2018 Annual American Control Conference (ACC)
June 27–29, 2018. Wisconsin Center, Milwaukee, USA

Permissive Barrier Certificates for Safe Stabilization Using Sum-of-squares *

Li Wang, Dongkun Han, and Magnus Egerstedt†

***Abstract*— Motivated by the need to simultaneously guarantee safety and stability of safety-critical dynamical systems, we construct permissive barrier certificates in this paper that explicitly maximize the region where the system can be stabilized without violating safety constraints. An iterative search algorithm is developed to search for the maximum volume barrier certified region of safe stabilization. The barrier certified region, which is allowed to take any arbitrary shape, is proved to be strictly larger than safe regions generated with Lyapunov sublevel set based methods. The proposed approach effectively unites a Lyapunov function with multiple barrier functions that might not be compatible with each other. Simulation results of the iterative search algorithm demonstrate the effectiveness of the proposed method.**

I. INTRODUCTION

The controller design of safety critical dynamical systems, such as power systems, autonomous vehicles, industrial robots, and chemical reactors, requires simultaneous satisfaction of performance specifications and multiple safety constraints [2], [15], [4]. Violation of safety constraints might result in system failures and injuries. The problem of safe stabilization, i.e., to stabilize the system while staying in a given safe set, poses a challenge to the controller design task.

The formal design for stabilization of nonlinear dynamical systems is oftentimes achieved using Control Lyapunov Functions (CLFs). Meanwhile, the safety of dynamical systems can be established with barrier certificates, which guarantee that the state of the system never enters specified unsafe regions [12]. Barrier certificates are useful tools for safety verification in autonomous dynamical systems, see [12], [16], and references therein. While in control dynamical systems, barrier certificates can provably enforce dynamical safety constraints in various applications [24], [20], [21]. Since the safety and stabilization objectives might be in conflict, a common control that satisfies both objectives does not necessarily exist [14], [23].

In order to simultaneously achieve safety and stabilization of dynamical systems, a number of control design methods have been proposed in the literature to unite CLF with barrier certificates. For example, a barrier function was explicitly incorporated into the design phase of the CLF [17], [14], which resulted in a "control Lyapunov barrier function". However, no feedback controller can be designed if these two objectives were in conflict. The condition for multiple barrier constraints to be compatible with each other was characterized in [23], [20]. To deal with conflicting safety and stabilization objectives, an optimization based controller was developed in [1] such that safety is strictly guaranteed while convergence to goal is relaxed when conflict occurs.

In contrast to the aforementioned methods, this paper deals with the conflict between the safety and stabilization objectives by finding a region of safe stabilization, which is both contractive to the equilibrium and safe with respect to state constraints. Since it is often not easy to obtain the exact region of safe stabilization for arbitrary dynamics, a good approximation algorithm to compute the region of safe stabilization is required. For instance, safe stabilization funnels were designed to be sublevel sets of the Lyapunov function in [8]. In this paper, we will present an approximation algorithm based on barrier certificates, which generates an estimate of the region that is strictly larger than the estimate based on Lyapunov sublevel set. In contrast to [1], [24], no relaxation on the Lyapunov constraint is needed when it is united with the permissive barrier certificates, because the certificates and the Lyapunov constraint are always compatible by construction.

Estimating the region of safe stabilization is closely related to estimating the Domain of Attraction (DoA) of an equilibrium state, except for the extra consideration of safety constraints. Among the various DoA approximation methods proposed in the literature, methods using the subset of Lyapunov-like functions, such as quadratic Lyapunov functions [18] and rational polynomial Lyapunov functions [3], are proved to be effective [11]. Further improvements on the Lyapunov sublevel set based methods are developed in [6], [19], [5] to reduce the conservativeness with invariant sets. In this paper, the set invariance property is established with barrier certificates, which are allowed to take arbitrary shapes rather than the sublevel set of the Lypapunov function.

The contribution of this paper is threefold. First, permissive barrier certificates that are guaranteed compatible with the Lyapunov function are synthesized to ensure simultaneous stabilization and safety enforcement of control dynamical systems. Second, iterative search algorithms to compute the maximum barrier certified region of safe stabilization are developed based on sum-of-squares (SOS) programs. Third, barrier certificates are used to construct a non-conservative estimate of DoA that takes arbitrary shapes.

*The work by the first and third authors was sponsored by Grant No. N0014-15-1-2115 from the U.S. Office for Naval Research, and the work of the second author was sponsored by the NASA Grant NNX16AH81A.

†Li Wang and Magnus Egerstedt are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA, Email: {liwang, magnus}@gatech.edu. Dongkun Han is with the Department of Aerospace Engineering, University of Michigan, 1320 Beal Ave, Ann Arbor, MI 48109, USA. Email: dongkunh@umich.edu.

978-1-5386-5428-6/$31.00 ©2018 AACC

II. Preliminaries: Barrier Certificates for Dynamical Systems

Preliminary results on barrier certificates are revisited here to set the stage for DoA estimation and safe stabilization. More specifically, applications of barrier certificates in safety verification of autonomous systems and safe controller synthesis for control dynamical systems will be discussed.

