

Correctness Guarantees for the Composition of Lane Keeping and Adaptive Cruise Control

Xiangru Xu, *Member, IEEE*, Jessy W. Grizzle, *Fellow, IEEE*, Paulo Tabuada, *Senior Member, IEEE*, Aaron D. Ames, *Member, IEEE*

Abstract—This paper develops a control approach with correctness guarantees for the simultaneous operation of lane keeping and adaptive cruise control. The safety specifications for these driver assistance modules are expressed in terms of set invariance. Control barrier functions are used to design a family of control solutions that guarantee the forward invariance of a set, which implies satisfaction of the safety specifications. The control barrier functions are synthesized through a combination of sum-of-squares program and physics-based modeling and optimization. A real-time quadratic program is posed to combine the control barrier functions with performance-based control Lyapunov functions, such that the generated feedback control guarantees the safety of the composed driver assistance modules in a formally correct manner. Importantly, the quadratic program admits a closed-form solution that can be easily implemented.

Index Terms—Lane keeping, Adaptive cruise control, Correct-by-construction, Control barrier functions, Quadratic program, Sum of squares

I. INTRODUCTION

Recent years have witnessed a growing number of safety or convenience modules for automobiles [1], [2]. One such system is Adaptive Cruise Control (ACC), which is a driver assistance system that significantly enhances conventional cruise control [3], [4]. When there is no preceding vehicle, an ACC-equipped vehicle maintains a constant speed set by the driver, just as in conventional cruise control; when a preceding vehicle is detected and is driving at a speed slower than the preset speed, an ACC-equipped vehicle changes its control objective to maintaining a safe following distance. Lane keeping, also called active lane keeping or lane keeping assist, is an evolution of lane departure warning [5], [6], [7], where instead of simply warning of imminent lane departure through vibration of the steering wheel or an audible alarm, the system corrects the vehicle’s direction to keep it within its lane. Early systems corrected vehicle direction by differential braking, but current systems actively control steering to maintain lane centering, which is what we will term Lane Keeping (LK) in this paper. In addition to increasing safety and driver convenience, such modules can also help to reduce traffic congestion [8] and fuel consumption [9].

This research is supported by NSF CPS Award 1239037.

X. Xu and J.W. Grizzle are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA. email: xuxiangr@umich.edu, grizzle@umich.edu.

P. Tabuada is with the Department of Electrical Engineering, University of California, Los Angeles, CA, USA. email: tabuada@ucla.edu.

A. D. Ames is with the George W. Woodruff School of Mechanical Engineering and the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA. email: ames@gatech.edu.

Worldwide, most of the major manufacturers are now offering passenger vehicles equipped with ACC and LK. Moreover, these features can be activated simultaneously at highway speeds and require limited driver supervision. In terms of the levels of automation defined by the National Highway Traffic Safety Administration (NHTSA) [10], such vehicles are already at Level 2 (automation of at least two primary control functions designed to work in unison without driver intervention), and they are approaching Level 3 (limited self-driving). The simultaneous control of the longitudinal and lateral dynamics of a vehicle is an important milestone in the bottom-up approach to full autonomy, and therefore, it is crucial to prove that the controllers associated with ACC and LK behave in a formally correct way when they are both activated.

Applying formal methods to the field of (semi-)autonomous driving has attracted much attention in recent years [11],[12]. Particularly, formal correctness guarantees on individual ACC or LK system have been developed by various means. For example, the verification of cruise control systems has been accomplished using formal methods such as satisfiability modulo theory, theorem proving [13] and a counter-example guided approach [14]; safety guarantees for LK have been established using Lyapunov stability analysis by assuming the longitudinal speed is constant [15], [16] or varying [5], [17]. Furthermore, the so-called correct-by-construction control design, which aims to synthesize controllers to guarantee the closed-loop system satisfies the specification by construction and hence eliminating the need for verification, has also emerged as a viable means of achieving safety. For example, in [18], two provably correct control design methods were proposed for ACC, which rely on fixed-point computations of certain set-valued mappings on the continuous state space or a finite-state abstraction, respectively.

For the simultaneous operation of two (or even more) safety or convenience modules, which are typically coupled through the vehicle’s dynamics, it is more challenging to establish correctness guarantees. A contract-based design method employing assume-guarantee reasoning is a potential recipe for the compositional design of complex systems [19], [20]. Its main idea is to formally define the assumptions and guarantees of each subsystem, which are called contracts among the subsystems, and based on the contracts, to design (or establish) formal guarantees on the overall system. Different types of assume-guarantee formalisms have been proposed, such as temporal logic formulas [21] and supply/demand rates [22]. The composition of LK and ACC has been studied on the

basis of contracts. A passivity-based approach was proposed in [23], where the ACC and LK dynamics are described as multi-modal port Hamiltonian systems, based on which some energy functions are constructed to prove trajectories of the composed system do not enter a specified unsafe region. In [24], the system dynamics are represented as discrete-time linear parameter-varying systems, and contracts are established for the variables that couple the two subsystems; controlled-invariant sets are constructed for the ACC and LK subsystems individually to meet the terms of the contracts using an iterative algorithm. The algorithm is guaranteed to terminate, and under mild conditions, for any given epsilon, it is guaranteed to find an invariant set that is epsilon close to the maximal controlled invariant set. Despite these very interesting initial contributions, many safety guarantee problems on the composition of LK and ACC are still largely open and deserve further investigation.

Turning now to the more general literature on safety specifications, when safety is expressed as set invariance, controlled invariant sets are used to encode both the correct behavior of the closed-loop system and a set of feedback control laws that will achieve it (see [25], [26], [27], [28] and references therein). Under the name of *invariance control*, [25] and [26] extended Nagumo's Theorem to allow higher-order derivative conditions on the boundary of the controlled invariant set. As an add-on control scheme, *reference and command governors* utilize the notion of controlled invariance to enforce constraint satisfaction and ensure that the modified reference command is as close as possible to the original reference command [27]. In [28], characterization of the controlled invariant set for LK was given, which was then used to derive a feedback control strategy to maintain a vehicle in its lane. The common intent of these methods is to construct a controlled invariant set that encodes the safety specifications, and then construct a feedback law that ensures that trajectories of the controlled systems are confined within the set.

A barrier function (certificate) is another means to prove a safety property of a system based on set invariance. It seeks a function whose sub-level sets (or super-level sets, depending on the context) are all invariant, without the difficult task of computing the system's reachable set [29], [30]. In [31], the barrier condition in [29] was relaxed by only requiring a single super-level set of the function, which represents the safe region, to be invariant. A control barrier function (CBF) extends barrier functions from dynamical systems to control systems. When CBFs are unified with control Lyapunov functions (CLFs) representing the control objective, through a quadratic programming (QP) framework, safety can be always guaranteed while the control objective is mediated when safety and performance are in conflict. The QP-CBF-CLF approach was in fact introduced in [31] where it was applied to ACC safety control design. Further work along this line is available in [32], [33], [34], [35], [36].

This paper develops a modular correct-by-construction control approach that allows for individual and simultaneous activation of LK and ACC, whose dynamics are described by a continuous-time linear system and a linear parameter-varying system, respectively. The interactions of the two modules

through the dynamics of the vehicle and the environment are captured in a "contract", which consists of a set of assumptions and guarantees. CBFs are constructed to respect the contract where the CBF for LK is synthesized with the help of sum-of-squares (SOS) optimization [37], [38], [39] and the CBF for ACC is constructed by SOS and physics-based modeling and optimization. Through a QP that unifies the CBFs and CLFs, the controller that mediates the safety and performance is designed, which is correct by construction under a clearly delineated set of assumptions. The practicality of the approach will be illustrated through calculations and simulation on a model of a mid-size passenger vehicle.

The rest of the paper is organized as follows. Section II introduces the definition and some theoretic results about control barrier functions. Section III gives the dynamical models and the safety specifications for lane keeping and adaptive cruise control, based on which the composition problem studied in the paper is formulated. After providing the assumptions and guarantees between LK and ACC, Section IV constructs CBFs for LK and ACC, respectively. Section V gives the CBF-CLF-based quadratic programs, based on which the input that solves the composition problem is provided. Simulation results are presented in Section VI and finally, some conclusions in Section VII.

Notation. The boundary and the interior of a set \mathcal{S} are denoted as $\partial\mathcal{S}$ and $\text{Int}(\mathcal{S})$ (or $\overset{\circ}{\mathcal{S}}$), respectively. The commutative ring of real valued polynomials in n variables x_1, \dots, x_n is denoted as $\mathcal{R}[x_1, \dots, x_n]$, and as $\mathcal{R}_m[x_1, \dots, x_n]$ if the degree is m . The set of sum of squares polynomials in n variables x_1, \dots, x_n is denoted as $\Sigma[x_1, \dots, x_n]$, and as $\Sigma_m[x_1, \dots, x_n]$ if the degree is m .

II. PRELIMINARIES ON CONTROL BARRIER FUNCTIONS

As mentioned in the introduction, a control barrier function primarily focuses on establishing forward invariance of a given set. We briefly review the basic definitions and theorems in [31] and [32] for later use.

Consider a nonlinear system on \mathbb{R}^n ,

$$\dot{x} = f(x), \quad (1)$$

with f locally Lipschitz continuous. The solution of (1) with initial condition $x_0 \in \mathbb{R}^n$ is denoted by $x(t, x_0)$ (or simply $x(t)$). A set \mathcal{S} is called *forward invariant* if for every $x_0 \in \mathcal{S}$, $x(t, x_0) \in \mathcal{S}$ for all $t \in I(x_0)$, where $I(x_0)$ is the *maximal interval of existence* of $x(t, x_0)$.

Given a continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$, define a closed set \mathcal{C} as follows

$$\mathcal{C} = \{x \in \mathbb{R}^n : h(x) \geq 0\}. \quad (2)$$

In what follows, it will also be assumed that \mathcal{C} is nonempty and has no isolated points, that is, $\text{Int}(\mathcal{C}) \neq \emptyset$ and $\overline{\text{Int}(\mathcal{C})} = \mathcal{C}$.

Definition 1. [32] Consider a dynamical system (1) and the set \mathcal{C} defined by (2) for some continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$. If there exist a constant $\gamma > 0$ and a set \mathcal{D} with $\mathcal{C} \subseteq \mathcal{D} \subset \mathbb{R}^n$ such that

$$L_f h(x) \geq -\gamma h(x), \forall x \in \mathcal{D}, \quad (3)$$

then the function h is called a (zeroing) barrier function.

Existence of a (zeroing) barrier function implies the forward invariance of \mathcal{C} , as shown by the following theorem.

Theorem 1. [32] *Given a dynamical system (1) and a set \mathcal{C} defined by (2) for some continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$, if h is a barrier function defined on the set \mathcal{D} with $\mathcal{C} \subseteq \mathcal{D} \subset \mathbb{R}^n$, then \mathcal{C} is forward invariant.*

Consider an affine control system of the following form

$$\dot{x} = f(x) + g(x)u, \quad (4)$$

with f and g locally Lipschitz continuous, $x \in \mathbb{R}^n$ and $u \in U \subset \mathbb{R}^m$.

