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

TU Kaiserslautern
Fachbereich Informatik
AG Softwaretechnik

Handout 6: Specification and Verification Using Higher-Order Logic (summer term 2008)

Juni 17th, 2008

Exercise 1 Elevator

a) Downlaod theory file "ElevatorWithSketch.thy" 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.

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

d) Consider the following type declarations from the theory ElevatorWithSketch:

```
consts reachable :: "label => estate => bool"
consts itNonOpenSuccTraces ::"nat => floor => (label*estate) list set
                                => (label*estate) list set"
```

Write definitions of the predicate `reachable` and the function `itNonOpenSuccTraces` which have the same functionality as corresponding ML functions in the file "elevator.sml".

e) Prove the lemma

```
lemma non_open_succ_traces_empty:
     "(reachable (BtTo g) es)
       --> (itNonOpenSuccTraces 12 g {((BtTo g),es)#[]} ) = {}"
```

in the theory "ElevatorWithSketch".