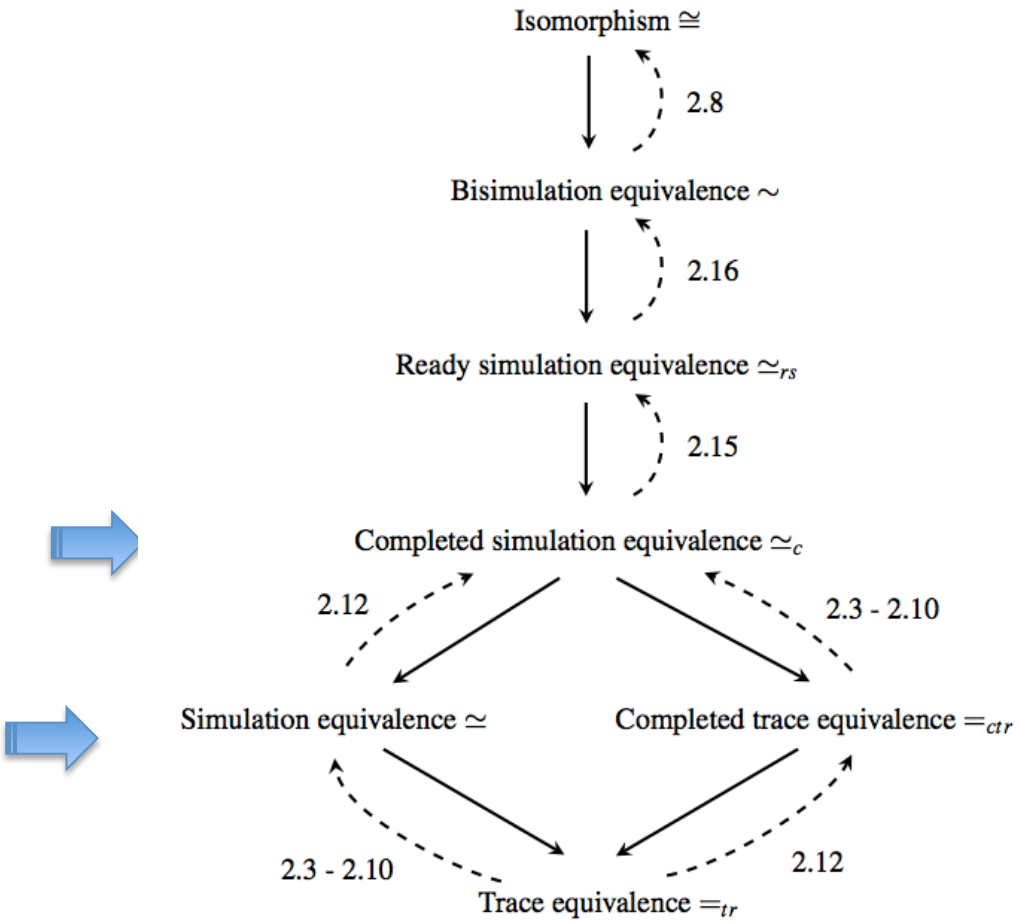
Lezione 5 MSC
Equivalenze forti – seconda parte (di 3)

Roberto Gorrieri

Gerarchia – dove siamo?



Simulation preorder and equiv. (1)

Definition 2.12. Let $TS = (Q, A, \rightarrow)$ be a transition system. A *simulation* is a relation $R \subseteq Q \times Q$ such that if $(q_1, q_2) \in R$ then for all $\mu \in A$

- $\forall q_1'$ such that $q_1 \xrightarrow{\mu} q_1'$, $\exists q_2'$ such that $q_2 \xrightarrow{\mu} q_2'$ and $(q_1', q_2') \in R$

