From Strong Bisimulation to Weak Bisimulation

- applying strong bisimilarity: a simple buffer
- weak bisimilarity and weak bisimulation games
- properties of weak bisimilarity
- example: a communication protocol and its modelling in CCS
- concurrency workbench (CWB)

Example – Buffer

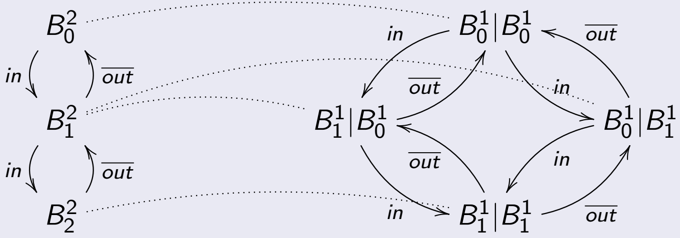
Buffer of Capacity 1

$$B_0^1 \stackrel{\text{def}}{=} in.B_1^1$$
$$B_1^1 \stackrel{\text{def}}{=} \overline{out}.B_0^1$$

Buffer of Capacity n

$$B_0^n \stackrel{\text{def}}{=} in.B_1^n$$ capacity
$$B_i^n \stackrel{\text{def}}{=} in.B_{i+1}^n + \overline{out}.B_{i-1}^n \quad \text{for } 0 < i < n$$
$$B_n^n \stackrel{\text{def}}{=} \overline{out}.B_{n-1}^n$$

Example: $B_0^2 \sim B_0^1 | B_0^1$



Example – Buffer

Theorem

For all natural numbers n: $B_0^n \sim \underbrace{B_0^1|B_0^1|\cdots|B_0^1}_{n\ times}$

Proof.

Construct the following binary relation, where $i_1, i_2, \ldots, i_n \in \{0, 1\}$:

$$R = \{\left(B_i^n,\ B_{i_1}^1|B_{i_2}^1|\cdots|B_{i_n}^1\right) \mid \sum_{j=1}^{n} i_j = i\}$$

- $\left(B_0^n,\ B_0^1|B_0^1|\cdots|B_0^1\right) \in R$
- R is a strong bisimulation

$\square$

But still Internal Actions must be Abstracted away

Question

Does $a.\tau.Nil \sim a.Nil$ hold? NO!

Problem

Strong bisimilarity does not abstract away from τ actions.

Example: SmUni $\not\sim$ Spec

$$
\begin{tikzcd}
\mathrm{SmUni} \arrow[d, "\overline{pub}"] & \not\sim & \mathrm{Spec} \arrow[loop below, "\overline{pub}"] \\
(CM \mid CS_1) \setminus \{coin, coffee\} \arrow[d, "\tau"] & & \\
(CM_1 \mid CS_2) \setminus \{coin, coffee\} \arrow[d, "\tau"] & & \\
(CM \mid CS) \setminus \{coin, coffee\} \arrow[uu, bend right=60, "\overline{pub}"'] & &
\end{tikzcd}
$$

Weak Transitions will (mostly) hide τ actions

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS such that $\tau \in Act$.

Definition of Weak Transition Relation

τ es la silent action → que significa que a un estado hace cosas consigo mismo que desde fuera no se ve.

$$\stackrel{a}{\Longrightarrow} = \begin{cases} (\xrightarrow{\tau})^* \circ \xrightarrow{a} \circ (\xrightarrow{\tau})^* & \text{if } a \neq \tau \\ (\xrightarrow{\tau})^* & \text{if } a = \tau \end{cases}$$

P τ

What does $s \stackrel{a}{\Longrightarrow} t$ informally mean?

- If $a \neq \tau$ then $s \stackrel{a}{\Longrightarrow} t$ means that
  from s we can get to t by doing zero or more τ actions, followed by the action a, followed by zero or more τ actions.
- If $a = \tau$ then $s \stackrel{\tau}{\Longrightarrow} t$ means that
  from s we can get to t by doing zero or more τ actions.

Weak Bisimilarity

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS such that $\tau \in Act$.

Weak Bisimulations

A binary relation $R \subseteq Proc \times Proc$ is a weak bisimulation iff whenever $(s, t) \in R$ then for each $a \in Act$ (including τ):

- if $s \xrightarrow{a} s'$ then $t \stackrel{a}{\Longrightarrow} t'$ for some t' such that $(s', t') \in R$
- if $t \xrightarrow{a} t'$ then $s \stackrel{a}{\Longrightarrow} s'$ for some s' such that $(s', t') \in R$.

Entonces este relaciones es como decir que ambos procesos son equivalentes salvo acciones silenciosas.

Weak Bisimilarity

Two processes $p_1, p_2 \in Proc$ are weakly bisimilar ($p_1 \approx p_2$) if and only if there exists a weak bisimulation R such that $(p_1, p_2) \in R$.

$$\approx \; = \; \cup\{R \mid R \text{ is a weak bisimulation}\}$$

Weak Bisimulation Game

Definition

Just as the Strong game except that

- defender can now reply using $\stackrel{a}{\Longrightarrow}$ moves.

The attacker is still using only $\stackrel{a}{\longrightarrow}$ moves.

Theorem

- States s and t are weakly bisimilar if and only if the defender has a universal winning strategy starting from the configuration (s, t).
- States s and t are not weakly bisimilar if and only if the attacker has a universal winning strategy starting from the configuration (s, t).

