Formal Methods (VIMIM100)	**2016/2017. year II. semester**					23. March 2017.
First Mid-term Exam	1.	2.	3.	4.	5.	Σ
Name: ______________________						
NEPTUN code: ______________________	12 points	14 points	8 points	8 points	8 points	50 points

1. Theoretical questions (12 points)

1.1. Give the *formal definition* of a *Kripke structure*! Describe the basic *difference* between a Kripke structure and a *labeled transition system* (LTS)! **3 points**

A Kripke structure KS over a set of atomic propositions $AP = \{P, Q, R, \dots\}$ is a tuple (S, I, R, L) where

- $S = \{s_1, s_2, \dots, s_n\}$ is a finite set of states,
- $I \subseteq S$ is the set of initial states,
- $R \subseteq S \times S$ is the set of transitions and
- $L : S \to 2^{AP}$ is the labeling of states by atomic propositions

The basic difference is that in Kripke structures, we label states (with zero or more atomic propositions), while in LTSs, we label transitions with exactly one action.

1.2. Describe the most important *restrictions* (constraints) in CTL compared to CTL*! Give an *example formula* that is a valid CTL* expression but not a valid CTL expression! **3 points**

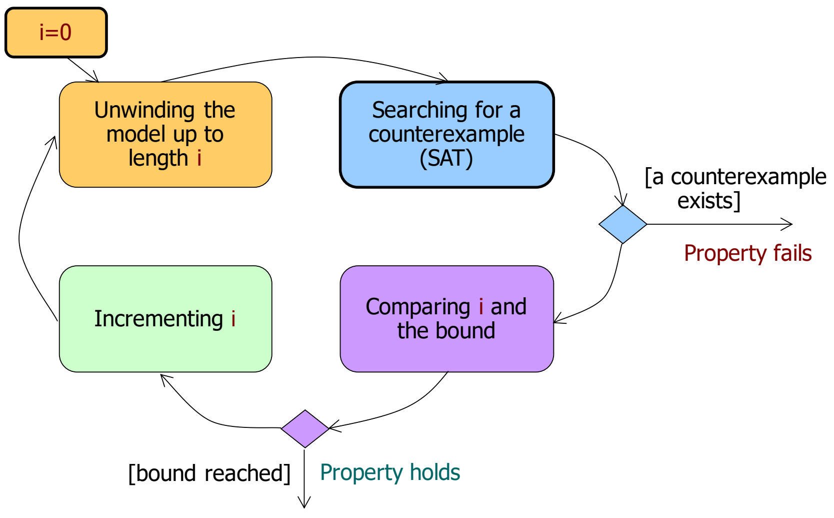
In CTL, operands are composed of exactly one path quantifier and one temporal operator (connective). Example: EXXp (not CTL because of XX).

1.3. How can we reach a *contradicting branch* when using the *tableau decomposition* method for PLTL model checking and applying the decomposition rules for *1)* operator **X** *2)* and operator **U**? **3 points**

1. (X, U): atomic propositions contradict each other or the labeling of the state
2. (X, U): there is no next state
3. (U): loop of *p* without *q*.

1.4. Describe the basic idea of *bounded model checking* (BMC) and describe with a *flow chart* how to use it in an *iterative* strategy to cover the state space up to a given bound! **3 points**

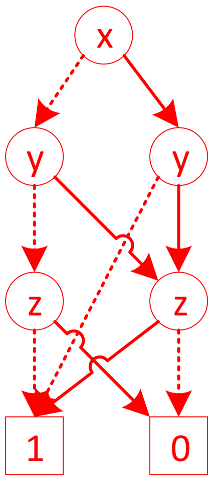
By using characteristic functions, describe a path of length *i* leading to a state that violates the invariant to check. Look for a satisfying model with a SAT solver. If a model is found, it induces a counterexample, otherwise the bound *i* should be increased.

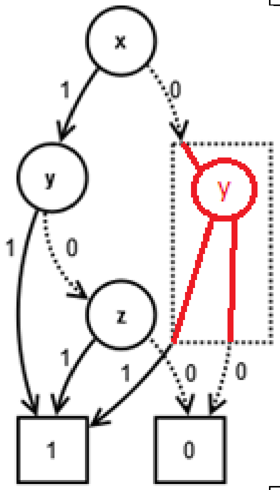

i=0
Unwinding the model up to length i
Searching for a counterexample (SAT)
[a counterexample exists]
Property fails
Incrementing i
Comparing i and the bound
[bound reached]
Property holds

2. Binary Decision Diagrams (12 points) **Please provide the solution on a new sheet!**

2.1. Give the *reduced ordered binary decision diagram* (ROBDD) representation of the function f given by the truth table below! Use the variable order x, y, z in the ROBDD representation! **3 points**

