Interdependence quantification for compositional control synthesis with an application in vehicle safety systems

Stanley W. Smith, Petter Nilsson, Necmiye Ozay

Abstract— **Composing controllers designed individually for interacting subsystems, while preserving the guarantees that each controller provides on each subsystem is a challenging task. Motivated by this challenge, we consider in this paper the problem of synthesizing safety controllers for linear parameter varying subsystems, where the system matrices of each subsystem depend (possibly nonlinearly) on the states of the other subsystems. In particular, we propose a method for synthesis of controlled invariant sets and associated controllers, that is robust against affine parametric uncertainties in the system matrices. Then we show for certain classes of parameter dependencies how to quantify the uncertainty imposed on the other subsystems by convexifying, with an affine map, the effects of these parameters. An analysis of this quantification is provided. In the second part of the paper, we focus on an application of this method to vehicle safety systems. We demonstrate how controllers for lane-keeping and adaptive cruise control can be synthesized in a compositional way using the proposed method. Our simulations illustrate how these controllers keep their individual safety guarantees when implemented simultaneously, as the theory suggests.**

I. Introduction

Engineering complex systems consisting of several interacting subsystems is a challenging task. Recent delays in the delivery of new generation aircraft and safety recalls for cars due to software bugs are indications of some of the challenges in system integration [16], [9]. Due to the high complexity of these systems, it is not possible to employ monolithic design tools that take into account all the interactions and specifications at once. Therefore, compositional design methodologies with correctness guarantees are needed.

Assume-guarantee reasoning and contract-based design are proposed as principled means for analysis and synthesis of complex systems in a compositional way [7], [3], [15]. The main idea in these approaches is to capture the interactions between subsystems in terms of formally stated assumptions and guarantees. The particular assumption-guarantee formalism depends on the type of specifications the system has to satisfy. For instance, the assumptions and guarantees could be given as automata [7], temporal logic formulas [15] or supply/demand rates [10]. Inspired by these ideas, in this paper, we propose a compositional safety control synthesis method where assumptions and guarantees are given in terms of polyhedral sets that are controlled invariant [5]. Set invariance is widely used for imposing safety in control systems [5] and we leverage a fixed point based characterization of invariant sets (e.g., [4], [6]) in this work.

In particular, we consider two subsystems, each with linear parameter varying models, where the parameters affecting the dynamics of a subsystem are the states of the other system. When the parameter dependence is affine and the parameters are constrained in a pre-specified polyhedral set, we present fixed point operations that can be applied separately to each subsystem in order to compute invariant sets. When the parameter dependence is through a nonlinear function but this function satisfies certain convexity or monotonicity conditions, we show how to compute a new dynamical model that is affine in a new set of parameters and that covers the effects of the original parameters on the original dynamics. Specifically, we show that there is no conservatism in such a covering when the constraint set of the new parameters is the convex hull of the image of the original parameter set through the nonlinear function. Note that this covering quantifies the effects of one subsystem over the other one. Therefore, a controlled invariant set that is robust against such parametric uncertainty is guaranteed to remain invariant as long as the other subsystem constrains its states to its pre-specified safe set.

In the second part of the paper, we focus on an application of these ideas to advanced safety and driver assistance systems, a path towards autonomous driving. We consider two subsystems: an adaptive cruise control (ACC) subsystem and a lane keeping (LK) subsystem. The ACC subsystem is responsible for tracking a desired speed or following a lead car while maintaining a certain distance to the lead car. The LK subsystem is responsible for keeping the vehicle in the lane. Although the states, control inputs and specifications are separate for these two subsystems, the longitudinal dynamics of the vehicle are not independent of its lateral dynamics and vice versa [18], [13], [1]. For instance, it is not possible for the LK subsystem to guarantee that the vehicle does not violate the lane boundary constraints from certain initial conditions, within its actuator limits, at very low forward speeds. Similarly, if the ACC subsystem does not make any additional assumptions on the operation of the LK subsystem, it cannot guarantee that a lead vehicle or desired speed is persistently tracked within a given bound. We first specify the requirements for each of these systems in terms of polyhedral safe sets and then compute the effects of each subsystem dynamics onto the other. Finally we separately synthesize controlled invariant sets and associated controllers

This work was supported in part by NSF grants CNS-1239037, CNS-1446298 and ECCS-1553873. The authors would like to thank Jessy Grizzle and Huei Peng for useful discussions regarding vehicle safety systems.

The authors are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI. Emails: swsmth,pettni,necmiye@umich.edu

for each subsystem and demonstrate the effectiveness of the proposed method via simulations where safety-enforcing controllers are implemented simultaneously.

In Section II below, we introduce notation and certain monotonicity concepts. Then we state the problem we seek to solve in Section III, and present our solution in Section IV. We illustrate the approach in Section V with an application to a LK and ACC system, before concluding the paper in Section VI.

II. Preliminaries

A. Notation

For two sets A and B, their *Minkowski sum* is denoted by $A \oplus B := \{a + b : a \in A,\ b \in B\}$. The *Minkowski difference*, denoted $A \ominus B$, is the maximal (w.r.t. inclusion) solution of $X \oplus B = A$. The infinity-norm ball around a with radius r will be denoted as $\mathcal{B}_\infty(a, r) := \{b : \|a - b\|_\infty \leq r\}$. For a mapping $f : \mathbb{R}^n \to \mathbb{R}^m$, the *image* of $A \subset \mathbb{R}^n$ is $f(A) := \{f(a) : a \in A\} \subset \mathbb{R}^m$, and the *pre-image* of $B \subset \mathbb{R}^m$ is $f^{-1}(B) := \{x \in \mathbb{R}^n : f(x) \in B\}$.

We will denote the k-simplex as $\Delta_k := \{\boldsymbol{\alpha} \in \mathbb{R}^k_+ : \sum_{i=1}^k \alpha_i = 1\}$. The convex hull of a set A can then be written as

$$\mathrm{Conv}(A) := \bigcup_{k \geq 1} \left\{ \sum_{i=1}^k \alpha_i a_i,\ \boldsymbol{\alpha} \in \Delta_k,\ a_i \in A\ \forall\ i \right\}.$$

If the set A is finite, i.e. $A = \{a_1, \dots, a_k\}$ for some $k \in \mathbb{N}$, the convex hull is $\mathrm{Conv}(A) = \left\{ \sum_{i=1}^k \alpha_i a_i \ :\ \boldsymbol{\alpha} \in \Delta_k \right\}$.

