Instructor: Edmund M. Clarke TA: Qinsi Wang

Due date: 3pm, 04/25/2014 15414sta@gmail.com

Assignment 4

1 Models for well defined CTL formulae (30 points)

Give a model for each of the following well defined CTL formulae. (Hint: a model can be presented as a computation tree. The solution to each formula is not unique.)

1. AX(p ∧ q)
2. EF(p ∧ AXq)
3. EGp
4. EG(p ∧ EXq)
5. A(p U (q ∧ r))

Submission: type in or scan your solution, and send the electronic version of your solution to the TA together with your solution to the second problem.

2 Modeling an Elevator Controller (70 points)

You are to model and verify a simple elevator controller. Specifically, implement and check a controller using NuSMV model checker.

The elevator services a building with three floors. On each floor, there is a button to call the elevator to that floor (floor button). Inside the elevator, there is a button for each floor (elev. button), and an OpenDoor button that is used to keep the elevator door open for an extra time unit.

The elevator takes 2 time units to move between two consecutive floors. For example, to go from floor 1 to 2, it starts at 1, then goes between the floors for a time unit, and finally arrives at 2. The elevator cannot change direction while moving between floors.

When the OpenDoor button is pressed, the doors remain open for an extra time unit. However, the user should not be able to keep the door open infinitely often if there is a request for service.

You elevator controller must satisfy the following properties. The properties are given in a natural language. For each property, formalize it in CTL and verify using NuSMV.

1. Calls to the elevator from floors (i.e., floor button) are eventually serviced.
2. Calls from within the elevator (elev. button) are eventually serviced.
3. The elevator never moves with its doors open.
4. The elevator doors remain open until there is a request to use it.

5. It takes exactly 2 time units for the elevator to move between two consecutive floors.
6. If there are no requests for another floor, the elevator should not move.
7. The elevator cannot change direction between floors.

Additionally, create 2 more specifications (not equivalent to the ones above) that are vital for correct operation of the controller. Specify and verify them as well.

Modeling Instructions

- Ensure that the environment is modeled correctly. That is, there are no unnecessary constraints, and any constraints (such as fairness) are well documented
- Use FAIRNESS correctly. For each FAIRNESS statement give a short description why the assumption is meaningful.
- For each specification, describe its meaning in English, and provide CTL formalization. Ensure that properties are not satisfied vacuously.
- You may find property patterns useful for formalizing the specifications. `http://patterns.projects.cis.ksu.edu/documentation/patterns.shtml`
- Submit the following to the TA via the given email address.
  - `model.smv` : NuSMV Model
  - `report.pdf` : Brief report describing 1) assumptions made about the environment, 2) modeling decisions, 3) additional properties you have provided, and 4) verification time for the properties