A. Barrier Certificates for Autonomous Dynamical Systems

Using the invariant set principle, barrier certificates can certify that state trajectories starting from an initial set $\mathscr{X}_0$ do not enter an unsafe set $\mathscr{X}_u$. Consider an autonomous system

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

where $x \in \mathscr{X}$, and f is locally Lipschitz continuous. The barrier certificate [12], $h(x) : \mathbb{R}^n \to \mathbb{R}$, needs to satisfy

$$\frac{\partial h(x)}{\partial x} f(x) \geq 0, \forall x \in \mathscr{X}, \tag{2}$$

where $h(x)$ is non-negative in $\mathscr{X}_0$ and negative in $\mathscr{X}_u$, so that the safety of the system is guaranteed.

The condition (2) is often too restrictive, since $h(x)$ has to be non-decreasing. A more permissive barrier certificate is presented in [1], [24]. The condition (2) can be relaxed to

$$\frac{\partial h(x)}{\partial x} f(x) \geq -\kappa(h(x)), \forall x \in \mathscr{X}, \tag{3}$$

where $\kappa : \mathbb{R} \to \mathbb{R}$ is an extended class-κ function (strictly increasing and $\kappa(0) = 0$). Let the certified safe area be defined as $\mathscr{C} = \{x \in \mathscr{X} \mid h(x) \geq 0\}$. By allowing the derivative of the barrier certificate to grow within the safe set $\mathscr{C}$, this barrier certificate can ensure the forward invariance of $\mathscr{C}$ in a non-conservative manner.

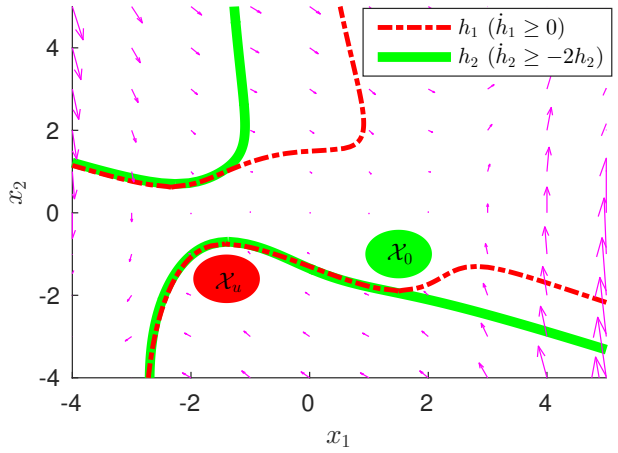

Fig. 1: Comparison of two types of barrier certificates. The barrier certified safe region based on (3) (area between the solid green lines) is significantly larger than the safe region based on (2) (area between the dashed red lines).

The difference between these two types of barrier certificates can be illustrated with a simple example. Consider a 2D autonomous dynamical system,

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ -x_1 + \frac{1}{3}x_1^3 - x_2 \end{bmatrix}.$$

The initial and unsafe sets are specified as $\mathscr{X}_0 = \{x \mid 0.25 - (x_1 - 1.5)^2 - (x_2 + 1)^2 \geq 0\}$ and $\mathscr{X}_u = \{x \mid 0.25 - (x_1 + 1.4)^2 - (x_2 + 1.6)^2 \geq 0\}$, respectively. Both types of barrier certificates are computed using the SOS technique in [12] and illustrated in Fig. 1. The area of the barrier certified safe region generated with (3) is much larger than (2), which means that (3) allows for a significantly more permissive safety certificate than (2).

B. Barrier Certificates for Control Dynamical Systems

For a control-affine dynamical system

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

where $x \in \mathscr{X}$ and $u \in U$ are the state and control of the system, and f and g are both locally Lipschitz continuous.

Barrier certificate can be designed to regulate the controller u, such that the safety constraint is never violated. The barrier certificate for control system is designed with control barrier functions (CBF). The function $h(x)$ is a CBF, if there exists an extended class-κ function κ such that

$$\sup_{u \in U} \left\{ \frac{\partial h(x)}{\partial x} f(x) + \frac{\partial h(x)}{\partial x} g(x)u + \kappa(h(x)) \right\} \geq 0, \forall x \in \mathscr{X}.$$

With $h(x)$, barrier certificates for (4) are defined as

$$K(x) = \left\{ u \in U \;\middle|\; \frac{\partial h(x)}{\partial x} f(x) + \frac{\partial h(x)}{\partial x} g(x)u + \kappa(h(x)) \geq 0 \right\}.$$

By constraining the controller u in $K(x)$, the state trajectory will never leave the safe set $\mathscr{C}$ [1], [24].

