## An Example

$$P_{1} \xrightarrow{a} P_{1}^{'}$$
  $P_{2} \xrightarrow{b} P_{1}$ 
 $Q_{1} \xrightarrow{a} Q_{1}^{'}$   $Q_{2} \xrightarrow{b} Q_{1}$ 
 $P_{2} \sim P_{1}^{'}$ 
 $Q_{2} \sim Q_{1}^{'}$ 

Q:  $P_1$  and  $Q_1$  are bisimilar, i.e.  $P_1 \sim Q_1$ ?

### An Example

$$P_1 \xrightarrow{a} P_1'$$
  $P_2 \xrightarrow{b} P_1$ 
 $Q_1 \xrightarrow{a} Q_1'$   $Q_2 \xrightarrow{b} Q_1$ 
 $P_2 \sim P_1'$ 
 $Q_2 \sim Q_1'$ 

$$R = \{(P_1, Q_1), (P_2, Q_2)\}$$

Q: Such R must be a strong bisimulation?

A: NO. In fact,  $\sim R \sim$  is a strong bisimulation.

## **Up-to Bisimulation**

Note that  $\sim S \sim$  is the composition of three relations, so that  $P \sim S \sim Q$  means that for some P' and Q' we have

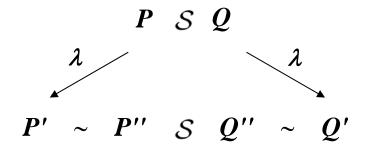
$$P \sim P' \mathcal{S} Q' \sim Q$$

Definition S is a strong bisimulation up to  $\sim$  if P S Q implies, for all  $\lambda \in A$ ,

- (i) If  $P \xrightarrow{\lambda} P'$  then for some Q',  $Q \xrightarrow{\lambda} Q'$  and P'  $\sim S \sim Q'$
- (ii) If  $Q \xrightarrow{\lambda} Q'$  then for some P',  $P \xrightarrow{\lambda} P'$  and P'  $\sim S \sim Q'$

## **Up-to Bisimulation**

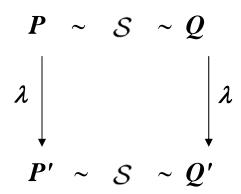
Pictorially, clause (i) says that if  $QSP \xrightarrow{\lambda} P'$  then we can fill in the following diagram:

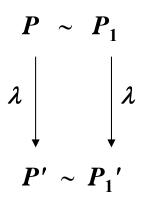


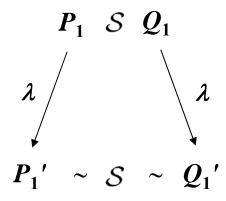
## **Up-to Bisimulation**

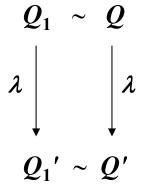
Lemma If s is a strong bisimulation up to  $\sim$ , then  $\sim s \sim$  is a strong bisimulation.

*Proof.* Let  $P \sim S \sim Q$  and  $P \xrightarrow{\lambda} P'$ . By symmetry it will be enough to show that we can fill in the following diagram:









## Making Use of the Up-to Bisimulation

Proposition If  $_{\mathcal{S}}$  is a strong bisimulation up to  $\sim$  then  $_{\mathcal{S}} \subseteq \sim$ .

Proof.  $S \subseteq Id S Id \subseteq \sim S \sim \subseteq \sim$ .

Hence, to prove  $P \sim Q$ , we only have to find a strong bisimulation up to  $\sim$  which contains (P, Q).

## An Example for Up-to Technique

$$P_1 \xrightarrow{a} P_1' \qquad P_2 \xrightarrow{b} P_1$$

$$Q_1 \xrightarrow{a} Q_1' \qquad Q_2 \xrightarrow{b} Q_1$$

$$P_2 \sim P_1$$

$$Q_2 \sim Q_1$$

 $R = \{(P_1, Q_1), (P_2, Q_2)\}$  is a strong bisimulation up – to ~.

