Formal Methods (VIMIMA07)	Year 2019/2020, Spring semester					19. 05. 2020.
ME2A Second midterm exam, group A	1.	2.	3.	4.	5.	Σ
Please start each task on a separate page!						
Please indicate your name and Neptun code on each page!	5 points	6 points	8 points	8 points	8 points	35 points

1. Software model checking with abstraction

2+1+2 points

A short piece of source code can be seen in the right.

```
        z : int
0:      if (z > 0) {
1:              z := z-1;
        }
2:      assert(z>=0);
```

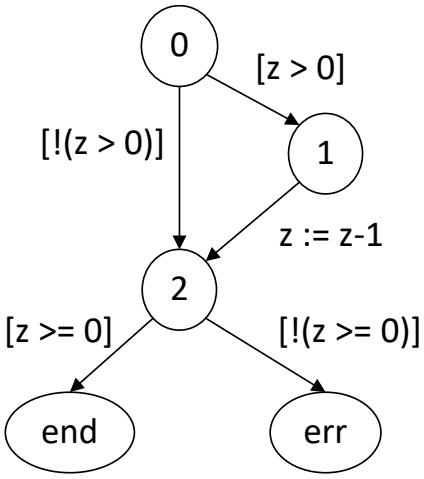
a) Draw the *Control Flow Automaton* (CFA) model that represents the code! Use the line numbers (0, 1, 2) to label the locations of the CFA! Represent assertion violations with a location labeled *err* and represent the normal ending of the program with a location labeled *end*!

b) We are using location and predicate abstraction with a single predicate (*z==1*) for model checking the CFA. What are the possible initial states in the abstract state space if the value of *z* can be arbitrary in the beginning? Give them in the following form: *(location, predicate)*!

c) Is the following abstract path a real or spurious counterexample? Explain your answer!
(0, false) → *(1, false)* → *(2, true)* → *(err, true)*

Solution:

a) The CFA model:



b) (0, false) and (0, true)

c) The path is spurious:

(0, false) → *(1, false)* transition has the condition z>0 and the predicate is z!=1, it is possible.

(1, false) → *(2, true)* here the predicate becomes z==1.

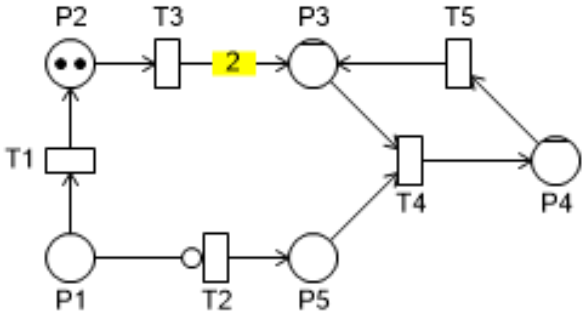
(2, true) → *(err, true)* transition has the condition z<0, which is in contradiction with the z==1 predicate.

2. Coverability graph of a Petri net

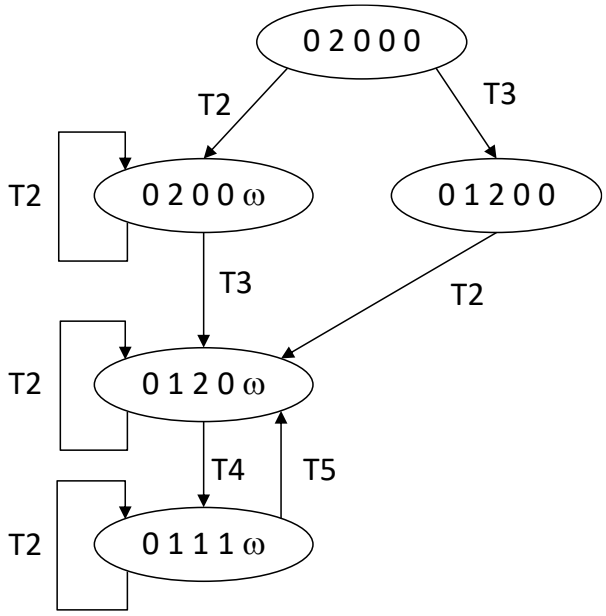
6 points

Consider the following Petri net where places *P3* and *P4* have a finite capacity: *K(P3) = 2* and *K(P4) = 1*. The other places have infinite capacity. Numbers on the edges are the weights of the edges.

