Homework 3 (NuSMV): ComS/CprE/SE 412, ComS 512

Due-date: Feb 27 at 11:59PM (via Blackboard)

Homework must be individual's original work. You can discuss with your classmates in the course to better understand the problem; however, the solutions should be your own.

---

1. **Planning Problem**. A group of m Vulcans and n Klingons are on the east bank of a river. Consider that $m \geq n$. They need to cross over to the west bank. They have a boat, which can hold at most two riders. The boat cannot move from one bank of the river to the other on its own. If on any bank the Vulcans are outnumbered by the Klingons, then the Klingons may kill the Vulcans on that bank. Now that is a big problem for the Vulcans.

   But the Vulcans are brilliant logicians. They came up with a plan such that all of them (Klingons and Vulcans) will be able to cross the river using the boat and none of the Vulcans will get killed by the Klingons.

   Specify the problem in NuSMV (name the file $\langle yournetid \rangle$-hw3.1.txt: submit this) and obtain a solution to the problem by verifying the specification against a carefully selected CTL formula. Consider $m = 3$ and $n = 3$.

   (a) Extensively comment your code to explain your specification: what does the variables describe, how do their values change with each transition, etc.

   (b) Write the solution you obtain (if you can find a solution) in $\langle yournetid \rangle$-hw3.1.README (submit this as well).

   [**Additional Questions for Students in COMS 512. Write the answers in $\langle yournetid \rangle$-hw3.1.README.**]

   (a) Explain how you can extend the specification of the problem so that the existence of solution can be checked for different values of m and n with minimal changes to the specificaton.

   (b) Present solution, if any, when $m = n = 2$.

   (c) Present solution, if any, when $m = n = 4$.

2. Load balancing is an important aspect in aircrafts; it is involved with "evenly" distributing the weight of the passengers, cargo and fuel throughout the aircraft. This is necessary to ensure that the aircraft's center of gravity remains close to its center of pressure. Fuel distribution control system in an aircraft plays a vital role in this context, distributing fuel appropriately among many fuel tanks.

   We will consider a part of the fuel distribution control system in the aircraft which is responsible for making sure that the forward tanks contain fuel at a necessary level. **You are required to model its behavior following the specification in this assignment**. The control system consists of five components:

   (a) Master fuel distributor

   (b) Backup fuel distributor

   (c) Bus

   (d) Tank sensor controller

   (e) Tank fuel controller

   The master and backup fuel distributors communicate directly. All other components communicate via the bus; the bus consists of dedicated channels for communicating components, i.e., if components i and j exchange messages via the bus, the latter provides a dedicated channel to allow such exchange. The specification of the behavior of the distribution control system is as follows:

(a) If the tank sensor controller senses that the fuel level in the forward tanks has fallen below a threshold, it sends that information to the master distributor.

If the tank sensor controller senses that the forward tank fuel level has been below a threshold for a certain period of time, it also sends that information to the backup distributor.

The tank sensor stops sending information whenever it records that the fuel level is increasing.

(b) Whenever the master distributor receives information of low fuel level in the forward tanks, it signals the tank fuel controller to push fuel to the forward tanks.

(c) Whenever the backup distributor receives information of low fuel level in the forward tanks, it checks whether the master distributor is unresponsive or not. If it finds the master distributor to be unresponsive, it signals the tank fuel controller to push fuel to the forward tanks.

(d) Whenever the tank fuel controller pushes fuel to the forward tanks, the tank sensor immediately senses the increase in the fuel levels.

Consider the following hazards provided by the system engineer:

Hazard 1. Master distributor can become unresponsive at any time.

Hazard 2. Bus can lose information being transferred through it finitely many times. This is interpreted as follows:

- The bus has multiple communication channels. All channels are reliable infinitely often, i.e., do not remain un-reliable all the time.

Hazard 3. Bus can lose all information being sent from the master distributor.

In the presence of each hazard, prove/disprove the property that the fuel level does not permanently remain below threshold in the forward tanks.

You are required to use NuSMV model checker and CTL for this assignment.

Strategies for capturing system behavior.

- Make each component a module in NuSMV.
- Make each channel a module as well.
- If module A changes its state due to message it receives from module B, then you can model this behavior by changing the state of the A based on B's state. I.e., make sure that A's definition takes B's state as a parameter input, so that the guards on the `next` description in A can use the B's state.
- Use FAIRNESS to model paths in the Kripke structure where certain phenomenon occurs infinitely often.

  ```
  FAIRNESS !p;
  ```

  implies that only the paths where states satisfying $!p$ hold (i.e., p does not hold) infinitely often are considered for model checking.

You are required to submit

- the NuSMV model along with necessary CTL formula in a file named: $\langle yournetid \rangle$-hw3.2.txt. The model must be commented appropriately, explaining clearly (a) how your model aligns with the specification of the fuel distribution control system and the hazards. (You will have three different modifications for three different hazards – explicitly mention the commenting/uncommenting of the code necessary to capture each hazard); (b) how your CTL formula capture the property being considered.

- the explanation text file named: $\langle yournetid \rangle$-hw3.2.README. The file will contain your results: how you proved/disproved the above property regarding fuel level.

  COMS 512. If your results show that the above property is violated under any hazard, provide an alternate behavioral specification of the system to the system engineer such that the violation can be avoided under the hazard. Explain how such alternate model can be realized from your original model.