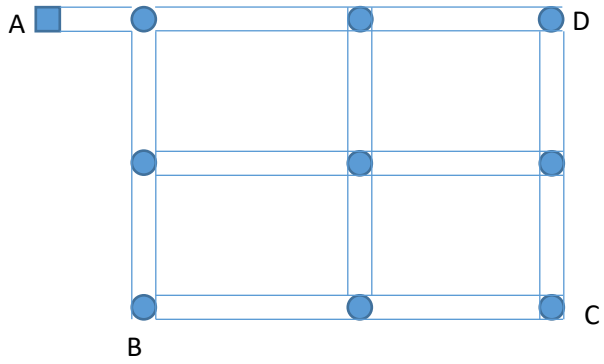
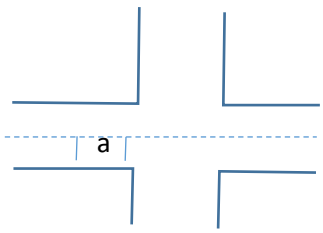
ECEN689-602/CSCE689-603
Introduction to Formal Verification Fall 2021
Project Overview

This project is to design a simplified traffic system and verify its properties. The road system is like below,



which has three horizontal roads and three vertical roads. Each circle is a road intersection. Each vehicle departs from A, visits B, C and D in any order and returns to A. The distance between two neighboring circles is 0.5 mile and the distance from a square to its adjacent circle is 1/30 mile. A car can either run with speed of 30 miles per hour or stop.

Each road segment between two intersections is divided into 30 uniform-sized slots. Each control step (or time step) is 2 seconds. At each control step, a car must be within a slot. In the next step, it can either stay there or move to the next slot. Along each direction, there is a single lane. For example, in the figure below, there is one intersection among four edges. Car 'a' is at the rightmost slot of the left segment. In the next step, it can go to either of the following: (1) go straight to leftmost slot of the right segment, (2) turn right to the topmost slot of the bottom segment, (3) turn left to the bottom slot of the top segment. Between two consecutive time steps, there is at most 1 car crossing an intersection. If at any moment, there are more than one car in the same slot, that is counted as a collision. A car must stop at "red" light as well, and cannot make right turn. The problem formulation is to maximize the total number of cars reaching each of the 4 square node destinations per hour, without any collision, without any red-light signal violation. Each i-group must verify and report the number of collisions and red-light signal violations. There are green and red lights, but no yellow lights.



Additional specifications to the system:

- On each direction of each road, there is a single lane.
- At each intersection, between two consecutive time steps, there is at most 1 car crossing the intersection.
- There are at most 4 signal lights at each intersection. At any time, at most 1 light can be green.
- A car can see another car in front it on the same direction with distance no more than 0.5 mile away without any other third car in between.
- At an intersection, a car can see other cars at the same intersection.
- A fundamental constraint is that a car cannot run in a lane opposite its driving direction.
- U-turn is not allowed.
- A v-group knows the number of cars stopping at each intersection as congestion information. "Stopping" means no move from the previous time step to the current time step.
- The three constraints: no collision, no violation of red light signal, no run of opposite direction lane, should be verified in both i-group and v-group. And the verification results should match.
- If there is collision, the reason may be from either i-group or v-group, depending actual cases.
- At a time-step, if car P sees another car Q in front of P along the same direction, car P cannot move to the next time step.

There are 43 students in the class. They are divided into 10 teams. Each team has one infrastructure groups (i-group), and one vehicle groups (v-group). Each group has two students. You are required to sign up a google spreadsheet to form groups by October 15, Friday. If you do not sign up, I will assign arbitrarily.

An i-group will develop a software simulating road infrastructure. It can receive vehicle signals from v-group to know vehicle location, speed and moving directions. But i-group does not know if a car would make turn or go straight at an intersection. It will decide the green/red light on/off at each road intersection. Each v-group will develop a software simulating a number of vehicles in the road system. A vehicle starts from point A, visits B, C and D in any order, and then returns to A. It can receive traffic congestion map from itself, and then decide the best route to reach its destination in the shortest time. The results for both i-group and v-group are evaluated by overall throughput (number of cars completing the tour per hour) of the road system, the number of collisions, the number of illegal running directions, the number of U-turns, and the number of red-light violations.

Important deadlines:

1. Sign up groups by Oct 15, Friday.
2. Project phase A design report (13 points) due on November 2, Tuesday.
3. Project phase B (7 points), due on November 11, Thursday.
4. Project phase C verification report (15 points), due on November 24, Wednesday.

Phase A: each group finishes its part of software design, debugging, and shows results.

Phase B: codes of two groups of the same team are merged, debugged with results; find a verification tool, run a small example to demonstrate the use of this tool.

Phase C: finishing verifying specified properties for both i-group and v-group.