Specification and Verification of Programs

Course Project Due date: July 10, 2019

Consider the street network in small town with crazy drivers represented with a graph (probably crossroads and streets should be represent by nodes and/or edges!).

Assume that time has a *discrete* nature and the speed of all cars are equal to preserve the simplicity of passing of time. For each street a fixed value, *capacity*, is defined which is the minimum number of cars that will cause the traffic speed to become zero in the street. In each time step, the *traffic load* of each street is calculated as the number of cars in the street.

Moreover, for each street there is a given *normal travel time* which indicates the number of time steps needed for moving from the beginning to the end of the street. Obviously, this amount of time should change according to the *traffic load* in the street. You should consider a linear relation between traffic load and travel time (reaching infinity if the load is greater than the street capacity).

The way of a car is *blocked* (intuitively for a limited time from current time step) in a crossroad if for all outgoing streets the load is equal to or more than the street capacity.

Each driver has a *source* and a *sink* (i.e., two states in the modeled transition system) but she decides to choose a way in a greedy manner: select the edge with lowest traffic load. *Congestion* is defined as having a node with incoming traffic greater than its outgoing traffic.

You should describe the specification of the system and then model the problem in NuSMV. Then check various properties such as followings:

a) All drivers will reach their destinations.

b) Their will not be some congestions in the network now and then during some time periods but the congestion will be removed sooner or later.

c) The trip time of each car is rational.

d) …. (Fill the blanks!)

To show the correctness of your specification, you need good samples for street network. Here a very simple example is provided in which c stands for capacity and tt denotes travel time. Assume a single source and a single sink for all cars. Running this example is necessary but not sufficient.