione d'equivalenza $R_1 = \{\{a, b, c\}, \{d, e\}\}$, si mostri il grafo di T/R_1 .

Si verifichi se T simula T/R_1 e viceversa se T/R_1 simula T .

Traccia.

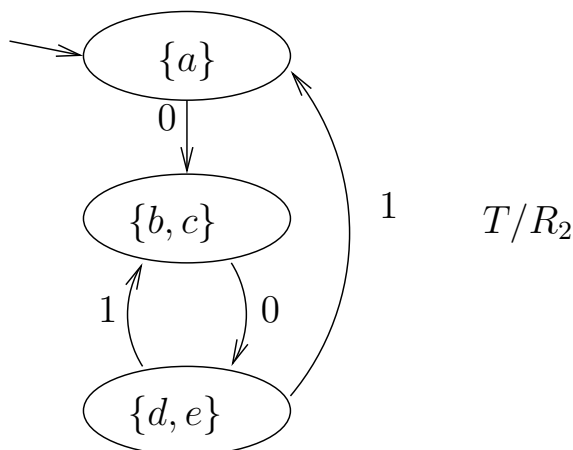


T non simula T/R_1 ; a dovrebbe simulare $\{a, b, c\}$, ma quando $\{a, b, c\}$ sotto 0 va in $\{d, e\}$, a sotto 0 va in b o c pero' ne' b ne' c simulano $\{d, e\}$ (non hanno transizioni sotto 1).

3. Data la relazione d'equivalenza $R_2 = \{\{a\}, \{b, c\}, \{d, e\}\}$, si mostri il grafo di T/R_2 .

Si verifichi se T simula T/R_2 e viceversa se T/R_2 simula T .

Traccia.

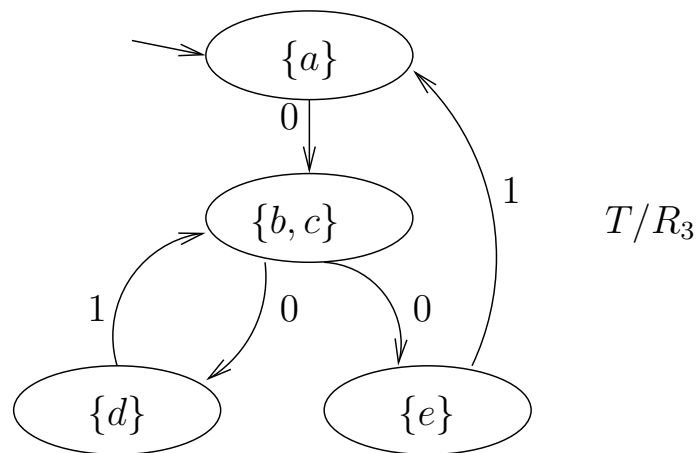


T non simula T/R_2 ; sotto l'ingresso 00 T/R_2 va in $\{d, e\}$ e T va o in d o in e , ma ne' d ne' e simulano $\{d, e\}$. Infatti $\{d, e\}$ puo' produrre la stringa 1010 che e non puo' produrre, inoltre $\{d, e\}$ puo' produrre la stringa 1001 che d non puo' produrre.

4. Data la relazione d'equivalenza $R_3 = \{\{a\}, \{b, c\}, \{d\}, \{e\}\}$, si mostri il grafo di T/R_3 .

Si verifichi se T simula T/R_3 e viceversa se T/R_3 simula T .

Traccia.



T simula T/R_3 , come indicato dalla seguente relazione di simulazione

$$R'_{T/R_3-T} = \{(\{a\}, a), (\{b, c\}, b), (\{d\}, d), (\{e\}, e)\},$$

oppure da

$$R''_{T/R_3-T} = \{(\{a\}, a), (\{b, c\}, c), (\{d\}, d), (\{e\}, e)\},$$

la cui unione

$$R_{T/R_3-T} = \{(\{a\}, a), (\{b, c\}, b), (\{b, c\}, c), (\{d\}, d), (\{e\}, e)\}$$

da' la relazione di simulazione massima.

5. Data la relazione d'equivalenza $R_4 = \{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$, si mostri il grafo di T/R_4 .

