CS5219 Assignment #1

6 February 2017

Please read this assignment specification ***fully***. You are responsible for ***everything*** it contains.

Deadline

This assignment is due at **18:00 (6:00pm) on Monday 13 March 2017**. Please plan your time accordingly, as there will be ***absolutely no late submissions*** allowed. And have fun!

Problem Statement

In this coursework, you will use Spin to construct, simulate and verify a Promela model of a *self-driving car*. You will carry out this assignment on an *individual* basis, as specified in detail at the end of this assignment specification.

To complete the assignment, you will need to familiarize yourself with Spin's features and the Promela language, and you must either download and install Spin (iSpin) on your own computer, or else use the version of Spin installed in Programming Lab 1 (COM1-B1-12).

Please let Yamilet (yserrano@comp.nus.edu.sg) know if you want to set up a consultation about the assignment.

Background

In 2014, Google unveiled a fully functioning self-driving car. This prototype is a driverless car that has neither a steering well nor pedals. In a self-driving car, driving is handled by software and sensors.

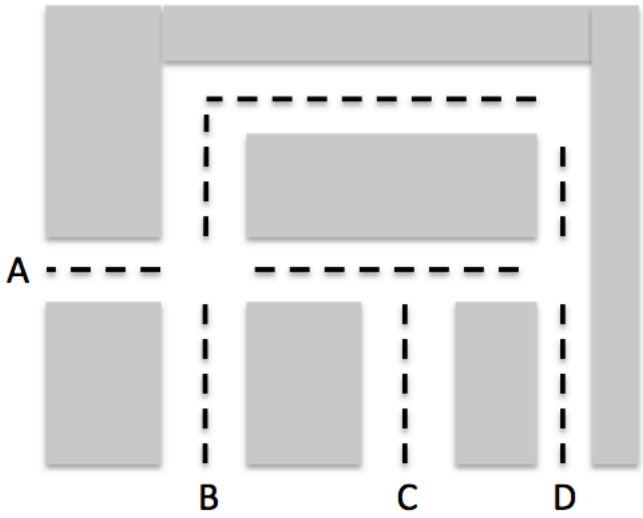
The self-driving car uses sensors that detect objects as far as two football fields always in all directions. The software then classifies these objects based on their size, shape and movement pattern; for instance, a cyclist will ride down a street, while a pedestrian will cross the street. The software chooses a safe speed and trajectory for the car based on its analysis of the detected objects; for instance, the car nudges away from the cyclist and slows down to yield to the pedestrian.

In addition, the self-driving car maintains information about the street it is on and which lane it is in through an internal map plus information from the sensors. In order to reduce the kinetic energy of the car in any possible crash, the speed of the car is limited to 25 miles per hour. Note that the self-driving car has defensive behavior for protecting both the passengers and other road users.

The following are some suggestions for how to go about specifying your model:

- Model self-driving cars as Promela processes. You should be able to construct a self-driving car process and instantiate it multiple times. In constructing your model, ***think abstractly!***

- Consider the following two-dimensional map as the scenario where self-driving cars could move. A car moves only forward on the street. Backward motion is not allowed.



- Use appropriate Promela features to represent the above map and the possible movements of the car. Recall that the software of a self-driving car chooses its trajectory.
- The initial position of each car could be random, such as one of the four entries (A, B, C and D).
- Use simplifying assumptions regarding the configuration of a car's speed. For instance, suppose the car can drive in only two speeds. Remember the limited speed is 25mph.
- Consider the set of properties that can involve some conflicts in the driving of the cars. Note that you are not necessarily expected to produce a collision-free model.
- ***Bonus:*** You might create a different map where the self-driving cars can move, and you might determine other features that have not been specified in this assignment.

Requirements

For the assignment, you must complete the following steps:

1. Specify in Promela a model of self-driving cars to at least a level of detail as suggested above.
2. Identify important properties of the model and specify them using Promela *assertion* statements, *never* claims, and/or *ltl* formulas.

3. Use Spin to generate an example execution trace for your model.
4. Use Spin to generate a verifier from your model, compile it, and run the generated verifier to verify your model against your properties. Generate verifier output for your model.
5. Upload a ***single ZIP file*** to the folder **Assignment 1 Submissions** of the workbin in *IVLE*. ***Include your matriculation number in the filename.*** Put the following deliverables in the ZIP file:
    a. The Promela model
    b. The property specifications
    c. Your set of generated execution traces
    d. Your set of verifier outputs
    e. A 1-page report discussing your assumptions, insights, difficulties, etc., in specifying and debugging your model, specifying properties, or any other aspect of completing the coursework.

You may complete this coursework using either the command-line version of Spin or a GUI-based version of Spin such as iSpin.

Grading

This coursework is worth 15 marks toward your final module result, with the marks allocated as follows:

- Promela model (65%)
- property specifications (25%)
- execution traces and verification outputs (5%)
- 1-page report (5%)

At a minimum you are expected to produce a functioning model and some verifiable properties. Higher marks will be earned for greater originality and effort, such as through a more complex and detailed model, more elaborate properties, greater range of features, a more extended use of Spin, and so on.

Individual Effort

This coursework is to be completed as an *individual effort*. *All* work should be *completely original*, completed *solely* by the individual, and *without* derivation from or reference to *any* models or solutions that may be accessible from other sources. (If you can find it, I can find it!)

In uploading your deliverables to the workbin, you are confirming that you understand and agree to *all* of the above requirements, and that you have abided by the university's policy on plagiarism:

http://www.nus.edu.sg/osa/images/osa/downloads/code_of_student_conduct.pdf