Prof. Gabriele Taentzer
Alexander Lauer

Formal Methods
Homework 4

In this homework sheet, we again use the programming language Promela and the model checking tool SPIN. Download and install the tool if you have not already done so. On the website spinroot.com you will find installation instructions for Windows, Unix/Linux and Mac systems. There are also some tutorials available for using SPIN.

1 LTL formulae

Consider the transition system shown in Figure 1 from the last tutorial. Formulate the following system properties, formulated in natural language or as LT properties, as LTL formulae, where $AP = \{scanned, stored, printed\}$.

a*) Whenever the system is in the start state, it scans in the next step.

b*) After the first step, the system never returns to the start state.

c*) $\{A_0A_1A_2... \in (2^{AP})^\omega \mid \forall j \geq 0 : (A_j \models scanned \implies \exists k \geq j : A_k \models printed)\}$

d*) $\{A_0A_1A_2... \in (2^{AP})^\omega \mid \forall j \geq 1 : \exists k \geq j : A_k \models (\neg scanned \wedge \neg stored \wedge \neg printed) \wedge \forall j \leq l < k : A_l \models (scanned \vee stored \vee printed)\}$

2 LTL formulas with Promela (10 points)

In the following, we consider a traffic light system at a 4-way intersection. For each direction of travel, the junction has one traffic light for left-turning traffic, one traffic light for traffic travelling straight ahead and right-turning traffic and one pedestrian light. The pedestrian lights change from red to green and back to red. The traffic lights change from red to red-yellow to green to yellow and back to red. In addition, the pedestrian lights each have a button with which pedestrians can signal that they want to cross the corresponding pedestrian light. The traffic lights can be switched in the same way for oncoming traffic. The traffic light system should fulfil the following properties:

- Each of the traffic lights will turn green over and over and over again.
- If a pedestrian wants to cross a pedestrian light, the corresponding light will turn green at some point.

- There are never two traffic lights or one traffic light and one pedestrian light green at the same time.

a) Model the traffic light system in Promela [5 points].

b) Formulate the above properties as LTL formulas. Use SPIN to check whether your system fulfils these properties. Attach a screenshot of the output of SPIN to your submission. [4 points]

c) Describe how your traffic light system works. [1 point]

Note: Use the commands `spin -a -run <filename>.pml` and `./pan -a -N p0` to check the LTL formula `p0`. If SPIN finds a counterexample, this can be output with the command `spin -t -p <filename>.pml`.

3 Wolf, goat and cabbage

We consider the problem of wolf, goat and cabbage. A man wants to cross a river in a boat together with a wolf, a goat and a cabbage. The boat only holds one other passenger besides the man. If the wolf and goat are alone on one bank, the wolf eats the goat. If the goat and cabbage are alone on the same bank, the goat eats the cabbage. The aim is for everyone to reach the other shore unharmed.

a*) Model the problem of wolf, goat and cabbage in Promela.

b*) Specify an LTL formula so that SPIN returns a counterexample that contains the solution to the wolf, goat and cabbage problem. Attach a screenshot of the counterexample to your solution.

4 Equivalent expressions (*)

Prove that the following equivalence holds:

$$\bigcirc(\varphi \mathbin{\mathsf{U}} \psi) \equiv (\bigcirc\varphi) \mathbin{\mathsf{U}} (\bigcirc\psi)$$

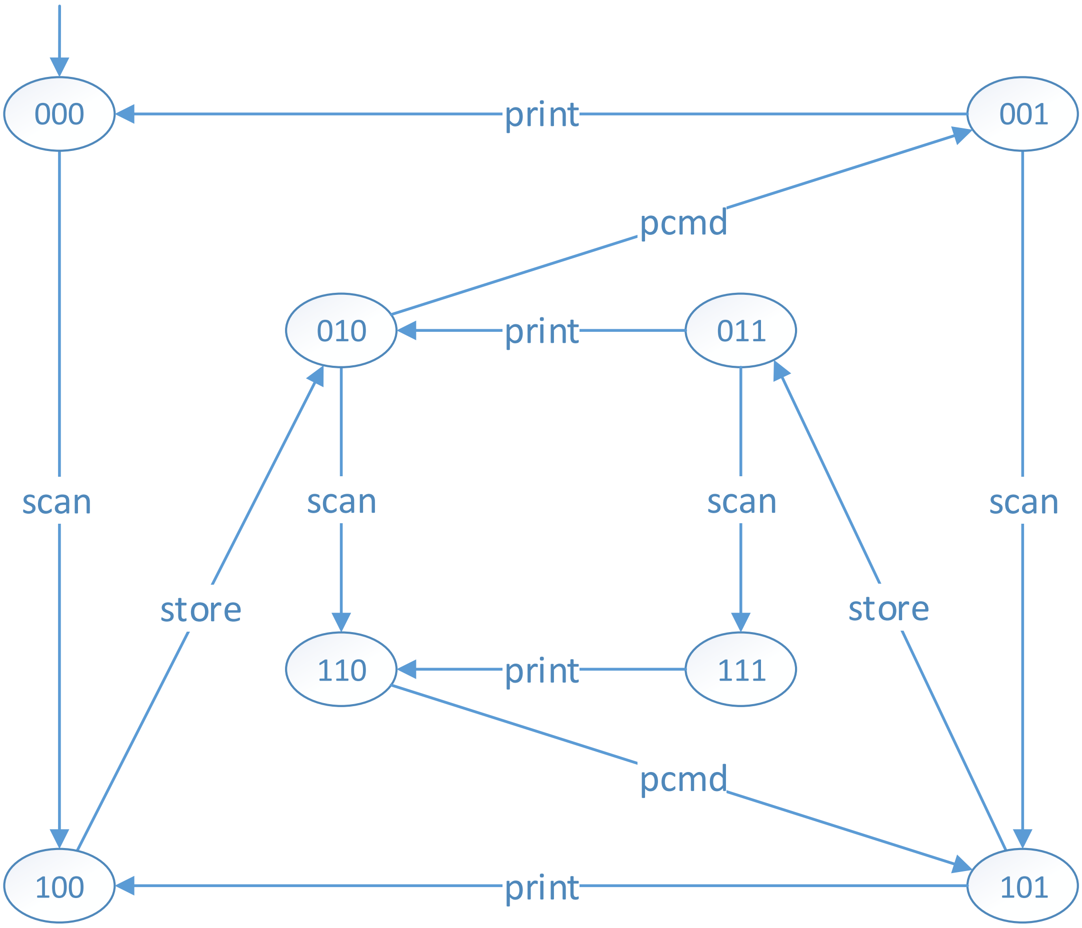

Figure 1: Transition system of the automatic pay station from the last tutorial. The state labelling encodes which of the atomic properties of the set $AP = \{scanned, stored, printed\}$ are true in the respective state. For example, in state 110 *scanned* and *stored* are true.