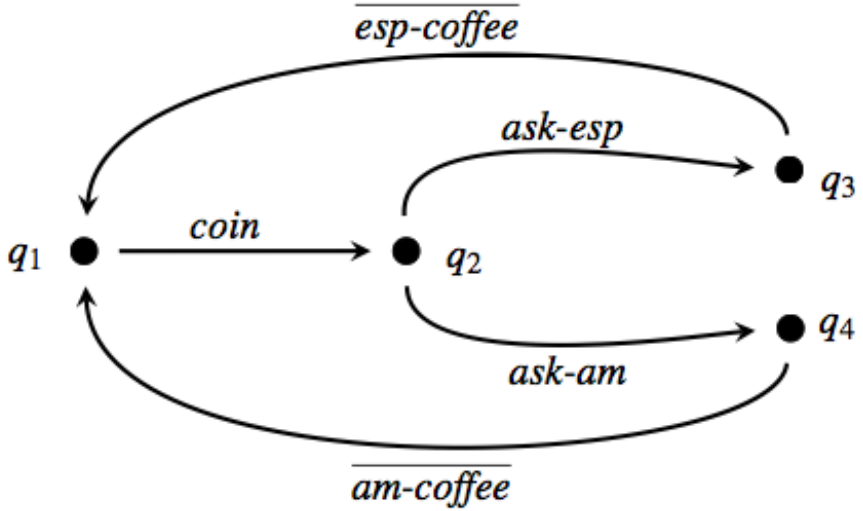
State q is simulated by q', denoted $q \lesssim q'$, if there exists a simulation R such that $(q, q') \in R$. Two states q and q' are *simulation equivalent*, denoted $q \simeq q'$, if $q \lesssim q'$ and $q' \lesssim q$. □

Remark 2.4. The definition above comprises also the case of a simulation between two lts's, say, $TS_1 = (Q_1, A_1, \rightarrow_1)$ and $TS_2 = (Q_2, A_2, \rightarrow_2)$ with $Q_1 \cap Q_2 = \emptyset$ [5]. In such a case, we may consider just one single lts $TS = (Q_1 \cup Q_2, A_1 \cup A_2, \rightarrow_1 \cup \rightarrow_2)$. A simulation $R \subseteq Q_1 \times Q_2$ is also a simulation on $(Q_1 \cup Q_2) \times (Q_1 \cup Q_2)$. We say that the rooted lts $TS_1 = (Q_1, A_1, \rightarrow_1, q_1)$ is simulated by the rooted lts $TS_2 = (Q_2, A_2, \rightarrow_2, q_2)$ if there exists a simulation $R \subseteq Q_1 \times Q_2$ containing the pair (q_1, q_2). □

Simulation preorder and equiv. (2)

- Come si dimostra che q è simulato da q'? Esibire una simulazione R che contenga la coppia (q, q').
- Come si "costruisce" una simulazione? Come si dimostra che una data relazione è una simulazione?
- Quante relazioni di simulazione diverse ci sono per dimostrare che q è simulato da q'?
- Come si dimostra che non esiste una simulazione tra due stati?
- Come si dimostra che q e q' sono simulation equivalent? Esibire due simulazioni R_1 e R_2 tali che (q, q') appartenga a R_1 e (q', q) a R_2.

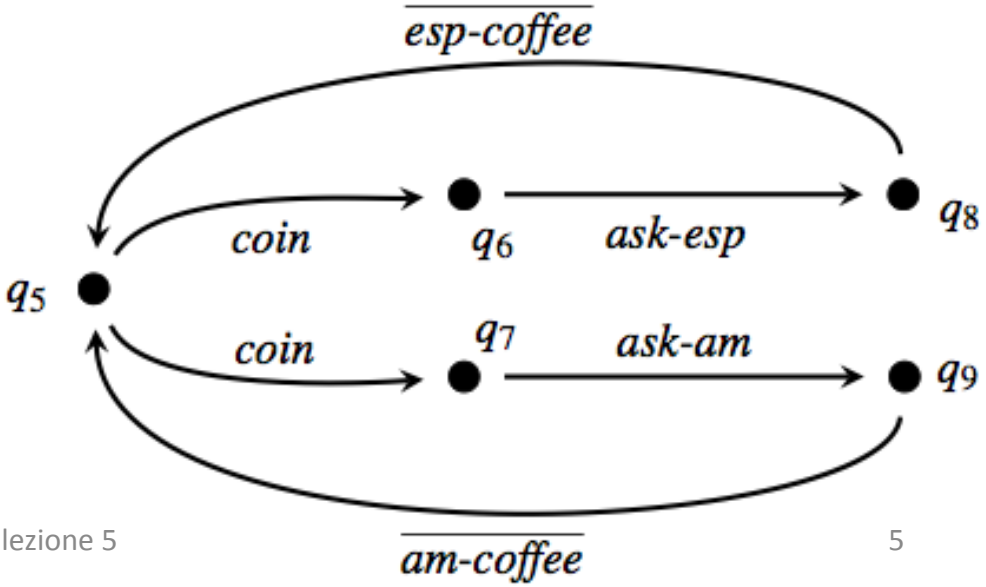
Vending machines



R = {(q_5,q_1), (q_6,q_2), (q_7,q_2), (q_8,q_3), (q_9,q_4)} è una simulazione che dimostra che q_5 è simulato da q_1.

