PSC 2023/24 (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni
http://www.di.unipi.it/~bruni/

http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/start

20 - Weak semantics

CCS syntax

p, q	$::=$	$\mathbf{nil}$	inactive process
	$\mid$	x	process variable (for recursion)
	$\mid$	$\mu.p$	action prefix
	$\mid$	$p \backslash \alpha$	restricted channel
	$\mid$	$p[\phi]$	channel relabelling
	$\mid$	$p + q$	nondeterministic choice (sum)
	$\mid$	$p \vert q$	parallel composition
	$\mid$	$\mathbf{rec}\ x.\ p$	recursion

(operators are listed in order of precedence)

CCS op. semantics

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

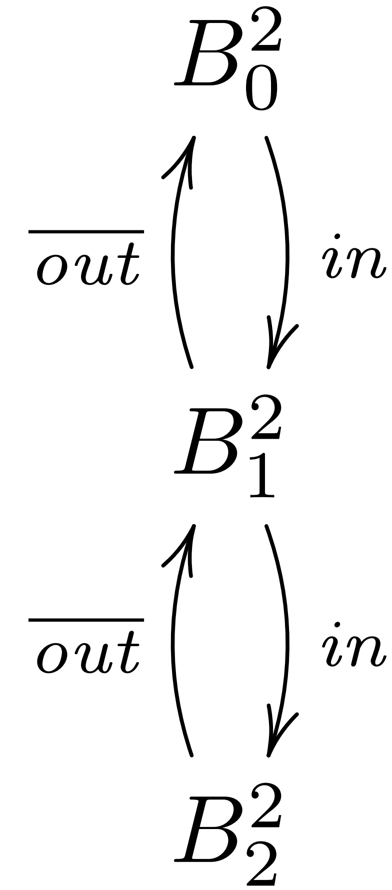
CCS
Weak transitions

Sequential buffer

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

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

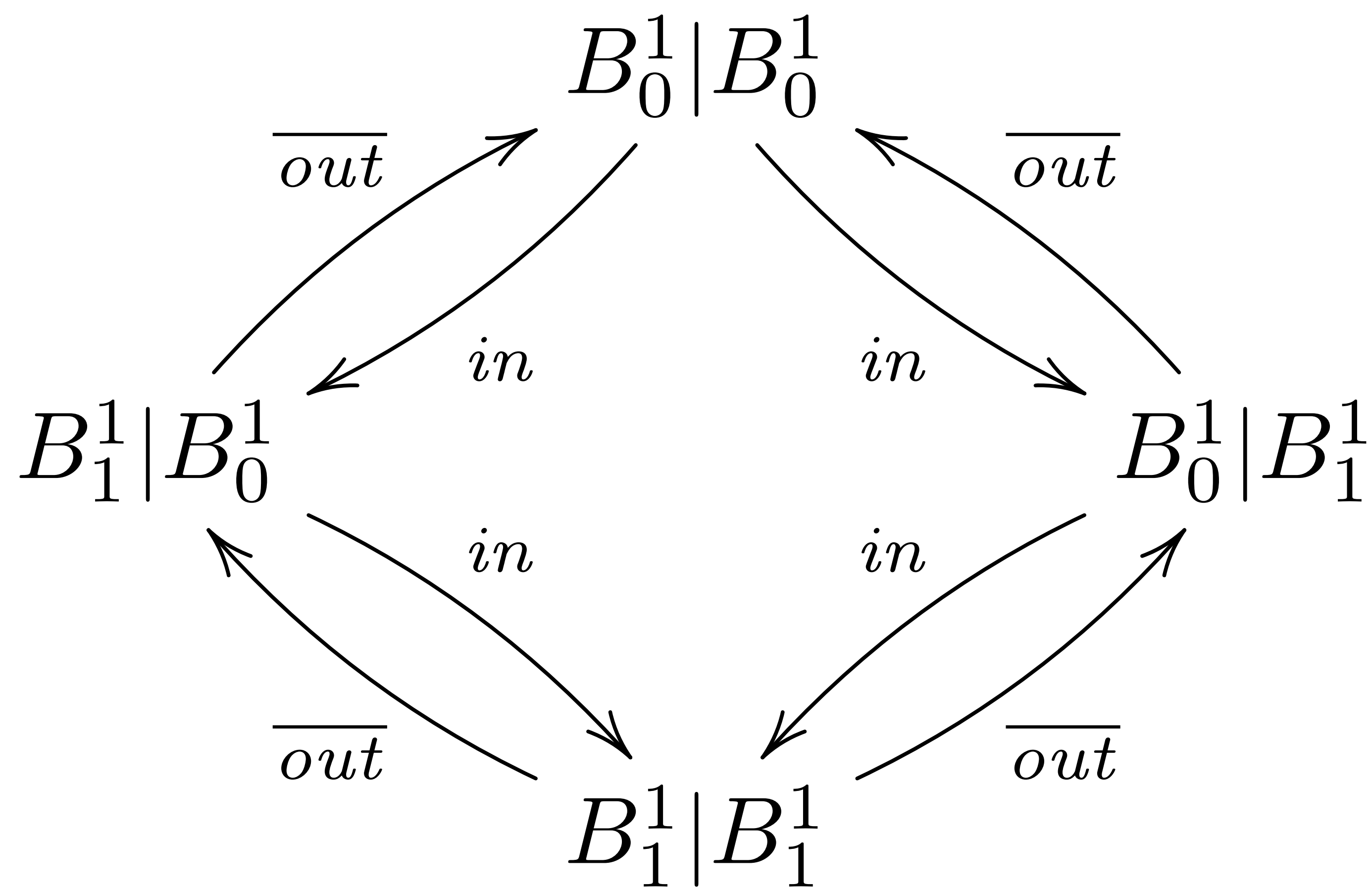
$$B_2^2 \triangleq \overline{out}.B_1^2$$



