Introduction to Model Checking (VO) — WS 2007/2008 — LVA 703503

First name: ______________________________

Last name: ______________________________

Matriculation number: ______________________________

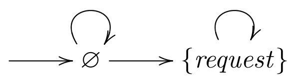
- Write your name and matriculation number on every page.
- Please answer all exercises in a readable and precise way. Do *not* write with a pencil or a red pen. Please cross out solution attempts which are replaced by another solution.
- Cheating is not allowed. Everyone who is caught will fail the exam.
- Please do not remove the staples of the exam.

Exercise	**Maximal points**	**Points**
1	**12**	
2	**24**	
3	**15**	
4	**19**	
Σ	**70**	
Grade		

First name	Last name	Matriculation number

Exercise 1 (12 points)

Each correct answer is worth four points. A wrong answer results in zero points. Giving no answer is worth one point.

	Yes	No
The CTL formula $(\mathsf{A\,G\,A\,F}\,\mathit{request}) \Rightarrow (\mathsf{A\,G\,A\,F}\,\mathit{response})$ is equivalent to the LTL formula $(\mathsf{G\,F}\,\mathit{request}) \Rightarrow (\mathsf{G\,F}\,\mathit{response})$. 		✓
Every language $L \subseteq \Sigma^\omega$ can be recognized by some NBA. (We have the result as for NFAs: regular ω-languages do not cover all ω-languages. A formal prove can be done as follows: For all NBAs $\mathcal{A}$ we know that if $\mathcal{L}(\mathcal{A}) \neq \varnothing$ then by the non-emptyness check we figure out a word $w = vu^\omega \in \mathcal{L}(\mathcal{A})$ for finite words v, u. Hence, the language $L = \{\pi\} \in \{0-9, .\}^\omega$ cannot be accepted by an NBA since π is not a rational number.)		✓
Emptiness of $\mathcal{L}(\mathcal{A})$ for some GNBA $\mathcal{A}$ can directly be decided using an SCC-based analysis, without first translating $\mathcal{A}$ into some NBA. ($\mathcal{L}(\mathcal{A}) \neq \varnothing$ iff there is an SCC of $\mathcal{A}$ that is reachable from the initial state and that contains a state from each set F_i of final states)	✓	

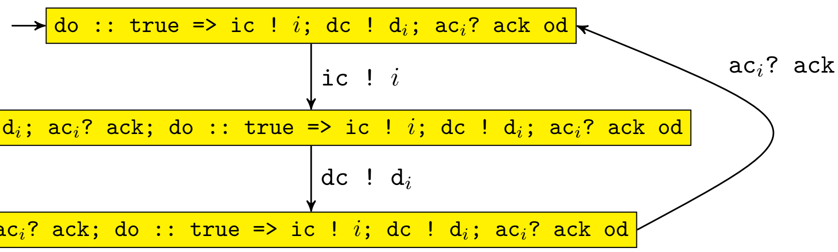
Exercise 2 (21 + 3 points)

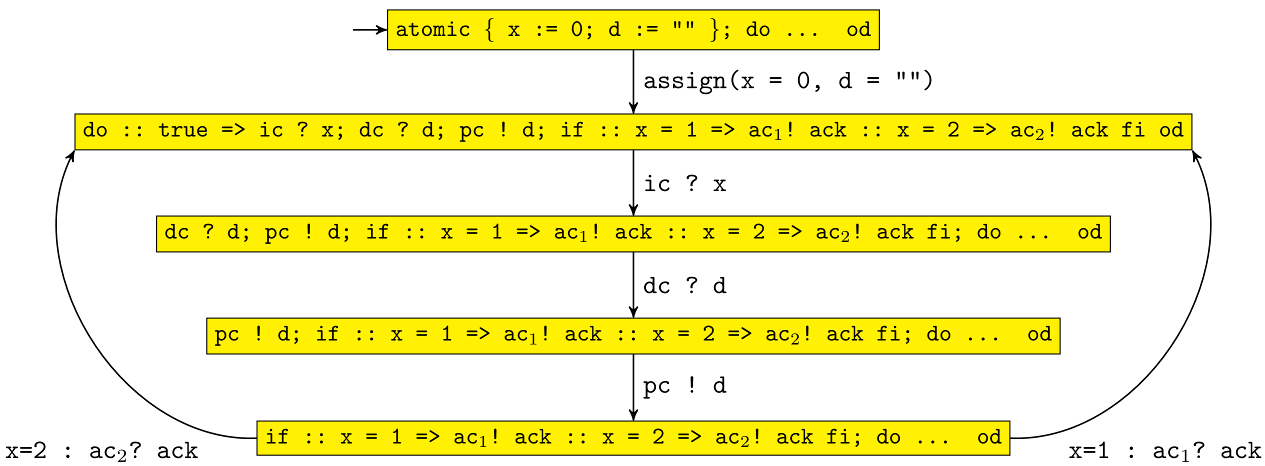
Consider the following nanoPromela program which has two clients ($i \in \{1, 2\}$) which send their data via a scheduler to a printer. After a clients data $\mathtt{d}_i$ is delivered at the printer, client i gets an acknowledgement.