Definition 2. [32] *Given a set $\mathcal{C} \subset \mathbb{R}^n$ defined by (2) for a continuously differentiable function $h : \mathbb{R}^n \rightarrow \mathbb{R}$, the function h is called a (zeroing) control barrier function defined on set \mathcal{D} with $\mathcal{C} \subseteq \mathcal{D} \subset \mathbb{R}^n$, if there exists a constant $\gamma > 0$ such that¹*

$$\sup_{u \in U} [L_f h(x) + L_g h(x)u + \gamma h(x)] \geq 0, \quad \forall x \in \mathcal{D}. \quad (5)$$

Given a CBF h , for all $x \in \mathcal{D}$, define the set

$$K_{\text{zcbf}}(x) = \{u \in U : L_f h(x) + L_g h(x)u + \gamma h(x) \geq 0\}. \quad (6)$$

The following result guarantees the forward invariance of \mathcal{C} when inputs are selected from $K_{\text{zcbf}}(x)$.

Theorem 2. [32] *Assume given a set $\mathcal{C} \subset \mathbb{R}^n$ defined by (2) for a continuously differentiable function h . If h is a CBF on \mathcal{D} , then any locally Lipschitz continuous controller $u : \mathcal{D} \rightarrow U$ such that $u(x) \in K_{\text{zcbf}}(x)$ will render the set \mathcal{C} forward invariant.*

It will be seen later that for ACC, seeking a CBF that is everywhere continuously differentiable can be too restrictive. Below, it is briefly pointed out how the assumption of continuous differentiability can be relaxed to a continuous function constructed from a finite set of continuously differentiable functions.

Consider p ($p \geq 2$) continuously differentiable functions h_1, \dots, h_p where $h_i : \mathbb{R}^n \rightarrow \mathbb{R}$. Assume that the sets $\mathcal{C}_i := \{x \in \mathbb{R}^n : h_i(x) \geq 0\}$ satisfy $\text{Int}(\mathcal{C}_i) \neq \emptyset$ and $\overline{\text{Int}(\mathcal{C}_i)} = \mathcal{C}_i$. Suppose that \mathbb{R}^n is partitioned into p closed sets $\mathcal{S}_1, \dots, \mathcal{S}_p$ such that $\cup_{i=1}^p \mathcal{S}_i = \mathbb{R}^n$ and $\text{Int}(\mathcal{S}_i) \cap \text{Int}(\mathcal{S}_j) = \emptyset, \forall i, j, i \neq j$. For any i, j such that $\mathcal{S}_i \cap \mathcal{S}_j \neq \emptyset$, assume that $h_i(x) = h_j(x)$ for $x \in \mathcal{S}_i \cap \mathcal{S}_j$. Then the function $h : \mathbb{R}^n \rightarrow \mathbb{R}$ by

$$h|_{\mathcal{S}_i}(x) = h_i(x) \quad (7)$$

is well defined and continuous, and the set $\mathcal{C} = \{x \in \mathbb{R}^n | h(x) \geq 0\}$ is closed, has non-empty interior, and does not have isolated points.

Example 1. Consider $h_1(x_1, x_2) = -x_1^2 - x_2 + 3$, $h_2(x_1, x_2) = -0.2x_1^2 - x_2 + 1$ and $\mathcal{S}_1 = (-\infty, \sqrt{10}/2] \times (-\infty, \infty)$, $\mathcal{S}_2 = [\sqrt{10}/2, \infty) \times (-\infty, \infty)$. Clearly, $\text{Int}(\mathcal{S}_1) \cap \text{Int}(\mathcal{S}_2) = \emptyset$ and $h_1(x_1, x_2) = h_2(x_1, x_2)$ for any $x_1 =$

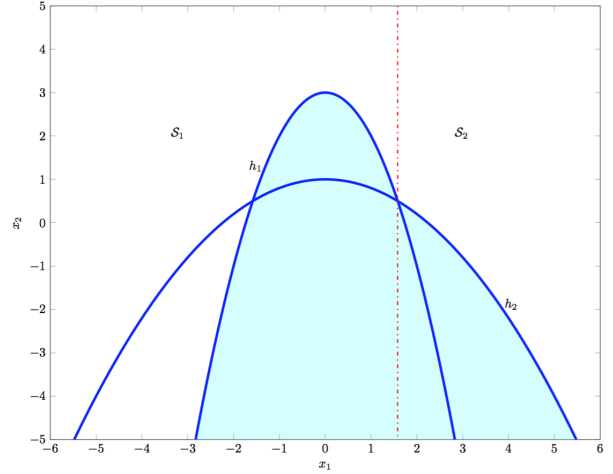


Fig. 1. The safe set \mathcal{C} in Example 1, which is defined by a continuous function h with respect to functions h_1, h_2 and state space partition $\mathcal{S}_1, \mathcal{S}_2$, is shown in light blue.

$\sqrt{10}/2, x_2 \in \mathbb{R}$. Therefore, the set \mathcal{C} can be defined, which is shown as the light blue area in Figure 1.

For all $x \in \mathcal{S}_i$ ($1 \leq i \leq p$), suppose that there exists a constant $\gamma_i > 0$ such that

$$\sup_{u \in U} [L_f h_i(x) + L_g h_i(x)u + \gamma_i h_i(x)] \geq 0,$$

and define the set $K^i(x)$ as

$$K^i(x) = \{u \in U | L_f h_i(x) + L_g h_i(x)u + \gamma_i h_i(x) \geq 0\}.$$

For any $x \in \mathbb{R}^n$, define the set $K(x)$ as

$$K(x) = \cap_{s \in \{i | x \in \mathcal{S}_i\}} K^s(x). \quad (8)$$

The following proposition extends Theorem 2 to the case of a safe set defined by a continuous function.

Proposition 1. *Given p ($p \geq 2$) continuously differentiable functions h_1, \dots, h_p where $h_i : \mathbb{R}^n \rightarrow \mathbb{R}$ and a partition of \mathbb{R}^n by p closed sets $\mathcal{S}_1, \dots, \mathcal{S}_p$ such that if $\mathcal{S}_i \cap \mathcal{S}_j \neq \emptyset$, then $h_i(x) = h_j(x)$ for $x \in \mathcal{S}_i \cap \mathcal{S}_j$, define a function h as in (7) and the set $\mathcal{C} = \{x \in \mathbb{R}^n | h(x) \geq 0\}$. If $K(x) \neq \emptyset$ for each $x \in \mathbb{R}^n$, then any locally Lipschitz continuous controller $u : \mathbb{R}^n \rightarrow K(x)$ will render the set \mathcal{C} forward invariant under the closed-loop system associated with (4).*

The proof is similar to the proof of Theorem 2 and is omitted here.

III. MODELS AND SAFETY SPECIFICATIONS

In this section, we first introduce the individual models and specifications for lane keeping and adaptive cruise control, respectively, and then we formulate a composition problem.

A. Dynamic Models

In this paper, the LK model we use is the lateral-yaw model as described in [5], [6], [40], and the ACC model is the point-mass model in [18], [31]. Their dynamics are given in (9) and (10), respectively.

¹A more general definition for the (zeroing) CBFs that involves extended class \mathcal{K} functions can be found in [32].

$$\begin{pmatrix} \dot{y} \\ \dot{\nu} \\ \Delta\dot{\psi} \\ \dot{r} \end{pmatrix} = \begin{pmatrix} 0 & 1 & v_f & 0 \\ 0 & -\frac{C_f+C_r}{mv_f} & 0 & \frac{bC_r-aC_f}{mv_f} - v_f \\ 0 & 0 & 0 & 1 \\ 0 & \frac{bC_r-aC_f}{I_z v_f} & 0 & -\frac{a^2 C_f + b^2 C_r}{I_z v_f} \end{pmatrix} \begin{pmatrix} y \\ \nu \\ \Delta\psi \\ r \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{C_f}{m} \\ 0 \\ \frac{aC_f}{I_z} \end{pmatrix} u_1 + \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix} d. \quad (9)$$

$$\begin{pmatrix} \dot{v}_f \\ \dot{v}_l \\ \dot{D} \end{pmatrix} = \begin{pmatrix} -\frac{c_0+c_1 v_f}{m} \\ a_L \\ v_l - v_f \end{pmatrix} + \begin{pmatrix} \frac{1}{m} \\ 0 \\ 0 \end{pmatrix} u_2 + \begin{pmatrix} -\nu r \\ 0 \\ 0 \end{pmatrix}. \quad (10)$$

Equation (9) describes the lateral-yaw dynamics of the controlled vehicle. In (9), $\mathbf{x}_1 := (y, \nu, \Delta\psi, r)'$ is the state, where $y, \nu, \Delta\psi$ and r represent the lateral displacement from the center of the lane, the lateral velocity, the yaw angle deviation in road-fixed coordinates, and the yaw rate, respectively; the input $u_1 = \delta_f$ is the steering angle of the front wheels; and d is the desired yaw rate, which is viewed as a time-varying external disturbance and computed from road curvature by $d = v_f/R_0$ where R_0 is the (signed) radius of the road curvature and v_f is the vehicle's longitudinal velocity. Moreover, m is the total mass of the vehicle, and C_f, C_r, a and b are parameters of the tires and vehicle geometry that are all positive numbers.

Equation (10) describes the longitudinal dynamics of the preceding vehicle and controlled vehicle. In (10), $\mathbf{x}_2 := (v_f, v_l, D)'$ is the state, which represent the following car's speed, the lead car's speed and the distance between them, respectively; $u_2 = F_w$ is the input that represents the longitudinal force developed by the wheels; $F_r = c_0 + c_1 v_f$ is the aerodynamic drag, with constants c_0 and c_1 ; and $a_L \in [-a_l g, a'_l g]$ is the overall acceleration/deceleration of the lead car.

Equations (9) and (10) are rewritten compactly as follows:

$$\dot{\mathbf{x}}_1 = f_1(\mathbf{x}_1, v_f) + g_1(\mathbf{x}_1)u_1 + \Delta f_1(d), \quad (11)$$

$$\dot{\mathbf{x}}_2 = f_2(\mathbf{x}_2) + g_2(\mathbf{x}_2)u_2 + \Delta f_2(\nu r, a_L), \quad (12)$$

where

$$\begin{aligned} f_1(\mathbf{x}_1, v_f) &= A_1(v_f)\mathbf{x}_1, \quad g_1(\mathbf{x}_1) = B_1, \quad \Delta f_1(d) = E_1 d, \\ f_2(\mathbf{x}_2) &= A_2 \mathbf{x}_2, \quad g_2(\mathbf{x}_2) = B_2, \quad \Delta f_2(\nu r, a_L) = E_2, \end{aligned}$$

with

$$A_1(v_f) = \begin{pmatrix} 0 & 1 & v_f & 0 \\ 0 & -\frac{C_f+C_r}{mv_f} & 0 & \frac{bC_r-aC_f}{mv_f} - v_f \\ 0 & 0 & 0 & 1 \\ 0 & \frac{bC_r-aC_f}{I_z v_f} & 0 & -\frac{a^2 C_f + b^2 C_r}{I_z v_f} \end{pmatrix},$$

$$B_1 = \begin{pmatrix} 0 \\ \frac{C_f}{m} \\ 0 \\ \frac{aC_f}{I_z} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} -\frac{c_1}{m} & 0 & 0 \\ 0 & 0 & 0 \\ -1 & 1 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} \frac{1}{m} \\ 0 \\ 0 \end{pmatrix},$$

$$E_2 = \begin{pmatrix} -\nu r - \frac{c_0}{m} \\ a_L \\ 0 \end{pmatrix}.$$

It is supposed that a bound is imposed on the steering angle δ_f of the controlled vehicle, that is, the set of admissible inputs for LK is

$$U_{lk} := [-\hat{\delta}_f, \hat{\delta}_f], \quad (13)$$

where $\hat{\delta}_f > 0$ is the maximum steering angle. At highway speeds, this number will be much smaller than the maximum turning angle of the vehicle, say two or three degrees, versus 35 degrees.