Parallel buffer

$$B^1_0 \triangleq in.B^1_1$$

$$B^1_1 \triangleq \overline{out}.B^1_0$$

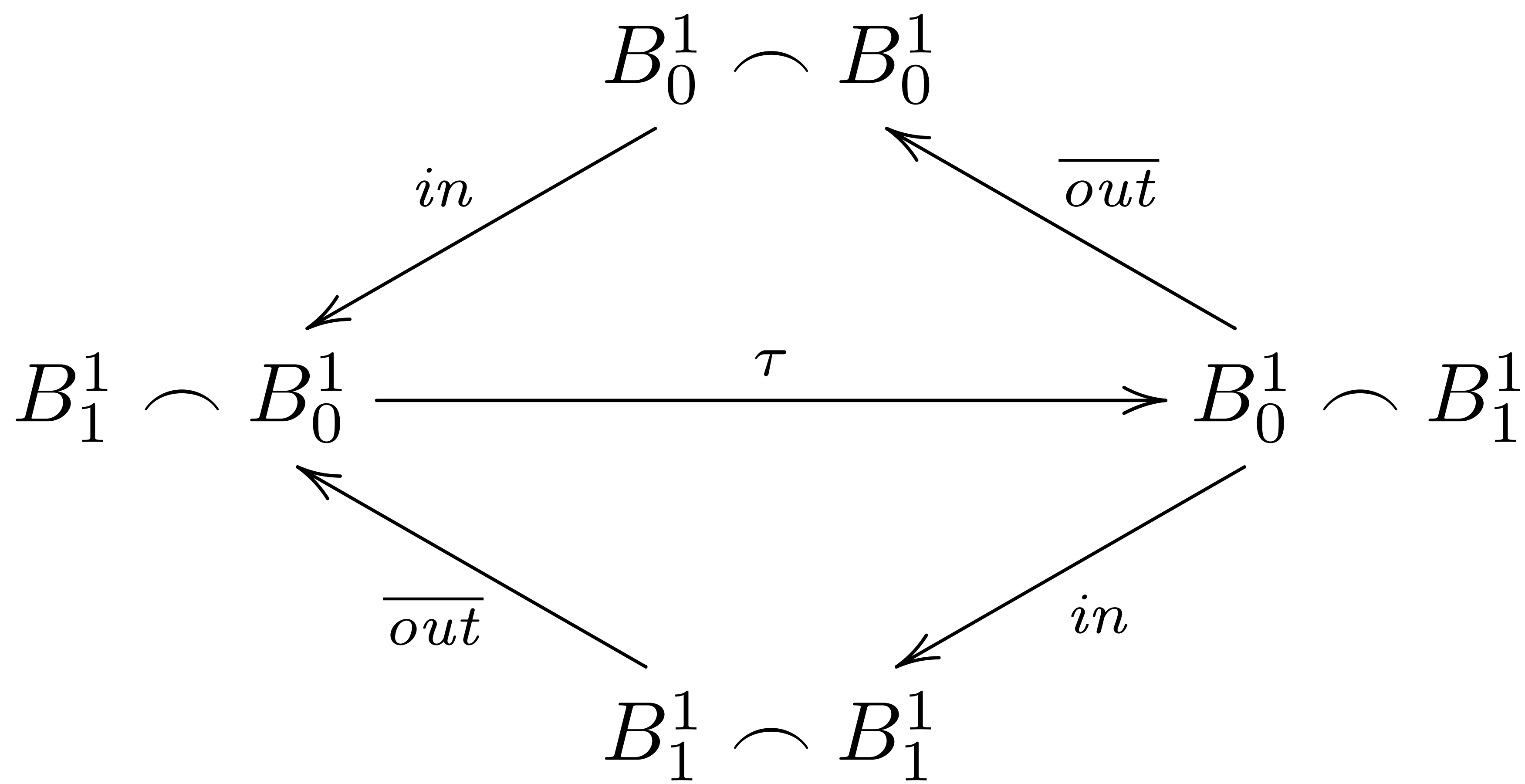


Linked buffer

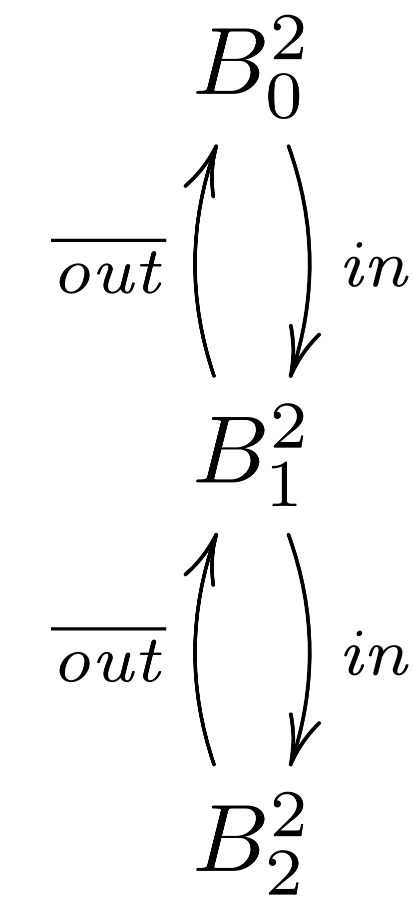
$$B_0^1 \triangleq in.B_1^1 \qquad \eta(out) = c$$

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

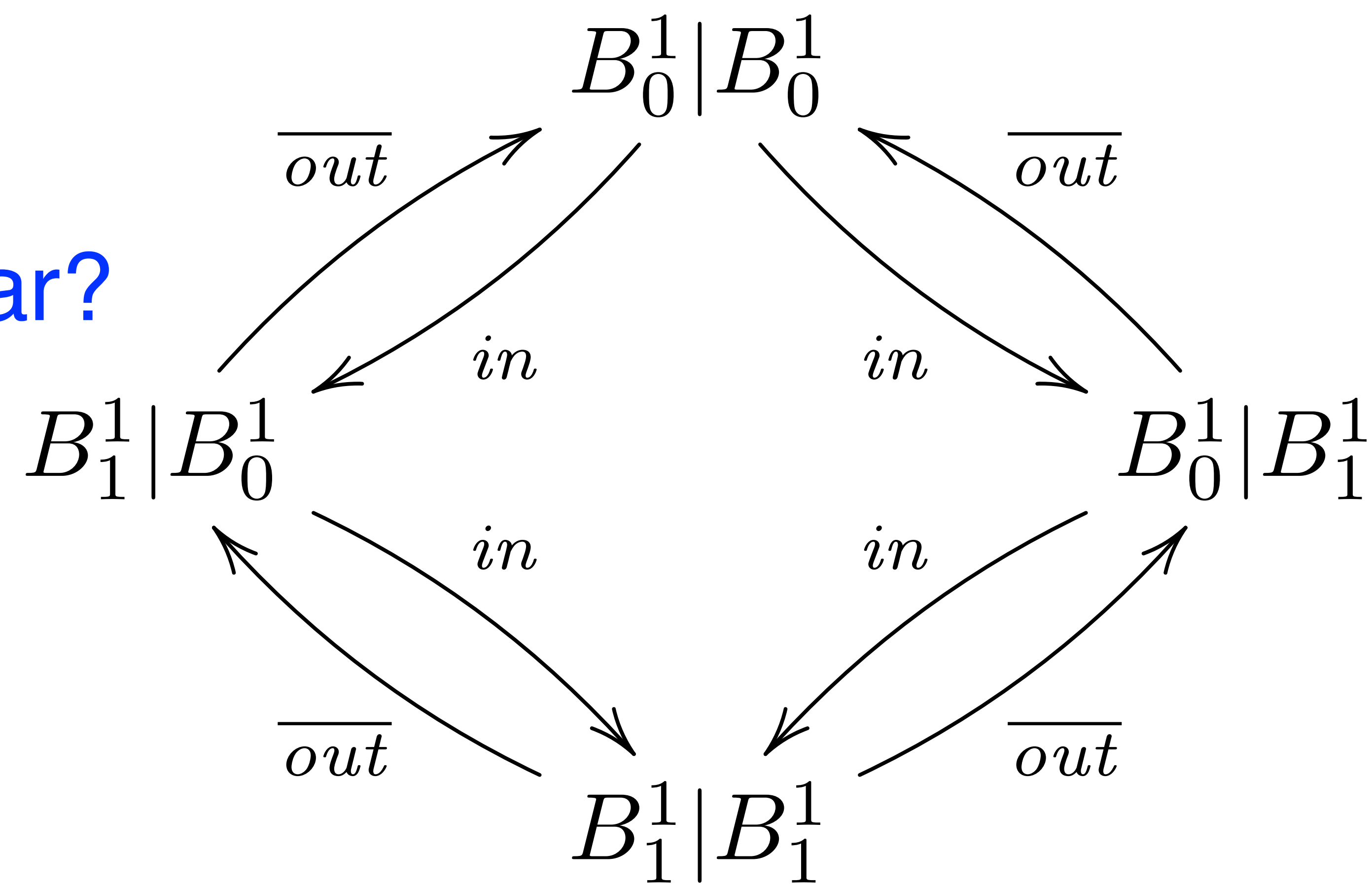
$$B_1^1 \triangleq \overline{out}.B_0^1 \qquad \phi(in) = c$$

