Labelled Transition System (LTS)

Vediamo adesso come generalizzare il concetto di automa in modo da adattarlo alle nostre esigenze e poter così definire un'adeguata nozione di equivalenza comportamentale tra sistemi.

Definizione 5 (LTS, sistema di transizioni etichettate) *Un LTS su un insieme di etichette Act è una coppia* $(\mathcal{Q}, \mathcal{T})$ *dove:*

- $\mathcal{Q}$ *è un insieme di stati*

- $\mathcal{T} \subseteq (\mathcal{Q} \times Act \times \mathcal{Q})$ *è una relazione ternaria chiamata relazione delle transizioni.*

Se $(q, \alpha, q') \in \mathcal{T}$ *allora scriveremo* $q \xrightarrow{\alpha} q'$ *e chiameremo* q *la* **sorgente** *e* q' *la* **destinazione** *della transizione. Se* $q \xrightarrow{\alpha_1} q_1 \xrightarrow{\alpha_2} q_2 \ldots \xrightarrow{\alpha_n} q_n$*, allora chiameremo* q_n **derivato** *di* q *sotto* $\alpha_1\alpha_2\ldots\alpha_n$*.*

- Un LTS **rappresenta** solo le **transizioni** di un automa.

- In un LTS non vi è né stato iniziale né stati finali, ma solo transizioni.

- Avevamo già visto come, per le nostre esigenze, fosse possibile lavorare senza stati finali.

- Adesso, eliminando anche gli stati iniziali, un medesimo LTS $(\mathcal{Q}, \mathcal{T})$ può essere istanziato per rappresentare differenti automi; uno per ogni stato.

- Ad esempio, se $\mathcal{Q} = \{q, q', q''\}$, allora un LTS $(\mathcal{Q}, \mathcal{T})$ può modellare tre diversi automi, a seconda se si scelga q, q' o q'' come stato iniziale.

Simulazione forte (strong simulation)

- **Domanda**:

  "Quando possiamo dire che due stati in un LTS sono equivalenti?"

- L'esperienza della macchina del tè ci ha fatto capire che se ci limitiamo ad osservare il comportamento di **automi da un un punto**

di vista reattivo, allora automi come quelli riportati a pag. 17 non dovrebbero essere considerati equivalenti.

- Introduciamo quindi la nozione di **simulazione** tra stati. Intuitivamente, q **simula** p se per ogni transizione $p \xrightarrow{\alpha} p'$, al variare di α, esiste una transizione $q \xrightarrow{\alpha} q'$, per qualche stato q', tale che q' **simula ancora** p'.

- La nozione di simulazione sembra in qualche modo essere *ricorsiva*. E infatti...

Definizione 6 (Simulazione forte) *Sia $(\mathcal{Q}, \mathcal{T})$ un LTS, e sia $\mathcal{S}$ una relazione binaria definita su $\mathcal{Q}$. Allora, $\mathcal{S}$ è una* **simulazione forte** *su $(\mathcal{Q}, \mathcal{T})$ se, per ogni coppia di stati (p, q) tale che $p \, \mathcal{S} \, q$*

$$\text{se } p \xrightarrow{\alpha} p' \text{ allora esiste } q' \in Q \text{ tale che } q \xrightarrow{\alpha} q' \text{ e } p' \, \mathcal{S} \, q'.$$

Definizione 7 *Uno stato q* **simula in maniera forte** *p se esiste una simulazione forte $\mathcal{S}$ per cui $p \, \mathcal{S} \, q$.*

- Continuando con l'esempio a pag. 17, mostriamo che

$$\mathcal{S}= \{ (q_0, p_0),\ (q_1, p_1),\ (q_1', p_1),\ (q_2, p_2),\ (q_3, p_3) \}$$

  è una simulazione forte. Per far ciò dobbiamo considerare ogni coppia $(q, p) \in \mathcal{S}$. Facciamolo....

- Poichè $\mathcal{S}$ è una simulazione forte, ne consegue, per definizione, che p_0 simula q_0, e così anche per le altre coppie in $\mathcal{S}$.