It is also supposed that the acceleration/deceleration of the controlled car is bounded, that is, the set of admissible inputs for ACC is

$$U_{acc} := [-a_f mg, a'_f mg], \quad (14)$$

where $a_f, a'_f > 0$. Typical bounds for driver comfort would be two or three tenths of gravitational acceleration. Additionally, we assume that $a_f = a_l$, where $-a_l$ is the maximal deceleration a_L of the lead car. That is, the two cars are assumed to have the same deceleration capability. This latter assumption can be relaxed as in [41].

B. Safety Specifications

For both LK and ACC, "hard constraints" and "soft constraints" are given, where the "hard constraints" are the safety specifications that must be satisfied for all time, and the "soft constraints" represent the control performance objectives that are to be achieved "as closely as possible" when they are not in conflict with safety.

The primary safety constraint of LK is to keep the car within its lane. That is, the absolute value of the lateral displacement y is less than some given constant y_m , which is related to the width of the lane and the car. Specifically, this specification is expressed as

$$|y| \leq y_m, \quad (15)$$

where y_m is a given positive real number.

In addition to the lateral displacement, the other state variables should also be bounded. These bounds are stated as the following specifications:

$$|\nu| \leq \nu_m, |\Delta\psi| \leq \Delta\psi_m, |r| \leq r_m, \quad (16)$$

where $\nu_m, \Delta\psi_m, r_m$ are given positive real numbers.

A soft constraint for LK is for the vehicle's yaw rate $r(t)$ to track $d(t)$, the yaw or turning rate of the road. Particularly, for $d(t) = d_0$ constant and d_0 bounded by $|d_0| \leq d_{\max}$, the objective is

$$\lim_{t \rightarrow \infty} r(t) - d(t) = 0. \quad (17)$$

Another optional soft constraint is for the lateral acceleration to be upper bounded by a number that respects driver comfort, e.g., $|\dot{\nu}| \leq 0.25g$.

On the other hand, the primary constraint for ACC is that the controlled vehicle maintain a safe distance from the lead car [42], which is expressed as the following hard constraint

$$D \geq \tau_d v_f + D_0, \quad (18)$$

where τ_d is the desired time headway and D_0 is the minimal distance between cars when they are fully stopped.

The soft constraint for ACC, which is the performance objective of the controlled car, is to achieve a desired speed v_d set by the driver. This specification can be expressed as

$$\lim_{t \rightarrow \infty} v_f(t) - v_d = 0, \quad (19)$$

for a given positive constant v_d .

C. Formulating the Composition Problem

The correctness guarantee for the composition of LK and ACC is formulated as the following problem.

Problem. Given LK model (11) and ACC model (12), find a control strategy $X \rightarrow U_{acc} \times U_{lk}$ such that the hard constraints (15), (16) and (18) are satisfied for all time, and the soft constraints (17) and (19) are achieved as closely as possible.

Although the safety specifications for LK and ACC are given separately, the dynamics of LK and ACC are coupled because $A_1(v_f)$ depends on v_f and $\Delta f_2(\nu r, a_L)$ depends on the product of lateral velocity and yaw rate through the term νr . To achieve the specifications simultaneously, in Section IV, we will design a *contract* between the LK and ACC subsystems and construct CBFs for them separately, such that the contract will be respected provided that the two subsystems constrain their behaviors in a controlled invariant set corresponding to their individual CBF. Once the safety specifications and the contract are dealt with, Section V will synthesize a provably correct solution to the composition problem via a QP that unifies CBFs and CLFs.

IV. CONTROL BARRIER FUNCTIONS FOR LK AND ACC

In this section, we provide CBFs for the lane keeping model (9) and the adaptive cruise control model (10), respectively. To this end, we first provide assumptions and guarantees between LK and ACC, and then translate the hard constraints of Sect. III-B into conditions that a control barrier function must satisfy so that, by the results of Sect. II, the trajectories of the closed-loop system will satisfy the safety portion of the specification.

A. Assumptions and Guarantees Between LK and ACC

As mentioned in the introduction, the compositional design of complex systems can be achieved using the contract-based method, which formally defines a set of assume-guarantee protocols among subsystems in a ‘‘circular’’ manner [19], [20]. The basic idea is that each subsystem ensures that its behavior (i.e., set of trajectories) satisfies its own guarantees, under the assumption that all the other subsystems do the same, so that a formal guarantee on the behavior of the overall system can be established.

For the composition of LK and ACC, we provide assumptions and guarantees between them in terms of the bounds of their respective coupling variables. To this end, a set of assumptions are given first.

In the LK model (11), there are two varying parameters v_f and d . Suppose that $\underline{v} \leq v_f \leq \bar{v}$ where $\bar{v}, \underline{v} > 0$ are the upper and lower bound of the longitudinal speed, respectively, with $\underline{v} < \bar{v}$. This can be expressed equivalently as $v_f \in \mathcal{D}_{v_f} \subset \mathbb{R}$ where \mathcal{D}_{v_f} is a semi-algebraic set defined as

$$\mathcal{D}_{v_f} = \{v_f \in \mathbb{R} | (\bar{v} - v_f)(v_f - \underline{v}) \geq 0\}. \quad (20)$$

Because of (19), we assume that $\bar{v} \geq v_d$.

Suppose that $|d| \leq d_{\max}$ where d_{\max} is the bound for the desired yaw rate defined by the road curvature. This can be expressed equivalently as $d \in \mathcal{D}_d \subset \mathbb{R}$ where \mathcal{D}_d is a semi-algebraic set defined as

$$\mathcal{D}_d = \{d \in \mathbb{R} | d_{\max}^2 - d^2 \geq 0\}. \quad (21)$$

Moreover, let the state variable $\mathbf{x}_1 = (y, \nu, \Delta\psi, r)^\top$ of LK be bounded by some positive numbers $y_m, \nu_m, \Delta\psi_m, r_m$, respectively. That is to say, \mathbf{x}_1 is confined in the set \mathcal{X}_{LK} where

$$\mathcal{X}_{LK} = \{\mathbf{x}_1 \in \mathbb{R}^4 | |y| \leq y_m, |\nu| \leq \nu_m, |\Delta\psi| \leq \Delta\psi_m, |r| \leq r_m\}. \quad (22)$$

On the other hand, there are two varying parameters in the term $\Delta f_2(\nu r, a_L)$ of the ACC model (12). As mentioned previously, we suppose that the acceleration/deceleration of the lead car is bounded by $-a_l g$ and $a_l' g$. That is, $a_L \in \mathcal{D}_{a_L}$ where

$$\mathcal{D}_{a_L} = \{a \in \mathbb{R} | (a + a_l g)(a_l' g - a) \geq 0\}. \quad (23)$$

Finally, suppose that the state variable $\mathbf{x}_2 = (v_f, v_l, D)^\top$ of ACC is confined in the set \mathcal{X}_{ACC} where

$$\mathcal{X}_{ACC} = \{\mathbf{x}_2 \in \mathbb{R}^3 | (\bar{v} - v_f)(v_f - \underline{v}) \geq 0, (v_{\max} - v_l)(v_l - v_{\min}) \geq 0, D \geq D_0\},$$

where $v_{\max}, v_{\min} > 0$ represent the maximal and minimum speed of the lead car, respectively.

Therefore, the assume-guarantee ‘‘contract’’ between the LK and the ACC subsystems can be stated as follows:

The LK subsystem assumes that $v_f \in \mathcal{D}_{v_f}$ and guarantees that $\mathbf{x}_1 \in \mathcal{X}_{LK}$, and the ACC subsystem assumes that $|\nu r| \leq \nu_m r_m$ and guarantees that $v_f \in \mathcal{D}_{v_f}$.

In the following two subsections, CBFs that respect the above contract are constructed for LK and ACC, respectively.

B. CBFs For LK

For the LK subsystem, we construct a polynomial function $h_{lk}(\mathbf{x}_1) \in \mathcal{R}_\alpha[\mathbf{x}_1]$ that has the following form, in which α is some given positive integer indicating the polynomial degree:

$$h_{lk}(\mathbf{x}_1) = \kappa - \hat{h}_{lk}(\mathbf{x}_1) \quad (24)$$

where $\kappa \in \mathbb{R}$ is some positive number, $\hat{h}_{lk}(\mathbf{x}_1) \in \mathcal{R}_\alpha[\mathbf{x}_1]$ is a polynomial that is nonnegative. Then the safe set for LK is defined as

$$\mathcal{C}_{lk} := \{\mathbf{x}_1 \in \mathbb{R}^4 | h_{lk}(\mathbf{x}_1) \geq 0\}.$$

Here, κ is a variable used to enlarge the volume of \mathcal{C}_{lk} , which will be discussed in detail later.

Our objective is for $h_{lk}(\mathbf{x}_1)$ to satisfy the following properties:

$$\text{(LK-P1)} \quad \mathcal{C}_{lk} := \{\mathbf{x}_1 \in \mathbb{R}^4 | h_{lk}(\mathbf{x}_1) \geq 0\} \neq \emptyset, \quad (25)$$

$$\text{(LK-P2)} \quad \mathcal{C}_{lk} \subset \mathcal{X}_{LK}, \quad (26)$$

$$\text{(LK-P3)} \quad \forall \mathbf{x}_1 \in \mathcal{C}_{lk}, \forall v_f \in \mathcal{D}_{v_f}, \forall d \in \mathcal{D}_d, \\ \sup_{u_1 \in U_{lk}} [L_{f_1 + \Delta f_1} h_{lk}(\mathbf{x}_1) + L_{g_1} h_{lk}(\mathbf{x}_1) u_1 + \gamma h_{lk}(\mathbf{x}_1)] \geq 0, \quad (27)$$

where $\gamma > 0$ is a given number representing the gain in (5).

The property (LK-P1) ensures that the safe set \mathcal{C}_{lk} is non-empty, property (LK-P2) ensures that $\mathbf{x}_1 \in \mathcal{X}_{LK}$ as long as $\mathbf{x}_1 \in \mathcal{C}_{lk}$, and property (LK-P3) ensures that h_{lk} is a control barrier function for any longitudinal velocities in \mathcal{D}_{v_f} and any desired yaw rates in \mathcal{D}_d . Note that properties (LK-P1)-(LK-P3) imply the satisfaction of the hard constraints (15) and (16).

In summary, h_{lk} with properties (LK-P1)-(LK-P3) guarantees that, for any speed $v_f \in \mathcal{D}_{v_f}$ and desired yaw rate $d \in \mathcal{D}_d$, there exists steering angle $\delta_f \in U_{lk}$ such that the trajectory of the LK system stays in the set \mathcal{C}_{lk} (and thus set \mathcal{X}_{LK}) if starting from \mathcal{C}_{lk} .

Recalling that the set \mathcal{D} is the region for which the CBF condition holds (cf. Definition 1), Theorem 3 provides a sufficient condition for the existence of h_{lk} with $\mathcal{D} = \mathcal{X}_{LK}$, which is the key step in translating the properties (LK-P1)-(LK-P3) into a set of sufficient conditions that can then be synthesized by sum-of-squares programs [37], [43]. In fact, we assume that $\mathcal{D} = \mathcal{X}_{LK}$ for now, which simplifies the procedure to construct h_{lk} , and we will discuss the case $\mathcal{D} = \mathcal{C}_{lk}$ later.