Si verifichi se T simula T/R_4 e viceversa se T/R_4 simula T .

Traccia.

$$T/R_4 \equiv T.$$

T simula T/R_4 poiche' i due grafi sono isomorfi.

6. Si traggano delle conclusioni sull'esistenza di una simulazione tra T e T/R , e viceversa.

Traccia.

Se R e' una relazione d'equivalenza su T , e' sempre vero che T/R simula T . Ogni stato s in T e' simulato dallo stato B in T/R tale che $s \in B$. Dato che una relazione d'equivalenza partiziona gli stati di T in blocchi disgiunti, per ogni stato s in T c'e' un unico blocco B di T/R che contiene s .

Nell'altro verso in generale non e' vero che T simuli T/R . Cio' avviene solo quando la relazione di equivalenza e' stata definita in modo da preservare la funzione di transizione, intuitivamente quando gli stati accorpati in un medesimo blocco della relazione di equivalenza generano i medesimi linguaggi, cioe' sono equivalenti come comportamento.

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

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

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), $Q = \{q_1, \dots, q_m\}$
- $X = \{x_1, \dots, x_n\}$, $\mathbf{X} = R^n$
- $Init = \{\{q_i\} \times \widehat{Init_{q_i}(x)}\}_{i=1}^m$, 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 $Inv_q(x) \in \Phi(X)$, $\forall q \in Q$
- $E \subseteq Q \times Q$
- $G(e, x) = \widehat{G_e(x)}$, dove $G_e(x) \in \Phi(X)$, $\forall e = (q, q') \in E$
- $R(e, x)$ o lascia x_i invariato o lo azzerava, $\forall e \in E$

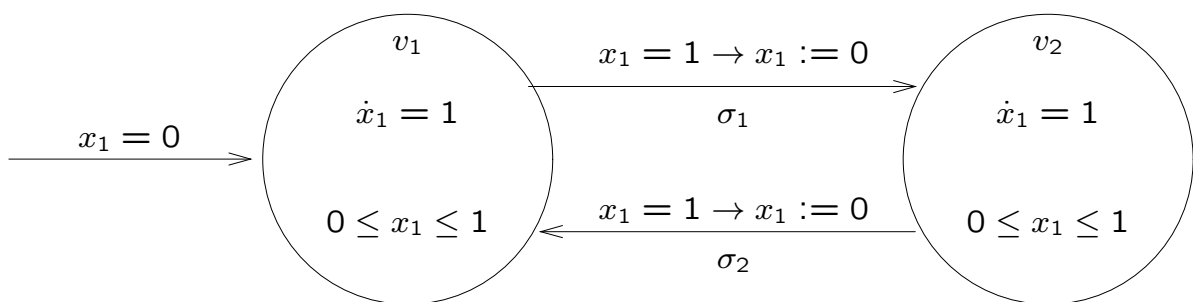
Per semplicita' nel costruire la bisimulazione si assumera'

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

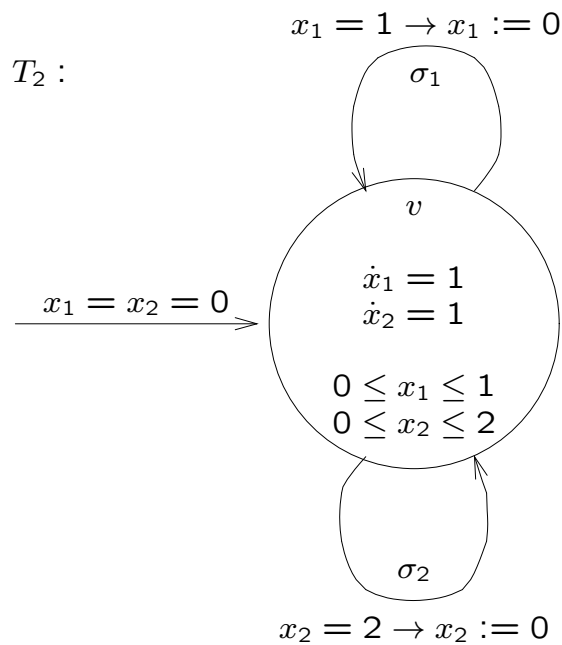
Automi Temporizzati

Esempio di automa a tempo con 1 orologio.

