Formal Methods – Course Project (Undergraduate Students)

Objective

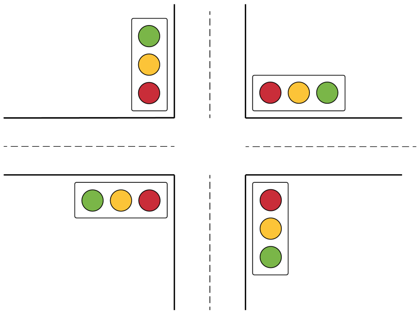
Formally specify a Traffic Control System (TCS) and verify its correctness using TLA+ and PlusCal.

Format

This project is to be carried out in groups of 2-3 students. Students are allowed to self-organize in groups. (Use the class time or the forum on the Coursespaces Web site to team up with other group members. Contact your instructor ASAP if you have difficulties finding team members.)

Part 1: Simple TCS

The TCS shall control a four-way intersection. The lights are automatically toggled based on a predefined interval.



Prove that your specification meets the following properties:

1. Either NS direction or EW direction are green (or yellow) but not both.
2. Traffic lights always cycle in the same order, from red to green to yellow to red… etc.
3. The system behaviour is lively, i.e., no traffic light gets stuck at a particular colour.

Part 2: TCS with pedestrian crossing

We now add pedestrian crossings in each direction. Pedestrians can push a button, indicating that they are willing to cross. Pedestrian lights remain red unless a pedestrian has indicated a willingness to cross. Pedestrians have a limited amount of time for crossing (green phase).

Create a new specification for the TCS with pedestrian crossings. Prove that the new specification is an implementation of the specification of Part 1, under a refinement mapping.

Prove that your specification meets the following properties:

1. A button press by a pedestrian will eventually lead to a green pedestrian light in the desired direction.
2. A pedestrian light can only become green when all vehicle lights are red.
3. If a pedestrian light is green in a particular direction (NS or EW), then traffic lights in the opposite direction must be red.
4. Pedestrian lights cycle orderly (red → green → yello → red, etc.)
5. The green-yellow interval for pedestrians is shorter than the green-yellow interval for vehicles in the same direction.

Part 3: TCS with Traffic-awareness

We now add vehicle sensors in the road for traffic-awareness in our TCS. The idea of a travel-aware TCS is to maximize green cycles based on vehicle traffic load. Each lane oncoming to the intersection now has a vehicle occupation sensor. This allows the TCS to consider oncoming traffic when controlling the traffic light. You may assume that the vehicle sensor is perfect (even detects bicycles), so that light-switching of the new TCS system can be controlled completely by sensors rather than time-based switch.

Create a new specification for the TCS with traffic-awareness. Prove that the new specification is an implementation of the specification of Part 2, under a refinement mapping.

Prove that your specification meets the following properties:

1. If a vehicle is detected in an oncoming lane, eventually the traffic light in the corresponding direction will switch to green.

Part 4: Implement your TCS programs

Implement all three versions of the TCS system in a language of your choice. The programs should be able to simulate and visualize the intersection

Annotate your program code for traceability to the specification, i.e., your annotations should show how your source code relates to your specification. (This is called taceability. It is required in many standards on developing safety-critical systems.)

Also add automated unit tests to test your program implementation.

Submission

Submit a zipped archive (please use Zip – not another archiver) containing the following on the course Web site by Nov. 21:

- A PDF document documenting your specification and proofs for Part 1-3.

- The corresponding .TLA files for your specifications (Part 1-3)
- Your program (executable and source code)
- A description on how to run and use your program
- A work-log document that indicates which team member worked on what aspect of this project at what time (including team meetings).

Evaluation

	100%	75%	50%	25%
Contents	All four parts have been completed correctly	Three parts have been completed correctly	Two parts have been completed correctly	One part has been completed correctly
Form	The specifications, program and report are complete and well structured	The specifications, program and report are complete but the structure or presentation could be improved	The specifications, program and report are partially complete or there are significant structural or presentational weaknesses	The specification, program and report are incomplete

The work-log document may be used for differential grading, only in cases where there is an imbalance between the effort committed by the different team members.