Technische Universität München (I7) **Summer Semester 2022**
Jan Křetínský / M. Azeem / K. Grover **16.05.2022**

Model Checking – Exercise sheet 3

Exercise 3.1

There are two traffic lights at a road intersection, and they can either be `red` or `green`. Does the formula $\mathbf{G}[(t_1 = \texttt{red} \wedge t_2 = \texttt{green}) \vee (t_1 = \texttt{green} \wedge t_2 = \texttt{red})]$ specify that 'both of the lights should not be green at a given time'? If it does, give an accepting run, otherwise give a counterexample and the correct formula. Also, write an LTL formula that says 'Both of the lights become green infinitely many times'.

Exercise 3.2

You are on your quest to bring balance to the galaxy. You have a plan but you want to be sure that it works and therefore decided to use model checking. Your model is ready but now you need to write an LTL formula which specifies that you save the galaxy i.e. killing Darth Vader before dying and whenever you find a death star, destroy it.
Atomic propositions used in the model:

- f : Found a death star.
- d : Destroy a death star.
- k : Kill Darth Vader.
- a : You are alive.

Exercise 3.3

Let $\varphi = \mathbf{FG}p \rightarrow \mathbf{GF}(q \vee r)$ and $\psi = \neg(r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg\mathbf{XX}s)$ be LTL formulas over the atomic propositions $AP = \{p, q, r, s\}$. Say whether the following sequences satisfy φ and ψ. Justify your answers.

(a) $\emptyset^\omega$

(b) $\{p, q, r, s\}^\omega$

(c) $\{p\}^\omega$

(d) $\{r\}\emptyset\{p, q, s\}^\omega$

(e) $\{r\}\emptyset\{p\}\{q, r\}(\{p, s\}\emptyset)^\omega$

(f) $\{q, r\}\emptyset\{p, q\}\emptyset\{r, s\}^\omega$

Exercise 3.4

Let $AP = \{s, r, g\}$ be actions of a process: **s**ending a message, **r**eceiving a message, and **g**iving a result, respectively. Specify the following properties in LTL, and give example sequences that satisfy and violate the formulas.

(a) The process always gives a result.

(b) The process stops communicating after giving its result.

(c) The process only gives a result once.

(d) The process does nothing until it receives a message.

Exercise 3.5

Let $AP = \{p, q\}$. An LTL formula is a tautology if it is satisfied by all sequences over 2^{AP}. Which of the following LTL formulas are tautologies? Justify each answer with a counterexample or a proof.

(a) $\mathbf{G}p \rightarrow \mathbf{F}p$

(b) $\mathbf{G}(p \rightarrow q) \rightarrow (\mathbf{G}p \rightarrow \mathbf{G}q)$

(c) $\mathbf{FG}p \vee \mathbf{FG}\neg p$

(d) $\neg\mathbf{F}p \rightarrow \mathbf{F}\neg\mathbf{F}p$

(e) $\neg(p \mathbin{\mathbf{U}} q) \leftrightarrow (\neg p \mathbin{\mathbf{U}} \neg q)$

(f) $(\mathbf{G}p \rightarrow \mathbf{F}q) \leftrightarrow (p \mathbin{\mathbf{U}} (p \vee q))$

Exercise 3.6

Let $AP = \{p, q\}$ and let $\Sigma = 2^{AP}$. Give Büchi automata recognizing the ω-languages over Σ defined by the following LTL formulas:

(a) $\mathbf{XG}\neg p$

(b) $(\mathbf{GF}p) \rightarrow (\mathbf{F}q)$

(c) $p \wedge \neg(\mathbf{XF}p)$

(d) $\mathbf{G}(p \mathbin{\mathbf{U}} (p \rightarrow q))$

(e) $\mathbf{F}q \rightarrow (\neg q \mathbin{\mathbf{U}} (\neg q \wedge p))$

Solution 3.1

Counter example: $\{t_1 = red, t_2 = red\}^\omega$
Correct formula: $\neg\mathbf{F}(t_1 = green \wedge t_2 = green) \equiv \mathbf{G}(t_1 = red \vee t_2 = red)$
LTL formula for the other property: $\mathbf{GF}(t_1 = green) \wedge \mathbf{GF}(t_2 = green)$

Solution 3.2

$\mathbf{G}(a \wedge f \rightarrow a \wedge \mathbf{X}d) \wedge (a \;\mathbf{U}\; k)$

Solution 3.3

(a)
- $\emptyset^\omega \models \mathbf{FG}p \rightarrow \mathbf{GF}(q \vee r)$ since $\emptyset^\omega \not\models \mathbf{FG}p$ which follows from the fact that p does not occur at all.
- $\emptyset^\omega \not\models \neg(r \;\mathbf{U}\; \mathbf{X}p) \;\mathbf{U}\; (q \wedge \neg\mathbf{XX}s)$ since q never holds.