Theorem 3. *Given the LK model (11), the variable bounds $y_m, \nu_m, \Delta\psi_m, r_m$, the admissible set U_{lk} defined in (13), a positive definite polynomial $p(\mathbf{x}_1)$ and the sets $\mathcal{D}_{v_f}, \mathcal{D}_d$ defined in (20) and (21), if there exist $\gamma > 0$, $\rho > 0$, some positive integer α , polynomial $h_{lk}(\mathbf{x}_1) \in \mathcal{R}_\alpha[\mathbf{x}_1]$, non-negative polynomials $s_0, s_1, \dots, s_4 \in \Sigma[\mathbf{x}_1]$ and $s_5, \dots, s_{10} \in \Sigma[\mathbf{x}_1, d, v_f]$ such that*

$$h_{lk}(\mathbf{x}_1) - (\rho - p(\mathbf{x}_1))s_0(\mathbf{x}_1) \geq 0, \quad (28)$$

$$(y^2 - y_m^2)s_1 + h_{lk}(\mathbf{x}_1) < 0, \quad (29)$$

$$(\nu^2 - \nu_m^2)s_2 + h_{lk}(\mathbf{x}_1) < 0, \quad (30)$$

$$(\Delta\psi^2 - \Delta\psi_m^2)s_3 + h_{lk}(\mathbf{x}_1) < 0, \quad (31)$$

$$(r^2 - r_m^2)s_4 + h_{lk}(\mathbf{x}_1) < 0, \quad (32)$$

$$\sup_{u_1 \in U_{lk}} [L_{f_1 + \Delta f_1} h_{lk}(\mathbf{x}_1) + L_{g_1} h_{lk}(\mathbf{x}_1) u_1 + \gamma h_{lk}(\mathbf{x}_1)]$$

$$\begin{aligned} & - (y_m^2 - y^2)s_5 - (\nu_m^2 - \nu^2)s_6 - (\Delta\psi_m^2 - \Delta\psi^2)s_7 \\ & - (r_m^2 - r^2)s_8 - (d_{\max}^2 - d^2)s_9 - (\bar{v} - v_f)(v_f - \underline{v})s_{10} \geq 0, \end{aligned} \quad (33)$$

then $h_{lk}(\mathbf{x}_1)$ satisfies properties (LK-P1)-(LK-P3) defined in (25)-(27).

Proof. Condition (28) implies (LK-P1) because $h_{lk}(\mathbf{x}_1) \geq 0$ whenever $p(\mathbf{x}_1) \leq \rho$, which means that $\{\mathbf{x}_1 | p(\mathbf{x}_1) \leq \rho\} \subseteq \mathcal{C}_{lk}$ and therefore $\mathcal{C}_{lk} \neq \emptyset$. Based on the S-procedure, conditions (29)-(32) imply (LK-P2) because $|y| < y_m, |\nu| < \nu_m, |\Delta\psi| < \Delta\psi_m$ and $|r| < r_m$ whenever $h_{lk}(\mathbf{x}_1) \geq 0$. Condition (33) implies condition (LK-P3), since (27) holds whenever $\mathbf{x}_1 \in \mathcal{X}_{LK}, v_f \in \mathcal{D}_{v_f}, d \in \mathcal{D}_d$. \square

In addition to the properties (LK-P1)-(LK-P3), it is desirable for h_{lk} to maximize the volume of \mathcal{C}_{lk} , the portion of the safe set that the CBF renders controlled invariant. To this end, we normalize the coefficients of \hat{h}_{lk} by adding the constraint $\hat{h}_{lk}((1, \dots, 1)^\top) = 1$ (i.e., the sum of the coefficients is equal to 1) and maximizing κ . Note that the normalization is necessary to make the maximization of κ valid, since otherwise the coefficients of \hat{h}_{lk} can be scaled accordingly with κ that results in the same \mathcal{C}_{lk} , which makes maximizing κ have no meaning. The normalization method has also been used in finding the maximal region of attraction of a control system using Lyapunov function and SOS [39], [44].

The terms ρs_0 in (28) and γh_{lk} in (33) involve products of the unknowns, but it can be turned into linear constraints on the unknowns through bisecting ρ and γ . Moreover, the maximization over the allowed steering angles in (33) also involves a product of the unknowns, which can be overcome by finding an explicit formula for the controller and iterating between improving the current control solution and the CBF.

In what follows, we explain in detail the iterative procedure to construct h_{lk} , which satisfies (28)-(33) and maximizes the volume of \mathcal{C}_{lk} , using SOS programs.

1. Initialization. The iteration process is initialized by first computing an LQR controller for a nominal value of $v_f \in \mathcal{D}_{v_f}$ and $d = 0$. More specifically, we first choose weight matrices $Q \in \mathbb{R}^{4 \times 4}$ penalizing the state and $R \in \mathbb{R}$ penalizing the input, where look-ahead of the road curvature can be taken into account in Q [5]. Then we solve for the LQR gain $K \in \mathbb{R}^{1 \times 4}$ for the system $(A(v_f), B)$ with a given and fixed $v_f \in \mathcal{D}_{v_f}$. Based on the gain K , we fix the control $u_1 = \frac{-K\mathbf{x}_1}{1 + \eta(K\mathbf{x}_1)^2}$ and solve for h_{lk} using a feasibility SOS program, with η selected as $\eta = 1/(2\hat{\delta}_f)^2$. This value implies that $|\frac{-K\mathbf{x}_1}{1 + \eta(K\mathbf{x}_1)^2}| \leq \hat{\delta}_f$ and therefore $u_1 \in U_{lk}$.

Remark 1. *The motivation for scaling the LQR control $-K\mathbf{x}_1$ by $1 + \eta(K\mathbf{x}_1)^2$ includes: (i) an LQR controller gain K is easily computed; (ii) the value function of the LQR controller corresponds to a quadratic form, and there always exists a sufficiently small sublevel set of the quadratic form contained in \mathcal{X}_{LK} , for which the values of the controller over that sublevel set lie in U_{lk} ; and (iii), while there is no guarantee that the controller u_1 computed in this manner will result in a feasible SOS program (i.e., the following (\mathcal{P}_0)) for all $v_f \in \mathcal{D}_{v_f}$ and $d \in \mathcal{D}_d$, this has not been a problem in the*

examples we have worked when ρ is sufficiently small. Of course, the user is free to use other control synthesis methods to initiate the iteration process. It is also a choice whether or not to feed forward the desired yaw rate.

Given an LQR gain K , we choose values for $\gamma > 0$ and sufficiently small $\rho_0 > 0, \varepsilon > 0$ and use the following feasibility SOS program for initialization.

(\mathcal{P}_0) :

find $h_{lk} \in \mathcal{R}_\alpha[\mathbf{x}_1], s_0, s_1, \dots, s_4 \in \Sigma[\mathbf{x}_1], s_5, \dots, s_{10} \in \Sigma[\mathbf{x}_1, d, v_f]$
such that

$$h_{lk} - (\rho_0 - p)s_0 \in \Sigma[\mathbf{x}_1], \quad (34)$$

$$-h_{lk} - (y^2 - y_m^2)s_1 - \varepsilon \in \Sigma[\mathbf{x}_1], \quad (35)$$

$$-h_{lk} - (\nu^2 - \nu_m^2)s_2 - \varepsilon \in \Sigma[\mathbf{x}_1], \quad (36)$$

$$-h_{lk} - (\Delta\psi^2 - \Delta\psi_m^2)s_3 - \varepsilon \in \Sigma[\mathbf{x}_1], \quad (37)$$

$$-h_{lk} - (r^2 - r_m^2)s_4 - \varepsilon \in \Sigma[\mathbf{x}_1], \quad (38)$$

$$\begin{aligned} \frac{\partial h_{lk}}{\partial \mathbf{x}_1} [A(v_f)\mathbf{x}_1 + Ed][1 + \eta(K\mathbf{x}_1)^2]v_f + \frac{\partial h_{lk}}{\partial \mathbf{x}_1} B(-K\mathbf{x}_1)v_f \\ + \gamma h_{lk}[1 + \eta(K\mathbf{x}_1)^2]v_f - (y_m^2 - y^2)s_5 - (\nu_m^2 - \nu^2)s_6 \\ - (\Delta\psi_m^2 - \Delta\psi^2)s_7 - (r_m^2 - r^2)s_8 - (d_{\max}^2 - d^2)s_9 \\ - (\bar{v} - v_f)(v_f - \underline{v})s_{10} \in \Sigma[\mathbf{x}_1, d, v_f], \end{aligned} \quad (39)$$

where $\eta = 1/(2\hat{\delta}_f)^2$.

Note that (34) implies (LK-P1), (35)-(38) imply (LK-P2) based on the S-procedure, and (39) implies that for any $\mathbf{x}_1 \in \mathcal{X}_{LK}, v_f \in \mathcal{D}_{v_f}, d \in \mathcal{D}_d$,

$$\frac{\partial h_{lk}}{\partial \mathbf{x}_1} [A(v_f)\mathbf{x}_1 + B \frac{-K\mathbf{x}_1}{1 + \eta(K\mathbf{x}_1)^2} + Ed] + \gamma h_{lk} \geq 0. \quad (40)$$

Thus, (40) means that the control $u_1 = \frac{-K\mathbf{x}_1}{1 + \eta(K\mathbf{x}_1)^2} \in U_{lk}$ results in the CBF condition $\dot{h}_{lk}(\mathbf{x}_1, v_f, d, u_1) + \gamma h_{lk}(\mathbf{x}_1) \geq 0$ holding. Because $A(v_f)$ is a rational matrix with the denominator v_f in some of its entries, it needs to be multiplied with v_f so that it becomes a polynomial [43]. Note that in (\mathcal{P}_0) and in what follows, the degrees of the multipliers s_i are not specified explicitly and assumed to be chosen appropriately.

If (\mathcal{P}_0) is infeasible, we repeat it by modifying parameters $Q, R, \gamma, \rho_0, \varepsilon$ and increasing α ; otherwise, h_{lk} is obtained as a polynomial that satisfies properties (LK-P1)-(LK-P3). Then, the following two steps will be used to find a polynomial h_{lk} that increases the volume of \mathcal{C}_{lk} .

2.Synthesize Controller. Given the polynomial h_{lk} from the initialization step, which is denoted as h_{lk}^{old} in the subsequent (\mathcal{P}_1), we use the following maximization SOS program to find a new controller $u \in \mathcal{R}_\beta[\mathbf{x}_1, d, v_f]$ with some positive integer $\beta, \kappa \in \mathbb{R}$ and multipliers $s_i (0 \leq i \leq 22)$, such that $u \in U_{lk}$, κ is maximized and for any $\mathbf{x}_1 \in \mathcal{X}_{LK}, v_f \in \mathcal{D}_{v_f}, d \in \mathcal{D}_d$, the CBF condition (27) holds.

