LTS per processi concorrenti

- Diamo adesso la **semantica operazionale** per processi concorrenti attraverso transizioni del tipo $P \stackrel{\alpha}{\longrightarrow} P'$.
- Nel caso di azioni osservabili (cioè per $\alpha = a$ o $\alpha = \overline{a}$ dove $a \in Act \setminus \{\tau\}$), le transizioni $P \stackrel{\alpha}{\longrightarrow} P'$ modellano la capacità di P di interagire con il mondo esterno attraverso il canale a.
- Mentre azioni della forma $P \stackrel{\tau}{\longrightarrow} P'$ modellano evoluzioni interne (e quindi non osservabili) del processo P.
- Si noti che due processi che differiscono per α-conversione vengono considerati sostanzialmente **uguali**.

Definizione 28 *L'***LTS** *per processi concorrenti sull'insieme di azioni* $\mathcal{L} \cup \{\tau\}$ *è dato dalla coppia* $(\mathcal{P}, \mathcal{T})$, *dove* $\mathcal{P}$ *è l'insieme di processi e* $\mathcal{T}$ *sono le transizioni generate dalle seguenti regole:*

$$\text{(SUM:)}\quad M+\alpha.P+N \xrightarrow{\alpha} P \qquad\qquad \text{(REACT)}\quad \frac{P \xrightarrow{\lambda} P' \qquad Q \xrightarrow{\overline{\lambda}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'}$$

$$\text{(L-PAR)}\quad \frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \qquad\qquad \text{(R-PAR)}\quad \frac{Q \xrightarrow{\alpha} Q'}{P \mid Q \xrightarrow{\alpha} P \mid Q'}$$

$$\text{(RES)}\quad \frac{P \xrightarrow{\alpha} P'}{(\nu a)P \xrightarrow{\alpha} (\nu a)P'} \qquad \text{if } \alpha \notin \{a, \overline{a}\}$$

$$\text{(IDENT)}\quad \frac{\{\vec{b}/\vec{a}\}P_A \xrightarrow{\alpha} P'}{A\langle\vec{b}\rangle \xrightarrow{\alpha} P'} \qquad \text{if } A(\vec{a}) \stackrel{\text{def}}{=} P_A$$

$$\text{(ALPHA)}\quad \frac{P =_\alpha P' \qquad P' \xrightarrow{\alpha} Q' \qquad Q =_\alpha Q'}{P \xrightarrow{\alpha} Q}$$

Tabella 1: Transizioni per processi concorrenti

Esempio 29 *Sia* $P \stackrel{def}{=} (\nu a)((a.Q_1 + b.Q_2) \mid \overline{a}.\mathbf{0}) \mid (\overline{b}.a.R_1 + \overline{a}.R_2)$*. Tale sistema può evolvere internamente in maniera non deterministica in due modi differenti. Vediamo il primo:*

$$\begin{array}{rcll} P & \xrightarrow{\tau} & (\nu a)(Q_1 \mid \mathbf{0}) \mid (\overline{b}.a.R_1 + \overline{a}.R_2) & c \textit{ fresh} \\ & \equiv & (\nu a)Q_1 \mid (\overline{b}.a.R_1 + \overline{a}.R_2) & \end{array}$$

Questo è il **diagramma di inferenza** *(inference diagram) della transizione:*

$$(l\text{-}p)\left(\frac{(res)\left(\frac{(rct)\left(\frac{(sum)\left(\frac{-}{(a.Q_1 + b.Q_2) \xrightarrow{a} Q_1 \qquad \overline{a}.\mathbf{0} \xrightarrow{\overline{a}} \mathbf{0}}\right.}{(a.Q_1 + b.Q_2) \mid \overline{a}.\mathbf{0} \xrightarrow{\tau} Q_1 \mid \mathbf{0}}\right.}{(\nu a)((a.Q_1 + b.Q_2) \mid \overline{a}.\mathbf{0}) \xrightarrow{\tau} (\nu a)(Q_1 \mid \mathbf{0})}\right.}{(\nu a)((a.Q_1 + b.Q_2) \mid \overline{a}.\mathbf{0}) \mid (\overline{b}.a.R_1 + \overline{a}.R_2) \xrightarrow{\tau} (\nu a)(Q_1 \mid \mathbf{0}) \mid (\overline{b}.a.R_1 + \overline{a}.R_2)}\right.$$

