Technische Universität München (I7)
J. Křetínský / M. Azeem / K. Grover

Summer Semester 2022
23.05.2022

Model Checking – Exercise sheet 4

Exercise 4.1

Using the *Compare* feature in Spot (`https://spot.lrde.epita.fr/app`) give an LTL formula equivalent to

(a) $p \,\mathbf{R}\, q$, which does not contain $\neg$ but may contain $\mathbf{U}, \mathbf{G}$ or $\mathbf{F}$.

(b) $(\mathbf{G}p)\,\mathbf{U}\,q$ which does not contain $\mathbf{U}$.

(c) $(\mathbf{F}p)\,\mathbf{U}\,q$, which does not contain $\mathbf{U}$.

Exercise 4.2

Given the following Kripke structures and LTL formulae, answer the following questions

(a) Which of $\mathcal{K}_1, \mathcal{K}_2$ and $\mathcal{K}_3$ satisfy $\phi = \mathbf{G}(\mathbf{X}q \rightarrow p)$?

(b) Give an LTL formula which exactly characterizes $\mathcal{K}_3$, i.e. both the formula and the Kripke structure accept exactly the same words.

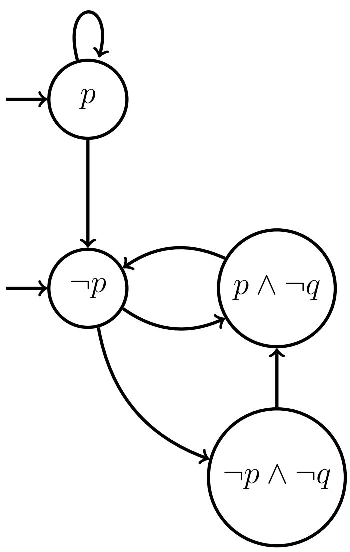


Figure 1: $\mathcal{K}_1$

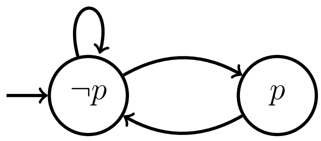


Figure 2: $\mathcal{K}_2$

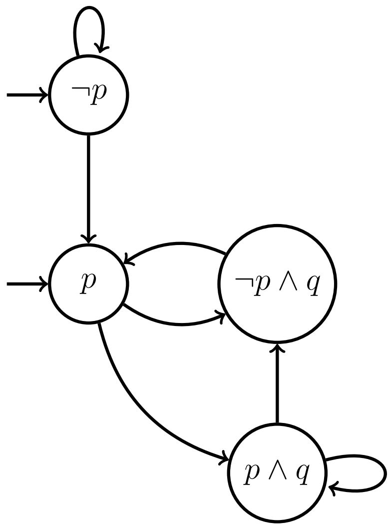
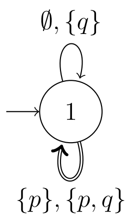


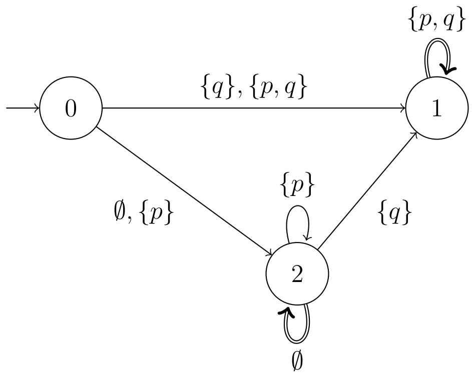
Figure 3: $\mathcal{K}_3$

Exercise 4.3
Convert the following Büchi automata with transition-based acceptance condition ("doubled"-transitions have to be seen infinitely often) to equivalent Büchi automata with state-based acceptance conditions. Moreover, give a general procedure to perform this conversion.

(a)



(b)



Exercise 4.4

Extend the set of rules of the LTL to Büchi automata translation to directly deal with the $\mathbf{F}$ and $\mathbf{G}$ operators.

