π- calculus continued

$x, y, z, a, b, c \in$ Channel Names

$P, Q ::=$	$x(y).P$	receive y on x
	$x[y].P$	send y on x
	$P \mid Q$	parallel composition
	$(\nu x)\ P$	channel scope / creation
	$!P$	repeat P
	0	halt

$P \equiv Q$ structural congruence

$x[z].P \mid x(y).Q \longrightarrow P \mid Q[z/y]$ communication

In Lambda Calculus: <u>Contextual</u> <u>Equivalence</u>

$M =_{ctx} N$ iff $\forall C.\ C[M]\Downarrow$ iff $C[N]\Downarrow$

What do we do for π-calculus?

$\underset{\sim}{\alpha} ::= x(y) \mid x[y] \mid \tau$ "actions"

$\mid (\nu y)\, x[y]$ "observations"

(Strong)
<u>Dynamic binding simulation</u> is the largest symmetric relation $\mathcal{S}$ s.t.

if $(P, Q) \in \mathcal{S}$ implies that for all contexts $C[\,]$

when $C[P] \xrightarrow{\alpha} P'$ there exists Q' such that $C[Q] \xrightarrow{\alpha} Q'$ and $(P', Q') \in \mathcal{S}$

- an equivalence relation
- a congruence
- includes α-equivalec $\equiv\ \subseteq \mathcal{S}$

$\boxed{(0,\ \nu x.\, x[x]) \in \mathcal{S}}$

Bisimulations

Labeled Transitions Systems (LTS)