Let the stabilization objective be encoded in a control Lyapunov function (CLF) $V(x)$. Since a common control that satisfies both the CBF and the CLF does not necessarily exist, a typical way to unite the pre-designed CLF and CBF is to use a QP-based controller [24], [1], [9], i.e.,

$$\begin{aligned} u^* \quad &= \operatorname*{argmin}_{u \in \mathbb{R}^n} J(u) + k_\delta \delta^2 \\ \text{s.t.} \quad &\frac{\partial V(x)}{\partial x} g(x)u \leq -\frac{\partial V(x)}{\partial x} f(x) + \delta, \\ &-\frac{\partial h(x)}{\partial x} g(x)u \leq \frac{\partial h(x)}{\partial x} f(x) + \kappa(h(x)), \end{aligned} \tag{5}$$

where δ is a relaxation factor, such that the non-negotiable safety constraint is always satisfied by relaxing the CLF. In this paper, instead of relaxing the stabilization term, we will compute an estimate of the region of safe stabilization with permissive barrier certificates, such that both the stabilization and safety constraints are strictly respected.

III. DoA Estimation with Barrier Certificates for Autonomous Dynamical Systems

Computing estimates of the region of safe stabilization is closely related to computing estimates of DoA, because both try to maximize the volume of interested region subject to certain matrix inequalities. We will show that the DoA estimate derived with barrier certificates is strictly larger than the maximum contractive Laypunov sublevel set.

A. Expanding Estimate of DoA with Barrier Certificates

Assume the system (1) is locally asymptotically stable at the origin. Let $\psi(t;x_0)$ denote the state trajectory of the system (1) starting from x_0. The DoA of the origin is defined as the set of all initial states which eventually converge to the origin as time goes to infinity,

$$\mathscr{D} = \{x_0 \in \mathscr{X} \mid \lim_{t\to\infty} \psi(t;x_0) = 0\}.$$

A commonly used method to estimate the DoA is to compute the sublevel set of a given Lyapunov function $V(x)$. Let $\mathscr{V}(c) = \{x \in \mathscr{X} \mid V(x) \le c\}$ be a sublevel set of $V(x)$. The largest inner estimate of the DoA using the sublevel set of the Lyapunov function can be computed with

$$\begin{aligned} c^* = \quad & \max_{c\in\mathbb{R}} \ c \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x} f(x) > 0, \quad \forall x \in \mathscr{V}(c) \setminus \{0\}. \end{aligned} \tag{6}$$

This estimate $\mathscr{V}(c^*)$ is often very conservative compared to invariant set based methods. This is because the shape of $\mathscr{V}(c^*)$ is restricted to the Lyapunov sublevel set.

Next, we will show that the estimate of DoA can be further expanded using barrier certificates and the given Lyapunov function. This is achieved by allowing the barrier certificates to take an arbitrary shape instead of the sublevel set of $V(x)$. The most permissive barrier certified region $\mathscr{C}$ is

$$\begin{aligned} h^*(x) = \operatorname*{argmax}_{h(x)\in\mathscr{P}} \quad & \mu(\mathscr{C}) \\ \text{s.t.} \ -\frac{\partial V(x)}{\partial x} f(x) > 0, \quad & \forall x \in \mathscr{C} \setminus \{0\}, \\ \frac{\partial h(x)}{\partial x} f(x) \ge -\kappa(h(x)), \quad & \forall x \in \mathscr{C}, \end{aligned} \tag{7}$$

where $\mu(\mathscr{C})$ is the volume of $\mathscr{C}$. The largest estimate of the DoA with barrier certificates is achieved with $\mathscr{C}^* = \{x \in \mathscr{X} \mid h^*(x) \ge 0\}$. By maximizing the volume of the barrier certified region, $\mathscr{C}^*$ is guaranteed to be larger than $\mathscr{V}(c^*)$.

Lemma 3.1: Given system (1) that is locally asymptotically stable at the origin, the estimate of DoA with barrier certificates is no smaller than the estimate with the sublevel set of Lyapunov function, i.e., $\mu(\mathscr{V}(c^*)) \le \mu(\mathscr{C}^*)$.

Proof: See [22]. ∎

Remark 1: With *Lemma* 3.1, (6) can be reformulated into an optimization problem similar to (7), i.e.,

$$\begin{aligned} c^* = \quad & \max_{c\in\mathbb{R}} \ c \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x} f(x) > 0, \quad && \forall x \in \mathscr{V}(c) \setminus \{0\}, \\ & \frac{\partial (c - V(x))}{\partial x} f(x) \ge -\kappa(c - V(x)), \quad && \forall x \in \mathscr{V}(c). \end{aligned}$$

We can see that (6) searches for a maximum barrier certificate with the shape of a sublevel set of $V(x)$. Since a specific shape of the certified region is not required, (7) is more permissive than (6). In addition, $h(x)$ is allowed to decrease within the estimated DoA instead of monotone increasing.

The fact that $\mathscr{C}^*$ is an inner estimate of the DoA can be established with the following theorem.

Theorem 3.2: Given an autonomous dynamical system (1) that is locally asymptotically stable at the origin, the estimate of the DoA with barrier certificates, $\mathscr{C}^*$, is a subset of the true DoA $\mathscr{D}$. And $\mathscr{C}^*$ is guaranteed to be non-empty.