And a strong bisimulaiton is  $R' = R \square \sim$ 

Q: Such R must be a strong bisimulation?

A: NO. The fact is, a bisimulation ~R~ could be given based on R.

# Property of Strong bisimilarity

- Dynamic laws
  - involving only the dynamic combinators (Prefix, Summation, Constants)
- Static laws
  - involving only the static combinators (Composition, Restriction, Relabelling)
- Expansion law
  - to grow a derivation tree to build a complete transition graph

## **Dynamic Laws**

### **Proposition** Monoid laws

(1) 
$$P + Q \sim Q + P$$

(2) 
$$P + (Q + R) \sim (P + Q) + R$$

(3) 
$$P + P \sim P$$

(4) 
$$P + 0 \sim P$$

### Static Laws

### Proposition

- (1)  $P \mid Q \sim Q \mid P$
- (2)  $P | (Q | R) \sim (P | Q) | R$
- (3)  $P \mid 0 \sim P$
- (4)  $P \setminus L \sim P$  if  $\mathcal{L}(P) \cap (L \cup \overline{L}) = \emptyset$
- (5)  $P \setminus K \setminus L \sim P \setminus (K \cup L)$
- (6)  $P[f] \setminus L \sim P \setminus f^{-1}(L)[f]$
- (7)  $(P \mid Q) \setminus L \sim P \setminus L \mid Q \setminus L \quad \text{if } \mathcal{L}(P) \cap \overline{\mathcal{L}(Q)} \cap (L \cup \overline{L}) = \emptyset$
- (8)  $P[Id] \sim P$
- (9)  $P[f] \sim P[f']$  if  $f \upharpoonright \mathcal{L}(P) = f' \upharpoonright \mathcal{L}(P)$
- $(10)P[f][f'] \sim P[f' \circ f]$
- $(11)(P|Q)[f] \sim P[f]|Q[f]$  if  $f \upharpoonright (L \cup \overline{L})$  is one-to-one, where  $L = \mathcal{L}(P) \cup \mathcal{L}(Q)$

# **Expansion Law**

Let 
$$P \equiv (P_1[f_1] \mid \dots \mid P_n[f_n]) \setminus L$$
, with  $n \geq 1$ . Then 
$$P \sim \sum \{f_i(\lambda).(P_1[f_1] \mid \dots \mid P_i'[f_i] \mid \dots \mid P_n[f_n]) \setminus L:$$
 
$$P_i \xrightarrow{\lambda} P_i', f_i(\lambda) \not\in L \cup \overline{L}\} + \sum \{\tau.(P_1[f_1] \mid \dots \mid P_i'[f_i] \mid \dots \mid P_j'[f_j] \mid \dots \mid P_n[f_n]) \setminus L:$$
 
$$P_i \xrightarrow{\alpha_1} P_i', P_j \xrightarrow{\alpha_2} P_j', f_i(\alpha_1) = \overline{f_j(\alpha_2)}, i < j\}$$

*Proof.* We shall first consider the simpler case in which there is no Relabelling or Restriction. In fact, we shall prove the following by induction on n:

If 
$$P \equiv P_1 \mid \cdots \mid P_n$$
,  $n \geq 1$ , then

$$P \sim \sum \{\lambda.(P_1 \mid \dots \mid P'_i \mid \dots \mid P_n) : 1 \leq i \leq n, P_i \xrightarrow{\lambda} P'_i\}$$

$$+ \sum \{\tau.(P_1 \mid \dots \mid P'_i \mid \dots \mid P'_j \mid \dots \mid P_n) :$$

$$1 \leq i < j \leq n, P_i \xrightarrow{\alpha} P'_i, P_j \xrightarrow{\overline{\alpha}} P'_j\}$$

For n=1, we are reduced to proving  $P_1 \sim \sum \{\lambda.P_1': P_1 \xrightarrow{\lambda} P_1'\}$ , which is immediate. So assume the result for n, and consider  $R \equiv P \mid P_{n+1}$ .