T_1 :



Esempio di automa a tempo con 2 orologi.



Automi Temporizzati

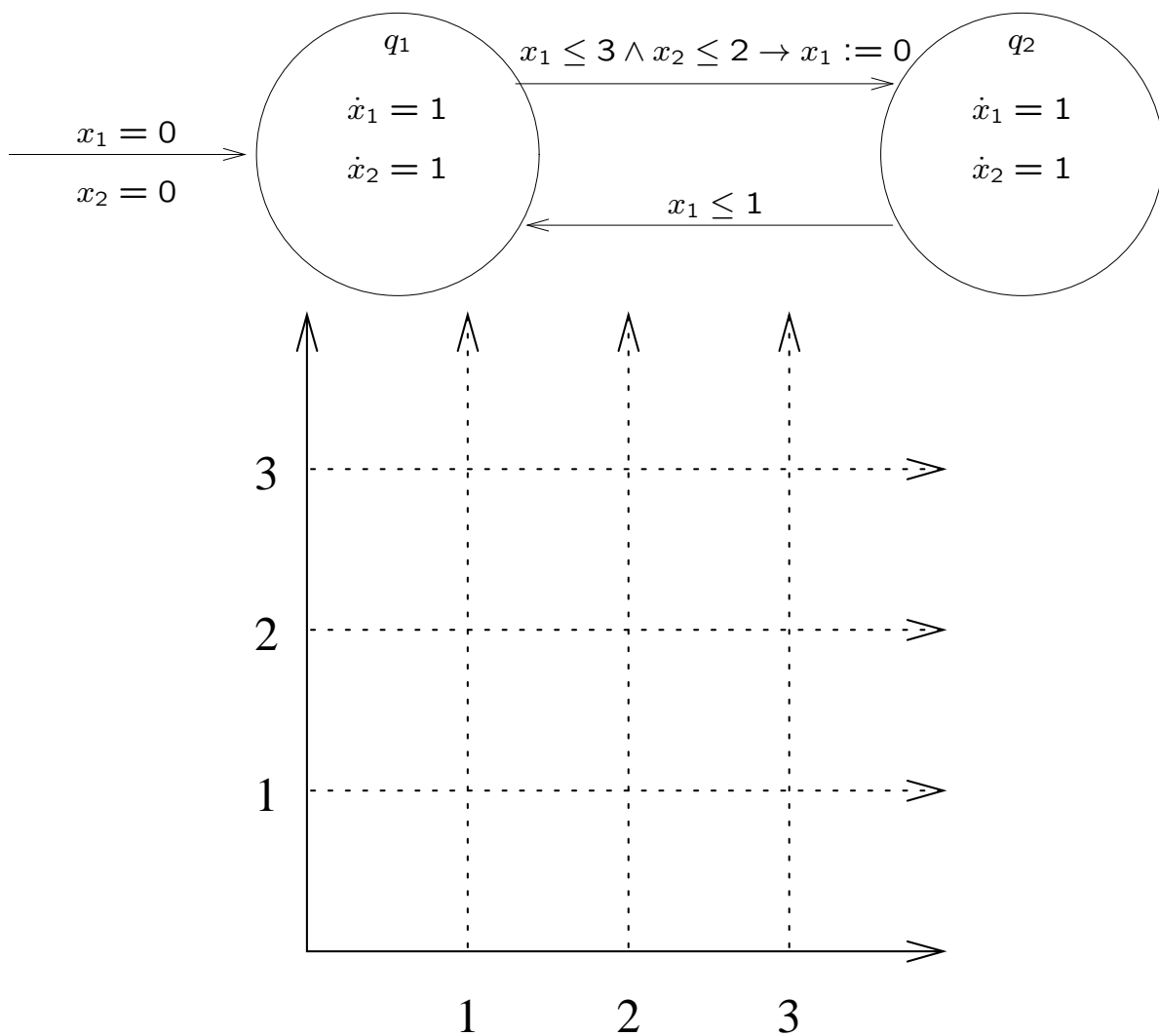
Un automa temporizzato, con un insieme di stati finali $F = \{\{q_i\} \times \widehat{F}_{q_i}\}_{i=1}^m$, dove $F_{q_i} \in \Phi(X)$ si puo' vedere come un sistema di transizione $T = (S, \Sigma, \rightarrow, S_0, S_F)$ dove

1. $S = Q \times X$
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 $q = q'$, $\exists t \geq 0 : x' = x + t(1, \dots, 1)$
5. $S_0 = Init$
6. $S_F = F$

Automi Temporizzati

Esempio di automa a tempo.