B. Monotonicity

We will leverage the concept of monotonicity to find over-approximations of set images. Monotonicity is defined with respect to a given *cone*, which is a set $K \subset \mathbb{R}^n$ such that $x, y \in K$ implies $x + y \in K$, and such that $x \in K$ implies $\alpha x \in K$ for all scalars $\alpha \geq 0$. A cone K induces a partial ordering $\leq_K$ on $\mathbb{R}^n$ given by

$$x \leq_K y \quad \iff \quad y - x \in K.$$

An *interval* with respect to a cone K is a set X for which there exist extreme points $x^-, x^+ \in X$ such that $x^- \leq_K x \leq_K x^+$ for all $x \in X$. We denote the intervals by $[x^-, x^+]_K$, and omit the cone K and write $[x^-, x^+]$ when K is clear from the context. For instance, when the cone K corresponds to one of the orthants in $\mathbb{R}^n$, intervals are essentially hyper rectangles. Note that intervals are convex sets.

Given two cones $K_1 \subset \mathbb{R}^n$ and $K_2 \subset \mathbb{R}^m$, we say that a function $f : \mathbb{R}^n \to \mathbb{R}^m$ is *monotone* on the set X with respect to K_1 and K_2 if for all $x, y \in X$, $x \leq_{K_1} y$ implies that $f(x) \leq_{K_2} f(y)$.

Evidently, monotone functions preserve intervals. In particular, suppose f is monotone on X with respect to the cones K_1 and K_2 and consider an interval $Y = [y^-, y^+]_{K_1} \subset X$. Then

$$f(Y) \subset [f(y^-), f(y^+)]_{K_2}. \tag{1}$$

This fact will be exploited later in the paper to find convex over-approximations of the image $f(Y)$.

III. Problem formulation

For simplicity of the notation, we state the problem we seek to solve for two interdependent subsystems, however, it is possible to extend the ideas in this paper to an arbitrary number of subsystems. Consider a dynamical system with states $x = [x_1^\intercal, x_2^\intercal]^\intercal$, split into two components corresponding to the states of the individual subsystems. We assume that the dynamics of the overall system is of the following form:

$$\begin{aligned} x_1^+ &= A^1(x_2)x_1 + B^1 u_1 + F^1(x_2), \\ x_2^+ &= A^2(x_1)x_2 + B^2 u_2 + F^2(x_1), \end{aligned} \tag{2}$$

where each subsystem $i \in \{1, 2\}$ is affine in its own states x_i; and its system matrices depend (possibly nonlinearly) on the other system's states x_j, $j \neq i$. We further assume that the inputs u_i and the states x_i are constrained to polyhedral sets U^i and X^i, respectively. The problem we seek to solve can be formally stated as follows.

Problem 1: Given a system of the form (2) together with input and state constraints for each subsystem, find sets $C^i \subset X^i$ such that

$$\forall x_i \in C^i,\ \ \forall x_j \in C^j\ j \neq i,\ \ \exists u_i \in U^i\ \ :\ x_i^+ \in C^i, \tag{3}$$

for each $i \in \{1, 2\}$.

Before proceeding to provide an approach to solve this problem, a few remarks regarding the existence and non-uniqueness of the solutions are in order. Note that if we can find a pair of inputs $(u_1^e, u_2^e) \in U^1 \times U^2$ that renders $(x_1^e, x_2^e) \in X^1 \times X^2$ an equilibrium point for the dynamics (2), then the singleton sets $C^1 = \{x_1^e\}$ and $C^2 = \{x_2^e\}$ constitute a solution to Problem 1. As a consequence of the Brouwer fixed point theorem and certain continuity results [2], existence of such an equilibrium is also a necessary condition for Problem 1 to have a solution.

On the other hand, given that a solution exists, it is desirable to find a solution where each C^i is as large as possible to increase the number of initial states from where invariance of the X^i's can be enforced. However, a larger C^1 potentially implies a smaller C^2 since subsystem 2 needs to tolerate more uncertainty in its system matrices as C^1 gets larger; and vice versa. Therefore, in general, there is no unique globally maximal solution in the sense of set inclusion. Any solution can be thought of as an assume-guarantee contract, where one can think of C^i's as contracts each subsystem is promising to the other. Along this analogy, we develop an approach that decouples the computation of invariant sets, where we start with promises from each subsystem and seek invariant sets for subsystems separately; and we exchange information if the promises cannot be met.

IV. Approach

We propose a solution to Problem 1 based on polyhedral sets that are controlled invariant for families of systems. The synthesis problem is symmetric with respect to the system index $i \in \{1, 2\}$, we therefore restrict attention to a single parametric subsystem. In the following, we first describe how polyhedral controlled invariant sets are computed for affine systems, and then extend the computation to families of affine systems. Subsequently, we describe two methods to find over-approximations of parametrized systems in the form of families of affine systems. We then piece these parts together in Section IV-D to obtain an algorithm that solves Problem 1.

A. Polyhedral Controlled Invariant Sets

In order to introduce invariant set computations for affine systems, we consider discrete-time affine systems of the form

$$\mathcal{S} : \begin{cases} x^+ = Ax + Bu + F, \\ u \in U. \end{cases} \tag{4}$$

Definition 1: The *one-step backwards reachability operator* of a set X under dynamics $\mathcal{S}$ is

$$\mathrm{Pre}_{\mathcal{S}}(X) := \{x \ : \ \exists u \text{ s.t. } Ax + Bu + F \in X\}. \tag{5}$$

In the case when the sets X and U are *polyhedra*, i.e., are defined by linear inequalities $X = \{x : H_x x \leq h_x\}$ and $U = \{u : H_u u \leq h_u\}$, $\mathrm{Pre}_{\mathcal{S}}(X)$ can be computed as the projection of a polyhedron in $x-u$-space according to

$$\mathrm{Pre}_{\mathcal{S}}(X) = \left\{x : \exists u \text{ s.t. } \begin{bmatrix} H_x A & H_x B \\ 0 & H_u \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} \leq \begin{bmatrix} h_x - H_x F \\ h_u \end{bmatrix} \right\}.$$

Later, we are interested in establishing safety guarantees when systems are composed. Safety is immediately related to the concept of controlled invariance, which is defined as follows.

Definition 2: A set X is *controlled invariant* under the dynamics $\mathcal{S}$ if for all $x \in X$ there exists a $u \in U$ such that $Ax + Bu + F \in X$.