It is immediate form the semantic rules  $Com_1$ ,  $Com_2$  and  $Com_3$  that

$$R \sim \sum \{\lambda.(P'|P_{n+1}): P \xrightarrow{\lambda} P'\}$$

$$+ \sum \{\lambda.(P|P'_{n+1}): P_{n+1} \xrightarrow{\lambda} P'_{n+1}\}$$

$$+ \sum \{\tau.(P'|P'_{n+1}): P \xrightarrow{\alpha} P', P_{n+1} \xrightarrow{\overline{\alpha}} P'_{n+1}\}$$

Now using the inductive assumption for  $P \equiv P_1 \mid \ldots \mid P_n$ , the righthand side can be reformulated as follows:

$$\sum \{\lambda.(P_{1} \mid \dots \mid P'_{i} \mid \dots \mid P_{n} \mid P_{n+1}) : 1 \leq i \leq n, P_{i} \xrightarrow{\lambda} P'_{i}\} 
+ \sum \{\tau.(P_{1} \mid \dots \mid P'_{i} \mid \dots \mid P'_{j} \mid \dots \mid P_{n} \mid P_{n+1}) : 
1 \leq i < j \leq n, P_{i} \xrightarrow{\alpha} P'_{i}, P_{j} \xrightarrow{\overline{\alpha}} P'_{j}\} 
+ \sum \{\lambda.(P_{1} \mid \dots \mid P_{n} \mid P'_{n+1}) : P_{n+1} \xrightarrow{\lambda} P'_{n+1}\} 
+ \sum \{\tau.(P_{1} \mid \dots \mid P'_{i} \mid \dots \mid P_{n} \mid P'_{n+1}) : 
1 \leq i \leq n, P_{i} \xrightarrow{\alpha} P'_{i}, P_{n+1} \xrightarrow{\overline{\alpha}} P'_{n+1}\}$$

Now we may combine the first with the third sum, and the second with the fourth, to yield as required

$$R \sim \sum \{\lambda.(P_1 \mid \dots \mid P'_i \mid \dots \mid P_{n+1}) : 1 \leq i \leq n+1, P_i \xrightarrow{\lambda} P'_i\}$$
  
+ 
$$\sum \{\tau.(P_1 \mid \dots \mid P'_i \mid \dots \mid P'_j \mid \dots \mid P_{n+1}) :$$
  
$$1 \leq i < j \leq n+1, P_i \xrightarrow{\alpha} P'_i, P_j \xrightarrow{\overline{\alpha}} P'_j\}$$

It will now be enough just to outline the steps from the simple case to the full theorem. First we can add the Relabellings, by considering  $P_i \equiv Q_i[f_i]$  in the above case, and observing that  $P_i$  has a transition  $P_i \xrightarrow{\lambda} P_i'$  iff  $Q_i$  has a transition  $Q_i \xrightarrow{\gamma} Q_i'$  such that  $\lambda = f(\gamma)$  and  $P_i' = Q_i'[f_i]$ . Then we can add the restriction, using the strong equivalence

$$Q\backslash L\sim \sum\{\gamma.(Q'\backslash L):Q\stackrel{\gamma}{\longrightarrow}Q',\gamma\not\in L\cup\overline{L}\}$$
 where  $Q\equiv Q_1[f_1]\mid\ldots\mid Q_n[f_n].$ 

# Congruence Property

We wish to establish that if *E* is any agent expression containing the variable *X*, and  $P \sim Q$ , then  $E\{P/X\} \sim E\{Q/X\}$ .

Proposition Suppose  $P_1 \sim P_2$ . Then

- (1)  $\lambda . P_1 \sim \lambda . P_2$
- (2)  $P_1 + Q \sim P_2 + Q$
- (3)  $P_1 | Q \sim P_2 | Q$
- (4)  $P_1 \backslash L \sim P_2 \backslash L$
- (5)  $P_1[f] \sim P_2[f]$

## Bisimilarity on Process Expressions

Consider expressions with variables. The definition of  $\sim$  could be extended as follows

Definition Let E and F contain variable X at most. Then  $E \sim F$  if, for all processes P, it holds that  $E\{P/X\} \sim F\{P/X\}$ .

