Project 2017/18

Reactive Systems Verification

MSc in Computer Science

University of Camerino

Prof. Luca Tesei

Description

Consider the traffic flow of some cars on a one-lane bridge that has two traffic lights on both sides (left and write) to regulate the access. The following information is given for this scenario:

- the bridge cannot sustain more than N cars at the same time;
- a car may decide, at a certain point (including the initial time), to approach the bridge at one of the two sides; this is signalled to the controller by a sensor on the road;
- a car can (actively) idle in its initial state, even for nearly all the time;
- after approaching the bridge, from any side, a car starts waiting until it is given explicit access to it by the controller with a signal (e.g. a green light);
- when on the bridge, a car crosses it and then exits;
- a car exiting the bridge is signalled to the controller by another sensor on the road;
- after exiting the bridge a car goes to its initial state and may immediately approach the bridge again, on any side;
- if no cars are on the bridge and there are cars approaching on both sides, then the access is given to the side whose turn is active;
- whenever a side uses its turn, then the turn is given to the other side; initially the turn is on the right side;
- if there are cars on the bridge and there are cars approaching on both sides, then the access is not given to any side until all the cars currently on the bridge exited it;
- if no cars are on the bridge and if there are cars waiting only on one side, they are given access to the bridge no matter which side the turn is of; this does not change the turn;
- if there are cars on the bridge and if there are cars waiting only on one side, they are given access to the bridge only if there is room and their flow is equal to that of the one(s) currently on the bridge; otherwise they have to wait at least until the bridge becomes empty;
- the flow of a car (left to right or right to left) on the bridge cannot change;
- the waiting cars are given access to the bridge with a FIFO (first in first out) policy.

Your tasks are:

1. Model the above scenario in SPIN; instantiate N with 2 and ensure the presence of at least 3 cars.
2. Write the following properties as LTL formulas and model check them with SPIN on the given model:
   (a) it is never the case that more than $N(= 2)$ cars are on the bridge;
   (b) it is never the case that $N(= 2)$ cars with different flows are on the bridge;
   (c) a car that approached the bridge from the left side must exit from the right side;
   (d) whenever a car approaches the bridge from the left side, it will eventually leave the bridge on the right side;
   (e) if a car approaches the bridge from the right side infinitely many times, it will cross the bridge infinitely many times;
   (f) whenever a car is on the bridge, it eventually will leave it;
   (g) if from a certain time on no cars approach the right traffic light, then eventually the turn stops changing between sides;

Submission

Prepare a written report describing your model of the scenario and how you expressed the properties. You can use screenshots to show some of the results.

Send by email to the teacher the SPIN files and the report in pdf. The sending must occur before the starting of a written test (fixed for each exam session): a student that has not sent the project before the written test can not participate to the written test. The exam is passed when both the following conditions are satisfied:

1. the project has been sent and has been approved;
2. the written test has been passed;

In case a student does not pass the written test, he/she does not have to resend the (approved) project before the next attempt(s) to the written test. The final grade is a combination of the grades of the two tasks.