2010 Paper 9 Question 13

Specification and Verification II

REG is a unit-delay register initialising to some unknown value, the combinational devices TEST and STEP compute the functions test (which returns a Boolean) and step, respectively, and MUX is a multiplexer. These are specified by:

$$\begin{array}{ll} \mathsf{REG}(in,\ out) & = \forall t.\ out(t{+}1)\ =\ in\ t \\ \mathsf{TEST}(in,\ out) & = \forall t.\ out\ t\ =\ \mathsf{test}(in\ t) \\ \mathsf{STEP}(in,\ out) & = \forall t.\ out\ t\ =\ \mathsf{step}(in\ t) \\ \mathsf{MUX}(select,\ in_1,\ in_2,\ out) & = \forall t.\ out\ t\ =\ \texttt{if}\ select\ t\ \texttt{then}\ in_1\ t\ \texttt{else}\ in_2\ t \end{array}$$

These components can be used to design a device, INIT, that attempts to initialise to an output value satisfying test by applying step zero or more times to the initial value of REG (i.e. the value output at time 0) until test yields T. INIT indicates that initialisation has succeeded by outputting T on the output line *done*; it simultaneously outputs the value found by repeatedly applying step on the output line *out*. Formally, INIT is specified by two properties:

$$\begin{array}{l} \mathsf{INIT}(done, out)\ \Rightarrow\ \forall t.\ done\ t\ =\ \mathsf{test}(out\ t) \\ \mathsf{INIT}(done, out)\ \Rightarrow\ \forall t.\ out(t{+}1)\ =\ \ \texttt{if}\ done\ t\ \texttt{then}\ out\ t\ \texttt{else}\ step(out\ t) \end{array}$$

(*a*) Give a design for INIT in the form of a circuit diagram using REG, TEST, STEP and MUX. [6 marks]

(*b*) Carefully explain why your design meets its specification. [4 marks]

(*c*) Write down a formal model of your design. [4 marks]

(*d*) Outline how you could prove that your design meets its specification (you need not give a detailed proof, but you should provide evidence that you know how to produce such a proof, and what the main steps would be). [6 marks]