If a set X is controlled invariant, a controller can guarantee that states outside of X are never reached, thus fulfilling a safety specification. An important problem is to find a controlled invariant set contained in a given safe set. Given the one-step backwards reachability operator $\mathrm{Pre}_{\mathcal{S}}$, the iterations $C_0 = Y$, $C_{k+1} = Y \cap \mathrm{Pre}_{\mathcal{S}}(C_k)$ will result in a monotonically decreasing (w.r.t. set inclusion) sequence of sets that converges to the maximal controlled invariant set contained in Y [4]. However, the iterations may not converge in a finite number of steps and if the algorithm is terminated early, the result is not controlled invariant. To overcome this limitation, the iterations can be "robustified" as

$$\begin{aligned} C_0 &= Y, \\ C_{k+1} &= Y \cap \mathrm{Pre}_{\mathcal{S}}(C_k \ominus \mathcal{B}_\infty(0, \epsilon)). \end{aligned} \tag{6}$$

It can be shown that for any $\epsilon > 0$, these iterations will produce a controlled invariant inner approximation of the maximal controlled invariant set in a finite number of iterations [6]. Since the inner approximation is itself controlled invariant, it can be used to implement a controller that guarantees safety. The tightness of the inner approximation will increase as ϵ decreases, the paper [6] contains an algorithm that estimates the maximal ϵ needed to achieve a given approximation error.

Remark 1: For brevity, we consider systems of the form (4) in this paper. However, the Pre operator, and hence also the invariant set algorithm, can be augmented in order to treat systems with disturbances, piecewise linearities, and state-dependent input constraints [12].

B. Extension to systems with uncertain A,F matrices

In the following, we extend the invariant set algorithm to finite *families* of discrete-time linear systems $\{\mathcal{S}_i\}_{i \in I}$, where for each $i \in I$,

$$\mathcal{S}_i : \begin{cases} x^+ = A_i x + Bu + F_i, \\ u \in U. \end{cases} \tag{7}$$

We will be interested in all convex combinations of systems in $\{\mathcal{S}_i\}_{i \in I}$, which is a concept that warrants a precise definition.

Definition 3: Consider the set $\mathfrak{C}$ of pairs (A, F) defined as follows

$$\mathfrak{C} := \left\{ (A, F) : \begin{array}{c} \exists \boldsymbol{\alpha} \in \Delta_{|I|} \text{ s.t. } A = \sum_{i \in I} \alpha_i A_i, \\ F = \sum_{i \in I} \alpha_i F_i \end{array} \right\}.$$

Then, the *convex hull* of $\{\mathcal{S}_i\}_{i \in I}$, is defined as the collection of systems

$$\mathrm{Conv}\left(\{\mathcal{S}_i\}_{i \in I}\right) := \left\{ \begin{cases} x^+ = Ax + Bu + F \\ u \in U \end{cases}, \ (A, F) \in \mathfrak{C} \right\}.$$

Analogous to Definition 1, we define a backwards reachability operator for families of systems.

Definition 4: The *one-step backwards reachability operator* of a set X of a family $\{\mathcal{S}_i\}_{i \in I}$ of systems is

$$\begin{aligned} \mathrm{Pre}_{\{\mathcal{S}_i\}_{i \in I}}(X) := \{x \ : \ &\forall (A_i, F_i) \\ &\exists u_i \in U \text{ s.t. } A_i x + Bu_i + F_i \in X\}. \end{aligned}$$

It directly follows from the definition that $\mathrm{Pre}_{\{\mathcal{S}_i\}_{i \in I}}(X)$ can be computed as

$$\mathrm{Pre}_{\{\mathcal{S}_i\}_{i \in I}}(X) = \bigcap_{i \in I} \mathrm{Pre}_{\mathcal{S}_i}(X). \tag{8}$$

Now, in order to compute invariant sets for families of systems, it suffices to replace the single-system Pre operator in the iterations (6) with its counterpart for families of systems given in (8).

Due to linearity, we can show that only the extremal systems (i.e., systems that are not linear combinations of other systems) in a family $\{\mathcal{S}_i\}_{i \in I}$ will affect the backwards reachable set. As a consequence, "over approximating" a family $\{\mathcal{S}_i\}_{i \in I}$ with $\mathrm{Conv}(\{\mathcal{S}_i\}_{i \in I})$ does not introduce conservatism in the invariant set computation.

Proposition 1: Given a convex set X, we have $x \in \mathrm{Pre}_{\{\mathcal{S}_i\}_{i \in I}}(X)$ if and only if $x \in \mathrm{Pre}_{\mathcal{S}}(X)$ for all $\mathcal{S} \in \mathrm{Conv}\left(\{\mathcal{S}_i\}_{i \in I}\right)$.

Proof: The "if" direction is trivial, therefore we only prove the "only if" direction. Assume $x \in \mathrm{Pre}_{\{\mathcal{S}_i\}_{i \in I}}(X)$. By assumption, there exist $u_1, u_2, \ldots, u_{|I|}$ such that $A_i x + Bu_i + F_i = x_i' \in X$. Let $\mathcal{S} \in \mathrm{Conv}\left(\{\mathcal{S}_i\}_{i \in I}\right)$. Then there exists $\boldsymbol{\alpha} \in \Delta_{|I|}$ such that the system matrices of $\mathcal{S}$ can be written as $A = \sum_{i\in I} \alpha_i A_i$ and $F = \sum_{i\in I} \alpha_i F_i$. Choose $u = \sum_{i\in I} \alpha_i u_i$. Then,

$$x' = Ax + Bu + F = \left(\sum_{i\in I} \alpha_i A_i\right) x + B \sum_{i\in I} \alpha_i u_i + \sum_{i\in I} \alpha_i F_i$$
$$= \sum_{i\in I} \alpha_i \left(A_i x + B u_i + F_i\right) = \sum_{i\in I} \alpha_i x'_i.$$

Since X is convex and each $x'_i \in X$, the result x' is also an element of X, proving $x \in Pre_{\mathcal{S}}(X)$. ■

Remark 2: Above, we assumed that the B matrices are equal for all systems $\mathcal{S}_i$, which enables the convexity argument in the proof of Proposition 1. In the case the systems have different B matrices, Proposition 1 does not hold. However, if $\mathrm{Pre}_{\{\mathcal{S}_i\}_{i\in I}}$ is re-defined so that instead of for each $i \in I$ finding some u_i such that $A_i x + B u_i + K_i \in X$, the quantifiers are switched and a single u such that $A_i x + B_i u + K_i \in X$ for all $i \in I$ is computed, then the result in Proposition 1 holds also for families with distinct B matrices.

C. Finding convex over-approximations of matrices

We now give algorithms that for a given parametrized system $x^+ = A(v)x + Bu + F(v)$ and a set of $V \subset \mathbb{R}^p$ of parameters, computes a finite family of systems $\{\mathcal{S}_i\}_{i\in I}$ such that the original system is a member of $\mathrm{Conv}\left(\{\mathcal{S}_i\}_{i\in I}\right)$ for all parameter values in the set V.

