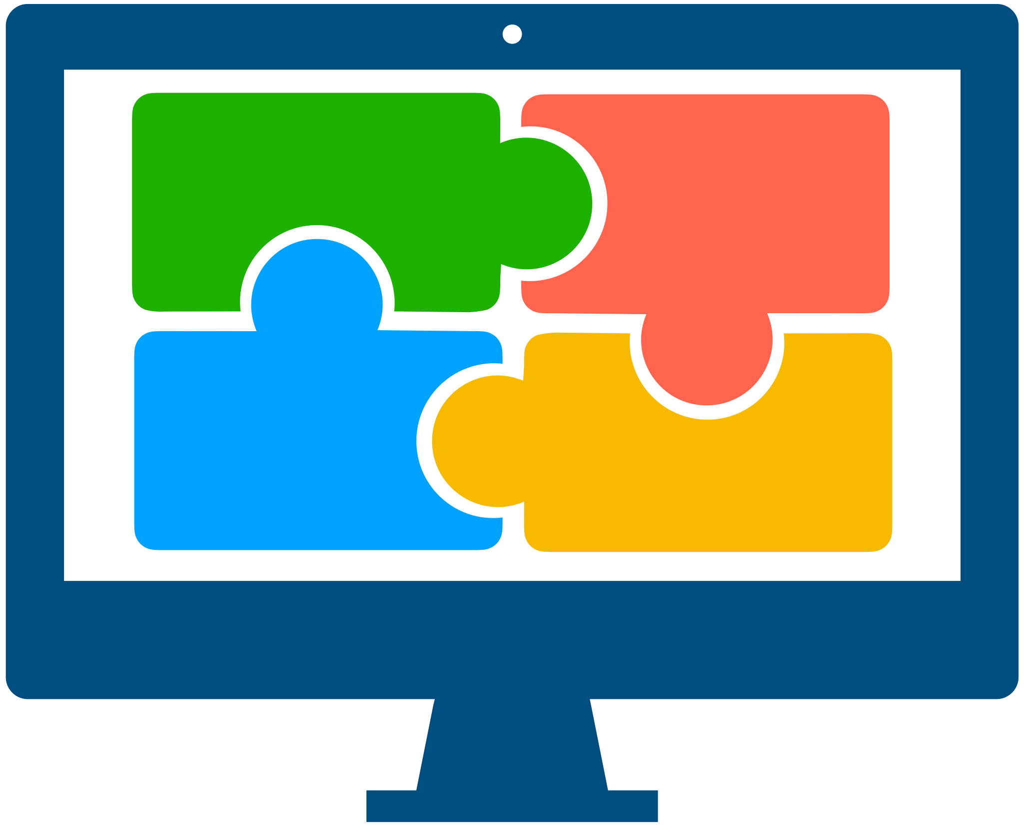


Linguaggi di Programmazione

Roberta Gori

Semantica debole-11.8

CCS: sintassi

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

(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

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

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

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

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

$$
\begin{tikzcd}
B^2_0 \arrow[d, bend left, "in"] \\
B^2_1 \arrow[u, bend left, "\overline{out}"] \arrow[d, bend left, "in"] \\
B^2_2 \arrow[u, bend left, "\overline{out}"]
\end{tikzcd}
$$

sono bisimili?

$$
\begin{tikzcd}
 & B^1_0 | B^1_0 \arrow[dl, bend left, "in"] \arrow[dr, bend left, "in"] & \\
B^1_1 | B^1_0 \arrow[ur, bend left, "\overline{out}"] \arrow[dr, bend left, "in"] & & B^1_0 | B^1_1 \arrow[ul, bend left, "\overline{out}"] \arrow[dl, bend left, "in"] \\
 & B^1_1 | B^1_1 \arrow[ul, bend left, "\overline{out}"] \arrow[ur, bend left, "\overline{out}"] &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & B^1_0 \frown B^1_0 \arrow[dl, "in"'] & \\
B^1_1 \frown B^1_0 \arrow[rr, "\tau"] & & B^1_0 \frown B^1_1 \arrow[ul, "\overline{out}"'] \arrow[dl, "in"] \\
 & B^1_1 \frown B^1_1 \arrow[ul, "\overline{out}"] &
\end{tikzcd}
$$

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

$$B^2_0 \not\models F$$

$$B^1_0 | B^1_0 \not\models F$$

$$B^1_0 \frown B^1_0 \models F$$

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

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

cosa succede se Alice sceglie una transizione silenziosa?