Proof: See [22]. ∎

B. Iterative Search of Permissive Barrier Certificates

The optimization problem (7) is difficult to solve for general systems, since checking non-negativity is often computationally intractable [10]. However, if non-negativity constraints are relaxed to SOS constraints, (7) can be converted to a numerically efficient convex optimization problem. To this end, we restrict (1) to polynomial dynamical systems.

Let $\mathscr{P}$ be the set of polynomials for $x \in \mathbb{R}^n$. The polynomial $l(x)$ can be written in Square Matrix Representation (SMR) [2] as $Z^T(x)QZ(x)$, where $Z(x)$ is a vector of monomials, and $Q \in \mathbb{R}^{k\times k}$ is a symmetrical coefficient matrix. A polynomial function $p(x)$ is a SOS polynomial if $p(x) = \sum_{i=1}^m p_i^2(x)$ for some $p_i(x) \in \mathscr{P}$. $\mathscr{P}^{\text{SOS}}$ is the set of SOS polynomials. In SMR form, $p(x)$ has a positive semidefinite coefficient matrix $Q \succeq 0$. The trace and determinant of a square matrix $A \in \mathbb{R}^{n\times n}$ are $\text{trace}(A)$ and $\det(A)$, respectively.

To maximize the volume of $\mathscr{C}$, this objective function $\max(\text{vol}(\mathscr{C}))$ is non-convex and usually cannot be described by an explicit mathematical expression. In order to solve this issue, a typical way adopted in the literature is to approximate the volume by using $\text{trace}(Q)$, where $h(x) = Z(x)^T QZ(x)$. In this paper, we would like to maximize $\text{trace}(Q)$ to get the largest $\mathscr{C}$ similar to [2].

To deal with nonnegativity constraints over semialgebraic sets, we will introduce the Positivestellensatz (P-satz).

Lemma 3.3: ([13]) For polynomials $a_1,\ldots,a_m$, $b_1,\ldots,b_l$ and p, define a set

$$\begin{aligned} \mathscr{B} \quad = \quad & \{x \in \mathbb{R}^n : a_i(x) = 0, \ \forall i = 1,\ldots,m, \\ & b_i(x) \ge 0, \ \forall j = 1,\ldots,l\}. \end{aligned}$$

Let $\mathscr{B}$ be compact. The condition $p(x) > 0, \forall x \in \mathscr{B}$ holds if the following condition is satisfied:

$$\begin{cases} \exists r_1,\ldots,r_m \in \mathscr{P}, \ s_1,\ldots,s_l \in \mathscr{P}^{\text{SOS}}, \\ p - \sum_{i=1}^m r_i a_i - \sum_{i=1}^l s_i b_i \in \mathscr{P}^{\text{SOS}}. \end{cases}$$

This lemma provides an important perspective that any strictly positive polynomial $p(x) \in \mathscr{B}$ is actually in the cone generated by a_i and b_i. Using the Real P-satz and the SMR form of $h(x)$, (7) can be formulated into a SOS program,

$$\begin{aligned} \max_{\substack{h(x)\in\mathscr{P},\ L_1(x)\in\mathscr{P}^{\text{SOS}} \\ L_2(x)\in\mathscr{P}^{\text{SOS}}}} \quad & \text{Trace}(Q) \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x} f(x) - L_1(x)h(x) \in \mathscr{P}^{\text{SOS}}, \\ & \frac{\partial h(x)}{\partial x} f(x) + \gamma h(x) - L_2(x)h(x) \in \mathscr{P}^{\text{SOS}}, \end{aligned} \tag{8}$$

where a linear function $\kappa(x) = \gamma x$ is adopted. The SOS program (8) involves bilinear decision variables. It can be solved efficiently by splitting into several smaller SOS programs, which leads to the following iterative search algorithm.

Remark 2: Notice that (8) requires an initial value of $h(x)$ to start with. From *Lemma* 3.1, a good initial value can be picked as $\bar{h}(x) = c^* - V(x)$. This SOS program is guaranteed to generate a barrier certificate better than $\bar{h}(x)$.

Algorithm 1:

Step 1: Calculate an initial value for $h(x)$

Specify a Lyapunov function $V(x)$, and find c^* using the bilinear search method, i.e.,

$$\begin{aligned} c^* = & \max_{c\in\mathbb{R}, L(x)\in\mathscr{P}^{\mathrm{SOS}}} c \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x} f(x) - L(x)(c - V(x)) \in \mathscr{P}(x)^{\mathrm{SOS}}. \end{aligned}$$

Set the initial value for $h(x)$ as $\bar{h}(x) = c^* - V(x)$.