Exercise 4.5

Let $\phi = \mathbf{G}\left((\mathbf{X}(p \; \mathbf{U} \; q)) \rightarrow ((\neg p \land \mathbf{F}q) \lor (q \; \mathbf{U} \; \mathbf{X}q))\right)$ and $\mathcal{G}$ be a generalized Büchi automaton translated from ϕ using the construction presented in the lecture and the extended set of rules defined in the previous exercise.

(a) Write down the set of subformulae $Sub(\phi)$.

(b) What is the size of $CS(\phi)$?

(c) How many sets of accepting states does $\mathcal{G}$ have?

(d) Is $\{\phi\}$ an accepting state of $\mathcal{G}$?

(e) Give a reachable state that has no successors.

(f) Give a successor state of the smallest consistent state containing $\{\phi, q, q \; \mathbf{U} \; \mathbf{X}q, \mathbf{F}q\}$.

(g) Give a predecessor state of the smallest consistent state containing $\{\phi, q, q \; \mathbf{U} \; \mathbf{X}q, \mathbf{F}q\}$.

Solution 4.1

(a) $(q\ \mathbf{U}\ (p \wedge q)) \vee \mathbf{G}q$

(b) $(\mathbf{F}q \wedge \mathbf{G}p) \vee q$.

(c) $q \vee \mathbf{F}(\mathbf{F}p \wedge \mathbf{X}q)$ or
another longer solution: $\mathbf{F}(q \wedge \mathbf{F}p) \vee \mathbf{F}(p \wedge \mathbf{X}q) \vee \mathbf{G}q \vee q$

Solution 4.2

(a) $\mathcal{K}_1$

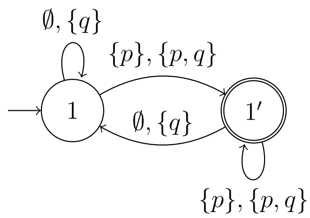
(b) $\mathbf{G}\neg p \vee (\neg p\ \ \mathbf{U}\ \ \mathbf{G}(p \to \mathbf{X}q\ \ \wedge\ \ \neg p \to \mathbf{X}p))$

Solution 4.3

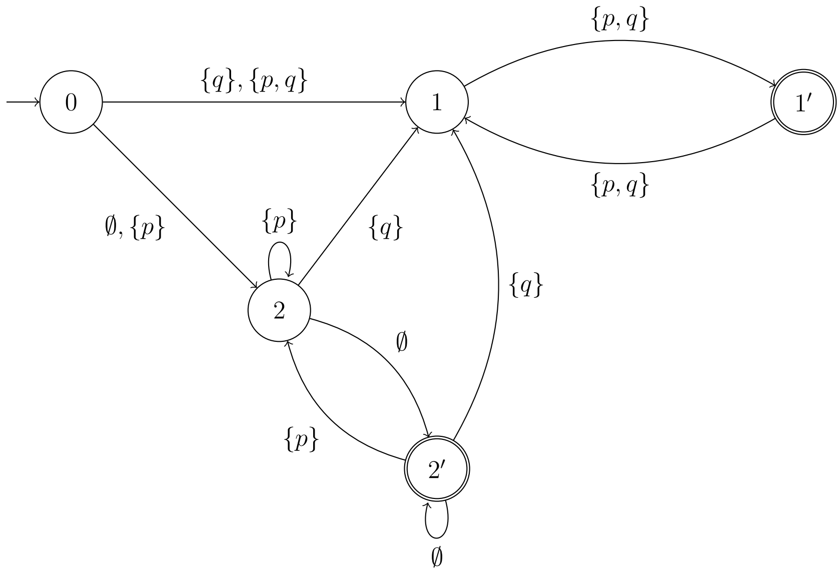
The general procedure is as follows.

Let the states of the original automaton be relabeled to $S \times \{1\}$ and create a copy of the states labeled by $S \times \{2\}$. For every accepting transition from $(s_1, 1) \to (s_2, 1)$, change the destination to $(s_2, 2)$. For every non-accepting transition from $(s_1, 2) \to (s_2, 2)$, change the destination to $(s_2, 1)$.