We assume that we are given a finite collection $\{f_j\}_{j=1}^q$ of q non-constant functions $f_j : V \to \mathbb{R}$, linearly independent on V, such that $A(v)$ and $F(v)$ can be represented as $A(v) = A_0 + \sum_{j=1}^q A_j f_j(v)$ and $F(v) = F_0 + \sum_{j=1}^q F_j f_j(v)$, where A_j and F_j are constant matrices for all $j = 0, \dots, q$. Note that such a collection always exists and has at most $n^2 + n$ elements if $x \in \mathbb{R}^n$, but q can in general be much smaller than $n^2 + n$. Define the function $f : V \to \mathbb{R}^q$ such that

$$f : v \mapsto [f_1(v)\ f_2(v) \dots f_q(v)]^\intercal. \tag{9}$$

Next, we argue that finding a finite family of systems $\{\mathcal{S}_i\}_{i\in I}$ such that the original system is a member of $\mathrm{Conv}\left(\{\mathcal{S}_i\}_{i\in I}\right)$ for all parameter values in the set V is equivalent to finding a convex hull that covers the image $f(V)$.

Theorem 1: Suppose that f is defined as in (9), and furthermore that there exist $\{c_i\}_{i\in I}$, $c_i \in \mathbb{R}^q$ such that $f(V) \subset \mathrm{Conv}\left(\{c_i\}_{i\in I}\right)$. Then a family $\{\mathcal{S}_i\}_{i\in I}$ of systems can be constructed such that $\mathcal{S} : x^+ = A(v)x + Bu + F(v), u \in U$ is in $\mathrm{Conv}\left(\{\mathcal{S}_i\}_{i\in I}\right)$ for all $v \in V$.

Proof: For all $v \in V$, $\mathcal{S}$ can be written as

$$x^+ = A(v)x + Bu + F(v) =$$
$$\Big(A_0 + \sum_{j=1}^q A_j f_j(v)\Big)x + Bu + F_0 + \sum_{j=1}^q F_j f_j(v).$$

Since $f(V) \subset \mathrm{Conv}\left(\{c_i\}_{i\in I}\right)$, there is an $\boldsymbol{\alpha} \in \Delta_q$ such that $f(v) = \sum_{i\in I} \alpha_i c_i$. Let $c_i = [c_{i,1}, \dots, c_{i,q}]^\intercal$. Then, $f_j(v) = \sum_{i\in I} \alpha_i c_{i,j}$ for all $j = 1, \dots, q$. Therefore,

$$A(v) = A_0 + \sum_{j=1}^q A_j \sum_{i\in I} \alpha_i c_{i,j},\ F(v) = F_0 + \sum_{j=1}^q F_j \sum_{i\in I} \alpha_i c_{i,j}.$$

Define, for all $i \in I$, $\mathcal{S}_i : x^+ = \bar{A}_i x + Bu + \bar{F}_i, u \in U$, where $\bar{A}_i = A_0 + \sum_{j=1}^q A_j c_{i,j}$ and $\bar{F}_i = F_0 + \sum_{j=1}^q F_j c_{i,j}$. Then, it is clear that $\mathcal{S} \in \mathrm{Conv}\left(\{\mathcal{S}_i\}_{i\in I}\right)$ as $A(v) = \sum_{i\in I} \alpha_i \bar{A}_i$ and $F(v) = \sum_{i\in I} \alpha_i \bar{F}_i$. ■

This theorem essentially tells us that in order to tightly cover the dynamics of the parametrized system, the convex hull of $f(V)$ is required. Before discussing some techniques for computing the convex hull of $f(V)$, some remarks are in order. When $\mathrm{Conv}(f(V))$ is a polyhedron (i.e., it can be described as the convex hull of finitely many vertices), the Pre operator of the parametrized system can be exactly computed by Proposition 1. In general, when $\mathrm{Conv}(f(V))$ is not a polyhedron, it can be outer approximated to arbitrary precision by a polyhedron, which results in an inner approximation of the backwards reachability operator Pre for the parametrized system. The fixed point iterations (6) return a (non-maximal) controlled invariant set also when inner approximations of Pre are used, which makes outer approximations of $\mathrm{Conv}(f(V))$ useful in practice.

Next we discuss two explicit techniques for computing an over-approximation of $\mathrm{Conv}(f(V))$ when f and V satisfy certain conditions.

1) Convex-hull computation with monotone functions: In this section, we present a method for computing an over approximation of $\mathrm{Conv}(f(V))$ when f satisfies certain monotonicity conditions and V is a hyper rectangle. A simple condition to verify monotonicity of a function $f_i : \mathbb{R}^p \to \mathbb{R}$ is the sign stability of its gradient:

Proposition 2: Given a hyper rectangle $V \subset \mathbb{R}^p$, a mapping $f_i : V \to \mathbb{R}$ is monotone on V if each element of the gradient of f_i maintains its sign on V. That is, for all $j \in \{1, \dots, p\}$, there exists $\sigma_j \in \{0, 1\}$ such that

$$(-1)^{\sigma_j} \frac{\partial f_i}{\partial v_j}(v) \geq 0 \quad \forall v \in V,$$

then f_i is monotone with respect to the cones $K_1^i = \{x = [x_1, \dots, x_p]^\intercal \in \mathbb{R}^p \mid (-1)^{\sigma_j} x_j \geq 0 \quad j = 1, \dots, p\}$, $K_2 = [0, \infty)$. Moreover, if all components f_i, $i = 1, \dots, q$, of a function $f : \mathbb{R}^p \to \mathbb{R}^q$ are monotone with respect to some cones K_1^i and $K_2 = [0, \infty)$, then $f(V) \subset \prod_{i=1}^p [f_i(v^{i,-}), f_i(v^{i,+})]$, where $v^{i,-}$ and $v^{i,+}$ are extreme points of V with respect to the order induced by K_1^i.

Note that since $\prod_{i=1}^p [f_i(v^{i,-}), f_i(v^{i,+})]$ in the above proposition is a convex set, it contains $\mathrm{Conv}(f(V))$. Given f and V, if the conditions in the above proposition fail, i.e., the gradients of component functions of f are not sign stable on V, but there is a finite cover $\{V_l\}_{l\in L}$ of V with $V = \cup_{l\in L} V_l$ and each V_l is a hyper rectangle where the conditions of the proposition hold, then it is still possible to find a convex over approximation of $\mathrm{Conv}(f(V))$. This is done by over approximating the convex hull of each $f(V_l)$ with a hyper rectangle using the proposition above, and then taking the convex hull of these hyper rectangles. The next result shows that, under certain conditions, it is possible to obtain an arbitrarily tight over approximation of $\mathrm{Conv}(f(V))$ by covering V with hyperboxes with decreasing size. The idea is illustrated in the left part of Fig. 1.

