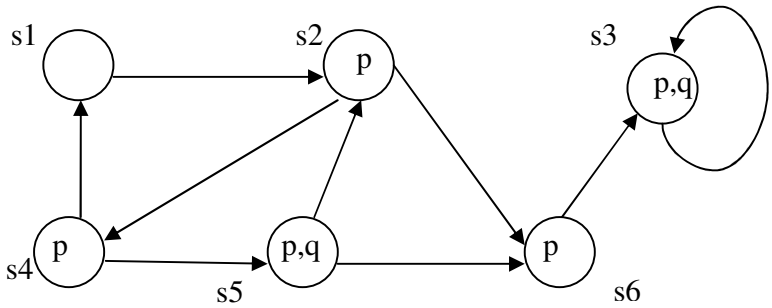
LIACS
Leiden University

Examination Program Correctness
11 June 2008, 14:00 - 17:00

---

1. **[1,5 points]** a) Prove the CTL equivalence between AG(p ∧ q) and AGp ∧ AGq.
   b) Give a CTL model with a state satisfying the CTL formula ¬EG p but not satisfying AG¬p

2. **[2 points]** Using the *labelling algorithm*, calculate the set of states of the following transition system that satisfy the CTL formula E[p U AFq]:



3. **[1,5 points]** a) Draw a Kripke structure whose initial state satisfies G(p ∨ q) but not Gp ∨ Gq.
   b) Is the LTL formula GFp equivalent to the CTL formula AGAFp? I.e., any Kripke structure satisfying GFp satisfies AGAFp and vice-versa? Justify your answer.

4. **[1 point]** Let us extend the command language with two statements. The first one, `error`, is a statement such that {false} error {ϕ} for every assertion ϕ. The second statement is `assert b`, for a Boolean expression b: if b holds in the initial state then it does nothing, otherwise it is an error. Thus `assert b` ≡ `if b then skip else error fi`. Exhibit a proof tree showing that the Hoare triple {b ∧ ϕ} `assert b` {ϕ} is valid.

5. **[2 points]** Calculate the weakest precondition of the following commands
   a) {???} a[i] := x { a[i] = 3 }
   b) {???} a[i] := x {a[1] = 3}
   c) {???} a[a[i]]:= x { a[i] = 3 }
   d) {???} a[a[i]]:= x { a[x] = 3 }
   where `a[1..5]` is an array of integers and `i` and `x` are two integer variables.

6. **[2 points]** Consider the following Hoare triple of a command computing the m-th power of n, and storing the result in the variable `x`:

```
{m ≥ 0 ∧ n > 0}
 x := 1;
 y := 0;
 while (y < m) do
       x := x * n;
       y := y + 1
 od
{x = n^m}
```

   a) Find an invariant and give a proof outline for *partial* correctness.
   b) Find a variant and give a proof outline for *total* correctness.

The final score is given by the sum of the points obtained.