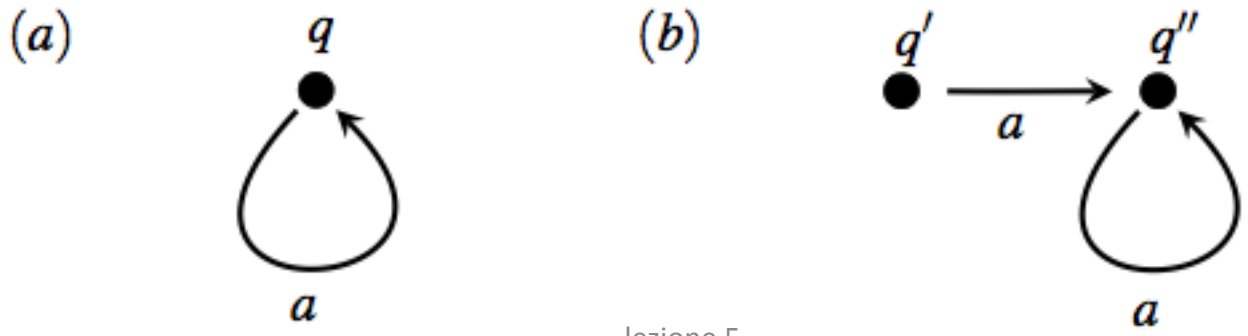
Come l'ho costruita?

Per dimostrare che R è una simulation, dobbiamo mostrare che, per ogni coppia (q_i,q_j) ∈ R, per ogni a, per tutti i q'_i tale che q_i −a→q'_i esiste q'_j tale che q_j −a→q'_j e (q'_i, q'_j) ∈ R.

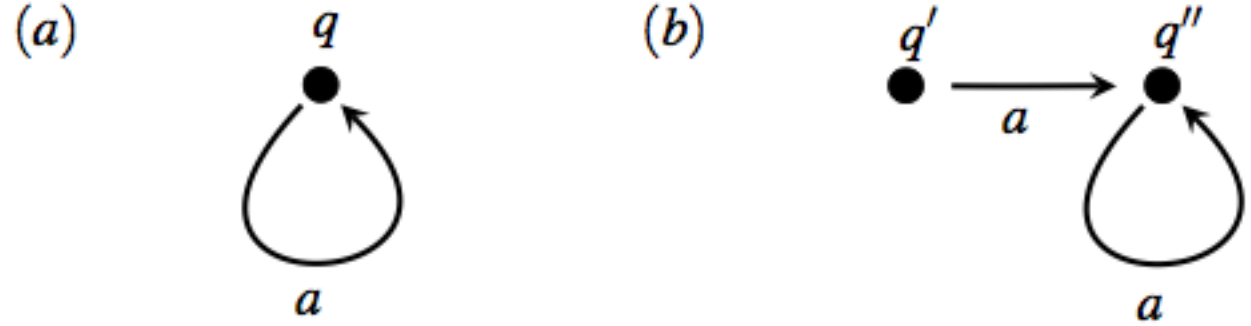


Esercizio

- Dimostrare che q può essere simulato da q’ (ed anche da q’’). Quante diverse simulazioni riesci a trovare? Ad esempio R = {(q, q)} è una simulazione? Si, ma non contiene (q, q’). Ma R’ = {(q, q’)} lo è? E la relazione R’’ = {(q,q’), (q, q’’), (q’’, q)} lo è? Esiste una “largest simulation”?
- Dimostrare che vale anche il viceversa!



