# Application of Abstractions to verifying MoveOn’s VTL simulation

Abstractions are techniques used to simplify the model or state machine under verification, which could possibly lead to faster verification. In VTL+, there are various modules of the system that can be abstracted out and verified independently including normal traffic lights, VTL only traffic lights, and so on. This involves removing variables, states and transitions from the model which are unnecessary in a particular subsystem and preserving those that are required.

We made all cars travel at the same speed. This resulted in a state-space explosion of having cars of different speeds or acceleration. This meant that all cars accelerated instantaneously after each other, which made it easier and more efficient to verify that all cars crossed the intersection safely within a specified amount of time of 3 seconds. Similarly, we also assumed that the cars were of the same length. This does not match the real world, for example a mini and a limousine are obviously not the same length and as such each car would spend different amounts of time in the intersection. Assuming that the cars are the same length allowed us to assume that the cars would all take the same amount of time to cross the intersection.

To make the model simpler we didn’t have cars turning at the intersections. This meant that the intersection only had two phases, cars traveling North/South moving, or cars traveling East/West moving. This also simplified the VTL controller as VTL cars didn’t not have to worry about other VTL cars turning across the path of each other.

In order to simplify the system for verification, each subsystem was abstracted out and verified independently. For example, having non-VTL cars only allows verification of normal traffic lights. In this subsystem, we verified for that the system cannot have both non-red lights for two intersecting roads. This is a stronger property which satisfies the one-way preservation, as if this property fails, it may (but not necessarily) imply a dissatisfaction of a property in the entire system. However, if this property passes, it ensures that the property in the entire system is safe. A similar abstraction was used for having VTL-only cars on the intersection and having only pedestrians on the intersection.

There are also potential abstractions which could have been used to simplify the system for verification that we did not use. We could have reduced the model to have only two light stages by abstracting out the orange light. This would have reduced the number of requirements needed to verify the system. Also we could have reduced the model to be a pedestrian intersection on a straight road. This would have simplified the verification for pedestrians, however it would have been an oversimplification when trying to verify the system for vehicles.