Formale Spezifikation und Verifikation

Mirco Tribastone

Institut für Informatik
Ludwig-Maximilians-Universität München
`tribastone@pst.ifi.lmu.de`

Process Algebras

Behavioural Equivalences

Black-Box Experiments

Experiment in VM_1	Experiment in VM_2	Experiment in VM_2
coin $\overline{tea}$ $\overline{coffee}$	*coin* $\overline{tea}$ $\overline{coffee}$	*coin* $\overline{tea}$ $\overline{coffee}$
press $\overline{coin}$	press $\overline{coin}$	press $\overline{coin}$
coin $\overline{tea}$ $\overline{coffee}$	*coin* $\overline{tea}$ $\overline{coffee}$	*coin* $\overline{tea}$ $\overline{coffee}$

Main Idea

Two processes are behaviourally equivalent if and only if an external observer cannot tell them apart.

Bisimulation Relation

Strong Bisimulation

Let $(Q, A, \{\xrightarrow{a} \mid a \in A\})$ be an LTS. A relation $R \subseteq Q \times Q$ is *strong bisimulation* if, for any pair of states p and q such that $(p, q) \in R$, the following holds:

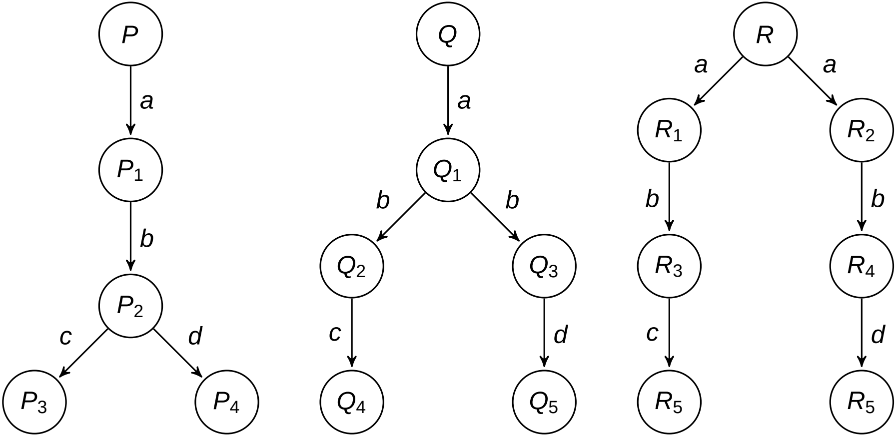
1. for all $a \in A$ and $p' \in Q$, if $p \xrightarrow{a} p'$ then $q \xrightarrow{a} q'$ for some $q' \in Q$ such that $(p', q') \in R$;
2. for all $a \in A$ and $q' \in Q$, if $q \xrightarrow{a} q'$ then $p \xrightarrow{a} p'$ for some $p' \in Q$ such that $(p', q') \in R$.

Bisimilarity

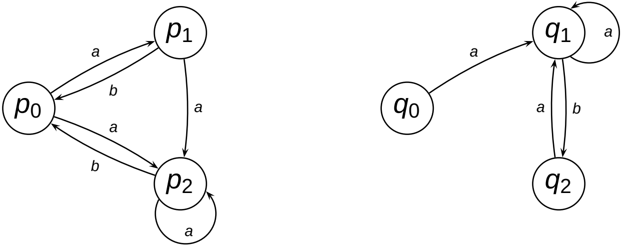
Two states $p, q \in Q$ are strongly *bisimilar*, written $p \sim q$, if there exists a strong bisimulation R such that $(p, q) \in R$.

$$\sim \; = \bigcup \{R \mid R \text{ is a strong bisimulation}\}$$

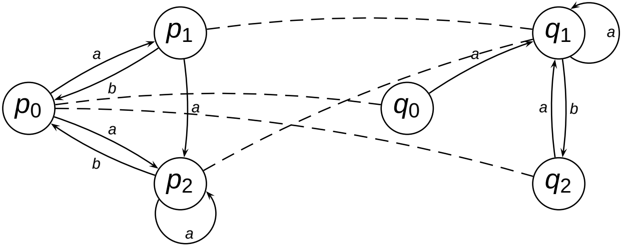
Examples



P, Q, and R are not bisimulation equivalent.