T_1 :



Automi Temporizzati

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

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'automata 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 : $x_i = \lfloor x_i \rfloor + \langle x_i \rangle$, $\lfloor x_i \rfloor \in \mathbb{Z}$, $\langle x_i \rangle \in [0, 1)$.

Si consideri la relazione binaria $\sim \subseteq (\mathbb{Q} \times \mathbf{X}) \times (\mathbb{Q} \times \mathbf{X})$, 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 $x_i \leq c_i$

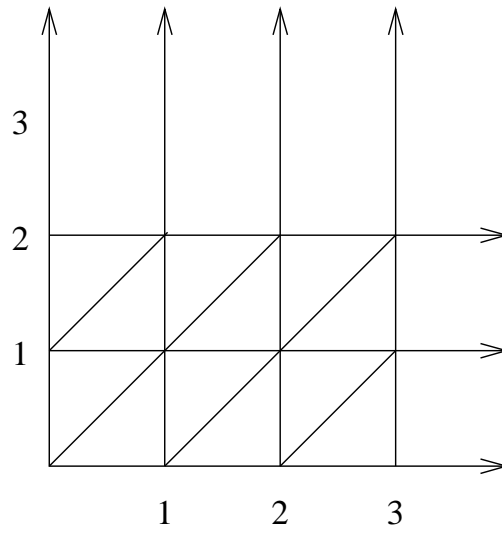
$$(\langle x_i \rangle = 0) \Leftrightarrow (\langle x'_i \rangle = 0)$$

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

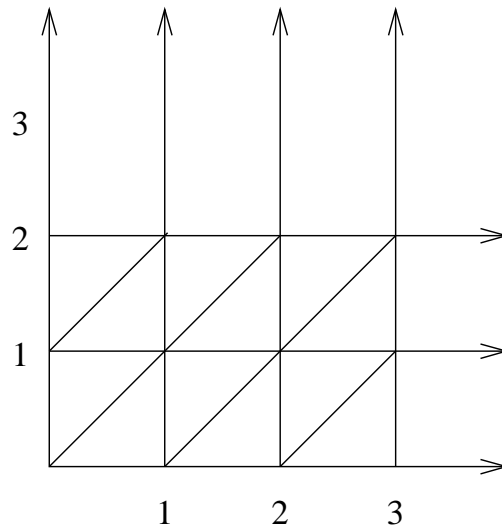
Compito. Dimostrarlo.

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': $2 \times (12 \text{ punti} + 30 \text{ linee} + 18 \text{ regioni}) = 120$.

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 $\delta \in \Phi(X)$, $\hat{\delta} = \{x \in \mathbf{X}: \delta(x) = True\}$ e' un'unione di classi d'equivalenza (solo sulle variabili X), poiche' $\hat{\delta}$ 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,

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

e' un'unione di classi d'equivalenza.

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

$$Pre_{\tau}(P) = \{(q, x) \in \mathbf{Q} \times \mathbf{X} : \\ \exists (q', x') \in P, t \geq 0, q = q', x' = x + t(1, \dots, 1)\}$$

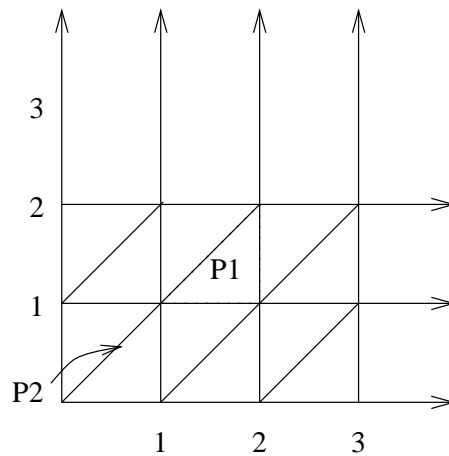
e' un'unione di classi d'equivalenza.

