Introduction to Model Checking (VO) — WS 2008/2009 — LVA 703503

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.
- Please do not remove the staples of the exam.
- Cheating is not allowed. Everyone who is caught will fail the exam.

Exercise	Maximal points	Points
1(i)	12	
1(ii)	12	
2	18	
3	19	
4	9	
Σ	70	
Grade		

Exercise 1 (12 + 12 points)

Consider the following property.

Between every two neighboring occurrences of "green", "red" is valid all the time strictly in between. $(\star)$

One might formulate this property as the following LTL-formula φ.

$$\varphi = \neg \mathsf{F}\,(\mathsf{green} \wedge \neg(\mathsf{red}\,\mathsf{U}\,\mathsf{green}))$$

(i) φ is equivalent to the formula $\psi = \neg(\mathsf{true}\,\mathsf{U}\,(\mathsf{green} \wedge \neg(\mathsf{red}\,\mathsf{U}\,\mathsf{green})))$. Construct parts of the GNBA for ψ using the *improved* translation from LTL to GNBAs.

- $cl'(\psi) = \mathsf{green}, \mathsf{red}, \mathsf{red}\,\mathsf{U}\,\mathsf{green}, \mathsf{true}\,\mathsf{U}\,(\mathsf{green} \wedge \neg(\mathsf{red}\,\mathsf{U}\,\mathsf{green}))$
- $(c_1, \ldots, c_4)^T \in \delta((b_1, \ldots, b_4)^T, (d_1, d_2)^T)$ iff $d_1 \Leftrightarrow c_1$, $d_2 \Leftrightarrow c_2$, $b_3 \Leftrightarrow (b_1 \vee (b_2 \wedge c_3))$, and $b_4 \Leftrightarrow (b_1 \wedge \neg b_3) \vee c_4$
- $(c_1, \ldots, c_4)^T \in \delta(q_0, (d_1, d_2)^T)$ iff $d_1 \Leftrightarrow c_1$, $d_2 \Leftrightarrow c_2$, and $\neg c_4$.

(ii) φ does not correspond to the textual property $(\star)$. Write down an infinite word w that distinguishes φ from $(\star)$. Moreover, write down an LTL-formula χ which corresponds to $(\star)$.

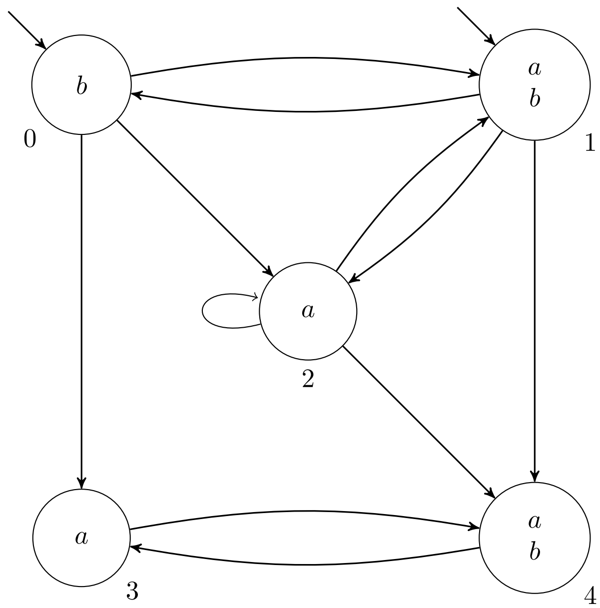
There are two reasons why φ does not correspond to $(\star)$.

- The timing of the formula $\varphi_1 = \mathsf{green} \wedge \neg(\mathsf{red}\,\mathsf{U}\,\mathsf{green})$ does not work. Whenever green is satisfied then obviously, $\mathsf{red}\,\mathsf{U}\,\mathsf{green}$ is satisfied and hence $\neg(\mathsf{red}\,\mathsf{U}\,\mathsf{green})$ is not satisfied. Thus, φ_1 is unsatisfiable and therefore φ is a tautology. Hence, $w = \{\mathsf{green}\}\,\varnothing\,\{\mathsf{green}\}\ldots$ does not satisfy $(\star)$ but it satisfies φ.
- The second problem (if one fixes the timing) is that φ does not take into account that green might occur only finitely often. A corrected version is

$$\chi = \neg \mathsf{F}\,(\mathsf{green} \wedge \mathsf{X}\,\mathsf{F}\,\mathsf{green} \wedge \mathsf{X}\,\neg(\mathsf{red}\,\mathsf{U}\,\mathsf{green})) \equiv \mathsf{G}\,(\mathsf{green} \Rightarrow \mathsf{X}\,(\mathsf{G}\,\neg\mathsf{green} \vee (\mathsf{red}\,\mathsf{U}\,\mathsf{green}))).$$

Exercise 2 (18 points)

Consider the following transition system *TS*.



Perform CTL*-model checking for the formula

$$\Phi = \mathsf{E}\,(\mathsf{X}\,(a \wedge \neg b) \wedge \mathsf{X}\,\mathsf{A}\,(b\,\mathsf{U}\,\mathsf{G}\,a))$$

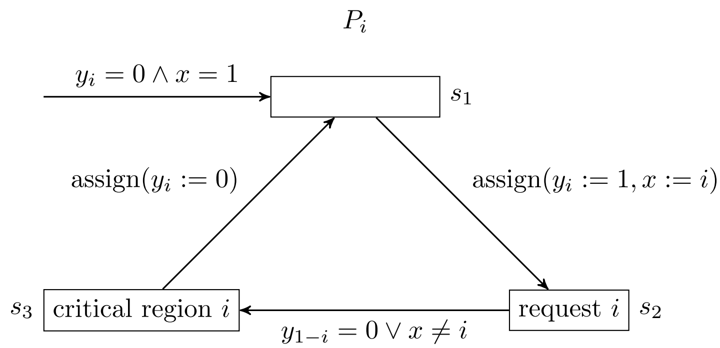
Here, the sets $Sat(\Psi)$ should be indicated for every non-atomic state-subformula Ψ of Φ. Note that the subformula $a \wedge \neg b$ of Φ should be seen as a state-formula. It is not necessary to perform the LTL-model checking explicitly, but write down each LTL-formula that is checked.

