Programming Assignment I: CTL Model Checking + NuSMV

Due-date: Mar 15 at 11:59PM (via Canvas). If you submit by Mar 12 at 11:59PM, you can earn 20% extra credit. Submissions after the deadline will not be graded unless explicit prior permission is granted.

Homework must be individual's original work. Collaborations of any form with any students (except our TA) or other faculty members are not allowed. If you have any questions/doubts/concerns, post your questions/doubts/concerns on Piazza and/or directly ask our TA or me.

Learning Outcomes.

1. Ability to encode design specification in NuSMV.
2. Ability to abstract specification details that are irrelevant in the context of verification of desirable properties/requirements.
3. Ability to apply formal methods (interpret model checking results, apply/encode temporal logic).

1 Problem 1: Verification

1.1 Specification

A train is controlled by a driver using two levers: a motion-lever and a door-lever. The driver can control the speed of the train using the motion-lever with the signals: `accelerate`, `break`. Similarly the doors of the train are controlled using the door-lever using the signals: `open`, `close`.

The states of the train are as follows:

- stopped: when its speed is 0 kmph.
- accelerating: when the speed goes up till it reaches 100 kmph.
- steady: when the speed of the train remains at 100 kmph.
- decelerating: when the speed goes down till it reaches 0 kmph.

The specification of the train movement is described as follows:

- if the train is stopped, the doors are closed and the driver accelerates, then the train goes to the accelerating state.
- If the train is accelerating and
  - the driver breaks, then the train goes to the decelerating state
  - the driver does nothing or accelerates, the train keeps accelerating till it reaches steady state.
- If the train is decelerating and

  - the driver accelerates, then the train starts accelerating
  - the driver does nothing or breaks, then the train keeps decelerating till it reaches stopped state.

- If the train is in steady state and
  - the driver breaks, then the train starts decelerating
  - the driver does nothing or accelerates, then the train remains in steady state.

The doors of the train can be in the following states: `open`, `opening`, `closing` and `closed`. The specification of the door functionality is described as follows:

- If the doors are closed, the train is not moving and the driver sends open signal via the door-lever, then the doors go to opening state.
- If the doors are opening and
  - the driver sends close signal, then the doors go to closing state
  - the driver does nothing, then the doors go to open state.
- If the doors are closing and
  - the driver sends open signal, then the doors go to opening state
  - the driver does nothing, then the doors go to closed state.
- If the door is open and the driver sends a close signal, then the doors go to closing state.

1.2 To Do

Use SMV model checker to prove/disprove that the doors are always closed unless the train is stopped.

1.3 To Submit

1. Submit one file: PA1-P1-⟨your-net-id⟩.txt. It should contain the encoding of the specification and the CTL property that you used to prove/disprove the above property.
2. At the top of the file, in comments, write the result of your verification. If verification result is true, then write the following:

   ```
   -- Property is proved to be satisfied
   ```

   If verification result is false, then write the following:

   ```
   -- Property is proved to be violated
   ```

   followed by multiple comment lines, where you will need to explain why the property is violated. That, what sequence of events as per the specification leads to the violation of the property. *Do not simply copy-paste the counter-example generated by NuSMV*, rather interpret the counter-example.

2 Problem 2: Planning

2.1 Specification

Fett sisters Xoba, Yoba and Zoba are accompanying three padawans (student or learner) to planet Tatooine. Each sister is responsible for taking care of her padawan. The Fetts do not trust each other and as a result, none of the sisters can leave her padawan with any one of the other sisters (for example, if Xoba leaves her padawan unattended with either Yoba or Zoba or both, then Xoba's padawan may be in mortal danger - grim situation it is).

On their way to Tatooine, the Fetts and their padawans need to move through hyperspace between two deserted planets: Isi and Iju. They have been able to "get" one lightspeed vessel, which can take them from planet Isi to planet Iju. Unfortunately, the vessel is a two-person vessel (for example, at a time two sisters or one sister and one padawan or two padawans can use the vessel). To further complicate the situation, the vessel is not equipped with Alset auto-drive, which implies someone needs to drive it. The Fetts (and padawans) need to strategize a way to use the vessel multiple times such that they can all safely escort their padawans from Isi to Iju.

2.2 To do

Model all possible movements between the planets and use a "safety" property to verify whether there exists a plan (sequence of movements) that will enable the Fett sisters to take their respective padawans from Isi to Iju.

2.3 To Submit

1. Submit one file: PA1-P2-⟨your-net-id⟩.txt. It should contain your encoding along with the property you used. (Follow the same technique as the farmer-goat-wolf-cabbage problem discussed).

2. At the top of the file, in comments, write the result of your finding. If there is no plan, then write

   ```
   -- No plan exists.
   ```

   and explain why (also in comments). If there is a plan, then write the steps in the plan as part of the comments.

3 Subscript

Before you start with this assignment, you will need to (a) download NuSMV, (b) get familiar with how NuSMV works and (c) know how to encode in NuSMV and interpret its outputs. *Late start and/or commencing with the assignment without completing these tasks may result is less than satisfactory score for this assignment*.