- Mostriamo adesso che non esiste una simulazione forte $\mathcal{R}$ che contenga la coppia (p_1, q_1). E che quindi q_1 non simula p_1. Questo perchè una delle transizioni di p_1 non può essere simulata da q_1.

- Poichè q_1 non simula p_1 ne consegue che anche q_0 **non simula in maniera forte** p_0.

- **Ma allora ci siamo!!**

- Abbiamo trovato un modo per distinguere gli automi a pag. 17. Infatti lo stato p_0 simula in maniera forte lo stato q_0, ma non vale il viceversa. E quindi gli automi corrispondenti non sono equivalenti: uno simula l'altro ma non viceversa.

- È possibile fomalizzare meglio l'intuizione racchiusa nella parola 'viceversa'? Certo!

- Ricordate che la relazione inversa $\mathcal{S}^{-1}$ di una relazione binaria $\mathcal{S}$ è data dall'insieme delle coppie (y, x) tali che $(x, y) \in \mathcal{S}$.

Definizione 8 (Bisimulazione forte, Equivalenza forte)

- *Una relazione binaria $\mathcal{S}$ su un insieme di stati $\mathcal{Q}$ è una* **bisimulazione forte** *su un LTS $(\mathcal{Q}, \mathcal{T})$ se sia $\mathcal{S}$ che la sua inversa sono simulazioni.*

- *Due stati p e q sono* **equivalenti in maniera forte**, *e lo scriveremo $p \sim q$, se esiste una bisimulazione $\mathcal{S}$ per cui $p\ \mathcal{S}\ q$.*

- Finalmente possiamo affermare in maniera rigorosa che gli automi a pag. 17 non sono equivalenti secondo la Definizione 8.

- Consideriamo adesso l'LTS nell'Esempio 3.7 a pagina 18. Intuitivamente tale LTS rappresenta due automi. Mostriamo allora che

$p_0 \sim q_0$. Per provare ciò definiamo la relazione

$$\mathcal{S} = \{(p_0, q_0), (p_0, q_2), (p_1, q_1), (p_2, q_1)\}$$

Mostreremo che $\mathcal{S}$ è una bisimulazione. E poichè $p_0 \ \mathcal{S} \ q_0$ ne consegue, per definizione, $p_0 \sim q_0$.

- Spesso è utile collegare graficamente gli stati bisimili.
- Per provare che $\mathcal{S}$ è una bisimulazione dobbiamo mostrare che sia $\mathcal{S}$ che la sua inversa $\mathcal{S}^{-1}$ sono simulazioni. Fatelo a casa.
- In altri casi sarà nostra intenzione mostrare che due stati p e q non sono equivalenti in maniera forte, cioè che $p \not\sim q$. Il metodo tipico è quello di mostrare che non esiste alcuna bisimulazione che contenga la coppia (p, q).

Osservazione 9 (Importante!) *Si noti che* $p \sim q$ **non equivale a dire che** p **simula** q**, ed allo stesso tempo,** q **simula** p**.** *In realtà vuol dire qualcosa di ben più forte!!!*

- Consideriamo i due processi (si noti che adesso cominciamo a chiamarli processi) nell'Esercizio 3.10 a pagina 20 e proviamo che p simula q, ed allo stesso tempo, q simula p.

- Per fare ciò abbiamo bisogno di due simulazioni, una in ogni direzione.

  - Per mostrare che p **simula** q scegliamo:

$$\mathcal{S} = \{(q,p),(q_1,p_1),(q_2,p_2)\}$$

  - Per mostrare che q **simula** p scegliamo:

$$\mathcal{R} = \{(p,q),(p_1',q_1),(p_1,q_1),(p_2,q_2)\}$$

  Si noti però che le due simulazioni **non sono una l'inversa dell'altra!!**

- In effetti è possibile mostrare che $p \not\sim q$, cioè non esiste alcuna simulazione $\mathcal{S}$ che contenga (p,q) tale che $\mathcal{S}^{-1}$ è anch'essa una simulazione. Provatelo.