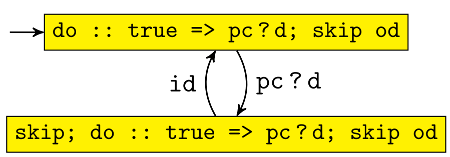
```
------- CLIENT i ------------
do :: true => ic ! i; dc ! d_i; ac_i ? ack od

------- SCHEDULER -----------
atomic { x := 0; d := "" };
do :: true => ic ? x; dc ? d; pc ! d; if :: x = 1 => ac_1 ! ack :: x = 2 => ac_2 ! ack fi od

------- PRINTER -------------
do :: true => pc ? d; skip od
```

- Construct the channel-system for the nanoPromela program.

First name	Last name	Matriculation number





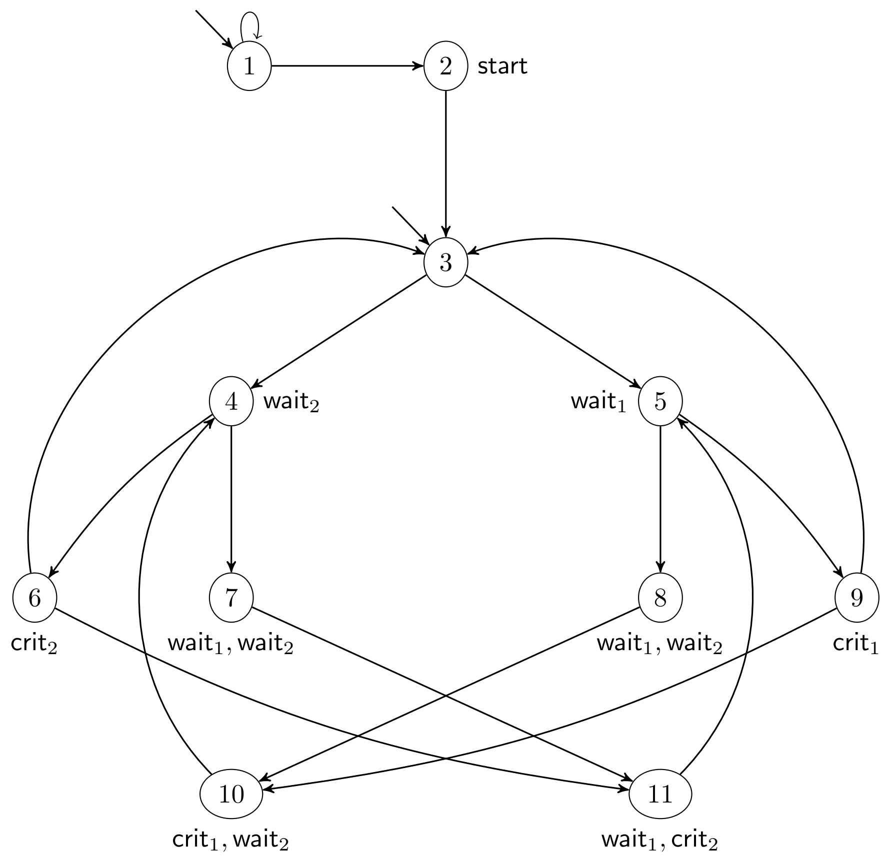


- Does the program contain a serious bug using asynchronous communication? If so, shortly describe it.

  Consider the following situation. Client 1 sends its id which is read by the scheduler. Then client 2 sends both id and data. Then client 1 sends its data, but the scheduler reads the data of client 2, sends it to the printer, but then falsely sends the acknowledgement to client 1.

