Introduction to process algebra (2)

Luís S. Barbosa

HASLab - INESC TEC
Universidade do Minho
Braga, Portugal

8 April, 2015

Observable transitions

$$\stackrel{a}{\Longrightarrow} \subseteq \mathbb{P} \times \mathbb{P}$$

- $L \cup \{\epsilon\}$
- A $\stackrel{\epsilon}{\Longrightarrow}$-transition corresponds to zero or more non observable transitions
- inference rules for $\stackrel{a}{\Longrightarrow}$:

$$\frac{}{E \stackrel{\epsilon}{\Longrightarrow} E}\,(O_1)$$

$$\frac{E \stackrel{\tau}{\longrightarrow} E' \quad E' \stackrel{\epsilon}{\Longrightarrow} F}{E \stackrel{\epsilon}{\Longrightarrow} F}\,(O_2)$$

$$\frac{E \stackrel{\epsilon}{\Longrightarrow} E' \quad E' \stackrel{a}{\longrightarrow} F' \quad F' \stackrel{\epsilon}{\Longrightarrow} F}{E \stackrel{a}{\Longrightarrow} F}\,(O_3) \quad \text{for } a \in L$$

Example

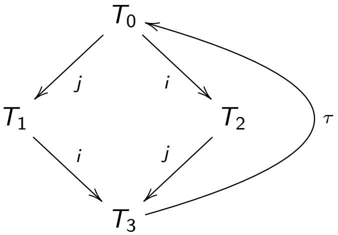
$$
\begin{aligned}
T_0 &\triangleq j.T_1 + i.T_2 \\
T_1 &\triangleq i.T_3 \\
T_2 &\triangleq j.T_3 \\
T_3 &\triangleq \tau.T_0
\end{aligned}
$$

and

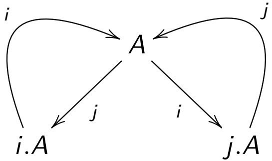
$$A \triangleq i.j.A + j.i.A$$

Example

From their graphs,



and



we conclude that $T_0 \not\approx A$ (why?).

Observational equivalence

$E \approx F$

- Processes E, F are observationally equivalent if there exists a weak bisimulation S st $\{\langle E, F\rangle\} \in S$.
- A binary relation S in $\mathbb{P}$ is a weak bisimulation iff, whenever $(E, F) \in S$ and $a \in L \cup \{\epsilon\}$,

$$\begin{array}{rl} \text{i)} & E \stackrel{a}{\Longrightarrow} E' \;\Rightarrow\; F \stackrel{a}{\Longrightarrow} F' \;\wedge\; (E', F') \in S \\ \text{ii)} & F \stackrel{a}{\Longrightarrow} F' \;\Rightarrow\; E \stackrel{a}{\Longrightarrow} E' \;\wedge\; (E', F') \in S \end{array}$$

I.e.,

$$\approx \;=\; \bigcup\{S \subseteq \mathbb{P} \times \mathbb{P} \mid S \text{ is a weak bisimulation}\}$$

Observational equivalence

Properties

- as expected: $\approx$ is an equivalence relation
- basic property: for any $E \in \mathbb{P}$,

$$E \;\approx\; \tau.E$$

(proof idea: $\mathrm{id}_{\mathbb{P}} \cup \{(E, \tau.E) \mid E \in \mathbb{P}\}$ is a weak bisimulation

- weak vs. strict:

$$\sim \subseteq \approx$$

Is $\approx$ a congruence?

Lemma

Let $E \approx F$. Then, for any $P \in \mathbb{P}$ and $K \subseteq L$,

$$a.E \approx a.F$$
$$E \mid P \approx F \mid P$$
$$\text{new } K\ E \approx \text{new } K\ F$$

but

$$E + P \approx F + P$$

does not hold, in general.

Is $\approx$ a congruence?

