6 Hoare Logic and Model Checking (cp526)

Consider the temporal logic CTL over atomic propositions $p \in AP$:

\[
\psi \in \text{StateProp} ::= \bot \mid \top \mid \neg \psi \mid \psi_1 \land \psi_2 \mid \psi_1 \lor \psi_2 \mid \psi_1 \rightarrow \psi_2 \mid p \mid A \phi \mid E \phi,
\]

\[
\phi \in \text{PathProp} ::= X\psi \mid F\psi \mid G\psi \mid \psi_1 U \psi_2
\]

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

(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 $AP = \{p, q, r\}$, 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.

1: $\{p, r\}$

2: $\{r\}$

3: $\{r\}$

4: $\{q\}$

5: $\{\}$

(i) $A(r U (EXq))$ [2 marks]

(ii) $(AFp) \land (AGEFq)$ [3 marks]

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

13: $\{r\}$

12: $\{p, r\}$

11: $\{\}$

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

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