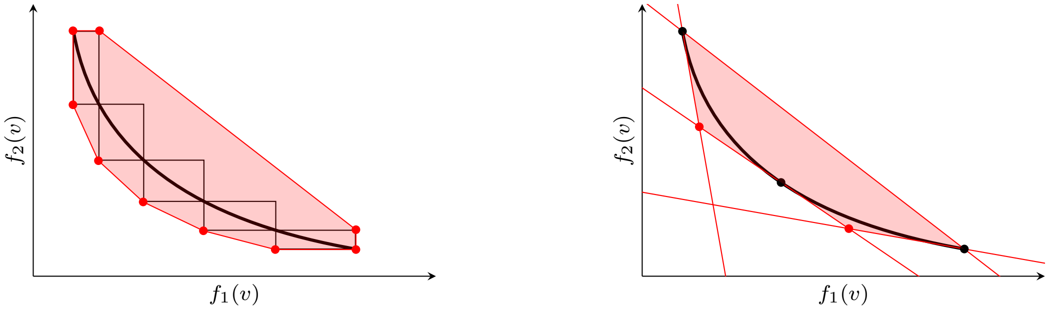

Fig. 1. Convex hull constructed around a curve using the monotonicity (left) and gradient (right) methods.

Theorem 2: Let $\{V_l\}_{l\in L}$ be a hyper rectangular cover of V, i.e., $V = \cup_{l\in L} V_l$ and each V_l is a hyper rectangle. Assume that the gradients of the component functions of f are sign stable on each V_l. Also, let $[V_l]_\epsilon$ be a finite hyper rectangular cover of V_l, where the size of the maximum edge of each hyper rectangle $R \in [V_l]_\epsilon$ is at most ϵ and $V_l = \cup_{R\in[V_l]_\epsilon} R$. Then, $\text{Conv}(f(V)) = \lim_{\epsilon\to 0} \text{Conv}(\{\{f(R)\}_{R\in[V_l]_\epsilon}\}_{l\in L})$.

Proof: The result follows from the following properties: i) for any sets A and B, $\text{Conv}(A \cup B) = \text{Conv}(\text{Conv}(A) \cup \text{Conv}(B))$, and ii) for sets A and B such that $h(A, B) \leq \epsilon$, we have $h(\text{Conv}(A), \text{Conv}(B)) \leq \epsilon$, where h is the Hausdorff distance function.

Claim i) follows directly from the definition of convex hulls. To show ii), take any $a \in \text{Conv}(A)$, it can be written as $a = \sum_{i\in I} \alpha_i a_i$ with $\boldsymbol{\alpha} \in \Delta_{|I|}$ and $a_i \in A$. For each a_i we can find $b_i \in B$ s.t. $\|a_i - b_i\| \leq \epsilon$. Evidently, $b := \sum_{i\in I} \alpha_i b_i \in \text{Conv}(B)$, and $\|a - b\| = \|\sum_i \alpha_i(a_i - b_i)\| \leq \sum_{i\in I} \alpha_i \|a_i - b_i\| \leq \epsilon$, which shows $h(\text{Conv}(A), \text{Conv}(B)) \leq \epsilon$. ∎

2) Convex-hull computation with convex projections: Ideas similar to those for monotonicity can also be used when the component functions f_i of f are convex or concave on some convex polyhedral sets V_l that cover the set V. Note that when f_i is convex (concave), the minimum (maximum) of f_i on each V_l can be found by convex programming and the maximum (minimum) can be found by evaluating the function f_i on the vertices of V_l. Such a strategy again creates a collection of hyper rectangles that over approximate $f(V)$. However, the convex hull of these hyper rectangles can potentially have a large number of vertices. Next, we restrict attention to a very special case with a single parameter, valid for the lane keeping application studied later in the paper, for which over approximations with smaller numbers of vertices can be computed.

Consider the special case of a map $f := (f_1, f_2) : [v_{min}, v_{max}] \rightarrow \mathbb{R}^2$ where f_2 is convex in f_1 over $[v_{min}, v_{max}]$, i.e., the function $f_2 \circ f_1^{-1} : f_1([v_{min}, v_{max}]) \rightarrow \mathbb{R}$ is a convex function. In this case, we know the line connecting $f(v_{min})$ to $f(v_{max})$ lies completely above the graph of $f([v_{min}, v_{max}])$. Furthermore, we also know that any tangent line to $f([v_{min}, v_{max}])$ lies completely below the graph of $f([v_{min}, v_{max}])$. The right part of Fig. 1 illustrates the idea, where one hyperplane constraint is constructed using the former fact, and three hyperplane constraints are constructed using the latter fact. In particular, the former constraint is of the form:

$$-mf_1(v) + f_2(v) \leq f_2(v_{min}) - mf_1(v_{min}),$$

where $m = \frac{f_2(v_{max}) - f_2(v_{min})}{f_1(v_{max}) - f_1(v_{min})}$; the latter constraints are of the form

$$m_1 f_1(v) + m_2 f_2(v) \geq m_1 f_1(v_i) + m_2 f_2(v_i),$$

where $m_1 \frac{df_1}{dv}(v_i) + m_2 \frac{df_2}{dv}(v_i) = 0$ and $v_i \in [v_{min}, v_{max}]$.

This method can also be applied in higher dimensions, i.e., when $f : [v_{min}, v_{max}] \rightarrow \mathbb{R}^n$, provided that the components $f_1, \ldots, f_n$ of f pairwise satisfy the convexity property described above. In this case, two-dimensional sets $\mathcal{P}_{ij}$ can be computed for all i, j with $i \neq j$, and then lifted to n dimensions to obtain $\text{Conv}(f(V)) \subset \mathcal{P} := \{[x_1, \ldots, x_n]^\intercal : (x_i, x_j) \in \mathcal{P}_{ij} \ \forall\, i \neq j\}$.

D. Overall procedure

Given the pieces described in the preceding sections, the overall procedure to solve Problem 1 proceeds as follows. We start with safe sets X^i for each subsystem $i \in \{1, 2\}$. We compute a polyhedral convex over approximation for $A^j(X^i), F^j(X^i)$, $i \neq j$ as explained in Section IV-C, which results in a family $\{\mathcal{S}_k^j\}_{k\in I_j}$ of affine systems such that $\text{Conv}(\{\mathcal{S}_k^j\}_{k\in I_j})$ encapsulates all systems $\mathcal{S}_j : x^+ = A^j(x_i)x_j + Bu_j + F_j(x_i)$ corresponding to some $x_i \in X^i$. Robust controlled invariant sets C^1, C^2 are then computed using the iterations in (6) with the Pre operator defined in (8). There are three possibilities at this step:

1) If both C^1 and C^2 are non-empty, return.
2) If C^i is non-empty but C^j is empty, then compute convex over approximations for $A^j(C^i), F^j(C^i)$ and recompute C^j for this uncertainty set. If C^j is non-empty, return. Else go to *.
3) If both C^1 and C^2 are empty, go to *.