Lemma

Let $E \approx F$. Then, for any $P \in \mathbb{P}$ and $K \subseteq L$,

$$a.E \approx a.F$$
$$E \mid P \approx F \mid P$$
$$\text{new}\, K\; E \approx \text{new}\, K\; F$$

but

$$E + P \approx F + P$$

does not hold, in general.

Is $\approx$ a congruence?

Example (initial τ restricts options 'menu')

$$i.\mathbf{0} \approx \tau.i.\mathbf{0}$$

However

$$j.\mathbf{0} + i.\mathbf{0} \not\approx j.\mathbf{0} + \tau.i.\mathbf{0}$$

Actually,

Is $\approx$ a congruence?

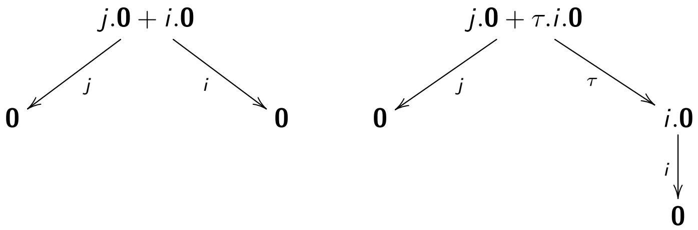
Example (initial τ restricts options 'menu')

$$i.\mathbf{0} \;\approx\; \tau.i.\mathbf{0}$$

However

$$j.\mathbf{0} + i.\mathbf{0} \not\approx j.\mathbf{0} + \tau.i.\mathbf{0}$$

Actually,



Forcing a congruence: $E = F$

Solution: force any initial τ to be matched by another τ

Process equality

Two processes E and F are equal (or observationally congruent) iff

i) $E \approx F$

ii) $E \xrightarrow{\tau} E' \;\Rightarrow\; F \xrightarrow{\tau} X \overset{\epsilon}{\Longrightarrow} F'$ and $E' \approx F'$

iii) $F \xrightarrow{\tau} F' \;\Rightarrow\; E \xrightarrow{\tau} X \overset{\epsilon}{\Longrightarrow} E'$ and $E' \approx F'$

- note that $E \neq \tau.E$, but $\tau.E = \tau.\tau.E$

Forcing a congruence: $E = F$

Solution: force any initial τ to be matched by another τ

Process equality

Two processes E and F are equal (or observationally congruent) iff

i) $E \approx F$

ii) $E \xrightarrow{\tau} E' \;\Rightarrow\; F \xrightarrow{\tau} X \stackrel{\epsilon}{\Longrightarrow} F'$ and $E' \approx F'$

iii) $F \xrightarrow{\tau} F' \;\Rightarrow\; E \xrightarrow{\tau} X \stackrel{\epsilon}{\Longrightarrow} E'$ and $E' \approx F'$

- note that $E \neq \tau.E$, but $\tau.E = \tau.\tau.E$

Forcing a congruence: $E = F$

$=$ can be regarded as a restriction of $\approx$ to all pairs of processes which preserve it in additive contexts

Lemma

Let E and F be processes st the union of their sorts is distinct of L. Then,

$$E = F \;\equiv\; \forall_{G \in \mathbb{P}} \,.\, (E + G \approx F + G)$$

Properties of $=$

Lemma

$$E \approx F \;\equiv\; (E = F) \vee (E = \tau.F) \vee (\tau.E = F)$$

- note that $E \neq \tau.E$, but $\tau.E = \tau.\tau.E$

Properties of $=$

Lemma

$$\sim \;\subseteq\; = \;\subseteq\; \approx$$

So,

$$\boxed{\text{the whole} \sim \text{theory remains valid}}$$

Additionally,

Lemma (additional laws)

$$a.\tau.E = a.E$$
$$E + \tau.E = \tau.E$$
$$a.(E + \tau.F) = a.(E + \tau.F) + a.F$$

Solving equations

Have equations over $(\mathbb{P}, \sim)$ or $(\mathbb{P}, =)$ (unique) solutions?

