Linguaggi di Programmazione

Roberta Gori

Bisimilarita' debole-11.8

CCS: sintassi

$$
\begin{array}{rcll}
p, q & ::= & \mathbf{nil} & \text{processo inattivo} \\
& | & x & \text{variabile di processo (per la ricorsione)} \\
& | & \mu.p & \text{prefisso azione} \\
& | & p\backslash\alpha & \text{canale ristretto} \\
& | & p[\phi] & \text{rietichettatura del canale} \\
& | & p + q & \text{scelta nondeterministica (somma)} \\
& | & p|q & \text{composizione parallela} \\
& | & \mathbf{rec}\ x.\ p & \text{ricorsione}
\end{array}
$$

(gli operatori sono elencati in ordine di precedenza)

CCS op. semantica

Act) $$\frac{}{\mu.p \xrightarrow{\mu} p}$$

Res) $$\frac{p \xrightarrow{\mu} q \quad \mu \notin \{\alpha, \overline{\alpha}\}}{p\backslash\alpha \xrightarrow{\mu} q\backslash\alpha}$$

Rel) $$\frac{p \xrightarrow{\mu} q}{p[\phi] \xrightarrow{\phi(\mu)} q[\phi]}$$

SumL) $$\frac{p_1 \xrightarrow{\mu} q}{p_1 + p_2 \xrightarrow{\mu} q}$$

SumR) $$\frac{p_2 \xrightarrow{\mu} q}{p_1 + p_2 \xrightarrow{\mu} q}$$

ParL) $$\frac{p_1 \xrightarrow{\mu} q_1}{p_1|p_2 \xrightarrow{\mu} q_1|p_2}$$

Com) $$\frac{p_1 \xrightarrow{\lambda} q_1 \quad p_2 \xrightarrow{\overline{\lambda}} q_2}{p_1|p_2 \xrightarrow{\tau} q_1|q_2}$$

ParR) $$\frac{p_2 \xrightarrow{\mu} q_2}{p_1|p_2 \xrightarrow{\mu} p_1|q_2}$$

Rec) $$\frac{p[{}^{\mathbf{rec}\ x.\ p}/_{x}] \xrightarrow{\mu} q}{\mathbf{rec}\ x.\ p \xrightarrow{\mu} q}$$

CCS
transizioni deboli

Buffer sequenziale

$$B_0^2 \triangleq in.B_1^2$$

$$B_1^2 \triangleq in.B_2^2 + \overline{out}.B_0^2$$

$$B_2^2 \triangleq \overline{out}.B_1^2$$

$$\begin{tikzcd}
B_0^2 \arrow[d, bend left, "in"] \\
B_1^2 \arrow[u, bend left, "\overline{out}"] \arrow[d, bend left, "in"] \\
B_2^2 \arrow[u, bend left, "\overline{out}"]
\end{tikzcd}$$

Buffer parallelo

$$B_0^1 \triangleq in.B_1^1$$

$$B_1^1 \triangleq \overline{out}.B_0^1$$

$$\begin{tikzcd}
& B_0^1|B_0^1 \arrow[dl, shift left, "in"] \arrow[dr, shift left, "in"] & \\
B_1^1|B_0^1 \arrow[ur, shift left, "\overline{out}"] \arrow[dr, shift left, "in"] & & B_0^1|B_1^1 \arrow[ul, shift left, "\overline{out}"] \arrow[dl, shift left, "in"] \\
& B_1^1|B_1^1 \arrow[ul, shift left, "\overline{out}"] \arrow[ur, shift left, "\overline{out}"] &
\end{tikzcd}$$

Buffer collegato

$$B_0^1 \triangleq in.B_1^1 \qquad \eta(out) = c$$

$$B_1^1 \triangleq \overline{out}.B_0^1 \qquad \phi(in) = c$$

$$p \frown q \triangleq (p[\eta] | q[\phi]) \backslash c$$

$$\begin{tikzcd}
 & B_0^1 \frown B_0^1 \arrow[dl, "in"'] & \\
B_1^1 \frown B_0^1 \arrow[rr, "\tau"] & & B_0^1 \frown B_1^1 \arrow[ul, "\overline{out}"'] \arrow[dl, "in"] \\
 & B_1^1 \frown B_1^1 \arrow[ul, "\overline{out}"] &
\end{tikzcd}$$