(b)
- $\{p, q, r, s\}^\omega \models \mathbf{FG}p \rightarrow \mathbf{GF}(q \vee r)$ since p always occurs and q occurs infinitely often.
- $\{p, q, r, s\}^\omega \not\models \neg(r \;\mathbf{U}\; \mathbf{X}p) \;\mathbf{U}\; (q \wedge \neg\mathbf{XX}s)$ since $\neg\mathbf{XX}s$ never holds.

(c)
- $\{p\}^\omega \not\models \mathbf{FG}p \rightarrow \mathbf{GF}(q \vee r)$ since $\{p\}^\omega \models \mathbf{FG}p$ but $\{p\}^\omega \not\models \mathbf{GF}(q \vee r)$. The former follows from the fact that p occurs infinitely often, and the latter from the fact that q and r never occur.
- $\{p\}^\omega \not\models \neg(r \;\mathbf{U}\; \mathbf{X}p) \;\mathbf{U}\; (q \wedge \neg\mathbf{XX}s)$ since q never occurs.

(d)
- $\{r\}\emptyset\{p, q, s\}^\omega \models \mathbf{FG}p \rightarrow \mathbf{GF}(q \vee r)$ since p eventually always occurs and q occurs infinitely often.
- $\{r\}\emptyset\{p, q, s\}^\omega \not\models \neg(r \;\mathbf{U}\; \mathbf{X}p) \;\mathbf{U}\; (q \wedge \neg\mathbf{XX}s)$ since $(q \wedge \neg\mathbf{XX}s)$ never holds.

(e)
- $\{r\}\emptyset\{p\}\{q, r\}(\{p, s\}\emptyset)^\omega \models \mathbf{FG}p \rightarrow \mathbf{GF}(q \vee r)$ since p does not occur eventually always.
- $\{r\}\emptyset\{p\}\{q, r\}(\{p, s\}\emptyset)^\omega \not\models \neg(r \;\mathbf{U}\; \mathbf{X}p) \;\mathbf{U}\; (q \wedge \neg\mathbf{XX}s)$ since $\neg(r \;\mathbf{U}\; \mathbf{X}p)$ and $q \wedge \neg\mathbf{XX}s$ does not hold at the first position.

(f)
- $\{q, r\}\emptyset\{p, q\}\emptyset\{r, s\}^\omega \models \mathbf{FG}p \to \mathbf{GF}(q \vee r)$ since p does not occur eventually always.
- $\{q, r\}\emptyset\{p, q\}\emptyset\{r, s\}^\omega \models \neg(r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg\mathbf{XX}s)$ since $q \wedge \neg\mathbf{XX}s$ already holds at the first position, i.e. q occurs at the first position and s does not occur at the third position.

Solution 3.4

In the following table, σ and σ' are two example sequences such that $\sigma \models \varphi$ and $\sigma' \not\models \varphi$.

	φ	σ	σ'
(a)	$\mathbf{F}g$	$\{g\}\emptyset^\omega$	$\emptyset^\omega$
(b)	$\mathbf{G}(g \to \mathbf{G}(\neg s \wedge \neg r))$	$\{g\}\emptyset^\omega$	$\{g, s\}\emptyset^\omega$
	or if "after" is strict		
	$\mathbf{G}(g \to \mathbf{XG}(\neg s \wedge \neg r))$	$\{g\}\emptyset^\omega$	$\{g\}\{s\}\emptyset^\omega$
(d)	$\mathbf{F}g \wedge \mathbf{G}(g \to \mathbf{XG}\neg g)$	$\{g\}\emptyset^\omega$	$\{g\}\{g\}\emptyset^\omega$
(f)	$(\neg s \wedge \neg g) \ \mathbf{W} \ r$	$\{r\}\{g\}^\omega$	$\{g\}^\omega$

