An Example

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

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

$$P_2 \sim P_1'$$

$$Q_2 \sim Q_1'$$

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

An Example

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

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

$$P_2 \sim P_1'$$

$$Q_2 \sim Q_1'$$

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

Q: Such R must be a strong bisimulation?

A: NO. In fact, ~R~ is a strong bisimulation.

Up-to Bisimulation

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

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

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

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

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

Up-to Bisimulation

形象地

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

$$\begin{tikzcd}[column sep=small]
 & & P \arrow[dll, "\lambda"'] & \mathcal{S} & Q \arrow[drr, "\lambda"] & & \\
P' & \sim & P'' & \mathcal{S} & Q'' & \sim & Q'
\end{tikzcd}$$

Up-to Bisimulation

Lemma If $\mathcal{S}$ is a strong bisimulation up to $\sim$, then $\sim \mathcal{S} \sim$ is a strong bisimulation.

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

$$
\begin{array}{ccccc}
P & \sim & \mathcal{S} & \sim & Q \\
{\scriptstyle\lambda}\big\downarrow & & & & \big\downarrow{\scriptstyle\lambda} \\
P' & \sim & \mathcal{S} & \sim & Q'
\end{array}
$$

Proof

$$
\begin{tikzcd}
P \arrow[d, "\lambda"'] & \sim & P_1 \arrow[d, "\lambda"] \\
P' & \sim & P_1'
\end{tikzcd}
\qquad
\begin{tikzcd}
 & P_1 \arrow[dl, "\lambda"'] & \mathcal{S} & Q_1 \arrow[dr, "\lambda"] & \\
P_1' & \sim & \mathcal{S} & \sim & Q_1'
\end{tikzcd}
\qquad
\begin{tikzcd}
Q_1 \arrow[d, "\lambda"'] & \sim & Q \arrow[d, "\lambda"] \\
Q_1' & \sim & Q'
\end{tikzcd}
$$

Making Use of the Up-to Bisimulation

Proposition If $\mathcal{S}$ is a strong bisimulation up to ~ 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 ~ 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* $\sim$.

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

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

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

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

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

$(4)\ P + \mathbf{0} \sim P$

Static Laws

Proposition

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

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

(3) $P \mid \mathbf{0} \sim P$

(4) $P \backslash L \sim P$ if $\mathcal{L}(P) \cap (L \cup \overline{L}) = \emptyset$

(5) $P \backslash K \backslash L \sim P \backslash (K \cup L)$

(6) $P[f] \backslash L \sim P \backslash f^{-1}(L)[f]$

(7) $(P \mid Q) \backslash L \sim P \backslash L \mid Q \backslash L$ 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 $f \restriction \mathcal{L}(P) = f' \restriction \mathcal{L}(P)$

(10) $P[f][f'] \sim P[f' \circ f]$

(11) $(P \mid Q)[f] \sim P[f] \mid Q[f]$ if $f \restriction (L \cup \overline{L})$ is one-to-one, where $L = \mathcal{L}(P) \cup \mathcal{L}(Q)$

Expansion Law

Let $P \equiv (P_1[f_1] \mid \ldots \mid P_n[f_n])\backslash L$, with $n \geq 1$. Then

$$
\begin{aligned}
P \;\sim\; & \sum\{f_i(\lambda).(P_1[f_1] \mid \ldots \mid P_i'[f_i] \mid \ldots \mid P_n[f_n])\backslash L : \\
& \qquad\qquad P_i \xrightarrow{\lambda} P_i', f_i(\lambda) \notin L \cup \overline{L}\} + \\
& \sum\{\tau.(P_1[f_1] \mid \ldots \mid P_i'[f_i] \mid \ldots \mid P_j'[f_j] \mid \ldots \mid P_n[f_n])\backslash L : \\
& \qquad\qquad P_i \xrightarrow{\alpha_1} P_i', P_j \xrightarrow{\alpha_2} P_j', f_i(\alpha_1) = \overline{f_j(\alpha_2)}, i < j\}
\end{aligned}
$$

Proof

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

$$\begin{aligned} P \;\sim\; & \sum\{\lambda.(P_1 \mid \ldots \mid P_i' \mid \ldots \mid P_n) : 1 \leq i \leq n, P_i \xrightarrow{\lambda} P_i'\} \\ & + \sum\{\tau.(P_1 \mid \ldots \mid P_i' \mid \ldots \mid P_j' \mid \ldots \mid P_n) : \\ & \qquad\qquad 1 \leq i < j \leq n, P_i \xrightarrow{\alpha} P_i', P_j \xrightarrow{\overline{\alpha}} P_j'\} \end{aligned}$$

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 $R \equiv P \mid P_{n+1}$.