Buffers collegati

$$\begin{tikzcd}
B_0^2 \arrow[d, bend left, "in"] \\
B_1^2 \arrow[u, bend left, "\overline{out}"] \arrow[d, bend left, "in"] \\
B_2^2 \arrow[u, bend left, "\overline{out}"]
\end{tikzcd}$$

sono bisimili?

$$\begin{tikzcd}
& B_0^1|B_0^1 \arrow[dl, bend right, "in"'] \arrow[dr, bend left, "in"] & \\
B_1^1|B_0^1 \arrow[ur, bend left, "\overline{out}"] \arrow[dr, bend left, "in"] & & B_0^1|B_1^1 \arrow[ul, bend right, "\overline{out}"'] \arrow[dl, bend right, "in"'] \\
& B_1^1|B_1^1 \arrow[ul, bend left, "\overline{out}"] \arrow[ur, bend right, "\overline{out}"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
& B_0^1 \frown B_0^1 \arrow[dl, "in"'] & \\
B_1^1 \frown B_0^1 \arrow[rr, "\tau"] & & B_0^1 \frown B_1^1 \arrow[ul, "\overline{out}"'] \arrow[dl, "in"] \\
& B_1^1 \frown B_1^1 \arrow[ul, "\overline{out}"] &
\end{tikzcd}$$

$$F \triangleq \Diamond_{in} \Diamond_{\tau} \mathbf{tt}$$

$$B_0^2 \not\models F$$

$$B_0^1|B_0^1 \not\models F$$

$$B_0^1 \frown B_0^1 \models F$$

Transizioni silenziose

Le transizioni τ sono silenziose, non osservabili

rappresentano passi interni del sistema

sono usate solo per riportare che ci sono

possiamo astrarre da loro?

possiamo trovare un'equivalenza più ampia?

necessarie per mettere in relazione una specifica astratta (che usa poche τ)

con un'implementazione concreta (con molte τ)

il gioco della simulazione

equivalenza più grossolana: più potere al difensore!

Alice sceglie un processo e una transizione ordinaria

Bob risponde potendo usando molte transizioni silenziose aggiuntive

arbitrariamente molte, ma finite

tali sequenze sono chiamate transizioni deboli

$$p \overset{\mu}{\Rightarrow} q$$

cosa succede se Alice sceglie una transizione silenziosa?

Bob può semplicemente lasciare l'altro processo inattivo

cioè può scegliere di non muoversi

Transizioni deboli

$$p \stackrel{\tau}{\Rightarrow} q \quad \text{iff} \quad p\ (\stackrel{\tau}{\rightarrow})^* q$$

$$p = q \ \vee \ p \stackrel{\tau}{\rightarrow} \ldots \stackrel{\tau}{\rightarrow} q$$

p può raggiungere q attraverso una sequenza finita di transizioni τ (eventualmente vuota)

$$p \stackrel{\lambda}{\Rightarrow} q \quad \text{iff} \quad \exists p', q'.\ p \stackrel{\tau}{\Rightarrow} p' \stackrel{\lambda}{\rightarrow} q' \stackrel{\tau}{\Rightarrow} q$$

p può raggiungere q attraverso una transizione λ
eventualmente preceduta e seguita
da sequenze vuote/finite di transizioni τ

Esempio

$$
\begin{tikzcd}
 & B_0^1 \frown B_0^1 \arrow[dl, "in"'] & \\
B_1^1 \frown B_0^1 \arrow[rr, "\tau"] & & B_0^1 \frown B_1^1 \arrow[ul, "\overline{out}"'] \arrow[dl, "in"] \\
 & B_1^1 \frown B_1^1 \arrow[ul, "\overline{out}"] &
\end{tikzcd}
$$

$$B_0^1 \frown B_0^1 \stackrel{\tau}{\Rightarrow} B_0^1 \frown B_0^1$$

$$B_0^1 \frown B_0^1 \stackrel{in}{\Longrightarrow} B_0^1 \frown B_1^1$$

$$B_1^1 \frown B_0^1 \stackrel{\overline{out}}{\Longrightarrow} B_0^1 \frown B_0^1$$