(*) Redefine the safe sets $(X^i)' = X^i \ominus \mathcal{B}_\infty(0, \epsilon)$ for each $i \in \{1, 2\}$ and for some parameter $\epsilon > 0$. Restart if $(X^i)'$ are non-empty and return otherwise.

The procedure is guaranteed to terminate as long as the initial safe sets are bounded and a controlled invariant set computation with termination guarantees is used as in iterations (6). For the application example we considered, a non-empty pair C^1, C^2 is found in the first step.

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{bmatrix} y \\ \nu \\ \Delta\Psi \\ r \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & u & 0 \\ 0 & -\frac{C_{\alpha f}+C_{\alpha r}}{mu} & 0 & \frac{bC_{\alpha r}-aC_{\alpha f}}{mu} - u \\ 0 & 0 & 0 & 1 \\ 0 & \frac{bC_{\alpha r}-aC_{\alpha f}}{I_z u} & 0 & -\frac{a^2 C_{\alpha f}+b^2 C_{\alpha r}}{I_z u} \end{bmatrix}}_{A_{LK}} \begin{bmatrix} y \\ \nu \\ \Delta\Psi \\ r \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{C_{\alpha f}}{m} \\ 0 \\ a\frac{C_{\alpha f}}{I_z} \end{bmatrix} \delta_f + \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \end{bmatrix} r_d \tag{10}$$

A related problem is considered in our earlier work [14], where an approach for computation of decoupled invariant sets for linear systems and synthesis of modular local controllers to achieve additional high-level specifications is presented. The computation of the invariant sets was done in a centralized manner. In the current paper, the overall system is nonlinear and the computation of the invariant sets is also done in a compositional manner. Therefore, in terms of the dynamics that can be handled, the system class considered in [14] is a special case of this paper. On the other hand, the additional iterations modifying the initial safe sets X_i as in step 3 above is not needed for the optimization based approach in [14] since the controlled invariant sets are computed simultaneously.

V. Application: Correct-by-construction composition of Lane Keeping and Adaptive Cruise Control

In this section, the method presented in Section IV is applied to synthesize a lane-keeping (LK) controller and an adaptive cruise controller (ACC) whose composition is guaranteed to be safe. We employ the following model of longitudinal motion

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{bmatrix} u \\ h \end{bmatrix} = \begin{bmatrix} -f_1/m & 0 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} u \\ h \end{bmatrix} + \begin{bmatrix} F_w/m - f_0/m - \nu r \\ v_L \end{bmatrix}, \tag{11}$$

and the lateral dynamics given in (10). The goal of ACC is to compute the applied longitudinal force F_w so that either a desired longitudinal speed $u = u_{des}$ is achieved, or so that the headway h stays above some minimal value. Correspondingly, the goal of LK is to control the steering angle δ_f in a way that prevents lane departure.

Both these models are linearized versions of non-linear force-balance equations. For more information we refer to [12] and [17], respectively, and just describe the physical meaning of each state briefly. For the ACC model, the two states u and h represent longitudinal velocity and headway, respectively. The headway is the distance to a lead car, which is assumed to travel at velocity v_L. The LK model has four states $y, \nu, \Delta\Psi$ and r, which describe lateral displacement from the center of the lane, lateral velocity, yaw angle, and yaw rate, respectively. The input to the LK system is the steering angle δ_f, and there is also an exogenous disturbance r_d coming from the curvature of the road. We assume that $|r_d| \leq 0.05$, which is in line with the maximal recommended curvature of freeways in Michigan [11].

As can be seen, the state u pertaining to the ACC system appears in the system matrix of (10). Conversely, the states ν and r from the LK system appear in the offset term of the ACC system. Furthermore, both of these interdependencies are nonlinear.

TABLE I

Parameter values for ACC and LK models.

m	1650 kg	f_0	-24 N	f_1	19 Ns/m
a	1.11 m	$C_{\alpha f}$	133000 N	I_z	2315 kg m^2
b	1.59 m	$C_{\alpha r}$	98800 N	v_L	26 m/s

TABLE II

State constraints for ACC and LK models.

State	Lower bound	Upper bound
u	25 m/s	30 m/s
h	42 m	∞
y	-0.9 m	0.9 m
ν	-1.2 m/s	1.2 m/s
$\Delta\psi$	-0.05 rad	0.05 rad
r	-0.3 rad/s	0.3 rad/s

In the following, we settle for the parameter values given in Table I and for comfort reasons we impose the control input bounds of $F_w \in [-3m, 2m]$ and $\delta_f \in [\pi/90, \pi/90]$, respectively. For combined safety and comfort reasons, we pose the state constraints given in Table II. The bound $y \in [-0.9, 0.9]$ prevents lane departure, while the bounds $h \geq 42$ implies a time headway[1] of 1.4 s at $u = 25$ m/s, which is a common recommendation.

If we can find a LK controller that keeps the states $y, \nu, \Delta\psi, r$ within the bounds in Table II whenever u is within its bounds, and correspondingly for the ACC system, safety is guaranteed. The system models are given in continuous time, in order to apply the methods from Section IV we therefore time-discretize the models using Euler forward with a time step of 0.1 s, which preserves the base $\{f_i\}_{i=1}^q$ from which the system matrices are composed. When implementing a correct discrete-time controller in continuous time, inter-sample constraint violations may occur, as well as differences from the omission of higher-order terms in the Euler forward approximation (as opposed to the exact exponential map). It is possible to correct this by adding certain robustness margins [8], but we omit those details.

a) Solving the LK part: We can see that the entries of A_{LK} in (10) are composed of two linearly independent nonlinearities, u and $1/u$. Using the method in Section IV-C.2, we find the polyhedron $\mathcal{P}_{LK} \subset \mathbb{R}^2$ depicted in Fig. 3 that is an over-approximation of all values the function $u \mapsto [u, 1/u]$ can take when u varies in the interval $[25, 30]$. By lifting $\mathcal{P}_{LK}$ into the matrix space, we obtain a family of four systems, one for each vertex of $\mathcal{P}_{LK}$, whose convex hull contains all systems corresponding to some u in the

[1] Time headway, or *time to collision*, is defined as $\tau = h/u$.

