Prof. Dr. A. Poetzsch-Heffter
Dipl.-Inform. J. O. Blech
Dipl.-Inform. M. J. Gawkowski

TU Kaiserslautern
Fachbereich Informatik
AG Softwaretechnik

Handout 7: Specification and Verification Using Higher-Order Logic (summer term 2008)

July 1th, 2008

Exercise 1 Elevator

a) Downlaod theory files "ElevatorWithSketch.thy" and "Pdl.thy" as well as and ML file "elevator.sml" from our lecture homepage.

b) Make yourself familiar with constant definitions, function definitions, and proofs provided by the theory ElevatorWithSketch and Pdl.

c) Make yourself familiar with the content of the file "elevator.sml".

d) Read Section 6.6 "Case Study: Verified Model Checking" in Isabelle/HOL tutorial "a Proof Assistant for Higher-Order Logic".

e) Formalize the Computational Tree Logic (CTL) as presented in Section 6.6.2 in a theory file Ctl.

f) Consider the lemma

```
lemma elevator_liveness:
      "((BtTo g),es)#t:ftrace
       --> ( EX n::nat. (ts@((BtTo g),es)#t):ftrace  & (length ts) >= n
             --> (EX i < length ts . fst(ts!i) = (Open g) ) )"
sorry
```

in the theory ElevatorWithSketch which formalizes a liveness property of the elevator system. Specify the same property of the elevator system using the CTL logic.