

Compositions of Multiple Control Barrier Functions Under Input Constraints

Joseph Breeden and Dimitra Panagou

Abstract—This paper presents a methodology for ensuring that the composition of multiple Control Barrier Functions (CBFs) always leads to feasible conditions on the control input, even in the presence of input constraints. In the case of a system subject to a single constraint function, there exist many methods to generate a CBF that ensures constraint satisfaction. However, when there are multiple constraint functions, the problem of finding and tuning one or more CBFs becomes more challenging, especially in the presence of input constraints. This paper addresses this challenge by providing tools to 1) decouple the design of multiple CBFs, so that a CBF can be designed for each constraint function independently of other constraints, and 2) ensure that the set composed from all the CBFs together is a viability domain. Thus, a quadratic program subject to all the CBFs simultaneously is always feasible. The utility of this methodology is then demonstrated in simulation for a nonlinear orientation control system.

I. INTRODUCTION

Control Barrier Functions (CBFs) are a control synthesis method for ensuring that system state trajectories always remain within some specified *safe set* [1]. In general, there may exist points within the safe set for which all feasible trajectories originating at these points will eventually exit the safe set. In such cases, one often seeks to construct a CBF so that a subset of the safe set, herein called the *CBF set*, is rendered forward invariant, where the CBF set is a *viability domain* (i.e. a controlled invariant set) for the given system dynamics and input bounds. The problem of finding a CBF is equivalent to the problem of finding a description for such a viability domain. This in itself is a challenging problem, but for simple safe sets, i.e. safe sets that can be described as a sublevel set of a single *constraint function*, several authors have proposed strategies to find CBFs as functions of the constraint function, including [1]–[5] among others.

One open challenge in the CBF literature is that most works assume that the viability domain is sufficiently simple to be described by the zero sublevel (or superlevel) set of a single CBF. More complex viability domains could be expressed as the intersection of the zero sublevel sets of multiple CBFs, e.g. when each CBF represents a single obstacle in a cluttered environment. This is sometimes achieved by taking a smooth [6], nonsmooth [7], or adaptive [8] maximum over several CBFs, or by simply applying multiple CBFs at once in a Quadratic Program (QP) [9], [10]. However, these approaches all assume that one is able to find

This work was supported by the National Science Foundation Graduate Research Fellowship Program and the François Xavier Bagnoud Fellowship. The authors are with the Department of Aerospace Engineering, University of Michigan, Ann Arbor, MI, USA. Email: {jbreeden, dpanagou}@umich.edu

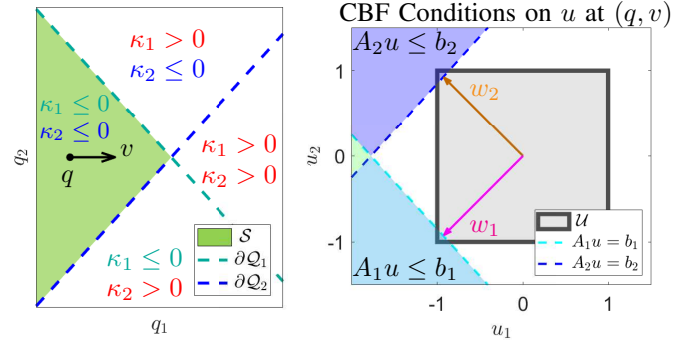


Fig. 1: Left: Visualization of the safe positions $q = (q_1, q_2) \in \mathbb{R}^2$ (green) for a double-integrator agent with two constraints κ_1, κ_2 as in Example 1. The state $x_0 = (q, v) \in \mathbb{R}^4$ in Example 1 has position q labeled above and velocity v pointing to the right. Right: Visualization of the control space at x_0 in Example 1. Both CBF conditions are individually feasible via control inputs w_1 and w_2 , but there is no $u \in \mathcal{U}$ satisfying both conditions simultaneously, so the intersection of the CBF sets is not a viability domain.

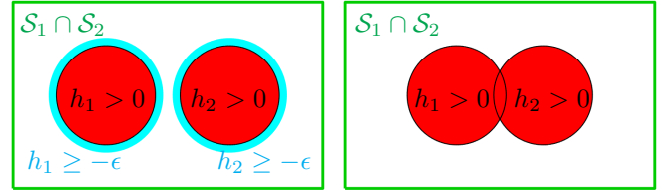


Fig. 2: Left: In [13], the problem of multi-CBF safety is simplified by assuming that $\{x \mid h_1(x) = 0\} \cap \{x \mid h_2(x) = 0\} = \emptyset$, and then designing separate safe controllers for the cases $h_1(x) \geq -\epsilon$ and $h_2(x) \geq -\epsilon$. Right: By contrast, this work is interested in the case where $\{x \mid h_1(x) = 0\} \cap \{x \mid h_2(x) = 0\} \neq \emptyset$, and thus both CBF conditions must be simultaneously satisfied, potentially resulting in conflicts such as that in Fig. 1.

a collection of CBFs whose CBF sets form a viability domain when intersected, or else the QP could become infeasible, as is illustrated by the two planar constraints in Fig. 1. Finding such a collection of CBFs is a much more challenging problem than finding a single CBF. The authors are not aware of any general algorithms analogous to [1]–[5] for finding several CBFs at once, excepting learning approaches [11], [12], which can only yield probabilistic safety guarantees.