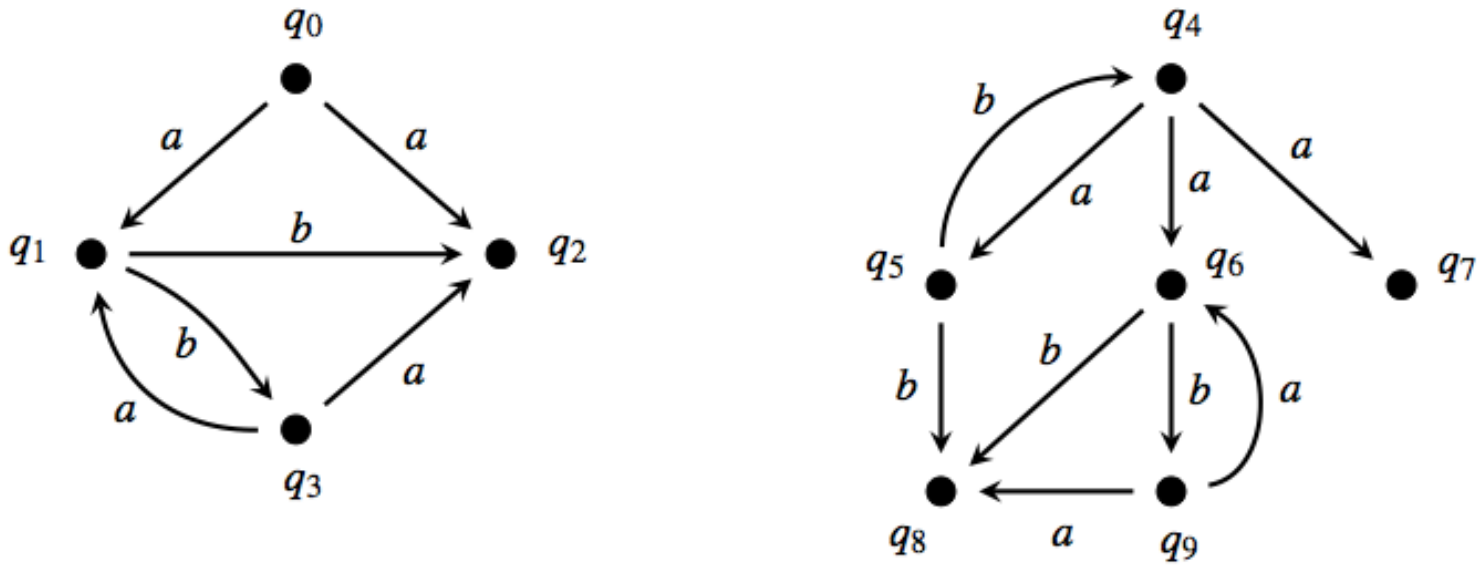
Esercizio



Considerando i due lts di sopra, verifica che solo una delle sequenti relazioni non è una simulazione:

- $S_0 = \{(q,q)\}$
- $S_1 = \{(q,q'),(q,q''),(q'',q)\}$
- $S_2 = \{(q,q'),(q,q''),(q'',q')\}$
- $S_3 = \emptyset$.

Esercizio (2)



- Build a simulation relation containing the pair (q0, q4)

Simulation vs Traces

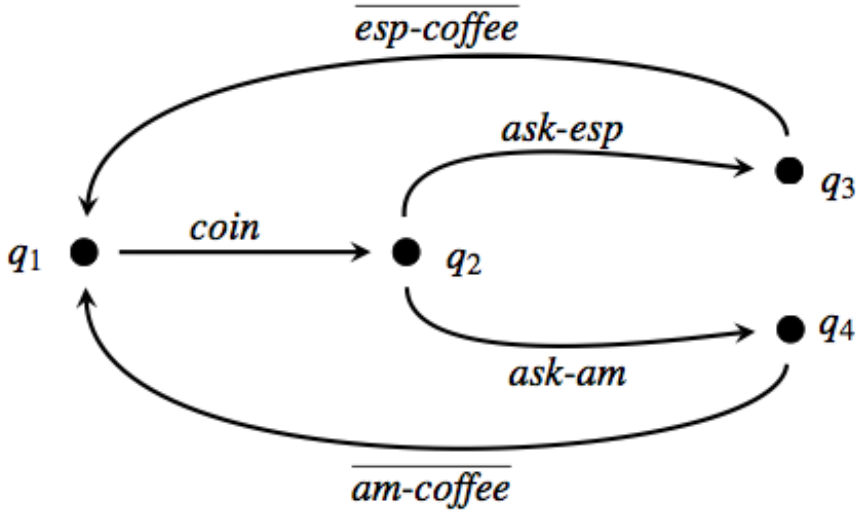
Proposition 2.1. *Let $TS = (Q, A, \rightarrow)$ be a transition system. For any $q, q' \in Q$, if $q \lesssim q'$ then $q \leq_{tr} q'$, i.e., $Tr(q) \subseteq Tr(q')$.*

