Programming Assignment I: CTL Model Checking + NuSMV

Due-date: Mar 7 at 11:59PM (via Canvas).

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.

1 Problem 1: Verification

1.1 Specification

Amir Pnueli (Turing Award Winner) presented the following mutual exclusion protocol for two processes.

```
// represents the behavior of process i, where i is either 0 or 1.
l0: loop forever do
    begin
    l1: Noncritical section
    l2: (y_i, s) := (true, i);  // y_i is assigned to true
                                // and s is assigned to i
                                // single step assignments
    l3: wait until ((y_{1-i} = false) OR (s != i));
    l4: Critical section
    l5: y_i := false
end.
```

The processes share a variable s which is either 0 or 1 (indicating the process ids). It is initialized to 1. The processes have a local variable boolean y_i that are initialized to false.

1.2 To do

1. Model the above protocol in NuSMV.
2. Verify the property that the processes do not have access to the critical section at the same time.
3. Verify the property that whenever a process wants enter the critical section, it will always eventually be able to do so. That is, it will not wait for unbounded time.

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 results of your verification. For each result, if the verification result is true, then write the following:

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

If verification result is false, then write the following:

```
-- Property X 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*.