Draw the *coverability graph* for the Petri net! Label arcs of the graph with transitions!



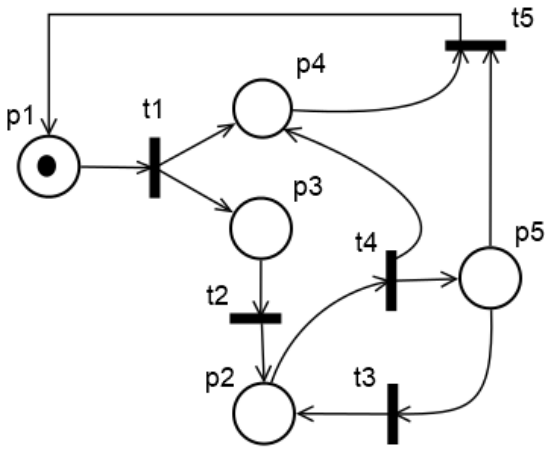
Solution:



3. Structural properties of Petri nets

4*2 points

A Petri net is given in the right.



a) Give the *weighted incidence matrix* of the net!

b) Check if the following vector is a P-invariant of the net (explain your answer): $\mathbf{(1,0,1,1,0)^T}$

c) Check if the following vector is a T-invariant of the net (explain your answer): $\mathbf{(1,1,3,2,1)^T}$

d) Does the following CTL expression hold for the Petri net with the given initial marking? The notation *m(pi)* for *pi* (*i*=1, 2, …, 5) describes the number of tokens in place *pi*. Explain your answer!

AF(*m(p1) + m(p2) + m(p3) + m(p5) = 2*)

Solution:

a) The weighted incidence matrix:

$$\boldsymbol{W} = \begin{bmatrix} \mathbf{-1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{-1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{-1} \\ \mathbf{0} & \mathbf{-1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{-1} & \mathbf{-1} \end{bmatrix}$$

b) $\boldsymbol{W} * (\mathbf{1,0,1,1,0})^{\boldsymbol{T}} = (\mathbf{1,-1,0,1,0})$

The result is not $\mathbf{0}$, this way the given vector is not a P-invariant.

c) $\boldsymbol{W^T} * (\mathbf{1,1,3,2,1})^{\boldsymbol{T}} = (\mathbf{0,2,0,2,-2})$

The result is not $\mathbf{0}$, this way the given vector is not a T-invariant.

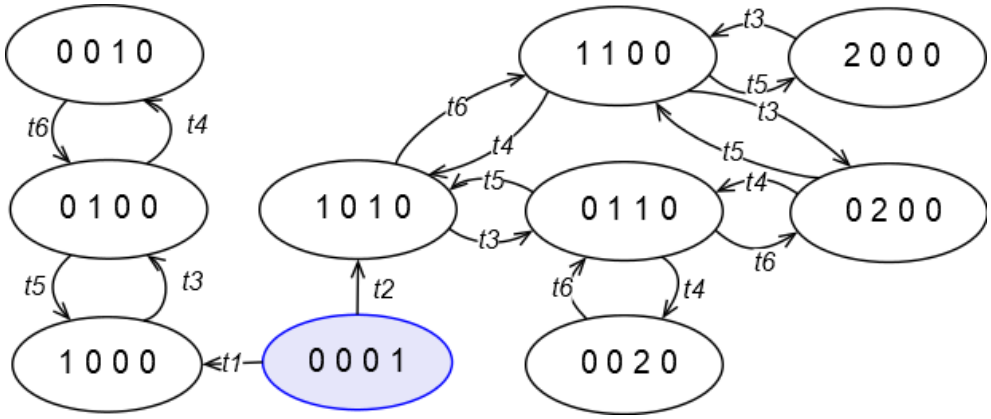
d) The CTL expression does not hold.
In the initial state, the weighted sum of the tokens in the CTL expression is $(\mathbf{1,0,0,0,0}) * (\mathbf{1,1,1,0,1})^{\boldsymbol{T}} = \mathbf{1.}$
Furthermore, $\boldsymbol{W} * (\mathbf{1,1,1,0,1})^{\boldsymbol{T}} = (\mathbf{0,0,0,0,0})$, thus the weight vector in the CTL expression is a P-invariant of the net. This way the weighted sum of the tokens will remain 1, it will never be 2.

