Provably safe composition of two autonomous driving functions via set-based contracts

Stanley Smith, Petter Nilsson, Necmiye Ozay

UNIVERSITY OF MICHIGAN

Introduction

For society to trust that automated systems will operate as expected, it is necessary to provide safety guarantees regarding their behavior. In the case of autonomous vehicles, the ability to do so is becoming increasingly important as more safety regulations are being enacted. Therefore, our motivation is to allow companies to assure safety officials that complex automated systems can be trusted to be safe.

Our approach can be outlined as follows:

- Consider the system as a composition of multiple subsystems
- Each subsystem's dynamics are dependent on the other subsystems' states
- Use assume guarantee reasoning to create subsystem contracts in the form of polyhedral invariant sets (Figure 1)
- Design sets such that, if every subsystems remains in its set, the overall composition is guaranteed to be safe

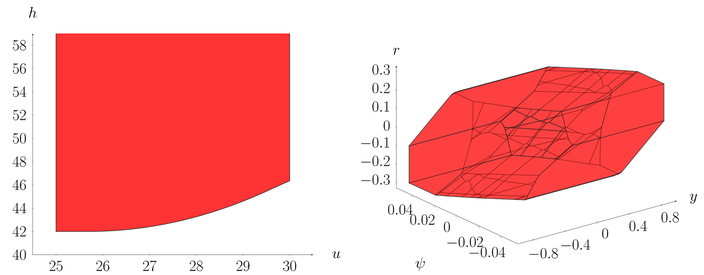

Figure 1 : Invariant sets for ACC and Lane Keeping that represent contracts

Main contributions

- Decomposed synthesis with overall guarantees
- Interdependence quantification via convex over-approximation
- Ability to handle nonlinear terms in uncertain system dynamics
- Monotonicity and convex projection approaches to finding convex hulls
- Demonstration with application to ACC+LK

I. Convex over-approximation

To quantify the interdependence between the subsystems, we take the state dependent terms of each subsystem's dynamics and then arrange them into a function which we wish to cover with a convex over-approximation (see Figure 2). The resulting convex hull can then be used to find a family of linear systems (see II. below).

We suggest two methods for finding these convex hulls depending on whether the aforementioned function exhibits certain properties - specifically, convexity and monotonicity. Such an approach is proven to not introduce conservatism.

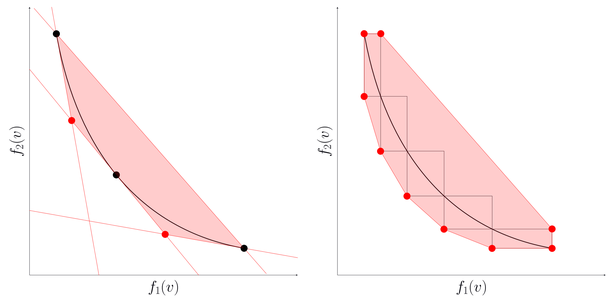

Figure 2 : The range of a function $f(v) = [f_1(v), f_2(v)]$ covered using the convex hull method (left) and the monotonicity method (right). The results can be used to over-approximate a system of the form $\dot{x} = A(v)x$, where the terms in $A(v)$ are linear combinations of f_1 and f_2.

II. Families of linear systems

A vertex of each resulting convex over-approximation corresponds to a member of a family of linear systems for the associated subsystem. The family of linear systems for each subsystem is a set of linear systems that has been constructed such that its convex hull covers all the possible values of the subsystem's dynamics (which are dependent on the states of the other subsystems). We find such a family for each subsystem, to be used during robust safety synthesis.

III. Robust safety synthesis

We first define the one-step backwards reachability operator of a set X of a family of systems. We iterate this operator on a safe set Y as

$$C_0 = Y, C_{k+1} = Y \cap Pre_{\{\mathcal{S}_i\}_{i\in I}}(C_k)$$

in order to converge inward to the maximal invariant set within Y. These iterations may not converge in a finite number of steps, so they are "robusitified" in the following manner as $C_0 = Y, C_{k+1} = Y \cap Pre_{\{\mathcal{S}_i\}_{i\in I}}(C_k \ominus \mathcal{B}_\infty(0, \epsilon))$ which is guaranteed to converge in a finite number of steps to an inner approximation of the maximal invariant set.

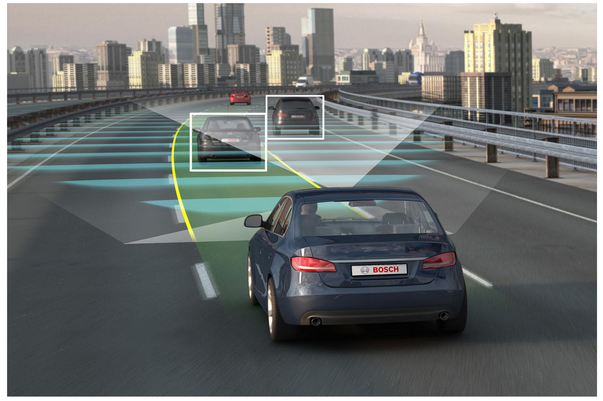

Image credit: Bosch

Example: ACC + Lane keeping

As an application, we synthesize controllers for two autonomous driving functions: adaptive cruise control and lane keeping. These subsystems exhibit interdependencies on eachother which manifest as state dependent terms appearing in the dynamics of each subsystem. We use the method outlined in I. II. and III. to compute controlled invariant sets for each subsystem. During simulation (shown in Figure 3), we choose steering and tire force inputs to enforce the state constraints imposed by these sets.

Results:

- All bounds are respected throughout the simulation as expected
- Controllers show ability to handle full level of system disturbance
- Positive results are achieved both in Simulink and Carsim

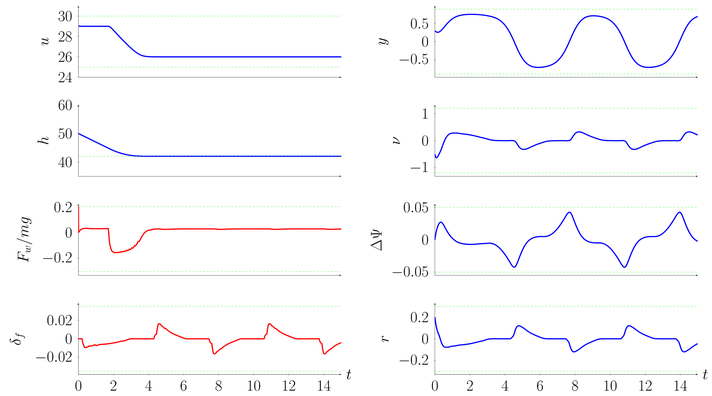

Figure 3 : Simultaneous implementation of ACC and LK controllers

Acknowledgments: This work is supported in part by NSF grants CNS-1239037, CNS-1446298 and ECCS-1553873.

swsmth@umich.edu, pettni@umich.edu, necmiye@umich.edu