

2G1516 Formal Methods 2G1521 Formal Methods for SEDS

SOLUTIONS TO EXAMINATION PROBLEMS
10 January 2005, 3pm–8pm

Mads Dam
KTH/IMIT

Give solutions in English or Swedish, each problem beginning on a new sheet. Write your name on all sheets. The maximal number of points is given for each problem. Textbook, copies of slides, other written course material and English dictionaries are admissible. Computers, mobile phones, other written material, is not. Grades are given in the range F, 3, 4, 5 with the following cut-off points: 3: 45, 4: 60, 5: 80

1.

15p

1. flatten; skolem -1 x ; skolem 1 y , inst -1 y ; inst 1 x
2. flatten; skolem -1 x ; inst -2 x ; split

2.

15p

- $\xi, i \models \eta$ iff $\xi(i) \in \rho(\eta)$
- $\xi, i \models \neg\phi$ iff not $\xi, i \models \phi$
- $\xi, i \models \phi \wedge \psi$ iff $\xi, i \models \phi$ and $\xi, i \models \psi$
- $\xi, i \models \phi U \psi$ iff exists $k \geq i$ such that $\xi, k \models \psi$ and for all $j : i \geq j < k$, $\xi, j \models \phi$
- $\xi, i \models O\phi$ iff $\xi, i+1 \models \phi$
- $\xi, i \models \phi S \psi$ iff exists $k \leq i$ such that $\xi, k \models \psi$ and for all $j : k < j \leq i$, $\xi, j \models \phi$
- $\xi, i \models P\phi$ iff $i \geq 1$ and $\xi, i-1 \models \phi$

Properties:

1. $trueS\phi$
2. $\neg(trueS\neg\phi)$
3. $P(\neg\phi S(\phi \wedge P(\neg(trueS\phi))))$

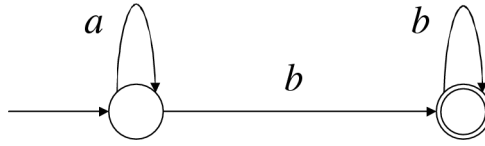


Figure 1: Buchi automaton for question 3

3. The Buchi automaton is shown on fig. 1.

15p

4. The transition diagram is shown on fig. 2. A transition network is obtained by the assignments:

25p

- $s_0 \mapsto x \geq 1$
- $s_f \mapsto y = x!$
- $s \mapsto y = \frac{x!}{z!}$

The network is consistent with respect to the given pre- and post-condition. To prove it is consistent we need to establish

- $x \geq 1 \rightarrow 1 = \frac{x!}{x!}$
- $y = \frac{x!}{z!} \wedge z = 1 \rightarrow y = x!$
- $y = \frac{x!}{z!} \wedge z > 1 \rightarrow yz = \frac{x!}{(z-1)!}$

which are all immediate.

5.

15p

1. The equivalence does not hold. The left hand side can perform the transition

$$b.0 + \tau.(a.0 + \tau.b.0) \xrightarrow{\tau} b.0$$

and $b.0$ cannot perform an a . This transition cannot be matched by any $\xrightarrow{\tau}$ transition of $b.0 + \tau.(a.0 + b.0)$. This is so since if

$$b.0 + \tau.(a.0 + b.0) \xrightarrow{\tau} Q$$

for some Q then Q can perform an \xrightarrow{a} -transition.

2. The equivalence does hold. A weak bisimulation relation containing the pair

$$(b.0 + \tau.(a.0 + \tau.b.0), b.0 + \tau.b.0 + \tau.(a.0 + \tau.b.0))$$

is the relation

$$I \cup (b.0 + \tau.(a.0 + \tau.b.0), b.0 + \tau.b.0 + \tau.(a.0 + \tau.b.0))$$

where I is the identity relation.

6.

15p

- $C^4 == C_0^4$
- $C_0^4 == zero.C_0^4 + inc.C_1^4$
- $C_i^4 == nonzero.C_i^4 + inc.C_{i \oplus 1}^4$ where $1 \leq i \leq 3$ and \oplus is addition modulo 4.

Let

- $P == z_h.(z_l.(\overline{zero}.P + inc.\overline{i_l}.P) + n_l.(\overline{nonzero}.P + inc.\overline{i_l}.\overline{i_h}.P)) + n_h.(z_l.(\overline{nonzero}.P + inc.\overline{i_l}.P) + n_l.(\overline{nonzero}.P + inc.\overline{i_l}.\overline{i_h}.P))$
- $f_1 = [z_l/zero, n_l/nonzero, i_l/inc]$
- $f_2 = [z_h/zero, n_h/nonzero, i_h/inc]$
- $L = \{z_l, n_l, i_l, z_h, n_h, i_h\}$

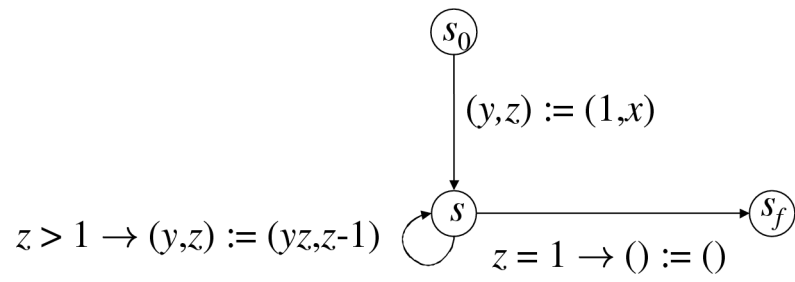


Figure 2: Transition diagram for question 4