Frankfurt University of Applied Sciences
High Integrity Systems

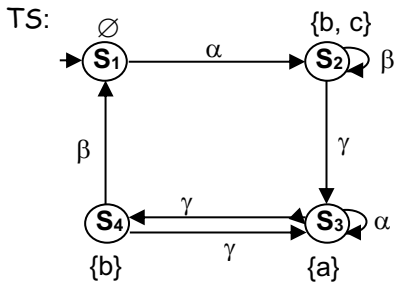
Prof. Dr. Ruth Schorr

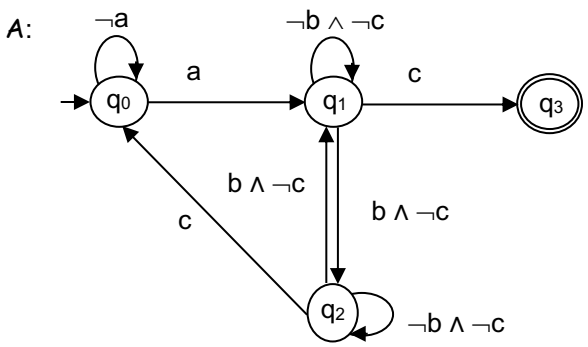
10th June 2022

Formal Specification and Verification
Summer Term 2022
Exercise Sheet 6

Question 1:

Let AP = {a, b, c}. Consider the following NFA A over the alphabet 2^{AP} and the following transition system TS:

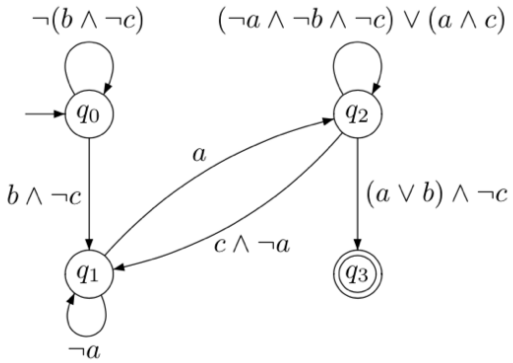




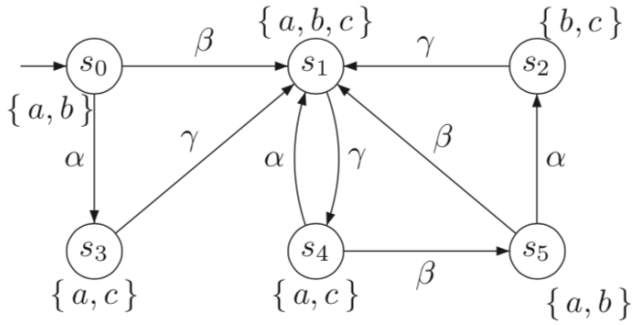
Construct the product TS $\otimes A$ of the transition system and the NFA.

Question 2:

Let AP = {a, b, c}. Consider the following NFA A over the alphabet 2^{AP}



and the following transition system TS:



a) Which of the following words are accepted by the NFA *A*?

1) {b} Ø {a, b} {a, b, c}
2) {b} {a, c} {a} {a, b, c}
3) {a, b} {a, b} Ø {b, c}
4) {b} {a, c} {a, c} {a, b, c}

b) Describe informally the language accepted by the NFA *A*?

c) Construct the product TS $\otimes$ *A* of the transition system and the NFA.

Question 3:

Let AP = {a, b, c}. Provide an NFA *A* that accepts (a*b)*(bc*)*.

Question 4 (mandatory for pre-requisite):

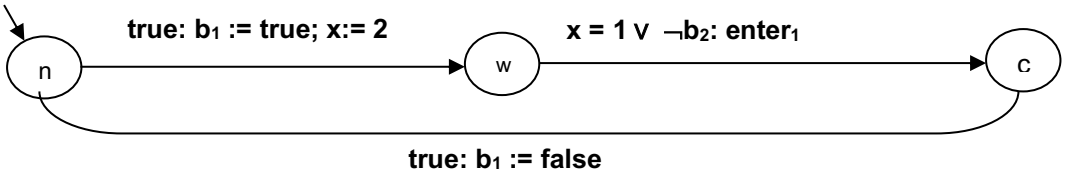
Consider the following mutual exclusion algorithm from Peterson

```
P1    loop forever
      ...                                   (* non-critical actions *)
      <b1 := true; x := 2>;                 (* request; assignments are being
                                               considered as indivisible actions *)
      wait until (x = 1 ∨ ¬b2)
      do critical section od
      b1 := false                           (* release *)
      ...
                                            (* non-critical actions *)
      end loop
```

