BISIMILARITY

When are two processes equivalent?

Bisimulation

A symmetric binary relation R on agents, s.t.:

$$P R Q \text{ and } P \xrightarrow{\alpha} P'$$

implies

$$\exists Q' : Q \xrightarrow{\alpha} Q' \wedge P' R Q'.$$

Two agents are bisimilar if they can indefinitely mimic the transitions of each other.

STRONG BISIMULATION

A symmetric binary relation R on agents, s.t.:

$P R Q$ and $P \xrightarrow{\alpha} P'$ where bn(α) is fresh

implies that

(i) If $\alpha = a(x)$ then

$\exists Q' : Q \xrightarrow{a(x)} Q' \land \forall u : P'\{u/x\} \, R \, Q'\{u/x\}$

(ii) If α is not an input then

$\exists Q' : Q \xrightarrow{\alpha} Q' \land P' R Q'$

P and Q are strongly bisimilar, written

$$P \dot{\sim} Q$$

if they are related by a bisimulation.

Example 1.

$$P = a \mid \bar{b}$$

$$Q = a.\bar{b} + \bar{b}.a$$

$$\begin{tikzcd}
 & \bar{b} \arrow[r, "\bar{b}"] & \emptyset \\
P \arrow[ur, "a"] \arrow[dr, "\bar{b}"'] & & \\
 & a \arrow[r, "a"] & \emptyset
\end{tikzcd}$$

$$\begin{tikzcd}
 & \bar{b} \arrow[r, "\bar{b}"] & \emptyset \\
Q \arrow[ur, "a"] \arrow[dr, "\bar{b}"'] & & \\
 & a \arrow[r, "a"] & \emptyset
\end{tikzcd}$$

So, we say $P \dot{\sim} Q$.

Example 2

$P = a(u)$

$Q = a(x).(\nu v)\bar{v}\underline{\underline{u}}$

Transition $P \xrightarrow{\overbrace{a(u)}} \emptyset$ cannot be simulated by Q because x cannot be α-converted to u in Q, since u appears free in Q.

But intuitively P and Q behave the same.

Example 3

$$P = a(x).\bar{b}x$$
$$Q = a(y).\bar{b}y$$

$$P \xrightarrow{a(x)} \bar{b}x$$

$$Q \xrightarrow{a(x)} \bar{b}x$$ (after α-conversion: $a(y).\bar{b}y \equiv a(x).\bar{b}x$ by STRUCT rule.)

$\forall u$: $\bar{b}x\{u/x\}\ R\ \bar{b}x\{u/x\}$

since $\bar{b}u \sim \bar{b}u$.

In general,

$P \equiv Q$ implies $P \dot\sim Q$.

Example 4.

$$P_1 = a(x).P + a(x).0$$

$$P_2 = a(x).P + a(x).\text{if } x=u \text{ then } P$$

If we assume $P \not\sim 0$ then

$$P_1 \not\sim P_2$$

since the transition

$$P_1 \xrightarrow{a(x)} 0$$

cannot be simulated by P_2.

$$P_2 \xrightarrow{a(x)} \text{if } x=u \text{ then } P$$

for the substitution $\{u/x\}$. $\square$

Example 5.

$$P = a \mid \bar{a}$$

$$Q_1 = a.\bar{a} + \bar{a}.a + \tau$$

$$Q_2 = a.\bar{a} + \bar{a}.a$$

$P \dot{\sim} Q_2$ but $P \not\dot{\sim} Q_2$ since the empty transition cannot be simulated by Q_2.

So, in general, $\dot{\sim}$ is not closed under substitutions. i.e, from $P \dot{\sim} Q$ we can<u>not</u> conclude $P\sigma \dot{\sim} Q\sigma$.

Example 6

$$P = c(a).(a \mid \bar{b})$$
$$Q = c(a).(a.\bar{b} + \bar{b}.a)$$

$P \not\dot\sim Q$ since for ~~input~~ substitution $\{b/a\}$,

$$(a \mid \bar{b}) \not\dot\sim (a.\bar{b} + \bar{b}.a)$$

i.e. $$(b \mid \bar{b}) \not\dot\sim (b.\bar{b} + \bar{b}.b)$$

In general, $\dot\sim$ is not preserved by input prefix.

i.e. from $P \dot\sim Q$ we <u>cannot</u> conclude

$$a(x).P \dot\sim a(x).Q .$$

PROPOSITION 1 EXAMPLE

$$P = \underbrace{(\nu x)\,Q}\;|\;y(z).R$$

$$\equiv (\nu x')\,(Q\{x'/x\}\;|\;y(z).R)$$

for $x' \notin P$.

Proof.

$$(\nu x)\,Q\;|\;y(z).R$$

$$\equiv (\nu x')\,Q\{x'/x\}\;|\;y(z).R \quad \text{by } \alpha\text{-conversion}$$

$$\equiv y(z).R\;|\;(\nu x')\,Q\{x'/x\} \quad \text{by commutativity}$$

$$\equiv (\nu x')\,(y(z).R\;|\;Q\{x'/x\}) \quad \text{by scope extension law 2, right to left}$$

$$\equiv (\nu x')\,(Q\{x'/x\}\;|\;y(z).R) \quad \text{by commutativity}$$

D.

PROPOSITION 2.

If $P \dot\sim Q$ and σ is injective,
then $P\sigma \dot\sim Q\sigma$.

PROPOSITION 3.

$\dot\sim$ is an equivalence.
(Reflexive, symmetric, and transitive).

PROPOSITION 4.

$\dot\sim$ is preserved by all operators except
input prefix.

CONGRUENCE

Two agents P and Q are (strongly) congruent, written $P \sim Q$, if $P\sigma \dot{\sim} Q\sigma$ for all substitutions σ.

Example 7

$P = a \mid \bar{b}$

$Q = a.\bar{b} + \bar{b}.a + \text{if } a=b \text{ then } \tau.$

$P \sim Q$ since every substitution σ (including $\{b/a\}$ and $\{a/b\}$) preserves $P\sigma \dot{\sim} Q\sigma$.

EQUATIONAL THEORY -- AXIOMS FOR STRONG BISIMILARITY

STR If $P \equiv Q$ then $P = Q$

CONGR1 if $P = Q$ then $\bar{a}u.P = \bar{a}u.Q$

$\tau.P = \tau.Q$

$P + R = Q + R$

$(\nu x)P = (\nu x)Q$

CONGR2 if $P\{y/x\} = Q\{y/x\}$ for all $y \in fn(P, Q, x)$ then $a(x).P = a(x).Q$.

S $P + P = P$

M1 if $x = x$ then $P = P$

M2 if $x = y$ then $P = \emptyset$ if $x \neq y$

MM1 if $x \neq x$ then $P = \emptyset$

MM2 if $x \neq y$ then $P = P$ if $x \neq y$

R1 $(\nu x)\alpha.P = \alpha.(\nu x)P$ if $x \notin \alpha$

R2 $(\nu x)\alpha.P = \emptyset$ if x is the subject of α.

R3 $(\nu x)(P + Q) = (\nu x)P + (\nu x)Q$