UNIVERSITY OF INNSBRUCK
2ND EXAM

INSTITUTE OF COMPUTER SCIENCE
JANUARY 20, 2009

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

First name: ______________________________

Last name: ______________________________

Matriculation number: ______________________________

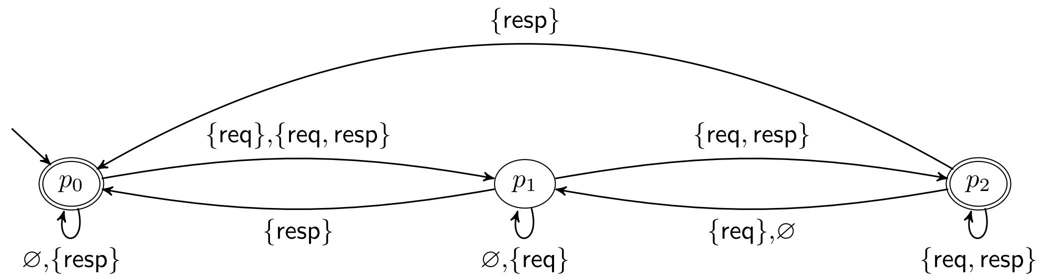
- Please answer all exercises in a readable and precise way.
- Please cross out solution attempts which are replaced by another solution.
- Please do not remove the staples of the exam.
- Cheating is not allowed. Everyone who is caught will fail the exam.

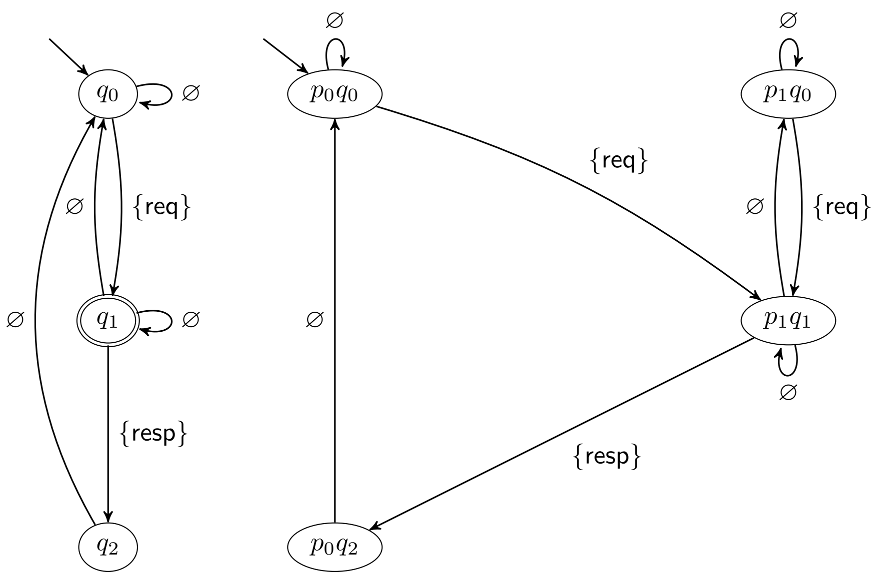
Exercise	**Maximal points**	**Points**
1	**18**	
2	**19**	
3	**13**	
4	**20**	
Σ	**70**	
Grade		

Exercise 1 (9+3+2+4 points)

The GNBA $\mathcal{A}_1 = (\{p_0, p_1, p_2\}, \Sigma, p_0, \delta_1, \{p_0, p_2\})$ accepts $\mathcal{L}(\varphi)$ for some LTL-formula φ. Moreover, we also have a GNBA $\mathcal{A}_2 = (\{q_0, q_1, q_2\}, \Sigma, q_0, \delta_2, \{q_1\})$ which encodes a transition system TS, i.e., $\mathcal{L}(\mathcal{A}_2) = Traces(TS)$.

(i) Construct the GNBA $\mathcal{A}$ for the intersection of $\mathcal{A}_1$ and $\mathcal{A}_2$. Only write down those states which are reachable from the initial state.





(ii) Write down the final states set(s) of $\mathcal{A}$ explicitly. Again, you only have to mention the reachable states.

$F_1 = \{p_0q_0, p_0q_2\}$ and $F_2 = \{p_1q_1\}$.

(iii) Is $\mathcal{L}(\mathcal{A}) = \varnothing$? If not, provide a word which is contained in $\mathcal{L}(\mathcal{A})$.

$(\{\text{req}\}\{\text{resp}\}\varnothing)^\omega \in \mathcal{L}(\mathcal{A})$.

(iv) Is it possible to answer "$TS \models \varphi$?" using only the answer to part (iii)? Explain your answer shortly.

