T-79.186 **Spring 2003**
Reactive Systems
Home Exercise 5
Deadline 25.2-2003 8:45

Return your answer by email (Postscript or PDF) to Timo Latvala at Timo.Latvala@hut.fi, or on paper to the lecture. All rounds will be 6 points maximum. Please remember to include your name and student number to your answer.

1.) Which ones of the following properties are safety properties? (See book Bérard et al., Chapter 7, p. 83–89). Give also a short argument in each case why your answer is correct.

   a) If in the initial state of the system a request arrives, it will be eventually acknowledged.
   b) In all states of the system it holds that an acknowledgement only arrives after a request has has been sent before.
   c) Whenever a request input becomes high, it stays high until an acknowledgement input becomes high.
   d) In all states of the system it holds that request stays high if the acknowledgement never becomes high.
   e) In all states of the system a request is followed in five time units by an acknowledgement.

2.) In the book (Bérard et al., Chapter 7.4, p. 87–89) the history variables method is described. The basic idea is to introduce a new Boolean variable h_i for each (past) temporal subformula, and initialize all of them to `false` in the initial state. After this the verification model is changed to record the changes to these history variables according to "rules" following the semantics of past temporal operators.

   Let $h_i{}'$ denote the value of the temporal subformula variable h_i in the previous time step, f_1, f_2 the values of variables corresponding to subformulas at the current time step, and finally $f_1{}', f_2'$ the values of variables corresponding to subformulas at the previous time step.

   Now the update rule for the formula $h = \mathbf{X}^{-1} f_1$ (based on) is:

   – $h_i := f_1{}'$.

   Give the update rules for all the other formula types:

   a) $h_i = p$, for $p \in AP$ (atomic propositions),
   b) $h_i = \neg f_1$,
   c) $h_i = f_1 \vee f_2$,
   d) $h_i = \mathbf{G}^{-1} f_1$, and
   e) $h_i = f_1 \mathbf{S} f_2$.

3.) Consider the automaton of Figure 7.1 of the book (Bérard et al., p. 87). Add history variables to the model to model check temporal formulas containing past time temporal operators by using a standard CTL model checker. (Use the translation scheme of the previous exercise (2.) above on this concrete case.) Also give the CTL formulas to model check in the following two cases:

   a) $\mathbf{AG}(\mathbf{X}^{-1}\texttt{alarm} \Rightarrow \mathbf{F}^{-1}\texttt{crash})$
   b) $\mathbf{AG}(\mathbf{F}^{-1}\texttt{alarm} \Rightarrow ((\texttt{crash} \vee \texttt{alarm})\mathbf{S}(\mathbf{X}^{-1}\texttt{ok})))$

   Give the models with history variables added in expressions in similar style to Fig. 7.2, or notation similar to that of the exercise (2.) above, if the notation given in the book proves to be insufficient for the task.