(\mathcal{P}_1) :

max κ

over $\kappa \in \mathbb{R}, u \in \mathcal{R}_\beta[\mathbf{x}_1, d, v_f], s_0, s_1, \dots, s_4 \in \Sigma[\mathbf{x}_1],$

$s_5, \dots, s_{22} \in \Sigma[\mathbf{x}_1, d, v_f]$, such that

$$h_{lk} - h_{lk}^{old} s_0 \in \Sigma[\mathbf{x}_1], \quad (41)$$

(35) – (38) hold,

$$\begin{aligned} \frac{\partial h_{lk}}{\partial \mathbf{x}_1} [A(v_f)\mathbf{x}_1 + Bu(\mathbf{x}_1, d, v_f) + Ed]v_f + \gamma h_{lk}v_f \\ - (y_m^2 - y^2)s_5 - (\nu_m^2 - \nu^2)s_6 - (\Delta\psi_m^2 - \Delta\psi^2)s_7 \\ - (r_m^2 - r^2)s_8 - (\bar{v} - v_f)(v_f - \underline{v})s_9 \\ - (d_{\max}^2 - d^2)s_{10} \in \Sigma[\mathbf{x}_1, d, v_f], \end{aligned} \quad (42)$$

$$\begin{aligned} u(\mathbf{x}_1, d, v_f) + \hat{\delta}_f - (y_m^2 - y^2)s_{11} - (\nu_m^2 - \nu^2)s_{12} \\ - (\Delta\psi_m^2 - \Delta\psi^2)s_{13} - (r_m^2 - r^2)s_{14} - (d_{\max}^2 - d^2)s_{15} \\ - (\bar{v} - v_f)(v_f - \underline{v})s_{16} \in \Sigma[\mathbf{x}_1, d, v_f], \end{aligned} \quad (43)$$

$$\begin{aligned} -u(\mathbf{x}_1, d, v_f) + \hat{\delta}_f - (y_m^2 - y^2)s_{17} - (\nu_m^2 - \nu^2)s_{18} \\ - (\Delta\psi_m^2 - \Delta\psi^2)s_{19} - (r_m^2 - r^2)s_{20} - (d_{\max}^2 - d^2)s_{21} \\ - (\bar{v} - v_f)(v_f - \underline{v})s_{22} \in \Sigma[\mathbf{x}_1, d, v_f]. \end{aligned} \quad (44)$$

Condition (42) means that with such u , the CBF condition $\dot{h}_{lk}(\mathbf{x}_1, v_f, d, u) + \gamma h_{lk}(\mathbf{x}_1) \geq 0$ holds, for any $\mathbf{x}_1 \in \mathcal{X}_{lk}, d \in \mathcal{D}_d, v_f \in \mathcal{D}_{v_f}$. Conditions (43)-(44) mean that the synthesized $u \in \mathcal{R}_\beta[\mathbf{x}_1, d, v_f]$ satisfies $|u| \leq \hat{\delta}_f$, which implies that $u \in U_{lk}$, for any $\mathbf{x}_1 \in \mathcal{C}_{lk}, d \in \mathcal{D}_d, v_f \in \mathcal{D}_{v_f}$.

When the procedure goes from (\mathcal{P}_0) to (\mathcal{P}_1), which will happen only once, it is not guaranteed that (\mathcal{P}_1) will be feasible. In case of infeasibility, we can increase the degree of u and repeat (\mathcal{P}_1). However, in all examples we have worked, (\mathcal{P}_1) has been feasible, even when u is chosen to be of degree two. On the other hand, (\mathcal{P}_1) will always be feasible when executed after (\mathcal{P}_2), another SOS program that will be discussed shortly. Therefore, we assume that (\mathcal{P}_1) is feasible at initialization and proceed.

Remark 2. If we choose the controller in (\mathcal{P}_1) to be a rational function in the form of $\tilde{K}_1\mathbf{x}_1/(1 + \mathbf{x}_1^\top \tilde{K}_2\mathbf{x}_1)$ where $\tilde{K}_1 \in \mathbb{R}^{1 \times 4}, \tilde{K}_2 \in \mathbb{R}^{4 \times 4}$ positive definite, then (\mathcal{P}_1) is guaranteed to be feasible because (40) holds and u_1 in (\mathcal{P}_0) is a rational polynomial function of the same form. Higher order terms can also be included in the numerator/denominator of the rational function. The following algorithms remain true after appropriate modifications, if the rational functions template are used for the controller. This also validates the above assumption that (\mathcal{P}_1) is always feasible.

3.Synthesize Barrier. Given the controller $u(\mathbf{x}_1, d, v_f)$ and the CBF h_{lk} from (\mathcal{P}_1), which will be denoted as h_{lk}^{old} in the subsequent (\mathcal{P}_2), the following SOS program finds a new CBF h_{lk} and multipliers s_0, s_1, \dots, s_{10} to maximize κ .

(\mathcal{P}_2) :

max κ

over $\kappa \in \mathbb{R}, \hat{h}_{lk} \in \mathcal{R}_\alpha[\mathbf{x}_1], s_0, s_1, \dots, s_4 \in \Sigma[\mathbf{x}_1],$

$s_5, \dots, s_{10} \in \Sigma[\mathbf{x}_1, d, v_f]$, such that

(35) – (38), (41) and (42) hold.

Note that (\mathcal{P}_2) is always feasible since u and κ in (\mathcal{P}_1) constitute a feasible solution, and the resulting h_{lk} is a polynomial satisfying (28)-(33) and therefore properties (LK-P1)-(LK-P3).

With the new CBF h_{lk} constructed, we return to Step 2 to continue the iterative procedure until convergence. Because \mathcal{X}_{LK} is a compact set and the constructed set \mathcal{C}_{lk} in each step of (\mathcal{P}_1) - (\mathcal{P}_2) is no smaller than in the previous step, asymptotic convergence is guaranteed. In practice, we can either terminate the algorithm when the change of κ is below some threshold, or simply set in advance the number of iterations. Furthermore, when we return to (\mathcal{P}_1) , it is guaranteed to be feasible since u in the last step, i.e., (\mathcal{P}_2) , is a feasible solution.

Algorithm 1 and Proposition 2 summarize the above results.

Algorithm 1 Synthesis of Control Barrier Functions for LK

Input: $y_m, \nu_m, \Delta\psi_m, r_m, \hat{\delta}_f, d_{\max}, \bar{v}, \underline{v}, Q, R, \gamma, \varepsilon, \rho_0, p, \alpha, \beta$

Output: $\kappa, \hat{h}_{lk}(\mathbf{x}_1), u(\mathbf{x}_1, d, v_f)$

- 1: Solve for the LQR gain K and solve (\mathcal{P}_0)
 - 2: **while** (\mathcal{P}_0) is not feasible **do**
 - 3: Modify Q, R, γ, ρ_0 and solve (\mathcal{P}_0)
 - 4: **end while**
 - 5: converged = false
 - 6: **while** \neg converged **do**
 - 7: Fix \hat{h}_{lk} , find u, s_i, κ and maximize κ by solving (\mathcal{P}_1)
 - 8: Fix u , find $\hat{h}_{lk}, s_i, \kappa$ and maximize κ by solving (\mathcal{P}_2)
 - 9: **if** $|\kappa^{new} - \kappa^{old}| \leq$ some threshold **then**
 - 10: converged = true
 - 11: **end if**
 - 12: **end while**
-

Proposition 2. *If (\mathcal{P}_0) is feasible, then Algorithm 1 terminates and the polynomial $h_{lk}(\mathbf{x}_1)$ returned by it satisfies properties (LK-P1)-(LK-P3).*

Remark 3. *There are no efficient and reliable solvers for semi-definite programs with bilinear constraints in the decision variables, which are non-convex and known to be NP-hard in general. Iterative procedures have therefore been commonly used to bypass the bilinear constraints for SOS programs; for instance, they were used to search for control Lyapunov functions in [45] and to construct an invariant funnel along trajectories in [39]. However, in contrast to the cited results, the particular controller constructed in Algorithm 1 is not important to us since it will not be implemented directly on the system; indeed, the actual control input will be generated by solving a quadratic program that will be explained in Section V. In fact, it is the CBF h_{lk} that is crucial to us, because it characterizes the safe set \mathcal{C}_{lk} that can be rendered controlled invariant using input values selected from U_{lk} . These observations allow us to focus on the construction of the CBFs instead of the control law (recall the discussion in Remark 2 about the flexible form of the controller).*

By fixing h_{lk} and u obtained from Algorithm 1, we can further maximize γ by solving the following SOS program:

$$\begin{aligned} & \max \gamma \\ & \text{over } \gamma \in \mathbb{R}, s_0, \dots, s_4 \in \Sigma[\mathbf{x}_1], s_5, \dots, s_{10} \in \Sigma[\mathbf{x}_1, d, v_f] \\ & \text{such that (42) holds.} \end{aligned}$$

With the maximal γ , we obtain the maximal allowable input set $K_{zcbf}(x)$ (cf. Definition 6) w.r.t. the CBF h_{lk} , from which

the input can render the set \mathcal{C}_{lk} controlled invariant under the dynamics of the LK system.

Remark 4. *Since the CBF h_{lk} satisfies $\dot{h}_{lk} + \gamma h_{lk} \geq 0$ in \mathcal{X}_{LK} , the set \mathcal{C}_{lk} is asymptotically stable in \mathcal{X}_{LK} under a control law taking values from $K_{zcbf}(x)$. Therefore, we can take into account affine disturbances in (9) similar to the argument in [32], by which it can be shown that the LK system is input-to-state stable with respect to the disturbances and a larger controlled invariant set containing \mathcal{C}_{lk} can be quantitatively given.*

The argument above shows that, if we choose $\mathcal{D} = \mathcal{X}_{LK}$, then \mathcal{C}_{lk} is controlled invariant and is attractive within \mathcal{X}_{LK} under control from $K_{zcbf}(x)$. On the other hand, if we choose $\mathcal{D} = \mathcal{C}_{lk}$, we will get a larger set \mathcal{C}_{lk} in principle (since it is not attractive outside \mathcal{C}_{lk}), but constructing h_{lk} that defines such \mathcal{C}_{lk} would then become more involved. Note that for this case, Theorem 3 is still true if condition (42) is changed into:

$$\begin{aligned} & \frac{\partial h_{lk}}{\partial \mathbf{x}_1} [A(v_f)\mathbf{x}_1 + Bu(\mathbf{x}_1, d, v_f) + Ed]v_f + \gamma h_{lk}v_f - h_{lk}s_5 \\ & - (\bar{v} - v_f)(v_f - \underline{v})s_6 - (d_{\max}^2 - d^2)s_7 \in \Sigma[\mathbf{x}_1, d, v_f]. \end{aligned} \quad (45)$$

where $s_5, s_6, s_7 \in \Sigma[\mathbf{x}_1, d, v_f]$ are multipliers to be found.

As shown in (45), $h_{lk}s_5$ is an additional bilinear term of the unknowns if SOS programs are applied to construct h_{lk} for $\mathcal{D} = \mathcal{C}_{lk}$. To bypass this difficulty, we can divide (\mathcal{P}_1) into two steps as follows: (i) fix h_{lk} , search for $u \in \mathcal{R}_\beta[\mathbf{x}_1, d, v_f]$, $s_i \in \Sigma[\mathbf{x}_1, d, v_f]$ by solving a feasibility SOS program, (ii) fix \hat{h}_{lk} , the control u and the multipliers s_i obtained in (i), search for κ and maximize it by solving a maximization SOS program. Then, if Line 7 of Algorithm 1 is replaced with these two steps, the resulting CBF h_{lk} will satisfy properties (LK-P1)-(LK-P3).

Remark 5. *A bound on lateral acceleration \dot{v} , which was introduced as a soft constraints for LK in Subsection III-B, can be added as a (hard) constraint to the SOS programs. However, by doing this, the feasibility of (\mathcal{P}_1) and (\mathcal{P}_2) will no longer be guaranteed. Thus, this constraint is not considered, and will be discussed later in Section V.*

Remark 6. *Using the SOS optimization is not the only way to design CBFs. Gerdes et al. developed a Lagrangian model of the lateral dynamics and then augmented the corresponding Hamiltonian with an additional potential term to enforce the invariance of a set delineated by the lane boundaries, in the face of road curvature variations [5]. However, with this method, it is unclear how to address bounds on steering angle, yaw rate and lateral velocity, as we have done in (29)-(32); moreover, there is no distinction between safety—staying within the lane markers—and performance—how much to override the driver or how close to remain centered in the lane. When applying LQR to the LK problem, the cost-to-go function resulting from solving the Riccati equation for a constant longitudinal speed v_f does yield a quadratic barrier function for the closed-loop lateral-yaw model, with v_f in a small neighborhood of the nominal speed, and hence is also a CBF for the open-loop lateral-law model for the same range of*

longitudinal speed. However, the LQR approach to developing a CBF cannot handle the bounded input/state or the varying road curvature constraints; moreover, our experience is that the associated safe set computed from a sub-level set of the cost-to-go function is unacceptably small.