Proof. *If $q \lesssim q'$, then there exists a simulation $R \subseteq Q \times Q$ such that $(q, q') \in R$. We then prove, by induction on the length of traces, a sligthly stronger result: if $q \xrightarrow{\sigma}{}^{*} q_1$, then $q' \xrightarrow{\sigma}{}^{*} q_1'$ with $(q_1, q_1') \in R$; this implies the thesis $Tr(q) \subseteq Tr(q')$. The base case is when $\sigma = \varepsilon$ and is trivial as $q \xrightarrow{\varepsilon}{}^{*} q$ and $q' \xrightarrow{\varepsilon}{}^{*} q'$ with $(q, q') \in R$. Now if $q \xrightarrow{\sigma}{}^{*} q_1$ with $|\sigma| = n+1$, then by Exercise 2.4, there exist a state $\overline{q}$, a trace σ' and an action μ such that $q \xrightarrow{\sigma'}{}^{*} \overline{q} \xrightarrow{\mu} q_1$ with $\sigma = \sigma'\mu$. Hence, induction can be applied to conclude that a state $\overline{q}'$ exists such that $q' \xrightarrow{\sigma'}{}^{*} \overline{q}'$ with $(\overline{q}, \overline{q}') \in R$. As R is a simulation, a state q_1' exists such that transition $\overline{q} \xrightarrow{\mu} q_1$ is to be matched by $\overline{q}' \xrightarrow{\mu} q_1'$ with $(q_1, q_1') \in R$, and so $q' \xrightarrow{\sigma}{}^{*} q_1'$ by Exercise 2.4. Summing up, transition $q \xrightarrow{\sigma}{}^{*} q_1$ is matched by $q' \xrightarrow{\sigma}{}^{*} q_1'$ with $(q_1, q_1') \in R$, as required.* □

Simulation vs Traces (2)

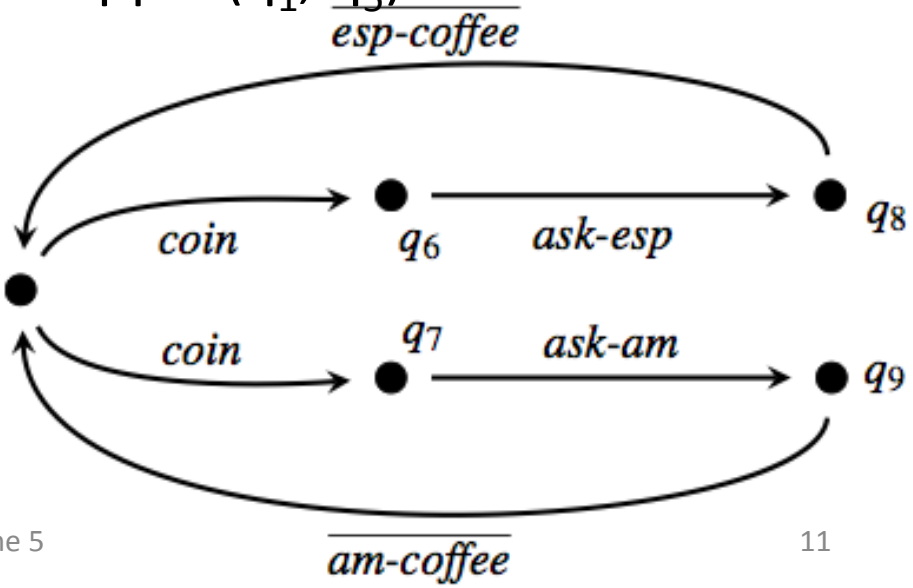
- Corollario: se q e q’ sono simulation equivalent, allora Tr(q) = Tr(q’).
- Vale il viceversa? NO! (vedi prossimo lucido)

Trace preorder non implica simulation preorder



A q_1 −coin→ q_2, q_5 deve replicare con q_5 −coin → q_6 o q_5 −coin → q_7; allora o (q_2,q_6) o (q_2,q_7) deve appartenere a R. Ma ciò è impossibile: se (q_2,q_6) ∈ R allora q_6 non può replicare a q_2−ask-am →q_4. Lo stesso accade se (q_2,q_7) ∈R.

$Tr(q_1) = Tr(q_5)$, ma non esiste una simulation R che contenga la coppia (q_1, q_5). Come lo dimostro? Per assurdo, supponiamo di avere una simulazione R che contenga la coppia (q_1, q_5)



Proprietà

Proposition 2.2. *For any lts* $TS = (Q, A, \rightarrow)$, *the following hold:*

1. *the identity relation* $\mathscr{I} = \{(q,q) \mid q \in Q\}$ *is a simulation;*
2. *the relational composition* $R_1 \circ R_2 = \{(q,q'') \mid \exists q'.(q,q') \in R_1 \wedge (q',q'') \in R_2\}$ *of two simulations* R_1 *and* R_2 *is a simulation.*
3. *the union* $\bigcup_{i \in I} R_i$ *of simulations* R_i *is a simulation.*