Il sistema può comunque evolvere in maniera differente attraverso una sincronizzazione sul canale b:

$$P \xrightarrow{\tau} (\nu a)(Q_2 \mid \overline{a}.\mathbf{0}) \mid a.R_1$$

Il diagramma di inferenza è il seguente:

$$(RES)\left(\dfrac{(LPAR)\left(\dfrac{(SUM)\left(\dfrac{-}{(a.Q_1+b.Q_2) \xrightarrow{b} Q_2}\right.}{(a.Q_1+b.Q_2) \mid \overline{a}.\mathbf{0} \xrightarrow{b} Q_2 \mid \overline{a}.\mathbf{0}}\right.}{(\nu a)((a.Q_1+b.Q_2) \mid \overline{a}.\mathbf{0}) \xrightarrow{b} (\nu a)(Q_2 \mid \overline{a}.\mathbf{0})}\right.$$

Inoltre

$$(SUM)\left(\dfrac{-}{\overline{b}.a.R_1+\overline{a}.R_2 \xrightarrow{\overline{b}} a.R_1}\right.$$

E quindi grazie alla (REACT):

$$() \left(\frac{(\nu a)((a.Q_1 + b.Q_2) \mid \overline{a}.\mathbf{0}) \xrightarrow{b} (\nu a)(Q_2 \mid \overline{a}.\mathbf{0}) \quad \overline{b}.a.R_1 + \overline{a}.R_2 \xrightarrow{\overline{b}} a.R_1}{(\nu a)((a.Q_1 + b.Q_2) \mid \overline{a}.\mathbf{0}) \Big| \overline{b}.a.R_1 + \overline{a}.R_2 \xrightarrow{\tau} (\nu a)(Q_2 \mid \overline{a}.\mathbf{0}) \mid a.R_1} \right.$$

Esempio 30 (Lotteria) *Si supponga di voler costruire una macchina della lotteria L attraverso cui è possibile estrarre a caso una pallina da un insieme* $\{b_1, \ldots, b_n\}$*. Dopo l'***estrazione***, (azione osservabile) la pallina estratta viene rimessa nell'urna e si ricomincia di nuovo. Usando l'azione* τ *per rappresentare la* **scelta interna** *della pallina potremmo rappresentare la specifica della macchina come:*

$$Lotspec \stackrel{def}{=} \tau.b_1.Lotspec + \ldots + \tau.b_n.Lotspec$$

Notate che in questo modo dobbiamo cambiare definizione al variare di n*.*

È possibile invece costruire un processo lotteria in maniera modulare partendo da un **numero fisso** *di componenti. Vediamo un tentativo per* $n = 3$*. Definiamo:*

$$
\begin{array}{rcl}
A(x,y,z) & \stackrel{def}{=} & \overline{x}.C\langle x,y,z\rangle \\
C(x,y,z) & \stackrel{def}{=} & \tau.B\langle x,y,z\rangle + z.A\langle x,y,z\rangle \\
B(x,y,z) & \stackrel{def}{=} & y.C\langle x,y,z\rangle
\end{array}
$$

Adesso definiamo le seguenti istanze:

$$
\begin{array}{rclcl}
A_i & \stackrel{def}{=} & A\langle a_i, b_i, a_{i+1}\rangle & = & \overline{a_i}.C_i \\
B_i & \stackrel{def}{=} & B\langle a_i, b_i, a_{i+1}\rangle & = & b_i.C_i \\
C_i & \stackrel{def}{=} & C\langle a_i, b_i, a_{i+1}\rangle & = & \tau.B_i + a_{i+1}.A_i
\end{array}
$$

per $1 \leq i \leq 3$ *ed aritmetica modulo 3. Consideriamo i seguenti tre stati:*

$$
\begin{array}{rcl}
L_1 & \stackrel{def}{=} & (\nu a_1 a_2 a_3)(C_1 \mid A_2 \mid A_3) \\
L_2 & \stackrel{def}{=} & (\nu a_1 a_2 a_3)(A_1 \mid C_2 \mid A_3) \\
L_3 & \stackrel{def}{=} & (\nu a_1 a_2 a_3)(A_1 \mid A_2 \mid C_3)
\end{array}
$$