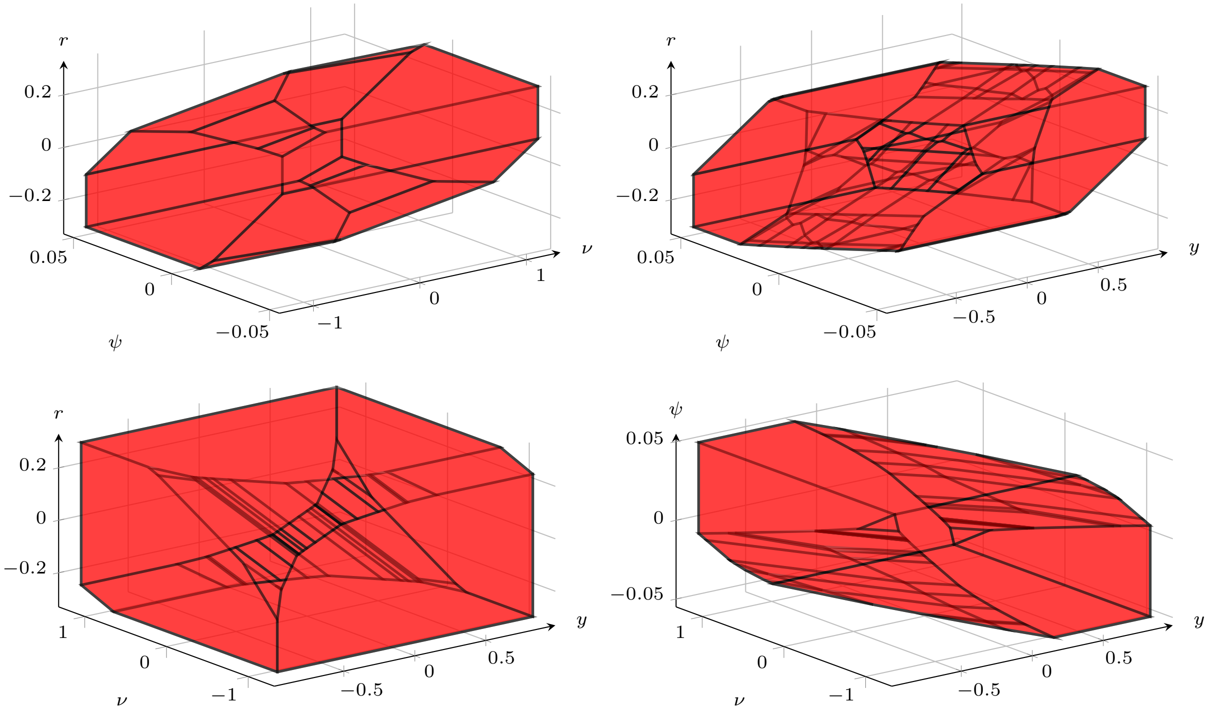

Fig. 2. Projections of the four-dimensional controlled invariant set C_{LK} for the LK system (10) onto different dimensions.

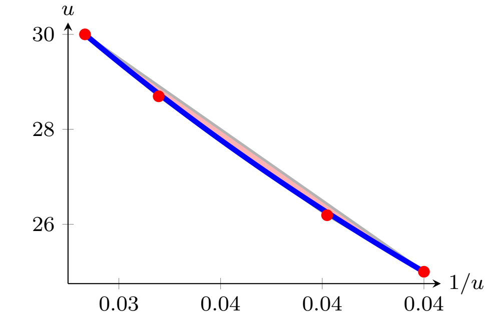

Fig. 3. All possible values of $[1/u, u]$ (in blue) are covered by a polyhedron $\mathcal{P}_{LK}$ with four vertices (in red).

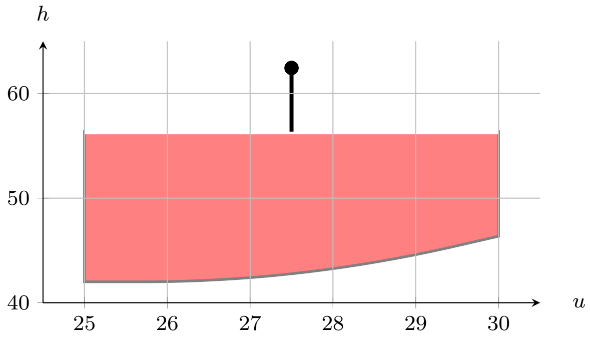

Fig. 5. Controlled invariant set C_{ACC} for the ACC system (11)

interval $[25, 30]$. Applying the invariant set computation[2] for the four vertex systems using the bounds for the LK states as the initial set, we obtain the 4-dimensional polyhedron C_{LK} depicted in Fig. 2, which is controlled invariant for all $u \in [25, 30]$.

b) Solving the ACC part: In the ACC system (11), there is one offset term νr that is a function of the state of the LK system. Our goal is to find a polyhedron $\mathcal{P}_{ACC} \subset \mathbb{R}$ that is an over approximation of the range of the function $f : [\nu, r] \mapsto \nu r$ where $\nu \in [-1.2, 1.2]$ and $r \in [-0.3, 0.3]$. The exact range of this function can easily be seen to be $[-0.36, 0.36]$, however we will formalize the derivation of this range using the monotonicity method described in Section IV-C.1. In fact, since f maps to $\mathbb{R}$, this method will also produce the exact range of f. We first note that $\nabla f = [r, \nu]$, which is sign stable on each quadrant of the (ν, r) plane. Consider quadrant one, where f is monotone w.r.t. the cones $K_1 = \{x \in \mathbb{R}^2 \mid x_j \geq 0 \quad \forall j = 1, 2\}$, $K_2 = [0, \infty)$. Therefore, the maximum value of f on the first quadrant occurs at $(\nu, r) = (1.2, 0.3)$, and the minimum value occurs at the origin so that $f([0, 1.2]) \times [0, 0.3]) = [f(0, 0), f(1.2, 0.3)] = [0, 0.36]$. Similarly, the range of f on quadrant three is found to be $[0, 0.36]$, and the range of f on quadrants two and four is identically $[-0.36, 0]$. Thus, the range of f is precisely $\text{Conv}([-0.36, 0], [0, 0.36]) = [-0.36, 0.36]$. Using this bound, we then proceed as with the LK system to obtain the controlled invariant 2-dimensional polyhedron C_{ACC} shown in Fig. 5.

Once the two sets C_{ACC} and C_{LK} that satisfy (3) are obtained, controllers that guarantee invariance can be implemented by choosing for a given state $x_{ACC} \in C_{ACC}$ and $x_{LK} \in C_{LK}$ an input u_{ACC} such that $A(x_{LK})x_{ACC} + Bu_{ACC} + F(x_{LK}) \in C_{ACC}$, and conversely for x_{LK}. Finding such inputs amounts to enforcing certain linear constraints which by construction are feasible. In particular,

[2] Since the system contains exogenous disturbance, we use a modified reachability operator Pre that is robust with respect to disturbance. See [12] for details.