Remember that $q \lesssim q'$ if there exists a simulation containing the pair (q,q'). This means that $\lesssim$ is the union of all simulations, i.e.,

$$\lesssim = \bigcup \{R \subseteq Q \times Q \mid R \text{ is a simulation}\}.$$

Dimostrazione

Proof. The proof of (1) is immediate: $(q,q) \in \mathscr{I}$ *is a simulation pair because whatever transition* q *performs (say,* $q \xrightarrow{\mu} q'$*), the other* q *in the pair does exactly the same transition* $q \xrightarrow{\mu} q'$ *with* $(q',q') \in \mathscr{I}$*.*

The proof of (2) is also easy: given a pair $(q,q'') \in R_1 \circ R_2$*, there exists a state* q' *such that* $(q,q') \in R_1$ *and* $(q',q'') \in R_2$*; as* $(q,q') \in R_1$*, if* $q \xrightarrow{\mu} q_1$*, there exists* q_2 *such that* $q' \xrightarrow{\mu} q_2$ *with* $(q_1,q_2) \in R_1$*. But as* $(q',q'') \in R_2$*, we have also that there exists* q_3 *such that* $q'' \xrightarrow{\mu} q_3$ *with* $(q_2,q_3) \in R_2$*. Summing up, for any pair* $(q,q'') \in R_1 \circ R_2$*, if* $q \xrightarrow{\mu} q_1$*, then there exists a state* q_3 *such that* $q'' \xrightarrow{\mu} q_3$ *with* $(q_1,q_3) \in R_1 \circ R_2$*, as required.*

The proof of (3) is trivial, too: assume $(q,q') \in \bigcup_{i \in I} R_i$*; then, there exists* $j \in I$ *such that* (q,q') *belongs to simulation* R_j*. If* $q \xrightarrow{\mu} q_1$*, then there must exist* q_2 *such that* $q' \xrightarrow{\mu} q_2$ *with* $(q_1,q_2) \in R_j$*. Hence,* $(q_1,q_2) \in \bigcup_{i \in I} R_i$ *as* $R_j \subseteq \bigcup_{i \in I} R_i$*. So* $\bigcup_{i \in I} R_i$ *is a simulation, too.* □

Esercizi

Dato un qualunque lts TS = (Q, A →),

- dimostrare che il simulation preorder è davvero un preordine, ovvero riflessivo e transitivo;
- dimostrare che la simulation equivalence è davvero una relazione d'equivalenza (dopo aver visto la prova nel prossimo lucido);
- Dimostrare che il simulation preorder è la più grande simulazione che possa essere definita su TS (vedi prossimo lucido, per la soluzione di questo punto).

Exercise 2.24. Given a simulation $S \subseteq Q \times Q$, argue that, for any pair $(q_1, q_2) \in S$, if q_2 is a deadlock, then also q_1 is a deadlock, i.e., if $q_2 \not\rightarrow$ then $q_1 \not\rightarrow$.

Moreover, argue that if we add to simulation S a pair (q, q') such that q is a deadlock, then $S \cup \{(q, q')\}$ is still a simulation. In particular, as $S = \emptyset$ is a simulation, also $\{(q, q')\}$ is a simulation. □

Largest simulation

Remember that $q \lesssim q'$ if there exists a simulation containing the pair (q, q'). This means that $\lesssim$ is the union of all simulations, i.e.,

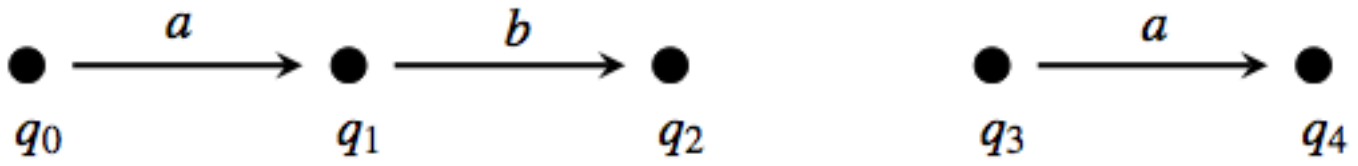
$$\lesssim = \bigcup \{R \subseteq Q \times Q \mid R \text{ is a simulation}\}.$$

By Proposition 2.2(3), $\lesssim$ is also a simulation, hence the largest such relation.