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

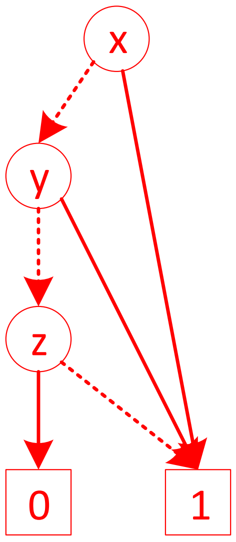




2.2. There is *exactly one* node missing from the dotted rectangle in the ROBDD above. (Note that this ROBDD is not related to the function f in the previous subtask.) Which variable(s) may belong to this missing node? *For each* possible variable, give the *algebraic form* of the function described by the ROBDD! **4 points**

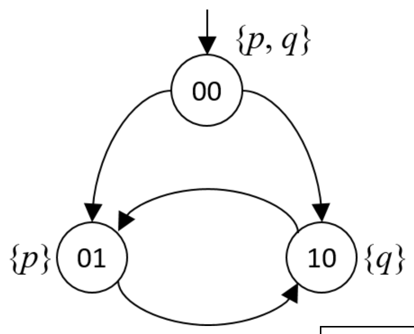
Only y is good, because otherwise the node would be identical to the other z node.
Algebraic form: $(x \wedge y) \vee (x \wedge \neg y \wedge z) \vee (\neg x \wedge y)$

2.3. Select *one* of the possible functions from the previous subtask (2.2) and denote this function by g. Compute the ROBDD representation of the function $f \vee g$! Perform the computation *directly using the ROBDD operations* on f and g (OR operation)! Use the same variable order as before (x, y, z)! **7 points**



3. Symbolic model checking (8 points) **Please provide the solution on a new sheet!**

The following Kripke structure is given including the bit vector encoding of the states:



3.1. Describe the characteristic function of *each state* (using variables x_1 and x_2)! 1 point

$$C_{00} = \neg x_1 \wedge \neg x_2;\ C_{01} = \neg x_1 \wedge x_2;\ C_{10} = x_1 \wedge \neg x_2;$$

3.2. Describe the characteristic function of the *set of states* labeled with *p*! 1 point

$$C_{\{00,01\}} = (\neg x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$$

3.3. Describe the characteristic function of the *transition relation* (containing *all* transitions of the Kripke structure)! 2 points

$$\begin{aligned} C_R = {} & (\neg x_1 \wedge \neg x_2 \wedge \neg x_1' \wedge x_2') \vee \\ & (\neg x_1 \wedge \neg x_2 \wedge x_1' \wedge \neg x_2') \vee \\ & (\neg x_1 \wedge x_2 \wedge x_1' \wedge \neg x_2') \vee \\ & (x_1 \wedge \neg x_2 \wedge \neg x_1' \wedge x_2') \end{aligned}$$

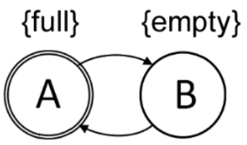
3.4. Run the semantics-based model checking procedure based on the *iterative labeling algorithm* to check if the CTL expression **A**((**EX** *p*) **U** ¬*q*) holds *for the initial state*! *For every step* of the iteration, give the labeling expression and enumerate the labeled states! 4 points

1. iteration: (labeling with ¬*q*)
   01
2. iteration: (labeling with **EX** *p*)
   00
   10
3. iteration: (labeling with **A**((**EX** *p*) **U** ¬*q*))
   01 (because of ¬*q*)
   10 (because of **EX** *p* and every successor is labeled with **A**((**EX** *p*) **U** ¬*q*))
   00 (because of **EX** *p* and *now* every successor is labeled with **A**((**EX** *p*) **U** ¬*q*))

4. LTL requirement formalization (8 points)

The behavior of a *beer* in a dormitory room is modeled with the Kripke structure on the right (the initial state is A). The behavior of *Steve* (a student in the dormitory) is defined by the following rules (the rules are in the form: `<condition> -> <state transition>`):

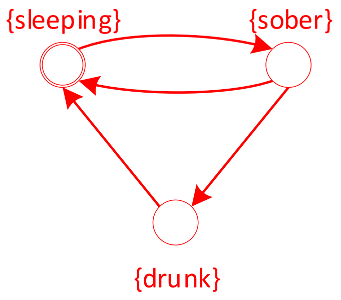
```
var steve: {sleeping, sober, drunk}
initialization:
        steve := sleeping
transition rules:
        steve = sober && beer = full -> steve := drunk
        steve = sober && beer = empty -> steve := sleeping
        steve = sleeping -> steve := sober
        steve = drunk -> steve := sleeping
```

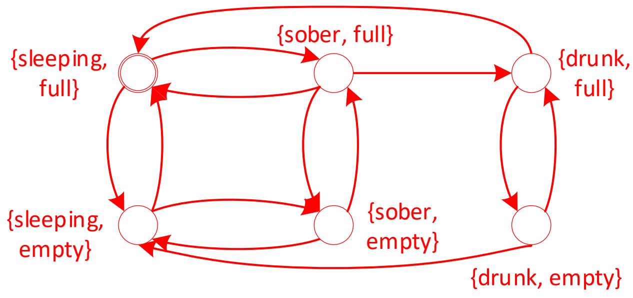


Furthermore, we know that during the time Steve gets drunk, he drinks all the beer.

