

Observational Equivalence

Luís Soares Barbosa



Universidade do Minho



UNITED NATIONS
UNIVERSITY

UNU-EGOV

Interaction & Concurrency Course Unit (Lcc)

Universidade do Minho

Observable transitions

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

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

$$\frac{}{E \Longrightarrow^\epsilon E} (O_1)$$

$$\frac{E \xrightarrow{\tau} E' \quad E' \Longrightarrow^\epsilon F}{E \Longrightarrow^\epsilon F} (O_2)$$

$$\frac{E \Longrightarrow^\epsilon E' \quad E' \xrightarrow{a} F' \quad F' \Longrightarrow^\epsilon F}{E \Longrightarrow^a F} (O_3) \quad \text{for } a \in L$$

Example

$$T_0 \hat{=} j.T_1 + i.T_2$$

$$T_1 \hat{=} i.T_3$$

$$T_2 \hat{=} j.T_3$$

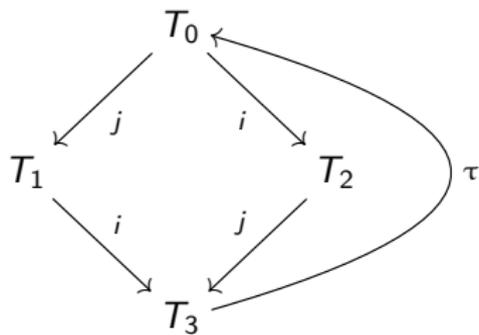
$$T_3 \hat{=} \tau.T_0$$

and

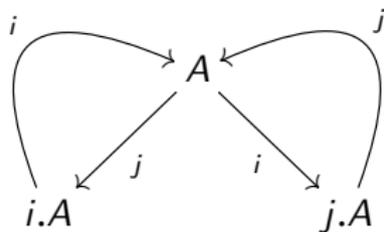
$$A \hat{=} i.j.A + j.i.A$$

Example

From their graphs,



and



we conclude that $T_0 \approx A$ (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 $a \in L \cup \{\epsilon\}$,

$$\begin{aligned} \text{i) } E &\xrightarrow{a} E' \Rightarrow F \xrightarrow{a} F' \wedge (E', F') \in S \\ \text{ii) } F &\xrightarrow{a} F' \Rightarrow E \xrightarrow{a} E' \wedge (E', F') \in S \end{aligned}$$

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: $id_{\mathbb{P}} \cup \{(E, \tau.E) \mid E \in \mathbb{P}\}$ 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 $K \subseteq L$,

$$a.E \approx a.F$$

$$E \mid P \approx F \mid P$$

$$E \setminus K \approx F \setminus K$$

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 $K \subseteq L$,

$$a.E \approx a.F$$

$$E \mid P \approx F \mid P$$

$$E \setminus K \approx F \setminus K$$

but

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

does **not** hold, in general.

Is \approx a congruence?

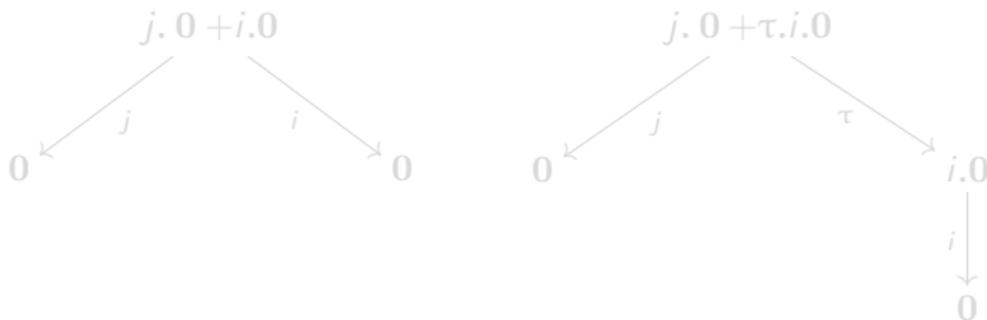
Example (initial τ restricts options 'menu')

$$i.0 \approx \tau.i.0$$

However

$$j.0 + i.0 \not\approx j.0 + \tau.i.0$$

Actually,



Is \approx a congruence?