Proposition 2.3. *For any LTS $TS = (Q, A, \rightarrow)$, relation $\lesssim \subseteq Q \times Q$ is the largest simulation relation.* □

Simulation preorder: esempi

- q_3 è simulato da q_0! Ma non vale il viceversa.



- a.0 è simulato da a.0 + b.0? Vale il viceversa?
- E questi due?

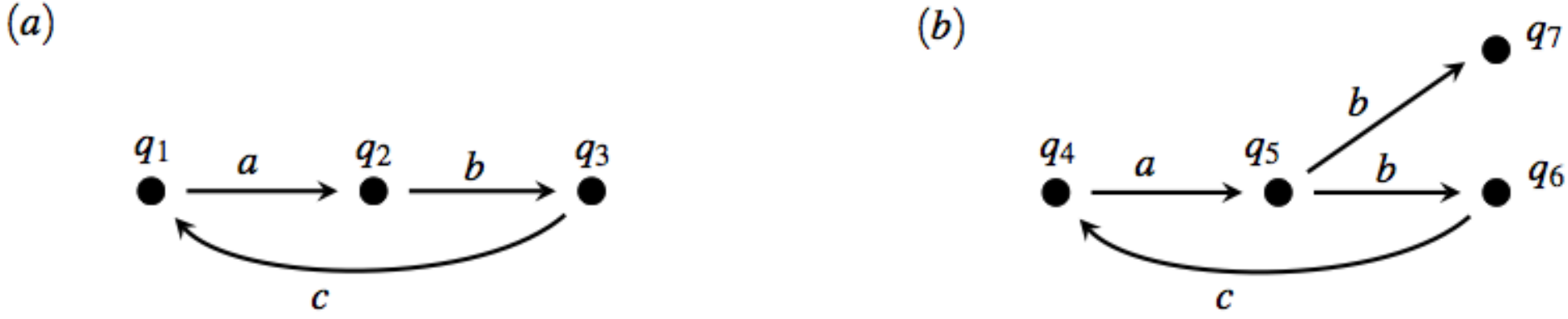


Fig. 2.14 Two not completed trace equivalent systems

Esercizi

- Dimostra che esiste un lts con un solo stato che può essere simulato da qualsiasi altro lts (cioè tale rooted lts è un elemento minimo nel simulation preorder).
- Dimostra anche che, fissato un insieme A di labels, esiste un lts con un solo stato che può simulare ogni altro rooted lts su A (cioè tale rooted lts è un elemento massimo nel simulation preorder).

Complessità

- È stato dimostrato che il simulation preorder è il più "grossolano" (coarsest) preordine incluso nel trace preorder (cioè appena un po' più fine del trace preorder) che sia noto essere decidibile in tempo polinomiale e spazio polinomiale.
- Quindi la simulazione tra due processi è efficiente e, dall'esempio delle vending machine, piuttosto intuitivo.
- Ma presenta ancora problemi discutibili ….

Simulazione vs Deadlock

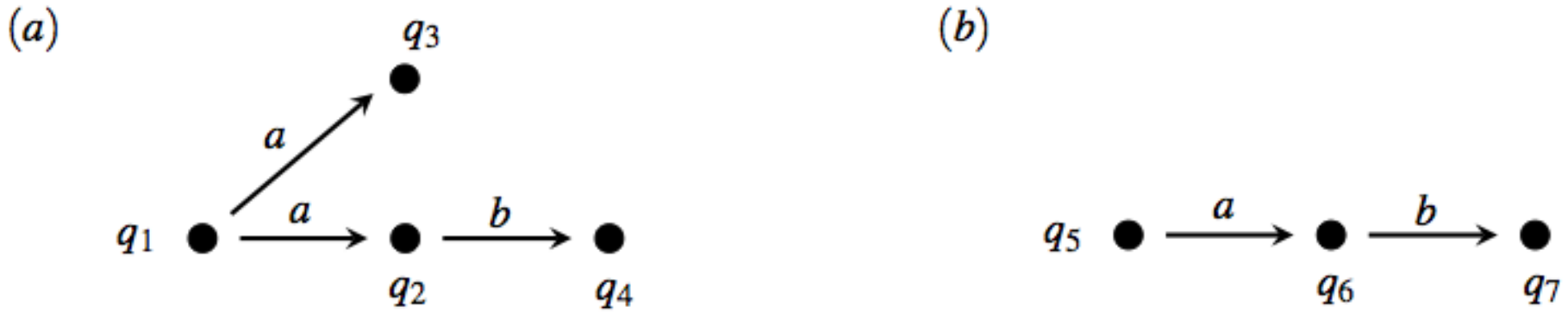


Fig. 2.12 Deadlock is not observable

- Verifica che $R_1 = \{(q_5,q_1),(q_6,q_2),(q_7,q_4)\}$ è una simulation relation che dimostra che q_5 è simulato da q_1.
- Esercizio: fornisci la simulazione che dimostra che q_1 è simulato da q_5.
- Allora simulation equivalence non è sensibile al deadlock!
- Però vale che, per ogni (q, q') in una simulazione, se q' è un deadlock allora q è un deadlock.