Non è difficile convincersi che la lotteria può ciclare all'infinito attraverso gli stati L_i *in cui ogni palla* b_i *può essere scelta.*

$$
L_1 \xrightarrow{\tau} L_2 \xrightarrow{\tau} L_3 \xrightarrow{\tau} L_1.
$$

Esercizio 31 *Mostrare usando le regole di riduzione che in ciascuno stato L_i è possibile decidere l'estrazione della pallina b_i attraverso un'azione τ:*

(1) $L_1 \xrightarrow{\tau} (\nu a_1 a_2 a_3)(B_1 \mid A_2 \mid A_3)$
(2) $L_2 \xrightarrow{\tau} (\nu a_1 a_2 a_3)(A_1 \mid B_2 \mid A_3)$
(3) $L_3 \xrightarrow{\tau} (\nu a_1 a_2 a_3)(A_1 \mid A_2 \mid B_3)$

Nell'esempio precedente appare chiaro che le azioni interne $\xrightarrow{\tau}$ modellano solamente il comportamento interno della macchina della lotteria. Per rappresentare invece le interazioni con l'esterno dobbiamo usare azioni della forma $\xrightarrow{b_i}$ per modellare l'estrazione della pallina b_i. Ad esempio, se $L_1 \xrightarrow{\tau} (\nu a_1 a_2 a_3)(B_1 \mid A_2 \mid A_3)$ allora:

$$(\nu a_1 a_2 a_3)(B_1 \mid A_2 \mid A_3) \xrightarrow{b_1} (\nu a_1 a_2 a_3)(C_1 \mid A_2 \mid A_3).$$

Induzione sulle transizioni di un processo

Provare che la proprietà $\mathsf{Prop}(P \xrightarrow{\alpha} P')$ è vera per ogni transizione $P \xrightarrow{\alpha} P'$:

- **Caso base:** Provare $\mathsf{Prop}(\mathit{conclusione})$ per tutti gli assiomi della forma

$$(\text{Assioma}) \ \frac{-}{\mathit{conclusione}}$$

- **Caso induttivo:** Per ogni regola della forma

$$(\text{Regola}) \ \frac{\mathit{prem}_1 \ \ \mathit{prem}_2 \ \ \ldots \ \ \mathit{prem}_n}{\mathit{conclusione}}$$

  provare $\mathsf{Prop}(\mathit{conclusione})$ assumendo vere, per ipotesi, $\mathsf{Prop}(\mathit{prem}_i)$ per ogni premessa prem_i.

Vediamo un esempio in cui si applica l'induzione sulle transizioni.

Lemma 32 *Se $P \xrightarrow{\lambda} P'$, allora P e P' possono essere espresse, a meno di congruenza strutturale, nella forma:*

$$\begin{array}{rcl} P & \equiv & (\nu\vec{z})((\lambda.Q + M) \mid R) \\ P' & \equiv & (\nu\vec{z})(Q \mid R) \end{array}$$

dove λ non è ristretto da $(\nu\vec{z})$.

Prova Per induzione sulle transizioni $P \xrightarrow{\lambda} P'$. Si effettua un'analisi dei casi sull'ultima regola d'inferenza applicata. Nota che poichè $\lambda \neq \tau$, l'ultima regola applicata non può essere (REACT).

- Sia (SUM) l'ultima regola applicata per dedurre $P \xrightarrow{\lambda} P'$. Cioè $P = M + \lambda.P' + N$ per qualche M, N, λ, P'. Allora $P \equiv (\nu\ )(\lambda.P' + M + N \mid \mathbf{0})$ e $P' \equiv (\nu)(P' \mid \mathbf{0})$.

