Bisimilarity is a bisimulation

Exercise: $\sim$ is (1) an equivalence and (2) a bisimulation.

Proof (1) For reflexivity, it is enough to show that the identity relation over $\mathcal{Q}$, that is the relation $Id_{\mathcal{Q}} = \{(p,p) \mid p \in \mathcal{Q}\}$, is a bisimulation. This is easy.

For symmetry, we have to show that if $\mathcal{S}$ is a bisimulation then so is its converse $\mathcal{S}^{-1}$. But this is obvious from Definition 3.6.

For transitivity, we must show that if $\mathcal{S}_1$ and $\mathcal{S}_2$ are bisimulations, then so is their relational composition

$$\mathcal{S}_1\mathcal{S}_2 = \{(p,r) \mid \exists q.\ p\mathcal{S}_1 q \text{ and } q\mathcal{S}_2 r\}\ .$$

It is enough to show that this is a simulation. Let $(p,r) \in \mathcal{S}_1\mathcal{S}_2$, and $p \xrightarrow{\alpha} p'$. Since there exists q such that $p\mathcal{S}_1 q$ and $q\mathcal{S}_2 r$, there exist also q' such that $q \xrightarrow{\alpha} q'$ and $p'\mathcal{S}_1 q'$, and hence r' such that $r \xrightarrow{\alpha} r'$ and $q'\mathcal{S}_2 r'$. So $(p',r') \in \mathcal{S}_1\mathcal{S}_2$, and we have established the simulation condition for $\mathcal{S}_1\mathcal{S}_2$.

(2) Let $p \sim q$. Then by definition $p\mathcal{S}q$ for some bisimulation $\mathcal{S}$. Therefore if $p \xrightarrow{\alpha} p'$, there exists q' for which $q \xrightarrow{\alpha} q'$ and $p'\mathcal{S}q'$ – hence also $p' \sim q'$. Thus $\sim$ satisfies the simulation condition, and by symmetry so does its converse. ■

Bisimilarity: Back-and-forth property

Theorem

$p \sim q$ if and only if

1. $p \xrightarrow{\alpha} p'$ *implies for some* q', $q \xrightarrow{\alpha} q'$ *and* $p' \sim q'$
2. $q \xrightarrow{\alpha} q'$ *implies for some* p', $p \xrightarrow{\alpha} p'$ *and* $p' \sim q'$

Definition

Define $p \sim' q$ if and only if

1. $p \xrightarrow{\alpha} p'$ implies for some q', $q \xrightarrow{\alpha} q'$ and $p' \sim q'$
2. $q \xrightarrow{\alpha} q'$ implies for some p', $p \xrightarrow{\alpha} p'$ and $p' \sim q'$

Proof.

By showing that $\sim' = \sim$. Since $\sim$ is a bisimulation $\sim \subseteq \sim'$ (*). To show $\sim' \subseteq \sim$, verify that $\sim'$ is a bisimulation. This can be done by using (*) to show that if $p' \sim q'$ then $p' \sim' q'$.

□

Proof of commutativity of $\|$:

<u>Proposition</u> $P \mid Q \sim Q \mid P$

<u>Proof</u> We need to find a bisimulation which contains the pair $(P|Q, Q|P)$ for arbitrary P and Q. In fact we shall show that the set of <u>all</u> such pairs

$$\mathcal{S} \stackrel{\text{def}}{=} \{ (P|Q, Q|P) \mid P, Q \in \mathcal{P} \}$$

is a strong bisimulation. To show this consider an arbitrary transition $P|Q \xrightarrow{\alpha} R_1$; we have to find a matching transition $Q|P \xrightarrow{\alpha} R_2$ with $(R_1, R_2) \in \mathcal{S}$. There are three cases, according to how the given transition is inferred:

<u>Case 1</u> $R_1 \equiv P'|Q$, with the transition inferred by <u>Com</u>, from $P \xrightarrow{\alpha} P'$. Then we can infer $Q|P \xrightarrow{\alpha} Q|P'$ by <u>Com</u>$_2$, and take $R_2 \equiv Q|P'$.