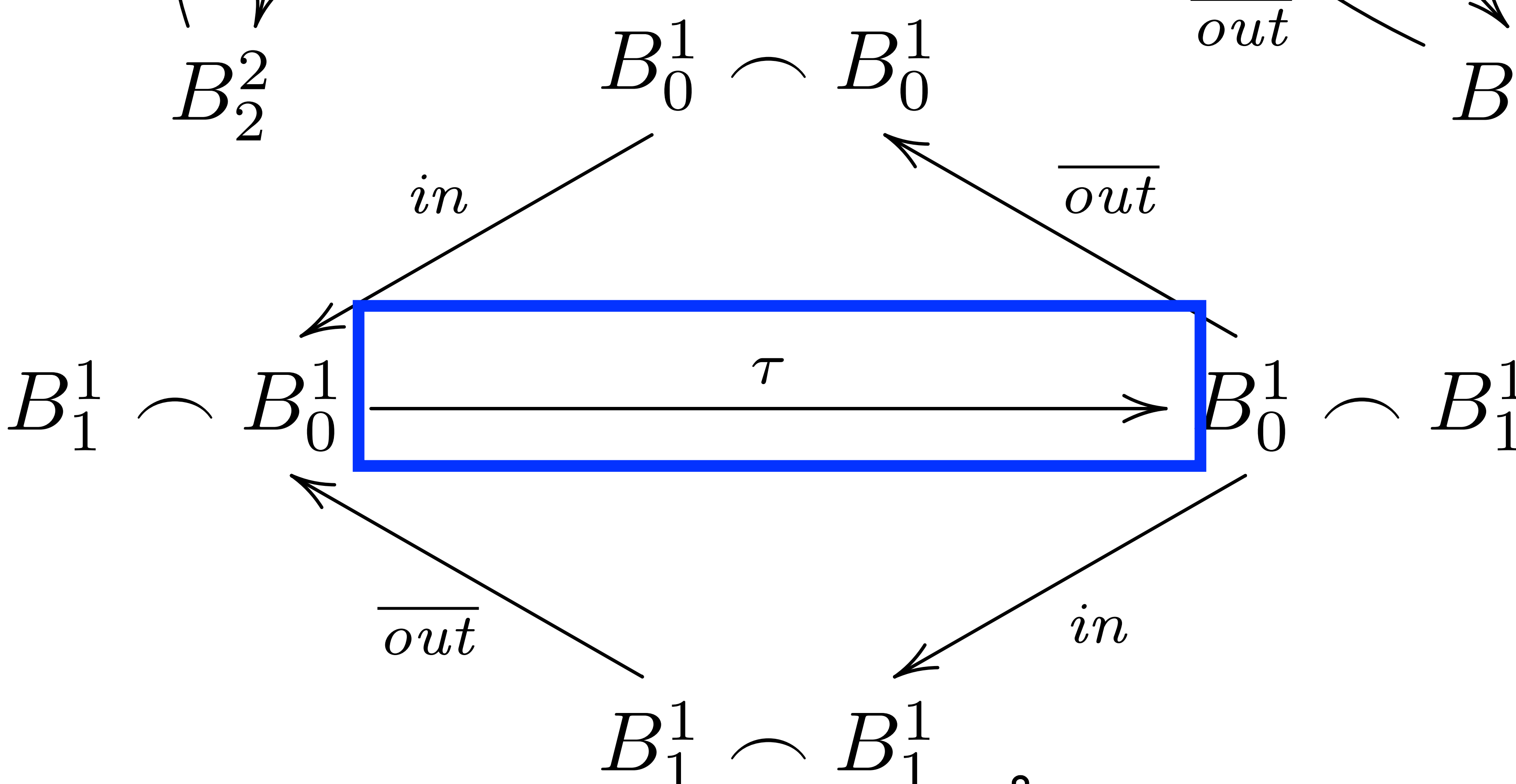


Comparing buffers



are they all strong bisimilar?





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

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

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

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

Silent transitions

τ-transitions are silent, non observable

they represent internal steps of the system

they can be used just for bookkeeping

can we abstract away from them?

can we find a broader equivalence?

necessary to relate an abstract specification (little use of τ)
with a concrete implementation (lots/tons of τ)

Weak bisimulation game

coarser equivalence: more power to the defender!

Alice picks a process and an ordinary transition

Bob replies possibly using many additional silent transitions

arbitrarily many, but finitely many

such sequences are called *weak* transitions

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

what if Alice picks a silent transition?