CCS
bisimulazione debole

Bisimulazione debole

$\mathbf{R}$ è una bisimulazione debole se

$$\forall p,q.\ (p,q) \in \mathbf{R} \Rightarrow \begin{cases} \forall \mu, p'.\ p \xrightarrow{\mu} p' & \Rightarrow \quad \exists q'.\ \boxed{q \stackrel{\mu}{\Rightarrow} q'} \wedge p'\ \mathbf{R}\ q' \\ \wedge & \\ \forall \mu, q'.\ q \xrightarrow{\mu} q' & \Rightarrow \quad \exists p'.\ \boxed{p \stackrel{\mu}{\Rightarrow} p'} \wedge p'\ \mathbf{R}\ q' \end{cases}$$

Alice gioca

Bob responde

transizioni deboli

Bisimilarita' debole

Bisimilarita' debole:

$p \approx q \quad \text{sse} \quad \exists \mathbf{R}$ una bisimulazione debole con $(p, q) \in \mathbf{R}$

TH. la bisimilarità debole è una relazione di equivalenza

TH. ogni bisimulazione forte è una bisimulazione debole

Cor. la bisimilarità forte implica la bisimilarità debole

Bisimilarita' debole?

E se dessimo un potere extra anche ad Alice?

$$\forall p, q.\ (p,q) \in \mathbf{R} \Rightarrow \begin{cases} \forall \mu, p'.\ \boxed{p \stackrel{\mu}{\Rightarrow} p'} & \Rightarrow \quad \exists q'.\ q \stackrel{\mu}{\Rightarrow} q' \wedge p'\ \mathbf{R}\ q' \\ \wedge & \\ \forall \mu, q'.\ \boxed{q \stackrel{\mu}{\Rightarrow} q'} & \Rightarrow \quad \exists p'.\ p \stackrel{\mu}{\Rightarrow} p' \wedge p'\ \mathbf{R}\ q' \end{cases}$$