(a)



(b)



Solution 4.4
Extend the definition of NNF to include $\mathbf{F}$ and $\mathbf{G}$, extend the corresponding $Sub(\phi)$:

- if $\mathbf{F}\phi_1 \in Sub(\phi)$ then $\phi_1 \in Sub(\phi)$
- if $\mathbf{G}\phi_1 \in Sub(\phi)$ then $\phi_1 \in Sub(\phi)$,

and extend rules for transitions as follows: $(M, \sigma, M') \in \Delta$ iff $\sigma = M \cap AP$ and

- if $\mathbf{F}\phi_1 \in Sub(\phi)$, then $\mathbf{F}\phi_1 \in M$ iff $\phi_1 \in M$ or $\mathbf{F}\phi_1 \in M'$
- if $\mathbf{G}\phi_1 \in Sub(\phi)$, then $\mathbf{G}\phi_1 \in M$ iff $\phi_1 \in M$ and $\mathbf{G}\phi_1 \in M'$

Also, the acceptance condition must be extended for $\mathbf{F}$: $\mathcal{F}$ contains a set F_ψ, for every subformula ψ of the form $\mathbf{F}\phi_1$, where

$$F_\psi = \{M \in CS(\phi) \mid \phi_1 \in M \text{ or } \neg(\mathbf{F}\phi_1) \in M\}$$

Solution 4.5
Translate ϕ into an NNF formula:

$$\begin{aligned} \phi &= \mathbf{G}\left((\mathbf{X}(p\ \mathbf{U}\ q)) \rightarrow ((\neg p \wedge \mathbf{F}q) \vee (q\ \mathbf{U}\ \mathbf{X}q))\right) \\ &\equiv \mathbf{G}\left((\mathbf{X}(\neg p\ \mathbf{R}\ \neg q)) \vee ((\neg p \wedge \mathbf{F}q) \vee (q\ \mathbf{U}\ \mathbf{X}q))\right) \end{aligned}$$

(a) Let $\phi_1 = \neg p\ \mathbf{R}\ \neg q$, $\phi_2 = \neg p \wedge \mathbf{F}q$, and $\phi_3 = q\ \mathbf{U}\ \mathbf{X}q$. We have $\phi = \mathbf{G}(\mathbf{X}\phi_1 \vee (\phi_2 \vee \phi_3))$ and $Sub(\phi) = \{\mathbf{true}, \phi, \mathbf{X}\phi_1 \vee (\phi_2 \vee \phi_3), \mathbf{X}\phi_1, \phi_2 \vee \phi_3, \phi_1, \phi_2, \phi_3, \mathbf{F}q, \mathbf{X}q, p, q\} \cup \{\mathbf{false}, \neg\phi, \neg(\mathbf{X}\phi_1 \vee (\phi_2 \vee \phi_3)), \neg\mathbf{X}\phi_1, \neg(\phi_2 \vee \phi_3), \neg\phi_1, \neg\phi_2, \neg\phi_3, \neg\mathbf{F}q, \neg\mathbf{X}q, \neg p, \neg q\}$.

(b) Only $\phi, \mathbf{X}\phi_1, \phi_1, \phi_3, \mathbf{F}q, \mathbf{X}q, p, q$ can independently form consistent states. So, $|CS(\phi)| = 2^8 = 256$ states

(c) $\mathcal{F} = \{F_{q\mathbf{UX}q}, F_{\mathbf{F}q}\}$

(d) $\{\phi\} \in F_{q\mathbf{UX}q}$ and $\{\phi\} \in F_{\mathbf{F}q}$

(e) $\{\phi\}$ is reachable because it is an initial state, and it has no successors because $\mathbf{X}\phi_1 \vee (\phi_2 \vee \phi_3) \notin \{\phi\}$.

(f) $\{\phi, q\ \mathbf{U}\ \mathbf{X}q\}$

(g) $\{\phi, q\ \mathbf{U}\ \mathbf{X}q, \mathbf{F}q, \mathbf{X}q\}$