Formal Methods in Software Development
Exercise 7 (January 11)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.uni-linz.ac.at

December 9, 2009

The result is to be submitted by the deadline stated above via the Moodle interface as a PDF file which contains

- a cover page with the title of the course, your name, Matrikelnummer, and email-address,
- for each exercise, a section with the number and name of the exercise and the content of the exercise.

1 Modeling an Elevator (50)

Given a natural number $N > 0$, an *N-floor elevator* operates as follows:

1. The elevator is always at one of the floors $0 \dots N$ (we ignore the times when the elevator is between floors) and it is always in one of the states "stopped", "moving up", or "moving down". Initially the elevator is stopped at floor 0.
2. Inside the cabin, the elevator has buttons b_i for each floor i; each button is either "on" (its light is on) or "off" (its light is off). At any time, any button b_i that is "off" may become "on" (a person has pressed the button which indicates a request to move to floor i). Initially no button is on.
3. At any floor i, there are two request buttons u_i ("want up") and d_i ("want down") that may be "on" or "off". At any time, a button that is "off" may become "on" (a person has pressed the button which indicates a request for the elevator). Initially no button is on.
4. If no button is pressed, the elevator starts to move to floor 0, and then waits for a button b_i, u_i, d_i to be pressed. As soon as this happens, the elevator starts to move to floor i.
5. If the elevator moves and reaches a floor i, it stops at that floor in any of these cases (please note that multiple cases may hold at the same time):
   - the button b_i is on (in this case, button b_i becomes off and the elevator moves after the stop in the same direction as before the stop, unless there is no button b_j, d_j, d_j pressed for a floor j in that direction),
   - the button u_i is on and
     - if the elevator anyway has moved upward or if there is no floor $j < i$ with b_j, u_j, or d_j on.

     (in this case, button u_i becomes off and the elevator moves after the stop upwards),
   - the button d_i is on and
     - if the elevator anyway has moved downward or if there is no floor $j > i$ with b_j, u_j, or d_j on.

     (in this case, button d_i becomes off and the elevator moves after the stop downwards).

   Otherwise, the elevator continues its movement.

Model this system formally by defining its state space, initial state condition, and transition relation in the syntax specified in the lecture:

$State := \dots$
$I(\dots) :\Leftrightarrow \dots$
$R(\dots, \dots) :\Leftrightarrow \dots$

Do not overlook that you have to record in the system the direction of the movement of the elevator before it stopped.

Define auxiliary predicates for the definition of R which shall be as readable as possible. Also use comments to indicate your informal intentions.

Show (the initial part of) a run of the system (a sequence of states) for $N = 3$ with three buttons pressed until the elevator is again stopped at floor 0.

2 Modeling an Elevator System (50)

Model a system with $E \geq 1$ elevators of the kind similar to the one shown above. Each elevator e (with $0 \leq e < E$) has its own set of floor buttons b_i^e, but all elevators share a common set of request buttons u_i and d_i (if a request button is pressed, any elevator may stop to handle the request).

Model this system by defining its state space, initial state condition, and transition relation using the interleaving model of concurrency.

Redefine the transition relation defined in the previous assignment to a transition relation $R_e(\ldots,\ldots)$ for elevator e such that it may serve as a building block of the transition relation of the elevator system:

$$R(\ldots,\ldots) :\Leftrightarrow \ldots \vee (\exists e : 0 \leq e < E \wedge R_e(\ldots,\ldots))$$

Answer the questions (with informal but convincing justifications):

1. Is it guaranteed that, if an elevator reaches floor 0 or floor N, it will stop (before reverting its direction)?
2. Is it guaranteed that, if an elevator e stops at floor i with $0 < i < N$, no other elevator $e' \neq e$ will stop at floor i, unless $b_i^{e'}$ is pressed?
3. Is it guaranteed that, if two elevators e_1, e_2 stop at floor i with $0 < i < N$, no other elevator $e' \notin \{e_1, e_2\}$ will stop at floor i, unless $b_i^{e'}$ is pressed?
4. Is it guaranteed that by pressing button b_i^e, elevator e will eventually stop at floor i?
5. Is it guaranteed that by pressing button u_i/d_i, some elevator will eventually stop at floor i?

Hints

Let $\mathbb{B} := \{\mathsf{true}, \mathsf{false}\}$ and $\mathbb{N}_N := \{n \in \mathbb{N} : n < N\}$.

- A single button b can be modelled as a value $b \in \mathbb{B}$
- A sequence of N buttons can be modelled as a function $b : \mathbb{N}_N \to \mathbb{B}$, i.e. b_i $(= b(i))$ is the status of button i.
- E sequences of N buttons can be modelled as a function $b : (\mathbb{N}_E \times \mathbb{N}_N) \to \mathbb{B}$, i.e. b_i^e $(= b(e, i))$ is the status of button i in sequence e.