4. Dynamic properties of Petri nets

8*1 points

The figure below represents the state space of a Petri net as a reachability graph. The net contains 6 transitions denoted by *t1*, ..., *t6*. The states are denoted by token distribution vectors, for example the vector (0 1 0 0) represents: *m(p1) = 0*, *m(p2) = 1*, *m(p3) = 0* and *m(p4) = 0*. The initial state (0 0 0 1) is marked with a darker background.

Check on the basis of the reachability graph whether the following properties of the net hold, and indicate it with *true* (T), *false* (F) or *not decidable* (ND)! No explanation is needed here.



(a) Transition *t6* is not persistent.

(b) Transition *t1* is L2-live.

(c) Transition *t4* is L3-live.

(d) Transition *t2* is L0-live.

(e) The net is not reversible.

(f) The net does not have a home state.

(g) There is no deadlock in the net.

(h) The net is not bounded.

Solution:

(a) Transition *t6* is not persistent: F

(b) Transition *t1* is L2-live: F

(c) Transition *t4* is L3-live: T

(d) Transition *t2* is L0-live: F

(e) The net is not reversible: T

(f) The net does not have a home state: F

(g) There is no deadlock in the net: T

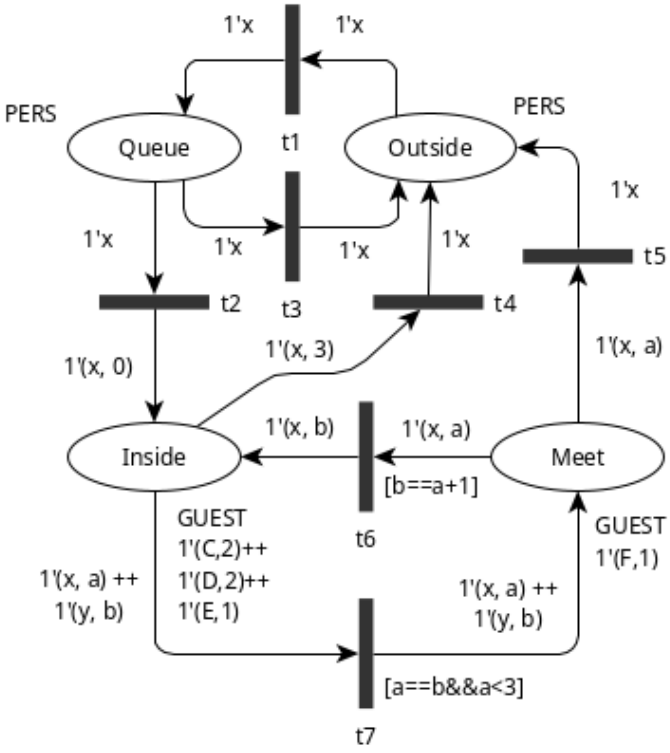
(h) The net is not bounded: F

5. Colored Petri nets

3+3+2 points

The following colored Petri net is given with its definition block. Types of places are denoted by capital words. The current marking is written below the type of the place and guards are given between square brackets.

```
colset PERS = with C | D | E | F;
colset GUEST = product PERS * int;
var x, y: PERS;
var a, b: int;
```



Answer the following questions:

a) List the enabled transition(s) with their binding(s) in the current marking.

b) Give the marking(s) after the firing of the enabled transition(s) with binding(s) found in point a).

c) Is there a reachable cyclic behavior (cyclic firing sequence) in the net? Explain your answer!

Solution:

a) Enabled transition with binding:	**b) The marking of the net after firing of the transition:**			
	Outside	**Queue**	**Inside**	**Meet**
t5 (x=F, a=1)	1'F		1'(C,2)++1'(D,2)++1'(E,1)	
t6 (x=F, a=1, b=2)			1'(C,2)++1'(D,2)++1'(E,1)++ 1'(F,2)	
t7 (x=C, y=D, a=2, b=2)			1'(E,1)	1'(C,2)++1'(D,2)++1'(F,1)
t7 (x=D, y=C, a=2, b=2)			1'(E,1)	1'(C,2)++1'(D,2)++1'(F,1)

c) Reachable, for example firing of t5 (x=F, a=1) is followed by the cyclic firing sequence

t1 (x=F) → t3 (x=F) → t1 (x=F) → t3 (x=F) → …