Technische Universität München (I7) **Summer Semester 2018**
J. Esparza / M. Blondin / P. Ashok **24.05.2018**

Model Checking – Exercise sheet 6

Exercise 6.1

Consider the Promela model below which addresses the mutual exclusion problem by using a semaphore `s`. When `s` is false, a process may enter its critical section and set `s` to true. The semaphore is reset to false when the process leaves its critical section.

```
bool s;

active [2] proctype m() {
idle:
  skip;
wait:
  atomic { (!s) -> s = true; }
cs:
  s = false;
  goto idle;
}
```

We consider the following properties:

a) Both processes cannot enter the critical section at the same time.

b) Whenever a process waits, it will eventually enter the critical section.

Follow step-by-step the outline given below to model check the properties:

(i) Construct a state transition system from the model.

(ii) Write down an atomic proposition AP and an LTL formula ϕ for each properties.

(iii) Construct a Büchi automaton $\mathcal{B}_{\neg\phi}$ for the negation of the formula ϕ.

(iv) Construct from the transition system the Kripke structure $\mathcal{K}$ and the Büchi automaton $\mathcal{B}_{\mathcal{K}}$ over AP.

(v) Construct the intersection Büchi automaton $\mathcal{B}$ for $\mathcal{B}_{\mathcal{K}}$ and $\mathcal{B}_{\neg\phi}$.

(vi) Run the emptiness algorithm in the lecture to check whether $\mathcal{L}(\mathcal{B}) = \emptyset$:

- If $\mathcal{L}(\mathcal{B}) = \emptyset$, the property holds, i.e. $\mathcal{K} \models \phi$.
- If $\mathcal{L}(\mathcal{B}) \neq \emptyset$, the property does not hold, i.e. $\mathcal{K} \not\models \phi$.
  In this case, find a counterexample run that violates the property. How to obtain a counterexample in general?

(vii) Use Spin to confirm your results.

First do step (i), and then steps (ii)-(vii) separately for each property (a) and (b). Write down all intermediary results.