Lemma

Recursive equations $\tilde{X} = \tilde{E}(\tilde{X})$ or $\tilde{X} \sim \tilde{E}(\tilde{X})$, over $\mathbb{P}$, have unique solutions (up to $=$ or $\sim$, respectively). Formally,

i) Let $\tilde{E} = \{E_i \mid i \in I\}$ be a family of expressions with a maximum of I free variables ($\{X_i \mid i \in I\}$) such that any variable free in E_i is weakly guarded. Then

$$\tilde{P} \sim \{\tilde{P}/\tilde{X}\}\tilde{E} \;\wedge\; \tilde{Q} \sim \{\tilde{Q}/\tilde{X}\}\tilde{E} \;\Rightarrow\; \tilde{P} \sim \tilde{Q}$$

ii) Let $\tilde{E} = \{E_i \mid i \in I\}$ be a family of expressions with a maximum of I free variables ($\{X_i \mid i \in I\}$) such that any variable free in E_i is guarded and sequential. Then

$$\tilde{P} = \{\tilde{P}/\tilde{X}\}\tilde{E} \;\wedge\; \tilde{Q} = \{\tilde{Q}/\tilde{X}\}\tilde{E} \;\Rightarrow\; \tilde{P} = \tilde{Q}$$

Solving equations

Have equations over $(\mathbb{P}, \sim)$ or $(\mathbb{P}, =)$ (unique) solutions?

Lemma

Recursive equations $\tilde{X} = \tilde{E}(\tilde{X})$ or $\tilde{X} \sim \tilde{E}(\tilde{X})$, over $\mathbb{P}$, have unique solutions (up to $=$ or $\sim$, respectively). Formally,

i) Let $\tilde{E} = \{E_i \mid i \in I\}$ be a family of expressions with a maximum of I free variables ($\{X_i \mid i \in I\}$) such that any variable free in E_i is weakly guarded. Then

$$\tilde{P} \sim \{\tilde{P}/\tilde{X}\}\tilde{E} \;\wedge\; \tilde{Q} \sim \{\tilde{Q}/\tilde{X}\}\tilde{E} \;\Rightarrow\; \tilde{P} \sim \tilde{Q}$$

ii) Let $\tilde{E} = \{E_i \mid i \in I\}$ be a family of expressions with a maximum of I free variables ($\{X_i \mid i \in I\}$) such that any variable free in E_i is guarded and sequential. Then

$$\tilde{P} = \{\tilde{P}/\tilde{X}\}\tilde{E} \;\wedge\; \tilde{Q} = \{\tilde{Q}/\tilde{X}\}\tilde{E} \;\Rightarrow\; \tilde{P} = \tilde{Q}$$

Solving equations

Have equations over $(\mathbb{P}, \sim)$ or $(\mathbb{P}, =)$ (unique) solutions?

Lemma

Recursive equations $\tilde{X} = \tilde{E}(\tilde{X})$ or $\tilde{X} \sim \tilde{E}(\tilde{X})$, over $\mathbb{P}$, have unique solutions (up to $=$ or $\sim$, respectively). Formally,

i) Let $\tilde{E} = \{E_i \mid i \in I\}$ be a family of expressions with a maximum of I free variables ($\{X_i \mid i \in I\}$) such that any variable free in E_i is weakly guarded. Then

$$\tilde{P} \sim \{\tilde{P}/\tilde{X}\}\tilde{E} \ \wedge\ \tilde{Q} \sim \{\tilde{Q}/\tilde{X}\}\tilde{E} \ \Rightarrow\ \tilde{P} \sim \tilde{Q}$$

ii) Let $\tilde{E} = \{E_i \mid i \in I\}$ be a family of expressions with a maximum of I free variables ($\{X_i \mid i \in I\}$) such that any variable free in E_i is guarded and sequential. Then

$$\tilde{P} = \{\tilde{P}/\tilde{X}\}\tilde{E} \ \wedge\ \tilde{Q} = \{\tilde{Q}/\tilde{X}\}\tilde{E} \ \Rightarrow\ \tilde{P} = \tilde{Q}$$