Bob può semplicemente lasciare l'altro processo inattivo

cioè può scegliere di non muoversi

Transizioni deboli

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

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

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

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

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

Esempio

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

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

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

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

CCS
bisimulazione debole

Bisimulazione debole

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

$$\forall p, q.\ (p,q) \in \mathbf{R} \Rightarrow \begin{cases} \forall \mu, p'.\ p \xrightarrow{\mu} p' \quad \Rightarrow \quad \exists q'.\ \boxed{q \overset{\mu}{\Rightarrow} q'} \wedge p'\ \mathbf{R}\ q' \\ \wedge \qquad \text{Alice gioca} \qquad\qquad \text{Bob responde} \\ \forall \mu, q'.\ q \xrightarrow{\mu} q' \quad \Rightarrow \quad \exists p'.\ \boxed{p \overset{\mu}{\Rightarrow} p'} \wedge p'\ \mathbf{R}\ q' \end{cases}$$

transizioni deboli

Bisimilarita' debole

Bisimilarita' debole:

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

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?

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

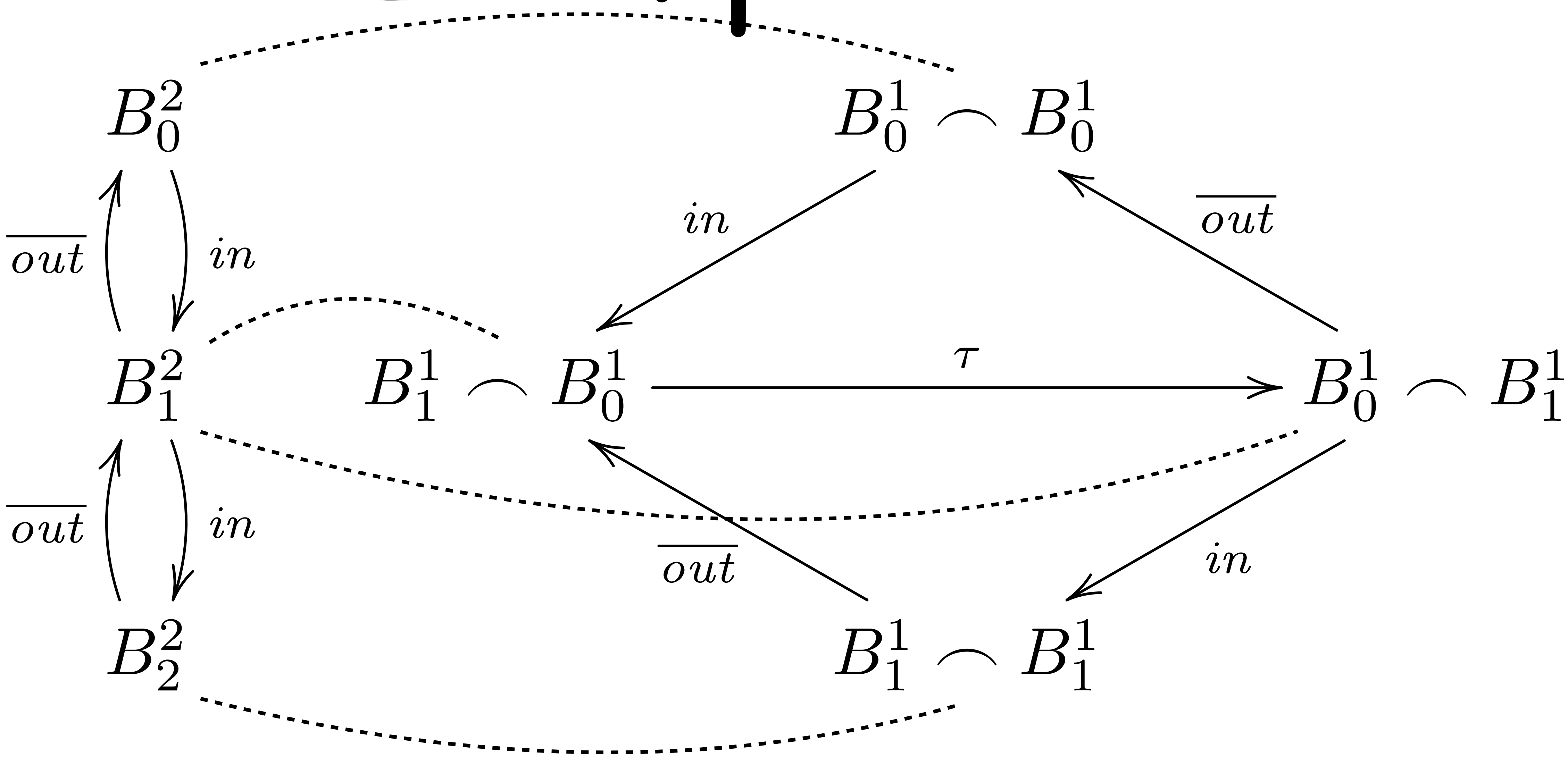
Alice gioca

Bob risponde

transizioni deboli

non cambia nulla: otteniamo ancora la stessa bisimilarità debole

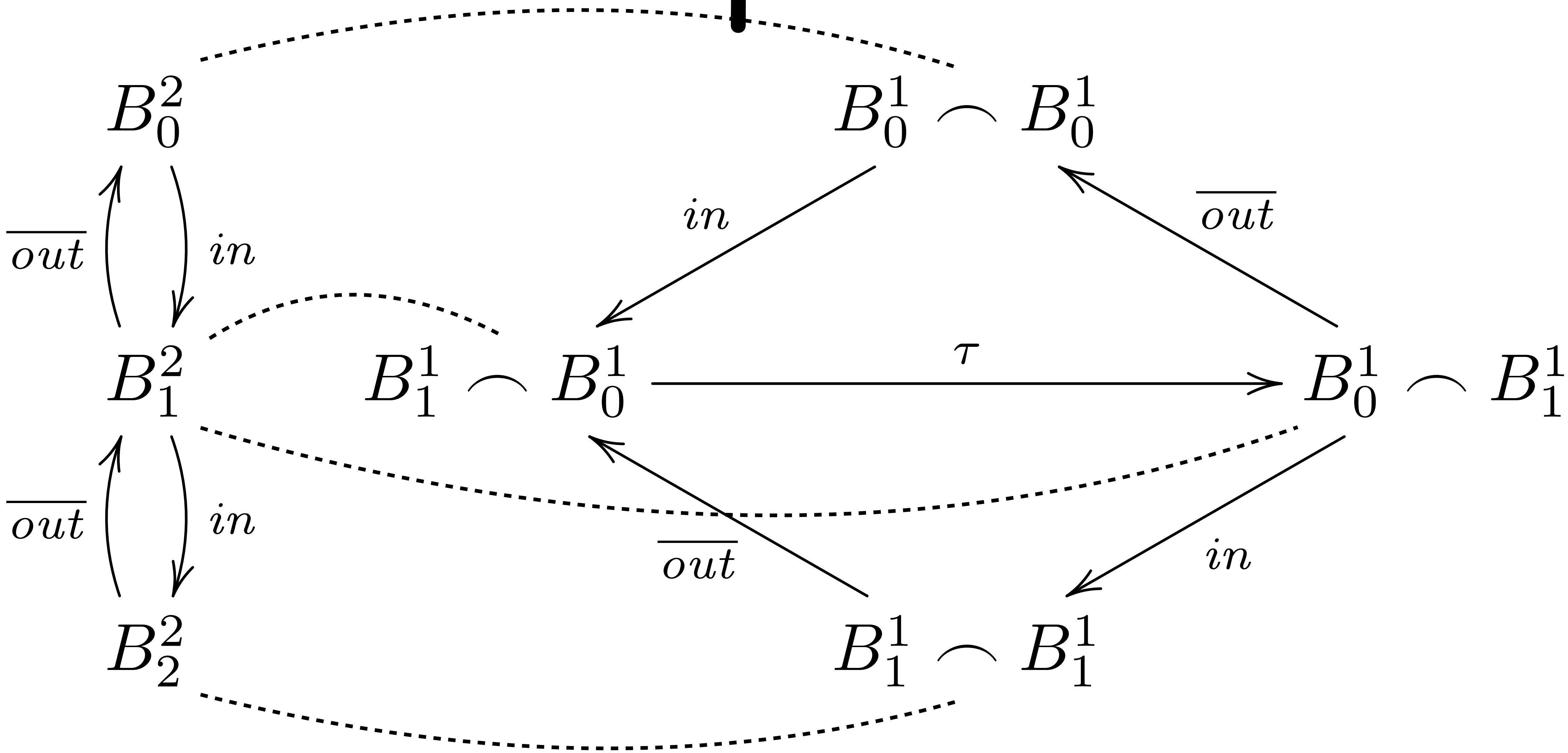
Esempio



$$\mathbf{R} \triangleq \left\{ \begin{array}{l} (B_0^2, B_0^1 \frown B_0^1), \\ (B_1^2, B_1^1 \frown B_0^1), \\ (B_1^2, B_0^1 \frown B_1^1), \\ (B_2^2, B_1^1 \frown B_1^1) \end{array} \right\}$$

