6 Hoare Logic and Model Checking (cp526)

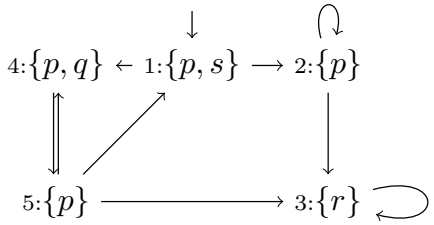
Consider the temporal logic CTL over atomic propositions $p \in \mathit{AP}$:
$\psi \in \mathsf{StateProp} ::= \bot \mid \top \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \psi_1 \rightarrow \psi_2 \mid p \mid \mathsf{A}\ \phi \mid \mathsf{E}\ \phi$,
$\phi \in \mathsf{PathProp}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

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

(*i*) If a state satisfying p cannot be reached, then q always holds. [3 marks]

(*ii*) From all reachable states, there is some path along which p holds, until it reaches a state from which no possible next state satisfies q. [3 marks]

(*b*) Consider a temporal model M over atomic propositions $\mathit{AP} = \{p, q, r, s\}$, with states $\{1, 2, 3, 4, 5\}$, initial state 1, and transitions and state labelling as shown in the diagram (e.g. in state 1, atomic propositions p and s 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*) $\mathsf{A}((q \wedge s)\mathsf{U}(\mathsf{EF}r))$ [2 marks]

(*ii*) $\mathsf{EG}(p \wedge \mathsf{AX}p)$ [3 marks]

(*c*) (*i*) Informally explain the difference in the properties that can be expressed by LTL and CTL. [3 marks]

(*ii*) Consider the LTL formula $\phi = p\mathsf{U}(\mathsf{X}q)$ and CTL formula $\psi = \mathsf{A}(p\mathsf{U}(\mathsf{AX}q))$, both over atomic propositions $\mathit{AP} = \{p, q\}$. Formally define a temporal model over AP that shows that ϕ and ψ are not equivalent. Explain why your temporal model satisfies one of the formulae but not the other. [6 marks]