Model Checking – Exercise sheet 5

Exercise 5.1
Consider the following NBA with the acceptance set \( F = \{ s_1, s_6 \} \). Apply the nested depth-first search approach to verify that \( L(A) \neq \phi \).

![NBA diagram]

Exercise 5.2
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.

```promela
1  bool s;
2
3  active [2] proctype m() {
4    idle:
5      skip;
6    wait:
7      atomic { (!s) -> s = true; }
8    cs:
9      s = false;
10    goto idle;
11  }
```

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 \( \phi \) for each properties.

(iii) Construct a Büchi automaton \( B_{\neg \phi} \) for the negation of the formula \( \phi \).

(iv) Construct from the transition system the Kripke structure \( K \) and the Büchi automaton \( B_K \) over \( AP \).

(v) Construct the intersection Büchi automaton \( B \) for \( B_K \) and \( B_{\neg \phi} \).

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

- If \( L(B) = \emptyset \), the property holds, i.e. \( K \models \phi \).
- If \( L(B) \neq \emptyset \), the property does not hold, i.e. \( K \not\models \phi \).

    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.