Completed Simulation

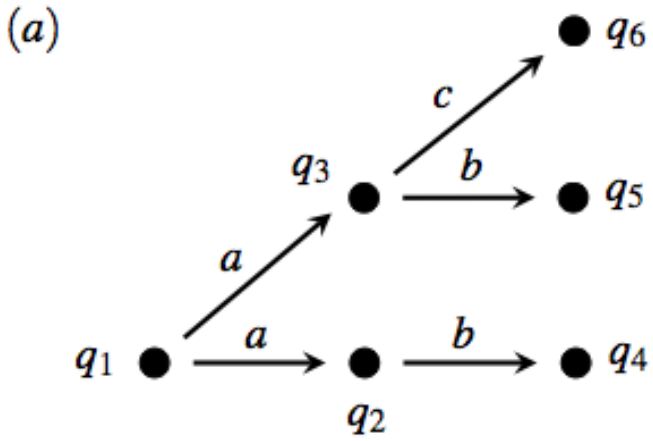
Definition 2.13. (Completed simulation) Let $TS = (Q, A, \rightarrow)$ be a transition system. A *completed simulation* is a simulation relation $R \subseteq Q \times Q$ such that, whenever $(q_1, q_2) \in R$, if $q_1 \not\rightarrow$ then $q_2 \not\rightarrow$.[6]

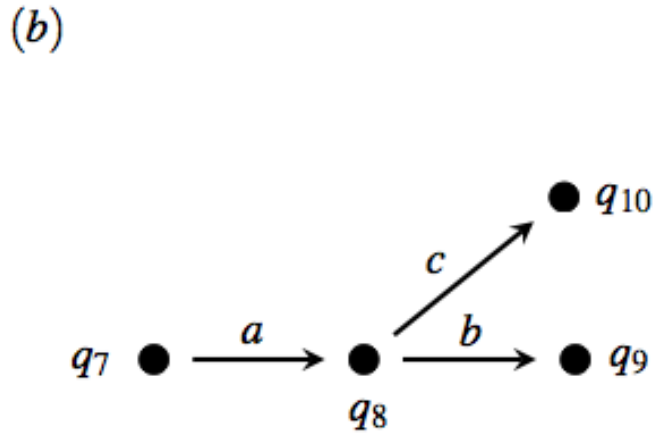
State q is completely simulated by q', denoted $q \lesssim_c q'$, if there exists a completed simulation R such that $(q, q') \in R$. Two states q and q' are *completed simulation equivalent*, denoted $q \simeq_c q'$, if $q \lesssim_c q'$ and $q' \lesssim_c q$ □

- Nei due sistemi del lucido precedente, q_1 non è simulato in modo completo da q_5 perché la coppia (q_3, q_6) non soddisfa il requisito aggiuntivo (q_3 è deadlock mentre q_6 no).
- Nota che la relazione R_1 del lucido precedente è invece una completed simulation.
- Dimostra che completed simulation equivalence implica completed trace equivalence (l'implicazione a rovescio non vale: considera le solite due vending machines).

Comp. Sim. vs Timing of choices

- Sebbene distingua correttamente le due vending machines, la simulazione completa non rispetta appieno il “timing of choices”. Questi due sotto sono completed simulation equiv.
- Questi due possono essere distinti da un osservatore che ripete esperimenti e nota che solo la seconda macchina, dopo aver fatto a, offre sempre sia b che c.





(Compl.) Simulation: pro e contro

Riassumendo, i vantaggi principali del (compl.) simulation preorder sono:

- una semplice tecnica di prova (semplicemente esibisci una relazione e prova facilmente che è una (compl.) simulation)
- Condizione sufficiente per (compl) trace inclusion, molto più facilmente verificabile, quindi utile quando si fa verifica di proprietà di safety.
- Esistenza di un semplicissimo elemento massimo (solo per simulation!), utile per verifica.

Principale svantaggio: ancora un po' troppo astratta, cioè identifica sistemi che dovrebbero essere distinti.