C. CBFs For ACC

Similar to LK, we can also use SOS programs to construct CBFs for ACC. Specifically, we seek a polynomial function $h_{acc}(\mathbf{x}_2) \in \mathcal{R}_{\alpha'}[\mathbf{x}_2]$ of the following form where α' is some given positive integer:

$$h_{acc}(\mathbf{x}_2) := D - \tau_d v_f - D_0 - \hat{h}_{acc}(v_f, v_l) \quad (46)$$

with $\hat{h}_{acc}(v_f, v_l) \in \mathcal{R}_{\alpha'}[v_f, v_l]$, such that h_{acc} satisfies the following properties:

$$(\text{ACC-P1}) \mathcal{C}_{acc} := \{\mathbf{x}_2 \in \mathbb{R}^3 | h_{acc}(\mathbf{x}_2) \geq 0\} \neq \emptyset, \quad (47)$$

$$(\text{ACC-P2}) \forall v_f \in \mathcal{D}_{v_f}, \forall v_l \in \mathcal{D}_{v_l}, h_a(v_f, v_l) \geq 0, \quad (48)$$

$$(\text{ACC-P3}) \forall \mathbf{x}_2 \in \mathcal{X}_{ACC}, \forall a_L \in \mathcal{D}_{a_L}, \forall |\nu r| \leq \nu_m r_m, \quad (49)$$

$$\sup_{u_2 \in \mathcal{U}_{acc}} [L_{f_2 + \Delta f_2} h_{acc}(\mathbf{x}_2) + L_{g_2} h_{acc}(\mathbf{x}_2) u_2] \geq 0.$$

A reason to use the particular form (46) for h_{acc} is to ensure (18) holds while the minimum D (the relative distance between the two cars) satisfying $h_{acc}(\mathbf{x}_2) \geq 0$ can be calculated easily. Because of this choice, we use the condition $\dot{h}_{acc}(\mathbf{x}_2, u_2) \geq 0$ instead of the CBF condition $\dot{h}_{acc}(\mathbf{x}_2, u_2) + \gamma h_{acc}(\mathbf{x}_2) \geq 0$, since $\dot{h}_{acc} + \gamma h_{acc}$ is a polynomial with which the maximal degree of D is 1, and therefore can not have a SOS decomposition. However, in the set \mathcal{C}_{acc} , $\dot{h}_{acc}(\mathbf{x}_2, u_2) \geq 0$ implies $\dot{h}_{acc}(\mathbf{x}_2, u_2) + \gamma h_{acc}(\mathbf{x}_2) \geq 0$ for any $\gamma > 0$.

Sufficient conditions on $h_{acc}(\mathbf{x}_2)$ for ACC can be given similar to Theorem 3, and the SOS program can be used to construct $h_{acc}(\mathbf{x}_2)$ similar to Algorithm 1. The constructed h_{acc} is guaranteed to satisfy properties (ACC-P1)-(ACC-P3), and therefore the hard constraint (18) for ACC.

When carrying out this procedure, we found the resulting function h_{acc} always yielded a ‘‘conservative’’ safe set, even when a high degree polynomial is chosen. More specifically, for any speed pair $\mathbf{x}_2 \in \mathcal{X}_{ACC}$, $\min\{D | h_{acc}(\mathbf{x}_2) \geq 0\}$ represents the minimum safe following distance between the two cars, as determined by the CBF, for guaranteeing satisfaction of the ACC specification. If this distance is overly cautious, traffic will continually cut in front of the ACC-controlled vehicle. When assuming h_{acc} to be continuously differentiable as in the LK problem, we found the resulting minimum safe following distance to be unacceptably large. One way to remedy this is to assume h_{acc} to be continuous and composed of a finite set of continuously differentiable functions (cf. Section II). As the number of ‘‘pieces’’ increases, a less conservative CBF can be constructed using SOS, albeit at the cost of increased computation and implementation burden.

Apart from the SOS optimization, we can also construct h_{acc} using physics-based optimization. The ACC subsystem (10) has the following monotone property: if $(\hat{D}, v_f, v_l) \in \mathcal{C}_{acc}$ when $a_L = -a_l g$ and $u_2 = -a_f g$, then $(D, v_f, v_l) \in$

\mathcal{C}_{acc} for any $D \geq \hat{D}$. In light of this, we can calculate $\min\{D | \mathbf{x}_2 \in \mathcal{C}_{acc}\}$ by fixing $a_L = -a_l g$ and $u_2 = -a_f g$. This property was exploited in our previous work to compute in closed form two sets of CBFs for ACC, given by a set of three or four continuously differentiable functions; see [41] and its supplemental material [46].

In the derivation in [46], we assumed that the first equality in (10) is simplified to

$$\dot{v}_f = \frac{\hat{u}_2}{m},$$

where $\hat{u}_2 \geq -\hat{a}_f m g$ for some $\hat{a}_f > 0$. Noting (10), we have $\hat{u}_2 = u_2 - (c_0 + c_1 v_f) - m \nu r$, and then in our setting,

$$\hat{a}_f \geq a_f + (c_0 + c_1 \underline{v})/m g - \nu_m r_m / g. \quad (50)$$

In summary, by using a conservative deceleration bound that takes into account the aerodynamic drag and the contract bound for the term $|\nu r|$, the closed-form CBFs proposed in [41] and [46] are used to construct h_{acc} satisfying properties (ACC-P1)-(ACC-P3), where \hat{a}_f are chosen to be the right hand side of (50).

V. COMPOSITIONAL CONTROL SYNTHESIS VIA QUADRATIC PROGRAM

In this section, a solution will be provided to the composition problem of LK and ACC formulated in subsection III-C. Roughly speaking, the controls are generated by quadratic programs that combine the hard constraints (i.e., safety), which are expressed as CBF conditions, and the soft constraints (i.e., control objectives), which indicate the closeness to some nominal control and are usually expressed as CLF conditions, so that the hard constraints are always satisfied and the soft constraints are mediated (via some relaxation variables) when they conflict with the hard constraints.

For the control system (4), a special class of CLF $V(x)$ is the so-called *exponentially stabilizing control Lyapunov function (ES-CLF)* [47], which yields a set of control inputs that exponentially stabilizes the system (4) to its zero dynamics and can be expressed as

$$K_c(x) = \{u \in U | L_f V(x) + L_g V(x) u + c V(x) \leq 0\}, \quad (51)$$

where c is some positive number that can be chosen to change the convergence rate. Therefore, the ES-CLF can be used to express the control objective that can be expressed as a stabilization problem, where a relaxation variable is added to the right hand side of (51) to make it a soft constraint. Apart from the CLFs, the control objectives can be also expressed as rendering the real control as close as possible to some nominal control, by adding a relaxation variable as well, where a similar idea was used in the reference governors [27].

As discussed in preceding sections, the hard constraints are expressed as the controlled invariance of the sets \mathcal{C}_{lk} for LK and \mathcal{C}_{acc} for ACC, using the CBF condition. Because of the assumptions and guarantees between the two subsystems, the controlled invariant set for the compositional system is a Cartesian product of \mathcal{C}_{lk} and \mathcal{C}_{acc} , and the behaviors of the LK and ACC subsystems can be decoupled as long as their states are confined within these two sets, respectively. Therefore,

local controllers for LK and ACC can be synthesized by solving two separate QPs.

Next, we show in detail how to construct the QPs with these constraints. The soft constraint (17) for LK can be expressed as follows:

$$u_1 = \bar{K}(\mathbf{x}_1 - \mathbf{x}_1^f) + \delta_1, \quad (52)$$

where $\delta_1 > 0$ is a relaxation variable, $\mathbf{x}_1^f = [0, 0, 0, d]^\top$ is a feedforward term, and \bar{K} is a feedback gain determined by solving a LQR problem such that $\mathbf{x}_1 \rightarrow \mathbf{x}_1^f$.

Moreover, we use a candidate control Lyapunov function $V(x) := (v_f - v_d)^2$ to express the soft constraint (19) for ACC, using the following CLF condition:

$$L_{f_2+\Delta f_2}V(x) + L_{g_1}V(x)u_2 + cV(x) \leq \delta_2, \quad (53)$$

where $\delta_2 > 0$ is the second relaxation variable, and $c > 0$ is a given constant.

Based on the CBFs $h_{lk}(\mathbf{x}_1)$, $h_{acc}(\mathbf{x}_2)$ constructed in Section IV with some positive gains γ_1, γ_2 , the hard constraints for LK and ACC can be expressed as follows

$$L_{f_1+\Delta f_1}h_{lk}(\mathbf{x}_1) + L_{g_1}h_{lk}(\mathbf{x}_1)u_1 + \gamma_1h_{lk}(\mathbf{x}_1) \geq 0, \quad (54)$$

$$L_{f_2+\Delta f_2}h_{acc}(\mathbf{x}_2) + L_{g_2}h_{acc}(\mathbf{x}_2)u_2 + \gamma_2h_{acc}(\mathbf{x}_2) \geq 0. \quad (55)$$

Then, among the set of controls that satisfy constraints (52)-(55), the *min-norm controllers* [48] are obtained by solving the following two QPs:

$$\mathbf{u}_1^*(x) = \underset{\mathbf{u}_1=[u_1, \delta_1]^\top \in \mathbb{R}^2}{\operatorname{argmin}} \frac{1}{2} \mathbf{u}_1^\top H_{lk} \mathbf{u}_1 + F_{lk}^\top \mathbf{u}_1 \quad (\text{QP-LK})$$

$$\text{s.t. } A_{lk} \mathbf{u}_1 \leq b_{lk},$$

$$u_1 = -K(\mathbf{x}_1 - \mathbf{x}_1^f) + \delta_1,$$

$$\mathbf{u}_2^*(x) = \underset{\mathbf{u}_2=[u_2, \delta_2]^\top \in \mathbb{R}^2}{\operatorname{argmin}} \frac{1}{2} \mathbf{u}_2^\top H_{acc} \mathbf{u}_2 + F_{acc}^\top \mathbf{u}_2 \quad (\text{QP-ACC})$$

$$\text{s.t. } A_{acc} \mathbf{u}_1 \leq b_{acc},$$

$$A_{acc}^{clf} \mathbf{u}_1 \leq b_{acc}^{clf} + \delta_2,$$

where

$$H_{lk} = \begin{bmatrix} 1 & 0 \\ 0 & p_2 \end{bmatrix}, \quad F_{lk} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

$$H_{acc} = \begin{bmatrix} \frac{1}{m^2} & 0 \\ 0 & p_1 \end{bmatrix}, \quad F_{acc} = - \begin{bmatrix} \frac{F_r}{m^2} \\ 0 \end{bmatrix},$$

$$A_{lk} = [-L_{g_1}h_{lk}(\mathbf{x}_1), 0],$$

$$b_{lk} = L_{f_1+\Delta f_1}h_{lk}(\mathbf{x}_1) + \gamma_1h_{lk}(\mathbf{x}_1),$$

$$A_{acc} = [-L_{g_2}h_{acc}(\mathbf{x}_2), 0],$$

$$b_{acc} = L_{f_2+\Delta f_2}h_{acc}(\mathbf{x}_2) + \gamma_2h_{acc}(\mathbf{x}_2),$$

$$A_{acc}^{clf} = [L_{g_2}V(x), -1],$$

$$b_{acc}^{clf} = -(L_{f_2+\Delta f_2}V(x) + cV(x)),$$

and $p_1, p_2 \gg 0$ are the penalizing weights for relaxation variables δ_1, δ_2 , respectively. Here, H_{acc}, F_{acc} are chosen as such due to partial input/output linearization of (10) [41].

