Specification and Verification II 2004 – Paper 9 Question 13 (MJCG)

(*a*) Model checking is used to automatically verify that properties hold of designs. It should be used when the design is small and the property to be verified can be expressed in temporal logic (i.e. when model checking algorithms will work). Theorem proving is needed when the property to be proved cannot be expressed in temporal logic, or if the design is too large for model checkers to handle (e.g. to avoid a state explosion).

An example of an application of model checking would be to show that a small set of registers is 'one hot'. For three registers r_1, r_2 and r_3 this can be expressed as a formula: $\texttt{always}(r_1 \wedge \neg r_2 \wedge \neg r_3 \ \vee\ \neg r_1 \wedge r_2 \wedge \neg r_3 \ \vee\ \neg r_1 \wedge \neg r_2 \wedge r_3)$.

An example where theorem proving would be appropriate would be to show that a floating point device implements the IEEE standard.

(*b*) First a specification in higher order logic is given, then one in the PSL/Sugar version of linear temporal logic (i.e. the PSL Foundation Language).

(*i*) $\mathrm{HOL}_{(i)}$: $\forall t.\ \exists i.\ i \leq 4 \wedge \phi i(t) \wedge \forall j.\ j \leq 4 \wedge j \neq i \Rightarrow \neg \phi j(t)$

$$\begin{aligned}\mathrm{PSL}_{(i)}\text{: } \texttt{always}\ & \phi1 \wedge \neg\phi2 \wedge \neg\phi3 \ \wedge \neg\phi4 \ \vee \\ & \neg\phi1 \wedge \phi2 \wedge \neg\phi3 \ \wedge \neg\phi4 \ \vee \\ & \neg\phi1 \wedge \neg\phi2 \wedge \phi3 \ \wedge \neg\phi4 \ \vee \\ & \neg\phi1 \wedge \neg\phi2 \wedge \neg\phi3 \ \wedge \phi4 \ \vee\end{aligned}$$

(*ii*) $\mathrm{HOL}_{(ii)}$: $\forall t.\ \forall i.\ i \leq 4 \wedge \phi i(t) \Rightarrow \phi(\texttt{if}\ i < 4\ \texttt{then}\ i{+}1\ \texttt{else}\ 1)(t{+}1)$

$$\begin{aligned}\mathrm{PSL}_{(ii)}\text{: } \texttt{always}\ & (\phi1 \rightarrow \texttt{next!}\ \phi2) \ \wedge \\ & (\phi2 \rightarrow \texttt{next!}\ \phi3) \ \wedge \\ & (\phi3 \rightarrow \texttt{next!}\ \phi4) \ \wedge \\ & (\phi4 \rightarrow \texttt{next!}\ \phi1)\end{aligned}$$

(*iii*) $\mathrm{HOL}_{(iii)}$: $\mathrm{HOL}_{(i)} \wedge \mathrm{HOL}_{(ii)} \Rightarrow \forall t.\ \phi1(t) \Rightarrow (\texttt{out}(t{+}3) = \texttt{in}(t{+}1))$

$\mathrm{PSL}_{(iii)}$: $\mathrm{PSL}_{(i)} \wedge \mathrm{PSL}_{(ii)} \rightarrow \texttt{always}\ \phi1 \rightarrow (\texttt{next!}[3]\texttt{out} \leftrightarrow \texttt{next!in})$

This question refers both to the parts of the course on modelling using higher order logic and the parts on model checking. Part (*a*) of the question asks for a general comparison of theorem proving and model checking. Part (*b*) uses an example that was given in the lectures, though only in the context of theorem proving, so the model checking angle will require a little thought.

For Part (*a*) I will give 4 marks for evidence that the candidates understands when model checking and theorem proving should be used, and 4 marks for good examples (which don't need to be the ones in the model answer).

For Part (*b*) I will give 4 marks for each of the three parts, 2 marks for the higher order logic and 2 marks for the temporal logic (in each case a flawed attempt that shows some understanding would get some marks).