Technische Universität München (I7) **Summer Semester 2018**
J. Esparza / M. Blondin / P. Ashok **19.04.2018**

Model Checking – Exercise sheet 2

Exercise 2.1
Let $\varphi = \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ and $\psi = (r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg \mathbf{XX}s)$ 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) $\{q\}^\omega$

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

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

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

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

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

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

Exercise 2.2
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 sends infinitely many messages.

(d) The process only gives a result once.

(e) The process receives a message after it sends one.

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

Exercise 2.3
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) $\mathbf{FG}p \lor \mathbf{FG}\neg p$

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

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

(f) $(\mathbf{G}p \rightarrow \mathbf{F}q) \leftrightarrow (p \; \mathbf{U} \; (p \lor q))$

Solution 2.1

(a)
- $\emptyset^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since $\emptyset^\omega \not\models \mathbf{GF}p$ which follows from the fact that p does not occur infinitely often (or at all).

- $\emptyset^\omega \not\models (r\ \mathbf{U}\ \mathbf{X}p)\ \mathbf{U}\ (q \wedge \neg\mathbf{XX}s)$ since q never holds.

(b)
- $\{p,q,r,s\}^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p occurs infinitely often and q eventually always occur.

- $\{p,q,r,s\}^\omega \not\models (r\ \mathbf{U}\ \mathbf{X}p)\ \mathbf{U}\ (q \wedge \neg\mathbf{XX}s)$ since $\neg\mathbf{XX}s$ never holds.

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

- $\{p\}^\omega \not\models (r\ \mathbf{U}\ \mathbf{X}p)\ \mathbf{U}\ (q \wedge \neg\mathbf{XX}s)$ since q never occurs.

(d)
- $\{q\}^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since $\{q\}^\omega \not\models \mathbf{GF}p$ which follows from the fact that p does not occur infinitely often (or at all).

- $\{q\}^\omega \models (r\ \mathbf{U}\ \mathbf{X}p)\ \mathbf{U}\ (q \wedge \neg\mathbf{XX}s)$ since $(q \wedge \neg\mathbf{XX}s)$ holds already at the first position of the sequence.

(e)
- $\{p,q\}^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p occurs infinitely often and q (eventually) always occur.

- $\{p,q\}^\omega \models (r\ \mathbf{U}\ \mathbf{X}p)\ \mathbf{U}\ (q \wedge \neg\mathbf{XX}s)$ since $(q \wedge \neg\mathbf{XX}s)$ holds already at the first position of the sequence.

(f)
- $\{r\}\emptyset\{p,q,s\}^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p occurs infinitely often and q eventually always occur.

- $\{r\}\emptyset\{p,q,s\}^\omega \not\models (r\ \mathbf{U}\ \mathbf{X}p)\ \mathbf{U}\ (q \wedge \neg\mathbf{XX}s)$ since $(q \wedge \neg\mathbf{XX}s)$ never holds.

(g)
- $\{r\}\emptyset(\{p,q\}\{r,s\})^\omega \not\models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p occurs infinitely often, and from position 2 onwards it is always the case that either q or r holds.

- $\{r\}\emptyset(\{p,q\}\{r,s\})^\omega \models (r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg\mathbf{XX}s)$ since the left-hand side of the topmost $\mathbf{U}$ holds at the two first positions, and the right-hand side holds at the third position. In more details:

  - $\{r\}\emptyset(\{p,q\}\{r,s\})^\omega \models r \ \mathbf{U} \ \mathbf{X}p$ since r holds at the first position and $\mathbf{X}p$ holds at the second position,

  - $\emptyset(\{p,q\}\{r,s\})^\omega \models r \ \mathbf{U} \ \mathbf{X}p$ since $\mathbf{X}p$ holds at the first position,

  - $(\{p,q\}\{r,s\})^\omega \models q \wedge \neg\mathbf{XX}s$ since q occurs at the first position and s does not occur at the third position.

(h)

- $\{r\}\emptyset\{p\}\{q,r\}(\{p,s\}\emptyset)^\omega \not\models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p occurs infinitely often but neither q nor r eventually always occur.

- $\{r\}\emptyset\{p\}\{q,r\}(\{p,s\}\emptyset)^\omega \not\models (r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg\mathbf{XX}s)$ since $q \wedge \neg\mathbf{XX}s$ only holds at the fourth position and $r \ \mathbf{U} \ \mathbf{X}p$ does not hold at the third position.

(i)

- $\{r\}\emptyset\{p\}\{p,q,r\}(\{s\}\emptyset)^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p does not occur infinitely often.

- $\{r\}\emptyset\{p\}\{p,q,r\}(\{s\}\emptyset)^\omega \models (r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg\mathbf{XX}s)$ since the left-hand side of the topmost $\mathbf{U}$ holds at the three first positions, and the right-hand side holds at the fourth position. In more details:

  - $\{r\}\emptyset\{p\}\{p,q,r\}(\{s\}\emptyset)^\omega \models r \ \mathbf{U} \ \mathbf{X}p$ since r occurs at the first position and $\mathbf{X}p$ holds at the second position,

  - $\emptyset\{p\}\{p,q,r\}(\{s\}\emptyset)^\omega \models r \ \mathbf{U} \ \mathbf{X}p$ since $\mathbf{X}p$ holds at the first position,

  - $\{p\}\{p,q,r\}(\{s\}\emptyset)^\omega \models r \ \mathbf{U} \ \mathbf{X}p$ since $\mathbf{X}p$ holds at the first position,

  - $\{p,q,r\}(\{s\}\emptyset)^\omega \models q \wedge \neg\mathbf{XX}s$ since q occurs at the first position and s does not occur at the third position.

(j)

- $\{q,r\}\emptyset\{p,q\}\emptyset\{r,s\}^\omega \models \mathbf{GF}p \rightarrow \mathbf{FG}(q \vee r)$ since p does not occur infinitely often.

- $\{q,r\}\emptyset\{p,q\}\emptyset\{r,s\}^\omega \models (r \ \mathbf{U} \ \mathbf{X}p) \ \mathbf{U} \ (q \wedge \neg\mathbf{XX}s)$ 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 2.2

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		
	$\mathbf{G}(g \to \mathbf{XG}(\neg s \wedge \neg r))$	$\{g\}\emptyset^\omega$	$\{g\}\{s\}\emptyset^\omega$
(c)	$\mathbf{GF}s$	$(\{s\}\{r\})^\omega$	$\{s\}\{s\}\{s\}\emptyset^\omega$
(d)	$\mathbf{F}g \wedge \mathbf{G}(g \to \mathbf{XG}\neg g)$	$\{g\}\emptyset^\omega$	$\{g\}\{g\}\emptyset^\omega$
(e)	$\mathbf{G}(s \to \mathbf{XF}r)$	$(\{s\}\{r\})^\omega$	$\{s\}\emptyset^\omega$
(f)	$(\neg s \wedge \neg g)\ \mathbf{W}\ r$	$\{r\}\{g\}^\omega$	$\{g\}^\omega$

Solution 2.3

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

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

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

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

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

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