Strong Bisimulation

Motivation

- The informal specification

  The sequence of actions $a_1 \dots a_n$ must be carried out cyclically starting with a_1

  cannot be formalised in HML (or CTL$^-$)

- More natural way of specifying this: When all actions but $a_1, \dots, a_n$ are restricted, the system should “behave like” the process P, defined by

$$P \stackrel{\text{def}}{=} \mathtt{a}_1.\mathtt{a}_2.\dots.\mathtt{a}_\mathtt{n}.P$$

- Generally: Many systems are informally specified by “behave like” statements.
  Example: When using `telnet` our machine should “behave like” the remote machine (abstracting from delays).

- But how to formalise “behavioural equivalence”?

The wish-list

1. Behavioural equivalence should be a reflexive, symmetric, and transitive relation.
2. Processes that may terminate (deadlock) should not be equivalent to processes that may not terminate (deadlock).
3. If a component Q of P is replaced by an equivalent component Q' yielding P', then P and P' should also be equivalent.
4. Two processes should be equivalent iff they satisfy exactly the same properties expressible in a nice modal or temporal logic.
5. It should abstract from silent actions.

We deal first with conditions (1)-(3), conditions (4) and (5) are considered later.

A first candidate: Trace equivalence

A trace of a process P is a sequence of actions $\sigma = \alpha_1, \ldots, \alpha_n$ such that $P \xrightarrow{\sigma} Q = P \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_n} Q$ for some process Q.

Two processes P and Q are trace-equivalent if they have the same traces.

This notion satisfies (1) but not (2). The following two clocks are trace-equivalent

$$
\begin{aligned}
\mathtt{Cl} &\stackrel{\text{def}}{=} \mathtt{tick.Cl} \\
\mathtt{Cl}_5 &\stackrel{\text{def}}{=} \mathtt{tick.Cl}_5 + \mathtt{tick.0}
\end{aligned}
$$

A second candidate:

Completed-trace equivalence

A completed trace of a process P is a sequence σ of actions such that $P \xrightarrow{\sigma} Q$ for some process Q that cannot execute any action.

Two processes P and Q are completed-trace equivalent if they are trace equivalent and have the same completed traces.

This notion satisfies (1) and (2), but not (3).

Consider the processes

$$
\begin{aligned}
\mathtt{Ven}_1 &\stackrel{\text{def}}{=} \mathtt{1p}.\mathtt{1p}.(\mathtt{tea}.\mathtt{Ven}_1 + \mathtt{coffee}.\mathtt{Ven}_1) \\
\mathtt{Ven}_2 &\stackrel{\text{def}}{=} \mathtt{1p}.(\mathtt{1p}.\mathtt{tea}.\mathtt{Ven}_2 + \mathtt{1p}.\mathtt{coffee}.\mathtt{Ven}_2) \\
\mathtt{Use} &\stackrel{\text{def}}{=} \overline{\mathtt{1p}}.\overline{\mathtt{1p}}.\overline{\mathtt{tea}}.\overline{\mathtt{ok}}.0
\end{aligned}
$$

$\mathtt{Ven}_1$ and $\mathtt{Ven}_2$ are completed-trace equivalent, but new K $(\mathtt{Ven}_1 \mid \mathtt{Use})$ and new K $(\mathtt{Ven}_2 \mid \mathtt{Use})$, where $K = \{\mathtt{1p}, \mathtt{tea}, \mathtt{coffee}\}$, are not.

A third candidate: Bisimulation equivalence

A binary relation B between processes is a (strong) bisimulation provided that, whenever $(P, Q) \in B$ and α an action,

- if $P \xrightarrow{\alpha} P'$ then $Q \xrightarrow{\alpha} Q'$ for some Q' such that $(P', Q') \in B$, and
- if $Q \xrightarrow{\alpha} Q'$ then $P \xrightarrow{\alpha} P'$ for some P' such that $(P', Q') \in B$

Two processes P and Q are bisimulation equivalent (or bisimilar) if there is a bisimulation relation B such that $(P, Q) \in B$. We write $P \sim Q$ if P and Q are bisimilar.

Showing Bisimilarity

To establish $P \sim Q$,

1. present a candidate relation B with $(P, Q) \in B$;
2. prove that B is a bisimulation.

