ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

D. Basin and P. Müller

Formal Methods and Functional Programming

Exercise Sheet 13: Model Checking and Repetition

Submission deadline: N/A

Assignment 1

Consider a lift system that services $N > 0$ floors, numbered 0 through $N - 1$. There is a door at each floor with a call button and an indicator light that signals whether or not the lift has been called. In the lift cabin, there are N send buttons (one for each floor) and N indicator lights that inform to which floor(s) the cabin is sent.

Specify the following properties of the lift system in LTL. Which of them are safety/liveness properties?

(a) A door is never open if the cabin is not present at that floor.

(b) If no indicator light is on and the cabin is on the ith floor, the cabin will wait on that floor until a button is pushed.

(c) If the call button on the ith floor is pushed, then the indicator light is turned on and the cabin will eventually stop at that floor and the door will open.

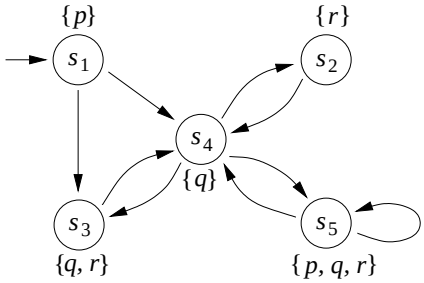
(d) When the call button on the top floor is pressed, the lift serves it immediately and does not stop on the way there.

Only use the following atomic propositions:

go_up	The cabin is going up.
go_down	The cabin is going down.
at_i	The cabin is at the ith floor.
$open_i$	The door at floor i is open.
$call_i$	Someone pressed the call button on the ith floor.
$send_i$	Someone pressed the send button in the lift for floor i.
$light\_floor_i$	The indicator light on floor i is on.
$light\_cabin_i$	The indicator light for serving the floor i in the cabin is on.

Assignment 2

Consider the transition system T over the set of atomic propositions $P = \{p, q, r\}$:



That is, T is the transition system $(\Gamma, s_1, \rightarrow, L)$ with $\Gamma = \{s_1, s_2, s_3, s_4, s_5\}$,

$$\rightarrow = \big\{(s_1, s_3), (s_1, s_4), (s_2, s_4), (s_3, s_4), (s_4, s_2), (s_4, s_3), (s_4, s_5), (s_5, s_4), (s_5, s_5)\big\},$$

and $L(s_1) = \{p\}$, $L(s_2) = \{r\}$, $L(s_3) = \{q\}$, $L(s_4) = \{q, r\}$ and $L(s_5) = \{p, q, r\}$.

Which of the following LTL formulas are satisfied in T, i.e., $T \models \varphi_i$? Justify your answer. If $T \not\models \varphi_i$, provide a trace t of T such that $t \not\models \varphi_i$.

$$\begin{aligned}
\varphi_1 &= \Diamond \Box r \\
\varphi_2 &= \Box \Diamond r \\
\varphi_2 &= \bigcirc \neg r \rightarrow \bigcirc \bigcirc r \\
\varphi_4 &= \Box p \\
\varphi_5 &= p \,\mathsf{U}\, \Box (q \vee r) \\
\varphi_6 &= (\bigcirc \bigcirc q) \,\mathsf{U}\, (q \vee r)
\end{aligned}$$

Assignment 3

Check whether the Promela model from the lecture of the Needham-Schroeder protocol satisfies the following properties specified as LTL formulas.

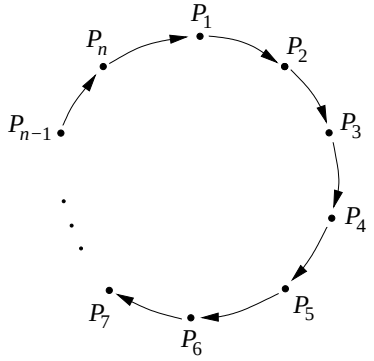
(a) $\Box\big(\texttt{statusA} = 1 \wedge \texttt{partnerA} = \texttt{agentB} \Rightarrow \texttt{knows\_nonceA} = 0\big)$

(b) $\Box\big(\texttt{statusB} = 1 \wedge \texttt{partnerB} = \texttt{agentA} \Rightarrow \texttt{knows\_nonceB} = 0\big)$

You can download the Promela model from the course webpage. Use never-claims for these checks. A never-claim is essential a Büchi automaton that represents the traces that satisfy the negated LTL formula. You can use Spin to automatically generate a never-claim from an LTL formula.

Assignment 4

Consider the following leader election protocol. For $n \geq 1$, the processes $P_1, \ldots, P_n$ are located in a ring topology, where each process is connected by an unidirectional channel to its neighbor as outlined in the figure to the right.



To distinguish the processes, each process has a unique identifier id with $1 \leq id \leq n$. The aim is to elect the process with the highest identifier as the leader within the ring. Therefore, each process executes the following algorithm:

send message id
loop
    receive message m
    if $m = id$ then stop
    if $m > id$ then send message m
end loop

(a) Model this leader election protocol for n processes in Promela.
Hint: Use an array of n channels of length 1, i.e.,

```
#define N 5  /* number of processes in the ring */
#define L 1  /* length of a channel */
chan c[N] = [L] of { byte };
```

Model a process in Promela as

```
proctype pnode(chan in, out; byte id) {
  /* algorithm for electing the leader ... */
}
```

(b) Assume that the channels are of length $n + 1$ instead of length 1 in your Promela model. Is there a state in some execution in which a channel stores more than n messages? Use Spin to verify your claim for some fixed values of n. What happens if the channels have length 0?

Assignment 5

Consider the statement s:

```
r := 0;
s := 1;
while s <= x do
  r := r + 1;
  s := s + (2*r + 1)
end
```

Show that $\vdash \{ \mathtt{x} \geq 0 \}\ s\ \{ \mathtt{r}^2 \leq \mathtt{x} \wedge \mathtt{x} < (\mathtt{r}+1)^2 \}$.