HW #5: Due May 31th 23:59 AM

1. Draw the transition system described by the ABP program.

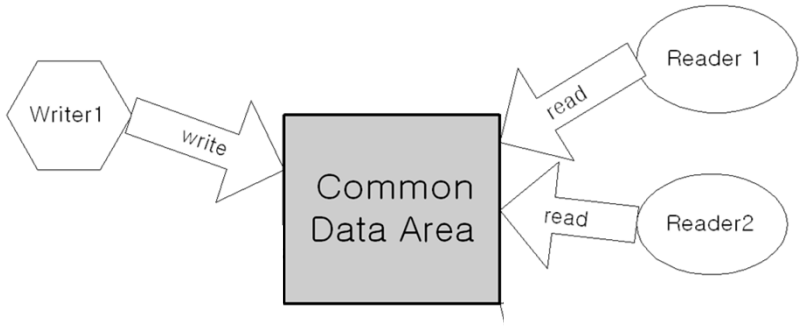
Remarks: There are 28 reachable states of the ABP program. (Looking at the program, you can see that the state is described by nine boolean variables, namely `S.st`, `S.message1`, `S.message2`, `R.st`, `R.ack`, `R.expected`, `msg_chan.output1`, `msg_chan.output2` and finally `ack_chan.output`. Therefore, there are $2^9 = 512$ states in total. However, only 28 of them can be reached from the initial state by following a finite path.)

If you abstract away from the contents of the message (e.g. by setting `S.message1` and `msg_chan.output1` to be constant 0), then there are only 12 reachable states. This is what you are asked to draw.

2. Model and verify 2 readers and 1 writer system in NuSMV

- 2-1. Design a system containing 2 readers and 1 writer that access the common data in NuSMV
- 2-2. Specify the following two properties in LTL and show that your system satisfies these properties

  - Concurrency (CON)
    - Multiple readers can read data concurrently
  - Exclusive writing (EW)
    - A writer can write into the data area at an instant with no readers



3. Prove that ϕ U $\psi \equiv \psi$ R $(\phi \vee \psi) \wedge$ F ψ

4. Prove that for all paths π of all models, $\pi \models \phi$ W $\psi \wedge$ F ψ implies $\pi \models \phi$ U ψ

5. (a) Beginning from state s_0, unwind this system into an infinite tree, and draw all computation paths up to length 4 (= the first four layers of that tree).

(b) Make the following checks $\mathcal{M}, s_0 \models \phi$, where ϕ is listed below. For that you need to explain why the check holds, or what reasons there are for its failure:

* (i) $\neg p \rightarrow r$

(ii) AF t

*(iii) $\neg$EG r

(iv) E(t U q)

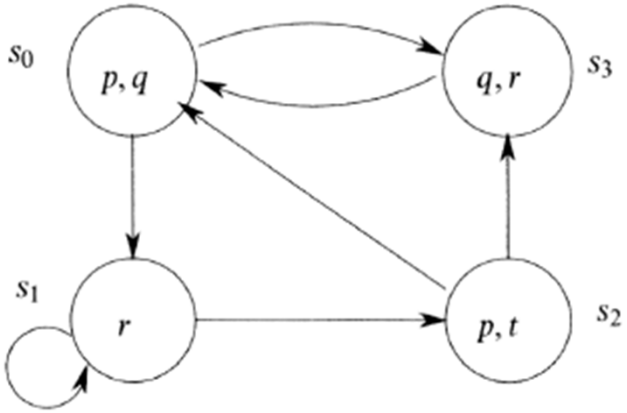
(v) AF q

(vi) EF q

(vii) EG r

(viii) AG $(r \vee q)$.

(c) Make the same checks as in (b) but now for state s_2.



6. Express the following properties in CTL and LTL whenever possible. If neither is possible, try to express the property in CTL*

   a) Whenever **p** is followed by **q** (after finitely many steps), then the system enters an 'interval' in which no r occurs until t

   b) Event **p** precedes **s** and **t** on all computation paths. (you may find it easier to code the negation of that specification first)

   c) After **p**, **q** is never true (Where this constraint is meant to apply on all computation paths)

   d) Between the events **q** and **r**, event **p** is never true.

   e) Transitions to states satisfying **p** occur at most twice.

   f) Property **p** is true for every second state along a path

7. Find a transition system which distinguishes the following pairs of CTL* formulas (i.e. show that they are *not* equivalent):

   (a) $\mathrm{AF\,G}\,p$ and $\mathrm{AF\,AG}\,p$

* (b) $\mathrm{AG\,F}\,p$ and $\mathrm{AG\,EF}\,p$

   (c) $\mathrm{A}[(p\ \mathrm{U}\ r) \vee (q\ \mathrm{U}\ r)]$ and $\mathrm{A}[(p \vee q)\ \mathrm{U}\ r)]$

* (d) $\mathrm{A}[X\,p \vee \mathrm{XX}\,p]$ and $\mathrm{AX}\,p \vee \mathrm{AX\,AX}\,p$

   (e) $\mathrm{E}[\mathrm{GF}\,p]$ and $\mathrm{EG\,EF}\,p$.