Software verification - Model checking an elevator

May 2, 2017

Project to be done in groups of two or three students. Hand in before tuesday 16 May, 23:59, CET.

Case Description

Consider an elevator that services 4 floors. At each floor, there is a door in front of the shaft. There are buttons to control the elevator inside the elevator, as well as on every floor. There are indicator lights to tell to which floor the elevator will go, both inside and outside the elevator. Obviously, it should be possible to implement a system as in the model: it should not allow physically impossible behaviour.

There is a list of specifications for this elevator:

1. Doors should not open if the elevator is not present.
2. A requested floor will be served sometime.
3. It is possible for a user to go from any floor to any other floor.
4. Again and again the elevator returns to floor 0.
5. The top-floor gets priority: when it is requested, the elevator serves it immediately, before other floors.
6. The indicator lights are correct: they are on if, and only if, the elevator goes to that floor.
7. If there is no request, the elevator does not move.

Assignments

a) Make a list of atomic propositions that you need to formalize the above specifications. Formalize the specifications in LTL or CTL. You can also come up with additional specifications for bonus points. (4 points)

b) Create a NuSMV2-model describing the elevator. Design it such that your specifications hold. If specifications contradict each other, decide which are most important (and therefore should be satisfied in your model). (4 points)

c) Check your model for all specifications, and make sure that all intended specifications hold. Also verify that specifications contradicting your chosen specifications do not hold (2 points).

Deliverables

Report on the solutions of all the assignments, the choices you have made in your specifications and models, and the conclusions from assignment c. Also add a (brief) reflection: what was the division of tasks in your group? Did the assignment give you additional insight? What was your experience with NuSMV2?

This report, together with the NuSMV2-model and formalized specifications, should be handed in before May 16, 23:59.