2G1516 Formal Methods   2G1521 Formal Methods for SEDS

EXAMINATION PROBLEMS
18 October 2004, 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 computing or communication equipment, 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. Prove each of the following formulas using the basic PVS proof rules. If you find that a formula is false, give a counterexample instead. **15p**

    1. $(\exists x : (P(x) \wedge \forall y : Q(x, y))) \rightarrow \forall y : \exists x : (P(x) \wedge Q(x, y))$
    2. $(\forall x : (P(x) \rightarrow \exists y : Q(x, y))) \rightarrow (\exists y : \forall x : (P(x) \rightarrow Q(x, y)))$

---

2. Consider a simple slot machine with four events, i (insert), l (lose), w (win) and j (jackpot). Coins can be inserted at any time, and winnings (including jackpots) and losses are possible only when the balance is non-zero. As state assertions use en_e and $exec_e$ where e is an event. Express the following properties in LTL: **15p**

    1. An event can only take place when it is enabled.
    2. If an insert event infinitely often takes place then a jackpot event will infinitely often take place as well.
    3. An l event is enabled if and only if a w event is.
    4. The events are exclusive, i.e. at all time instants, one and only one of the four events take place.
    5. Infinitely often a j event will be enabled without it also taking place.
    6. After a jackpot a coin must be inserted before another winning is possible.

---

3. Construct a Buchi automaton accepting the language $[] <> a \wedge [] <> b$. **15p**

Please Turn Over

4. Represent the following program as a transition system specification: **15p**

```
z := 0 ;
cobegin
  while x != 0 do z := z + 1 ; x := x - 1 od
      ||
  while y != 0 do z := z + 1 ; y := y - 1 od
coend
```

5. Prove the Hoare triple **20p**

$\{$`x=x0 && x0 >= 0 && z = 0`$\}$ `while x != 0 do z := z + 1 ; x := x - 1 od` $\{$`z=x0`$\}$.

Give your answer in terms of a valid proof outline.

6. Determine whether or not the following observational equivalences hold: **20p**

1. $a.0 \mid b.0 \approx a.0 \mid \tau.b.0$
2. $a.0 \mid b.0 \approx \tau.a.0 \mid \tau.b.0$

If you claim the equivalences hold, establish a weak bisimulation relation. If you claim they do not, prove that no such relation can exist.

Good luck!