It was shown in [41] that u_1, u_2 can be actually expressed in closed-forms and are locally Lipschitz continuous, which

makes it easier to use in real implementations. More importantly, the longitudinal force u_1 and the steering angle u_2 obtained by (QP-LK) and (QP-ACC) guarantee the simultaneous operation of LK and ACC in a formally correct way.

Theorem 4. *The solutions generated by (QP-LK) and (QP-ACC) constitute a locally Lipschitz continuous control strategy $X \rightarrow U_{acc} \times U_{lk}$ that ensures the hard constraints (15), (16) and (18) are satisfied for all time.*

The soft constraint about the lateral acceleration can be expressed as $|\dot{v}| \leq \dot{v}_{\max} + \delta_3$ where δ_3 is another relaxation variable and \dot{v}_{\max} is the given lateral acceleration bound. Therefore, adding this constraint and modifying the matrices H_{lk}, F_{lk} to (QP-LK) in an obvious way, we can still obtain a solution that ensures the satisfaction of the hard constraints.

VI. SIMULATION

In this section, we apply the control laws u_1, u_2 , which are obtained by solving QPs (QP-LK) and (QP-ACC), to the simultaneous operation of the LK model (11) and ACC model (12), respectively. The overall system is shown to operate in a correct way satisfying all of the safety specifications.

The SOS programs are solved using the MATLAB toolbox yalmip along with the SDP solver Mosek. The QPs are solved using the MATLAB command *quadprog*, but they could be just as easily solved in closed-form using the results in [41]. The parameter values used in the simulations are shown in Table I. We assume that the road has a maximal turn rate of $d_{max} = 0.05 \text{ rad/s}$, which is consistent with the recommended value in [49]. The controlled car is allowed to employ a maximal deceleration of 0.25 g , maximal steering angle of 0.06 rad (i.e., approximately 3.5 degrees), and have a desired pre-set speed $v_d = 22 \text{ m/s}$ and time-headway setting $\tau_d = 1.8$ seconds. The lateral displacement of the car from the road center is assumed to be bounded by $y_{\max} = 0.9 \text{ m}$, the lateral velocity is bounded by $v_{\max} = 1 \text{ m/s}$, the yaw angle deviation is bounded by $\Delta\psi_{\max} = 0.05 \text{ rad}$ and the yaw rate is bounded by $r_{\max} = 0.3 \text{ rad/s}$. Other parameter values and constraints can be easily found in Table I.

TABLE I
PARAMETER VALUES AND CONSTRAINTS

| | | | | | |
|------------------|----------------------------|-----------------|-----------------------|------------|------|
| m | 1650 kg | y_m | 0.9 m | p_1 | 1000 |
| c_0 | 51 N | v_m | 1.0 m/s | p_2 | 1000 |
| c_1 | 1.26 Ns/m | $\Delta\psi_m$ | 0.05 rad | p_3 | 100 |
| a | 1.11 m | r_m | 0.3 rad/s | a_f | 0.25 |
| b | 1.59 m | \underline{v} | 15 m/s | a'_f | 0.25 |
| C_f | 133000 N/rad | \bar{v} | 30 m/s | a_l | 0.25 |
| C_r | 98800 N/rad | v_{\min} | 15 m/s | a_i | 0.25 |
| I_z | 2315.3 kg · m ² | v_{\max} | 30 m/s | γ_2 | 2 |
| d_{\max} | 0.05 rad/s | v_d | 22 m/s | γ_1 | 2 |
| δ_f | 0.06 rad | D_0 | 0.2 m | c | 10 |
| \dot{v}_{\max} | 0.25 m/s ² | g | 9.81 m/s ² | τ_d | 1.8 |

The gain matrix \bar{K} in (52) is obtained by solving a LQR problem. Assume that the controlled car uses a lateral preview of approximately 0.4 seconds, which corresponds

to an “output” Cx with $C = [1, 0, 10, 0]$. Given the control weight $R = 600$ and the state weight matrix $Q = K_p C^T C + K_d C^T A_1^T A_1 C$, where A_1 is given in (11) and $K_p = 5, K_d = 0.4$, the feedback gain \bar{K} is determined by solving an LQR problem with such Q and R .

With the parameters given in Table I, Algorithm 1 terminates and returns the following CBF $h_{lk}(\mathbf{x}_1)$ for LK:

$$\begin{aligned} h_{lk}(\mathbf{x}_1) = & 2.4279 - 3.1156y^2 - 2.6144\nu^2 - 983.1484\Delta\psi^2 \\ & - 29.7346r^2 + 0.2882y\nu + 12.1793y\Delta\psi + 0.1532\nu\Delta\psi \\ & - 3.1066yr + 4.6898\nu r + 4.4091\Delta\psi r. \end{aligned}$$

Using $h_{lk}(\mathbf{x}_1)$ above and the set of “optimal barriers” $h_{acc}(\mathbf{x}_2)$ in [46], the simulation results are shown in Figure 2, where all the hard constraints are satisfied with the soft constraints achieved as well. Subfigure (a) shows the speed of the lead car v_f (in blue) and the following car v_l (in black), and the desired speed v_d and the lower speed bound \underline{v} (in dotted red); it can be seen that the following car achieves the desired speed $v_d = 22m/s$ roughly between $2s$ and $8s$, and between $13s$ and $26s$. Subfigure (b) shows the longitudinal force u_1 divided by mg (in black) and the bounds a_f, a'_f (in dotted red); it can be seen that $u_1 \in U_{acc}$. Subfigure (c) shows the value of h_{acc} (in black) and the zero-value line (in dotted red); it can be seen that h_{acc} is always positive as desired. Subfigure (d) shows the value of $D - \tau_d v_f - D_0$ (in black) and the zero-value line (in dotted red); it can be seen that $D - \tau_d v_f - D_0$ is always non-negative, which implies satisfaction of the hard constraint (18). Subfigure (e) shows the steering angle u_2 (in black) and the bound $\hat{\delta}_f, -\hat{\delta}_f$ (in dotted red); it can be seen that $u_2 \in U_{lk}$. Subfigure (f) shows the value of h_{lk} (in black) and the zero-value line (in dotted red); it can be seen that h_{lk} is always positive as desired. Subfigure (g) shows the yaw rate r (in black), the desired yaw rate d (in blue) and the bound $d_{max}, -d_{max}$ (in dotted red) for d ; it can be seen that r tracks the desired yaw rate d , which implies satisfaction of the soft constraint (17). Subfigure (h) shows the lateral acceleration $\dot{\nu}$ (in black) and its bound $\dot{\nu}_{max}$ (in dotted red). Subfigures (i)-(l) show the evolution of \mathbf{x}_2 (in black) and their respective bounds (in dotted red); it can be seen that $y, \nu, \Delta\psi, r$ are within their bounds, respectively.

VII. CONCLUSIONS

In this paper, we developed a control approach with correctness guarantees for the simultaneous operation of lane keeping and adaptive cruise control, where the longitudinal force and steering angle are generated by solving quadratic programs that guarantee safety of the closed-loop system through CBFs, and relaxes control Lyapunov-based performance objectives when they conflict with safety. The form of the QP used in the solution is known in closed form, and thus the proposed algorithm can be implemented without online optimization.

The SOS algorithm used to construct CBFs for the lane keeping is quite general and can be applied to other safety control problems as well. The assume-guarantee formalism is well adapted to modularity of the driver assistance modules studied in this paper because any control laws respecting the contracts given for lane keeping and adaptive cruise control,

respectively, will guarantee safety of the closed-loop system when the two modules are activated simultaneously. This means in particular that the individual modules do not have to be provided by the same supplier as long as an OEM provides the correct contract.

REFERENCES

- [1] M. Campbell, M. Egerstedt, J. P. How, and R. M. Murray, “Autonomous driving in urban environments: approaches, lessons and challenges,” *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 368, no. 1928, pp. 4649–4672, 2010.
- [2] C. Urmsion, J. Anhalt, D. Bagnell, C. Baker, R. Bittner, M. Clark, J. Dolan, D. Duggins, T. Galatali, C. Geyer *et al.*, “Autonomous driving in urban environments: Boss and the urban challenge,” *Journal of Field Robotics*, vol. 25, no. 8, pp. 425–466, 2008.
- [3] P. A. Ioannou and C.-C. C. Chien, “Autonomous intelligent cruise control,” *Vehicular Technology, IEEE Transactions on*, vol. 42, no. 4, pp. 657–672, 1993.
- [4] M. A. Goodrich and E. R. Boer, “Model-based human-centered task automation: a case study in ACC system design,” *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 33, no. 3, pp. 325–336, 2003.
- [5] E. J. Rossetter and C. J. Gerdes, “Lyapunov based performance guarantees for the potential field lane-keeping assistance system,” *Journal of Dynamic Systems, Measurement, and Control*, vol. 128, no. 3, pp. 510–522, 2006.
- [6] K. L. Talvala, K. Kritayakirana, and J. C. Gerdes, “Pushing the limits: From lanekeeping to autonomous racing,” *Annual Reviews in Control*, vol. 35, no. 1, pp. 137–148, 2011.
- [7] T. Pilutti and A. G. Ulsoy, “Identification of driver state for lane-keeping tasks,” *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 29, no. 5, pp. 486–502, 1999.
- [8] A. Kesting, M. Treiber, M. Schönhof, and D. Helbing, “Adaptive cruise control design for active congestion avoidance,” *Transp Res.-C: Emerging Technologies*, vol. 16, no. 6, pp. 668–683, 2008.
- [9] S. Li, K. Li, R. Rajamani, and J. Wang, “Model predictive multi-objective vehicular adaptive cruise control,” *Control Systems Technology, IEEE Transactions on*, vol. 19, no. 3, pp. 556–566, 2011.
- [10] “National Highway Traffic Safety Administration (NHTSA),” 2014. [Online]. Available: <http://www.nhtsa.gov>
- [11] M. Asplund, A. Manzoor, M. Bourouche, S. Clarke, and V. Cahill, “A formal approach to autonomous vehicle coordination,” in *FM 2012: Formal Methods*. Springer, 2012, pp. 52–67.
- [12] S. A. Seshia, D. Sadigh, and S. S. Sastry, “Formal methods for semi-autonomous driving,” in *Proceedings of the 52nd Annual Design Automation Conference*. ACM, 2015, pp. 148:1–148:5.
- [13] S. M. Loos, A. Platzer, and L. Nistor, “Adaptive cruise control: Hybrid, distributed, and now formally verified,” in *FM 2011: Formal Methods*. Springer, 2011, pp. 42–56.
- [14] O. Stursberg, A. Fehnker, Z. Han, and B. H. Krogh, “Verification of a cruise control system using counterexample-guided search,” *Control Eng. Pract.*, vol. 12, no. 10, pp. 1269–1278, 2004.
- [15] J. Guldner, H.-S. Tan, and S. Patwardhan, “Analysis of automatic steering control for highway vehicles with look-down lateral reference systems,” *Vehicle System Dynamics*, vol. 26, no. 4, pp. 243–269, 1996.
- [16] Y. S. Son, W. Kim, S.-H. Lee, and C. C. Chung, “Robust multirate control scheme with predictive virtual lanes for lane-keeping system of autonomous highway driving,” *Vehicular Technology, IEEE Transactions on*, vol. 64, no. 8, pp. 3378–3391, 2015.
- [17] K. L. R. Talvala and C. J. Gerdes, “Lanekeeping at the limits of handling: Stability via Lyapunov functions and a comparison with stability control,” in *ASME Dynamic Systems and Control Conference*, 2008, pp. 361–368.
- [18] 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 Transactions on Control Systems Technology*, vol. 24, no. 4, pp. 1294–1307, 2016.
- [19] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, “Taming dr. frankenstein: Contract-based design for cyber-physical systems,” *European journal of control*, vol. 18, no. 3, pp. 217–238, 2012.
- [20] L. Benvenuti, A. Ferrari, E. Mazzi, and A. S. Vincentelli, “Contract-based design for computation and verification of a closed-loop hybrid system,” in *Hybrid Systems: Computation and Control*. Springer, 2008, pp. 58–71.

