

## 2G1516 Formal Methods

EXAMINATION PROBLEMS, REFERENCE SOLUTIONS  
21 April 2004, 8am–1pm

*Mads Dam*  
KTH/IMIT

1. Domain specification: Variables are  $req_0, req_1, cs_0, cs_1, l$  and  $r$ . The first four range over  $\{0, 1\}$  as stated,  $l$  and  $r$  (the program counters) over  $\{0, 1, 2\}$ .

Initial condition: All variables have initial value 0

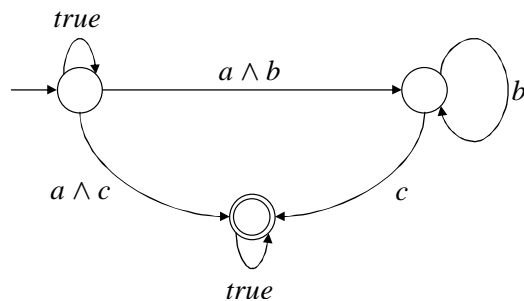
Transition specifications:

- $l = 0 \rightarrow (l, req_0) := (1, 1)$
- $l = 1 \wedge req_1 \neq 1 \rightarrow (l, cs_0) := (2, 1)$
- $l = 2 \rightarrow (l, req_0, cs_0) := (0, 0, 0)$
- $r = 0 \rightarrow (r, req_1) := (1, 1)$
- $r = 1 \wedge req_0 \neq 1 \rightarrow (r, cs_1) := (2, 1)$
- $r = 2 \rightarrow (r, req_1, cs_1) := (0, 0, 0)$

States in the generated state space have the shape  $\langle req_0, req_1, cs_0, cs_1, l, r \rangle$ , and the initial state is  $\langle 0, 0, 0, 0, 0, 0 \rangle$ . From the initial state, by executing the left process and the right process exactly once in random sequence the deadlocked state  $\langle 1, 1, 0, 0, 1, 1 \rangle$  is reached.

2.  $\Box \langle\langle a \wedge \Box \langle\langle b \rangle\rangle \rangle$ , or in CTL,  $AGAFa \wedge AGAFb$ .

3.



4. Let  $lhs = P + \alpha.Q + \alpha.(\tau.Q + R)$  and  $rhs = P + \alpha.(\tau.Q + R)$ . We show the relation  $S = \{(lhs, rhs)\} \cup Id$  is an observational congruence relation. To check this it is sufficient to note that

1. if  $lhs \xrightarrow{\beta} P'$  then either  $rhs \xrightarrow{\beta} P'$ , or  $rhs \xrightarrow{\beta} \circ \xrightarrow{\tau} P'$  in the case  $P' = Q$ , and
2. if  $rhs \xrightarrow{\beta} P'$  then  $lhs \xrightarrow{\beta} P'$ .

---

5. Let  $D = C^4[a/a_1, d/a_2, b/a_3, e/a_4]$ ,  $E = C^3[\bar{d}/a_1, c/a_2, \bar{e}/a_3]$ , and  $IMP = (D|E) \setminus \{d, e\}$ . To show  $IMP \approx SPEC$  we give a weak bisimulation relation  $R$ . The relation  $R$  contains the following pairs:

- $(IMP, SPEC)$ ,
- $((d.b.e.D|E) \setminus \{d, e\}, b.c.SPEC + c.b.SPEC)$ ,
- $((b.e.D|c.\bar{e}.E) \setminus \{d, e\}, b.c.SPEC + c.b.SPEC)$ ,
- $((e.D|c.\bar{e}.E) \setminus \{d, e\}, c.SPEC)$ ,
- $((b.e.D|\bar{e}.E) \setminus \{d, e\}, b.SPEC)$ ,
- $((e.D|\bar{e}.E) \setminus \{d, e\}, SPEC)$ .

---

6. The assertion network assigns assertions to nodes as follows:

- $s_0 \mapsto x \geq 1$
- $s_1 \mapsto y = \frac{x!}{z!} \wedge u = y$
- $s_2 \mapsto u = y(z - v + 1) \wedge y = \frac{x!}{z!}$
- $s_f \mapsto u = x!$

To prove the network is inductive there are six subcases to consider:

1.  $x \geq 1 \wedge x > 1 \rightarrow (y = \frac{x!}{z!} \wedge u = y)[x/y, x - 1/z, x/u]$ , which simplifies to  $x > 1 \rightarrow x = \frac{x!}{(x-1)!} \wedge x = x$ , which simplifies to true.
2.  $x \geq 1 \wedge x = 1 \rightarrow u = x![1/u]$  which simplifies to true.
3.  $y = \frac{x!}{z!} \wedge u = y \wedge z = 1 \rightarrow u = x!$  which simplifies to true.
4.  $y = \frac{x!}{z!} \wedge u = y \wedge z > 1 \rightarrow (u = y(z - v + 1) \wedge y = \frac{x!}{z!})[y/u, z/v]$  which simplifies first to  $y = \frac{x!}{z!} \wedge u = y \wedge z > 1 \rightarrow y = y(z - z + 1) \wedge y = \frac{x!}{z!}$  which simplifies further to true.
5.  $u = y(z - v + 1) \wedge y = \frac{x!}{z!} \wedge v > 1 \rightarrow (u = y(z - v + 1) \wedge y = \frac{x!}{z!})[u + y/u, v - 1/v]$  which simplifies to  $u = y(z - v + 1) \wedge y = \frac{x!}{z!} \wedge v > 1 \rightarrow u + y = y(z - (v - 1) + 1) \wedge y = \frac{x!}{z!}$  which simplifies to  $y(z - v + 1) + y = y(z - v + 2)$  which simplifies to true.

6.  $u = y(z - v + 1) \wedge y = \frac{x!}{z!} \wedge v = 1 \rightarrow (y = \frac{x!}{z!} \wedge u = y)[z - 1/z, u/y]$  which simplifies to  $u = yz \wedge y = \frac{x!}{z!} \rightarrow u = \frac{x!}{(z-1)!}$  which simplifies to true.

The network is trivially consistent.

---

7.

1.  $\langle 1p \rangle [1p] \text{false}$
  2.  $[1p] [1p] [1p] \text{false}$
  3.  $\nu X. ([1p] [1p] [1p] \text{false}) \wedge [-]X$
  4.  $\mu Y. \overline{\langle \text{coffee} \rangle \text{true}} \vee \langle 1p \rangle Y$
-