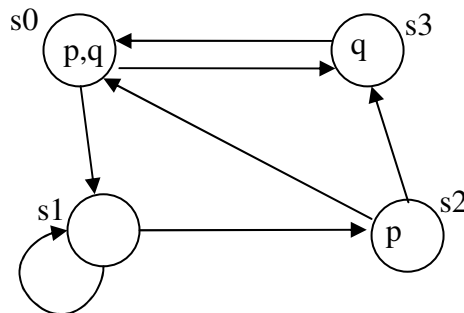


- [1 point] For each of the following four pairs of CTL formulas say if they are equivalent or find a model of one of the pair which is not a model of the other:
  - $AF(\phi \vee \psi)$  and  $AF\phi \vee AF\psi$
  - $\neg AF(\phi \vee \psi)$  and  $EF(\neg\phi \wedge \neg\psi)$
  - $true$  and  $AG\phi \rightarrow EF\phi$
  - $true$  and  $EG\phi \rightarrow AF\phi$ .
- [1,5 points] Use the labelling algorithm to give the set of all states of the following transition system satisfying the CTL formula  $AGAF(p \vee q)$ :



- [1,5 points] Prove the equivalence between the following three pairs of LTL formulas by explicitly referring to their formal semantics:
  - $\neg X\phi$  and  $X\neg\phi$
  - $\neg F\phi$  and  $G\neg\phi$
  - $G\neg\phi$  and  $\neg(true \text{ U } \phi)$ .
- [1,5 points] Let  $C$  be the command `while  $x \neq 0$  do  $x := x+1$  od`.
  - Is the *partial* correctness assertion  $\{false\} C \{true\}$  valid? Justify your answer.
  - For which preconditions  $\phi$  is the *partial* correctness assertion  $\{\phi\} C \{true\}$  valid?
  - For which preconditions  $\phi$  is the *total* correctness assertion  $\{\phi\} C \{true\}$  valid?
- [2 points] Exhibit a proof tree for the partial correctness of the following Hoare triple:

$$\{y \geq 0\} \text{ if } x > y \text{ then } x := y \text{ else if } x < 0 \text{ then } x := 0 \text{ fi fi } \{0 \leq x \leq y\}$$

- [2,5 points] Consider the following Hoare triple for a command computing the greatest common divisor  $\text{gcd}(m, n)$  of two positive integers  $m$  and  $n$ :

$$\{x \geq 1 \wedge y \geq 1 \wedge x = x_0 \wedge y = y_0\}$$

$$\text{while } (x \neq y) \text{ do}$$

$$\quad \text{if } (x < y) \text{ then}$$

$$\quad \quad y := y - x;$$

$$\quad \text{else}$$

$$\quad \quad x := x - y;$$

$$\quad \text{fi}$$

$$\text{od}$$

$$\{x = \text{gcd}(x_0, y_0)\}$$

Give a proof outline for *total* correctness. Clearly identify the *invariant* and the *variant*. Remember that  $\text{gcd}(m, n) = \text{gcd}(m, m-n)$  for positive integers  $m$  and  $n$  with  $n < m$ .