Technische Universität München **Summer Semester 2014**
I7
J. Esparza / A. Durand-Gasselin **25.04.2014**

Model Checking – Exercise sheet 2

In this exercise sheet, we use, in addition to the modalities $\mathbf{X}, \mathbf{U}$, the following ones:

- **G**lobally: $w \models \mathbf{G}\varphi \iff w \models \neg(\mathbf{true}\,\mathbf{U}\,\neg\varphi)$
- Eventually (**F**inally): $w \models \mathbf{F}\varphi \iff w \models \neg\mathbf{G}\neg\varphi$
- **R**elease: $w \models \varphi\,\mathbf{R}\,\psi \iff w \models \neg(\neg\varphi\,\mathbf{U}\,\neg\psi)$

Exercise 2.1

Determine an adequate set of atomic proposition **AP** and specify the following properties in **LTL**:

1. The process terminates
2. The process satisfies a given invariant
3. The process sends infinitely many messages
4. Each request is eventually acknoledged
5. After the process terminates, it sends no more messages

For each property give an exemple satisfying it and another violating it.

Exercise 2.2

Describe which properties the following formulas ensure. For each formula give an example of a word satisfying the formula an a counter example.

1. $P\,\mathbf{U}(Q \vee \mathbf{G}P)$
2. $\mathbf{G}(P \to \mathbf{F}S)$
3. $\mathbf{G}((Q \wedge \neg R \wedge \mathbf{F}R) \to (\neg P\,\mathbf{U}\,R))$
4. $\mathbf{G}(Q \wedge \neg R \to (\neg R\,\mathbf{U}(P \wedge \neg R)))$
5. $\mathbf{G}((Q \wedge \neg R \wedge \mathbf{F}R) \to (P \to (\neg R\,\mathbf{U}(S \wedge \neg R)))\,\mathbf{U}\,R)$

Exercise 2.3

Let $\Sigma = 2^{\mathbf{AP}}$ with $\mathbf{AP} \neq \emptyset$, and let $w \in \Sigma^\omega$, $w = w_0 w_1 \ldots$
We denote the i-th suffix of w as $w^i = w_i w_{i+1} \ldots$
Prove the following equivalences:

$$\begin{array}{lll} - & w \models \mathbf{G}\varphi & \iff \forall i \in \mathbb{N}\ w^i \models \varphi \\ - & w \models \varphi \,\mathbf{R}\, \psi & \iff \forall i \in \mathbb{N}\ (\forall j < i\ w^j \not\models \varphi) \rightarrow w^i \models \psi \\ - & w \models \neg(\varphi \,\mathbf{U}\, \psi) & \iff w \models \neg\varphi \,\mathbf{R}\, \neg\psi \\ - & w \models \varphi \,\mathbf{U}\, \psi & \iff w \models \psi \vee (\varphi \wedge \mathbf{X}(\varphi \,\mathbf{U}\, \psi)) \\ - & w \models \varphi \,\mathbf{R}\, \psi & \iff w \models \mathbf{G}\psi \vee (\varphi \,\mathbf{U} (\varphi \wedge \psi)) \end{array}$$

Exercise 2.4

A formula φ over the set of propositions $\mathbf{AP}$ is in *positive normal form* when the negations only appear directly in front of propositions $a \in \mathbf{AP}$. For instance $\neg\mathbf{G}a$ is not in positive normal form while $\mathbf{true}\,\mathbf{U}\,\neg a$ is.

We denote **NF-LTL** the set of formulas in positive normal form over the operators $\mathbf{X}, \mathbf{U}, \mathbf{G}, \wedge, \vee$ and $\neg$.

1. Show by induction, using the equivalences shown in the previous exercise that any **LTL** formula φ admits an equivalent **NF-LTL** formula.

2. Let $\textbf{NF-LTL}_{-\mathbf{G}}$ the formulas of **NF-LTL** in which the operator $\mathbf{G}$ does not occur. Show that for any formula φ in$\textbf{NF-LTL}_{-\mathbf{G}}$, for any word $w \in \Sigma^\omega$, such that $w \models \varphi$ there exists an integer $N_\varphi(w)$ such that $w_0 \ldots w_{N_\varphi(w)}$ characterizes whether $w \models \varphi$ or not. More formally for any $w' \in \Sigma^\omega$

$$w \models \varphi \iff w_0 \ldots w_{N_\varphi(w)} w' \models \varphi$$

3. Let $\textbf{NF-LTL}_{-\mathbf{X}}$ the set of **NF-LTL** in which $\mathbf{X}$ does not occur. Show that any $\textbf{NF-LTL}_{-\mathbf{X}}$ formula φ can not distinguish $w \in \Sigma^\omega$ and $D(w) = w_0 w_0 w_1 w_1 \ldots$, i.e.:

$$w \models \varphi \iff D(w) \models \varphi$$

Exercise 2.5

Let $K_1 = (S, \rightarrow_1, r, \mathbf{AP}, v)$ and $K_2 = (S, \rightarrow_2, r, \mathbf{AP}, v)$ two Kripke structures with same set of state S, same initial state r and same interpretation of the predicates in $\mathbf{AP}$. We write $K_1 \leq K_2$ if the transition relation $\rightarrow_2 \subseteq S \times S$ contains the transition relation $\rightarrow_1$, that is $\rightarrow_1 \subseteq \rightarrow_2$.

Show that if $K_1 \leq K_2$ then for any **LTL** formula φ:

$$K_2 \models \varphi \implies K_1 \models \varphi$$