# **Equivalence about Recursion**

### Proposition

If  $A \stackrel{\text{def}}{=} P$  then  $A \sim P$ .

# **Unique Solution**

### Proposition (in details)

Let E and F contain variables X at most.

### Suppose

```
A^{\text{def}} E\{A/X\}
```

$$B \stackrel{\text{def}}{=} F\{B/X\}$$

$$E \sim F$$

Then  $A \sim B$ 

Assume that

$$E \sim F$$
 $A \stackrel{\text{def}}{=} E\{A/X\}$ 
 $B \stackrel{\text{def}}{=} F\{B/X\}$ 

It will be enough to show that  $\mathcal S$  is a strong bisimulation up to  $\sim$ , where

$$S = \{(G\{A/X\}, G\{B/X\}) : G \text{ contains at most the variable } X\}$$

For then, by taking  $G \equiv X$ , it follows that  $A \sim B$ .

To show this, it will be enough to prove that

If 
$$G\{A/X\} \xrightarrow{\lambda} P'$$
 then, for some  $Q'$  and  $Q''$ ,  $(*)$   $G\{B/X\} \xrightarrow{\lambda} Q'' \sim Q'$ , with  $(P', Q') \in \mathcal{S}$ 

We shall prove (\*) by transition induction, on the depth of the inference by which the action  $G\{A/X\} \xrightarrow{\lambda} P'$  is inferred.

We argue by cases on the form of G:

1.  $G \equiv X$ .

Then  $G\{A/X\} \equiv A$ , so  $A \xrightarrow{\lambda} P'$ , hence also  $E\{A/X\} \xrightarrow{\lambda} P'$  by a shorter inference. Hence, by induction

$$E\{B/X\} \xrightarrow{\lambda} Q'' \sim Q', \text{ with } (P',Q') \in \mathcal{S}$$

But  $E \sim F$ , so  $F\{B/X\} \xrightarrow{\lambda} Q''' \sim Q'$ , and since  $B \stackrel{\mathsf{def}}{=} F\{B/X\}$ 

$$G\{B/X\} \equiv B \xrightarrow{\lambda} Q''' \sim Q' \text{ with } (P',Q') \in S$$

as required.

2.  $G \equiv \lambda . G'$ .

Then  $G\{A/X\} \equiv \lambda.G'\{A/X\}$ , so  $P' \equiv G'\{A/X\}$ ; also

$$G\{B/X\} \equiv \lambda.G'\{B/X\} \xrightarrow{\lambda} G'\{B/X\}$$

and clearly  $(G'\{A/X\}, G'\{B/X\}) \in \mathcal{S}$  as required.

3.  $G \equiv G_1 + G_2$ .

This is simpler than the following case, and we omit the proof.

4.  $G \equiv G_1 | G_2$ .

Then  $G\{A/X\} \equiv G_1\{A/X\} \mid G_2\{A/X\}$ . There are three cases for the action  $G\{A/X\} \xrightarrow{\lambda} P'$ , according to whether it arises from one or other component alone or from a communication. We shall treat only the case in which  $\lambda = \tau$ , and

$$G_1\{A/X\} \xrightarrow{\alpha} P_1', \ G_2\{A/X\} \xrightarrow{\overline{\alpha}} P_2'$$

where  $P' \equiv P'_1 \mid P'_2$ . Now each component action has a short inference, so by induction

$$G_1\{B/X\} \stackrel{\alpha}{\longrightarrow} Q_1'' \sim Q_1', \text{ with } (P_1', Q_1') \in \mathcal{S}$$
  
