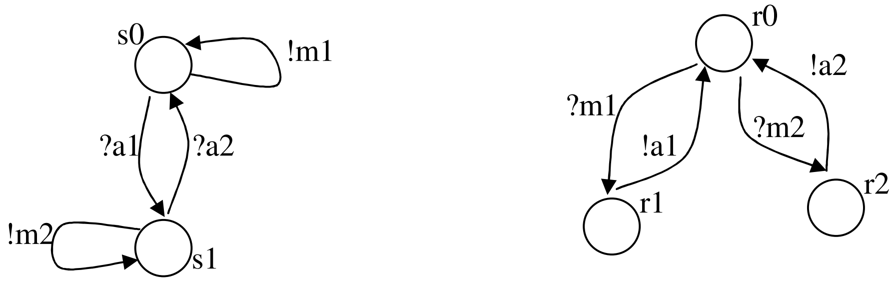
Examination Program Correctness

11 June 2002, 19:00 - 22:00

---

1. **[2 points]** a) Draw the transition system obtained by synchronising the following two transition systems with respect to the set Sync = {(!m1,?m1),(!m2,?m2),(?a1,!a1),(?a2,!a2)}



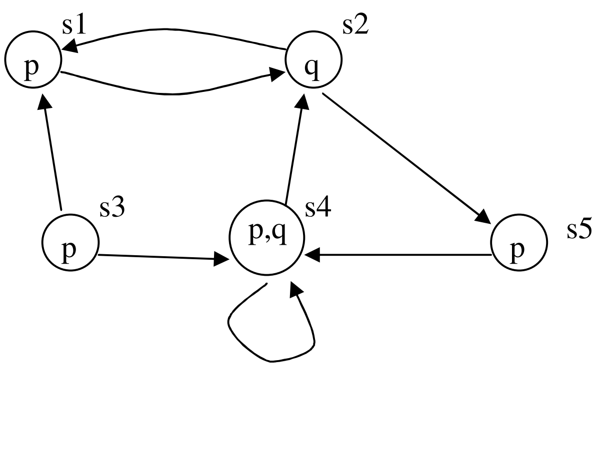
Sender Receiver

b) The transition system obtained describes the communication protocol between a sender and a receiver. The sending of messages is denoted by the actions !m1 and !m2, while the receiving of messages is denoted by the actions ?m1 and ?m2, respectively. Similarly, the sending of acknowledgements is denoted by !a1 and !a2, while their reception is denoted by ?a1 and ?a2, respectively.

Let p be the atomic proposition "m1 has been communicated" and q be the atomic proposition "m2 has been communicated". Write a CTL formula specifying that m2 will always be communicated after m1 has already been communicated.

c) If we label the state <s0,r1> of the synchronised transition system with the atomic proposition p, and the state <s1,r2> with q, which of these two states satisfy your CTL formula above.

2. **[2 points]** Using the labelling algorithm described in the course, give the set of all states of the following transition system satisfying the CTL formula E[p U AF q].



3. **[1 point]** Give a simple CTL model and a state satisfying the CTL formula $EF\neg p$ but not satisfying $\neg AF\, p$.

4. **[1 point]** Give the definition of validity of the partial correctness triple $(| \phi |)\ c\ (| \psi |)$ and of the total correctness triple $[| \phi |]\ c\ [| \psi |]$.

5. **[2 point]** The execution of the command

$$\underline{\text{repeat}}\ \{\ c\ \}\ \underline{\text{until}}\ b$$

is equivalent to c; <u>while</u> $\neg b$ { c }. Derive from the proof system for partial correctness given below a partial correctness proof rule for this repeat-until command.

6. **[3 point]** Given the following command c

```
while x ≠ y {
        if x < y then { y := y – x }
                 else { x := x – y }
        }
```

prove (using a proof outline) the validity of the following partial correctness triple

$$(| x \geq 0 \wedge y \geq 0 |)\ c\ (| x = y |)$$

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. $$\frac{(| \phi \wedge b |)\ c1\ (| \psi |) \quad (| \phi \wedge \neg b |)\ c2\ (| \psi |)}{(| \phi |)\ \underline{\text{if}}\ b\ \underline{\text{then}}\ \{ c1 \}\ \underline{\text{else}}\ \{ c2 \}\ (| \psi |)}$$

5. $$\frac{(| \phi \wedge b |)\ c\ (| \phi |)}{(| \phi |)\ \underline{\text{while}}\ b\ \underline{\text{do}}\ \{\ c\ \}\ (| \phi \wedge \neg b |)}$$

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