Bob can just leave the other process idle

i.e. can choose not to move

Weak transitions

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

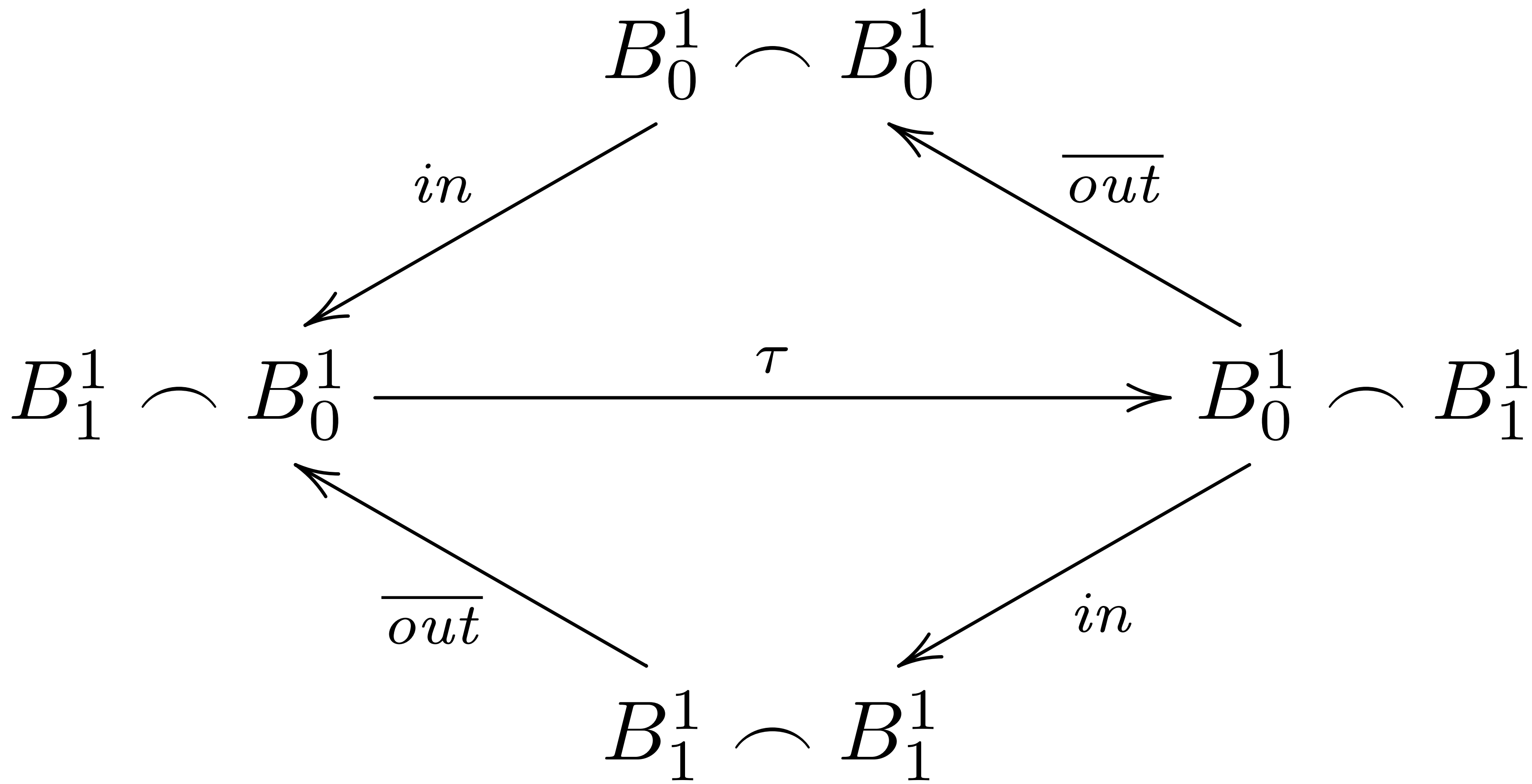
$$p = q \;\vee\; p \stackrel{\tau}{\rightarrow} \ldots \stackrel{\tau}{\rightarrow} q$$

p can reach *q* via a (possibly empty) finite sequence of τ-transitions

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

p can reach *q* via a λ-transition possibly preceded and followed by empty/finite sequences of τ-transitions

Example



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

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

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

CCS
weak bisimulation

Weak bisimulation

$\mathbf{R}$ is a *weak* bisimulation if

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

Alice plays

Bob replies

weak transitions

Weak bisimilariity

weak bisimilarity:

$p \approx q \quad \text{iff} \quad \exists \mathbf{R}$ a weak bisimulation with $(p, q) \in \mathbf{R}$

TH. weak bisimilarity is an equivalence relation

TH. any strong bisimulation is a weak bisimulation

Cor. strong bisimilarity implies weak bisimilarity

Weaker bisimilarity?

what if we give extra power to Alice as well?