 $G_2\{B/X\} \stackrel{\overline{\alpha}}{\longrightarrow} Q_2'' \sim Q_2', \text{ with } (P_2', Q_2') \in \mathcal{S}$ 

Hence, setting  $Q' \equiv Q_1' \mid Q_2'$  and  $Q'' \equiv Q_1'' \mid Q_2''$ ,

$$G\{B/X\} \equiv G_1\{B/X\} \mid G_2\{B/X\} \xrightarrow{\tau} Q'' \sim Q'$$

It remains to show that  $(P',Q') \in \mathcal{S}$ . But  $(P'_i,Q'_i) \in \mathcal{S}(i=1,2)$  so for some  $H_i$ ,  $P'_i \equiv H_i\{A/X\}$  and  $Q'_i \equiv H_i\{B/X\}(i=1,2)$ ; thus if we set  $H \equiv H_1 \mid H_2$  we have

$$(P',Q') \equiv (H\{A/X\},H\{B/X\}) \in \mathcal{S}$$

- 5.  $G \equiv G_1 \setminus L$ , or  $G_1[R]$ . These cases are simpler than Case 4, and we omit the proof.
- 6.  $G \equiv C$ , an agent Constant with associated definition  $C \stackrel{\text{def}}{=} R$ . Then, since X does not occur,  $G\{A/X\}$  and  $G\{B/X\}$  are identical with C and hence both have  $\lambda$ -derivative P'; clearly

$$(P',P') \equiv (P'\{A/X\},P'\{B/X\}) \in \mathcal{S}$$

# Weakly Guardedness

Question: Under what condition on the expression E is there a unique P up to ~ such that

$$P \sim E\{P/X\}$$

The unique solution is the process  $A = E\{A/X\}$ 

- Definition
  - X is weakly guarded in E if each occurrence of X is within some sub-expression  $\alpha . F$  of E.

### A Lemma

### Lemma

■ Suppose that the variable X is weakly guarded in E and  $E\{P/X\} \xrightarrow{\lambda} P'$  then P' takes the form  $E'\{P/X\}$  for some expression E', and moreover, for any Q it holds that  $E\{Q/X\} \xrightarrow{\lambda} E'\{Q/X\}$ 

 $Case1: E \equiv Y$ 

 $Case2: E \equiv \alpha.E'$ 

 $Case3: E \equiv E_1 + E_2$ 

 $Case4: E \equiv E_1 \mid E_2$ 

 $Case5: E \equiv F[R]orF \setminus L$ 

 $Case6: E \equiv C$ 

# Unique Solution of Equation

- Proposition (simply introduce)
  - Suppose the expression F contains at most the variables X and
    - X be weakly guarded in F
    - $P \sim F\{P/X\}$
    - $Q \sim F\{Q/X\}$

Then  $P \sim Q$ .

*Proof.* (2) We want to prove  $P_i \sim Q_i$   $(i \in I)$ , and this will follow (by taking  $E \equiv X_i$ ) if we can show that **E is different from E**<sub>1</sub>, ... **E**<sub>n</sub>

$$\mathcal{S} = \{ (E\{\widetilde{P}/\widetilde{X}\}, E\{\widetilde{Q}/\widetilde{X}\}) : Vars(E) \subseteq \widetilde{X} \} \cup Id_{\mathcal{P}}$$

is a strong bisimulation up to  $\sim$ . By symmetry it will be enough to prove that

If 
$$E\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\lambda} P'$$
, then  $E\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\lambda} Q'$  with  $P' \sim S \sim Q'$  (\*)

We argue by transition induction on the depth of the inference of  $E\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\lambda} P'$ . Consider the cases for E:

1.  $E \equiv X_i$ .

Then we have  $E\{\widetilde{P}/\widetilde{X}\} \equiv P_i \xrightarrow{\lambda} P'$ , so since  $P_i \sim E_i\{\widetilde{P}/\widetilde{X}\}$  we have  $E_i\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\lambda} P'' \sim P'$ . But the  $\widetilde{X}$  are weakly guarded in  $E_i$ , so by the lemma  $P'' \equiv E'\{\widetilde{P}/\widetilde{X}\}$  and  $E_i\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\lambda} E'\{\widetilde{Q}/\widetilde{X}\}$ . Hence  $P' \sim \mathcal{S} \sim Q'$ .