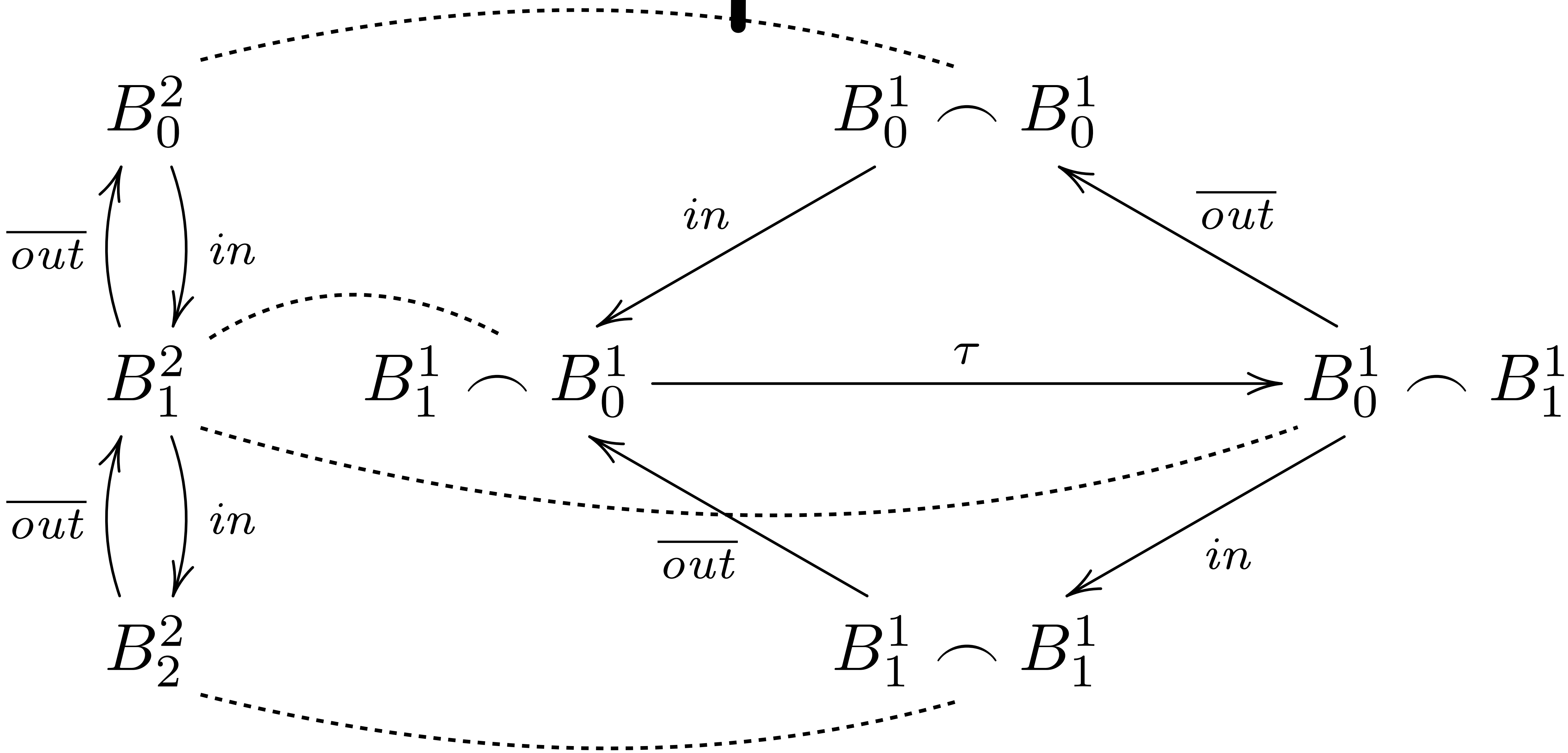
Alice gioca

Bob risponde

transizioni deboli

non cambia nulla: otteniamo ancora la stessa bisimilarità debole

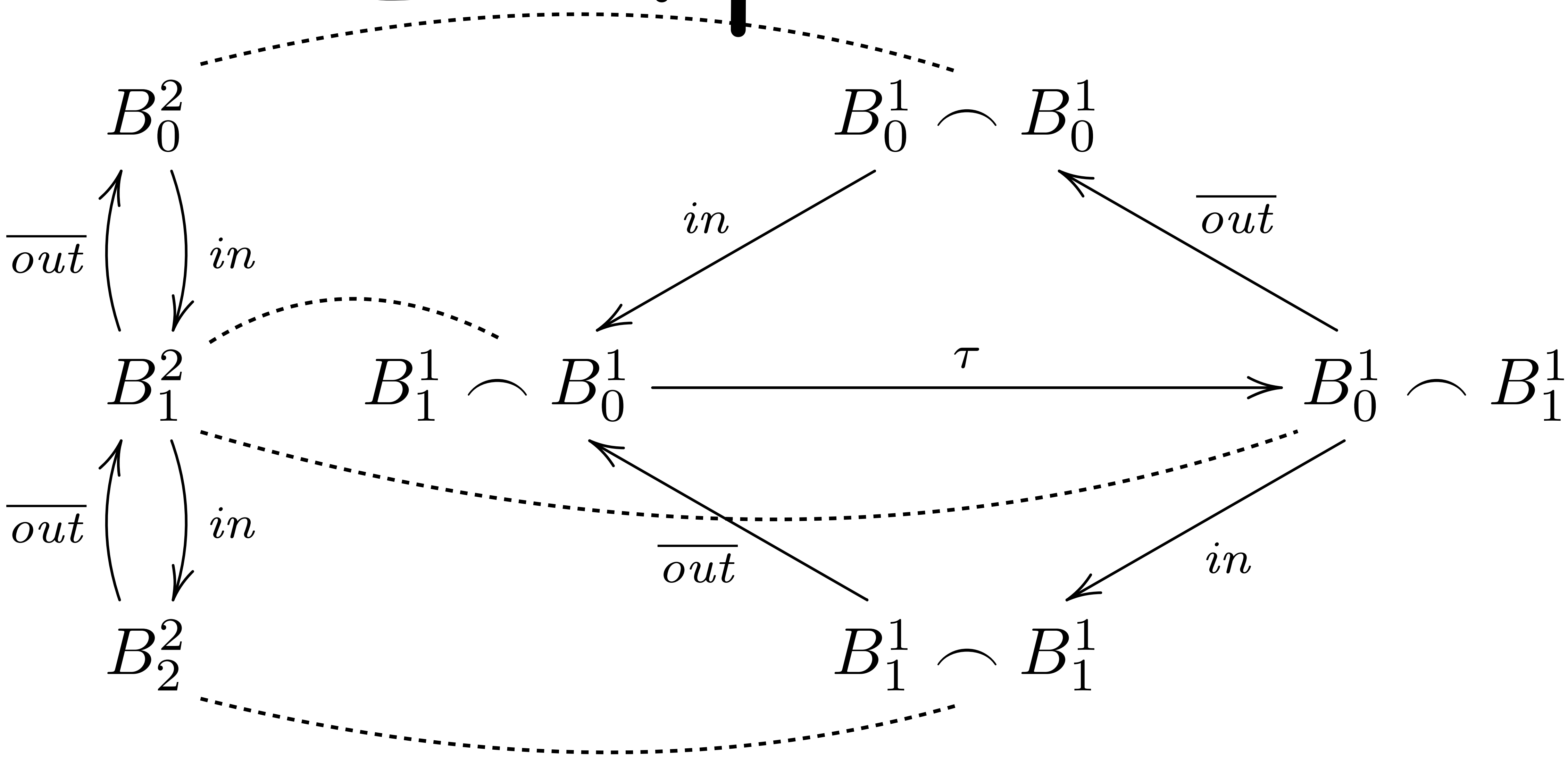
Esempio



$$\mathbf{R} \triangleq \left\{ \begin{array}{l} (B^2_0, B^1_0 \frown B^1_0), \\ (B^2_1, B^1_1 \frown B^1_0), \\ (B^2_1, B^1_0 \frown B^1_1), \\ (B^2_2, B^1_1 \frown B^1_1) \end{array} \right\}$$