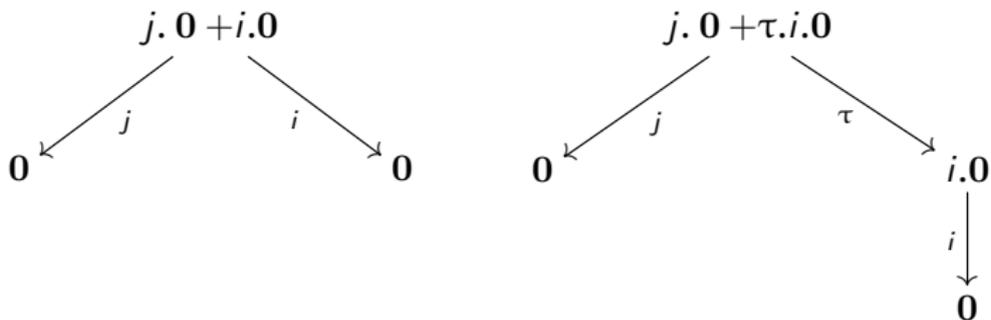
Example (initial τ restricts options 'menu')

$$i.0 \approx \tau.i.0$$

However

$$j.0 + i.0 \not\approx j.0 + \tau.i.0$$

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) $E \xrightarrow{\tau} E' \Rightarrow F \xrightarrow{\tau} X \xRightarrow{\epsilon} F'$ and $E' \approx F'$
- iii) $F \xrightarrow{\tau} F' \Rightarrow E \xrightarrow{\tau} X \xRightarrow{\epsilon} E'$ 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) $E \xrightarrow{\tau} E' \Rightarrow F \xrightarrow{\tau} X \xrightarrow{\epsilon} F'$ and $E' \approx F'$
- iii) $F \xrightarrow{\tau} F' \Rightarrow E \xrightarrow{\tau} X \xrightarrow{\epsilon} E'$ 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,

the whole \sim 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 $\tau.0 + a.X + b.a.X$ 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 $\tau.0 + a.X + b.a.X$ 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 $a \in \text{Act}$, or $\Sigma\tilde{E}$.

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

example: X is not sequential in $X = (\bar{a}.X \mid a.0) \setminus_{\{a\}}$

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 $X = (\bar{a}.X \mid a.0) \setminus \{a\}$

Example (1)

Consider

$$Sem \hat{=} get.put.Sem$$

$$P_1 \hat{=} \overline{get}.c_1.\overline{put}.P_1$$

$$P_2 \hat{=} \overline{get}.c_2.\overline{put}.P_2$$

$$S \hat{=} (Sem \mid P_1 \mid P_2) \setminus_{\{get, put\}}$$

and

$$S' \hat{=} \tau.c_1.S' + \tau.c_2.S'$$

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

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

Example (1)

Consider

$$Sem \hat{=} get.put.Sem$$

$$P_1 \hat{=} \overline{get}.c_1.\overline{put}.P_1$$

$$P_2 \hat{=} \overline{get}.c_2.\overline{put}.P_2$$

$$S \hat{=} (Sem \mid P_1 \mid P_2) \setminus_{\{get, put\}}$$

and

$$S' \hat{=} \tau.c_1.S' + \tau.c_2.S'$$

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

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

Example (1)

proof

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

for S' is immediate

Example (2)

Consider,

$$B \hat{=} in.B_1$$

$$B_1 \hat{=} in.B_2 + \overline{out}.B$$

$$B_2 \hat{=} \overline{out}.B_1$$

$$B' \hat{=} (C_1 \mid C_2) \setminus m$$

$$C_1 \hat{=} in.\overline{m}.C_1$$

$$C_2 \hat{=} m.\overline{out}.C_2$$

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 $B = B'$

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

Let $S_1 = (C_1 \mid \overline{out}.C_2) \setminus_m$ to proceed:

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

Example (2)

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

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

Example (2)

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

$$X = E(X, Y) = in.Y$$

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

Clearly, by substitution,

$$B = in.B_1$$

$$B_1 = in.\overline{out}.B_1 + \overline{out}.in.B_1$$

Example (2)

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

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

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