Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen

Christian Hensel, Matthias Volk

Introduction to Model Checking (Summer Term 2018)

— Solution 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 $\varphi = (a \to \bigcirc \neg b) \mathsf{W} (a \wedge b)$ 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 $closure(\varphi')$.

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

Solution:

(a) We transform $\neg\varphi$ into an equivalent LTL formula φ' similar to exercise 7.2:

$$
\begin{aligned}
& \neg\varphi \\
\equiv\ & \neg\big((a \rightarrow \bigcirc\neg b)\ \mathsf{W}\ (a \wedge b)\big) && \text{(* definition of } \varphi \text{ *)} \\
\equiv\ & \big((a \rightarrow \bigcirc\neg b) \wedge \neg(a \wedge b)\big)\ \mathsf{U}\ \big(\neg(a \rightarrow \bigcirc\neg b) \wedge \neg(a \wedge b)\big) && \text{(* duality of W and U *)} \\
\equiv\ & \big((\neg a \vee \bigcirc\neg b) \wedge \neg(a \wedge b)\big)\ \mathsf{U}\ \big(\neg(\neg a \vee \bigcirc\neg b) \wedge \neg(a \wedge b)\big) && \text{(* definition of } \rightarrow \text{ *)} \\
\equiv\ & \big((\neg a \vee \bigcirc\neg b) \wedge \neg(a \wedge b)\big)\ \mathsf{U}\ \big((a \wedge \neg\bigcirc\neg b) \wedge \neg(a \wedge b)\big) && \text{(* simplification *)} \\
\equiv\ & \big(\neg(a \wedge \neg\bigcirc\neg b) \wedge \neg(a \wedge b)\big)\ \mathsf{U}\ \big((a \wedge \neg\bigcirc\neg b) \wedge \neg(a \wedge b)\big) && \text{(* replace } \vee \text{ *)} \\
\equiv\ & \big(\neg(a \wedge \bigcirc b) \wedge \neg(a \wedge b)\big)\ \mathsf{U}\ \big((a \wedge \bigcirc b) \wedge \neg(a \wedge b)\big) && \text{(* duality of } \bigcirc \text{ *)}
\end{aligned}
$$

In the end

$$\varphi' = \big(\neg(a \wedge \bigcirc b) \wedge \neg(a \wedge b)\big)\ \mathsf{U}\ \big((a \wedge \bigcirc b) \wedge \neg(a \wedge b)\big)$$

(b) We denote:

$$
\begin{aligned}
\psi_1 &= a \wedge \bigcirc b \\
\psi_2 &= a \wedge b \\
\psi_3 &= \neg\psi_1 \wedge \neg\psi_2 \\
\psi_4 &= \psi_1 \wedge \neg\psi_2 \\
\varphi' &= \psi_3\ \mathsf{U}\ \psi_4
\end{aligned}
$$

We start by setting all possible combinations for “simple” subformulae:

#	a	b	$\bigcirc b$	$a \wedge \bigcirc b$ ψ_1	$a \wedge b$ ψ_2	$\neg\psi_1 \wedge \neg\psi_2$ ψ_3	$\psi_1 \wedge \neg\psi_2$ ψ_4	$\psi_3\ \mathsf{U}\ \psi_4$ φ'
1	0	0	0	0	0	1	0	x
2	0	0	1	0	0	1	0	x
3	0	1	0	0	0	1	0	x
4	0	1	1	0	0	1	0	x
5	1	0	0	0	0	1	0	x
6	1	0	1	1	0	0	1	x
7	1	1	0	0	1	0	0	x
8	1	1	1	1	1	0	0	x

Then we consider the first rule for local consistency for until formulae $\varphi_1\ \mathsf{U}\ \varphi_2$:

$$\varphi_2 \in B \Rightarrow \varphi_1\ \mathsf{U}\ \varphi_2 \in B$$

The result looks as follows:

