

## 2G1516 Formal Methods 2G1521 Formal Methods for SEDS

EXAMINATION PROBLEMS  
22 August 2005, 2pm–7pm

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.  $\forall x.((\exists x.R(x, x)) \rightarrow Q(x)) \rightarrow (R(x, x) \rightarrow Q(x))$

2.  $\forall x.((\forall x.R(x, x)) \rightarrow Q(x)) \rightarrow (R(x, x) \rightarrow Q(x))$

- 
2. In a distributed file application reading and writing of files is non-atomic. We therefore represent read and write events as pairs of events, *begin\_read(x)* and *end\_read(x)* for reading, and *begin\_write(x)* and *end\_write(x)* for writing, where *x* is a file. Express in LTL the following properties for a given file *x*: 15p

1. Each begin-event is always immediately followed by a corresponding end-event.

2. Each begin-event must be followed by a corresponding end-event some time later.

3. At each time instant at least one of the above four events takes place.

4. It is only possible to write to a file a finite number of times.

5. Before a read event can begin, a write event must have ended.

- 
3. Produce a Buchi automaton for property 5 of exercise 2 (note: I do not recommend using the LTL-Buchi translation procedure.) 15p

---

*Please Turn Over*

- 
4. Prove the Hoare triple, where  $a$  is an array from 1 to  $m$  of non-negative integers:

25p

```
{true}
x := 0 ;
i := 1 ;
while i <= m do
  if a[i] > x
  then x := a[i]
  else skip
  endif ;
  i := i + 1
od
{forall j. 1 <= j && j <= m implies x >= a[j]}
```

Give your answer as a valid proof outline.

- 
5. Determine whether or not the following observational equivalences hold:

15p

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

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

- 
6. Recall that a unary semaphore  $S^1$  is defined by the following equations:

15p

$$S^1 == p.S_1^1$$
$$S_1^1 == v.S^1$$

A binary semaphore  $s^2$  is defined similarly by the following three equations:

$$S^2 == p.S_1^2$$
$$S_1^2 == p.S_2^2 + v.S^2$$
$$S_2^2 == v.S_1^2$$

The CCS process  $I$  is obtained by chaining two unary semaphores in the following way:

$$I = (S^1[c/v] | S^1[\bar{c}/p]) \setminus \{c\}$$

Prove that  $I \approx S^2$  by exhibiting a suitable weak bisimulation relation.

---

*Good luck!*