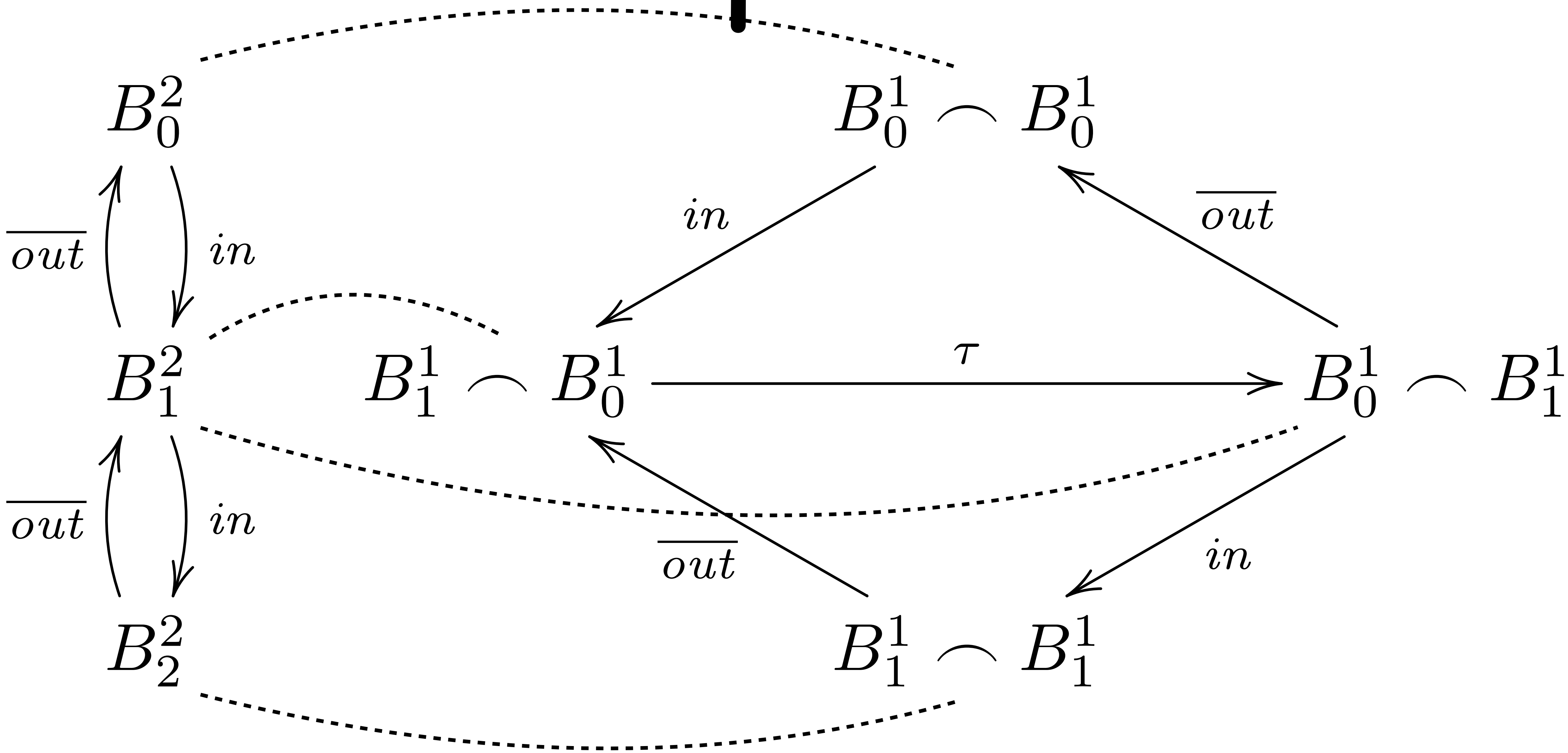
è una relazione di bisimulazione debole

Esempio



$$
\begin{tikzcd}
B_0^2 \arrow[d, "in"] & \mathbf{R} & B_0^1 \frown B_0^1 \arrow[d, Rightarrow, "in"] \\
B_1^2 & \mathbf{R} & B_1^1 \frown B_0^1
\end{tikzcd}
\qquad
\begin{tikzcd}
B_0^2 \arrow[d, Rightarrow, "in"] & \mathbf{R} & B_0^1 \frown B_0^1 \arrow[d, "in"] \\
B_1^2 & \mathbf{R} & B_1^1 \frown B_0^1
\end{tikzcd}
$$

Esempio



$$\begin{array}{ccc} B_1^2 & \mathbf{R} & B_1^1 \frown B_0^1 \\ \downarrow{\scriptstyle in} & & \Downarrow{\scriptstyle in} \\ B_2^2 & \mathbf{R} & B_1^1 \frown B_1^1 \end{array} \qquad \begin{array}{ccc} B_1^2 & \mathbf{R} & B_1^1 \frown B_0^1 \\ \downarrow{\scriptstyle \overline{out}} & & \Downarrow{\scriptstyle \overline{out}} \\ B_0^2 & \mathbf{R} & B_0^1 \frown B_0^1 \end{array}$$

Esempio

$$\begin{tikzcd}
B_0^2 \arrow[d, bend left, "in"] \arrow[rrr, dashed, dash, bend left] & & & B_0^1 \frown B_0^1 \arrow[dl, "in"'] & \\
B_1^2 \arrow[u, bend left, "\overline{out}"] \arrow[d, bend left, "in"] \arrow[rr, dashed, dash, bend left] \arrow[rrrr, dashed, dash, bend right] & & B_1^1 \frown B_0^1 \arrow[rr, "\tau"] & & B_0^1 \frown B_1^1 \arrow[ul, "\overline{out}"'] \arrow[dl, "in"] \\
B_2^2 \arrow[u, bend left, "\overline{out}"] \arrow[rrr, dashed, dash, bend right] & & & B_1^1 \frown B_1^1 \arrow[ul, "\overline{out}"] &
\end{tikzcd}$$

$$\begin{tikzcd}
B_1^2 \arrow[d, Rightarrow, "\tau"] & \mathbf{R} & B_1^1 \frown B_0^1 \arrow[d, "\tau"] \\
B_1^2 & \mathbf{R} & B_0^1 \frown B_1^1
\end{tikzcd}$$

(sta inattivo!)