Example

Consider the processes

$$\begin{aligned} \mathtt{Cl} &\stackrel{\mathrm{def}}{=} \mathtt{tick.Cl} \\ \mathtt{Cl}_2 &\stackrel{\mathrm{def}}{=} \mathtt{tick.tick.Cl}_2 \end{aligned}$$

$B_1 = \{(\mathtt{Cl}, \mathtt{Cl}_2)\}$ is not a bisimulation.

$B_2 = \{(\mathtt{Cl}, \mathtt{Cl}_2), (\mathtt{Cl}, \mathtt{tick.Cl}_2)\}$ is a bisimulation.

Exercise Prove that B_2 is a bisimulation.

Example

Consider the processes

$$
\begin{aligned}
\mathtt{Sem} &\stackrel{\text{def}}{=} \mathtt{get}.\mathtt{Sem}' \\
\mathtt{Sem}' &\stackrel{\text{def}}{=} \mathtt{put}.\mathtt{Sem}
\end{aligned}
$$

$$
\begin{aligned}
\mathtt{Sem2}_0 &\stackrel{\text{def}}{=} \mathtt{get}.\mathtt{Sem2}_1 \\
\mathtt{Sem2}_1 &\stackrel{\text{def}}{=} \mathtt{get}.\mathtt{Sem2}_2 + \mathtt{put}.\mathtt{Sem2}_0 \\
\mathtt{Sem2}_2 &\stackrel{\text{def}}{=} \mathtt{put}.\mathtt{Sem2}_1
\end{aligned}
$$

The relation

$$
\begin{aligned}
B \quad = \{ \quad & (\mathtt{Sem2}_0, \mathtt{Sem} \mid \mathtt{Sem}), \\
& (\mathtt{Sem2}_1, \mathtt{Sem}' \mid \mathtt{Sem}), \\
& (\mathtt{Sem2}_1, \mathtt{Sem} \mid \mathtt{Sem}'), \\
& (\mathtt{Sem2}_2, \mathtt{Sem}' \mid \mathtt{Sem}') \quad \}
\end{aligned}
$$

is a bisimulation.

Exercise Prove that B is a bisimulation.

Example

The processes $\mathtt{a}.(\mathtt{b}.0 + \mathtt{c}.0)$ and $\mathtt{a}.\mathtt{b}.0 + \mathtt{a}.\mathtt{c}.0$ are not bisimilar.

Assume there is a bisimulation B containing the pair

$$(\mathtt{a}.(\mathtt{b}.0 + \mathtt{c}.0), \mathtt{a}.\mathtt{b}.0 + \mathtt{a}.\mathtt{c}.0)$$

Then B also contains

$$((\mathtt{b}.0 + \mathtt{c}.0), \mathtt{b}.0)$$

The left process can do a c, but the right one cannot. Contradiction.

Example

Consider the processes new $c\,(A|B)$ and C_1

where

$$
\begin{array}{lcl}
A & \stackrel{\mathrm{def}}{=} & a.\overline{\mathsf{c}}.A \\
B & \stackrel{\mathrm{def}}{=} & c.\overline{\mathsf{b}}.B \\
C_0 & \stackrel{\mathrm{def}}{=} & \overline{\mathsf{b}}.C_1 + a.C_2 \\
C_1 & \stackrel{\mathrm{def}}{=} & a.C_3 \\
C_2 & \stackrel{\mathrm{def}}{=} & \overline{\mathsf{b}}.C_3 \\
C_3 & \stackrel{\mathrm{def}}{=} & \tau.C_0
\end{array}
$$

The relation

$$
\begin{array}{l}
B = \{(\text{new } c\,(A|B), C_1), (\text{new } c\,(\overline{\mathsf{c}}.A|B), C_3) \\
(\text{new } c\,(A|\overline{\mathsf{b}}.B), C_0), (\text{new } c\,(\overline{\mathsf{c}}.A|\overline{\mathsf{b}}.B), C_2)\}
\end{array}
$$

is a bisimulation.

Exercise Prove that B is a bisimulation.

Exercise

Which of the following are bisimilar?

