6 Hoare Logic and Model Checking (cp526)

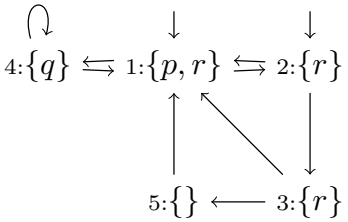
Consider the temporal logic CTL over atomic propositions $p \in \mathit{AP}$:
$\psi \in \mathsf{StateProp} ::= \bot \mid \top \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \psi_1 \rightarrow \psi_2 \mid p \mid \mathsf{A}\ \phi \mid \mathsf{E}\ \phi$,
$\phi \in \mathsf{PathProp}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

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

(*i*) There exists a path such that at some point p will always hold. [2 marks]

(*ii*) There exists a path such that at some point q holds, and from any state along the path until then, a state satisfying p can be reached. [3 marks]

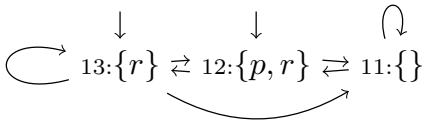
(*b*) Consider a temporal model M over atomic propositions $\mathit{AP} = \{p, q, r\}$, with states $\{1, 2, 3, 4, 5\}$, initial states 1 and 2, and transitions and state labelling as shown in the diagram (e.g. in state 1, atomic propositions p and r hold). Informally describe the meaning of each of the following CTL formulae over AP and explain why they hold in the model or give a counterexample if they do not.



(*i*) $\mathsf{A}(r\ \mathsf{U}\ (\mathsf{EX}q))$ [2 marks]

(*ii*) $(\mathsf{AF}p) \wedge (\mathsf{AGEF}q)$ [3 marks]

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



(*i*) Show that M' simulates M: define a relation R and show $M \preccurlyeq^R M'$. [6 marks]

(*ii*) Is your relation R a bi-simulation? Explain why or why not. [4 marks]