(etc. per le altre coppie)

bis. debole come punto fisso

$$\Psi(\mathbf{R}) \triangleq \left\{ (p,q) \;\middle|\; \begin{array}{lcl} \forall \mu, p'.\ p \xrightarrow{\mu} p' & \Rightarrow & \exists q'.\ \boxed{q \stackrel{\mu}{\Rightarrow} q'} \wedge p'\ \mathbf{R}\ q' \\ \wedge & & \\ \forall \mu, q'.\ q \xrightarrow{\mu} q' & \Rightarrow & \exists p'.\ \boxed{p \stackrel{\mu}{\Rightarrow} p'} \wedge p'\ \mathbf{R}\ q' \end{array} \right\}$$

$$\Psi : \wp(\mathcal{P} \times \mathcal{P}) \to \wp(\mathcal{P} \times \mathcal{P})$$

mappa relazioni in relazioni

$$\mathbf{R} \subseteq \Psi(\mathbf{R})$$

una bisimulazione debole

$$\approx\ = \Psi(\approx)$$

la bisimilarità debole è un punto fisso

CCS
problemi con la semantica debole

Problemi con la sem. debole

rispetto alle transizioni deboli,
i processi guardati possono avere LTS infinitamente ramificati

$$P \triangleq \mathbf{rec}\ x.\ \tau.x|\beta$$

$$\begin{tikzcd}
P \arrow[r, "\tau"] \arrow[d, "\beta"'] & P|\beta \arrow[r, "\tau"] \arrow[d, "\beta"'] & P|\beta|\beta \arrow[r, "\tau"] \arrow[d, "\beta"'] & \cdots \\
\tau.P & \tau.P|\beta & \tau.P|\beta|\beta &
\end{tikzcd}$$

molte frecce omesse

assumiamo $p|\mathbf{nil} = p$

$$\begin{tikzcd}
P \arrow[r, "\tau"] \arrow[d, Rightarrow, "\beta"'] \arrow[dr, Rightarrow, "\beta"'] \arrow[drr, Rightarrow, "\beta"] & P|\beta \arrow[r, "\tau"] \arrow[d, "\beta"'] & P|\beta|\beta \arrow[r, "\tau"] \arrow[d, "\beta"'] & \cdots \\
\tau.P & \tau.P|\beta & \tau.P|\beta|\beta &
\end{tikzcd}$$

evitare i prefissi τ?

$$P \triangleq \mathbf{rec}\ x.\ (\alpha.x|\overline{\alpha}|\beta)\backslash\alpha$$

Problemi con bis. debole

la bisimilarità debole non è una congruenza (con +)

prendiamo $P \triangleq \alpha$ $Q \triangleq \tau.\alpha$

se $P \xrightarrow{\alpha} \mathbf{nil}$ allora $Q \stackrel{\alpha}{\Rightarrow} \mathbf{nil}$

se $Q \xrightarrow{\tau} \alpha$ allora $P \stackrel{\tau}{\Rightarrow} P$

$P \approx Q$ $\mathbb{C}[P] \not\approx \mathbb{C}[Q]$

prendiamo il contesto $\mathbb{C}[\cdot] \triangleq [\cdot] + \beta$

$\mathbb{C}[P] \triangleq \alpha + \beta$

$\mathbb{C}[Q] \triangleq \tau.\alpha + \beta$

Alice gioca $\mathbb{C}[Q] \xrightarrow{\tau} \alpha$

Bob puo' rispondere $\mathbb{C}[P] \stackrel{\tau}{\Rightarrow} \mathbb{C}[P]$

Alice gioca $\mathbb{C}[P] \xrightarrow{\beta} \mathbf{nil}$

Bob non puo' rispondere $\alpha \stackrel{\beta}{\not\Rightarrow}$

Alice vince!

Problemi con bis. debole

non può distinguere tra stallo

e divergenza silenziosa

$$\mathbf{rec}\ x.\ \tau.x \approx \mathbf{nil}$$

$$\mathbf{rec}\ x.\ \tau.x \xrightarrow{\tau} \mathbf{rec}\ x.\ \tau.x \qquad \mathbf{nil} \stackrel{\tau}{\Rightarrow} \mathbf{nil}$$

CCS
Recuperare la congruenza con bisimilarita’ debole

Congruenza contenuta nella bisimililarita' debole

$$p \approxeq q \quad \text{iff} \quad p \approx \qquad \forall r.\ p + r \approx q + r$$

Equivalentemente

$$p \approxeq q \quad \text{iff} \quad \begin{cases} \forall p'.\ p \xrightarrow{\tau} p' & \Rightarrow \quad \exists q', q''.\ q \xrightarrow{\tau} q'' \overset{\tau}{\Rightarrow} q' \wedge p' \approx q' \\ \forall \lambda, p'.\ p \xrightarrow{\lambda} p' & \Rightarrow \quad \exists q'.\ q \overset{\lambda}{\Rightarrow} q' \wedge p' \approx q' \\ \text{and vice versa} & \end{cases}$$

non è una definizione ricorsiva!
(si riferisce alla bisimilarità debole)

a livello di gioco di bisimulazione:

