University of Innsbruck
1st exam

Institute of Computer Science
29 May 2009

Model Checking (VO) SS 2009 LVA 703521

First name: ____________________

Last name: ____________________

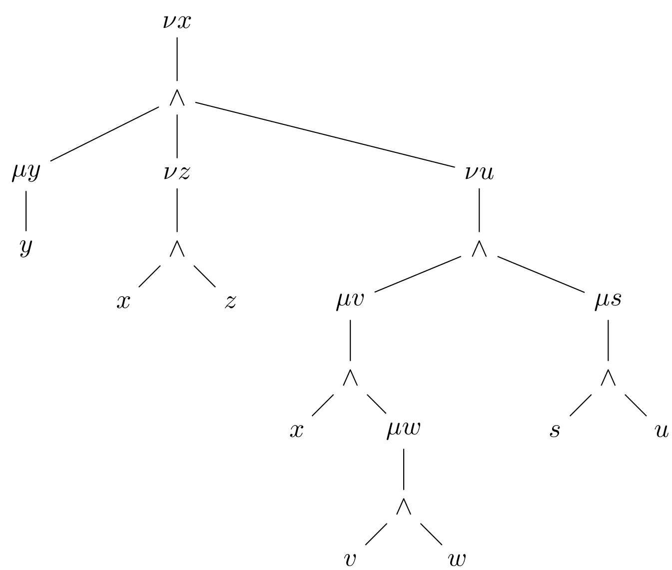
Matriculation number: ____________________

- Please answer all exercises in a readable and precise way. Please cross out solution attempts which are replaced by another solution.
- Cheating is not allowed. Everyone who is caught will fail the exam.
- Please do not remove the staples of the exam.

Exercise	Maximal points	Points
1	25	
2	25	
3	30	
4	20	
Σ	100	
Grade		

Exercise 1 ((2 + 4 + 6 + 8) + 5 points)

Consider the following formula φ.



- For each call $\mathsf{touch}(\alpha)$ where $\alpha \in \{z, v, u, x\}$ write down the set of variables that are invalidated and the set of variables that are reseted.

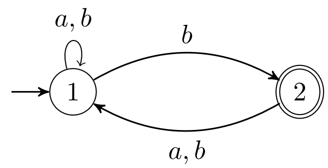
$\mathsf{touch}(z)$:	$\mathsf{Valid} := \mathsf{Valid} \setminus \varnothing$	$\mathsf{Reset} := \varnothing$
$\mathsf{touch}(v)$:	$\mathsf{Valid} := \mathsf{Valid} \setminus \{w\}$	$\mathsf{Reset} := \varnothing$
$\mathsf{touch}(u)$:	$\mathsf{Valid} := \mathsf{Valid} \setminus \{s\}$	$\mathsf{Reset} := \{s\}$
$\mathsf{touch}(x)$:	$\mathsf{Valid} := \mathsf{Valid} \setminus \{z, u, v, w\}$	$\mathsf{Reset} := \{v, w\}$

- Determine $[\![\varphi]\!]$. Just give the result (and apply the algorithm in a lazy way)

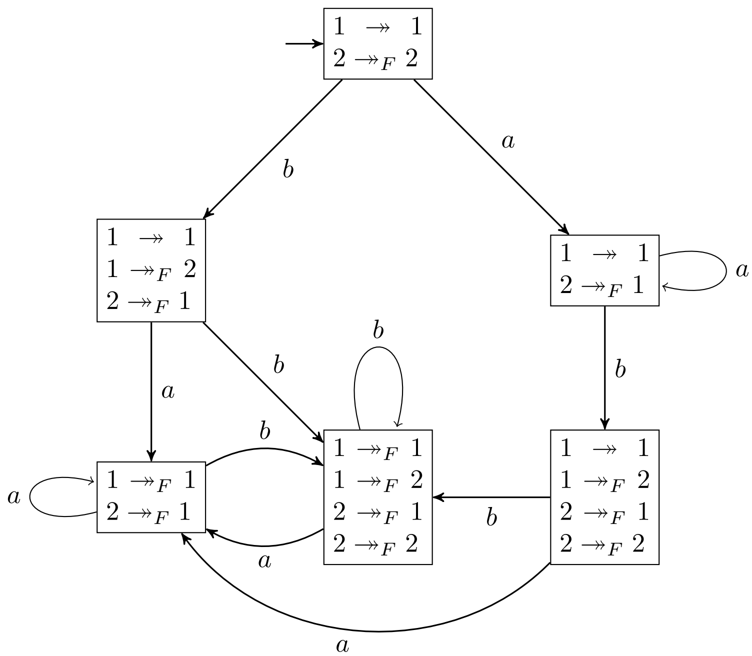
  Since $[\![\mu y.y]\!] = \varnothing$ it follows that $[\![\varphi]\!] = [\![\nu x.(\mu y.y) \wedge \ldots]\!] = \varnothing$.

Exercise 2 (18 + 3 + 4 points)

Consider the following NBA $\mathcal{A}$ over $\Sigma = \{a, b\}$.



- Compute the $\mathcal{A}$-equivalence classes by constructing the transition profile automaton.



- Let $\mathcal{B} = \Sigma^\omega \setminus \mathcal{L}(\mathcal{A})$. Describe $\mathcal{B}$ in your own words.

  $\mathcal{B}$ is the set of words which only contain finitely many b's.

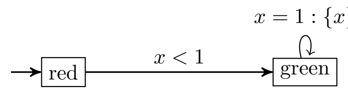
- From the lecture we know that $\mathcal{B} = \bigcup_{(i,j)\in I} U_i \cdot U_j^\omega$ for some index-set I where $U_1, \ldots, U_n$ are the $\sim_\mathcal{A}$ equivalence-classes that correspond to the transition profiles.

