6 Hoare Logic and Model Checking (cp526)

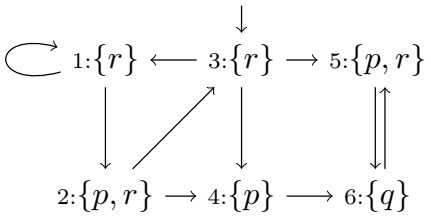
Consider the temporal logic CTL over atomic propositions $p \in \mathit{AP}$:
$\psi \in \mathsf{StateProp} ::= \bot \mid \top \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \psi_1 \to \psi_2 \mid p \mid \mathsf{A}\ \phi \mid \mathsf{E}\ \phi$,
$\phi \in \mathsf{PathProp} ::= \mathsf{X}\ \psi \mid \mathsf{F}\ \psi \mid \mathsf{G}\ \psi \mid \psi_1\ \mathsf{U}\ \psi_2$

(*a*) Specify the following properties as CTL formulae over $\mathit{AP} = \{p, q\}$.

(*i*) If a state satisfying p can be reached, then there is a path along which q holds until p does. [2 marks]

(*ii*) All next states have a path that traverses only states from where q cannot be reached. [3 marks]

(*b*) Consider a temporal model M over atomic propositions $\mathit{AP} = \{p, q, r\}$ with states 1, ..., 6, initial state 3 and transitions and state labelling as shown in the diagram (for example, in state 5, atomic propositions p and r hold).

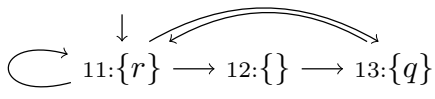


Informally describe the meaning of each of the following CTL formulae over AP and explain whether or not they hold in the model.

(*i*) $\mathsf{AG}((\mathsf{EX}p) \to (\mathsf{AF}p))$ [3 marks]

(*ii*) $\mathsf{E}(r\mathsf{U}(\mathsf{AX}(q \wedge \mathsf{AX}r)))$ [3 marks]

(*c*) Let M be the model from (*b*) over atomic propositions $\mathit{AP} = \{p, q, r\}$ and M' the temporal model over atomic propositions $\mathit{AP}' = \{q, r\}$ with states 11, 12, and 13, initial state 11, and transitions and labelling as shown below. Prove that M' simulates M, explaining your steps.



[6 marks]

(*d*) Consider CTL* formula $\psi_1 = \mathsf{A}(\mathsf{G}p \vee \mathsf{F}q)$ and CTL formula $\psi_2 = \mathsf{AG}(p \vee \mathsf{AF}q)$, both over atomic propositions $\mathit{AP} = \{p, q\}$. Formally define a temporal model over AP that shows that ψ_1 and ψ_2 are not equivalent. Explain why your temporal model satisfies one of the formulae but not the other. [3 marks]