LIACS
Leiden University

Examination Program Correctness
18 January 2005, 14:00 - 17:00

---

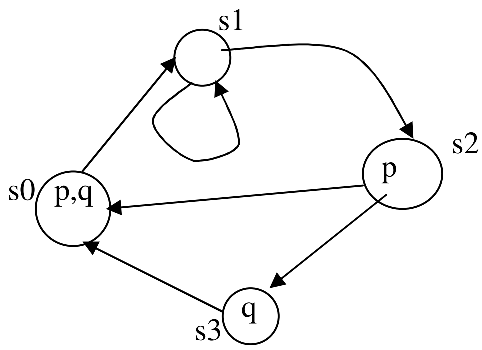
1. Consider a following generalization of CTL that permits reasoning about past state. It contains two new operators APϕ and EPϕ, with intended meaning given by

   - APϕ is true in state s if ϕ holds in all states immediately preceding s,
   - EPϕ is true in state s if ϕ holds in some state immediately preceding s.

   For each of the following propositions, indicates it they are true or not, providing either a justification or a model with a state s_0 in which the proposition is false

   a) $\phi \Rightarrow AX(AP\phi)$ **[5 pts]**
   b) $\phi \Rightarrow AX(EP\phi)$ **[5 pts]**
   c) $EX(AP\phi) \Rightarrow \phi$ **[5 pts]**
   d) $EX(EP\phi) \Rightarrow \phi$ **[5 pts]**

2. Using the fixed point method, give the set of states of the following transition system satisfying the CTL formula AG(AFq): **[15 pts]**



3. For each of the following pairs of CTL formulae exhibit a model with a state s_0 in which one formula is true but not the other:

   a) EF p and EG p **[5 pts]**
   b) $AF(p \vee q)$ and $AF\ p \vee AF\ q$ **[5 pts]**
   c) $EF\neg p$ and $\neg AFp$ **[5 pts]**
   d) True and $EG\ p \Rightarrow AG\ p$ **[5 pts]**
   e) A[p1 U A[p2 U p3]] and A[[p1 U p2] U p3]. **[5 pts]**

4. Consider the command c = `while x ≠ 4 do x := x+2 od`:
   a) Give a precondition P such that c does not terminates if P is satisfied. **[5 pts]**
   b) Prove { P } c { false } using the proof system for partial correctness. **[10 pts]**
   c) Prove { x = 0 } c { true } using the proof system for total correctness. **[10 pts]**

6. The following is an algorithm for the calculation of the factorial of a non-negative integer N.

```
{ x = N ∧ N > 0}
y := 1;
while x ≠ 1 do
      y := y*x;
      x := x - 1
od
{ y = N! ∧ N > 0}
```

   a) Give an invariant for the while command implying the above postcondition. **[5 pts]**
   b) Give a proof outline for the partial correctness of the above algorithm. **[10 pts]**
   c) Give a proof that the algorithm terminates. **[10 pts]**

The final score is given by the sum of the points obtained divided by 10 (with a maximum of 10).

Proof system for partial correctness:

1. $\{ \phi \}$ skip $\{ \phi \}$

2. $\{ \phi[e/x] \}$ x:= e $\{ \phi \}$

3. $$\frac{\{ \phi \}\ c1\ \{ \varphi \} \quad \{ \varphi \}\ c2\ \{ \psi \}}{\{ \phi \}\ c1\ ;\ c2\ \{ \psi \}}$$

4. $$\frac{\{ \phi \wedge b \}\ c1\ \{ \psi \} \quad \{ \phi \wedge \neg b \}\ c2\ \{ \psi \}}{\{ \phi \}\ \underline{if}\ b\ \underline{then}\ c1\ \underline{else}\ c2\ \underline{fi}\ \{ \psi \}}$$

5. $$\frac{\{ \phi \wedge b \}\ c\ \{ \phi \}}{\{ \phi \}\ \underline{while}\ b\ \underline{do}\ c\ \underline{od}\ \{ \phi \wedge \neg b \}}$$

6. $$\frac{\phi \Rightarrow \phi 1 \quad \{ \phi 1 \}\ c\ \{ \psi 1 \} \quad \psi 1 \Rightarrow \psi}{\{ \phi \}\ c\ \{ \psi \}}$$