COMPUTER SCIENCE TRIPOS Part II – 2026 – Paper 9

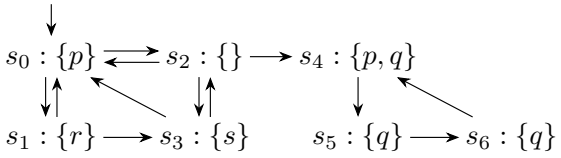
7 Hoare Logic and Model Checking (rb2018+hk590)

This question uses the following syntax for CTL:

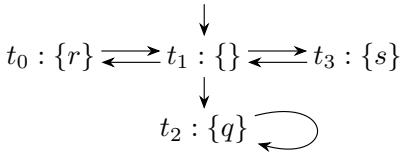
$$\psi \in \textbf{StateProp} ::= \bot \mid \top \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \psi_1 \to \psi_2 \mid p \mid A\,\phi \mid E\,\phi$$
$$\phi \in \textbf{PathProp} ::= X\,\psi \mid F\,\psi \mid G\,\psi \mid \psi_1\,U\,\psi_2.$$

(*a*) Consider CTL formulae over $\mathsf{AP} = \{\, p \,\}$. A student writes down the formula $AF\,AX\,p$, intending to express the property that "p holds at some future state *strictly after* the current state". However, it actually specifies a different property. Explain why the formula doesn't match the intention, using a concrete temporal model, and specify the correct CTL formula. [5 marks]

(*b*) Consider a temporal model M over atomic propositions $\mathsf{AP} = \{\, p, q, r, s \,\}$, with states $S = \{\, s_0, s_1, s_2, s_3, s_4, s_5, s_6 \,\}$, initial state s_0, transitions and state labelling as shown in the diagram below on the left. For example, the diagram indicates that in state s_0 the atomic proposition p holds. Describe the meaning of CTL formula $AG\,(EF\,s \to (EX\,EX\,p))$, and explain whether it holds in M. [4 marks]



Temporal model M



Temporal model M'

(*c*) Consider now the right side of the figure, which shows a temporal model M'.

(*i*) Show that M' does not simulate M. [2 marks]

(*ii*) Make M' simulate M by adding as few transitions as possible. State the transitions you add, specify a simulation relation, and show that the modified M' simulates M. [4 marks]

(*d*) CTL formula φ and LTL formula Ψ, over the same atomic propositions, are equivalent if, for every temporal model M, $M \models \varphi$ if and only if $M \models \Psi$. Prove that there is no LTL formula equivalent to $AF(q \wedge AX\,p)$. Hint: in 1988, Clarke and Draghicescu showed the following fact, which you may find useful:

> Let φ be a CTL formula and Ψ be an LTL formula that is obtained by eliminating all the path quantifiers in φ; for example, $AF\,EX\,p$ becomes $F\,X\,p$ by eliminating the path quantifiers. There then exists an LTL formula equivalent to φ if and only if φ is equivalent to Ψ.

[5 marks]