8 Hoare Logic and Model Checking (caw77)

This question is about modelling a program, defined below, consisting of two threads and a single (mathematical) integer variable $X$, initially set to 0. Each thread $t$ has its own program counter given by $pc_t$, initially set to 0, which describes the current line for that thread.

<table>
<thead>
<tr>
<th>Thread 1</th>
<th>Thread 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: $X := X+1$</td>
<td>0: IF IS_ODD($X$) THEN STOP_ALL</td>
</tr>
<tr>
<td>1: GOTO 0</td>
<td>1: GOTO 0</td>
</tr>
</tbody>
</table>

The program is executed by repeatedly carrying out execution steps, where one thread is non-deterministically selected, its entire current line is run, and its program counter is then updated appropriately. This continues until STOP_ALL is executed, which immediately terminates the whole program.

(a) The program state can be described by $(pc_1, pc_2, X, stopped)$, where $pc_1$, $pc_2$, and $X$ are mathematical integers, and $stopped$ is a boolean which is true iff STOP_ALL has been executed. Let $S$ be the set of all such states.

(i) Define $S_0$, the set of initial states of the program, such that $S_0 \subseteq S$. [1 mark]

(ii) Define a transition relation $R \subseteq S \times S$ describing the program’s execution. [2 marks]

(iii) Define a labelling function $L$ that labels all states where the program has terminated with the atomic property $\text{term}$. [2 marks]

(b) Explain why, taking the definitions from (a), the model $M_a = (S, S_0, R, L)$ is not a (finite) Kripke structure. [2 marks]

(c) Draw the finite state automaton for a model $M_b$ which is a Kripke structure, such that $M_a$ and $M_b$ are bisimilar. Justify your answer briefly. [5 marks]

[Note: A full formal proof of bisimilarity is not required.]

(d) (i) Give an LTL formula $\phi$ such that the judgement $M_b \models \phi$ corresponds to the statement “every execution of the program will eventually terminate”. [2 marks]

(ii) Either prove that $M_b \models \phi$ holds, or describe a counter-example trace. [2 marks]

(e) Consider the CTL formula $\psi = \text{AG(EF term)}$. Determine whether this is equivalent to your definition of $\phi$ from Part (d). $\phi$ and $\psi$ are equivalent iff, for all Kripke structures $M$, $(M \models \phi)$ iff $(M \models \psi)$. Justify your answer. [4 marks]