Model-Checking Exercises
Sommersemester 2009 / Sheet 1

April 23, 2009

We are going to discuss the examples together at 7.5 and 14.5. For questions about the exercises or examples, please send me an email `campetel@in.tum.de`.

Example 1.1: LTL Specifications

Find suitable atomic propositions and specify the following properties in LTL:

1. The process will terminate.
2. The process satisfies a certain invariant.
3. The process sends infinitely many messages.
4. Each request is eventually answered by an acknowledge.
5. After the process is terminated, it sends no messages.
6. The static initialization fiasco in C++: Before entering in the *main* routine no thread will be generated.

Specify for each of the above properties one fulfilling and non-fulfilling sequence. For which properties there are finite/infinite fulfilling/non-fulfilling sequences? How do appropriate Kripke structures look like?

Example 1.2: Further Temporal Operators

In the lecture were introduced the following:

- *Globally:* $w \models \mathbf{G}\phi \;\Leftrightarrow\; w \models \neg(\mathbf{true}\ \mathbf{U}\ \neg\phi)$
- *Release:* $w \models \phi\,\mathbf{R}\,\psi \;\Leftrightarrow\; w \models \neg(\neg\phi\ \mathbf{U}\ \neg\psi)$

Let $\Sigma = 2^{\mathbf{AP}}$ with $AP \neq \emptyset$, then write a word $w \in \Sigma^\omega$ where $w = w_0 w_1 \ldots$ and define the i-th suffix w^i with $w^i = w_i w_{i+1} \ldots$. Show the following

1. $w \models \mathbf{G}\phi \;\Leftrightarrow\; \forall i \in \mathbb{N}\ w^i \models \phi$
2. $w \models \phi\,\mathbf{R}\,\psi \;\Leftrightarrow\; \forall i \in \mathbb{N}\ (\forall j < i\ w^j \not\models \phi) \rightarrow w^i \models \psi$
3. $w \models \neg(\phi\ \mathbf{U}\ \psi) \;\Leftrightarrow\; w \models \neg\phi\,\mathbf{R}\,\neg\psi$
4. $w \models \phi\ \mathbf{U}\ \psi \;\Leftrightarrow\; w \models \psi \vee (\phi \wedge \mathbf{X}(\phi\ \mathbf{U}\ \psi))$
5. $w \models \phi\,\mathbf{R}\,\psi \;\Leftrightarrow\; w \models \mathbf{G}\psi \vee (\psi\ \mathbf{U}\ (\phi \wedge \psi))$

Example 1.3: Positive Normal Form

A formula ϕ over the propositions $\mathbf{AP}$ is in *positive Normal Form* if negation sign $\neg$ happens in ϕ only directly in front of the propositions $a \in \mathbf{AP}$. For example $\neg\mathbf{G}a$ is not in a positive Normal Form, whereas the equivalent formula $\mathbf{true}\ \mathbf{U}\neg a$ is in positive Normal Form. We denote the set of positive Normal Form formulas on the operators $\mathbf{X}, \mathbf{U}, \mathbf{G}, \vee, \wedge$ and $\neg$ as $\mathbf{NF} - \mathbf{LTL}$.

1. Show by induction on formula structure, that for any $\mathbf{LTL}$ formula ϕ exists an equivalent $\mathbf{NF} - \mathbf{LTL}$. Use for this task the equivalences from the exercise 1.2.

2. Let $\mathbf{NF} - \mathbf{LTL}_\mathbf{G}$ the set of all $\mathbf{NF} - \mathbf{LTL}$ formulas, where the operator $\mathbf{G}$ doesn't occur. Show for any formula $\phi \in \mathbf{NF} - \mathbf{LTL}_\mathbf{G}$ by induction on the Formula structure, that exists for every word $w = w_0 w_1 \ldots \in \Sigma^\omega$ with $w \models \phi$ a number $N_\phi(w) \in \mathbb{N}$, so that already decides with the first $N_\phi(w) + 1$ symbols $w_0 \ldots w_{N_\phi(w)}$ of this word whether $w \models \phi$ holds or not. In other words, for any sequel $w' \in \Sigma^\omega$ hold

$$w \models \phi \Leftrightarrow w_0 \ldots w_{N_\phi(w)} w' \models \phi$$

3. Let $\mathbf{NF} - \mathbf{LTL}_\mathbf{X}$ the set of all $\mathbf{LTL}$ formulas, where the operator $\mathbf{X}$ doesn't occur. Show that a formula $\phi \in \mathbf{NF} - \mathbf{LTL}_\mathbf{X}$ cannot be distinguished between $w = w_0 w_1 \ldots \in \Sigma^\omega$ and $D(w) = w_0 w_0 w_1 w_1 \ldots$, viz

$$w \models \phi \Leftrightarrow D(w) \models \phi$$

   hold for all $\phi \in \mathbf{NF} - \mathbf{LTL}_\mathbf{X}$ and $w \in \Sigma^\omega$.