Bisimulazione di Automi Temporizzati

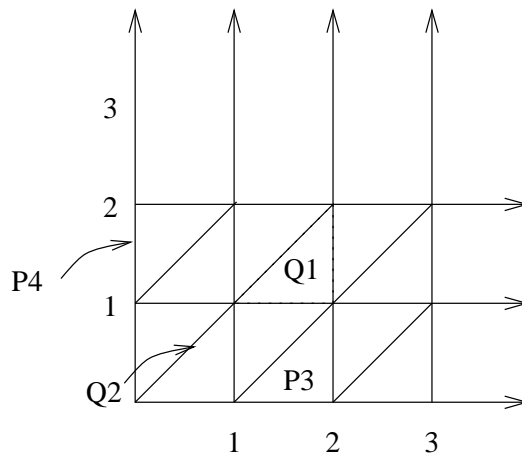
Dimostrazione per esempio :-)

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

Siano date le seguenti definizioni d'insiemi in R^2 :

$$\begin{aligned}P_1 &= (q_1, \{1 < x_2 < x_1 < 2\}), \\P_2 &= (q_1, \{0 < x_2 = x_1 < 1\}), \\P_3 &= (q_2, \{0 < x_2 < 1, 1 < x_1 < 2, x_2 < x_1 - 1\}), \\P_4 &= (q_2, \{1 < x_2 < 2, x_1 = 0\}). \\Q_1 &= (q_2, \{1 < x_2 < x_1 < 2\}), \\Q_2 &= (q_2, \{0 < x_2 = x_1 < 1\}).\end{aligned}$$

Per le transizioni $e_1 = (q_1, q_2)$, $e_2 = (q_2, q_1)$, gl'insiemi Pre si calcolano come segue.

$$\begin{aligned}Pre_{e_1}(P_1) &= \emptyset \\Pre_{e_1}(P_2) &= \emptyset\end{aligned}$$

$Pre_{e_1}(P_1) = Pre_{e_1}(P_2) = \emptyset$, perche' la locazione di P_1 e di P_2 e' q_1 e la transizione $e_1 = (q_1, q_2)$ porta a stati con locazione q_2 .

$$\begin{aligned}Pre_{e_2}(P_3) &= \emptyset \\Pre_{e_2}(P_4) &= \emptyset\end{aligned}$$

$Pre_{e_2}(P_3) = Pre_{e_2}(P_4) = \emptyset$, perche' la locazione di P_3 e di P_4 e' q_2 e la transizione $e_2 = (q_2, q_1)$ porta a stati con locazione q_1 .

Bisimulazione di Automi Temporizzati

$$\begin{aligned}Pre_{e_2}(P_1) &= R^{-1}((q_2, q_1), P_1) \cap (q_2, G((q_2, q_1))) \\ &= Q_1 \cap (q_2, \{x_1 \leq 1\}) \\ &= \emptyset\end{aligned}$$

Per calcolare $Pre_{e_2}(P_1)$, si noti che e_2 lascia la regione invariata e perciò ci si aspetterebbe che tutti gli stati in Q_1 finissero in P_1 per la transizione e_2 ; però la transizione e_2 avviene solo se è vera la guardia $x_1 \leq 1$, per cui

$$\begin{aligned}Pre_{e_2}(P_1) &= Q_1 \cap (q_2, \{x_1 \leq 1\}) \\ &= (q_2, \{1 < x_2 < x_1 < 2\}) \cap (q_2, \{x_1 \leq 1\}) \\ &= (q_2, \{1 < x_2 < x_1 < 2\} \cap \{x_1 \leq 1\}) \\ &= \emptyset.\end{aligned}$$

$$\begin{aligned}Pre_{e_2}(P_2) &= Q_2 \cap (q_2, \{x_1 \leq 1\}) \\ &= Q_2\end{aligned}$$