Solution 3.5

(a) $\mathbf{G}p \to \mathbf{F}p$ is a tautology since

$$\begin{aligned}
\mathbf{G}p \to \mathbf{F}p &\equiv \neg\mathbf{F}\neg p \to \mathbf{F}p \\
&\equiv \mathbf{F}\neg p \vee \mathbf{F}p \\
&\equiv \mathbf{F}(\neg p \vee p) \\
&\equiv \mathbf{F}\, true \\
&\equiv true.
\end{aligned}$$

(b) $\mathbf{G}(p \to q) \to (\mathbf{G}p \to \mathbf{G}q)$ is a tautology. For the sake of contradiction, suppose this is not the case. There exists σ such that

$$\sigma \models \mathbf{G}(p \to q), \text{ and} \tag{1}$$
$$\sigma \not\models (\mathbf{G}p \to \mathbf{G}q). \tag{2}$$

By (2), we have

$$\begin{aligned}
&\sigma \models \mathbf{G}p, \text{ and} \\
&\sigma \not\models \mathbf{G}q.
\end{aligned}$$

Therefore, there exists $k \geq 0$ such that $p \in \sigma(k)$ and $q \notin \sigma(k)$ which contradicts (1).

(c) $\mathbf{FG}p \lor \mathbf{FG}\neg p$ is not a tautology since it is not satisfied by $(\{p\}\{q\})^\omega$.

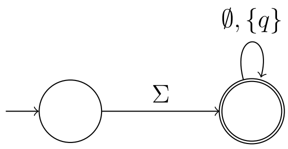
(d) $\neg\mathbf{F}p \to \mathbf{F}\neg\mathbf{F}p$ is a tautology since $\varphi \to \mathbf{F}\varphi$ is a tautology for every formula φ.

(e) $\neg(p \mathbin{\mathbf{U}} q) \leftrightarrow (\neg p \mathbin{\mathbf{U}} \neg q)$ is not a tautology. Let $\sigma = \{p\}\{q\}^\omega$. We have $\sigma \not\models \neg(p \mathbin{\mathbf{U}} q)$ and $\sigma \models \neg p \mathbin{\mathbf{U}} \neg q$.

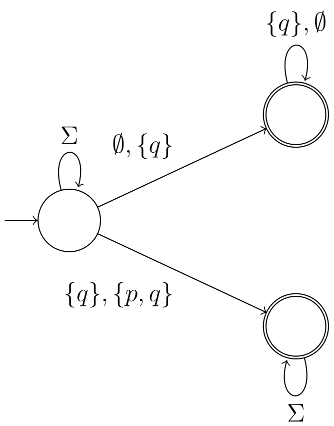
(f) $(\mathbf{G}p \to \mathbf{F}q) \leftrightarrow (p \mathbin{\mathbf{U}} (p \lor q))$ is not a tautology. Let $\sigma = \emptyset\{p,q\}^\omega$. We have $\sigma \models \mathbf{G}p \to \mathbf{F}q$ and $\sigma \not\models (p \mathbin{\mathbf{U}} (p \lor q))$.

Solution 3.6

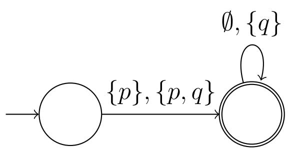
(a)



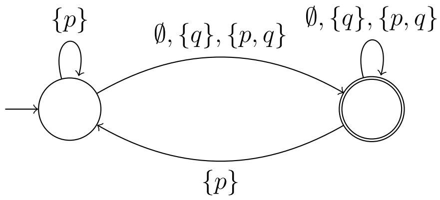
(b) Note that $(\mathbf{GF}p) \to (\mathbf{F}q) \equiv \neg(\mathbf{GF}p) \lor (\mathbf{F}q) \equiv (\mathbf{FG}\neg p) \lor (\mathbf{F}q)$. We construct Büchi automata for $\mathbf{FG}\neg p$ and $\mathbf{F}q$, and take their union:



(c) Note that $p \land \neg(\mathbf{XF}p) \equiv p \land \mathbf{XG}\neg p$. We construct a Büchi automaton for $p \land \mathbf{XG}\neg p$:



(d)



(e)