

## 2G1516 Formal Methods

SOLUTIONS  
20 December 2005, 2pm–7pm

Mads Dam  
KTH/IMIT

1.

20p

1.  $\Box(\text{WriteReq} \rightarrow \langle \rangle (\text{WriteSuccess} \vee \text{WriteFail}))$  or, if we interpret “later” as “strictly later”,  $\Box(\text{WriteReq} \rightarrow O \langle \rangle (\text{WriteSuccess} \vee \text{WriteFail}))$ .
2. First attempt:  $\text{WriteReq} \wedge \langle \rangle \text{WriteSuccess}$ . A better solution, though, would be to consider a successful write operation as one which starts with a write request and ends with a write success, with no intervening write events:

$$\text{WriteReq} \wedge ((\neg \text{WriteReq} \wedge \neg \text{WriteFail})U \text{WriteSuccess}).$$

If we rule out the simultaneous occurrence of *WriteReq* and *WriteSuccess* as a legitimate write operation an even better solution would be  $\text{GoodWrite} = \text{WriteReq} \wedge O((\neg \text{WriteReq} \wedge \neg \text{WriteFail})U \text{WriteSuccess})$ .

3.  $\text{BusyInitially} = \Box(V \rightarrow (\neg \text{GoodWrite}U P))$
4.  $\text{BusyThroughout} = \Box(\text{GoodWrite} \rightarrow (\neg VU \text{WriteSuccess}))$
5.  $\text{BusyInitially} \wedge \text{BusyThroughout}$

2.  $\Box(a \rightarrow ((O\neg a)Ub))$

15p

3. Let  $A = (Q, \Sigma, \Delta, I, F)$  where  $F = \{q_1, \dots, q_n\}$  let  $A_i = (Q, \Sigma, \Delta, I, \{q_i\})$ ,  $1 \leq i \leq n$ . We claim that  $L(A) = L(A_1) \cup \dots \cup L(A_n)$ . For  $\subseteq$ , if word  $w = a_1, a_2, \dots$  is accepted by  $A$  then there is a sequence  $q'_0 \xrightarrow{a_1} q'_1 \xrightarrow{a_2} \dots$  such that  $q'_0 \in I$  and  $q'_i \in F$  for infinitely many  $i$ . But then there is some  $j : 1 \leq j \leq n$  such that  $q'_i \in \{q_j\}$  for infinitely many  $i$ , i.e.  $w \in L(A_j)$ . Conversely, for  $\supseteq$ , if there is some  $j : 1 \leq j \leq n$  such that  $q'_i \in \{q_j\}$  for infinitely many  $i$  then  $q'_i \in F$  for infinitely many  $i$  as well, so  $w \in L(A)$ . This completes the proof.

4. Proof outline  $\Delta_1$ :

$$\begin{aligned} &\{x = 0 \vee x = 2\} \\ &x := x + 1 \\ &\{x = 1 \vee x = 3\} \end{aligned}$$

20p

Critical formulas:  $\phi_{1,1} : x = 0 \vee x = 2$ ,  $\phi_{1,2} : x = 1 \vee x = 3$ .

Proof outline  $\Delta_2$ :

$$\begin{aligned} & \{x = 0 \vee x = 1\} \\ & x := x + 2 \\ & \{x = 2 \vee x = 3\} \end{aligned}$$

Critical formulas:  $\phi_{2,1} : x = 0 \vee x = 1$ ,  $\phi_{2,2} : x = 2 \vee x = 3$ .

Proofs of interference freedom:

- $\{\phi_{1,1} \wedge \phi_{2,1}\}x := x + 2\{\phi_{1,1}\}$
- $\{\phi_{1,2} \wedge \phi_{2,1}\}x := x + 2\{\phi_{1,2}\}$
- $\{\phi_{2,1} \wedge \phi_{1,1}\}x := x + 1\{\phi_{2,1}\}$
- $\{\phi_{2,2} \wedge \phi_{1,1}\}x := x + 1\{\phi_{2,2}\}$

These are all immediate. By the Owicki-Gries rule:

$$\{\phi_{1,1} \wedge \phi_{2,1}\}P\{\phi_{1,2} \wedge \phi_{2,2}\}$$

hence  $\{x = 0\}P\{x = 3\}$  by the rule of consequence.

5.

15p

- If  $P$  and  $Q$  are identical they are observationally congruent and hence also weakly bisimilar.
- $P$  is  $a.0$ ,  $Q$  is  $X$ . A weak bisimulation relation is  $\{(a.0, X), (a.0, a.0), (0, 0)\}$ .  $P$  and  $Q$  are not observationally congruent since the transition  $Q \xrightarrow{\tau} Q$  is not matched by a corresponding  $\tau$  transition by  $P$ .
- $P$  is  $a.0$ ,  $Q$  is  $Y$ . A weak bisimulation relation is  $\{(a.0, Y), (0, 0)\}$ . As in the previous case  $P$  and  $Q$  are not observationally congruent since the transition  $Q \xrightarrow{\tau} Q$  is not matched by a corresponding  $\tau$  transition by  $P$ .
- $P$  is  $X$  and  $Q$  is  $Y$ . A weak bisimulation relation is  $\{(X, Y), (a.0, Y), (0, 0)\}$ . An observational congruence relation is  $\{(x, y)\}$ .

6.

15p

$$\begin{aligned} I &= (P \mid Q) \setminus \{a\} \\ &= b.(P \mid Q) \setminus \{a\} + \tau.b.(P \mid Q) \setminus \{a\} \\ &= b.I + \tau.b.(P \mid Q) \setminus \{a\} \\ &= b.I + \tau.b.I \\ &= \tau.b.I \end{aligned}$$

Hence  $P = S$  by unique fixed point induction.