

## 2G1516 Formal Methods

EXAMINATION PROBLEMS, REFERENCE SOLUTIONS  
18 December 2003, 8am–1pm

Mads Dam  
KTH/IMIT

1. Let

$$\text{Cyclic}(\phi_0, \phi_1, \phi_2) = \Box((\phi_0 \vee \phi_1 \vee \phi_2) \wedge (\phi_0 \rightarrow \bigcirc(\phi_0 U \phi_1)) \wedge (\phi_1 \rightarrow \bigcirc(\phi_1 U \phi_2)) \wedge (\phi_2 \rightarrow \bigcirc(\phi_2 U \phi_0)))$$

Suppose first that the conditions 1.–3. hold, and let  $k \geq 0$  be arbitrary. Then  $\xi^k \models \phi_0 \vee \phi_1 \vee \phi_2$ , by condition 1. Assume that  $\xi^k \models \phi_i$ ,  $i \in \{0, 1, 2\}$ . We must show that  $\xi^{k+1} \models \phi_i U \phi_{i \oplus 1}$ . By condition 2, either  $\xi^{k+1} \models \phi_i$  or  $\xi^{k+1} \models \phi_{i \oplus 1}$ . In the latter case we obtain  $\xi^k \models \bigcirc(\phi_i U \phi_{i \oplus 1})$  as desired. In the former case continue the construction. By condition 3 we will be able to find some  $k' > k$  such that  $\xi^{k'} \models \bigcirc(\phi_{i \oplus 1})$  and such that for all  $k''$  such that  $k \leq k'' \leq k'$ ,  $\xi^{k''} \models \phi_i$ . It follows that  $\xi^k \models \bigcirc(\phi_i U \phi_{i \oplus 1})$  also in this case.

Conversely, assume that  $\xi \models \text{Cyclic}(\phi_0, \phi_1, \phi_2)$  as defined above. Let  $k \geq 0$ . Condition 1 is trivially met. For condition 2, assume  $\xi^k \models \phi_i$ . Since  $\xi^k \models \bigcirc(\phi_i U \phi_{i \oplus 1})$  either  $\xi^{k+1} \models \phi_i$  or  $\xi^{k+1} \models \phi_{i \oplus 1}$ . For condition 3, observe that the use of the until operator forces  $\phi_{i \oplus 1}$  to eventually hold for some  $k' > k$  which is sufficient since  $i$  was chosen arbitrary.

An alternative, more direct, solution, is

$$\Box((\phi_0 \vee \phi_1 \vee \phi_2) \wedge (\phi_0 \rightarrow \bigcirc(\phi_0 \vee \phi_1)) \wedge (\phi_1 \rightarrow \bigcirc(\phi_1 \vee \phi_2)) \wedge (\phi_2 \rightarrow \bigcirc(\phi_2 \vee \phi_0)) \wedge \Diamond \phi_0 \wedge \Diamond \phi_1 \wedge \Diamond \phi_3)$$

2. (The construction is actually in Peled already!) Let

$$A_1 \otimes A_2 = (Q_1 \times Q_2, \Sigma, \{((q_1, q_2), a, (q'_1, q'_2)) \mid q_1 \xrightarrow{a} q'_1, q_2 \xrightarrow{a} q'_2\}, I_1 \times I_2, F_1 \times F_2).$$

Suppose  $w = a_1 a_2 \dots a_n \dots \in L(A_1) \cap L(A_2)$ . Then there is a run of  $A_1$  of the shape

$$q_{0,1} \xrightarrow{a_1} q_{1,1} \xrightarrow{a_2} q_{2,1} \xrightarrow{a_3} \dots \xrightarrow{a_n} q_{n,1} \xrightarrow{a_{n+1}} \dots \quad (1)$$

and one of  $A_2$  of the shape

$$q_{0,2} \xrightarrow{a_1} q_{1,2} \xrightarrow{a_2} q_{2,2} \xrightarrow{a_3} \dots \xrightarrow{a_n} q_{n,2} \xrightarrow{a_{n+1}} \dots \quad (2)$$

such that  $q_{0,1} \in I_1$ ,  $q_{0,2} \in I_2$ , and for infinitely many  $i$ ,  $q_{i,2} \in F_2$  (we already know that  $q_{j,1} \in F_1$  for all  $j \geq 0$ ). But then we obtain a run in  $A_1 \otimes A_2$  of the shape

