Behavioural abstraction

Luís S. Barbosa

HASLab - INESC TEC
Universidade do Minho
Braga, Portugal

8 March, 2015

Abstraction

Main idea:
Take a set of actions as internal or non-observable

Adding τ to the set of actions has a number of consequences:

- only external actions are observable
- the effects of an internal action can only be observed if it determines a choice

Approaches

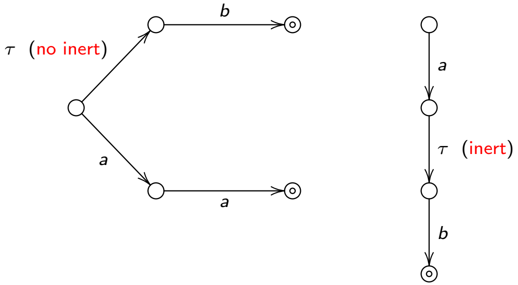
- R. Milner's weak bisimulation [Mil80]
- Van Glabbeek and Weijland's branching bisimulation [GW96]

Internal actions

τ abstracts internal activity

inert τ: internal activity is undetectable by observation

non inert τ: internal activity is indirectly visible



Branching bisimulation

- Intuition similar to that of strong bisimulation: But now, instead of letting a single action be simulated by a single action, an action can be simulated by a sequence of internal transitions, followed by that single action.
- An internal action τ can be simulated by any number of internal transitions (even by none).
- If a state can terminate, it does not need to be related to a terminating state: it suffices that a terminating state can be reached after a number of internal transitions.

Branching bisimulation

Definition

Given $\langle S_1, N, \downarrow_1, \longrightarrow_1\rangle$ and $\langle S_2, N, \downarrow_2, \longrightarrow_2\rangle$ over N, relation $R \subseteq S_1 \times S_2$ is a branching bisimulation iff for all $\langle p, q\rangle \in R$ and $a \in N$,

1. If $p \xrightarrow{a}_1 p'$, then
   - either $a = \tau$ and $p' R q$
   - or, there is a sequence $q \xrightarrow{\tau}_2 \cdots \xrightarrow{\tau}_2 q'$ of (zero or more) τ-transitions such that pRq' and $q' \xrightarrow{a}_2 q''$ with $p' R q''$.
2. If $p \downarrow_1$, then there is a sequence $q \xrightarrow{\tau}_2 \cdots \xrightarrow{\tau}_2 q'$ of (zero or more) τ-transitions such that pRq' and $q \downarrow_2$.

1'., 2'. symmetrically ...

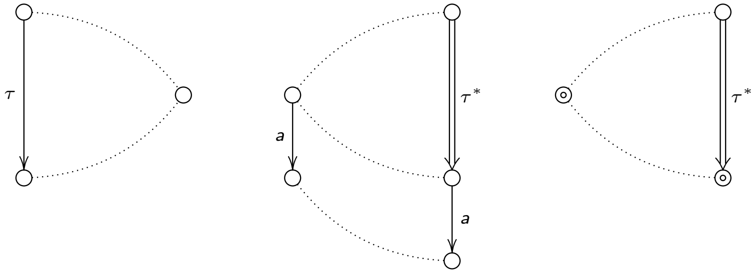
Branching bisimilarity

Definition

$$p \approx q \;\equiv\; \langle \exists\, R \;::\; R \text{ is a branching bisimulation and } \langle p, q \rangle \in R \rangle$$

Branching bisimilarity

... preserves the branching structure



Branching bisimilarity

... does not preserve τ-loops

satisfying a notion of fairness: if a τ-loop exists, then no infinite execution sequence will remain in it forever if there is a possibility to leave

Branching bisimilarity

Problem

If an alternative is added to the initial state then transition systems that were branching bisimilar may cease to be so.

Example: add a *b*-labelled branch to the initial states of

Rooted branching bisimilarity

Startegy

Impose a rootedness condition [R. Milner, 80]:

Initial τ-transitions can never be inert, *i.e.*, two states are equivalent if they can simulate each other's initial transitions, such that the resulting states are branching bisimilar.

Rooted branching bisimulation

Definition

Given $\langle S_1, N, \downarrow_1, \longrightarrow_1\rangle$ and $\langle S_2, N, \downarrow_2, \longrightarrow_2\rangle$ over N, relation $R \subseteq S_1 \times S_2$ is a rooted branching bisimulation iff

1. it is a branching bisimulation
2. for all $\langle p, q\rangle \in R$ and $a \in N$,
   - If $p \xrightarrow{a}_1 p'$, then there is a $q' \in S_2$ such that $q \xrightarrow{a}_2 q'$ and $p' \approx q'$
   - If $q \xrightarrow{a}_2 q'$, then there is a $p' \in S_1$ such that $p \xrightarrow{a}_1 p'$ and $p' \approx q'$

Rooted branching bisimilarity

Definition

$p \approx_r q \;\equiv\; \langle \exists\, R \;::\; R \text{ is a rooted branching bisimulation and } \langle p, q \rangle \in R \rangle$

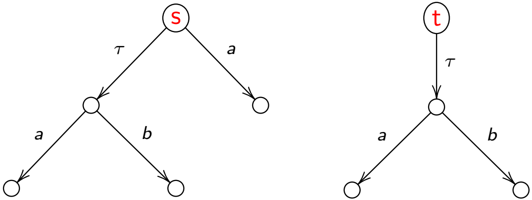
Lemma

$$\sim \;\subseteq\; \approx_r \;\subseteq\; \approx$$

Of course, in the absence of τ actions, $\sim$ and $\approx$ coincide.