2.  $E \equiv \lambda . F$ .

This case is very easy.

3.  $E \equiv E_1 + E_2$ .

Then from the assumption of (\*) we have  $E_i\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\lambda} P'$  (for i=1,2) by a shorter inference. Hence we can use (ast) to deduce  $E_i\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\lambda} Q'$  with  $P' \sim \mathcal{S} \sim Q'$ , and the result follows easily.

4.  $E \equiv E_1 \mid E_2$ , or  $F \setminus L$ , or F[R], or C (an agent Constant). In all these cases the argument is quite routine, following the style of these cases in the lemma.

This concludes the proof that S is a strong bisimulation up to  $\sim$ , and the proof of the proposition.

#### Definition

We define the function  $\mathcal{F}$ , over subsets of  $\mathcal{P} \times \mathcal{P}$  (i.e. binary relations over agents), as follows:

If  $\mathcal{R} \subset \mathcal{P} \times \mathcal{P}$ , then  $(P,Q) \in \mathcal{F}(\mathcal{R})$  iff for all  $\lambda \in \mathcal{A}$ :

- (i) Whenever  $P \xrightarrow{\lambda} P'$  then for some Q',  $Q \xrightarrow{\lambda} Q'$  and  $P'\mathcal{R}Q'$
- (ii) Whenever  $Q \xrightarrow{\lambda} Q'$  then for some P',  $P \xrightarrow{\lambda} P'$  and  $P'\mathcal{R}Q'$

#### Proposition

- (1)  $\mathcal{F}$  is monotonic; that is, if  $\mathcal{R}_1 \subseteq \mathcal{R}_2$  then  $\mathcal{F}(\mathcal{R}_1) \subseteq \mathcal{F}(\mathcal{R}_2)$
- (2)  $\mathcal{S}$  is a strong bisimulation iff  $\mathcal{S} \subseteq \mathcal{F}(\mathcal{S})$

### Proof

- (1) follows directly from Definition of  $\mathcal{F}$ .
- (2) is simply a reformulation of Definition of Strong Bisimulation. Note that 'implies' is reformulated as ' $\subseteq$ '.

We call  $\mathcal{R}$  is a fixed-point of  $\mathcal{F}$  if  $\mathcal{R} = \mathcal{F}(\mathcal{R})$ . Similarly, we say that  $\mathcal{R}$  is a pre-fixed-point of  $\mathcal{F}$  if  $\mathcal{R} \subseteq \mathcal{F}(\mathcal{R})$ .

So strong bisimulations are exactly the pre-fixed-points of  $\mathcal{F}$ .

#### Proposition

Strong equivalence is a fixed-point of  $\mathcal{F}$ ; that is,  $\sim = \mathcal{F}(\sim)$ . Moreover, it is the largest fixed-point of  $\mathcal{F}$ .

*Proof.* Since  $\sim$  is a strong bisimulation,  $\sim \subseteq \mathcal{F}(\sim)$ . Hence, because  $\mathcal{F}$  is monotonic,  $\mathcal{F}(\sim) \subseteq \mathcal{F}(\mathcal{F}(\sim))$ , i.e.  $\mathcal{F}(\sim)$  is also a pre-fixed-point of  $\mathcal{F}$ . But  $\sim$  is the largest pre-fixed-point of  $\mathcal{F}$ , hence it includes  $\mathcal{F}(\sim)$ , i.e.  $\mathcal{F}(\sim) \subseteq \sim$ . Hence  $\sim = \mathcal{F}(\sim)$ . Moreover  $\sim$  must be the largest fixed-point of  $\mathcal{F}$  since it is the largest pre-fixed-point.