Properties of Weak Bisimilarity

Properties of $\approx$

- $\approx$ is an equivalence relation
- $\approx$ is the largest weak bisimulation
- validates lots of natural laws, e.g.
  - $a.\tau.P \approx a.P$
  - $P + \tau.P \approx \tau.P$
  - $a.(P + \tau.Q) \approx a.(P + \tau.Q) + a.Q$
  - $P + Q \approx Q + P \qquad P|Q \approx Q|P \qquad P + Nil \approx P \qquad \ldots$
- strong bisimilarity is included in weak bisimilarity ($\sim \subseteq \approx$)
- $\approx$ (totally) abstracts τ loops

Is Weak Bisimilarity a Congruence for CCS?

Theorem

Let P and Q be CCS processes such that $P \approx Q$. *Then*

- $\alpha.P \approx \alpha.Q$ *for each action* $\alpha \in Act$
- $P \mid R \approx Q \mid R$ *and* $R \mid P \approx R \mid Q$ *for each CCS process R*
- $P[f] \approx Q[f]$ *for each relabelling function f*
- $P \setminus L \approx Q \setminus L$ *for each set of labels L.*

$\tau.a.Nil + b.Nil$ $\quad$ $a.Nil + b.Nil$

$(\tau.a.Nil, a.Nil) \in R$
$(b.Nil, b.Nil) \in R$
$(\tau.a.Nil, b.Nil) \notin R$
$(b.Nil, a.Nil) \notin R$

But what about choice?

+ Choice: External / ~~M~~ Mixed / Internal

$\tau.a.Nil \approx a.Nil$ but $\tau.a.Nil + b.Nil \not\approx a.Nil + b.Nil$

Conclusion

Weak bisimilarity is not a congruence for CCS.

$\tau.a.Nil + b.Nil$ $\qquad$ $a.Nil + b.Nil$

$$\underbrace{\qquad\qquad}\underbrace{\qquad\qquad}$$

$(\tau.a.Nil,\ a.Nil) \in R$ $\longleftarrow$ $\exists \xrightarrow{K}$ tal que $\xrightarrow{K} = \begin{cases} (\xrightarrow{\tau})^{*} \xrightarrow{a} & \text{cuando } K \neq a \\ \xrightarrow{a} & \text{cuando } K = a \end{cases} \implies \in R$

$(b.Nil,\ b.Nil) \in R$ $\longleftarrow$ $\exists \xrightarrow{K}$ tal que $\xrightarrow{K} = \begin{cases} (\xrightarrow{\tau})^{*} \xrightarrow{b} & u \neq b \\ \xrightarrow{b} & u = b \end{cases} \implies \in R$

$(\tau.a.Nil,\ b.Nil) \notin R$

$(b.Nil,\ a.Nil) \notin R$ $\longleftarrow$ $\nexists \xrightarrow{u}$ porque $\xrightarrow{u}$ tendría que ser $\xrightarrow{b}$ en algún punto y $\xrightarrow{a}$, pero $\xrightarrow{a} \neq \xrightarrow{b}$ y tampoco hay algún $\xrightarrow{u'}$ tal que $\xrightarrow{a}\xrightarrow{u'}\xrightarrow{b}$ ó $\xrightarrow{b}\xrightarrow{u'}\xrightarrow{a}$

Idem

$(\tau.a.Nil + b.Nil) \not\approx (a.Nil + b.Nil)$

Suponemos $(\tau.a + b,\ a+b) \in R$

$$\begin{array}{ccc} (\tau.a+b, & a+b) \in R \\ \tau\downarrow & \Downarrow\tau \\ (a, & a+b) & \nexists \xRightarrow{b} \\ \cancel{\Downarrow b} & \downarrow b \\ (a, & b) \notin R \end{array}$$

Case Study: A simple Communication Protocol

$$\begin{aligned} \mathsf{Send} &\stackrel{\text{def}}{=} \mathsf{acc.Sending} \\ \mathsf{Sending} &\stackrel{\text{def}}{=} \overline{\mathsf{send}}.\mathsf{Wait} \\ \mathsf{Wait} &\stackrel{\text{def}}{=} \mathsf{ack.Send} + \mathsf{error.Sending} \end{aligned}$$

$$\begin{aligned} \mathsf{Rec} &\stackrel{\text{def}}{=} \mathsf{trans.Del} \\ \mathsf{Del} &\stackrel{\text{def}}{=} \overline{\mathsf{del}}.\mathsf{Ack} \\ \mathsf{Ack} &\stackrel{\text{def}}{=} \overline{\mathsf{ack}}.\mathsf{Rec} \end{aligned}$$

$$\begin{aligned} \mathsf{Med} &\stackrel{\text{def}}{=} \mathsf{send}.\mathsf{Med}' \\ \mathsf{Med}' &\stackrel{\text{def}}{=} \tau.\mathsf{Err} + \overline{\mathsf{trans}}.\mathsf{Med} \\ \mathsf{Err} &\stackrel{\text{def}}{=} \overline{\mathsf{error}}.\mathsf{Med} \end{aligned}$$

Using Weak Bisimilarity for Verification

$$\mathsf{Impl} \stackrel{\text{def}}{=} (\mathsf{Send} \mid \mathsf{Med} \mid \mathsf{Rec}) \smallsetminus \{\mathsf{send}, \mathsf{trans}, \mathsf{ack}, \mathsf{error}\}$$

$$\mathsf{Spec} \stackrel{\text{def}}{=} \mathsf{acc}.\overline{\mathsf{del}}.\mathsf{Spec}$$

Question

$$\mathsf{Impl} \stackrel{?}{\approx} \mathsf{Spec}$$

1. Draw the LTS of Impl and Spec and prove (by hand) their equivalence.
2. This could be done (automatically) using the Concurrency WorkBench (CWB).