Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen
Christian Hensel, Matthias Volk

Introduction to Model Checking (Summer Term 2018)

— Exercise Sheet 8 (due 25th June) —

General Remarks

- The exercises are to be solved in groups of *three* students.
- You may hand in your solutions for the exercises just before the exercise class starts at 12:15 or by dropping them into the "Introduction to Model Checking" box at our chair *before 12:00*. Do *not* hand in your solutions via L2P or via e-mail.
- If a task asks you to justify your answer, an explanation of your reasoning is sufficient. If you are required to prove a statement, you need to give a *formal* proof.

General Notation

In the following we transform LTL formulae into the corresponding GNBAs. As an example consider the LTL formula $\varphi = a \mathsf{U} (\neg a \wedge b)$ from the lecture. We order the subformulae of φ from the innermost formulae to the outermost, and from left to right. In our example we get the subformulae a, b, $\neg a \wedge b$ and φ. The elementary sets are given in the following table where we order the sets by their binary encoding:

B	a	b	$\neg a \wedge b$	φ
B_1	0	0	0	0
B_2	0	1	1	1
B_3	1	0	0	0
B_4	1	0	0	1
B_5	1	1	0	0
B_6	1	1	0	1

Moreover, for the GNBA $\mathcal{G}_\varphi$ the transition relation can be given as a table where the rows and columns correspond to states of $\mathcal{G}_\varphi$ and the entries are either empty (representing "no transition") or contain an element from 2^{AP} (representing the character that can be used for the transition).

For example, an extract of the transition relation for the GNBA $\mathcal{G}_\varphi$ is given in the following.

	B_1	B_2	B_3	B_4	B_5	B_6
B_1	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
B_2			...			
B_3	$\{a\}$		$\{a\}$		$\{a\}$	
...			...			

Exercise 1★ (1+3+3 Points)

Let $\mathrm{AP} = \{a, b\}$. Let $\varphi = (a \rightarrow \bigcirc \neg b) \mathsf{W} (a \wedge b)$ as in exercise sheet 7.2.

(a) Transform $\neg\varphi$ into an equivalent LTL formula φ' (i.e., $\mathit{Words}(\neg\varphi) = \mathit{Words}(\varphi')$) which is constructed according to the following grammar:

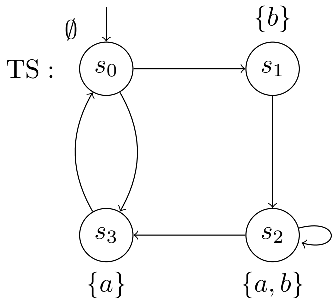
$$\varphi ::= \mathit{true} \mid \mathit{false} \mid a \mid b \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \mathsf{U} \varphi.$$

(b) Compute all elementary sets with respect to *closure*(φ').

(c) Construct the GNBA $\mathcal{G}_{\varphi'}$ according to the algorithm from the lecture such that $\mathcal{L}_\omega(\mathcal{G}_{\varphi'}) = \mathit{Words}(\varphi')$. It suffices to provide the initial states, the acceptance set and the transition relation of $\mathcal{G}_{\varphi'}$ as a table.

Exercise 2 (1+3+3+2+1+2 Points)

Let $\varphi = \Box(a \to ((\neg b) \,\mathsf{U}\, (a \wedge b)))$ over the set $AP = \{a, b\}$ of atomic propositions. We are interested in checking whether $\mathrm{TS} \models \varphi$ where TS is the following transition system:



(a) Convert $\neg\varphi$ into an equivalent LTL-formula ψ which is constructed according to the following grammar:

$$\varphi ::= \mathit{true} \mid \mathit{false} \mid a \mid b \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \,\mathsf{U}\, \varphi.$$

Derive *closure*(ψ).

(b) Give *all* elementary sets wrt. *closure*(ψ).

(c) Construct the GNBA $\mathcal{G}_\psi$ using the algorithm given in the lecture. It suffices to provide its initial states, its acceptance set and its transition relation.
Hint: Give the transition relation as a table where the rows and columns correspond to states of $\mathcal{G}_\psi$ and the entries are either empty (representing "no transition") or contain an element from 2^{AP} (representing the character that can be used for the transition).

(d) Now, construct a *non-blocking* NBA $\mathcal{A}_{\neg\varphi}$ **directly** from $\neg\varphi$, i.e. without relying on $\mathcal{G}_\psi$. Provide *an intuitive* explanation of why your automaton recognizes the right language. The latter is absolutely essential to earn points for this task.
Hint: Four states suffice. Consider rewriting $\neg\varphi$ using the release operator and recall that $\varphi \,\mathsf{R}\, \psi$ intuitively expresses that φ "releases" ψ. That is, ψ either holds all the time or at some point $\varphi \wedge \psi$ holds and at all previous positions ψ holds.

(e) Construct $\mathrm{TS} \otimes \mathcal{A}_{\neg\varphi}$.

(f) Apply the nested depth-first search (lecture 11, slides 150 and 159) to $\mathrm{TS} \otimes \mathcal{A}_{\neg\varphi}$ for the persistence property "eventually forever $\neg F$", where F is the acceptance set of $\mathcal{A}_{\neg\varphi}$. To illustrate the steps:

- before each *Pop* operation give:
  - for the first DFS the contents of stack π and set U, and
  - for the second DFS the contents of stack ξ and set V.
- indicate whenever *CYCLE_CHECK*(...) is called or returns a result (including the result itself).
- indicate when and which result the outer DFS returns.

Give the stack contents from left to right, in the sense that the topmost element is *on the right.* Does $\mathrm{TS} \models \varphi$ hold? In case the property is refuted, give the counterexample returned by the algorithm.

Exercise 3 (1 Points)

Let φ be an LTL-formula over a set of atomic propositions AP. Let $\mathcal{A} = (Q, 2^{\mathrm{AP}}, \delta, Q_0, \mathcal{F})$ be a GNBA for *Words*(φ) that is the result of the LTL-to-GNBA construction presented in the lecture applied to an LTL formula φ.

Prove that for all elementary sets $B \subseteq \mathit{closure}(\varphi)$ and for all $B' \in \delta(B, B \cap AP)$, it holds:

$$\neg \bigcirc \psi \in B \iff \psi \notin B'.$$