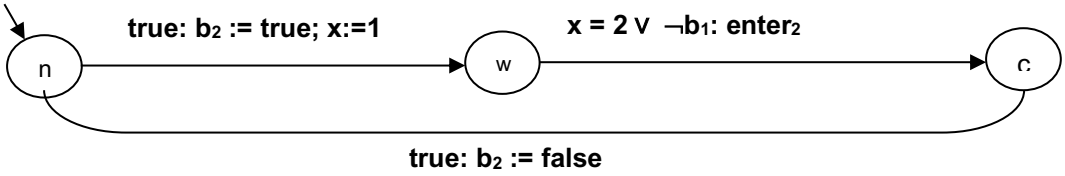
b_i is true if and only if process P_i is waiting or in critical section (i = {1, 2 }). Initially it is assumed that $b_1 = b_2$ = false. If both processes want to enter their critical section, x decides who gets access.

Process P_i (i = {1, 2 }) can be represented by program graph PG_i over Var = {x, b_1, b_2} with location n_i, w_i, and c_i as follows:

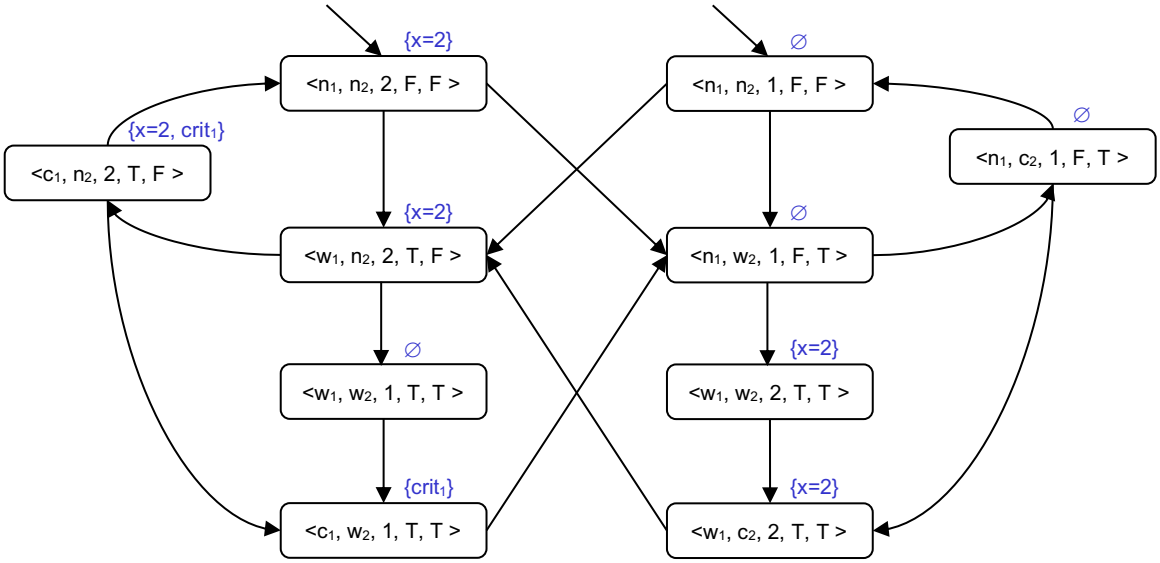
PG_1:



PG_2:



The reachable part of the underlying transition system $TS_{Peterson} = TS(PG_1 \,|||\, PG_2)$ for AP = { x = 2, crit1 } is as follows:



Each state in $TS_{Peterson}$ has the form <loc_1, loc_2, x, b_1, b_2>.

a) Derive an NFA $\mathcal{A}$ such that $L(\mathcal{A}) = \text{MinBadPref}(P)$ for P: “Process P_1 never enters its critical section from a state where x = 2”.

Please remember that the automaton needs to be non-blocking and no initial state should be a final state because we want to use the automaton for the product construction.

b) Construct $TS_{Peterson} \otimes \mathcal{A}$.

c) Check $TS_{Peterson} \models P$ using $TS_{Peterson} \otimes \mathcal{A}$. Explain your answer.