Conditions on variables

guarded :
X occurs in a sub-expression of type $a.E'$ for $a \in Act - \{\tau\}$

weakly guarded :
X occurs in a sub-expression of type $a.E'$ for $a \in Act$

in both cases assures that, until a guard is reached, behaviour does not depends on the process that instantiates the variable

example: X is weakly guarded in both $\tau.X$ and $\tau.\mathbf{0} + a.X + b.a.X$ but guarded only in the second

Conditions on variables

guarded :
X occurs in a sub-expression of type $a.E'$ for $a \in Act - \{\tau\}$

weakly guarded :
X occurs in a sub-expression of type $a.E'$ for $a \in Act$

in both cases assures that, until a guard is reached, behaviour does not depends on the process that instantiates the variable

example: X is weakly guarded in both $\tau.X$ and $\tau.\mathbf{0} + a.X + b.a.X$ but guarded only in the second

Conditions on variables

sequential :

X is sequential in E if every strict sub-expression in which X occurs is either $a.E'$, for $a \in Act$, or $\Sigma\tilde{E}$.

avoids X to become guarded by a τ as a result of an interaction

example: X is not sequential in $X = \text{new}\,\{a\}\,(\bar{a}.X \mid a.\mathbf{0})$

Conditions on variables

sequential :

X is sequential in E if every strict sub-expression in which X occurs is either $a.E'$, for $a \in Act$, or $\Sigma\tilde{E}$.

avoids X to become guarded by a τ as a result of an interaction

example: X is not sequential in $X = \mathsf{new}\,\{a\}\ (\overline{a}.X \mid a.\mathbf{0})$

Example (1)

Consider

$$
\begin{aligned}
Sem &\triangleq get.put.Sem \\
P_1 &\triangleq \overline{get}.c_1.\overline{put}.P_1 \\
P_2 &\triangleq \overline{get}.c_2.\overline{put}.P_2 \\
S &\triangleq \text{new}\,\{get, put\}\;(Sem \mid P_1 \mid P_2)
\end{aligned}
$$

and

$$S' \triangleq \tau.c_1.S' + \tau.c_2.S'$$

to prove $S \sim S'$, show both are solutions of

$$X = \tau.c_1.X + \tau.c_2.X$$

Example (1)

Consider

$$\begin{aligned} Sem &\triangleq get.put.Sem \\ P_1 &\triangleq \overline{get}.c_1.\overline{put}.P_1 \\ P_2 &\triangleq \overline{get}.c_2.\overline{put}.P_2 \\ S &\triangleq \text{new}\,\{get, put\}\ (Sem \mid P_1 \mid P_2) \end{aligned}$$

and

$$S' \triangleq \tau.c_1.S' + \tau.c_2.S'$$

to prove $S \sim S'$, show both are solutions of

$$X \ = \ \tau.c_1.X + \tau.c_2.X$$

Example (1)

proof

$$
\begin{aligned}
S = \ & \tau.\text{new } K \ (c_1.\overline{put}.P_1 \mid P_2 \mid put.Sem) + \tau.\text{new } K \ (P_1 \mid c_2.\overline{put}.P_2 \mid put.Sem) \\
= \ & \tau.c_1.\text{new } K \ (\overline{put}.P_1 \mid P_2 \mid put.Sem) + \tau.c_2.\text{new } K \ (P_1 \mid \overline{put}.P_2 \mid put.Sem) \\
= \ & \tau.c_1.\tau.\text{new } K \ (P_1 \mid P_2 \mid Sem) + \tau.c_2.\tau.\text{new } K \ (P_1 \mid P_2 \mid Sem) \\
= \ & \tau.c_1.\tau.S + \tau.c_2.\tau.S \\
= \ & \tau.c_1.S + \tau.c_2.S \\
= \ & \{S/X\}E
\end{aligned}
$$

for S' is immediate

Example (2)