Similmente, per calcolare $Pre_{e_2}(P_2)$, si noti che e_2 lascia la regione invariata e inoltre che questa volta tutti gli stati in Q_2 finiscono in P_2 per la transizione e_2 , perché la guardia $x_1 \leq 1$ è soddisfatta dagli stati in Q_2 , per cui

$$\begin{aligned}Pre_{e_2}(P_2) &= Q_2 \cap (q_2, \{x_1 \leq 1\}) \\ &= (q_2, \{0 < x_2 = x_1 < 1\} \cap \{x_1 \leq 1\}) \\ &= (q_2, \{0 < x_2 = x_1 < 1\}) \\ &= Q_2.\end{aligned}$$

Bisimulazione di Automi Temporizzati

$$\begin{aligned}Pre_{e_1}(P_3) &= R^{-1}((q_1, q_2), P_3) \cap (q_1, G((q_1, q_2))) \\ &= \emptyset \cap (q_1, \{x_1 \leq 3 \wedge x_2 \leq 2\}) \\ &= \emptyset\end{aligned}$$

Per calcolare $Pre_{e_1}(P_3)$, si noti che e_1 riassegna x_1 a 0, ma in P_3 tutti gli stati hanno $x_1 > 1$ perciò la transizione e_1 non può portare ad alcuno stato in P_3 , per cui

$$Pre_{e_1}(P_3) = \emptyset.$$

$$\begin{aligned}Pre_{e_1}(P_4) &= R^{-1}((q_1, q_2), P_4) \cap (q_1, G((q_1, q_2))) \\ &= (q_1, \{x_1 \geq 0 \wedge 1 < x_2 < 2\} \cap \{x_1 \leq 3 \wedge x_2 \leq 2\}) \\ &= (q_1, \{0 \leq x_1 \leq 3 \wedge 1 < x_2 < 2\})\end{aligned}$$

Per calcolare $Pre_{e_1}(P_4)$, si noti che in P_4 tutti gli stati hanno $x_1 = 0$ sicché potrebbero finire in P_4 tutti gli stati con $x_1 \in [0, \infty)$ e $x_2 \in (1, 2)$; però la transizione e_1 avviene solo se è vera la guardia $x_1 \leq 3$ e $x_2 \leq 2$, per cui

$$\begin{aligned}Pre_{e_1}(P_4) &= (q_1, \{0 \leq x_1 < \infty \wedge 1 < x_2 < 2\} \cap \\ &\quad \{x_1 \leq 3 \wedge x_2 \leq 2\}) \\ &= (q_1, \{0 \leq x_1 \leq 3 \wedge 1 < x_2 < 2\}).\end{aligned}$$

Bisimulazione di Automi Temporizzati

Gl'insiemi predecessori rispetto alla transizione τ (scorrere del tempo) si calcolano come segue:

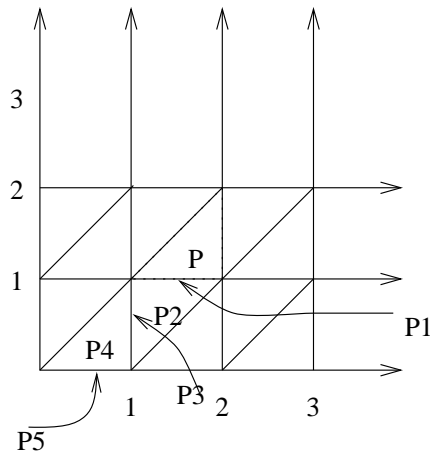
$$\begin{aligned}Pre_{\tau}(P_2) &= P_2 \cup (q_1, \{x_1 = x_2 = 0\}) \\Pre_{\tau}(P_3) &= P_3 \cup (q_2, \{(1 < x_1 < 2) \wedge (x_2 = 0)\}) \\Pre_{\tau}(P_4) &= P_4 \\Pre_{\tau}(P_1) &= P_1 \cup \\&\quad \cup (q_1, \{(1 < x_1 < 2) \wedge (x_2 = 1)\}) \\&\quad \cup (q_1, \{(1 < x_1 < 2) \wedge (0 < x_2 < 1) \wedge \\&\quad \wedge (x_1 - 1 < x_2)\}) \\&\quad \cup (q_1, \{(x_1 = 1) \wedge (0 < x_2 < 1)\}) \\&\quad \cup (q_1, \{(0 < x_1 < 1) \wedge (0 < x_2 < 1) \\&\quad \wedge (x_1 > x_2)\}) \\&\quad \cup (q_1, \{(0 < x_1 < 1) \wedge (x_2 = 0)\})\end{aligned}$$

Tutti gl'insiemi Pre sono unioni di elementi del grafo delle regioni.