- Sia (L-PAR) l'ultima regola applicata per dedurre $P \xrightarrow{\lambda} P'$. Cioè $P = P_1 \mid P_2$, $P_1 \xrightarrow{\lambda} P_1'$ e $P' = P_1' \mid P_2$. Allora, per ipotesi induttiva, $P_1 \equiv (\nu\vec{z})(\lambda.Q + M \mid R)$, per qualche Q, M e R e $P_1' \equiv$

$(\nu\vec{z})(Q \mid R)$. Quindi, a meno di sciegliere opportunamente $\vec{z}$, per evitare cattura di nomi in P_2, $P \equiv (\nu\vec{z})(\lambda.Q + M \mid (R \mid P_2))$ e $P' \equiv (\nu\vec{z})(Q \mid (R \mid P_2))$.

- Sia (R-PAR) l'ultima regola applicata per dedurre $P \xrightarrow{\lambda} P'$. Tale caso è simile al precedente.

- Sia (RES) l'ultima regola applicata per dedurre $P \xrightarrow{\lambda} P'$. Allora $P = (\nu a)P_1$, per qualche P_1, con $P_1 \xrightarrow{\lambda} P_1'$ e $P' \equiv (\nu a)P_1'$. Allora, per ipotesi induttiva, $P_1 \equiv (\nu\vec{z})(\lambda.Q + M \mid R)$, per qualche Q, M e R, e $P_1' \equiv (\nu\vec{z})(Q \mid R)$. Quindi, $P \equiv (\nu a\vec{z})(\lambda.Q + M \mid R)$ e $P' \equiv (\nu a\vec{z})(Q \mid R)$.

- Sia (IDENT) l'ultima regola applicata per dedurre $P \xrightarrow{\lambda} P'$. Allora $P = A\langle\vec{b}\rangle$ con $A(\vec{x}) \stackrel{\text{def}}{=} P_A$ e P_A somma. Ma allora $P = A\langle\vec{b}\rangle \equiv \{\vec{b}/\vec{x}\}P_A$. Poichè P_A è una somma anche $\{\vec{b}/\vec{x}\}P_A$ lo è. Possiamo perciò concludere.

- Sia (ALPHA) l'ultima regola applicata per dedurre $P \xrightarrow{\lambda} P'$. Fare per esercizio.

Proposizione 33 ($\equiv$ è una bisimulazione, pag. 40) *Se* $P \xrightarrow{\alpha} P'$ *e* $P \equiv Q$, *allora esiste* Q' *tale che* $Q \xrightarrow{\alpha} Q'$ *e* $P' \equiv Q'$.

Prova La prova è per induzione sulle transizioni etichettate. Chi è interessato può dare un'occhiata alla prova sul libro a pag. 40.

Proposizione 34

- *Dato* P, *esistono solo un numero finito di transizioni* $P \xrightarrow{\alpha} P'$.
- *Se* $P \xrightarrow{\alpha} P'$ *allora* $\mathsf{fn}(P', \alpha) \subseteq \mathsf{fn}(P)$.
- *Se* $P \xrightarrow{\alpha} P'$ *e* σ *è una sostituzione allora* $\sigma P \xrightarrow{\sigma\alpha} \sigma P'$.

Esempio 35 (Buffer bidirezionale) *(Guardare grafo di flusso a pag. 43). Sia*

$$A(a, a', b, b') \stackrel{def}{=} a.\overline{b}.A + b'.\overline{a'}.A \ .$$

o abbreviando

$$A \stackrel{def}{=} a.\overline{b}.A + b'.\overline{a'}.A \ .$$

A può essere trasmettere messaggi in entrambe le direzioni. Definiamo

$$B(b, b', c, c') \stackrel{def}{=} A\langle b, b', c, c'\rangle = b.\overline{c}.B + c'.\overline{b'}.B$$

abbreviando,

$$B \stackrel{def}{=} b.\overline{c}.B + c'.\overline{b'}.B$$

e mettiamolo in parallelo con A e restringiamo i nomi b e b'

$$P \stackrel{def}{=} (\nu bb')(A \mid B)$$

Allora P si comporta 'più o meno' come A. In realtà P è meno affidabile di A. Perchè?

Fare a casa esercizio 5.12.