Consider,

$$B \triangleq in.B_1 \qquad\qquad B' \triangleq \text{new } m\ (C_1 \mid C_2)$$
$$B_1 \triangleq in.B_2 + \overline{out}.B \qquad\qquad C_1 \triangleq in.\overline{m}.C_1$$
$$B_2 \triangleq \overline{out}.B_1 \qquad\qquad C_2 \triangleq m.\overline{out}.C_2$$

B' is a solution of

$$X = E(X, Y, Z) = in.Y$$
$$Y = E_1(X, Y, Z) = in.Z + \overline{out}.X$$
$$Z = E_3(X, Y, Z) = \overline{out}.Y$$

through $\sigma = \{B/X, B_1/Y, B_2/Z\}$

Example (2)

To prove B =B'

$$\begin{aligned} B' &= \text{new } m\,(C_1 \mid C_2) \\ &= in.\text{new } m\,(\overline{m}.C_1 \mid C_2) \\ &= in.\tau.\text{new } m\,(C_1 \mid \overline{out}.C_2) \\ &= in.\text{new } m\,(C_1 \mid \overline{out}.C_2) \end{aligned}$$

Let $S_1 = \text{new } m\,(C_1 \mid \overline{out}.C_2)$ to proceed:

$$\begin{aligned} S_1 &= \text{new } m\,(C_1 \mid \overline{out}.C_2) \\ &= in.\text{new } m\,(\overline{m}.C_1 \mid \overline{out}.C_2) + \overline{out}.\text{new } m\,(C_1 \mid C_2) \\ &= in.\text{new } m\,(\overline{m}.C_1 \mid \overline{out}.C_2) + \overline{out}.B' \end{aligned}$$

Example (2)

Finally, let, $S_2 = \text{new}\, m\, (\overline{m}.C_1 \mid \overline{out}.C_2)$. Then,

$$\begin{aligned} S_2 &= \text{new}\, m\, (\overline{m}.C_1 \mid \overline{out}.C_2) \\ &= \overline{out}.\text{new}\, m\, (\overline{m}.C_1 \mid C_2) \\ &= \overline{out}.\tau.\text{new}\, m\, (C_1 \mid \overline{out}.C_2) \\ &= \overline{out}.\tau.S_1 \\ &= \overline{out}.S_1 \end{aligned}$$

Example (2)

Note the same problem can be solved with a system of 2 equations:

$$\begin{aligned} X &= E(X,Y) = in.Y \\ Y &= E'(X,Y) = in.\overline{out}.Y + \overline{out}.in.Y \end{aligned}$$

Clearly, by substitution,

$$\begin{aligned} B &= in.B_1 \\ B_1 &= in.\overline{out}.B_1 + \overline{out}.in.B_1 \end{aligned}$$

Example (2)

On the other hand, it's already proved that $B' = ... = in.S_1$.
so,

$$\begin{aligned}
S_1 &= \text{new}\, m\ (C_1 \mid \overline{out}.C_2) \\
&= in.\text{new}\, m\ (\overline{m}.C_1 \mid \overline{out}.C_2) + \overline{out}.B' \\
&= in.\overline{out}.\text{new}\, m\ (\overline{m}.C_1 \mid C_2) + \overline{out}.B' \\
&= in.\overline{out}.\tau.\text{new}\, m\ (C_1 \mid \overline{out}.C_2) + \overline{out}.B' \\
&= in.\overline{out}.\tau.S_1 + \overline{out}.B' \\
&= in.\overline{out}.S_1 + \overline{out}.B' \\
&= in.\overline{out}.S_1 + \overline{out}.in.S_1
\end{aligned}$$

Hence, $B' = \{B'/X, S_1/Y\}E$ and $S_1 = \{B'/X, S_1/Y\}E'$