Prof. Dr. K. Madlener
Dipl.-Inf. P. Michel
Dipl.-Inf. C. Feller

University of Kaiserslautern
Department of Computer Science
AG Grundlagen der Informatik

Exercise Sheet 8: Specification and Verification with Higher-Order Logic (Summer Term 2011)

Date: 04.07.2011

Exercise 1 LTL Specifications, Rules and Proofs

Download the Elevator theory from the webpage of the lecture. It contains all the properties and proofs you have seen in the lecture. In particular, there is a deep embedding of Linear Temporal Logic (LTL) formulas which we will use in this exercise.

a) Specify the property that the elevator is never in more than one floor using LTL. Prove this property.

   Optional: Formulate and prove the similar property that the elevator is always at least in one floor.

b) Extend the LTL language by the `Next` operator ($\circ$), which states that a formula holds in the next state of the trace.

   Adjust the semantics accordingly.

c) Specify the property that the elevator only opens the door if the current floor was actually requested. Prove this property.

   Optional: Formulate and prove a similar property about closing the door.

d) To complete a deep embedding of LTL, it would be necessary to define a calculus within Isabelle/HOL. With such a deep embedding the proofs we have done so far could be completed with the calculus only.

   For this exercise we consider a very small calculus, which has only one axiom and one rule:

$$\frac{\models F}{\vdash F}\,(\texttt{ltl\_valid}) \qquad \frac{\vdash F \to \circ F}{\vdash F \to \Box F}\,(\texttt{ltl\_induct})$$

   The calculus is trivially *complete* because of the `ltl_valid` axiom.

   Formulate the set of provable formulas inductively and prove the *soundness* of the calculus.

e) Consider the following transition of the transition relation `tr`:

$$f \in T \Longrightarrow ((a, f, r, d, T), (Open, f, r, OP, T - \{f\})) \in tr$$

   It doesn't seem to make much sense to allow to *open* the door, even if the door was already open. Now assume we "fix" the transition:

$$f \in T \Longrightarrow ((a, f, r, CL, T), (Open, f, r, OP, T - \{f\})) \in tr$$

   Unfortunately, there are now states, in which the elevator can get stuck. Which are those states? Identify all states in which the elevator is either stuck or can only make transitions to a stuck state.

f) Specify the property that the elevator is `ok`, i.e. that it is *not* in such a state. Now specify a theorem stating that the elevator will always be `ok`, if it starts in an `ok` state.

   Prove this property using the LTL calculus.