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

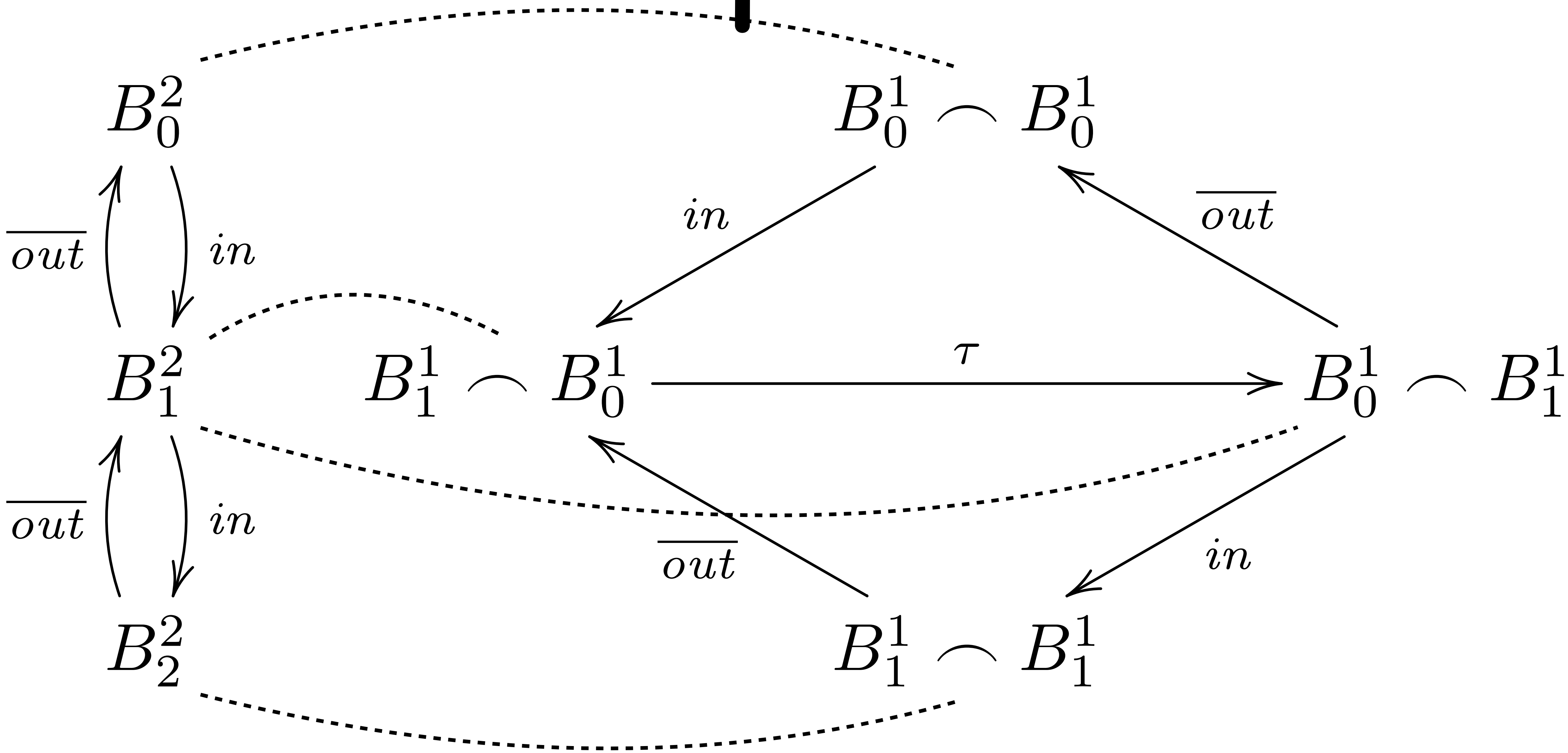
Alice plays

Bob replies

weak transitions

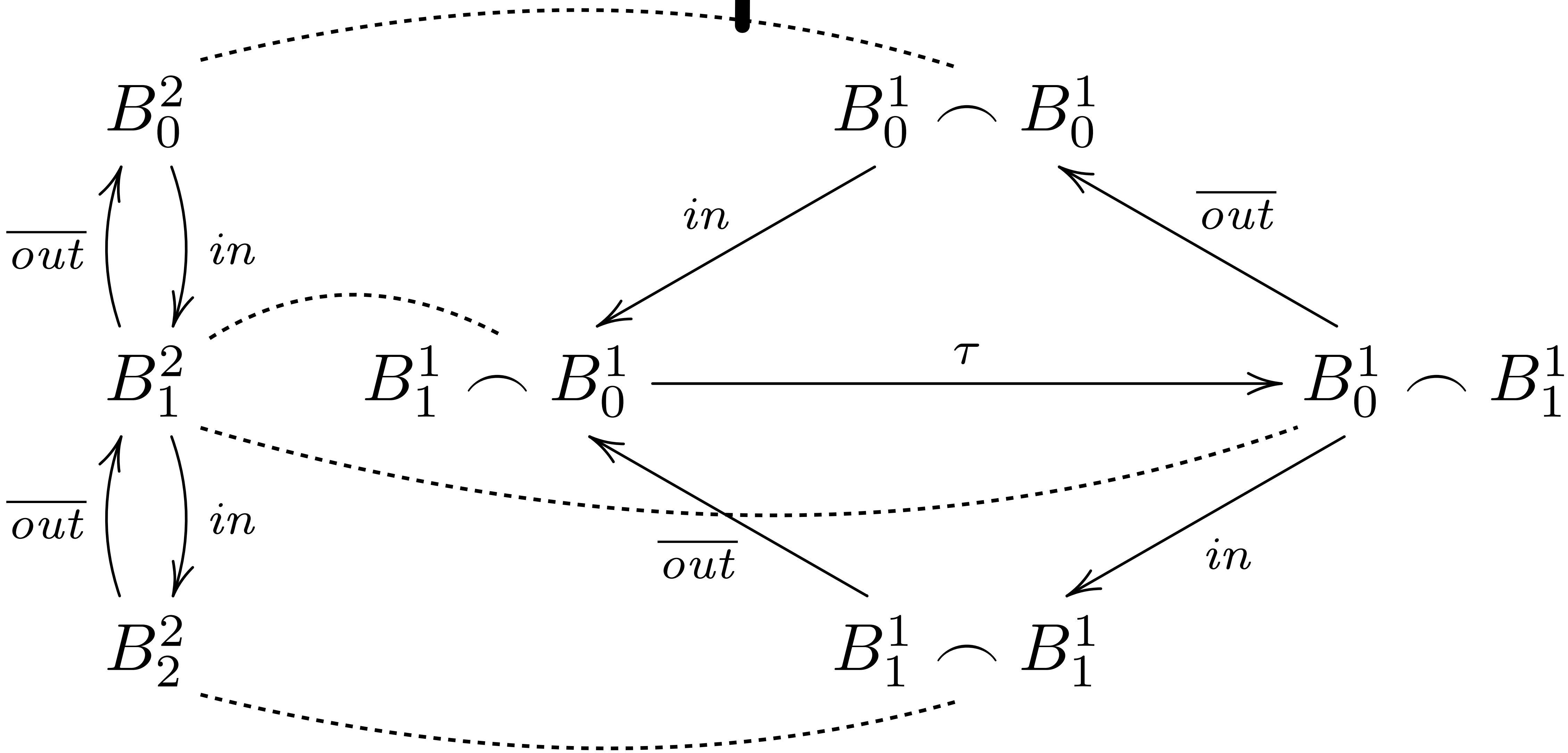
nothing changes: we still get the same weak bisimilarity