		Y/N
$\mathsf{a}.0$	$\mathsf{a}.\mathsf{a}.0$	
$\mathsf{a}.0$	$\mathsf{a}.0 + \mathsf{a}.0$	
$\mathsf{a}.0$	$\mathsf{a}.0 \mid \mathsf{a}.0$	
$\mathsf{a}.\mathsf{a}.0$	$\mathsf{a}.0 \mid \mathsf{a}.0$	
$\mathsf{a}.\mathsf{b}.0$	$\mathsf{a}.0 \mid \mathsf{b}.0$	
$\mathsf{a}.\mathsf{b}.0 + \mathsf{b}.\mathsf{a}.0$	$\mathsf{a}.0 \mid \mathsf{b}.0$	
$\mathsf{a}.\overline{\mathsf{a}}.0 + \overline{\mathsf{a}}.\mathsf{a}.0$	$\mathsf{a}.0 \mid \overline{\mathsf{a}}.0$	
$\mathsf{a}.\overline{\mathsf{a}}.0 + \overline{\mathsf{a}}.\mathsf{a}.0 + \tau.0$	$\mathsf{a}.0 \mid \overline{\mathsf{a}}.0$	
$\tau.0$	new $a\,(\mathsf{a}.0 \mid \overline{\mathsf{a}}.0)$	

A Bigger Example

$\texttt{Cnt} \sim \texttt{Ct}_0$

$$\begin{array}{lcl} \texttt{Cnt} & \stackrel{\mathrm{def}}{=} & \texttt{up}.(\texttt{Cnt} \mid \texttt{down}.0) \\ \texttt{Ct}_0 & \stackrel{\mathrm{def}}{=} & \texttt{up}.\texttt{Ct}_1 \\ \texttt{Ct}_{i+1} & \stackrel{\mathrm{def}}{=} & \texttt{up}.\texttt{Ct}_{i+2} + \texttt{down}.\texttt{Ct}_i \;\; i \geq 0. \end{array}$$

Let $\texttt{Proc}_i$ be the following families of processes for $i \geq 0$ (when brackets are dropped between parallel components)

$$\begin{array}{lcl} \texttt{Proc}_0 & = & \{\texttt{Cnt} \mid 0^j \;:\; j \geq 0\} \\ \texttt{Proc}_{i+1} & = & \{P \mid 0^j \mid \texttt{down}.0 \mid 0^k \;:\; P \in \texttt{Proc}_i \\ & & \quad \text{and } j \geq 0 \text{ and } k \geq 0\}, \end{array}$$

where $Q \mid 0^0 = Q$ and $Q \mid 0^{i+1} = Q \mid 0^i \mid 0$.

$$B \;=\; \{(P, \texttt{Ct}_i) \;:\; i \geq 0 \text{ and } P \in \texttt{Proc}_i\}$$

is a bisimulation.

Bisimilarity is an equivalence relation

Theorem: For all processes P, Q and R

1. $P \sim P$;
2. if $P \sim Q$ then $Q \sim P$;
3. if $P \sim Q$ and $Q \sim R$, then $P \sim R$.

Proof of 3: Since $P \sim Q$, $(P, Q) \in B_1$ for some bisimulation B_1. Since $Q \sim R$, $(Q, R) \in B_2$ for some bisimulation B_2. So $(P, R) \in B_1 \circ B_2$ where $\circ$ is relation composition. We show that $B_1 \circ B_2$ is a bisimulation. Let $(S_1, S_2) \in B_1 \circ B_2$ and $S_1 \xrightarrow{\alpha} S_1'$. We must find S_2' st. $S_2 \xrightarrow{\alpha} S_2'$ and $(S_1', S_2') \in B_1 \circ B_2$. As $(S_1, S_2) \in B_1 \circ B_2$, there is S such that $(S_1, S) \in B_1$ and $(S, S_2) \in B_2$. Since B_1 is bisimulation, there is S' such that $S \xrightarrow{\alpha} S'$ and $(S_1', S') \in B_1$. Since B_2 is bisimulation, there is S_2' such that $S_2 \xrightarrow{\alpha} S_2'$ and $(S', S_2') \in B_2$. Since $(S_1', S') \in B_1$ and $(S', S_2') \in B_2$, we have $(S_1', S_2') \in B_1 \circ B_2$.

Now check the case when $(S_1, S_2) \in B_1 \circ B_2$ and $S_2 \xrightarrow{\alpha} S_2'$. It is very similar.

Bisimilarity is a congruence

Proposition

The relation $\sim$ is a **congruence**: that is, given arbitrary processes P and Q with $P \sim Q$, then for any process R, for any set of actions K, for any action α and action names a, b,

1. $\alpha.P \sim \alpha.Q$
2. $P + R \sim Q + R$
3. $P \mid R \sim Q \mid R$
4. $P[b/a] \sim Q[b/a]$
5. $(\text{new } K)\, P \sim (\text{new } K)\, Q$

The proof of case 3 is the most interesting case. It is given on the next slide.