$R \triangleq \{(p_0, q_0), (p_0, q_2), (p_1, q_1), (p_2, q_1)\}$ is a strong bisimulation:



Basic Properties of Strong Bisimilarity

Theorem

$\sim$ is an equivalence relation (reflexive, symmetric and transitive).

Theorem

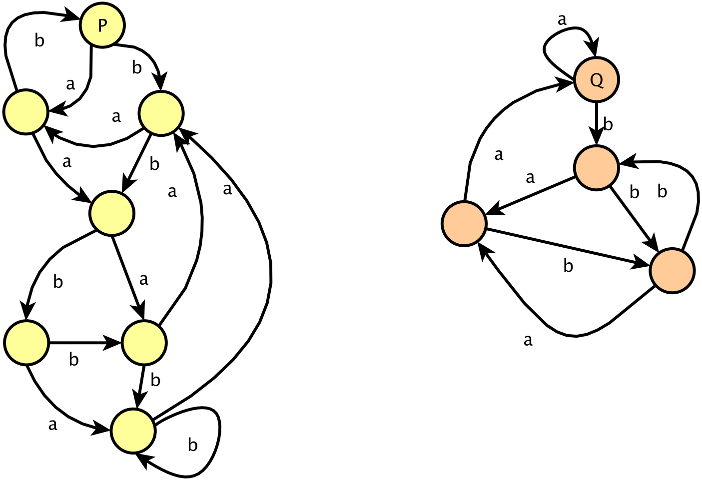
$\sim$ is the largest strong bisimulation.

Theorem

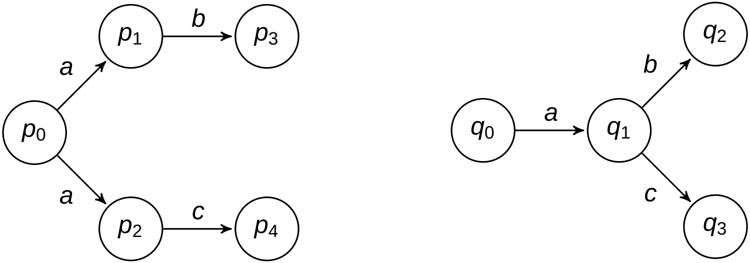
$s \sim t$ if and only if for each $a \in A$:

- *if $s \xrightarrow{a} s'$ then $t \xrightarrow{a} t'$ for some t' such that $s' \sim t'$*
- *if $t \xrightarrow{a} t'$ then $s \xrightarrow{a} s'$ for some s' such that $s' \sim t'$.*

Are P and Q Bisimilar?



How to Show Nonbisimilarity?



How to prove that $p_0 \not\sim q_0$:

- Enumerate all binary relations and show that none of them contains (s, t) and is a strong bisimulation. (Expensive: $2^{|Q|^2}$ relations.)
- Make certain observations which enable us to disqualify many bisimulation candidates in one step.
- Use the game characterization of strong bisimilarity.

Strong Bisimulation Game

Let $(Q, A, \{\xrightarrow{a} \mid a \in A\})$ be an LTS and $s, t \in Q$.

We define a two-player game of an 'attacker' and a 'defender' starting from s and t.

- The game is played in rounds, and configurations of the game are pairs of states from $Q \times Q$.
- In every round exactly one configuration is called current. Initially the configuration (s, t) is the current one.

Intuition

The defender wants to show that s and t are strongly bisimilar while the attacker aims at proving the opposite.

Rules of the Bisimulation Games

Game Rules

In each round the players change the current configuration as follows:

1. the attacker chooses one of the processes in the current configuration and makes an a-move for some $a \in A$, and
2. the defender must respond by making a move in the other process under the same action a.

The newly reached pair of processes becomes the current configuration. The game then continues by another round.

Result of the Game

- If one player cannot move, the other player wins.
- If the game is infinite, the defender wins.

Game Characterisation of Strong Bisimilarity

Theorem

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

Remark

The bisimulation game can be used to prove both bisimilarity and nonbisimilarity of two processes. It very often provides elegant arguments for the negative case.