First name	Last name	Matriculation number

Exercise 3 (15 points)



Consider the above transition system TS of a mutual exclusion protocol and the following CTL*-formula Φ.

$$\Phi = (\mathsf{A}\,((\mathsf{F}\,\mathsf{G}\,\neg\mathsf{start}) \wedge \mathsf{A}\,(\neg\mathsf{wait}_1 \vee \mathsf{F}\,\mathsf{crit}_1))) \wedge \mathsf{A}\,\mathsf{F}\,(\mathsf{crit}_1 \vee \mathsf{crit}_2)$$

Does $TS \models \Phi$ hold? Justify your answer by performing CTL*-model checking, and write down $Sat(\Psi)$ for every state-subformula Ψ of Φ. Whenever one computes a set $Sat(\mathsf{A}\,\varphi)$, additionally write down the corresponding LTL-formula φ' that is checked. However, it is not necessary to perform LTL-model checking explicitly.

- $Sat(\mathsf{start}) = \{2\}$
- $Sat(\mathsf{wait}_1) = \{5, 7, 8, 11\}$
- $Sat(\mathsf{crit}_1) = \{9, 10\}$
- $Sat(\mathsf{crit}_2) = \{6, 11\}$
- $Sat(\mathsf{A}\,\neg\mathsf{wait}_1 \vee \mathsf{F}\,\mathsf{crit}_1) = \{1 - 11\}$. This step involves LTL model checking of the formula $\neg\mathsf{wait}_1 \vee \mathsf{F}\,\mathsf{crit}_1$.

  Alternatively one could have computed $Sat(\neg\mathsf{wait}_1) = \{1-4, 6, 9, 10\}$ and then perform LTL model checking for the formula $a \vee \mathsf{F}\,\mathsf{crit}_1$ where a is a new proposition which is valid in states $Sat(\neg\mathsf{wait}_1)$.
- $Sat(\mathsf{A}\,((\mathsf{F}\,\mathsf{G}\,\neg\mathsf{start}) \wedge \mathsf{A}\,(\neg\mathsf{wait}_1 \vee \mathsf{F}\,\mathsf{crit}_1))) = \{1-11\}$. This step involves LTL model checking of the formula $\mathsf{A}\,((\mathsf{F}\,\mathsf{G}\,\neg\mathsf{start}) \wedge b)$ where b is a new proposition that is valid in states $Sat(\mathsf{A}\,(\neg\mathsf{wait}_1 \vee \mathsf{F}\,\mathsf{crit}_1))$, i.e., which is always valid.

First name	Last name	Matriculation number

Alternatively one could have computed $Sat(\neg \mathsf{start}) = \{1, 3 - 11\}$ and then perform LTL model checking for the formula $\mathsf{A}\,((\mathsf{F}\,\mathsf{G}\,c) \wedge b)$ where b is as above and c is another new proposition which is valid in states $Sat(\neg \mathsf{start})$.

- $Sat(\mathsf{A}\,\mathsf{F}\,(\mathsf{crit}_1 \vee \mathsf{crit}_2)) = \{2 - 11\}$. This step involves LTL model checking of the formula $\mathsf{F}\,(\mathsf{crit}_1 \vee \mathsf{crit}_2)$.

  Alternatively one could have computed $Sat(\mathsf{crit}_1 \vee \mathsf{crit}_2) = \{6, 9 - 11\}$ and then perform LTL model checking for the formula $\mathsf{F}\,d$ where d is a new proposition which is valid in states $Sat(\mathsf{crit}_1 \vee \mathsf{crit}_2)$.

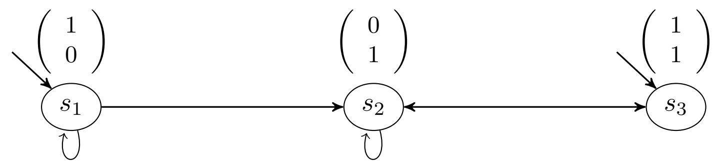
- $Sat(\Phi) = \{1 - 11\} \cap \{2 - 11\} = \{2 - 11\}$

