T-79.186 **Spring 2004**
Reactive Systems
Home Exercise 5
Deadline 31.3 16.15

Return your answers by email (Postscript or PDF) to Timo.Latvala@hut.fi, or on paper to the lecture. Remember to include your name *and* student number.

1.) Which of the properties specified below are safety properties (see Bérard et al: Chapter 7, p. 83–89)? Remember to motivate your answer.

   (a) If a request arrives in the initial state of the system, it will be answered.

   (b) In all states of the system, an acknowledgement arrives only after a request 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, a request stays high if the acknowledgement never becomes high.

   (e) In all states of the system, a request is followed by an acknowledgement in five time units.

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 them to **false** in the initial state. The model is instrumented to record changes in the truth of the past temporal subformulas 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.

   With this notation the update rule for the formula $h = \mathbf{X}^{-1} f_1$ becomes:
   $h_i := f'_1$. Give the update rules for all the other formula types:

   (a) $h_i = p$ for $p \in AP$,

   (b) $h_i = \neg f_1$,

   (c) $h_i = f_1 \vee f_2$,

   (d) $h_i = \mathbf{G}^{-1} f_1$, and

   (e) $f_1 \,\mathbf{S}\, f_2$.

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 a temporal formula containing past time temporal operators by using a standard CTL model checker. Also give the CTL formulas to model check in the following two cases.

(a) $\mathbf{AG}(\mathbf{X}^{-1} alarm \Rightarrow \mathbf{F}^{-1} crash)$

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

Give the models with history variables added in the expressions in similar style to Figure 7.2, or notation similar to that of the exercise above.