4.1. First, give the Kripke structure representing *Steve*. Note that in some cases the behavior of Steve depends on the state of the beer. In such cases assume that the beer can be in *any* state. Use the state labels {*sleeping*, *sober*, *drunk*} to describe Steve! Then, give the Kripke structure representing the *whole system* (i.e., Steve and the beer)! In this case, the states will be pairs.

2 points





4.2. Use *LTL expressions* to formalize the following requirements, which must apply to the behavior of the system in every case! Use the labels introduced in the previous subtask! Note that the requirements may or may not hold for the actual system.

6 points

4.2-1. It is universally true that Steve will eventually be sober.

GF *sober*

4.2-2. It is universally true that when Steve is drunk, he will be sleeping at the next step.

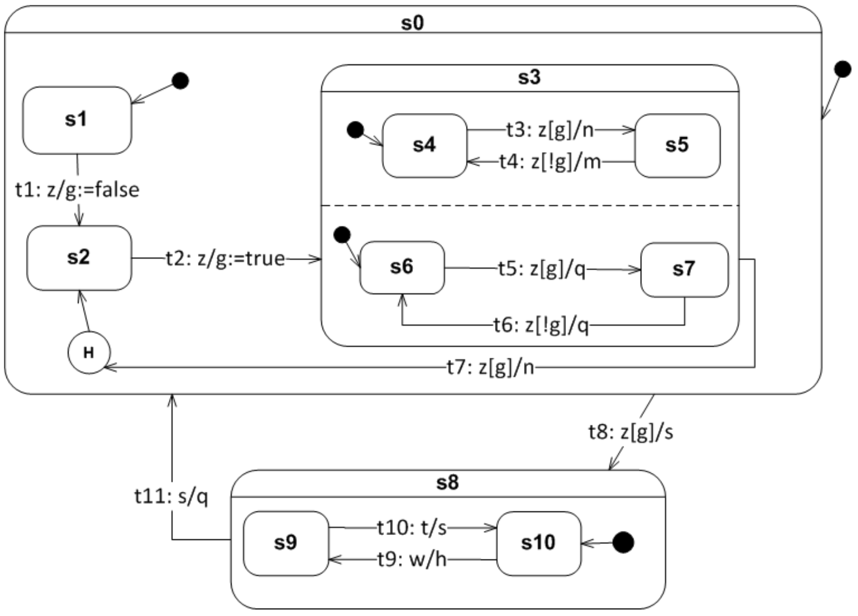
G (*drunk* ⇒ **X** *sleeping*)

4.2-3. It is universally true that if Steve is sober, he will not get drunk until the beer is empty.

G (*sober* ⇒ (¬*drunk* **U** *empty*))

5. Statecharts (8 points)

Consider the following statechart, in which for all states s_k there is also an entry action s_k*.entry* and an exit action s_k*.exit* that is not displayed in the figure. The expressions on the arrows (transitions) have the following form: *transition_name: trigger [guard] / action*. Guards are given as expressions, actions are given as letters (such as *n*) or by assignments (such as *g := true*).



The current state of the statechart is the following state configuration: (s0, s3, s4, s6) and the value of the logical variable *g* is *true*. The incoming event is *z*.

5.1. Which transitions are *enabled*? — 1 point

t3, t5, t7, t8

5.2. Which enabled transitions are *in conflict*? — 1 point

(t3, t7), (t3, t8), (t5, t7), (t5, t8), (t7, t8)

5.3. What is the set of *fireable* transitions after resolving the *conflicts*? If there are multiple sets of fireable transitions, give *all* sets! — 1 point

{t3, t5}

5.4. What is (are) the *next stable* state configuration(s)? If there are more than one possible stable state configurations, give *all* of them! Give the actions and their order during firing the transitions! Do not forget to include the entry and exit actions! — 2 points

Next stable state configuration: {s0, s3, s5, s7}
Actions: Any interleaving of (s4.exit, n, s5.entry) and (s6.exit, q, s7.exit), e.g. (s4.exit, n, s5.entry, s6.exit, q, s7.exit)

5.5. Decide whether the following statements are true or false! Explain the answer (on a separate sheet)! Reachability is considered from the initial configuration with arbitrary incoming event(s). — 3 points

a) A configuration can be reached where t_8 is *fireable*.
False, because in every state, there will be a higher-priority enabled transition (t1, t2 or t7).

b) The configuration (s0, s3, s4, s7) is reachable.
False, because the transitions in concurrent regions *must* fire together.

c) A configuration can be reached where the next configuration is *not deterministic* (there are more possibilities) even if the incoming event and the guard is known.
False, because there are no states with multiple outgoing transitions with the same trigger and overlapping guards.