#	a	b	$\bigcirc b$	$a \wedge \bigcirc b$ ψ_1	$a \wedge b$ ψ_2	$\neg\psi_1 \wedge \neg\psi_2$ ψ_3	$\psi_1 \wedge \neg\psi_2$ ψ_4	$\psi_3\ \mathsf{U}\ \psi_4$ φ'
1	0	0	0	0	0	1	0	x
2	0	0	1	0	0	1	0	x
3	0	1	0	0	0	1	0	x
4	0	1	1	0	0	1	0	x
5	1	0	0	0	0	1	0	x
6	1	0	1	1	0	0	1	1
7	1	1	0	0	1	0	0	x
8	1	1	1	1	1	0	0	x

Then we consider the second rule for local consistency for until formulae $\varphi_1 \mathsf{U} \varphi_2$:

$$\varphi_1 \mathsf{U} \varphi_2 \in B \text{ and } \varphi_2 \notin B \Rightarrow \varphi_1 \in B$$

The result looks as follows:

B	a	b	$\bigcirc b$	$a \wedge \bigcirc b$ ψ_1	$a \wedge b$ ψ_2	$\neg\psi_1 \wedge \neg\psi_2$ ψ_3	$\psi_1 \wedge \neg\psi_2$ ψ_4	$\psi_3 \mathsf{U} \psi_4$ φ'
B_1	0	0	0	0	0	1	0	0
B_2	0	0	0	0	0	1	0	1
B_3	0	0	1	0	0	1	0	0
B_4	0	0	1	0	0	1	0	1
B_5	0	1	0	0	0	1	0	0
B_6	0	1	0	0	0	1	0	1
B_7	0	1	1	0	0	1	0	0
B_8	0	1	1	0	0	1	0	1
B_9	1	0	0	0	0	1	0	0
B_{10}	1	0	0	0	0	1	0	1
B_{11}	1	0	1	1	0	0	1	1
B_{12}	1	1	0	0	1	0	0	0
B_{13}	1	1	1	1	1	0	0	0

Notice that three sets were removed because they were not locally consistent with respect to φ'.

In total, we have 13 elementary sets.

(c) The elementary sets form the states of the GNBA $\mathcal{G}_{\varphi'} = \left(Q, 2^{AP}, \delta, Q_0, \mathcal{F}\right)$. We have

$$\begin{aligned} Q &= \{B_1, \ldots, B_{13}\} \\ Q_0 &= \{B_2, B_4, B_6, B_8, B_{10}, B_{11}\} \\ \mathcal{F} &= \{F_{\psi_3 \mathsf{U} \psi_4}\}, \text{ where} \\ F_{\psi_3 \mathsf{U} \psi_4} &= \{B_1, B_3, B_5, B_7, B_9, B_{11}, B_{12}, B_{13}\} \end{aligned}$$

The transition relation is given as follows:

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}
B_1	$\emptyset$		$\emptyset$						$\emptyset$				
B_2		$\emptyset$		$\emptyset$						$\emptyset$	$\emptyset$		
B_3					$\emptyset$		$\emptyset$					$\emptyset$	$\emptyset$
B_4						$\emptyset$		$\emptyset$					
B_5	$\{b\}$		$\{b\}$						$\{b\}$				
B_6		$\{b\}$		$\{b\}$						$\{b\}$	$\{b\}$		
B_7					$\{b\}$		$\{b\}$					$\{b\}$	$\{b\}$
B_8						$\{b\}$		$\{b\}$					
B_9	$\{a\}$		$\{a\}$						$\{a\}$				
B_{10}		$\{a\}$		$\{a\}$						$\{a\}$	$\{a\}$		
B_{11}					$\{a\}$	$\{a\}$	$\{a\}$	$\{a\}$				$\{a\}$	$\{a\}$
B_{12}	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$					$\{a,b\}$	$\{a,b\}$	$\{a,b\}$		
B_{13}					$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$				$\{a,b\}$	$\{a,b\}$