Step 2: Fix $h(x)$, and search for $L_1(x)$ and $L_2(x)$

Using the $h(x)$ from previous step, we can search for $L_1(x)$ and $L_2(x)$ that give the largest margin on the barrier constraint. This is achieved by solving

$$\begin{aligned} & \max_{\substack{\varepsilon\geq 0,\ L_1(x)\in\mathscr{P}^{\mathrm{SOS}} \\ L_2(x)\in\mathscr{P}^{\mathrm{SOS}}}} \varepsilon \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x} f(x) - L_1(x)h(x) \in \mathscr{P}^{\mathrm{SOS}}, \\ & \frac{\partial h(x)}{\partial x} f(x) + \gamma h(x) - L_2(x)h(x) - \varepsilon \in \mathscr{P}^{\mathrm{SOS}}. \end{aligned}$$

Step 3: Fix $L_1(x)$ and $L_2(x)$, and search for $h(x)$

Parameterize $h(x)$ in the SMR form $h(x) = Z(x)^T Q Z(x)$. With $L_1(x)$ and $L_2(x)$ from previous step, the most permissive barrier certificate is computed by maximizing the trace of Q,

$$\begin{aligned} & \max_{h(x)\in\mathscr{P}} \quad \mathrm{trace}(Q) \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x} f(x) - L_1(x)h(x) \in \mathscr{P}^{\mathrm{SOS}}, \\ & \frac{\partial h(x)}{\partial x} f(x) + \gamma h(x) - L_2(x)h(x) \in \mathscr{P}^{\mathrm{SOS}}. \end{aligned}$$

This searching process is terminated if $\mathrm{trace}(Q)$ stops increasing, otherwise go back to *Step 2*.

Remark 3: In *Step 2*, since multiple $L_1(x)$ and $L_2(x)$ available, better options of $L_1(x)$ and $L_2(x)$ can be chosen by maximizing the margin ε of the barrier constraint. This method will expand the feasible space of $h(x)$ for optimization in *Step 3* and speed up the optimization procedure.

C. Simulation Results for Autonomous Dynamical Systems

The iterative search algorithm **1** is implemented on an example of autonomous dynamical systems. In the simulation, the Matlab toolboxes SeDuMi, SMRSOFT [2], and YALMIP [7] are used for solving the semidefinite and SOS programming problems.

Example 1: Consider the three-dimensional system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -x_1 + x_2 x_3^2 \\ -x_2 \\ -x_3 \end{bmatrix},$$

a Lyapunov function can be picked as $V(x) = x_1^2 + x_2^2 + x_3^2$. The largest DoA estimate based on Lyapunov sublevel set is

$$\mathscr{A}_1 = \{x \in \mathbb{R}^3 \mid V(x) \leq 8\}.$$

With barrier certificates, the largest DoA estimate is

$$\begin{aligned} \mathscr{A}_2 = \{x \in \mathbb{R}^3 \mid h(x) = 7.9999 - 1.2828x_3^2 - 0.2850x_1^2 \\ -0.5652x_2^2 - 0.6685x_1x_2 \geq 0\}. \end{aligned}$$

The barrier certificate is restricted to the same order as $V(x)$. Both estimates of DoA are illustrated in Fig.2. With the barrier certificate, the volume of the estimated region is increased by $\frac{\mu(\mathscr{A}_2)-\mu(\mathscr{A}_1)}{\mu(\mathscr{A}_1)} = 297.4\%$.

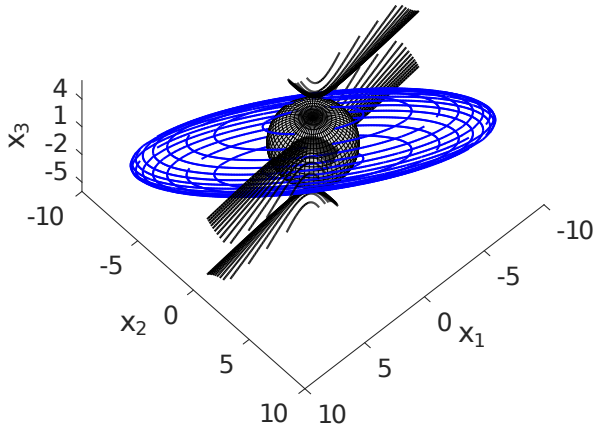

Fig. 2: Estimates of DoA for a three-dimensional autonomous dynamical system. The black and blue ellipsoids represent the largest estimate of DoA based on the Lyapunov function sublevel set and barrier certificates, respectively.

From this example, we can see that the barrier certificate based method provides a more permissive estimate of the DoA than the Lyapunov sublevel set based method.

IV. Safe Stabilization of Control Dynamical Systems

Permissive barrier certificates are developed in this section to maximize the estimated region of safe stabilization, where the system is stabilized without violating safe constraints.

