6 Hoare Logic and Model Checking (cp526)

Consider the temporal logic CTL over atomic propositions \( p \in AP \):
\[
\psi \in \text{StateProp} ::= \bot \mid \top | \neg \psi | \psi_1 \land \psi_2 | \psi_1 \lor \psi_2 | \psi_1 \rightarrow \psi_2 | p | A \phi | E \phi,
\phi \in \text{PathProp} ::= X \psi | F \psi | G \psi | \psi_1 U \psi_2
\]

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

(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 \( AP = \{p, q, r, s\} \), 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) \( A((q \land s) U (EFr)) \) [2 marks]

(ii) \( EG(p \land AXp) \) [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 \( \phi = p U (Xq) \) and CTL formula \( \psi = A(p U (AXq)) \), both over atomic propositions \( AP = \{p, q\} \). Formally define a temporal model over \( AP \) that shows that \( \phi \) and \( \psi \) are not equivalent. Explain why your temporal model satisfies one of the formulae but not the other. [6 marks]