Following the first rule $\bigcirc b \in B \implies b \in B'$ allows for the following transitions:

$$B_i \text{ with } i = 3, 4, 7, 8, 11, 13 \rightarrow B' \in \{B_5, B_6, B_7, B_8, B_{12}, B_{13}\}$$

Following the first rule $\bigcirc b \notin B \implies b \notin B'$ allows for the following transitions:

$$B_i \text{ with } i = 1, 2, 5, 6, 9, 10, 12 \rightarrow B' \in \{B_1, B_2, B_3, B_4, B_9, B_{10}, B_{11}\}$$

Following the second rule $\varphi_1 \mathsf{U} \varphi_2 \in B \implies (\varphi_2 \in B) \vee (\varphi_1 \in B \wedge \varphi_1 \mathsf{U} \varphi_2 \in B')$ allows for the following transitions:

$$B_i \text{ with } i = 2,4,6,8,10 \to B' \in \{B_2, B_4, B_6, B_8, B_{10}, B_{11}\} \text{ and } B_{11} \to B' \in \{B_1, ..., B_{13}\}$$

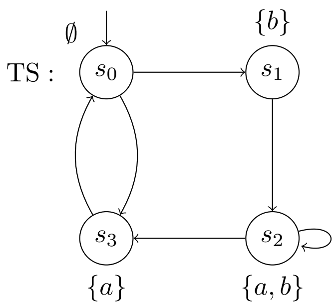
Following the second rule $\varphi_1 \mathsf{U} \varphi_2 \notin B \implies (\varphi_2 \notin B) \wedge (\varphi_1 \notin B \vee \varphi_1 \mathsf{U} \varphi_2 \notin B')$ allows for the following transitions:

$$B_i \text{ with } i = 1,3,5,7,9 \implies B' \in \{B_1, B_3, B_5, B_7, B_9, B_{12}, B_{13}\} \text{ and } B_{12}, B_{13} \to B' \in \{B_1, ..., B_{13}\}$$

The final transitions are the *intersection* of the transitions that are allowed by the first *and* the second rule for each elementary set B.

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

Let $\varphi = \square (a \to ((\neg b) \mathsf{U} (a \wedge b)))$ 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 $\mathit{closure}(\psi)$.

(b) Give *all* elementary sets wrt. $\mathit{closure}(\psi)$.

(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 TS $\models \varphi$ hold? In case the property is refuted, give the counterexample returned by the algorithm.

Solution:

(a)

$$\begin{aligned}
\neg\varphi &= \neg\Box\,(a \rightarrow (\neg b \mathbin{\mathsf{U}} (a \wedge b))) \\
&\equiv \Diamond\,\neg(\neg a \vee (\neg b \mathbin{\mathsf{U}} (a \wedge b))) \\
&\equiv \Diamond\,(a \wedge \neg(\neg b \mathbin{\mathsf{U}} (a \wedge b))) \\
&\equiv \underbrace{\mathit{true} \mathbin{\mathsf{U}} (a \wedge \neg(\neg b \mathbin{\mathsf{U}} (a \wedge b)))}_{\psi}
\end{aligned}$$

We then compute the closure:

$$\begin{aligned}
\mathit{closure}(\psi) = \{\, & \mathit{true}, \mathit{false}, a, \neg a, b, \neg b \\
& a \wedge b, \neg(a \wedge b), \neg b \mathbin{\mathsf{U}} (a \wedge b), \neg(\neg b \mathbin{\mathsf{U}} (a \wedge b)), \\
& a \wedge \neg(\neg b \mathbin{\mathsf{U}} (a \wedge b)), \neg(a \wedge \neg(\neg b \mathbin{\mathsf{U}} (a \wedge b))), \psi, \neg\psi \,\}
\end{aligned}$$