$$(q_{0,1}, q_{0,2}) \xrightarrow{a_1} (q_{1,1}, q_{1,2}) \xrightarrow{a_2} (q_{2,1}, q_{2,2}) \xrightarrow{a_3} \dots \xrightarrow{a_n} (q_{n,1}, q_{n,2}) \xrightarrow{a_{n+1}} \dots \quad (3)$$

such that  $(q_{0,1}, q_{0,2}) \in I_{A_1 \otimes A_2}$  and for infinitely many  $i$ ,  $(q_{i,1}, q_{i,2}) \in F_{A_1 \otimes A_2}$ , i.e.  $w \in L(A_1 \otimes A_2)$ . For the converse direction, if  $w = a_1 a_2 \dots a_n \dots \in L(A_1 \otimes A_2)$  then we find an accepting run of the shape (3). This run is split componentwise into the runs (1) and (2). Both runs will be accepting. Thus  $w \in L(A_1) \cap L(A_2)$ .

- 
3. Let  $c_1$  be the command  $x := x + 1 ; x := x + 1$  and  $c_2$  the program  $x := x + 2$ . We obtain that  $c_1 \simeq c_2$ . To see this observe first that  $\{\phi\}c_1\{\psi\}$  iff  $\{\phi\}x := x + 1\{\psi[x + 1/x]\}$  iff  $\models \phi \rightarrow \psi[x + 2/x]$  iff  $\{\phi\}c_2\{\psi\}$ . Let then  $c$  be the command  $x := 0$ . We prove that  $\{true\}c \parallel c_2 \{x = 0 \vee x = 2\}$ . To see this let  $\sigma$  be an arbitrary store. If  $(c \parallel c_2, \sigma) \rightarrow^* \sigma'$  then  $(c \parallel c_2, \sigma) \rightarrow (c'', \sigma'') \rightarrow \sigma'$  such that either  $c'' = c$ ,  $\sigma'' = \sigma[x + 2/x]$ , hence  $\sigma'(x) = 0$ , or  $c'' = c_2$  and  $\sigma'' = \sigma[0/x]$ , and then  $\sigma'(x) = 2$ . But the Hoare triple  $\{true\}c \parallel c_1 \{x = 0 \vee x = 2\}$  is false, since  $(c \parallel c_1, \sigma) \rightarrow^* \sigma_1$  for some  $\sigma_1$  such that  $\sigma_1(x) = 1$ .
- 

4. Let:

$$\phi_1 = \neg done1 \wedge (\neg done2 \rightarrow x = 0) \wedge (done2 \rightarrow x = 1)$$

$$\phi_2 = \neg done2 \wedge (\neg done1 \rightarrow x = 0) \wedge (done1 \rightarrow x = 1)$$

$$\psi_1 = done1 \wedge (\neg done2 \rightarrow x = 1) \wedge (done2 \rightarrow x = 2)$$

$$\psi_2 = done2 \wedge (\neg done1 \rightarrow x = 1) \wedge (done1 \rightarrow x = 2)$$

The following are valid proof outlines for each of the parallel components:

$$\{\phi_1\} (x, done1) := (x + 1, true) \{\psi_1\}$$

and

$$\{\phi_2\} (x, done2) := (x + 1, true) \{\psi_2\}.$$

The proof outlines are interference free. To check this we note that the following triples are valid:

- $\{\phi_2 \wedge \phi_1\} (x, done2) := (x + 1, true) \{\phi_1\}$
- $\{\phi_2 \wedge \psi_1\} (x, done2) := (x + 1, true) \{\psi_1\}$
- $\{\phi_1 \wedge \phi_2\} (x, done1) := (x + 1, true) \{\phi_2\}$
- $\{\phi_1 \wedge \psi_2\} (x, done1) := (x + 1, true) \{\psi_2\}.$

By the rule for parallel composition (Owicki-Gries) it follows that the triple

$$\{\phi_1 \wedge \phi_2\} \text{cobegin } (x, done1) := (x+1, true) \parallel (x, done2) := (x+1, true) \text{coend } \{\psi_1 \wedge \psi_2\}$$

is valid. Since

- $\models x = 0 \rightarrow (\phi_1 \wedge \phi_2)[false/done1, false/done2]$ , and
- $\models (\psi_1 \wedge \psi_2) \rightarrow x = 2$ ,

it follows that  $\{x = 0\} c \{x = 2\}$  is valid.