We will consider the safe stabilization problem described by (5) for a locally stabilizable control-affine dynamical system (4). Note that the locally stabilizable assumption ensures that an invariant and compact set for initial DoA estimation exists. Instead of relaxing the stabilization term to resolve conflicts, we will synthesize a permissive barrier certificate with the maximum volume possible that strictly

respects both the stabilization and safety constraints,

$$\begin{aligned} h^*(x) = & \underset{h(x)\in\mathscr{P},u(x)\in\mathscr{P}}{\operatorname{argmax}} \quad \mu(\mathscr{C}) \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x}f(x)-\frac{\partial V(x)}{\partial x}g(x)u(x)>0, \quad \forall x\in\mathscr{C}\setminus\{0\}, \\ & \frac{\partial h(x)}{\partial x}f(x)+\frac{\partial h(x)}{\partial x}g(x)u(x)+\kappa(h(x))\geq 0, \quad \forall x\in\mathscr{C}, \end{aligned} \tag{9}$$

where $\mu(\mathscr{C})$ is the volume of the certified safe set $\mathscr{C}$. Note that (9) is a semi-infinite program that generates a feedback controller $u(x)$ for every $x\in\mathscr{C}$, while (5) only products a point-wise optimal controller.

To enforce the safety constraints, it is required that the barrier certified region is contained within the complement of the unsafe region, i.e., $\mathscr{C}\subseteq\mathscr{X}_u^c$. For generality, the unsafe region is encoded with multiple polynomial inequalities,

$$\mathscr{X}_u=\{x\in\mathscr{X}\mid q_i(x)<0,\ \forall i\in\mathscr{M}\}, \tag{10}$$

where $q_i(x)$ are polynomials, and $\mathscr{M}=\{1,2,...,M\}$ is the index set of all the safety constraints.

Similar to *Lemma* 3.1, we can show that the region of safe stabilization estimated with barrier certificates is larger than the estimated region with Lyapunov sublevel set in [8].

Lemma 4.1: Given a dynamical control system (4) that is locally stabilizable at the origin, the barrier certified region of safe stabilization estimate is no smaller than the estimated region of safe stabilization using sublevel set of the Lyapunov function, i.e, $\mu(\mathscr{V}(c^*))\leq\mu(\mathscr{C}^*)$.

Proof: Similar to Lemma 3.1. ∎

The barrier certificate is written in SMR form, i.e., $h(x)=Z(x)^TQZ(x)$. Using the Real P-satz, the optimization problem (9) is formulated into a SOS program,

$$\begin{aligned} & \max_{\substack{h(x)\in\mathscr{P},\ u(x)\in\mathscr{P}\\ L_1(x)\in\mathscr{P}^{\mathrm{SOS}},\ L_2(x)\in\mathscr{P}^{\mathrm{SOS}}\\ J_i(x)\in\mathscr{P}^{\mathrm{SOS}},i\in\mathscr{M}}} \quad \mathrm{Trace}(Q) \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x}(f(x)+g(x)u(x))-L_1(x)h(x)\in\mathscr{P}^{\mathrm{SOS}}, \\ & \frac{\partial h(x)}{\partial x}(f(x)+g(x)u(x))+\gamma h(x)-L_2(x)h(x)\in\mathscr{P}^{\mathrm{SOS}}, \\ & -h(x)+J_i(x)q_i(x)\in\mathscr{P}^{\mathrm{SOS}},\forall i\in\mathscr{M}. \end{aligned} \tag{11}$$

The optimal barrier certificate obtained by solving the SOS program (11) is denoted by $h^*(x)$ with the corresponding controller $u^*(x)$. The following theorem shows that safe stabilization is ensured in the barrier certified region.

Theorem 4.2: Given a dynamical control system (4) that is locally stabilizable at the origin, a Lyapunov function $V(x)$, an unsafe region $\mathscr{X}_u$ in (10), and the solution $h^*(x)$ to (11), for any initial state x_0 in $\mathscr{C}^*=\{x\in\mathscr{X}\mid h^*(x)\geq 0\}$, there always exists a controller that drives the system to the origin without violating safety constraints.

Proof: See [22]. ∎

Remark 4: With the generated permissive barrier certificates, it is guaranteed by construction that the QP-based controller (5) is always feasible when δ is set to zero. This is because $u^*(x)$ is always a feasible solution for any $x\in\mathscr{C}^*$.

The optimization problem (11) contains bilinear decision variables and requires a feasible initial barrier certificate. It can be split into several SOS programs and solved with the following iterative search algorithm.

Algorithm 2:

Step 1: Calculate an initial guess for $h(x)$

Specify a Lyapunov function $V(x)$, and find c^* using bilinear search in [8]. With the optimized c^*, set the initial guess for the barrier certificate as $\bar{h}(x)=c^*-V(x)$,

Step 2: Fix h(x), search for $u(x)$, $L_1(x)$, and $L_2(x)$

Using the $h(x)$ from previous step, we can search for feasible $u(x)$, $L_1(x)$, and $L_2(x)$, while maximizing the barrier constraint margin ε.

