Using Control Synthesis to Generate Corner Cases: A Case Study on Autonomous Driving (EGSR_46)

G. Chou[1], Y. E. Sahin[1], L. Yang[1], K. J. Rutledge[1], P. Nilsson[2], and N. Ozay[1]

[1]*Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI*

[2]*Department of Electrical Engineering, California Institute of Technology, Pasadena, CA*

As complex autonomous driving systems start to be deployed in the real world, the need for methods that can detect faults in the self-driving software has become increasingly important. The process of generating difficult test cases which will cause the software to fail is known as falsification. In this work, we employ correct-by-construction control synthesis - in particular, controlled invariant set computations - to falsify self-driving software. A controlled invariant set describes the set of system configurations (in this case, the car orientation and velocity) from which there exists a control (steering/throttle command) to ensure the system behaves safely.

We show that if it is possible to compute a "large enough" controlled invariant set for either the true system model or some simplification of the system model, we can generate initial car configurations which falsify the software by sampling such configurations from the boundary of this controlled invariant set. Moreover, we show that even if the self-driving controller would crash under these initial conditions, we can use controls generated from the controlled invariant set to override (**supervise**) the self-driving controller to ensure safe system operation.

In addition to finding initial conditions which can falsify the controller during the initial transient, we use solutions from a dual game - a reachability game for the safety specification - to find road profiles (**disturbance inputs**) which can falsify the self-driving software after the initial transient. We also propose optimization-based heuristics for generating road profiles when the dual game has no solution. To demonstrate the proposed ideas, we consider case studies from basic autonomous driving functionality, in particular, adaptive cruise control and lane keeping.

We show how our proposed technique can be used to find interesting falsifying trajectories for classical control designs like proportional controllers, proportional integral controllers and model predictive controllers, as well as an open source real-world autonomous driving package. We also show we can supervise these controllers to guarantee safe behavior.