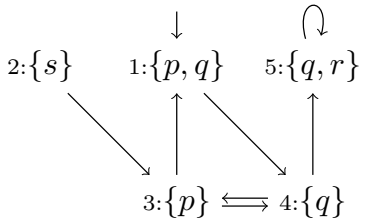
COMPUTER SCIENCE TRIPOS Part II – 2022 – Paper 9

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) Consider a temporal model 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 q 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 counter-example if they do not.



(i) $\mathsf{AG}\ (p \vee q)$ [2 marks]

(ii) $\mathsf{A}\ ((p \vee q)\ \mathsf{U}\ r)$ [3 marks]

(b) Specify the following properties as CTL formulae over AP as defined in (a).

(i) Once r holds, r always holds. [3 marks]

(ii) From every reachable state, it is always possible to reach another state from where on r always holds. [3 marks]

(c) John's car is getting old and parts can develop problems at any point. The car internally monitors its parts and reports, for each part, either no problem or a warning. When there is a warning for the engine (considered to be a single part) or for any three parts at once (John is lazy), John takes the car to the garage where all problems are fixed.

(i) Describe a temporal model M_1 of the car's status that keeps track of exactly which parts of the car have warnings. Assume initially there are no warnings/problems, and assume that each new state has at most one additional problem compared to the previous state. Use Parts as the set of parts of the car. Moreover, use $\mathit{AP} = \{\mathsf{needsRepair}\}$ as the set of atomic propositions, where $\mathsf{needsRepair}$ should hold in any state where any part has a warning. [4 marks]

(ii) Create a more abstract model M' over AP that only tracks the information John cares about, and give a simulation of M by M' (no proof needed).

[5 marks]