Bob non può usare una mossa inattiva al primo turno
(ai turni seguenti, gioco ordinario di bisimulazione debole)

TH. $\approxeq$ è la più grande congruenza contenuta in $\approx$

Congruenza contenuta nella bisimililarita' debole

Nota: $\approxeq$ non è una bisimulazione debole!

$$P \triangleq \alpha \qquad\qquad Q \triangleq \tau.\alpha$$

$$\begin{array}{ccc} \beta.P & \approxeq & \beta.Q \\ \Big\downarrow{\scriptstyle\beta} & & \Big\downarrow{\scriptstyle\beta} \\ P & \approx & Q \end{array}$$

$$P \not\approxeq Q$$

$$\approxeq \not\subseteq \Psi(\approxeq)$$

50 prigionieri tenuti in celle separate hanno avuto la possibilità di essere liberati: di volta in volta uno di loro verrà portato in una stanza speciale e poi riportato in cella. (in ordine sparso, possibilmente più volte consecutivamente, ma in modo equo per evitare attese infinite).

La stanza è completamente vuota, tranne che per un interruttore che può accendere o spegnere la luce (la luce non è visibile dall'esterno).

In qualsiasi momento, se uno di loro sostiene a ragione che tutti i prigionieri sono già entrati nella stanza almeno una volta, allora tutti i prigionieri saranno rilasciati (ma se si rivela sbagliato, allora la possibilità finisce e non saranno mai liberati).

I prigionieri hanno la possibilità di discutere in anticipo alcuni protocolli da seguire (non tutti i prigionieri devono comportarsi allo stesso modo).

È possibile trovare una strategia vincente per i prigionieri?
È possibile formalizzarla in CCS (per 2 o 4 prigionieri)?

- Caso facile: è noto che la luce nella stanza è inizialmente spenta.
- Caso difficile: lo stato iniziale della luce nella stanza non è noto.

[**Ex. 4**] Define a CCS process B_k^n that represents an in/out buffer with capacity n of which k positions are taken. Show that B_0^n is strongly bisimilar to n copies of B_0^1 that run in parallel.

[**Ex. 5**] Write a guarded CCS process whose LTS has infinitely many states without using parallel composition.

[**Ex. 6**] Prove that CCS strong bisimilarity is a congruence w.r.t. restriction, i.e., that for all p, q, α:

$$p \simeq q \;\Rightarrow\; p\backslash\alpha \simeq \; q\backslash\alpha$$

[**Ex. 7**] Prove that the CCS agents

$$p \stackrel{\text{def}}{=} \alpha.(\alpha.\beta.\mathbf{nil} + \alpha.(\beta.\mathbf{nil} + \gamma.\mathbf{nil})) \qquad \text{and} \qquad q \stackrel{\text{def}}{=} \alpha.(\alpha.\beta.\mathbf{nil} + \alpha.\gamma.\mathbf{nil})$$

are not strong bisimilar.

[**Ex. 8**] Let us consider the guarded CCS processes

$$p \stackrel{\text{def}}{=} \textbf{rec}\ x.(\alpha.x + \beta.x) \quad q \stackrel{\text{def}}{=} \textbf{rec}\ y.(\overline{\alpha}.\textbf{nil} + \gamma.y) \quad r \stackrel{\text{def}}{=} \textbf{rec}\ z.(\overline{\beta}.\textbf{nil} + \overline{\gamma}.z)$$

1. Draw the LTSs of the processes p, q, r and $s \stackrel{\text{def}}{=} (p|q|r)\backslash\alpha\backslash\beta\backslash\gamma$.
2. Show that s is strong bisimilar to the process $t \stackrel{\text{def}}{=} \textbf{rec}\ w.(\tau.w + \tau.\tau.\textbf{nil})$.

[**Ex. 9**] Prove that the following property is valid for any agent p, where $\approx$ is the weak bisimilarity:

$$p + \tau.p \approx \tau.p$$