Proof

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

$$
\begin{aligned}
R \;\sim\; & \sum\{\lambda.(P' \,|\, P_{n+1}) : P \xrightarrow{\lambda} P'\} \\
& + \sum\{\lambda.(P \,|\, P'_{n+1}) : P_{n+1} \xrightarrow{\lambda} P'_{n+1}\} \\
& + \sum\{\tau.(P' \,|\, P'_{n+1}) : P \xrightarrow{\alpha} P', P_{n+1} \xrightarrow{\overline{\alpha}} P'_{n+1}\}
\end{aligned}
$$

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

$$
\begin{aligned}
& \sum\{\lambda.(P_1 \,|\, \ldots \,|\, P'_i \,|\, \ldots \,|\, P_n \,|\, P_{n+1}) : 1 \le i \le n, P_i \xrightarrow{\lambda} P'_i\} \\
+ \; & \sum\{\tau.(P_1 \,|\, \ldots \,|\, P'_i \,|\, \ldots \,|\, P'_j \,|\, \ldots \,|\, P_n \,|\, P_{n+1}) : \\
& \qquad\qquad 1 \le i < j \le n, P_i \xrightarrow{\alpha} P'_i, P_j \xrightarrow{\overline{\alpha}} P'_j\} \\
+ \; & \sum\{\lambda.(P_1 \,|\, \ldots \,|\, P_n \,|\, P'_{n+1}) : P_{n+1} \xrightarrow{\lambda} P'_{n+1}\} \\
+ \; & \sum\{\tau.(P_1 \,|\, \ldots \,|\, P'_i \,|\, \ldots \,|\, P_n \,|\, P'_{n+1}) : \\
& \qquad\qquad 1 \le i \le n, P_i \xrightarrow{\alpha} P'_i, P_{n+1} \xrightarrow{\overline{\alpha}} P'_{n+1}\}
\end{aligned}
$$

Proof

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

$$\begin{aligned} R \;\sim\; & \sum\{\lambda.(P_1 \,|\, \ldots \,|\, P_i' \,|\, \ldots \,|\, P_{n+1}) : 1 \leq i \leq n{+}1, P_i \xrightarrow{\lambda} P_i'\} \\ & + \sum\{\tau.(P_1 \,|\, \ldots \,|\, P_i' \,|\, \ldots \,|\, P_j' \,|\, \ldots \,|\, P_{n+1}) : \\ & \qquad\qquad 1 \leq i < j \leq n{+}1, P_i \xrightarrow{\alpha} P_i', P_j \xrightarrow{\overline{\alpha}} P_j'\} \end{aligned}$$

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

$$Q\backslash L \sim \sum\{\gamma.(Q'\backslash L) : Q \xrightarrow{\gamma} Q', \gamma \notin L \cup \overline{L}\}$$

where $Q \equiv Q_1[f_1] \,|\, \ldots \,|\, Q_n[f_n]$. $\square$

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

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

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

  $$E \sim F$$

  Then $A \sim B$

Proof

Assume that

$$
\begin{aligned}
E &\sim F \\
A &\stackrel{\text{def}}{=} E\{A/X\} \\
B &\stackrel{\text{def}}{=} F\{B/X\}
\end{aligned}
$$

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

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

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

To show this, it will be enough to prove that

$$
\begin{aligned}
&\text{If } \; G\{A/X\} \xrightarrow{\lambda} P' \text{ then, for some } Q' \text{ and } Q'', \qquad (*) \\
&\phantom{\text{If } \;} G\{B/X\} \xrightarrow{\lambda} Q'' \sim Q', \text{with} (P', Q') \in \mathcal{S}
\end{aligned}
$$

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

Proof

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

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

   as required.

Proof

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 $G\{A/X\} \equiv G_1\{A/X\} \,|\, G_2\{A/X\}$. 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

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

Proof

where $P' \equiv P_1' \mid P_2'$. Now each component action has a short inference, so by induction

$$\begin{array}{lcl} G_1\{B/X\} & \xrightarrow{\alpha} & Q_1'' \sim Q_1', \text{ with } (P_1', Q_1') \in \mathcal{S} \\ G_2\{B/X\} & \xrightarrow{\overline{\alpha}} & Q_2'' \sim Q_2', \text{ with } (P_2', Q_2') \in \mathcal{S} \end{array}$$

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

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

Proof

5. $G \equiv G_1 \backslash L$, 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 $C \overset{\text{def}}{=} R$.
   Then, since X does not occur, $G\{A/X\}$ and $G\{B/X\}$ are identical with C and hence *both* have λ-derivative P'; clearly

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

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 $E\{Q/X\} \xrightarrow{\lambda} E'\{Q/X\}$

$$Case1 : E \equiv Y$$

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

$$Case3 : E \equiv E_1 + E_2$$

$$Case4 : E \equiv E_1 \mid E_2$$

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

$$Case6 : E \equiv C$$

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

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_1, … E_n**

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

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

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

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

Proof

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. $E \equiv E_1 \,|\, E_2$, or $F \backslash L$, 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 $\mathcal{S}$ is a strong bisimulation up to $\sim$, and the proof of the proposition. $\square$

Bisimulation as Fixpoint

Definition

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

If $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$, 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 $P'\mathcal{R}Q'$

Bisimulation as Fixpoint

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 '$\subseteq$'.

Bisimulation as Fixpoint

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 $\mathcal{F}$.

Bisimulation as Fixpoint

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. $\square$