- 
5.  $P = Q$  is proven by applying the definition of observational congruence. Define the relation  $S$  by

$$S = \{(P, Q)\}$$

Note that for all CCS processes  $P', P' \approx P'$ . We show that  $S$  is an observational congruence relation.

If  $P \xrightarrow{\alpha} P'$  then  $Q \xrightarrow{\tau} P \xrightarrow{\alpha} P'$  and  $P' \approx P'$ .

Symmetrically, if  $Q \xrightarrow{\alpha} Q'$  then  $P \xrightarrow{\tau} Q \xrightarrow{\alpha} Q'$  and  $Q' \approx Q'$ .

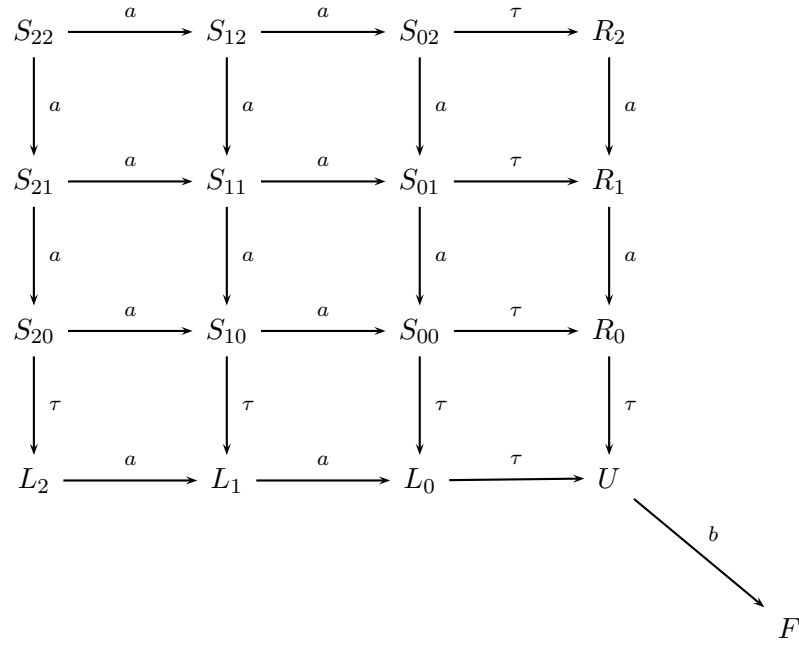
It follows that  $P = Q$ .

- 
6.  $\langle a \rangle [b]([c]false \vee [d]false)$

- 
7. We start with some abbreviations:

$$\begin{aligned} S_{ij} &\stackrel{\text{def}}{=} (\text{TR}(i)[c/b] \mid \text{TR}(j)[c/b] \mid \text{TR}(2)[c/a]) \setminus c & (0 \leq i, j \leq 2) \\ L_i &\stackrel{\text{def}}{=} (\text{TR}(i)[c/b] \mid 0[c/b] \mid \text{TR}(1)[c/a]) \setminus c & (0 \leq i \leq 2) \\ R_j &\stackrel{\text{def}}{=} (0[c/b] \mid \text{TR}(j)[c/b] \mid \text{TR}(1)[c/a]) \setminus c & (0 \leq j \leq 2) \\ U &\stackrel{\text{def}}{=} (0[c/b] \mid 0[c/b] \mid \text{TR}(0)[c/a]) \setminus c \\ F &\stackrel{\text{def}}{=} (0[c/b] \mid 0[c/b] \mid 0[c/a]) \setminus c \end{aligned}$$

The transition graph of system  $S$  (i.e.  $S_{22}$ ) is then:



Finally, notice that the following binary relation  $\mathcal{R}$  is a weak bisimulation, where  $S_{22} \mathcal{R} \text{TR}(4)$ .

$$\mathcal{R} = \{(S_{ij}, \text{TR}(i+j)), (L_i, \text{TR}(i)), (R_j, \text{TR}(j)), (U, \text{TR}(0)), (F, 0) \mid 0 \leq i, j \leq 2\}$$

We conclude that  $S \approx \text{TR}(4)$ .

---