(b) We let

$$\begin{aligned}
\psi_1 &= (a \wedge b) \\
\psi_2 &= \neg b \mathbin{\mathsf{U}} (a \wedge b) = \neg b \mathbin{\mathsf{U}} \psi_1 \\
\psi_3 &= a \wedge \neg(\neg b \mathbin{\mathsf{U}} (a \wedge b)) = a \wedge \neg\psi_2 \\
\psi_4 &= \mathit{true} \mathbin{\mathsf{U}} \psi_3
\end{aligned}$$

The elementary sets are as follows:

	a	b	$a \wedge b$ ψ_1	$\neg b \mathbin{\mathsf{U}} \psi_1$ ψ_2	$a \wedge \neg\psi_2$ ψ_3	$\mathit{true} \mathbin{\mathsf{U}} \psi_3$ ψ
B_1	0	0	0	0	0	0
B_2	0	0	0	0	0	1
B_3	0	0	0	1	0	0
B_4	0	0	0	1	0	1
B_5	0	1	0	0	0	0
B_6	0	1	0	0	0	1
B_7	1	0	0	0	1	1
B_8	1	0	0	1	0	0
B_9	1	0	0	1	0	1
B_{10}	1	1	1	1	0	0
B_{11}	1	1	1	1	0	1

(c) The elementary sets form the states of the GNBA $\mathcal{G}_{\neg\varphi} = \big(Q, 2^{AP}, \delta, Q_0, \mathcal{F}\big)$. We have

$$\begin{aligned}
Q &= \{B_1, \ldots, B_{11}\} \\
Q_0 &= \{B_2, B_4, B_6, B_7, B_9, B_{11}\} \\
\mathcal{F} &= \big\{F_{\neg b \mathbin{\mathsf{U}} (a \wedge b)}, F_{\psi}\big\}, \text{ where} \\
F_{\neg b \mathbin{\mathsf{U}} (a \wedge b)} &= \{B_1, B_2, B_5, B_6, B_7, B_{10}, B_{11}\} \\
F_{\psi} &= \{B_1, B_3, B_5, B_7, B_8, B_{10}\}
\end{aligned}$$

The transition relation is given as follows:

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}
B_1	$\emptyset$				$\emptyset$						
B_2		$\emptyset$				$\emptyset$	$\emptyset$				
B_3			$\emptyset$					$\emptyset$		$\emptyset$	
B_4				$\emptyset$					$\emptyset$		$\emptyset$
B_5	$\{b\}$		$\{b\}$		$\{b\}$			$\{b\}$		$\{b\}$	
B_6		$\{b\}$		$\{b\}$		$\{b\}$	$\{b\}$		$\{b\}$		$\{b\}$
B_7	$\{a\}$	$\{a\}$			$\{a\}$	$\{a\}$	$\{a\}$				
B_8			$\{a\}$					$\{a\}$		$\{a\}$	
B_9				$\{a\}$					$\{a\}$		$\{a\}$
B_{10}	$\{a,b\}$		$\{a,b\}$		$\{a,b\}$			$\{a,b\}$		$\{a,b\}$	
B_{11}		$\{a,b\}$		$\{a,b\}$		$\{a,b\}$	$\{a,b\}$		$\{a,b\}$		$\{a,b\}$

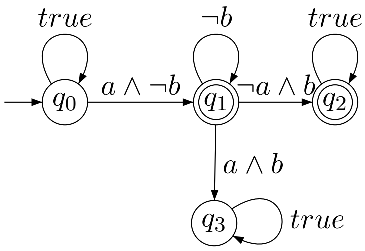
(d) We rewrite $\neg\varphi$ as follows:

$$\begin{aligned}\neg\varphi &\equiv \neg\Box\,(a \to (\neg b \,\mathsf{U}\, (a \wedge b)))\\ &\equiv \Diamond\,\neg(\neg a \vee (\neg b \,\mathsf{U}\, (a \wedge b)))\\ &\equiv \Diamond\,(a \wedge \neg(\neg b \,\mathsf{U}\, (a \wedge b)))\\ &\equiv \Diamond\,\underbrace{(a \wedge \underbrace{(b \,\mathsf{R}\, (\neg a \vee \neg b))}_{\psi_1})}_{\psi}\end{aligned}$$