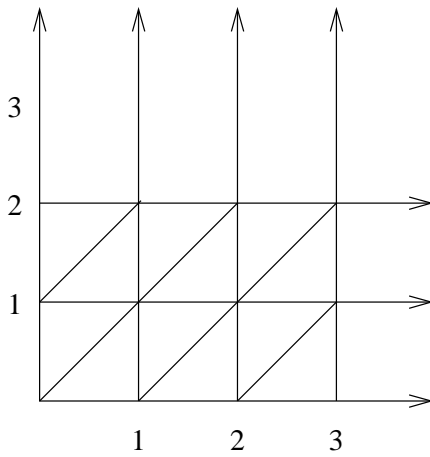
Bisimulazione di Automi Temporizzati

Un altro esempio di calcolo di Pre_τ . 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

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

(m modi, n orologi).

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

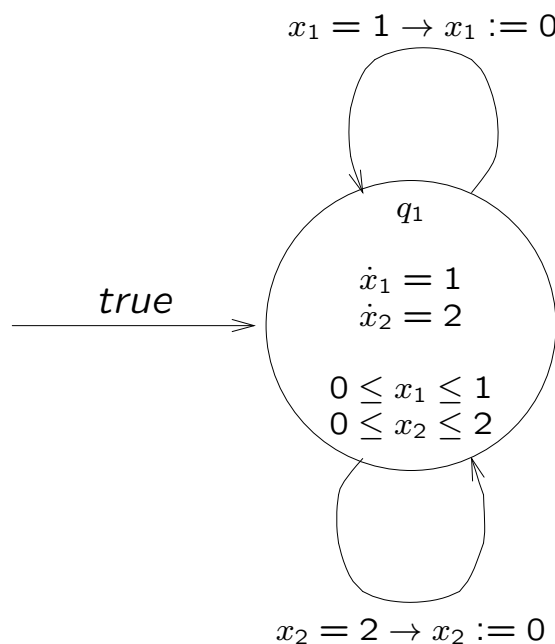
- o calcolare al volo la raggiungibilita' - spesso termina senza aver costruito l'intero grafo delle regioni
- o calcolare una bisimulazione piu' grezza, ad esempio il quoziente di bisimilarita' che spesso genera meno classi di equivalenza del grafo delle regioni

Ma il problema e' PSPACE-completo !

Automi a Pendenza Fissa

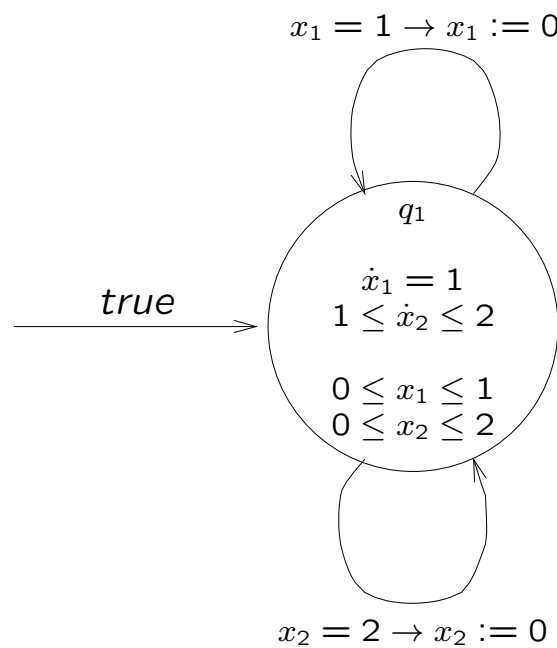
Gli automi a pendenza fissa generalizzano gli automi temporizzati ammettendo orologi del tipo $\dot{x}_i = a_i$, dove a_i e' una costante intera che non varia da modo a modo.

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.