

2G1516 Formal Methods

EXAMINATION PROBLEMS
21 April 2004, 8am–1pm

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: 70, 5: 90

-
1. The following program purports to solve mutual exclusion. Let $req_i, cs_i, i \in \{0, 1\}$, be variables over the domain of truthvalues $\{0, 1\}$ all with initial value 0. Let $P_i, i \in \{0, 1\}$, be the program: 12p

$$P_i : \text{while } 1 = 1 \text{ do } req_i := 1; req_{i \oplus 1} \neq 1 \rightarrow cs_i := 1; (cs_i, req_i) := (0, 0) \text{ od}$$

where \oplus is addition modulo 2. Represent the system $P_0 \parallel P_1$ as a transition system specification. Show that the generated state space has a deadlocked state.

-
2. Let a and b be primitive state assertions. Express the following property in LTL: Along all paths ξ there are infinitely many points n_0, n_1, n_2, \dots such that, when i is even, $\xi^{n_i} \models a$, and when i is odd, $\xi^{n_i} \models b$. Is this property also expressible in CTL? 12p

-
3. Produce a Buchi automaton equivalent to the LTL property $\langle \rangle (a \wedge (bUc))$. 12p

-
4. Prove the observational congruence $P + \alpha.Q + \alpha.(\tau.Q + R) = P + \alpha.(\tau.Q + R)$ 12p

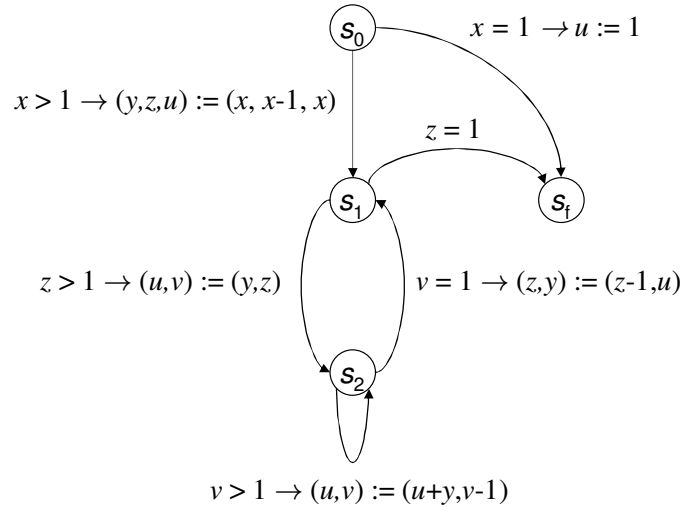
-
5. Let $\text{SPEC} == a.(b.c.\text{SPEC} + c.b.\text{SPEC})$. Define an n -cyclor thus: 18p

$$C^n == a_1.a_2.\dots.a_n.C^n.$$

Combine a 3-cyclor and a 4-cyclor using parallel composition, restriction, and relabelling, to obtain a process IMP for which you can prove that $\text{IMP} \approx \text{SPEC}$.

Please Turn Over

6. Consider the following transition diagram P where all variables range over the non-zero natural numbers:



Let ϕ_{pre} be the assertion $x \geq 1$ and ϕ_{post} be the assertion $u = x!$. Prove, using Floyd's inductive assertion method that P is partially correct for ϕ_{pre} and ϕ_{post} . (Hint: For s_1 use the invariant assertion $y = \frac{x!}{z!} \wedge u = y$ and for s_2 use the invariant assertion $u = y(z - v + 1) \wedge y = \frac{x!}{z!}$.)

7. Consider the following example of a "bad coffee machine":

$$P == 1p.\overline{tea}.P + 1p.1p.\overline{coffee}.P$$

Express the following properties of the coffee machine using HML and the modal μ -calculus:

1. In the initial state, after inserting a 1p coin it may happen that no further 1p coin can be entered.
2. In the initial state, no more than two consecutive 1p coins be entered.
3. It is never possible to enter more than two consecutive 1p coins.
4. In the initial state it is possible to produce coffee by entering some sequence of 1p coins.

Good luck!