In particular, we have

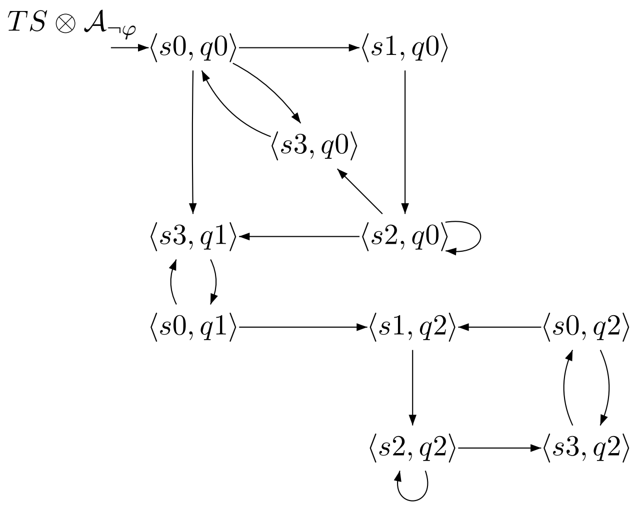
$$\begin{aligned}&(b \,\mathsf{R}\, (\neg a \vee \neg b))\\ &\equiv \Box\,(\neg a \vee \neg b) \vee \Big((\neg a \vee \neg b)\ \mathsf{U}\ \big(b \wedge (\neg a \vee \neg b)\big)\Big)\\ &\equiv \underbrace{\Box\,(\neg a \vee \neg b)}_{\psi_2} \vee \underbrace{\Big((\neg a \vee \neg b)\ \mathsf{U}\ (\neg a \wedge b)\Big)}_{\psi_3}\end{aligned}$$

From this form, we construct the NBA $\mathcal{A}_{\neg\varphi}$ that recognizes $Words(\neg\varphi)$ as follows:



The underlying idea is as follows. For an infinite word $\sigma = A_0A_1\ldots$, the automaton nondeterministically guesses the position i such that $A_iA_{i+1}\ldots \models \psi$ holds and loops in the first state q_0 until that point. In particular $A_iA_{i+1}\ldots \models \psi_1$ and therefore $a \in A_i$ and also $A_iA_{i+1}\ldots \models \psi_1$ and therefore $A_iA_{i+1}\ldots \models \psi_2 \vee \psi_3$. As $a \in A_i$, both ψ_2 and ψ_3 imply that $b \notin A_i$. Therefore, the transition from q_0 to q_1 requires $a \wedge \neg b$. If in q_1, we have already seen an a and only require ψ_1, or equivalently, $\psi_2 \vee \psi_3$ from this point on. Seeing $a \wedge b$ violates both disjuncts of $\psi_2 \vee \psi_3$ and therefore the corresponding transition leads into a trap state since no such word is accepted. Similarly, seeing $\neg a \wedge b$ makes the word satisfy ψ_3 and the corresponding transition leads into a state q_2 from which every continuation of the word is accepted. Finally, seeing $\neg b$ in q_1 leads back to q_1 itself as this intuitively delays the decision if the word is to be expected by one position. That is, after seeing any number of $\neg b$, the word may still satisfy $\psi_2 \vee \psi_3$ (by either looping in q_2 forever or seeing $\neg a \wedge b$) but may also still violate it (by seeing an $a \wedge b$).

(e) The product transition system $\mathrm{TS} \otimes \mathcal{A}_{\neg\varphi}$ is depicted below:



(f) To prove $\text{TS} \not\models \varphi$, we check the persistence property P_{pers} = "eventually forever $\neg\Phi$" where $\Phi = q_1 \vee q_2$ on the product transition system $\text{TS} \otimes \mathcal{A}_{\neg\varphi}$. Using the nested depth-first search algorithm, we search for a reachable cycle in the product containing at least one state whose second component corresponds to an accepting state in $\mathcal{A}_{\neg\varphi}$. We denote the stack content from *left to right* in the sense that the top element is on the right. The algorithm then proceeds as follows.

