ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

A. Podelski
A. Malkis
M. Wehrle

January 10, 2006
Discussion: Jan 14–Jan 18
Some room(s)

Tutorials for Verification
Exercise sheet 9

Exercise 1: Satisfaction of an LTL formula depends only on atomic propositions that occur in it
For an LTL formula ϕ over the set of atomic propositions AP, let $AP_\phi = \mathit{closure}(\phi) \cap AP$ be the set of those atomic propositions that actually occur in the formula. Show that for any LTL formula ϕ over AP, any $(A_i)_{i\geq 0} \in (2^{AP})^\omega$,

$$(A_i \cap AP_\phi)_{i\geq 0} \models \phi \quad \Leftrightarrow \quad (A_i)_{i\geq 0} \models \phi\,.$$

Exercise 2: Stating Properties in LTL
Consider a lift system that services N floors numbered 0 through $N-1$. Assume $\mathit{door}(i)$ indicates that the doors on the i-th floor are open, $\mathit{lift}(i)$ indicates that the lift is at floor i, and $\mathit{req}(i)$ indicates that the request button at floor i was pressed and is lit. In the lift cabin there are N buttons for the floors and $\mathit{send}(i)$ indicates that the i-th send button is lit.
State the following properties in LTL.

(a) A floor door is never open if the cabin is not present at that floor.

(b) A requested floor will be served sometime.

(c) The lift returns to floor 0 infinitely often.

(d) The lift does not move unless there is some request.

Exercise 3: LTL tautologies
Which of the following formulae are tautologies? An LTL formula is a tautology if it holds for any path in any system. Give a counterexample for any formula that does not always hold.

(a) $(\Box\,\varphi \rightarrow \Diamond\,\psi) \leftrightarrow (\varphi \mathbin{\mathsf{U}} (\psi \vee \neg\varphi))$

(b) $(\Diamond\,\Box\,\varphi \rightarrow \Box\,\Diamond\,\psi) \leftrightarrow \Box(\varphi \mathbin{\mathsf{U}} (\psi \vee \neg\varphi))$

(c) $\Diamond(\varphi \wedge \psi) \leftrightarrow \Diamond\,\varphi \wedge \Diamond\,\psi$

(d) $\Box(\varphi \rightarrow \bigcirc\varphi) \rightarrow (\varphi \rightarrow \Box\varphi)$

Exercise 4*: Expressiveness of LTL

The goal is to prove that there are ω-regular properties that cannot be expressed in LTL.

(a) Fill in the gaps in the following inductive proof:

For every formula φ there is a $n_0(\varphi)$ such that for all $n \geq n_0(\varphi)$ and all $A, B \subseteq AP$:

$$A^n B A^\omega \models \varphi \text{ iff } A^{n+1} B A^\omega \models \varphi$$

Proof by structural induction over φ. The base case is $\varphi = a$, $a \in AP$. Then choose $n_0(a) = 1$. Then we have for all $n \geq 1$:

$$A^n B A^\omega \models a \text{ iff } a \in A \text{ iff } A^{n+1} B A^\omega \models a\,.$$

Now assume that the induction hypothesis holds for φ and ψ. We now have to prove that it holds for $\neg\varphi$, $\varphi \wedge \psi$, $\bigcirc\varphi$ and $\varphi \mathsf{U} \psi$.

For $\neg\varphi$ choose $n_0(\neg\varphi) = n_0(\varphi)$. Then for all $n \geq n_0$, $A^n B A^\omega \models \neg\varphi$ iff ...

For $\varphi \wedge \psi$ ....

For $\bigcirc\varphi$ ....

For $\varphi \mathsf{U} \psi$ ....

(b) Use part (a) to prove that with $AP = \{ a \}$ there is no LTL formula for the LT-property:

$$P = \{ A_0 A_1 A_2 \ldots \in (2^{AP})^\omega | a \in A_{2i} \}\,.$$

(c) How can P be expressed as ω-regular expression?