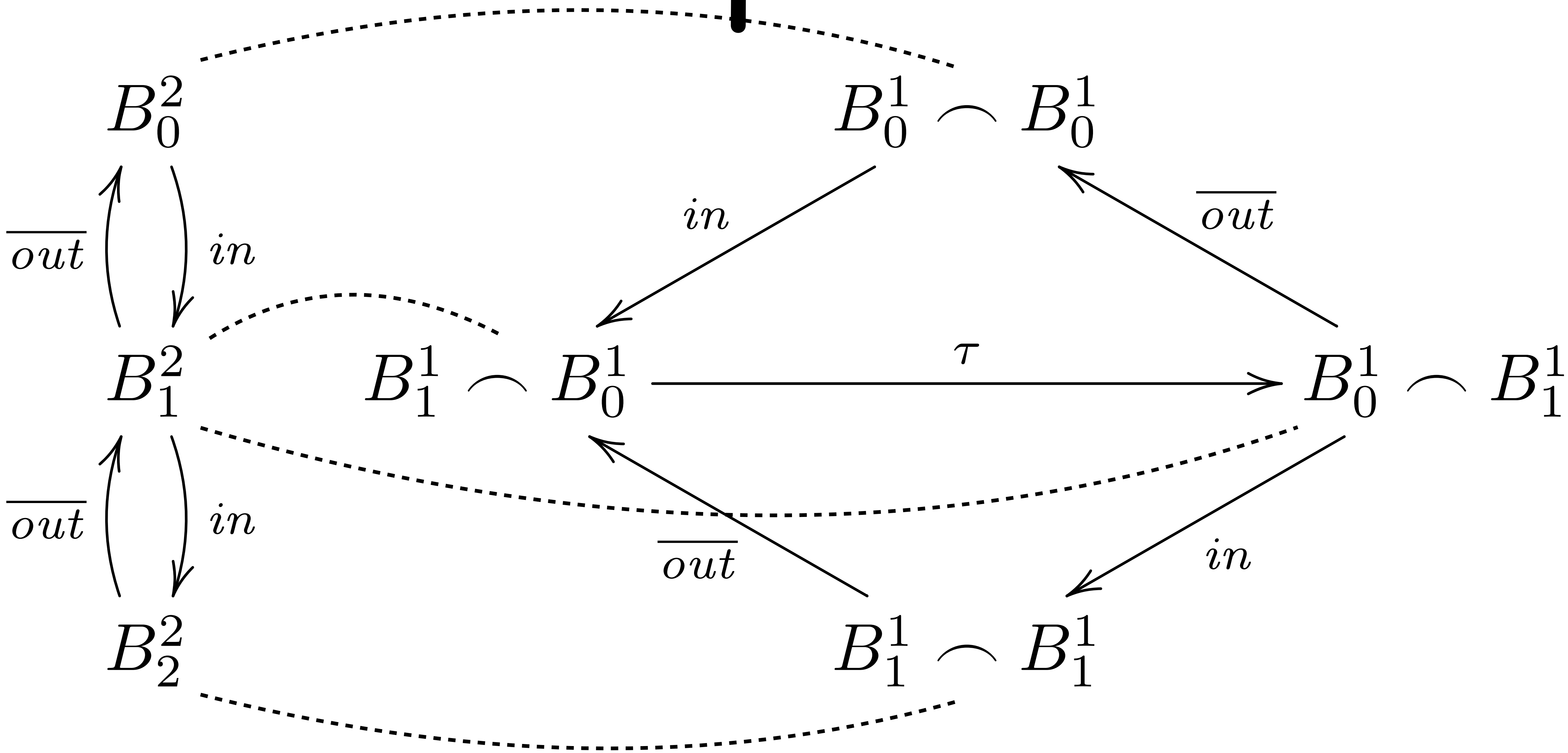
è una relazione di bisimulazione debole

Esempio



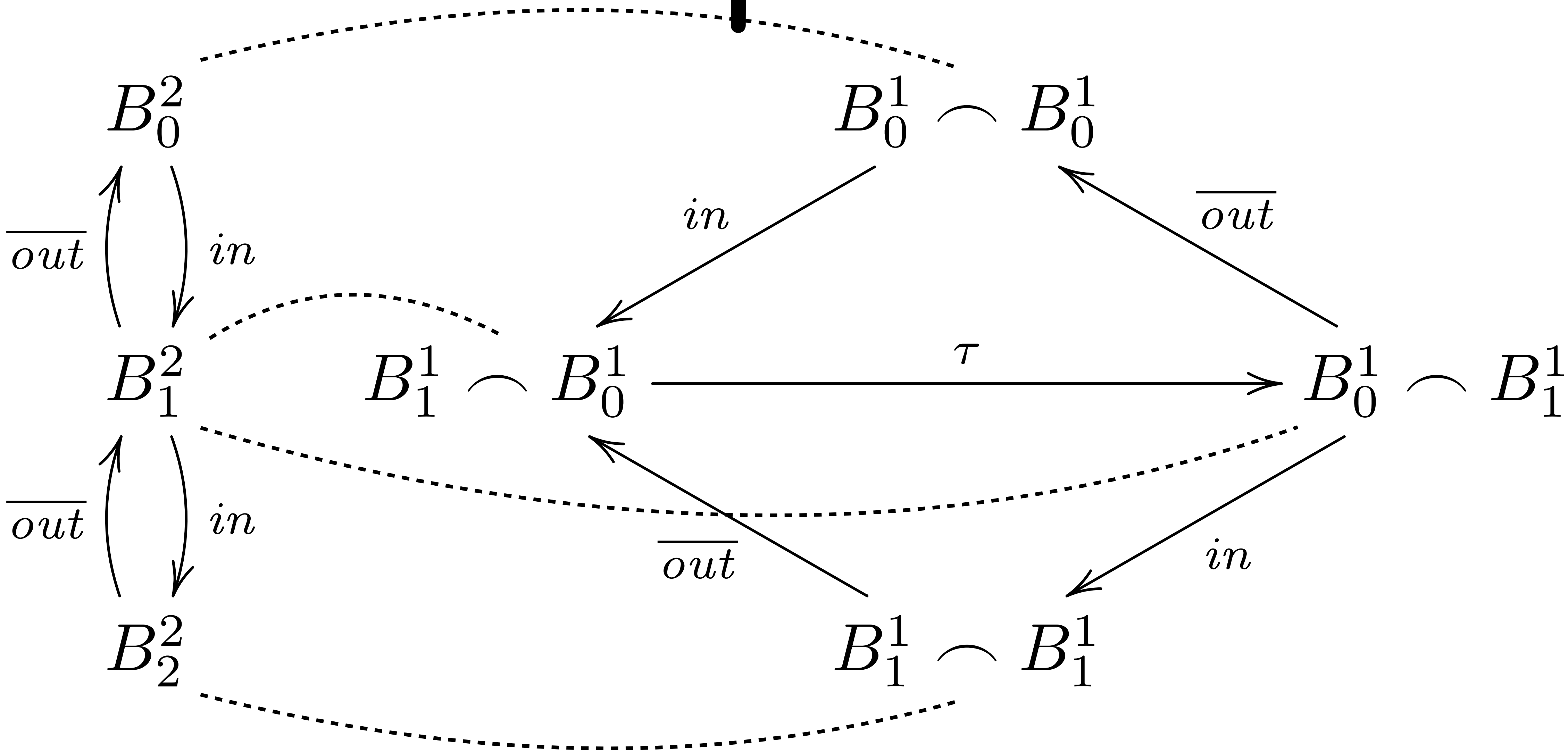
$$
\begin{array}{ccc}
B_0^2 & \mathbf{R} & B_0^1 \frown B_0^1 \\
\big\downarrow{\scriptstyle in} & & \Big\Downarrow{\scriptstyle in} \\
B_1^2 & \mathbf{R} & B_1^1 \frown B_0^1
\end{array}
\qquad\qquad
\begin{array}{ccc}
B_0^2 & \mathbf{R} & B_0^1 \frown B_0^1 \\
\Big\Downarrow{\scriptstyle in} & & \big\downarrow{\scriptstyle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