- Intuitivamente nell'ultimo esercizio, il processo p è meno affidabile di q. Infatti attraverso un'azione a, il processo p può raggiungere uno stato di **deadlock** o stallo. Vale a dire uno stato in cui non è possibile eseguire alcuna azione.

- Nella lezioni precedenti abbiamo affermato che è nostra cura individuare situazioni di stallo. Perciò non vorremo mai considerare equivalenti due processi come p e q in cui solo uno dei due presenta una situazione di stallo.

$\sim$ è una relazione d'equivalenza

L'equivalenza forte gode di alcune proprietà interessanti. Cominciamo a vederne alcune:

Proposizione 10

1. *La relazione* $\sim$ *è una* **equivalenza**, *cioè soddisfa le seguenti proprietà:*
   - **Riflessività:** *Per ogni* p, $p \sim p$

- **Simmetria:** *Se* $p \sim q$ *allora* $q \sim p$
- **Transitività:** *Se* $p \sim q$ *e* $q \sim r$*, allora* $p \sim r$*.*

2. *La relazione* $\sim$ *è essa stessa una bisimulazione.*

Queste proprietà sono tutte importanti. La riflessività, ad esempio, garantisce che una specifica è una corretta (sia pur inefficiente) implementazione di se stessa.

La transitività è comunque certamente più interessante. Infatti, si supponga di voler derivare, per raffinamenti successivi, un'implementazione a partire da una certa specifica Spec. Seguendo questo approccio, potremmo trasformare Spec nell'implementazione Impl passando attraverso una sequenza di implementazioni intermedie Impl_i $(0 \leq i \leq n)$. Questo approccio è corretto purchè ciascun passo intermedio preservi il comportamento del sistema:

$$\mathrm{Spec} \sim \mathrm{Impl}_0 \sim \mathrm{Impl}_1 \sim \ldots \sim \mathrm{Impl}_1 = \mathrm{Impl} \ .$$

La transitività ci consente di concludere che il raffinamento finale, ovvero l'implementazione, rispetta la specifica:

$$\mathrm{Spec} \sim \mathrm{Impl} \ .$$

Prova Proposizione 10. Iniziamo con la prima parte. Per la riflessività è sufficiente mostrare che la relazione

$$Id_{\mathcal{Q}} = \{(p, p) \mid p \in \mathcal{Q}\}$$

è una bisimulazione.

Per la simmetria dobbiamo mostrare che se $\mathcal{S}$ è una bisimulazione allora anche $\mathcal{S}^{-1}$ lo è. Ma questo deriva direttamente dalla definizione di bisimulazione.

La parte più delicata è la transitività. Dobbiamo mostrare che se $\mathcal{S}_1$ and $\mathcal{S}_2$ sono bisimulazioni allora anche la loro composizione

$$\mathcal{S}_1\mathcal{S}_2 = \{(p, r) \mid \exists q. p \, \mathcal{S}_1 \, q \text{ and } q \, \mathcal{S}_2 \, r\}$$

è una bisimulazione. Sia $(p, r) \in \mathcal{S}_1\mathcal{S}_2$ e $p \xrightarrow{\alpha} p'$. Poichè esiste q tale che $p \, \mathcal{S}_1 \, q$ e $q \, \mathcal{S}_2 \, r$, deve esistere anche un qualche q' tale che $q \xrightarrow{\alpha} q'$ e $p' \, \mathcal{S}_1 \, q'$, e quindi anche un r' tale che $r \xrightarrow{\alpha} r'$ e $q' \, \mathcal{S}_2 \, r'$. Così $(p', r') \in \mathcal{S}_1\mathcal{S}_2$ ed abbiamo verificato le condizioni di simulazione per $\mathcal{S}_1\mathcal{S}_2$.

La prova che $\sim$ è una bisimulazione è molto facile siete invitati a farla a casa verificandola con quella sul vostro libro di testo.