Largest bisimulation

Proposition $\sim$ is the largest bisimulation.

The proof is easy and left as an exercise.

Proof of case 3 We show that

$$B = \{(P \mid R, Q \mid R) \, : \, P \sim Q\}$$

is a bisimulation. Suppose that $((P \mid R), (Q \mid R)) \in B$ and $P \mid R \xrightarrow{\alpha} P' \mid R'$. There are three possibilities:

- $P \xrightarrow{\alpha} P'$ and $R = R'$. Because $P \sim Q$, we know that $Q \xrightarrow{\alpha} Q'$ and $P' \sim Q'$ for some Q'. Therefore $Q \mid R \xrightarrow{\alpha} Q' \mid R$, and so $((P' \mid R), (Q' \mid R)) \in B$.

- $R \xrightarrow{\alpha} R'$ and $P' = P$.
  So $Q \mid R \xrightarrow{\alpha} Q \mid R'$, and by definition $((P \mid R'), (Q \mid R')) \in B$.

- $P \mid R \xrightarrow{\tau} P' \mid R'$ and $P \xrightarrow{a} P'$ and $R \xrightarrow{\overline{a}} R'$ (or vice versa). $Q \xrightarrow{a} Q'$ for some Q' such that $P' \sim Q'$, so $Q \mid R \xrightarrow{\tau} Q' \mid R'$, and therefore $((P' \mid R'), (Q' \mid R')) \in B$.

  Observe that the symmetric case for $Q \mid R \xrightarrow{\alpha} Q' \mid R'$ is similiar.

More Properties

Proposition

1. $P + Q \sim Q + P$
2. $P + (Q + R) \sim (P + Q) + R$
3. $P + 0 \sim P$
4. $P + P \sim P$
5. $P \,|\, Q \sim Q \,|\, P$
6. $P \,|\, (Q \,|\, R) \sim (P \,|\, Q) \,|\, R$
7. $P \,|\, 0 \sim P$
8. $\mathrm{new}\, K\, (P+Q) \sim \mathrm{new}\, K\, (P) + \mathrm{new}\, K\, (Q)$
9. $\mathrm{new}\, K\, (a.P) \sim 0$ if $a \in K$
10. $\mathrm{new}\, K\, (a.P) \sim a.(\mathrm{new}\, K\, P)$ if $a \notin K$

Introduction to the Expansion Law

The expansion law states that a process with parallel compositions is bisimilar to a (possibly huge) process without parallel compositions.

Example

Given

$$
\begin{aligned}
P_1 &\sim a.P_{11} + b.P_{12} + a.P_{13} \\
P_2 &\sim \overline{a}.P_{21} + c.P_{22},
\end{aligned}
$$

then

$$
\begin{aligned}
P_1|P_2 \sim\ & a.(P_{11}|P_2) + b.(P_{12}|P_2) + a.(P_{13}|P_2) \\
& + \overline{a}.(P_1|P_{21}) + c.(P_1|P_{22}) \\
& + \tau.(P_{11}|P_{21}) + \tau.(P_{13}|P_{21})
\end{aligned}
$$

Expansion law

Generalised Choice

$\Sigma_{i \in I} P_i$ or $\Sigma\{P_i : i \in I\}$

Transition Rule

$$\frac{P_i \xrightarrow{\alpha} P_i'}{\Sigma_{i \in I} P_i \xrightarrow{\alpha} P_i'}$$

$P_i \sim \sum\{\alpha_{ij}.P_{ij} \ : \ 1 \leq j \leq n_i\}$, every $1 \leq i \leq m$.

$$P_1 \mid \ldots \mid P_m \ \sim$$
$$\sum\{\alpha_{ij}.Q_{ij} \ : \ 1 \leq i \leq m \text{ and } 1 \leq j \leq n_i\} +$$
$$\sum\{\tau.Q_{klij} \ : \ 1 \leq k < i \leq m \text{ and } \alpha_{kl} = \overline{\alpha}_{ij} \neq \tau\},$$

$$Q_{ij} \ = \ P_1 \mid \ldots \mid P_{i-1} \mid P_{ij} \mid P_{i+1} \mid \ldots \mid P_m$$

$$Q_{klij} \ = \ P_1 \mid \ldots \mid P_{k-1} \mid P_{kl} \mid P_{k+1} \mid \ldots \mid P_{i-1} \mid P_{ij} \mid P_{i+1} \mid \ldots \mid P_m.$$