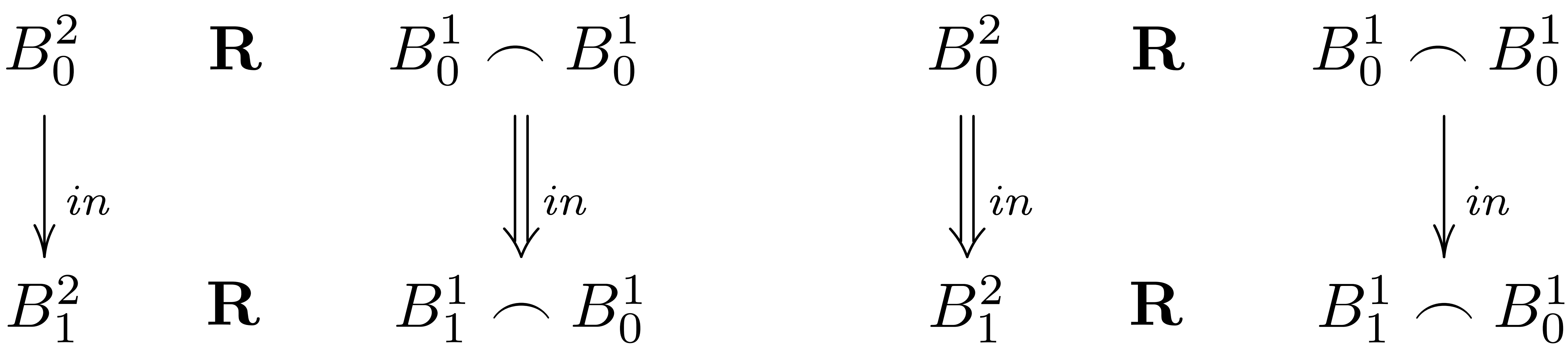
Example



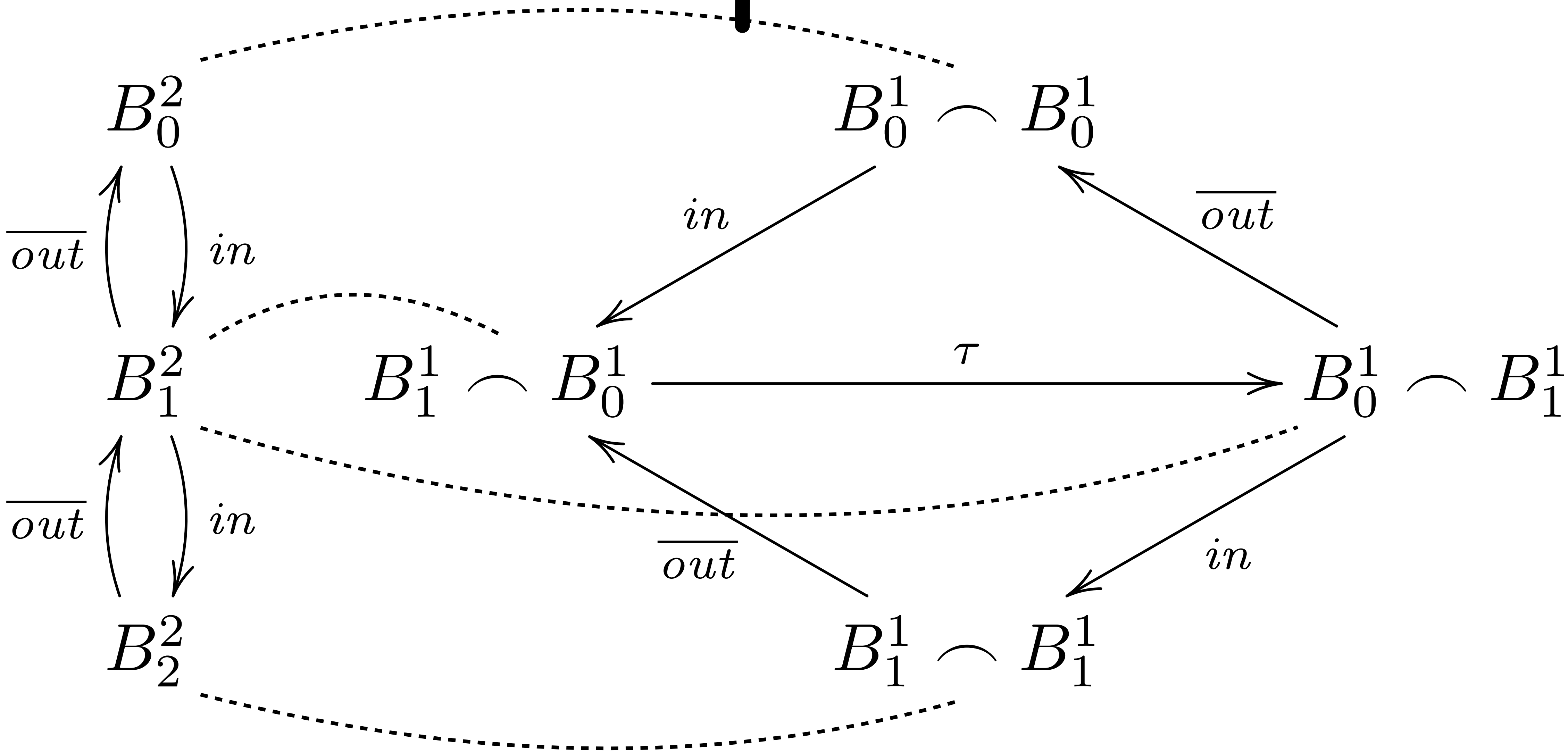
$$\mathbf{R} \triangleq \left\{ \begin{array}{l} (B^2_0, B^1_0 \frown B^1_0), \\ (B^2_1, B^1_1 \frown B^1_0), \\ (B^2_1, B^1_0 \frown B^1_1), \\ (B^2_2, B^1_1 \frown B^1_1) \end{array} \right\}$$ is a weak bisimulation relation

Example

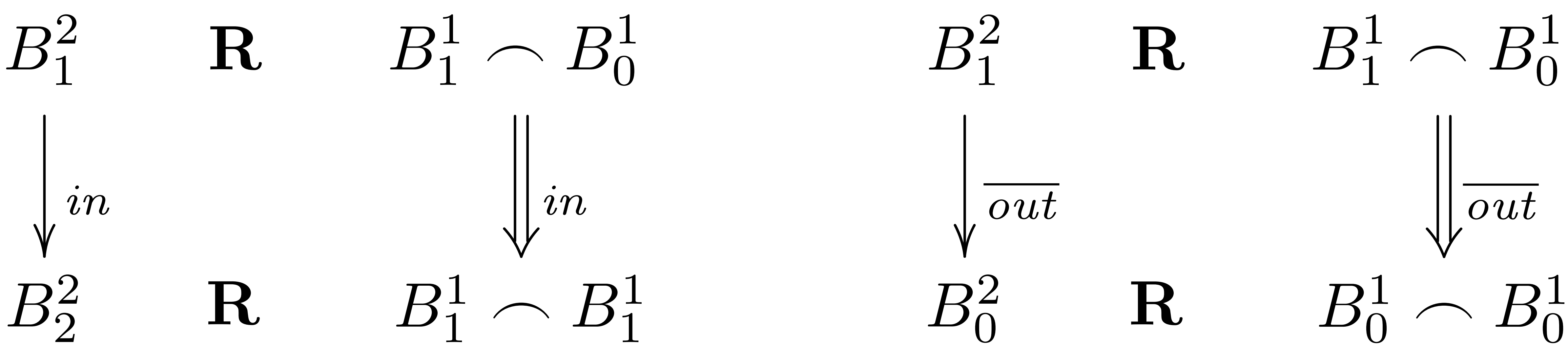

B^2_0
$B^1_0 \frown B^1_0$
$\overline{out}$
in
B^2_1
$B^1_1 \frown B^1_0$
τ
$B^1_0 \frown B^1_1$
B^2_2
$B^1_1 \frown B^1_1$


