University of Innsbruck — Institute of Computer Science
2nd exam — March 27, 2012

Introduction to Model Checking (VO) — WS 2011/2012 — 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.

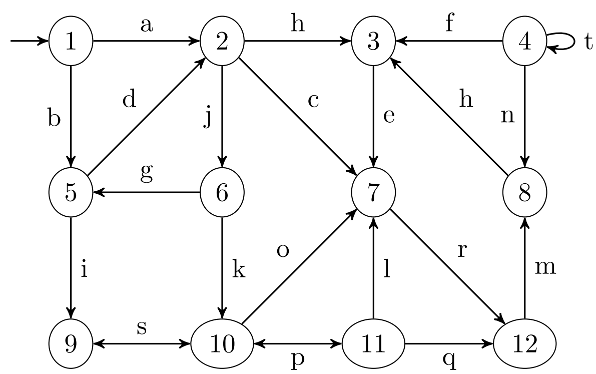
Exercise	Maximal points	Points
1	16	
2	10	
3	18	
4	16	
Σ	60	
Grade		

Exercise 1 (Büchi Automata, 8 + 8 points)

(i) Consider the GNBA $\mathcal{A}$ over $\Sigma = \{a, \dots, t\}$ where the 3 final state sets are

- $F_1 = \{n \in \mathbb{N} \mid n \leqslant 6\}$
- $F_2 = \{3n + 1 \mid n \in \mathbb{N}\}$
- $F_3 = \{n^2 \mid n \in \mathbb{N}\}$

and where the structure of the graph is as follows.

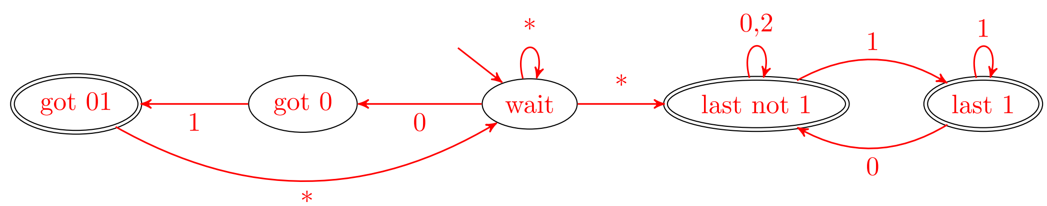


Use the algorithm to check emptyness of GNBAs to determine whether $\mathcal{L}(\mathcal{A}) = \varnothing$. If $\mathcal{L}(\mathcal{A}) \neq \varnothing$, also give an accepted word that the algorithm produces. Shortly explain your answer.

The SCCs of the graph are $\{2, 5, 6\}$, $\{9, 10, 11\}$, $\{3, 7, 8, 12\}$, and $\{4\}$ where all but $\{4\}$ are reachable. SCCs $\{2, 5, 6\}$ and $\{3, 7, 8, 12\}$ do not contain a state of F_3, and SCC $\{9, 10, 11\}$ does not contain a state of F_1. Hence, $\mathcal{L}(\mathcal{A}) = \varnothing$.

(ii) Let $\Sigma = \{0, 1, 2\}$. Formalize the following language over Σ as NBA.

$$\mathcal{L} = \{w \in \Sigma^\omega \mid w \text{ contains infinitely many often the sequence 01 or only finitely often the sequence 12}\}$$



Exercise 2 (Understanding LTL, 5 + 5 points)

Semantic entailment ($\models$) of LTL formulas is defined as

$$\varphi \models \psi \qquad \text{iff} \qquad \mathcal{L}(\varphi) \subseteq \mathcal{L}(\psi).$$

- Construct an algorithm to decide for given φ and ψ whether $\varphi \models \psi$ holds.
- Prove correctness of your algorithm.

- $\varphi \models \psi$ iff $\mathcal{L}(\neg(\varphi \Rightarrow \psi)) = \varnothing$. This algorithm is computable, since we can build a GNBA for $\neg(\varphi \Rightarrow \psi)$ and then check emptiness of this GNBA.
- $\varphi \models \psi$ iff $\mathcal{L}(\varphi) \subseteq \mathcal{L}(\psi)$ iff (for all w: $w \models \varphi$ implies $w \models \psi$) iff (for all w: $w \models \varphi \Rightarrow \psi$) iff (for no w: $w \models \neg(\varphi \Rightarrow \psi)$) iff $\mathcal{L}(\neg(\varphi \Rightarrow \psi)) = \varnothing$.

Exercise 3 (Automation of Model Checking, 18 points)

Consider the following formula:

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

Construct the automaton for φ using the improved translation.
$\mathcal{A}_\varphi = (\{q_0\} \uplus 2^6, 2^2, q_0, \delta, F_1, F_2, F_3)$ where

- The reduced Fischer Ladner closure is

$$cl'(\varphi) = \mathsf{push}, \mathsf{signal}, \underbrace{\text{true}\,\mathsf{U}\,\mathsf{signal}}_{\varphi_3}, \underbrace{\mathsf{X}\,\varphi_3}_{\varphi_4}, \underbrace{\text{true}\,\mathsf{U}\,(\mathsf{push} \wedge \varphi_4)}_{\varphi_5}, \text{true}\,\mathsf{U}\,\neg\varphi_5$$