($\alpha_{kl} = \overline{\alpha}_{ij} \neq \tau$ means $\alpha_{kl} = a$ and $\alpha_{ij} = \bar{\mathsf{a}}$ or $\alpha_{ij} = a$ and $\alpha_{kl} = \bar{\mathsf{a}}$, for action name a)

Bisimilarity and Hennessy-Milner Logic

Say $P \equiv_{HM} Q$ if P and Q satisfy exactly the same formulae of HM-Logic.

Proposition If $P \sim Q$ then $P \equiv_{HM} Q$.

Proof By induction on modal formulae Φ, we show that, for any P and Q, if $P \sim Q$, then $P \models \Phi$ iff $Q \models \Phi$.

Basis $\Phi = \mathtt{tt}$ or $\Phi = \mathtt{ff}$. Clear.

Induction step We consider only the case $\Phi = [L]\Psi$. By symmetry, it suffices to show that $P \models [L]\Psi$ implies $Q \models [L]\Psi$. Assume $P \models [L]\Psi$ and let $Q \xrightarrow{\alpha} Q'$ for arbitrary $\alpha \in L$. Since $P \sim Q$, there is a P' such that $P \xrightarrow{\alpha} P'$ and $P' \sim Q'$. Since $P \models [L]\Psi$, it follows that $P' \models \Psi$. By the induction hypothesis $Q' \models \Psi$, and so $Q \models \Phi$.

A process P is immediately image-finite if, for each action α, the set $\{Q \ : \ P \xrightarrow{\alpha} Q\}$ is finite.

P is **image-finite** if all processes reachable from it are immediately image-finite.

Proposition If P and Q are image-finite and $P \equiv_{\mathrm{HM}} Q$, then $P \sim Q$.

Proof We show that the following relation is a bisimulation.

$$\{(P, Q) \ : P \equiv_{\mathrm{HM}} Q \text{ and } P, Q \text{ are image-finite}\}$$

Suppose not. Then there exists R and S such that

$R \equiv_{\mathrm{HM}} S$,
$R \xrightarrow{\alpha} R'$ for some α and R',
$R' \not\equiv_{\mathrm{HM}} S'$ for any S' such that
$S \xrightarrow{\alpha} S'$.

Case 1 The set $\{S' \ : S \xrightarrow{\alpha} S'\}$ is empty.
Then $R \models \langle\alpha\rangle\mathtt{tt}$ but $S \not\models \langle\alpha\rangle\mathtt{tt}$, contradiction.

Case 2 The set $\{S' \ : S \xrightarrow{\alpha} S'\}$ is non-empty.

By image-finiteness, the set is $\{S_1, \ldots, S_n\}$ for some n. Since $R' \not\equiv_{\mathrm{HM}} S_i$ for each $i : 1 \leq i \leq n$, there are formulae $\Phi_1, \ldots, \Phi_n$ such that $R' \models \Phi_i$ and $S_i \not\models \Phi_i$.

(Here we use the fact that HML is closed under complement.)

Let $\Psi = \Phi_1 \wedge \ldots \wedge \Phi_n$.

$R \models \langle\alpha\rangle\Psi$ but $S \not\models \langle\alpha\rangle\Psi$ because each S_i fails to have property Ψ. Contradiction.

Example

Here is an example to show that the image-finiteness condition is necessary.

Consider the processes

$$\begin{aligned} \mathtt{Cl}^1 &\stackrel{\text{def}}{=} \mathtt{tick}.0 \\ \mathtt{Cl}^{i+1} &\stackrel{\text{def}}{=} \mathtt{tick}.\mathtt{Cl}^i, i \geq 1 \\ \mathtt{Cl} &\stackrel{\text{def}}{=} \mathtt{tick}.\mathtt{Cl} \end{aligned}$$

Now consider the processes

$$\begin{aligned} P &= \Sigma\{\mathtt{Cl}^i : i \geq 1\} \\ Q &\stackrel{\text{def}}{=} P + \mathtt{Cl} \end{aligned}$$

P and Q are not image finite.

P and Q are not bisimilar exercise

However, $P \equiv_{HM} Q$ a proof is in Stirling's book