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 10: Specification and Verification with Higher-Order Logic (Summer Term 2011)

Date: 20.07.2011

Exercise 1 Distributed Termination Detection

In this exercise we will consider a distributed termination detection algorithm as detailed by Dijkstra in

`http://userweb.cs.utexas.edu/users/EWD/ewd08xx/EWD840.PDF`.

The main goal is to model the setting described in the paper as state transition system. Using this model, it should be possible to specify and prove properties about the termination detection algorithm, specifically its correctness.

While the proofs give a good indication wether your model is suitable for this task, they are not in the focus of this exercise.

Hint: It might be useful to adapt the relevant parts of the elevator theory for this exercise.

We would advise to take the following approach:

a) Download and browse through the paper to get used to the setting or work with the slides from the lecture.

b) Define a `state` type for the transition system, which can represent the state of `N` machines, as well as the token.

c) Define a predicate which decides wether a value of your state type is indeed a proper state. Also define a reasonable `initial` state.

d) Define a transition relation (`tr`) on states, which models the behavior of the machines as described in the paper.

e) Define the set of infinite traces with regard to the transition relation.

f) Prove that every state on a trace starting with the initial state is proper.

g) Define atoms to represent useful properties of the state in LTL formulas and define the label function `L`, which calculates the set of all true atoms of a state.

h) Define (or copy) a deep embedding of LTL formulas based on the atoms you defined.

i) Specify and prove the invariant of the system described in the paper.

j) Specify and prove the correctness of the termination detection algorithm.