Reactive Systems Verification
alias
Model Checking I

Assignment 1

Luca Tesei

Academic Year 2015/16

Instructions

Reply to all questions justifying your answers as clearly as possible. Send an electronic (also handwritten and scanned, but readable) version to

`luca <dot> tesei <at> unicam <dot> it`

by

Friday 29th April 2016 23.59

Exercise 1

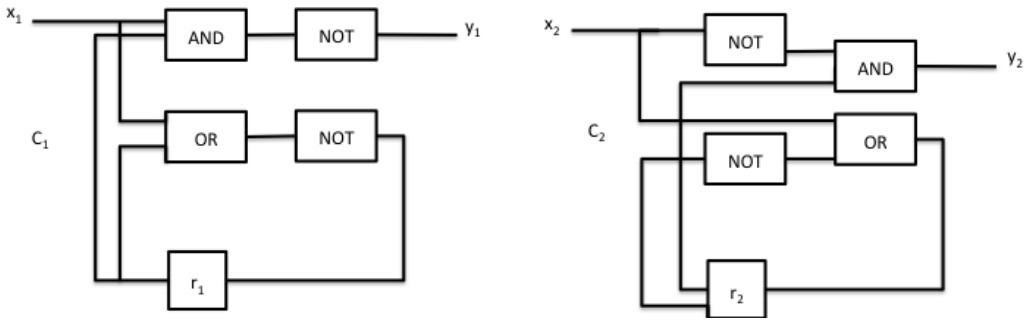
The following three processes describe the actions that students undertake.

- The PLAY process can go to pub, or go to clubbing or go to football and then it goes back to the process PLAY.
- The WORK process can go to lectures or laboratory or library or assessment and then it goes back to the process WORK.
- The DAY process makes the following actions in the specified order: wake, eat, dress, undress, sleep and then it goes back to the DAY process.

1. Draw three Transition Systems describing the behaviour of each process independently from the others. Use meaningful action names (e.g. `go_to_pub`). Show that the pure interleaving parallel composition of the three TS allows a student to go to lectures undressed.
2. Modify the three TS, introducing a set `Syn` of shared actions for hand-shacking synchronization, so that the parallel composition with synchronization of the three new TS does not produce silly action sequences, e.g. going to lectures undressed or performing PLAY actions before WORK actions are completed.

Exercise 2

Consider the following two hardware circuits.



1. Draw the two transitions systems T_1 and T_2 describing the behaviour of circuits C_1 and C_2 considering $AP = \{y_1, y_2\}$.
2. Draw the synchronous product $T_1 \otimes T_2$.
3. Determine if $T_1 \otimes T_2 \models E$ where

$$E = \{A_0 A_1 A_2 \cdots \in (2^{AP})^\omega \mid \exists i \in \mathbb{N} \colon \forall j \geq i \ \{y_1, y_2\} \notin A_j\}$$

Exercise 3

Consider a channel system $[\texttt{Controller} \mid \texttt{Monitor}_1 \mid \texttt{Monitor}_2]$ with two variables $\texttt{x} \in \{0, 1, 2\}$ and $\texttt{y} \in \{0, 1\}$ and two channels $\texttt{m}_1$ and $\texttt{m}_2$ both of capacity 0. For simplicity we will suppose that $\texttt{m}_1$ and $\texttt{m}_2$ are pure synchronization channels, i.e. no value is exchanged during the synchronization. Perform the following tasks:

1. Using the graphical formalism of channel systems, model the `Controller` process. It initializes the two variables (in any possible way), then activates the processes $\texttt{Monitor}_1$ (through channel $\texttt{m}_1$) and $\texttt{Monitor}_2$ (through channel $\texttt{m}_2$) and then terminates.
2. Model the process $\texttt{Monitor}_1$. It initially waits for activation through the channel $\texttt{m}_1$ and then starts monitoring the value of the variables. In this state, if the condition $\texttt{x} < 2$ is true then it performs action a_1 and returns back to the monitor state. Otherwise, if the condition $\texttt{x} == 2$ is true then it performs action e_1 and terminates. The effect of action a_1 must be the execution of the command $\texttt{atomic}\{\texttt{x} := \texttt{x} + 1; \texttt{y} := (\texttt{y} + 1)\%2\}$ and the effect of action e_1 is `skip`, i.e. the empty command.
3. Model the process $\texttt{Monitor}_2$. It initially waits for activation through the channel $\texttt{m}_2$ and then starts monitoring the value of the variables. In this state, if the condition $\texttt{y} == 1 \ \texttt{and} \ \texttt{x} > 0$ is true then it performs action a_2 and returns back to the monitor state. Otherwise, if the condition $\texttt{y} == 0 \ \texttt{or} \ \texttt{x} == 0$ is true then it performs action e_2 and terminates. The effect of action a_1 must be the execution of the command $\texttt{atomic}\{\texttt{y} := 0; \texttt{x} := \texttt{x} - 1\}$ and the effect of action e_2 is `skip`, i.e. the empty command.
4. Derive and draw (for the sake of clarity, possibly in different parts) the full transition system associated to the channel system $[\texttt{Controller} \mid \texttt{Monitor}_1 \mid \texttt{Monitor}_2]$ where the initial condition is $g_0 \equiv \texttt{x} == 0 \ \texttt{and} \ \texttt{y} == 0$. Assume that $AP = \{\}$ and that the labelling function is empty as well.
5. Determine, justifying your answers!, whether or not the obtained transition system satisfies the following properties:
   - *Termination*: for any initial assignment of the variables a state in which all three processes are terminated is always reached.

- *Confluence*: for any initial assignment of the variables there is only a possible terminal state, i.e. there are no different possible outcomes as effects of the actions of the monitors.
- *Weak Termination*: there exists an assignment of the variables for which a state in which all three processes are terminated is reached.
- *Weak Confluence*: there exists an assignment of the variables for which one and only one state in which all three processes are terminated is reached[1].

Exercise 4

Let $AP = \{A, B, C, D\}$ be a set of atomic propositions. Consider the following informally stated linear time properties:

(a) Whenever A holds then, at the same time, B holds and C does not hold

(b) A and D hold together at least once

(c) A and D hold together at least twice

(d) A and D hold together infinitely many times

(e) Whenever B holds then C holds after some steps

(f) Always B or C hold

(g) Eventually C holds

(h) If A and C hold together once then eventually B holds continuously for infinitely many times

(i) C holds at least once and only finitely many times

(j) If A holds infinitely many times then C must hold only finitely many times

(k) Whenever B holds then after two steps C holds

(l) Whenever C holds then it continues to hold until D holds

For each property above:

1. formalize it as a set of infinite traces on the alphabet 2^{AP} (use set expressions and first order logic)
2. determine whether it is a safety, liveness or mixed (safety and liveness) linear time property. Justify your answers!

[1] Note that the two weak properties are not linear time properties.