$$\begin{aligned} & \max_{\substack{\varepsilon\geq 0,\ u(x)\in\mathscr{P}\\ L_1(x)\in\mathscr{P}^{\mathrm{SOS}},\ L_2(x)\in\mathscr{P}^{\mathrm{SOS}}}} \quad \varepsilon \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x}(f(x)+g(x)u(x))-L_1(x)h(x)\in\mathscr{P}^{\mathrm{SOS}}, \\ & \frac{\partial h(x)}{\partial x}(f(x)+g(x)u(x))+\gamma h(x)-L_2(x)h(x)-\varepsilon\in\mathscr{P}^{\mathrm{SOS}}. \end{aligned}$$

Step 3: Fix $u(x)$, $L_1(x)$, and $L_2(x)$, search for $h(x)$

Rewrite the barrier certificate into SMR form $h(x)=Z(x)^TQZ(x)$. With the $u(x)$, $L_1(x)$, and $L_2(x)$ from the previous step, we can search for the maximum volume barrier certificate that respects all the safety constraints,

$$\begin{aligned} & \max_{\substack{h(x)\in\mathscr{P}\\ J_i(x)\in\mathscr{P}^{\mathrm{SOS}},\ i\in\mathscr{M}}} \quad \mathrm{trace}(Q) \\ \text{s.t.} \quad & -\frac{\partial V(x)}{\partial x}(f(x)+g(x)u(x))-L_1(x)h(x)\in\mathscr{P}^{\mathrm{SOS}}, \\ & \frac{\partial h(x)}{\partial x}(f(x)+g(x)u(x))+\gamma h(x)-L_2(x)h(x)\in\mathscr{P}^{\mathrm{SOS}}, \\ & -h(x)+J_i(x)q_i(x)\in\mathscr{P}^{\mathrm{SOS}},i\in\mathscr{M}. \end{aligned}$$

Terminate if trace(Q) stops increasing, otherwise go back to *Step 2*.

Remark 5: To avoid unbounded control inputs, an additional constraint can be added to limit the magnitude of the coefficients of the polynomial controller $u(x)$.

This iterative search algorithm is implemented on a control dynamical systems to achieve safe stabilization.

Example 2: Consider the three-dimensional system with multiple inputs,

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\end{bmatrix}=\begin{bmatrix}x_2-x_3^2\\ x_3-x_1^2+u_1\\ -x_1-2x_2-x_3+x_2^3+u_2\end{bmatrix}, \tag{12}$$

where $x=[x_1,x_2,x_3]^T\in\mathbb{R}^3$ and $u=[u_1,u_2]^T\in\mathbb{R}^2$ are the state and control of the system.

A Lyapunov function for the system is picked to be

$$V(x)=5x_1^2+10x_1x_2+2x_1x_3+10x_2^2+6x_2x_3+4x_3^2.$$

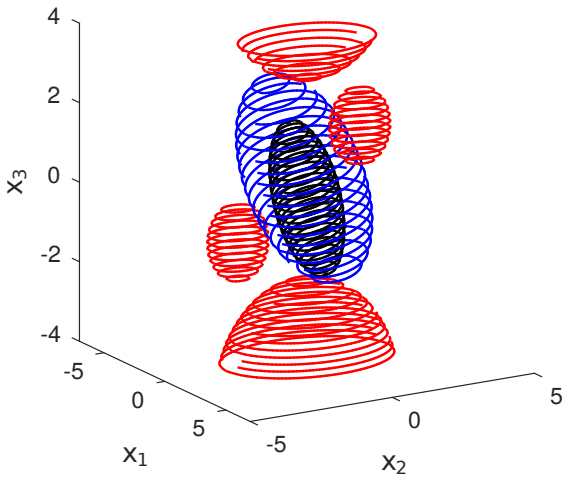

Fig. 3: Region of safe stabilization estimates for system (12). The red spheres represent unsafe regions. The barrier certified region of safe stabilization (blue ellipsoid) is significantly larger than the region (black ellipsoid) obtained with Lyapunov sublevel sets.

The unsafe region $\mathscr{X}_u = \{x \in \mathbb{R}^3 \mid q_i(x) < 0, i = 1,2,3,4\}$ is represented with polynomial inequalities

$$\begin{aligned} q_1(x) &= (x_1-2)^2+(x_2-1)^2+(x_3-2)^2-1<0,\\ q_2(x) &= (x_1+1)^2+(x_2+2)^2+(x_3+1)^2-1<0,\\ q_3(x) &= (x_1+0)^2+(x_2-0)^2+(x_3-6)^2-9<0,\\ q_4(x) &= (x_1+0)^2+(x_2+0)^2+(x_3+5)^2-9<0. \end{aligned}$$

The region of safe stabilization estimated with sublevel set of Lyapunov is

$$\mathscr{A}_1 = \{x \in \mathbb{R}^3 \mid V(x) \leq 13.0124\}.$$

Using the iterative search algorithm, the maximum permissive barrier certificate is

$$\begin{aligned} \mathscr{A}_2 = \{x \in \mathbb{R}^3 \mid h(x) &= 114.3555 + 1.4686x_1 + 7.2121x_2 \\ &+19.8479x_3 - 24.5412x_3^2 - 14.7734x_1^2 - 26.0129x_1x_2 \\ &-15.5440x_1x_3 - 28.3492x_2^2 - 27.5651x_2x_3 \geq 0\}. \end{aligned}$$

The results for region of safe stabilization estimates are shown in Fig. 3. In this example, the Lyapunov sublevel set search terminates as soon as the boundary of one safety constraint is reached, while the barrier certificate search terminates when all safety boundaries are touched. This also demonstrates the non-conservativeness of barrier certificates.