Implementation Verification

Implementation

$$CM \triangleq coin.\overline{coffee}.CM$$

$$PR \triangleq \overline{hello}.\overline{coin}.coffee.\overline{drink}.PR$$

$$UNI \triangleq (CM \mid PR)\backslash\{coin, coffee\}$$

Specification

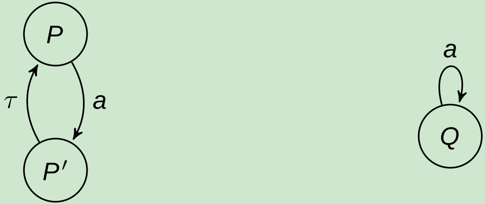
$$Spec \triangleq \overline{hello}.\tau.\tau.\overline{drink}.Spec$$

What is the relationship between *UNI* and *Spec*?

Weak Bisimilarity

- Strong bisimilarity treats all the actions equally.
- We recall that in CCS (and in other process calculi too) there is a distinguished silent (or invisible) action τ.
- Weak bisimilarity allows one to say that, in some sense, two processes are similar with respect to their visible actions.

Two Weakly Bisimilar Transition Systems



Are P and Q strongly bisimilar?

Weak Transition Relation

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

Definition of Weak Transition Relation

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

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

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

Weak Bisimilarity

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

Weak Bisimulation

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

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

Weak Bisimilarity

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

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

An Example

$$s \xrightarrow{\tau} s_1 \xrightarrow{\tau} s_2 \xrightarrow{a} s_3$$

$$t \xrightarrow{a} t_1$$

Question: Is $s \approx t$?

Solution: the relation

$$R = \{(s, t), (s_1, t), (s_2, t), (s_3, t_1)\}$$

is a weak bisimulation. Indeed,

- if $s \xrightarrow{\tau} s_1$ then $t \stackrel{\tau}{\Longrightarrow} t$ and $(s_1, t) \in R$;
- if $t \xrightarrow{a} t_1$ then $s \stackrel{a}{\Longrightarrow} s_3$ and $(s_3, t_1) \in R$;
- if $s_1 \xrightarrow{\tau} s_2$ then $t \stackrel{\tau}{\Longrightarrow} t$ and $(s_2, t) \in R$;
- if $t \xrightarrow{a} t_1$ then $s_1 \stackrel{a}{\Longrightarrow} s_3$ and $(s_3, t_1) \in R$;
- ...

Weak Bisimulation Game

Definition

All the same except that

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

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

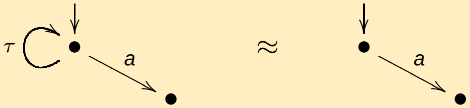
Theorem

- 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).

Weak Bisimilarity – Properties

Properties of $\approx$

- an equivalence relation
- the largest weak bisimulation
- strong bisimilarity is included in weak bisimilarity ($\sim \subseteq \approx$)
- abstracts from τ loops



Strong Bisimilarity in CCS

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS for CCS processes.

Strong Bisimulation

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

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

Strong Bisimilarity

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

$$\sim \, = \bigcup \{R \mid R \text{ is a strong bisimulation}\}$$

Example – Buffer

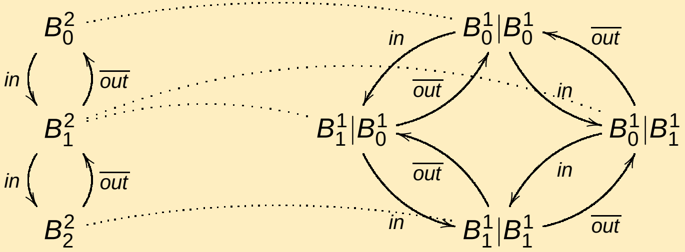
Buffer of Capacity 1

$$B_0^1 \triangleq in.B_1^1$$
$$B_1^1 \triangleq \overline{out}.B_0^1$$

Buffer of Capacity n

$$B_0^n \triangleq in.B_1^n$$
$$B_i^n \triangleq in.B_{i+1}^n + \overline{out}.B_{i-1}^n \;, \quad \text{for } 0 < i < n$$
$$B_n^n \triangleq \overline{out}.B_{n-1}^n$$