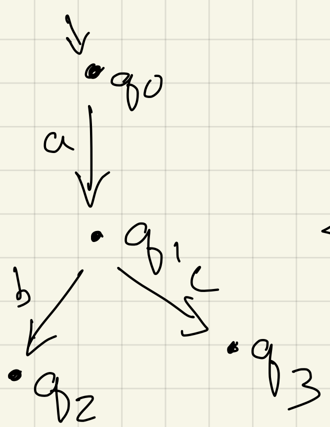
Some set of States Q

Some set of Actions Σ $\quad (\tau \in \Sigma)$

Transition Relation $\rightarrow$

$$\rightarrow \subseteq Q \times \Sigma \cup \{\tau\} \times Q$$

$$q_0 \xrightarrow{a} q_1 \quad (q_0, a, q_1) \in \rightarrow$$



$\Leftarrow \quad tr(q_0) = \{ab, ac\}$

Defn. Let $R \subseteq Q \times Q$ be a relation

R is a simulation if for all $(p, q) \in R$

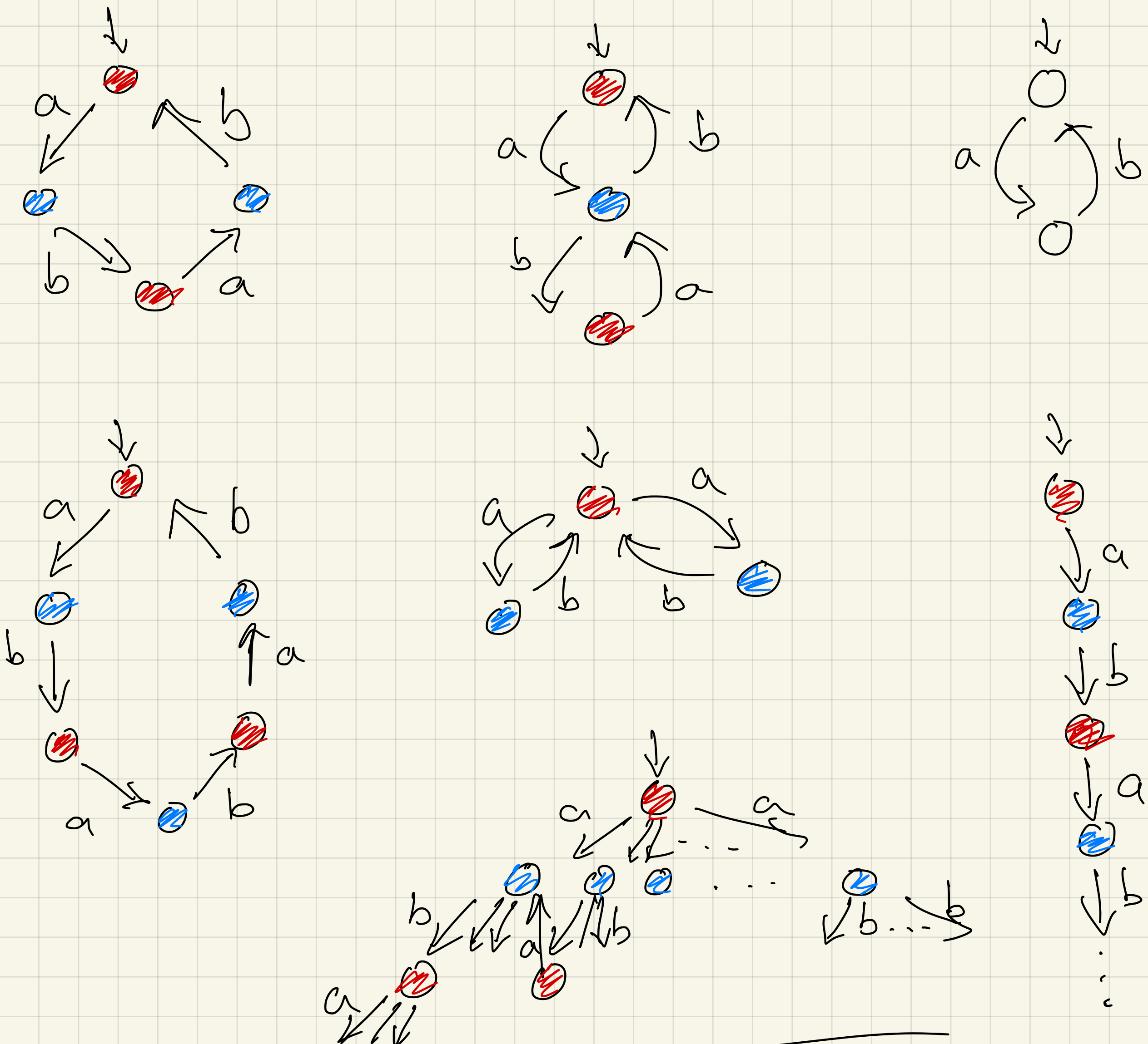
if $p \xrightarrow{a} p'$ then $\exists q'.\ q \xrightarrow{a} q'$

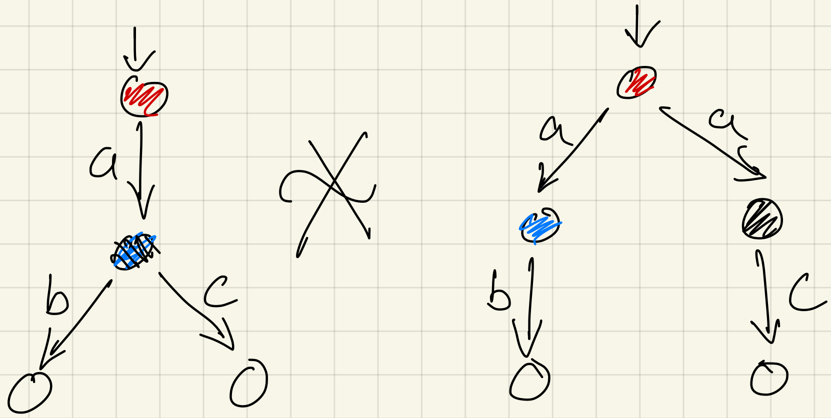
and $(p', q') \in R$.

R is a bisimulation if R and R^{-1} are simulations

Two states are bisimilar iff there exists a bisimulation that relates them $\boxed{p \sim q}$

Examples





{ab, ac}

not bisimilar

the same traces

Build an LTS for π-calculus

$\pi \qquad \alpha ::= x(y) \mid x[y] \mid \tau \mid (\nu y)\, x[y]$

$\quad Q = $ the set of π-calculus terms

$$x(y).P \xrightarrow{x(y)} P$$

$$x[y].P \xrightarrow{x[y]} P$$

$$\frac{P \xrightarrow{x[y]} P' \qquad Q \xrightarrow{x(z)} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'[y/z]} \quad (\text{com}) \qquad \text{add symmetric version}$$