B^2_0 $\mathbf{R}$ $B^1_0 \frown B^1_0$
in
B^2_1 $\mathbf{R}$ $B^1_1 \frown B^1_0$
B^2_0 $\mathbf{R}$ $B^1_0 \frown B^1_0$
in
B^2_1 $\mathbf{R}$ $B^1_1 \frown B^1_0$

Example

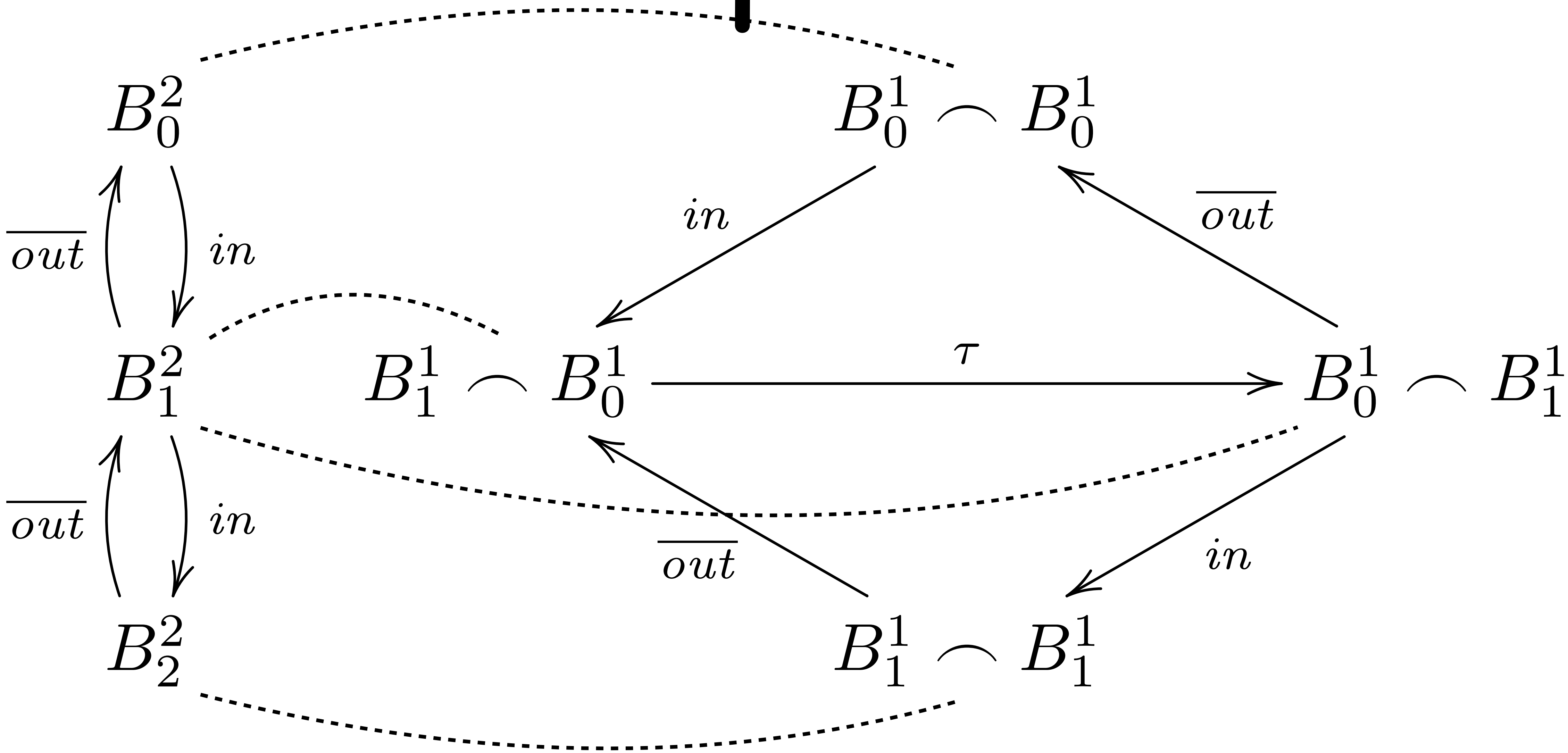


B_0^2
B_1^2
B_2^2
$\overline{out}$
in
$B_0^1 \frown B_0^1$
$B_1^1 \frown B_0^1$
$B_0^1 \frown B_1^1$
$B_1^1 \frown B_1^1$
τ

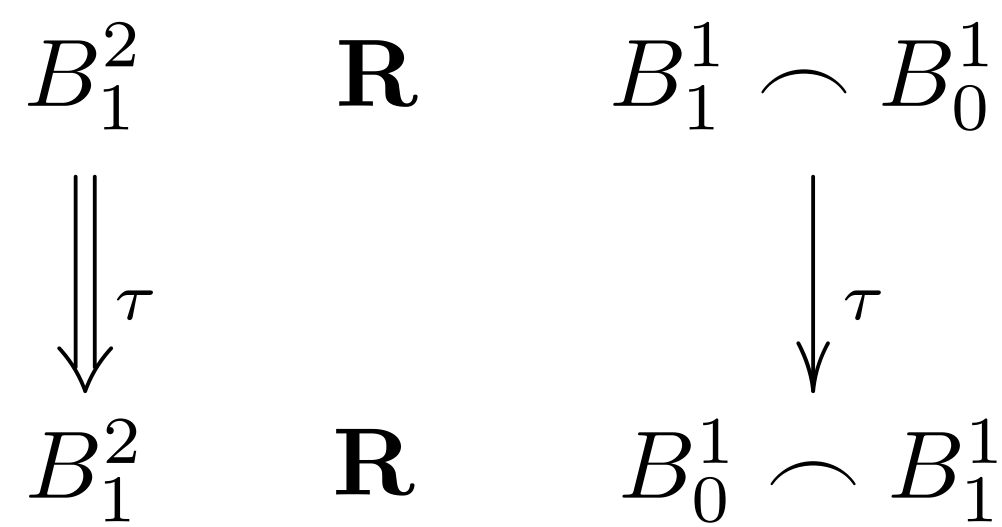


$B_1^2 \quad \mathbf{R} \quad B_1^1 \frown B_0^1$
in
$B_2^2 \quad \mathbf{R} \quad B_1^1 \frown B_1^1$
$B_1^2 \quad \mathbf{R} \quad B_1^1 \frown B_0^1$
$\overline{out}$
$B_0^2 \quad \mathbf{R} \quad B_0^1 \frown B_0^1$

Example



(stays idle!)