- $(c_1, \ldots, c_6)^T \in \delta(q_0, (d_1, d_2)^T)$ iff $(c_1 \Leftrightarrow d_1) \wedge (c_2 \Leftrightarrow d_2) \wedge \neg c_6$

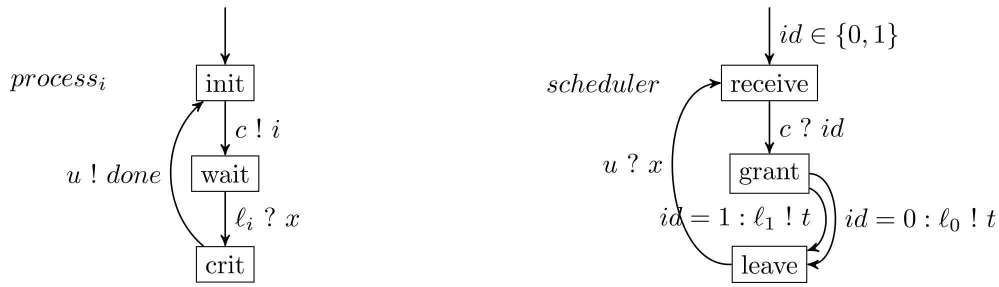
- $(c_1, \ldots, c_6)^T \in \delta((b_1, \ldots, b_6)^T, (d_1, d_2)^T)$ iff $(c_1 \Leftrightarrow d_1) \wedge (c_2 \Leftrightarrow d_2) \wedge (b_3 \Leftrightarrow b_2 \vee c_3) \wedge (b_4 \Leftrightarrow c_3) \wedge (b_5 \Leftrightarrow (b_1 \wedge b_4) \vee c_5) \wedge (b_6 \Leftrightarrow \neg b_5 \vee c_6)$

- $F_1 = \{(b_1, \ldots, b_6)^T \mid \neg b_3 \vee b_2\}$
  $F_2 = \{(b_1, \ldots, b_6)^T \mid \neg b_5 \vee (b_1 \wedge b_4)\}$
  $F_3 = \{(b_1, \ldots, b_6)^T \mid \neg b_6 \vee \neg b_5\}$

Compute the number of direct successor states of state $(0, 0, 0, 0, 0, 0)^T$. Simplifying the conditions yields *false*, hence there are no successor of this state.

Exercise 4 (Generation of Transition Systems, 16 points)

Consider the channel system $[process_0 \mid process_1 \mid scheduler]$ with $cap(\ell_0) = cap(\ell_1) = cap(c) = 0$ and $cap(u) = 1$ where for $process_i$ and $scheduler$ we have the following program graphs:

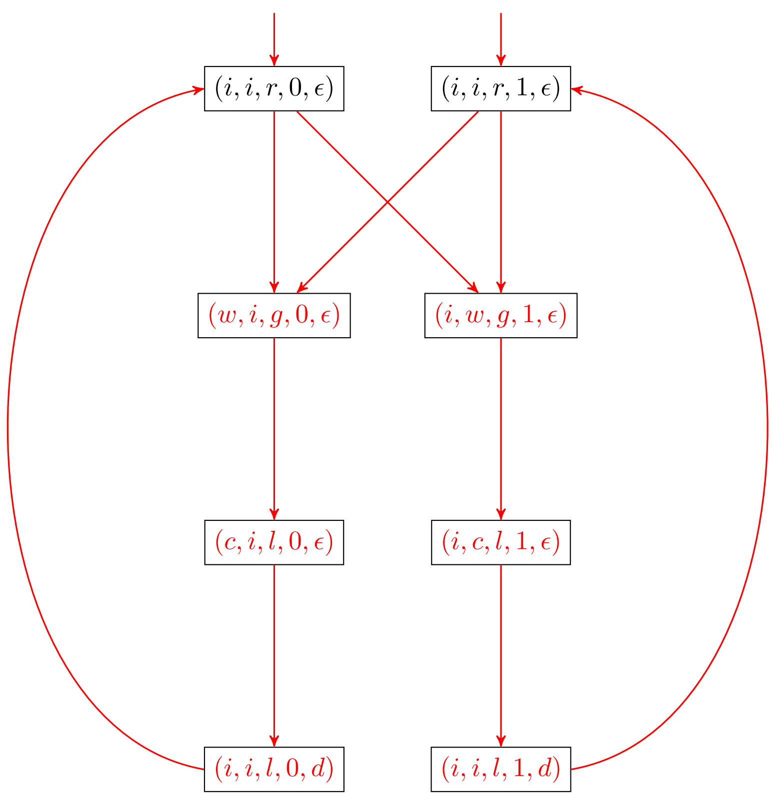


In the following diagram all reachable states for the corresponding transition system are given where the states are five-tuples of the following form:

(location process 0, location process 1, location scheduler, value of id, value of u)

Here, for the specification of states abbreviations like $(i, c, l, 1, \epsilon)$ are used for $(init, crit, leave, 1, \epsilon)$, etc.

- Insert all reachable states, insert all transitions, and mark initial states with an incoming edge.



- Which of the following properties does the channel system have?

(i) absence of deadlocks — yes ☑ no ☐

(ii) mutual exclusion — yes ☑ no ☐

(iii) fairness — yes ☐ no ☑

For your own notes