- Eliminating A yields the formula $\Phi' = \mathsf{E}\,(\mathsf{X}\,(a \wedge \neg b) \wedge \mathsf{X}\,\neg\mathsf{E}\,\neg(b\,\mathsf{U}\,\mathsf{G}\,a))$.
- $Sat(\neg b) = \{2, 3\}$
- $Sat(a \wedge \neg b = \Psi_1) = \{2, 3\}$
- $Sat(\mathsf{E}\,\neg(b\,\mathsf{U}\,\mathsf{G}\,a) = \Psi_2) = \{0, 1, 2\}$ (LTL model checking of formula $\neg(b\,\mathsf{U}\,\mathsf{G}\,a)$)
- $Sat(\neg\Psi_2 = \Psi_3) = \{3, 4\}$
- $Sat(\Phi') = \{0, 4\}$ (LTL model checking of formula $\mathsf{X}\,a_{\Psi_1} \wedge \mathsf{X}\,a_{\Psi_3}$)

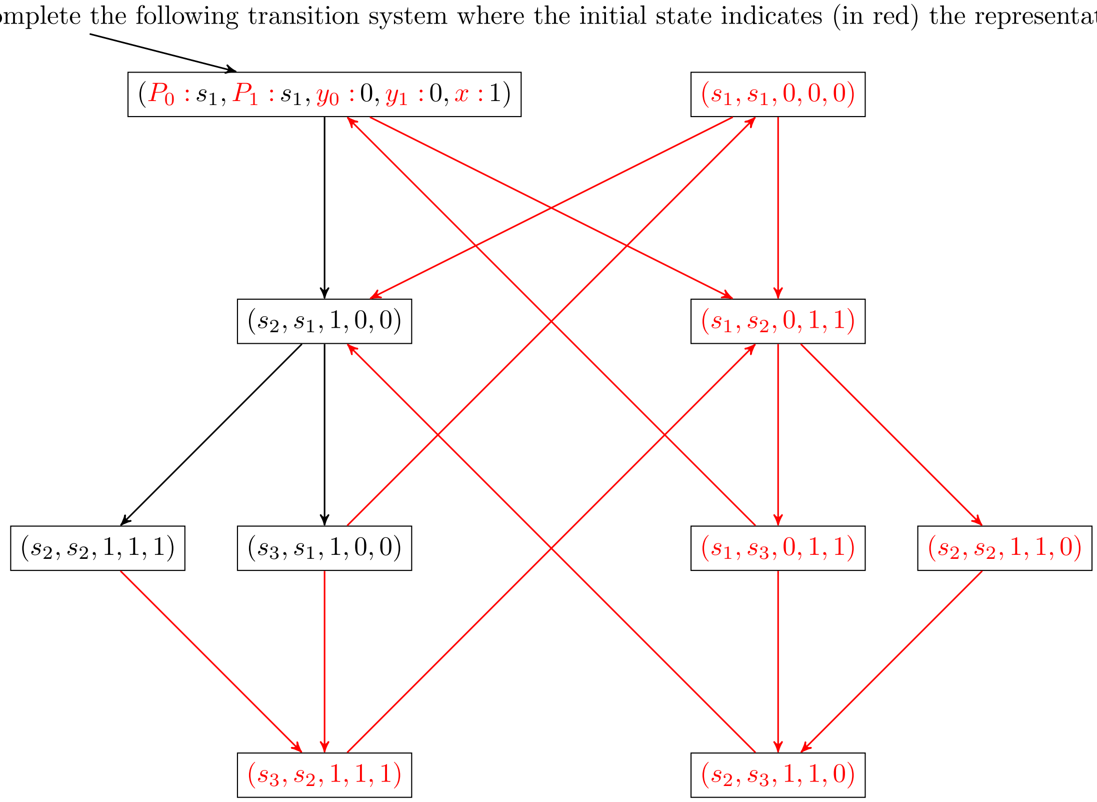
$\Rightarrow$ $TS \not\models \Phi$

Exercise 3 (19 points)

Consider the following channel system $[P_0 \mid P_1]$ which models a mutual exclusion protocol of Pnueli. Here, communication is done via a shared variable x.



Complete the following transition system where the initial state indicates (in red) the representation of states.



Exercise 4 (9 points)

Each correct answer is worth 3 points. A wrong answer results in zero points. Giving no answer is worth 1 point.

	Yes	No
There is some GNBA $\mathcal{A}$ such that there is no NBA $\mathcal{B}$ with $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$.		✓
When checking $TS \models \varphi$ for some LTL formula φ, as intermediate result one constructs a GNBA which accepts $\mathcal{L}(\varphi)$.		✓
If one wants to compute the intersection of NBAs then one can use a similar construction as for GNBAs: for $\mathcal{A}_i = (\mathcal{Q}_i, \Sigma, q_{0,i}, \delta_i, F_i)$ return $\mathcal{A} = (\mathcal{Q}_1 \times \mathcal{Q}_2, \Sigma, (q_{0,1}, q_{0,2}), \delta, F_1 \times F_2)$ where δ is defined as in the intersection automaton for GNBAs.		✓