(etc. for the other pairs)

Weak bis as a fixpoint

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

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

maps relations to relations

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

a weak bisimulation

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

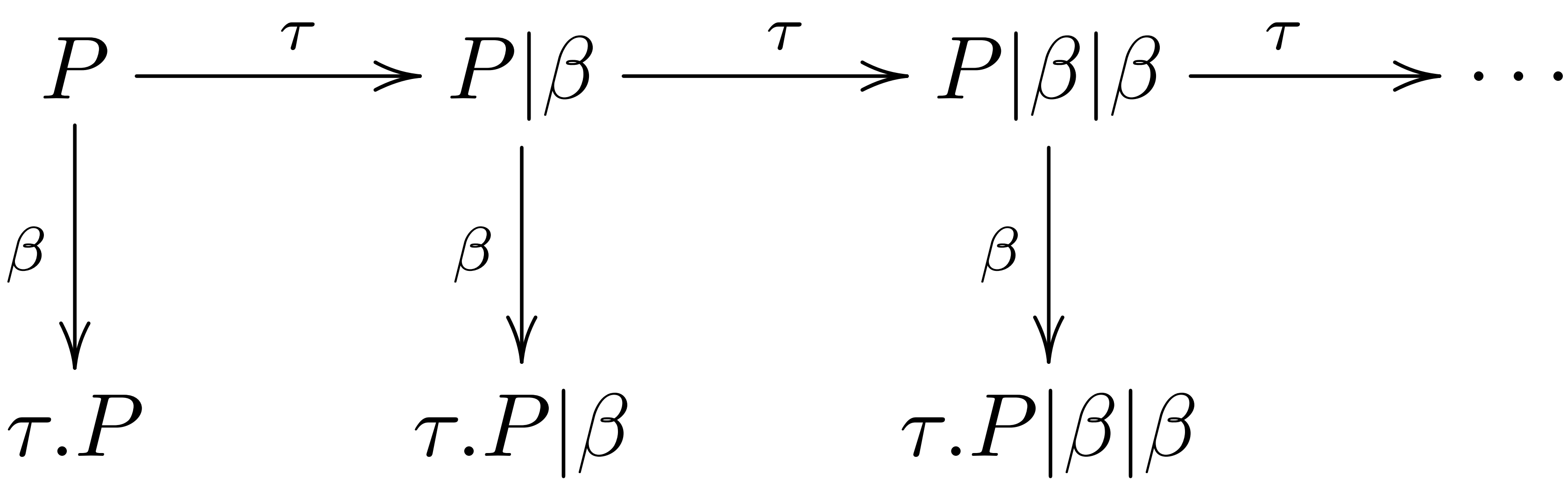
weak bisimilarity is a fixpoint

CCS
problems with weak semantics

Problems with weak bis

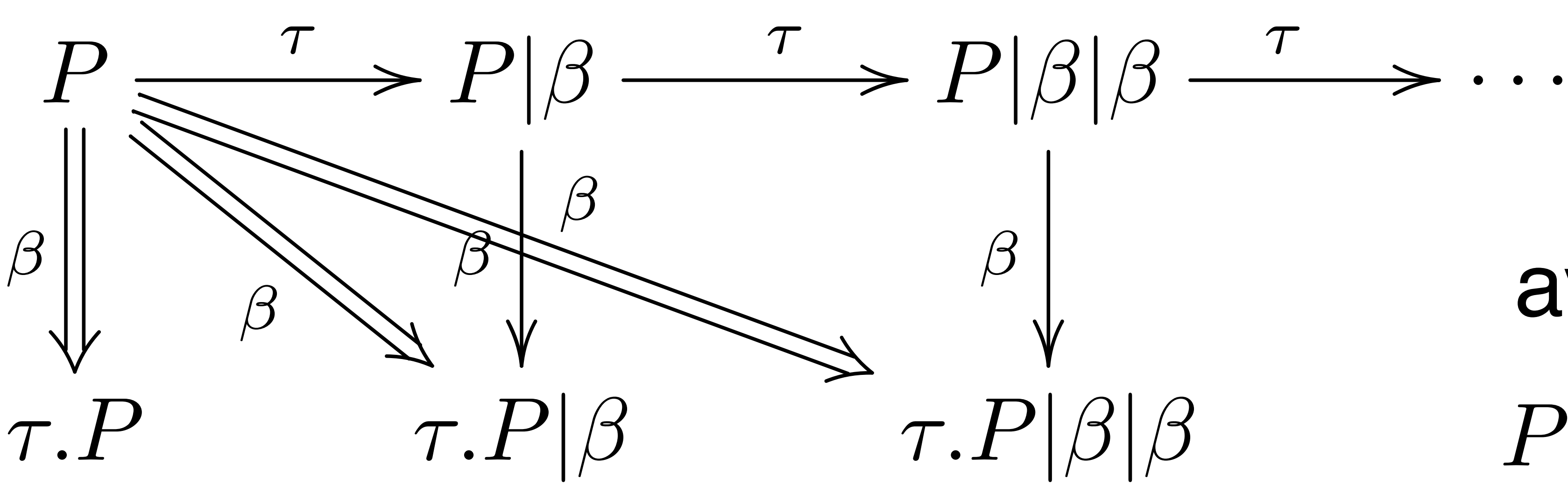
with respect to weak transitions,
guarded processes can have infinitely branching LTS

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



many arrows omitted

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



avoid τ-prefixes?

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

Problems with weak bis

weak bisimilarity is not a congruence (w.r.t. +)

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

if $P \xrightarrow{\alpha} \mathbf{nil}$ then $Q \stackrel{\alpha}{\Rightarrow} \mathbf{nil}$

if $Q \xrightarrow{\tau} \alpha$ then $P \stackrel{\tau}{\Rightarrow} P$

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

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

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

take the context $\mathbb{C}[\cdot] \triangleq [\cdot] + \beta$

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

Bob can only reply $\mathbb{C}[P] \stackrel{\tau}{\Rightarrow} \mathbb{C}[P]$

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

Bob cannot reply $\alpha \stackrel{\beta}{\not\Rightarrow}$

Alice wins!

Problems with weak bis

cannot distinguish between deadlock and silent divergence

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

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

CCS
weak observational congruence

Weak obs congruence

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

Equivalently

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

not a recursive definition!
(refers to weak bisimilarity)

at the level of bisimulation game:

Bob is not allowed to use an idle move at the very first turn
(at the following turns, ordinary weak bisimulation game)

TH. $\cong$ is the largest congruence contained in $\approx$

Weak obs congruence

Note: $\approxeq$ is not a weak bisimulation!

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

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

$$P \not\approxeq Q$$

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

Weak obs congruence

All the laws for strong bisimilarity are still valid

Additionally: Milner's τ-laws

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

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

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