  In this examples there is some j and I such that $\mathcal{B} = \bigcup_{i\in I} U_i \cdot U_j^\omega$. What is the transition profile that corresponds to U_j?

  Since $\mathcal{B}$ is the set of words which only contain finitely many a's, obviously, U_j must not contain any word that contains a b. Moreover, U_j cannot be $\{\epsilon\}$. Hence, $U_j = a^+$ and the corresponding transition profile is $1 \twoheadrightarrow 1, 2 \twoheadrightarrow_F 1$.

Exercise 3 (30 points)

Consider the following timed automaton TA.

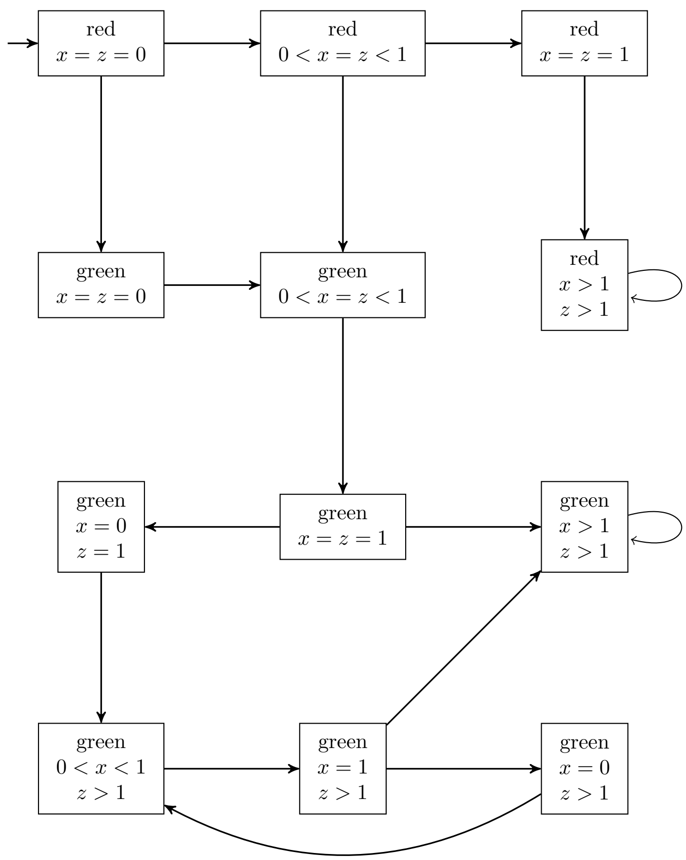


Formally apply the algorithm for TCTL-model checking to determine $TA \models \Phi$ where $\Phi = \mathsf{E}\,\neg\mathsf{green}\,\mathsf{U}^{>1}\mathsf{green}$.

For the solution it suffices to determine whether the initial state is in the satisfiability set. However, whenever you need to determine whether some state s satisfies a CTL formula then all reachable states of s have to be constructed.

To determine $TA \models \mathsf{E}\,\neg\mathsf{green}\,\mathsf{U}^{>1}\mathsf{green}$ we just have to determine whether $(\mathsf{red}, x = 0) \in \mathit{Sat}(\Phi)$ where $(\mathsf{red}, x = 0)$ is a state of $\mathit{RTS}(\mathit{TA}, \Phi)$. To this end, one has to determine $(\mathsf{red}, x = z = 0) \models \mathsf{E}\,\neg\mathsf{green} \vee \mathsf{green}\,\mathsf{U}\, z > 1 \wedge \mathsf{green} =: \Psi$ where $(\mathsf{red}, x = z = 0)$ is a state of $\mathit{RTS}(\mathit{TA} \uplus \{z\}, \Phi)$.

Hence, we construct the reachable part of $\mathit{RTS}(\mathit{TA} \uplus \{z\}, \Phi)$ starting from $(\mathsf{red}, x = z = 0)$.



Now CTL-model checking shows $(\mathsf{red}, x = z = 0) \models \Psi \equiv \mathsf{E}\,\mathsf{F}\, z > 1 \wedge \mathsf{green}$.

Hence, $(\mathsf{red}, x = 0) \in \mathit{Sat}(\Phi)$ and thus, $\mathit{TA} \models \Phi$.

Exercise 4 (10 + 10 points)

Let TS be a transition system. Let $R_1, \ldots, R_n$ be bisimulations for TS. Prove or disprove the following statements.

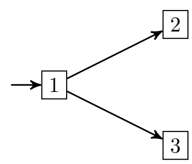
(i) $U = \bigcup_{1 \leqslant i \leqslant n} R_i$ is a bisimulation for TS.

We prove that U is bisimulation for TS. So, assume sUt. Hence, there is some i such that sR_it.

- Since R_i is a bisimulation for TS we know that $L(s) = L(t)$.
- If $s \to s'$ then there must be some t' such that $t \to t'$ and $s'R_it'$ since R_i is a bisimulation. But this also shows $s'Ut'$.
- If $t \to t'$ then there must be some s' such that $s \to s'$ and $s'R_it'$ since R_i is a bisimulation. But this also shows $s'Ut'$.

(ii) $I = \bigcap_{1 \leqslant i \leqslant n} R_i$ is a bisimulation for TS.

We show that in general, I is not a bisimulation. Consider the following transition system.



Then it is easy to see that $R_1 = \{(1,1), (2,2), (3,3)\}$ and $R_2 = \{(1,1), (2,3), (3,2)\}$ are bisimulations, but $I = R_1 \cap R_2 = \{(1,1)\}$ is not a bisimulation.