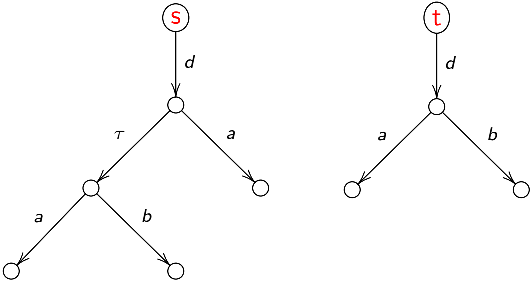
Example

branching bisimilar but not rooted



Example

rooted branching bisimilar



Weak bisimulation

Definition [Milner,80]

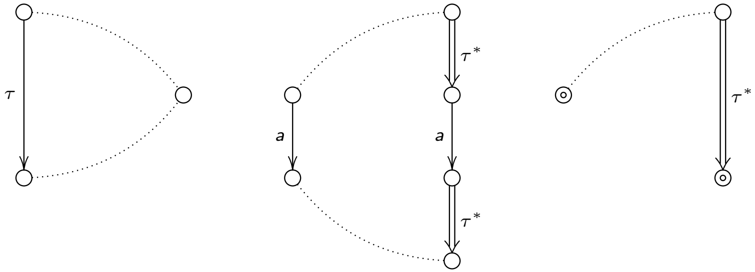
Given $\langle S_1, N, \downarrow_1, \longrightarrow_1\rangle$ and $\langle S_2, N, \downarrow_2, \longrightarrow_2\rangle$ over N, relation $R \subseteq S_1 \times S_2$ is a weak bisimulation iff for all $\langle p, q\rangle \in R$ and $a \in N$,

1. If $p \xrightarrow{a}_1 p'$, then
   - either $a = \tau$ and $p' R q$
   - or, there is a sequence $q \xrightarrow{\tau}_2 \cdots \xrightarrow{\tau}_2 t \xrightarrow{a}_2 t' \xrightarrow{\tau}_2 \cdots \xrightarrow{\tau}_2 q'$ involving zero or more τ-transitions, such that $p' R q'$.
2. If $p \downarrow_1$, then there is a sequence $q \xrightarrow{\tau}_2 \cdots \xrightarrow{\tau}_2 q'$ of (zero or more) τ-transitions such that $q' \downarrow_2$.

1'., 2'. symmetrically ...

Weak bisimulation

… does not preserve the branching structure



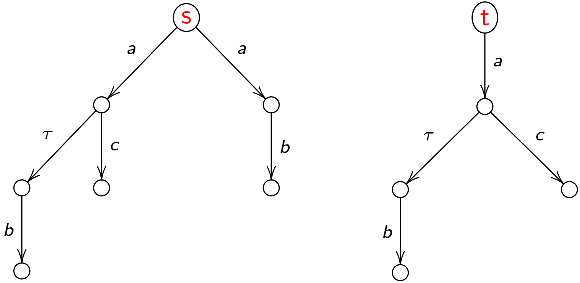
Weak bisimilarity

Definition

$$p \approx_w q \;\equiv\; \langle \exists\, R \;::\; R \text{ is a branching bisimulation and } \langle p, q \rangle \in R \rangle$$

Example

weak but not branching



Rooted weak bisimulation

Definition

Given $\langle S_1, N, \downarrow_1, \longrightarrow_1\rangle$ and $\langle S_2, N, \downarrow_2, \longrightarrow_2\rangle$ over N, relation $R \subseteq S_1 \times S_2$ is a rooted weak bisimulation iff for all $\langle p, q\rangle \in R$ and $a \in N$,

- If $p \xrightarrow{\tau}_1 p'$, then there is a non empty sequence of τ such that $q \xrightarrow{\tau}_2 \xrightarrow{\tau}_2 \ldots \xrightarrow{\tau}_2 \xrightarrow{\tau}_2 q'$ and $p' \approx_w q'$
- Symmetrically ...

Rooted weak bisimilarity

Definition

$$p \approx_{rw} q \;\equiv\; \langle \exists\, R \;::\; R \text{ is a rooted weak bisimulation and } \langle p, q \rangle \in R \rangle$$

Lemma

$$\begin{tikzcd}
& \approx_w \arrow[dl, dash] \arrow[dr, dash] & \\
\approx_b \arrow[dr, dash] & & \approx_{rw} \arrow[dl, dash] \\
& \approx_{rb} \arrow[d, dash] & \\
& \sim &
\end{tikzcd}$$

(ordered by $\subseteq$)

The questions to follow ...

- We already have a semantic model for reactive systems. With which language shall we describe them?
- How to compare and transform such systems?
- How to express and prove their proprieties?

$\rightsquigarrow$ process languages and calculi
cf. Ccs (Milner, 80), Csp (Hoare, 85),
Acp (Bergstra & Klop, 82),
π-*calculus* (Milner, 89), among many others

$\rightsquigarrow$ modal (temporal, hybrid) logics