COMPUTER SCIENCE TRIPOS Part II – 2021 – Paper 9

8 Hoare Logic and Model Checking (jp622)

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

(a) Alice (a), Bob (b), and Carol (c) are bank tellers. They sit at their till (t), until they need to give money to their customers, which they can do in gold (g) or silver (s) coins, which are stored in two different vaults. Each vault needs two tellers to turn keys simultaneously, but if it determines that there are more than two tellers present, it locks itself and phones the police. Once they have retrieved the coins, they can return with coin (r). This yields atomic propositions $AP = \mathit{Pers} \times \mathit{Loc}$, where $\mathit{Pers} ::= \mathsf{a} \mid \mathsf{b} \mid \mathsf{c}$ and $\mathit{Loc} ::= \mathsf{t} \mid \mathsf{g} \mid \mathsf{s} \mid \mathsf{r}$, so that for example a state labelled with $\{\mathsf{at}, \mathsf{bs}, \mathsf{cr}\}$ is one where Alice is at her desk, Bob is waiting to open the silver vault, and Carol is returning with coin.
Give CTL formulas for

(i) Alice repeatedly serves clients with coins. [2 marks]

(ii) When Bob picks a vault, he stays there until it gets opened. [2 marks]

(iii) Carol is always able to serve clients with coins. [2 marks]

(iv) The vaults never lock. [2 marks]

(b) Explain why Carol's property cannot be expressed in LTL. [2 marks]

(c) A chemist is trying to determine what can be synthesised from the chemicals they have. They know all possible reactions: $2\ H_2 + O_2 \rightarrow 2\ H_2O$, $C + O_2 \rightarrow CO_2$, etc.

(i) Describe a model of reactions from given starting quantities. [3 marks]

(ii) Keeping track of the exact amount of chemicals is challenging, so the chemist looks only at whether each is present. Describe such an abstract model, and give a simulation relation between the two models. [4 marks]

(iii) State, for each of these two properties, which of the models (i) and (ii) is such that if the property holds for it, then it holds for the other:
1/ that dangerous chemicals like CO are never synthesised;
2/ that desirable chemicals like pure gold (Au) can be synthesised.
Explain why. [3 marks]