„Model checking“
Prof. Dr. Marcel Kyas
Assignment 2, October 27, 2011

Freie Universität Berlin

Exercise 3 (4 Points) The following incorrect mutual exclusion algorithm has been published in the January 1966 issue of the „Communication of the ACM“. The algorithm is for two processes; let $i \in \{0, 1\}$ be their identities. It uses three shared variables turn, flag[0] and flag[1]. Initially, flag[0]=0 and flag[1]=0. The initial value of turn is either 0 or 1.

```
process P[i = 0,1] {
  for (;;) {
    // Remainder
    flag[i] = 1;
    while (turn == 1 − i) {
      await flag[1−i] == 0;
      turn = i;
    }
    // Critical section
    flag[i] = 0;
  }
}
```

1. Formalise this algorithm in Promela
2. Augment the program such that we can identify the error in the program
3. Use SPIN to find the error in this algorithm
4. Use the counter example generated by SPIN to explain the error in the program

Exercise 4 (6 Points) Give the set of traces on the set of atomic propositions $\{a, b\}$ of the following transition system.

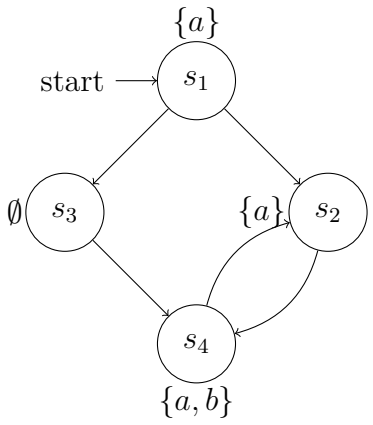

Figure 1: A transition system

Exercise 5 (12 Points) Give an algorithm, in pseudo-code, for invariant checking such that in case the invariant is refuted, a *minimal* counterexample, i.e. one of minimal length, is provided as an error indication.

Exercise 6 (15 Points) Recall the definition of P-deterministic transition systems. Let T and T' be transition systems with the same set of atomic propositions P. Prove the following relationship between trace inclusion and finite trace inclusion.

(a) For P-deterministic T and T':

$$\text{Traces}(T) = \text{Traces}(T') \text{ if and only if } \text{Traces}_{\text{fin}}(T) = \text{Traces}_{\text{fin}}(T').$$

(b) Give concrete examples of T and T' where at least one transition system is not P-deterministic, but

$$\text{Traces}(T) \not\subseteq \text{Traces}(T') \text{ and } \text{Traces}_{\text{fin}}(T) = \text{Traces}_{\text{fin}}(T')$$