V. Conclusions

A theoretical framework to generate permissive barrier certified region of safe stabilization was developed in this paper to strictly ensure simultaneous stabilization and safety enforcement of dynamical systems. Iterative search algorithms using SOS programming techniques were designed to compute the most permissive barrier certificates. The effectiveness of the iterative search algorithm was demonstrated with simulation results.

References

[1] A. D. Ames, J. W. Grizzle, and P. Tabuada. Control Barrier Function Based Quadratic Programs with Application to Adaptive Cruise Control. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 6271–6278, Dec 2014.

[2] G. Chesi. *Domain of attraction: analysis and control via SOS programming*, volume 415. Springer Science & Business Media, 2011.

[3] G. Chesi. Rational Lyapunov functions for estimating and controlling the robust domain of attraction. *Automatica*, 49(4):1051–1057, 2013.

[4] G. Chesi and Y. S. Hung. Analysis and synthesis of nonlinear systems with uncertain initial conditions. *IEEE Transactions on Automatic Control*, 53(5):1262–1267, 2008.

[5] D. Han, A. El-Guindy, and M. Althoff. Estimating the domain of attraction based on the invariance principle. In *Decision and Control (CDC), IEEE 55th Conference on*, pages 5569–5576. IEEE, 2016.

[6] D. Henrion and M. Korda. Convex computation of the region of attraction of polynomial control systems. *IEEE Transactions on Automatic Control*, 59(2):297–312, 2014.

[7] J. Lofberg. Yalmip: A toolbox for modeling and optimization in matlab. In *Computer Aided Control Systems Design, IEEE International Symposium on*, pages 284–289. IEEE, 2005.

[8] 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*, pages 4054–4061. IEEE, 2013.

[9] Q. Nguyen and K. Sreenath. Exponential control barrier functions for enforcing high relative-degree safety-critical constraints. In *American Control Conference (ACC), 2016*, pages 322–328. IEEE, 2016.

[10] A. Papachristodoulou and S. Prajna. On the construction of lyapunov functions using the sum of squares decomposition. In *Decision and Control, 2002, Proceedings of the 41st IEEE Conference on*, volume 3, pages 3482–3487. IEEE, 2002.

[11] P. A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*. PhD thesis, California Institute of Technology, 2000.

[12] 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*, 52(8):1415–1428, 2007.

[13] M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42(3):969–984, 1993.

[14] M. Z. Romdlony and B. Jayawardhana. Uniting control lyapunov and control barrier functions. In *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, pages 2293–2298. IEEE, 2014.

[15] M. Z. Romdlony and B. Jayawardhana. Stabilization with guaranteed safety using control lyapunov–barrier function. *Automatica*, 66:39–47, 2016.

[16] C. Sloth, G. J. Pappas, and R. Wisniewski. Compositional safety analysis using barrier certificates. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, pages 15–24. ACM, 2012.

[17] K. P. Tee, S. S. Ge, and E. H. Tay. Barrier Lyapunov Functions for the Control of Output-Constrained Nonlinear Systems. *Automatica*, 45(4):918–927, 2009.

[18] B. Tibken. Estimation of the domain of attraction for polynomial systems via LMIs. In *Proceedings of the Conference on Decision and Control*, volume 4, pages 3860–3864, 2000.

[19] G. Valmorbida and J. Anderson. Region of attraction analysis via invariant sets. In *Proceedings of the American Control Conference*, pages 3591–3596, 2014.

[20] L. Wang, A. D. Ames, and M. Egerstedt. Multi-objective compositions for collision-free connectivity maintenance in teams of mobile robots. In *Decisions and Control Conference (CDC)*, pages 2659–2664, 2016.

[21] L. Wang, A. D. Ames, and M. Egerstedt. Safe certificate-based maneuvers for teams of quadrotors using differential flatness. In *IEEE International Conference on Robotics and Automation*, pages 3293–3298, 2017.

[22] L. Wang, D. Han, and M. Egerstedt. Permissive barrier certificates for safe stabilization using sum-of-squares. *arXiv preprint arXiv:1802.08917*, 2018.

[23] X. Xu. Control sharing barrier functions with application to constrained control. In *Decision and Control (CDC), 2016 IEEE 55th Conference on*, pages 4880–4885. IEEE, 2016.

[24] X. Xu, J. W. Grizzle, P. Tabuada, and A. D. Ames. Correctness guarantees for the composition of lane keeping and adaptive cruise control. *arXiv preprint arXiv:1609.06807*, 2016.