No it is not possible, since $TS \models \varphi$ iff $Traces(TS) \subseteq \mathcal{L}(\varphi)$ iff $\mathcal{L}(\mathcal{A}_2) \subseteq \mathcal{L}(\mathcal{A}_1)$ iff $\mathcal{L}(\mathcal{A}_2) \cap \mathcal{L}(\mathcal{A}_1) = \mathcal{L}(\mathcal{A}_2)$ and since in part (iii) we only checked whether $\mathcal{L}(\mathcal{A}_2) \cap \mathcal{L}(\mathcal{A}_1) = \varnothing$.

Exercise 2 (6 + 13 points)

Consider the LTL-formula

$$\varphi = \neg(\text{true}\,\mathsf{U}\,(\mathsf{req} \wedge \mathsf{X}\,(\neg\mathsf{resp}\,\mathsf{U}\,\mathsf{req})))$$

(i) Formulate the meaning of φ in words where req and resp represent a *request* and *response*, respectively.
Between every two requests there is a response.

(ii) Construct major parts of the GNBA for ψ using the *improved* translation from LTL to GNBAs.

- $cl'(\psi) = \mathsf{req}, \mathsf{resp}, (\neg\mathsf{resp})\,\mathsf{U}\,\mathsf{req}, \mathsf{X}\,((\neg\mathsf{resp})\,\mathsf{U}\,\mathsf{req}), \text{true}\,\mathsf{U}\,(\mathsf{req} \wedge (\mathsf{X}\,((\neg\mathsf{resp})\,\mathsf{U}\,\mathsf{req})))$
- $(c_1, \ldots, c_5)^T \in \delta((b_1, \ldots, b_5)^T, (d_1, d_2)^T)$ iff $d_1 \Leftrightarrow c_1$, $d_2 \Leftrightarrow c_2$, $b_3 \Leftrightarrow (b_1 \vee (\neg b_2 \wedge c_3))$, $b_4 \Leftrightarrow c_3$, and $b_5 \Leftrightarrow ((b_1 \wedge b_4) \vee c_5)$.
- Write down the set(s) of final states.
  $F_1 = \{(b_1, \ldots, b_5)^T \mid \neg b_3 \vee b_1\}$ and $F_2 = \{(b_1, \ldots, b_5)^T \mid \neg b_5 \vee (b_1 \wedge b_4)\}$.

Exercise 3 (2 + 4 + 7 points)

Consider a buffer which consecutively reads commands in (to store something in the buffer) or out (to read something out of the buffer). Initially the buffer is empty.

There is the requirement that the buffer cannot output something if it is empty. To this end some properties have been identified for the allowed command sequences.

(i) The command sequence may not start with out.

$$\varphi_1 = \neg \mathsf{out}$$

(ii) At each moment, exactly one of the commands in and out is present.

$$\varphi_2 = \mathsf{G}\,(\mathsf{in} \Leftrightarrow \neg \mathsf{out})$$

(iii) The command sequence may not start with $(\mathsf{in}\ \mathsf{out})^*\mathsf{out}$.

$$\varphi_3 = \neg(((\mathsf{in} \Rightarrow \mathsf{X}\,\mathsf{out}) \wedge (\mathsf{out} \Rightarrow \mathsf{X}\,\mathsf{in}))\,\mathsf{U}\,(\mathsf{out} \wedge \mathsf{X}\,\mathsf{out}))$$

Provide three LTL formulas φ_1, φ_2, and φ_3 for these properties. Here, for φ_3 you can already assume that properties (i) and (ii) are satisfied.

Exercise 4 (20 points)

Consider the following nanoPromela statement.

```
do
  :: a  =>  if :: b => c ! b ; d ! e
               :: true => skip
            fi ;
            a := false;
od
```

Formally derive all transitions that are possible from this initial statement. You may use abbreviations like “`do` ... `od`” and “`if` ... `fi`”.

$$\dfrac{}{\text{do ... od} \xrightarrow{\neg a} \text{exit}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\text{skip} \rightarrow \text{exit}}}{\text{if ... fi} \rightarrow \text{exit}}}{\text{if ... fi; a := false} \rightarrow \text{a := false}}}{\text{do ... od} \xrightarrow{a} \text{a := false; do ... od}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\text{c ! b} \xrightarrow{\text{c ! b}} \text{exit}}}{\text{c ! b; d ! e} \xrightarrow{\text{c ! b}} \text{d ! e}}}{\text{if ... fi} \xrightarrow{\text{b : c ! b}} \text{d ! e}}}{\text{if ... fi; a := false} \xrightarrow{\text{b : c ! b}} \text{d ! e; a := false}}}{\text{do ... od} \xrightarrow{\text{a} \wedge \text{b : c ! b}} \text{d ! e; a := false; do ... od}}$$