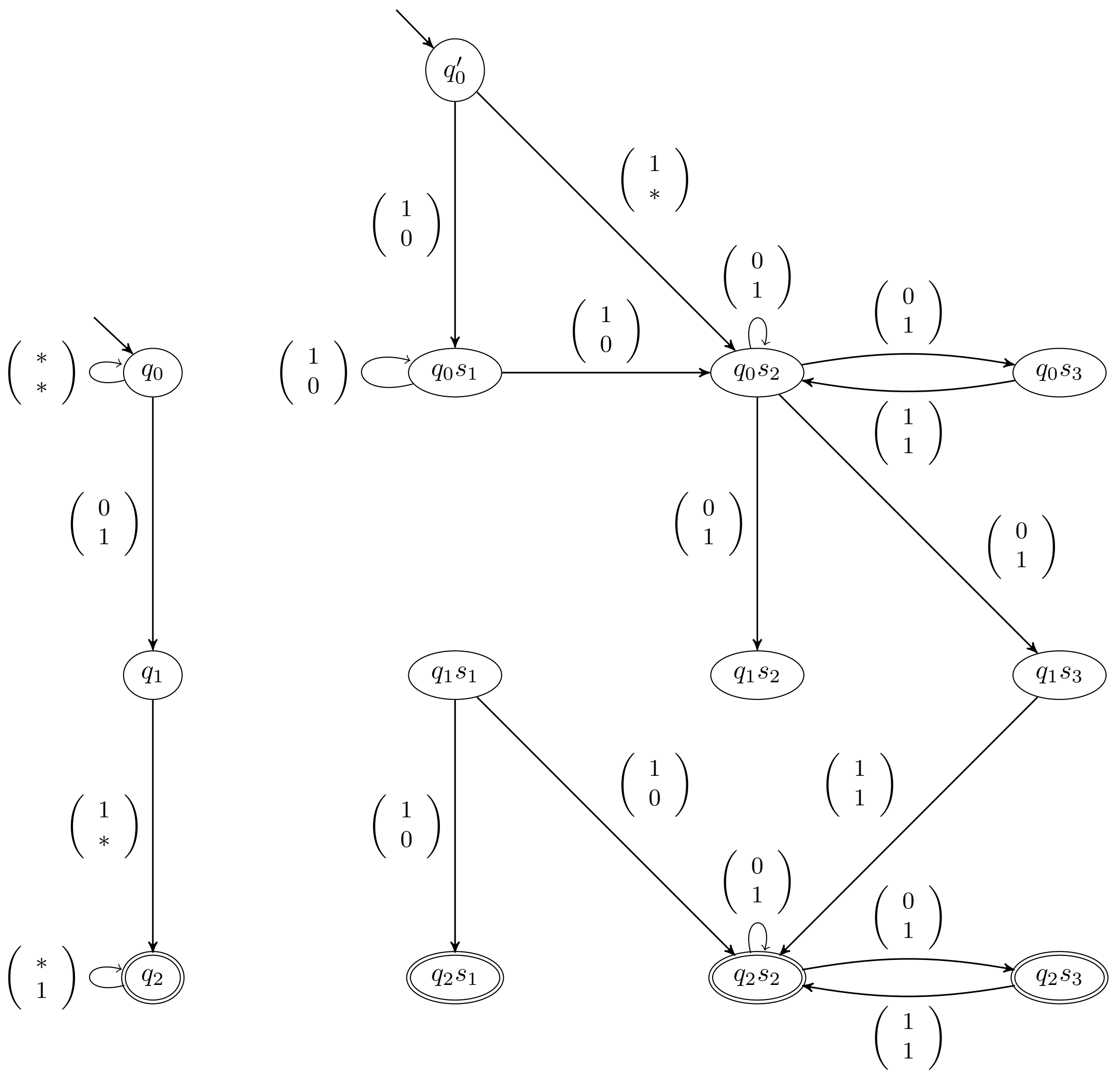
Since state 1 is initial and $1 \notin Sat(\Phi)$ we conclude $TS \not\models \Phi$.

First name	Last name	Matriculation number

Exercise 4 (18 + 1 points)

Consider the following NBA $\mathcal{A}$ and the following transition system TS.





- Construct the NBA $\mathcal{B} = TS \otimes \mathcal{A}$ which accepts $\mathcal{L}(TS) \cap \mathcal{L}(\mathcal{A})$.
- Is $\mathcal{L}(\mathcal{B}) = \varnothing$? If not, then provide a word which is contained in $\mathcal{L}(\mathcal{B})$.

$\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)^{\omega} \in \mathcal{L}(\mathcal{B})$.