Esempio



$$\begin{tikzcd}
B_1^2 \arrow[d, "in"] & \mathbf{R} & B_1^1 \frown B_0^1 \arrow[d, Rightarrow, "in"] \\
B_2^2 & \mathbf{R} & B_1^1 \frown B_1^1
\end{tikzcd}
\qquad
\begin{tikzcd}
B_1^2 \arrow[d, "\overline{out}"] & \mathbf{R} & B_1^1 \frown B_0^1 \arrow[d, Rightarrow, "\overline{out}"] \\
B_0^2 & \mathbf{R} & B_0^1 \frown B_0^1
\end{tikzcd}$$

Esempio



$$\begin{array}{ccc} B^2_1 & \mathbf{R} & B^1_1 \frown B^1_0 \\ \Big\Downarrow \tau & & \Big\downarrow \tau \\ B^2_1 & \mathbf{R} & B^1_0 \frown B^1_1 \end{array}$$

(sta inattivo!)

(etc. per le altre coppie)

bis. debole come punto fisso

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

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

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 sorvegliati 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 $Q \overset{\alpha}{\Rightarrow} \mathbf{nil}$

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

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

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 $\mathbb{C}[P] \overset{\tau}{\Rightarrow} \mathbb{C}[P]$

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

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

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
congruenza osservazionale debole

Congr. osservazionale debole

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

Equivalentemente

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

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 $\approx$

Congr. osservazionale debole

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

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

$$\begin{tikzcd}
\beta.P \arrow[d, "\beta"'] & \approxeq & \beta.Q \arrow[d, "\beta"] \\
P & \approx & Q
\end{tikzcd}$$

$$P \not\approxeq Q$$

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

Congr. osservazionale debole

Tutte le leggi per la bisimilarità forte sono ancora valide

Inoltre: le leggi τ di Milner

$$p + \tau.p \approxeq \tau.p$$

$$\mu.(p + \tau.q) \approxeq \mu.(p + \tau.q) + \mu.q$$

$$\mu.\tau.p \approxeq \mu.p$$