Structural rules

$$\frac{P \mid !P \xrightarrow{\alpha} P'}{!P \xrightarrow{\alpha} P'} \qquad \frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \quad (\text{and symm.})$$

$$\frac{P =_\alpha P' \quad P' \xrightarrow{\alpha} P''}{P \xrightarrow{\alpha} P''}$$

$$\frac{P \xrightarrow{\alpha} P'}{(\nu x) P \xrightarrow{\alpha} (\nu x) P'} \quad x \notin \text{names}(\alpha)$$

$$\frac{P \xrightarrow{x[y]} P'}{(\nu y) P \xrightarrow{(\nu y)\, x[y]} P'} \quad (x \neq y)$$

$$\frac{P \xrightarrow{(\nu y)\, x[y]} P' \qquad Q \xrightarrow{x(z)} Q'}{P \mid Q \xrightarrow{\tau} (\nu y)\, P' \mid Q'} \quad (\text{and symm})$$

$$P = a(x).\left(\underbrace{x[z] \mid b(y).y[w]}_{R}\right)$$

$$Q = a(x).0$$

$P \not\to \qquad Q \not\to \qquad P \not\sim Q$

$P \xrightarrow{a(x)} R \qquad Q \xrightarrow{a(x)} 0 \qquad R \not\sim 0$

$$P \mid a[b] \to b[z] \mid b(y).y[w] \to z[w]$$

$$Q \mid a[b] \to 0$$

- A relation $\mathcal{R}$ is an <u>open bisimulation</u> (→ symmetric)

if $(P,Q) \in \mathcal{R}$ implies that
for every substitution σ: Names $\to$ Names

whenever $\sigma(P) \xrightarrow{\alpha} P'$ there exists Q' s.t.
$\sigma(Q) \xrightarrow{\alpha} Q'$ and $(P',Q') \in \mathcal{R}$.

Say $P \sim_o Q$ iff $\exists \mathcal{R}$, open bisimulation $(P,Q) \in \mathcal{R}$

<u>Theorem</u> $\sim_o$ coincides with $\sim$

Dynamic binding simulation coincides with open bisimulation.

Weak Simulation

LTS $q \xrightarrow{\alpha} q'$ define $p \xRightarrow{a} q$ $a \in \Sigma$

$a \neq \tau$

$$p \xrightarrow{\tau}{}^{*} \xrightarrow{a} q$$

(A weak step of computation)

$p \approx q$ if there exists a weak open bisimulation R s.t. $(p, q) \in R$.

$$p \sim q \Rightarrow \boxed{p \approx q}$$

- Equivalence
- Congruence
- closed under substitution
- $\equiv \subseteq \approx$

Session Types as Intuitionistic Linear Propositions

Caires and Pfenning 2010

$$P ::= 0 \mid (\nu x) P \mid x[y].P \mid x(y).P$$
$$\quad P \mid Q \mid\ !x(y).P$$

only replicated input

new $\begin{cases} x.\mathrm{inl}; P \mid x.\mathrm{inr}; P \mid x.\mathrm{case}(P, Q) \end{cases}$

$$x.\mathrm{inl}; P \mid x.\mathrm{case}(Q, R) \to P \mid Q$$
$$x.\mathrm{inr}; P \mid x.\mathrm{case}(Q, R) \to P \mid R$$

Example

- Server that allows clients to make a purchase and get a receipt or request a price

product name, credit card pin

$$\mathrm{ServerBody}_s \triangleq s.\mathrm{case}\,(s(pn).s(cn).(\nu rc).s[rc].0,\ s(pn).(\nu p).s[p].0)$$

$$\mathrm{Server}_c \triangleq\ !c(s).\mathrm{ServerBody}_s$$

$$\mathrm{ClientBody}_s \triangleq s.\mathrm{inl}; (\nu\, item)\, s[item].(\nu\, pin)\, s[pin].s(receipt).0$$

$$\mathrm{Client}_c \triangleq (\nu s)\, c[s].\mathrm{ClientBody}_s$$

$$(\mathrm{ClientBody}_s \mid \mathrm{clientBody}_s \mid \mathrm{Server}_c) \not\Rightarrow$$

bad!

$$\mathrm{SessionProt} \triangleq \begin{array}{l} N \multimap I \multimap (N \otimes 1) \\ \& \; N \multimap (I \otimes 1) \end{array}$$

$$\mathrm{ServerProt} \triangleq \; !\,\mathrm{SessionProt}$$

$$\mathrm{ClientProt} \triangleq \begin{array}{l} N \otimes (I \otimes (N \multimap 1)) \\ \oplus \; N \otimes (I \multimap 1) \end{array}$$

Proposition: given a type A and distinct names x, y, there is a cut-free process $id_A(x,y)$

s.t. $x : A \vdash id_A(x,y) :: y : A$

$$x : 1 \vdash 0 :: y : 1$$

$$x : A \otimes B \vdash x(z).(\nu n)\, y[n].\,(id_B(x,n) \mid id_A(z,y)) :: y : B \otimes A$$