Model Checking WS 2011: Assignment 5

Institute for Formal Models and Verification, JKU Linz

Due 17.11.2011

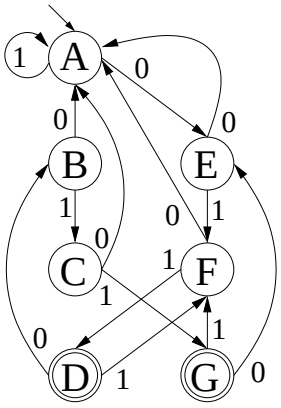
Exercise 17

Let A_1 and A_2 be two LTS. Prove the theorem from slide 40: If $A_1 \lesssim A_2$ then $L(A_1) \subseteq L(A_2)$.

Hint: let $L := (S, I, \Sigma, T)$ be an LTS. Let $w := a_1 a_2 \ldots a_{n-1} a_n$ be a trace of L for $s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \ldots \xrightarrow{a_{n-1}} s_{n-1} \xrightarrow{a_n} s_n$ where $s_0 \in I$ and length $|w| = n$ for $n \geq 0$. Note that w can not only be interpreted as a sequence $a_1 \ldots a_n$ of symbols a_i in Σ but also as a sequence $s_0 \ldots s_n$ of states s_i in S.

Exercise 18

Apply the fixpoint algorithm to minimize the FA shown on the right. Specify all intermediate steps of the algorithm and draw the minimized automaton.



Exercise 19

```
Program P {
  unsigned int x,y;      Thread A {            Thread B {
  // initial state:        while (true)          while (true)
  x = y = 0;                 if (x == y)           if (x != y)
                               x++;                  y++;
  A || B;                }                     }
}
```

Consider program `P` given above. Variables `x` and `y` represent two counters which are shared between two threads `A` and `B` running in parallel (operator `||`). Assume that read/write accesses to `x` and `y` are properly synchronized. Further assume that `unsigned int` has 4 bytes. A state of `P` can be represented in memory as a `PState` object as follows:

```
struct PState {
  unsigned int x;
  unsigned int y;
};
```

Justify your answers to the following questions:

a) When ignoring program semantics, what is the number of all *possible* states of program `P`?

b) How much memory in GB[1] is needed to store the `PState` objects for all *possible* states?

c) Considering initial state `x == 0 && y == 0` and program semantics, what is the number of *reachable* states of program `P`?

d) How much memory in GB is needed to store the `PState` objects for all *reachable* states?

Exercise 20

Read the article[2] *Model Checking: Algorithmic Verification and Debugging* by Clarke, Emerson, and Sifakis who are the inventors of model checking.

- Identify the milestones in the history of model checking.
- Position the techniques we encountered during the lecture in the big picture on model checking provided by this article.

[1] Assume that 1 kB $= 2^{10}$ bytes , 1 MB $= 2^{10}$ kB etc.

[2] You can also find the article on the KUSSS page of this course.