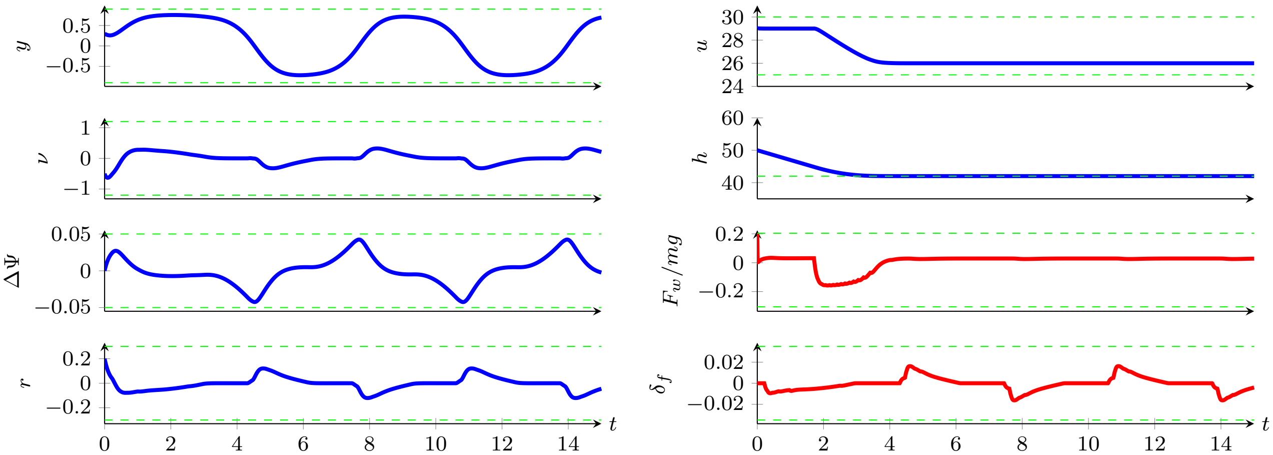

Fig. 4. Simultaneous simulation of the LK and ACC subsystems on a curvy road. States are shown in blue, and computed control inputs in red. The dashed green lines indicate state and control bounds that are guaranteed to hold. The ACC controller is programmed to maintain a desired speed of 29 m/s when possible. However, it is forced to slow down at $t = 2$ to avoid future violation of the headway constraint.

at each time step, we compute an input satisfying these constraints by solving a convex quadratic optimization problem. In Fig. 4 a simultaneous simulation of the ACC and LK systems is shown, where the road curvature r_d is in the form of a sinusoidal signal with maximal amplitude 0.05. As expected, all bounds are respected throughout the simulation.

VI. Conclusions

In this paper, we proposed an approach for compositional correct-by-construction safety controller synthesis by (i) quantifying the effects of each subsystem onto the other using convex sets, and (ii) computing controlled invariant sets robust against such effects given in terms of parametric uncertainty in the system matrices. We showed how these convex sets can be computed when the parameter dependencies satisfy certain monotonicity or convexity conditions. Due to the fact that the dynamics of each subsystem is affine in its own state, it is shown that using convex sets to over-approximate these interdependences does not introduce any conservatism in the computation of controlled invariant sets. In the second part of the paper, an adaptive cruise control and a lane keeping controller, together with their robust controlled invariant sets, were synthesized using the proposed approach. By construction, the composition of these controllers is guaranteed to satisfy the safety specifications when simultaneously implemented on the vehicle. The effectiveness of the approach was illustrated via simulations on this case study.

Our current contracts are in the form of static polyhedral safe sets which limit the effect each subsystem has on the others. In the future, it will be interesting to consider dynamic contracts capturing possible time evolution of these sets, in the same vein as Lyapunov or storage functions. Another direction for future work is an extension of the proposed approach to fully nonlinear systems.

References

[1] A. D. Ames, J. W. Grizzle, and P. Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In *Proc. of the IEEE CDC*, pages 6271–6278, 2014.

[2] J.-P. Aubin and A. Cellina. *Differential Inclusions*. Set-Valued Maps and Viability Theory. Springer, 1984.

[3] L. Benvenuti, A. Ferrari, E. Mazzi, and A. S. Vincentelli. Contract-based design for computation and verification of a closed-loop hybrid system. In *Proc. of HSCC*, pages 58–71, 2008.

[4] D. P. Bertsekas. Infinite Time Reachability of State-Space Regions by Using Feedback Control. *IEEE Trans. Autom. Control*, 17(5):604–613, 1972.

[5] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[6] E. De Santis, M. D. Di Benedetto, and L. Berardi. Computation of Maximal Safe Sets for Switching Systems. *IEEE Trans. Autom. Control*, 49(2):184–195, 2004.

[7] G. Frehse, Z. Han, and B. Krogh. Assume-guarantee reasoning for hybrid i/o-automata by over-approximation of continuous interaction. In *Proc. of the IEEE CDC*, pages 479–484, 2004.

[8] A. Girard. Reachability of Uncertain Linear Systems Using Zonotopes. In *Proc. of HSCC*, pages 291–305, 2005.

[9] D. Greising and J. Johnsson. Behind Boeing's 787 delays. *Chicago Tribune*, 10:2007, 2007.

[10] E. S. Kim, M. Arcak, and S. A. Seshia. Compositional controller synthesis for vehicular traffic networks. In *Proc. of the IEEE CDC*, pages 6165–6171, 2015.

[11] Michigan Department of Transportation. Road design manual, chapter 3 geometrics.

[12] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A. Ames, J. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Correct-by-construction adaptive cruise control: Two approaches. *IEEE Trans. Control Syst. Technol.*, 24(4):1294–1307, 2016.

[13] P. Nilsson, O. Hussien, Y. Chen, A. Balkan, M. Rungger, A. Ames, J. Grizzle, N. Ozay, H. Peng, and P. Tabuada. Preliminary results on correct-by-construction control software synthesis for adaptive cruise control. In *Proc. of the IEEE CDC*, pages 816–823, 2014.

[14] P. Nilsson and N. Ozay. Synthesis of separable controlled invariant sets for modular local control design. In *Proceedings of ACC*, pages 5656–5663, 2016.

[15] P. Nuzzo, H. Xu, N. Ozay, J. B. Finn, A. L. Sangiovanni-Vincentelli, R. M. Murray, A. Donzé, and S. A. Seshia. A contract-based methodology for aircraft electric power system design. *IEEE Access*, 2:1–25, 2014.

[16] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: the next computing revolution. In *Proc. of the ACM DAC*, pages 731–736, 2010.

[17] E. J. Rossetter and J. C. Gerdes. Lyapunov based performance guarantees for the potential field lane-keeping assistance system. *Journal of dynamic systems, measurement, and control*, 128(3):510–522, 2006.

[18] K. L. Talvala, K. Kritayakirana, and J. C. Gerdes. Pushing the limits: From lane keeping to autonomous racing. *Annual Reviews in Control*, 35(1):137–148, 2011.