- Initial state (1st DFS): $\langle s_0, q_0\rangle$

$$\begin{aligned}
\pi &= \langle s_0, q_0\rangle\langle s_3, q_1\rangle\langle s_0, q_1\rangle\langle s_1, q_2\rangle\langle s_2, q_2\rangle\langle s_3, q_2\rangle\langle s_0, q_2\rangle \\
U &= \{\langle s_0, q_0\rangle, \langle s_3, q_1\rangle, \langle s_0, q_1\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_0, q_2\rangle\} \\
\xi &= \varepsilon \\
V &= \emptyset
\end{aligned}$$

  State $\langle s_3, q_2\rangle$ is popped from π as all its successors ($\langle s_1, q_2\rangle$ and $\langle s_3, q_2\rangle$) are already in U.

- We have $\langle s_0, q_2\rangle \not\models \neg\Phi$ and therefore $CYCLE\_CHECK(s_0, q_2)$ is invoked.
- Initial state (2nd DFS): $\langle s_0, q_2\rangle$

$$\begin{aligned}
\pi &= \langle s_0, q_0\rangle\langle s_3, q_1\rangle\langle s_0, q_1\rangle\langle s_1, q_2\rangle\langle s_2, q_2\rangle\langle s_3, q_2\rangle \\
U &= \{\langle s_0, q_0\rangle, \langle s_3, q_1\rangle, \langle s_0, q_1\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_0, q_2\rangle\} \\
\xi &= \langle s_0, q_2\rangle\langle s_3, q_2\rangle \\
V &= \{\langle s_0, q_2\rangle, \langle s_3, q_2\rangle\}
\end{aligned}$$

  Since $\langle s_0, q_2\rangle \in \text{Post}(\langle s_3, q_2\rangle)$, $CYCLE\_CHECK(s_0, q_2)$ returns true.

- The outer DFS returns "no" and we conclude that $\text{TS} \not\models \varphi$. Additionally, the nested DFS algorithm returns the following counterexample (to be read from left to right)

$$reverse(\pi, \xi) = \underbrace{\langle s_0, q_0\rangle\langle s_3, q_1\rangle\langle s_0, q_1\rangle\langle s_1, q_2\rangle\langle s_2, q_2\rangle\langle s_3, q_2\rangle}_{reverse(\pi)}\underbrace{\langle s_0, q_2\rangle\langle s_3, q_2\rangle}_{reverse(\xi)}$$

Exercise 3 (1 Points)

Let φ be an LTL-formula over a set of atomic propositions AP. Let $\mathcal{A} = (Q, 2^{\text{AP}}, \delta, Q_0, \mathcal{F})$ be a GNBA for $Words(\varphi)$ 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 $B \subseteq closure(\varphi)$ and for all $B' \in \delta(B, B \cap AP)$, it holds:

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

Solution:

According to the definition of the transition function δ, it is:

$$\bigcirc\psi \in B \iff \psi \in B', \tag{8.1}$$

which is equivalent to

$$\bigcirc\psi \notin B \iff \psi \notin B'. \tag{8.2}$$

By the maximality constraint, we have

$$\bigcirc\ \psi \notin B \Rightarrow \neg\bigcirc\ \psi \in B. \tag{8.3}$$

Finally, by local consistency with respect to negation, we have

$$\neg\bigcirc\ \psi \in B \Rightarrow \bigcirc\psi \notin B \tag{8.4}$$

We can conclude

$$\neg\bigcirc\ \psi \in B \overset{(8.3+8.4)}{\iff} \bigcirc\psi \notin B \overset{(8.4)}{\iff} \psi \notin B'.$$