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



Example – Buffer

Theorem

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

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 strong bisimulation

□

Strong Bisimilarity is a Congruence for CCS Operations

Theorem

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

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

Other Properties of Strong Bisimilarity

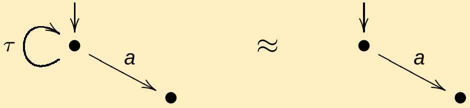
The Following Properties Hold for all CCS Processes P, Q, R

- $P + \mathbf{0} \sim P$ (Neutral element for $+$)
- $P \mid \mathbf{0} \sim P$ (Neutral element for $|$)
- $P + Q \sim Q + P$ (Commutativity of $+$)
- $P \mid Q \sim Q \mid P$ (Commutativity of $|$)
- $(P + Q) + R \sim P + (Q + R)$ (associativity of $+$)
- $(P \mid Q) \mid R \sim P \mid (Q \mid R)$ (associativity of $|$)
- $P + P \sim P$ (Idempotency of $+$)

Weak Bisimilarity – Properties

Properties of $\approx$

- an equivalence relation
- the largest weak bisimulation
- strong bisimilarity is included in weak bisimilarity ($\sim \subseteq \approx$)
- validates lots of natural laws, e.g.
  - $a.\tau.P \approx a.P$
  - $P + \tau.P \approx \tau.P$
  - $a.(P + \tau.Q) \approx a.(P + \tau.Q) + a.Q$
  - $P + Q \approx Q + P \qquad P|Q \approx Q|P \qquad P + \mathbf{0} \approx P \qquad \ldots$
- abstracts from 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* $\alpha \in Act$
- $P \mid R \approx Q \mid R$ *for each CCS process* R
- $R \mid P \approx R \mid Q$ *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.

What about choice? Counterexample

$$\tau.\mathbf{0} \approx \mathbf{0} \qquad \text{but} \qquad \tau.\mathbf{0} + a.\mathbf{0} \not\approx \mathbf{0} + a.\mathbf{0}$$

Case Study: Communication Protocol

- The protocol must be such that a message is delivered after the shared medium is accessed, i.e.,

$$Spec \triangleq acc.\overline{del}.Spec$$

- A possible implementation of this protocol may deal with a faulty medium, i.e.,

$$Impl \triangleq (Send \mid Med \mid Rec) \setminus \{send, trans, ack, error\}$$

- Implementation verification

$$Impl \overset{?}{\approx} Spec$$

Case Study: Communication Protocol

$$Impl \triangleq (Send \mid Med \mid Rec) \setminus \{send, trans, ack, error\}$$

- Sender's behaviour:

$$Send \triangleq acc.Sending$$
$$Sending \triangleq \overline{send}.Wait$$
$$Wait \triangleq ack.Send + error.Sending$$

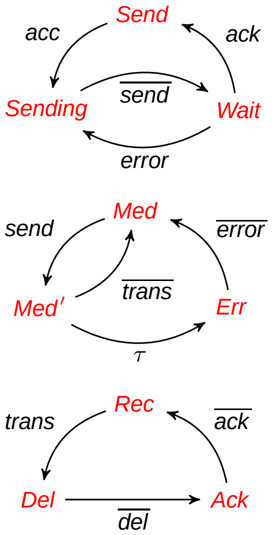
- Medium's behaviour:

$$Med \triangleq send.Med'$$
$$Med' \triangleq \tau.Err + \overline{trans}.Med$$
$$Err \triangleq \overline{error}.Med$$

- Receiver's behaviour:

$$Rec \triangleq trans.Del$$
$$Del \triangleq \overline{del}.Ack$$
$$Ack \triangleq \overline{ack}.Rec$$

Visual Execution of the Protocol



$$(Send \mid Med \mid Rec) \setminus \{send, trans, ack, error\}$$

1 Initial state

2 Medium accessed

3 Message sent

4 Message transmitted to receiver

5 Message delivered

6 Acknowledgement sent

7 **New message:** Medium accessed

8 Message sent

9 Invisible action

10 Error found

11 Message re-sent

12 New invisible action

13 New error found . . .