<u>Case 2</u> $R_1 \equiv P|Q'$, with the transition inferred by <u>Com</u>$_2$ from $Q \xrightarrow{\alpha} Q'$. This case is symmetric with Case 1.

<u>Case 3</u> $R_1 \equiv P'|Q'$, with the transition inferred by <u>Com</u>$_3$ from $P \xrightarrow{\ell} P'$ and $Q \xrightarrow{\bar{\ell}} Q'$ (same ℓ), and $\alpha = \tau$. Then we can also infer $Q|P \xrightarrow{\tau} Q'|P'$ by <u>Com</u>$_3$, and take $R_2 \equiv Q'|P'$.

⊠

Counter instructions

We have sequentialization and counters. For counter X replace C with X and *zero*, *inc*, *dec* with $zero_x, inc_X, dec_X$. As before we use t to signal termination.

- The instruction $X++$ corresponds to $\overline{inc_X}.\bar{t}$ and
- The instruction $X--$ corresponds to $dec_X.\bar{t} + zero_X.\bar{t}$
- Encode the assigment instruction $X := Y$.

Solution.

1. Provide R_X that resets X to 0, this is easy.
2. $M_{Y,X}(l)$ moves Y to X and produces $l_Y.\overline{inc_Y}.\overline{l_{Y-1}} \parallel \ldots \parallel l_1.\overline{inc_Y}.\bar{l}$.
   - $M_{Y,X}(l) \stackrel{def}{=} zero_Y.\bar{l} + dec_Y.\overline{inc_X}.\ (\nu l')(\ l'.\overline{inc_Y}.\bar{l} \ \parallel M_{Y,X}(l'))$.
3. The assigment instruction is given by $(\nu l)(\ R_X;\ (M_{Y,X}(l) \parallel l.\bar{t}))$

Recall our sequential composition $P; Q = (\nu\ s)(\ P[s/t] \parallel s.Q)$ where s is fresh and $\bar{t}$ is the last action of P.

Exercise: Prove that sequentialization is associative: $P; (Q; R) \sim (P; Q); R$.

Hint: Using the algebraic equations and the fact that $\sim$ is a congruence we get:

- $P; (Q; R) \sim (\nu s)(P[s/t] \parallel s.(\nu s')(Q[s'/t] \parallel s'.R)) \sim$
  - $\sim\ (\nu s)(\nu s')(P[s/t] \parallel s.(Q[s'/t] \parallel s'.R))$
- $(P; Q); R \sim (\nu s')((\nu s)(P[s/t] \parallel s.Q))[s'/t] \parallel s'.R)) \sim$ $(\nu s')(\nu s)(P[s/t] \parallel s.Q)[s'/t] \parallel s'.R)) \sim$
  - $\sim (\nu s)(\nu s')(P[s/t] \parallel s.Q[s'/t] \parallel s'.R))$
- It remains to prove that if s and s' are fresh then
  - $P[s/t] \parallel s.Q[s'/t] \parallel s'.R \sim P[s/t] \parallel s.(Q[s'/t] \parallel s'.R)$

Exercise: Prove that $p \sim q$ if and only if Player II (defender) has a winning strategy over Player I (attacker) for the game (p, q).

Definition. Say that p is game equivalent to q iff Player II has a winning stretegy for (p, q).

Proof: Assume that p is game equivalent to q. We show that $p \sim q$ by establishing that the relation $\mathcal{R} = \{(p, q) : p \text{ and } q \text{ are game equivalent}\}$ is a bisimulation. Suppose $p \xrightarrow{a} p'$, and as this is a possible move by player I we know that player II can respond with $q \xrightarrow{a} q'$ in such a way that $(p', q') \in \mathcal{R}$, and similarly when $q \xrightarrow{a} q'$. For the other direction suppose $p \sim q$, and so there is a bisimulation relation $\mathcal{R}$ such that $(p, q) \in \mathcal{R}$. We construct a winning strategy for player II for the game (p, q) : in any play, whatever move player I makes player II responds by making sure that the resulting pair of processes remain in the relation $\mathcal{R}$. Clearly player I cannot then win any play from (p, q). $\square$