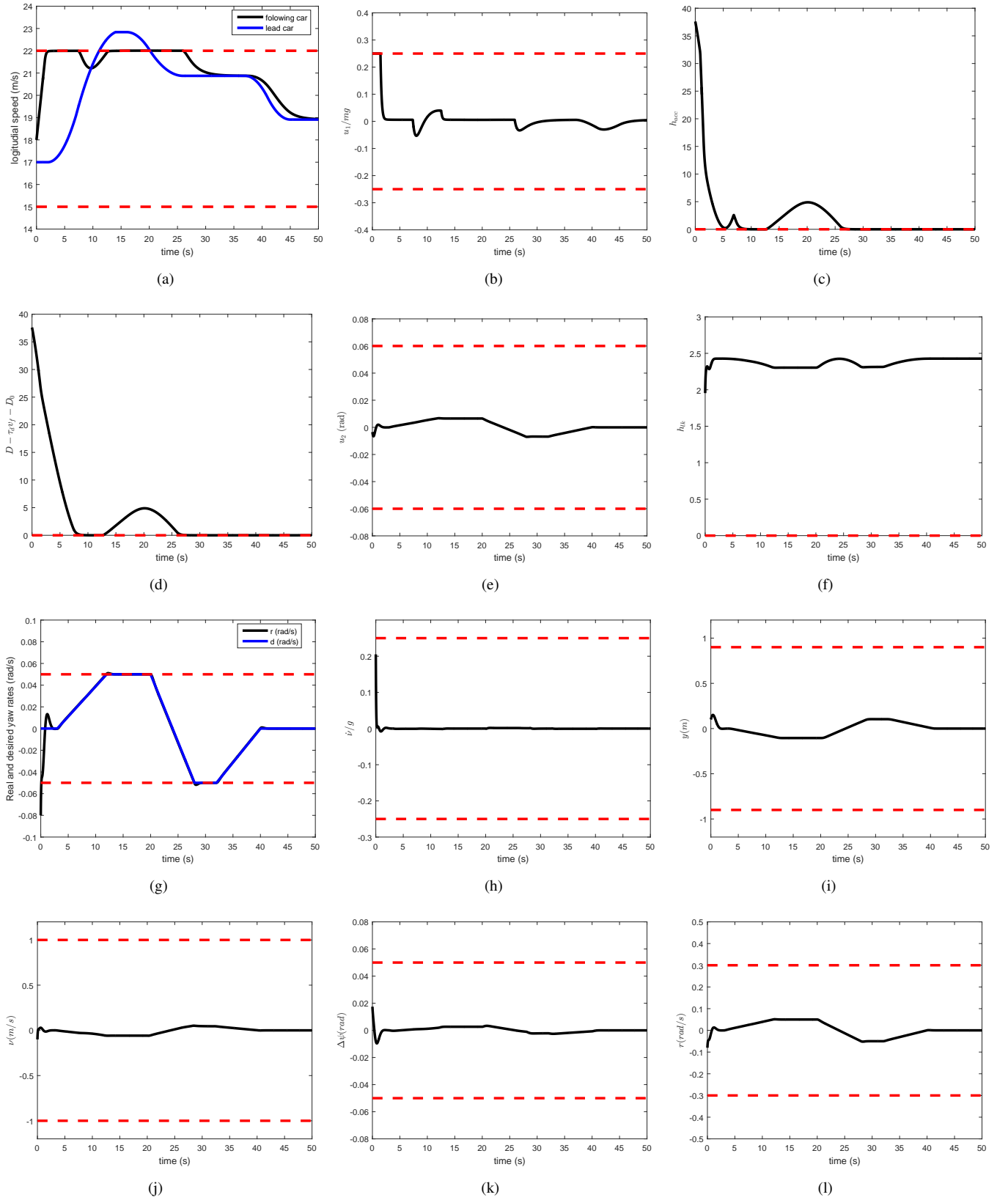


Fig. 2. (a) Speed of the controlled car v_f and the lead car v_l are shown in black and blue, respectively, and the desired speed v_d and the lower speed bound \underline{v} are shown in dotted red. The following car achieves v_d roughly between 2s and 8s, and between 13s and 26s, which implies the soft constraint (19). (b) Longitudinal force u_1 divided by mg is shown in black with its bound ± 0.25 in dotted red. (c) CBF h_{acc} is shown in black and the zero-value line in dotted red. (d) The value of $D - \tau_d v_f - D_0$ is shown in black, which is non-positive and implies satisfaction of the hard constraint (18). (e) The steering angle u_2 is shown in black with its bounded ± 0.06 in dotted red. (f) CBF h_{lk} is shown in black and the zero-value line in dotted red. (g) The yaw rate r is shown in black and the desired yaw rate d in blue, where tracking is achieved and implies soft constraint (17). (h) The lateral acceleration $\dot{\nu}$ is shown in black with its bound $\pm 0.25g$ in dotted red. (i)-(l) The values of $y, \nu, \Delta\psi, r$ are shown in black with their respective bounds $y_{\max} = 0.9, \nu_{\max} = 1, \Delta\psi_{\max} = 0.05$ and $r_{\max} = 0.3$ shown in dotted red, which imply the hard constraints (15), (16).

- [21] P. Nuzzo, H. Xu, N. Ozay, J. B. Finn, A. L. Sangiovanni-Vincentelli, R. M. Murray, A. Donz , and S. A. Seshia, "A contract-based methodology for aircraft electric power system design," *Access, IEEE*, vol. 2, pp. 1–25, 2014.
- [22] E. S. Kim, M. Arcak, and S. A. Seshia, "Compositional controller synthesis for vehicular traffic networks," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 6165–6171.
- [23] S. Dai and X. Koutsoukos, "Safety analysis of automotive control systems using multi-modal port-hamiltonian systems," in *19th ACM International Conference on Hybrid Systems: Computation and Control*, 2016.
- [24] S. Smith, P. Nilsson, and N. Ozay, "Interdependence quantification for compositional control synthesis: An application in vehicle safety systems," in *IEEE CDC*, 2016 (to appear).
- [25] J. Mareczek, M. Buss, and M. W. Spong, "Invariance control for a class of cascade nonlinear systems," *Automatic Control, IEEE Transactions on*, vol. 47, no. 4, pp. 636–640, 2002.
- [26] J. Wolff and M. Buss, "Invariance control design for constrained nonlinear systems," in *Proceedings of the 16th IFAC World Congress*. Elsevier, 2005, pp. 37–42.
- [27] I. Kolmanovsky, E. Garone, and S. Di Cairano, "Reference and command governors: A tutorial on their theory and automotive applications," in *American Control Conference*. IEEE, 2014, pp. 226–241.
- [28] D. Hoehener, G. Huang, and D. D. Vecchio, "Lane departure assist: A formal approach," in *preprint*.
- [29] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems: Computation and Control*, 2004, pp. 477–492.
- [30] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *Automatic Control, IEEE Transactions on*, vol. 52, no. 8, pp. 1415–1428, 2007.
- [31] A. D. Ames, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *53rd IEEE Conference on Decision and Control*. IEEE, 2014, pp. 6271–6278.
- [32] X. Xu, P. Tabuada, A. D. Ames, and J. W. Grizzle, "Robustness of control barrier functions for safety critical control," in *IFAC Conference on Analysis and Design of Hybrid Systems*, 2015, pp. 54–61.
- [33] A. Mehra, W.-L. Ma, F. Berg, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Adaptive cruise control: Experimental validation of advanced controllers on scale-model cars," in *American Control Conference*, 2015.
- [34] U. Borrmann, L. Wang, A. D. Ames, and M. Egerstedt, "Control barrier certificates for safe swarm behavior," *IFAC-PapersOnLine*, vol. 48, no. 27, pp. 68–73, 2015.
- [35] S.-C. Hsu, X. Xu, and A. D. Ames, "Control barrier function based quadratic programs with application to bipedal robotic walking," in *American Control Conference*. IEEE, 2015, pp. 4542–4548.
- [36] Q. Nguyen and K. Sreenath, "Exponential control barrier functions for enforcing high relative-degree safety-critical constraints," in *American Control Conference*, 2016.
- [37] P. A. Parrilo, "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization," Ph.D. dissertation, Citeseer, 2000.
- [38] R. Tedrake, I. R. Manchester, M. Tobenkin, and J. W. Roberts, "Lqr-trees: Feedback motion planning via sums-of-squares verification," *The International Journal of Robotics Research*, vol. 29, no. 8, pp. 1038–1052, 2010.
- [39] A. Majumdar, A. A. Ahmadi, and R. Tedrake, "Control design along trajectories with sums of squares programming," in *Robotics and Automation (ICRA), 2013 IEEE International Conference on*. IEEE, 2013, pp. 4054–4061.
- [40] R. Rajamani, *Vehicle dynamics and control*. Springer Science & Business Media, 2011.
- [41] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to automotive safety systems," preprint.
- [42] K. Vogel, "A comparison of headway and time to collision as safety indicators," *Accident Analysis & Prevention*, vol. 35, no. 3, pp. 427 – 433, 2003.
- [43] J. Anderson and A. Papachristodoulou, "Robust nonlinear stability and performance analysis of an F/A-18 aircraft model using sum of squares programming," *International Journal of Robust and Nonlinear Control*, vol. 23, no. 10, pp. 1099–1114, 2013.
- [44] W. Tan, "Nonlinear control analysis and synthesis using sum of squares programming," Ph.D. dissertation, University of California, Berkeley, 2006.
- [45] W. Tan and A. Packard, "Searching for control lyapunov functions using sums of squares programming," in *Allerton conference on communication, control and computing*, 2004, pp. 210–219.
- [46] "Supplemental material," <http://web.eecs.umich.edu/~grizzle/CBF>.
- [47] A. D. Ames, K. Galloway, J. W. Grizzle, and K. Sreenath, "Rapidly Exponentially Stabilizing Control Lyapunov Functions and Hybrid Zero Dynamics," *IEEE Transactions on Automatic Control*, vol. 59, no. 4, pp. 115–1130, 2014.
- [48] R. A. Freeman and P. V. Kokotovic, "Inverse optimality in robust stabilization," *SIAM Journal on Control and Optimization*, vol. 34, no. 4, pp. 1365–1391, 1996.
- [49] "Michigan department of transportation, road design manual, chapter 3." [Online]. Available: <http://mdotcf.state.mi.us/public/design/roadmanual/>