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 $G[(t_1 = \text{red} \land t_2 = \text{green}) \lor (t_1 = \text{green} \land t_2 = \text{red})]$ 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 $\varphi = FGp \rightarrow GF(q \lor r)$ and $\psi = \neg(r \ U X p) \ U (q \land \neg XXs)$ be LTL formulas over the atomic propositions $AP = \{p, q, r, s\}$. Say whether the following sequences satisfy $\varphi$ and $\psi$. Justify your answers.

(a) $\emptyset^\omega$

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

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

(d) $\{r\}0\{p, q, s\}^\omega$

(e) $\{r\}0\{p\}\{q, r\}\{\{p, s\}0\}^\omega$

(f) $\{q, r\}0\{p, q\}0\{r, s\}^\omega$
Exercise 3.4

Let \( AP = \{s, r, g\} \) be actions of a process: sending a message, receiving a message, and giving 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) \( Gp \rightarrow Fp \) 
(b) \( G(p \rightarrow q) \rightarrow (Gp \rightarrow Gq) \)
(c) \( FGp \lor FG\neg p \) 
(d) \( \neg Fp \rightarrow F\neg Fp \)
(e) \( \neg(p U q) \leftrightarrow (\neg p U \neg q) \)
(f) \( (Gp \rightarrow Fq) \leftrightarrow (p U (p \lor q)) \)

Exercise 3.6

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

(a) \( XG\neg p \)
(b) \( (GFp) \rightarrow (Fq) \)
(c) \( p \land \neg(XFp) \)
(d) \( G(p U (p \rightarrow q)) \)
(e) \( Fq \rightarrow (\neg q U (\neg q \land p)) \)
Solution 3.1

Counter example: \( \{t_1 = \text{red}, t_2 = \text{red}\}^\omega \)

Correct formula: \( \neg F(t_1 = \text{green} \land t_2 = \text{green}) \equiv G(t_1 = \text{red} \lor t_2 = \text{red}) \)

LTL formula for the other property: \( GF(t_1 = \text{green}) \land GF(t_2 = \text{green}) \)

Solution 3.2

\( G(a \land f \rightarrow a \land Xd) \land (a U k) \)

Solution 3.3

(a) \( \emptyset^\omega \models FGp \rightarrow GF(q \lor r) \) since \( \emptyset^\omega \not\models FGp \) which follows from the fact that \( p \) does not occur at all.

\( \emptyset^\omega \not\models \neg (r U Xp) U (q \land \neg XXs) \) since \( q \) never holds.

(b) \( \{p, q, r, s\}^\omega \models FGp \rightarrow GF(q \lor r) \) since \( p \) always occurs and \( q \) occurs infinitely often.

\( \{p, q, r, s\}^\omega \not\models \neg (r U Xp) U (q \land \neg XXs) \) since \( \neg XXs \) never holds.

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

\( \{p\}^\omega \not\models \neg (r U Xp) U (q \land \neg XXs) \) since \( q \) never occurs.

(d) \( \{r\} \emptyset \{p, q, s\}^\omega \models FGp \rightarrow GF(q \lor r) \) since \( p \) eventually always occurs and \( q \) occurs infinitely often.

\( \{r\} \emptyset \{p, q, s\}^\omega \not\models \neg (r U Xp) U (q \land \neg XXs) \) since \( (q \land \neg XXs) \) never holds.

(e) \( \{r\} \emptyset \{p\} \{q, r\} \{(p, s) \emptyset\}^\omega \models FGp \rightarrow GF(q \lor r) \) since \( p \) does not occur eventually always.

\( \{r\} \emptyset \{p\} \{q, r\} \{(p, s) \emptyset\}^\omega \not\models \neg (r U Xp) U (q \land \neg XXs) \) since \( \neg (r U Xp) \) and \( q \land \neg XXs \) does not hold at the first position.
(f) • \(\{q, r\} \emptyset \{p, q\} \emptyset \{r, s\} \omega \models \text{FG}p \rightarrow \text{GF}(q \lor r)\) since \(p\) does not occur eventually always.

• \(\{q, r\} \emptyset \{p, q\} \emptyset \{r, s\} \omega \models \neg(r \cup Xp) \cup (q \land \neg XXs)\) since \(q \land \neg XXs\) 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, \(\sigma\) and \(\sigma'\) are two example sequences such that \(\sigma \models \varphi\) and \(\sigma' \not\models \varphi\).

<table>
<thead>
<tr>
<th>(\varphi)</th>
<th>(\sigma)</th>
<th>(\sigma')</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) (Fg)</td>
<td>({g} \emptyset \omega)</td>
<td>(\emptyset \omega)</td>
</tr>
<tr>
<td>(b) (G(g \rightarrow G(\neg s \land \neg r)))</td>
<td>({g} \emptyset \omega)</td>
<td>({g, s} \emptyset \omega)</td>
</tr>
<tr>
<td></td>
<td>or if “after” is strict</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(G(g \rightarrow XG(\neg s \land \neg r)))</td>
<td>({g} \emptyset \omega)</td>
</tr>
<tr>
<td>(d) (Fg \land G(g \rightarrow XG \neg g))</td>
<td>({g} \emptyset \omega)</td>
<td>({g} {g} \emptyset \omega)</td>
</tr>
<tr>
<td>(f) ((\neg s \land \neg g) \text{ W r})</td>
<td>({r} {g} \omega)</td>
<td>({g} \omega)</td>
</tr>
</tbody>
</table>

Solution 3.5

(a) \(Gp \rightarrow Fp\) is a tautology since

\[
Gp \rightarrow Fp \equiv \neg F \neg p \rightarrow Fp
\]
\[
\equiv F \neg p \lor Fp
\]
\[
\equiv F(\neg p \lor p)
\]
\[
\equiv F \text{true}
\]
\[
\equiv \text{true}.
\]

(b) \(G(p \rightarrow q) \rightarrow (Gp \rightarrow Gq)\) is a tautology. For the sake of contradiction, suppose this is not the case. There exists \(\sigma\) such that

\[
\sigma \models G(p \rightarrow q), \quad \text{and}
\]
\[
\sigma \not\models (Gp \rightarrow Gq).
\]

By (2), we have

\[
\sigma \models Gp, \quad \text{and}
\]
\[
\sigma \not\models Gq.
\]

Therefore, there exists \(k \geq 0\) such that \(p \in \sigma(k)\) and \(q \not\in \sigma(k)\) which contradicts (1).
(c) $\mathsf{FG}p \lor \mathsf{FG}\neg p$ is not a tautology since it is not satisfied by $\left(\{p\}\{q\}\right)^\omega$.

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

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

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

Solution 3.6

(a)

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

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

(d)
(e)

\[
\begin{align*}
\emptyset, \{q\}, \{p, q\} & \quad \{p\} \\
\emptyset, \{q\}, \{p, q\} & \quad \{p\}
\end{align*}
\]