The most common strategy to employ multiple CBFs is to assume that all the CBFs act independently of each other [13]–[15]. For example, the CBFs may apply to different states with decoupled input channels [14], [15], or it may be the case that only one CBF acts at a time [13]. The latter is equivalent to assuming that the boundaries of the individual CBF zero sublevel sets, i.e. the CBF zero level sets, do not intersect, as shown in Fig. 2. In this case, the CBFs

may be designed in a one-at-a-time fashion using existing algorithms. However, if this does not hold, then the CBFs must be designed all-at-once, or else the intersection of the CBF sets may not be a viability domain.

There exist many tools for the computation of viability domains in the control verification literature [16]–[22]. Such tools have also been used to construct CBFs [23], and have been augmented via application of CBF concepts [24]. However, all of these algorithms are computationally expensive, even for linear systems [20], [21].

Compared to prior works, this paper presents two contributions. First, we present a methodology for decoupling the design of multiple CBFs in the presence of prescribed input bounds. This decoupling allows one to leverage existing single-CBF algorithms [1]–[5] while avoiding conflicts such as those in Fig. 1. Second, we present an iterative algorithm to find a viability domain parameterized by these decoupled CBFs. That is, instead of using zonotopes, [17], [18], polytopes [19], [20], or other parameterized functions [22], [24], [25], this paper expresses viability domains in terms of an intersection of CBF sets. As each CBF forbids state trajectories from crossing the boundary of its own CBF set, our algorithm focuses on verifying Nagumo’s condition only at the states where the boundaries of multiple CBF sets intersect. One can then compute safe control actions using a quadratic program (QP) [1], [26] subject to the CBF conditions arising from every CBF, and we show that this QP is always feasible. Note that, compared to [16]–[22], the viability domains resulting from this algorithm will generally be more conservative, as our intent is to enable the use of existing (usually conservative) CBF literature rather than to approximate the maximal viability kernel.

II. PRELIMINARIES

A. Notations

Given a set \mathcal{S} , let $\partial\mathcal{S}$ denote the boundary of \mathcal{S} , and $\text{int}(\mathcal{S})$ denote the interior of \mathcal{S} . Given a function $\psi : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2}$, denoted $\psi(q, v)$, let $\nabla_q \psi(q, v)$ denote the row vector of derivatives (i.e. the gradient) of ψ with respect to inputs $q \in \mathbb{R}^{n_1}$, and let $\nabla_v \psi(q, v)$ denote the row vector of derivatives of ψ with respect to inputs $v \in \mathbb{R}^{n_2}$. Let \mathcal{C}^r denote the set of functions r -times continuously differentiable in all arguments, and \mathcal{K} the set of class- \mathcal{K} functions. Let $a \cdot b$ denote the dot product between vectors a and b . Let a^T denote the transpose of the vector a . Let $\|\cdot\|_1$, $\|\cdot\|_2$, and $\|\cdot\|_\infty$ denote the 1-norm, 2-norm, and ∞ -norm respectively. Let $[N]$ denote the set of all integers between 1 and N . Given one or more vectors $\{v_1, \dots, v_N\}$, define $\text{proj}_{\{v_1, \dots, v_N\}} u = \sum_{i \in [M]} (u \cdot \hat{b}_i) \hat{b}_i$, where $\{\hat{b}_1, \dots, \hat{b}_M\}$ is an orthonormal basis spanning $\text{span}\{v_1, \dots, v_N\}$.

B. Model

Let $q \in \mathbb{R}^{n_1}$ be the coordinates, and $v \in \mathbb{R}^{n_2}$ the velocities, of a second-order system of the form

$$\dot{q} = g_1(q)v, \quad (1a)$$

$$\dot{v} = f(q, v) + g_2(q)u, \quad (1b)$$

with state $x \triangleq (q, v) \in \mathbb{R}^{n_1+n_2}$ and control input $u \in \mathcal{U} \subseteq \mathbb{R}^m$. Let $f : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \rightarrow \mathbb{R}^{n_2}$, $g_1 : \mathbb{R}^{n_1} \rightarrow \mathbb{R}^{n_1 \times n_2}$, and $g_2 : \mathbb{R}^{n_1} \rightarrow \mathbb{R}^{n_2 \times m}$ belong to \mathcal{C}^2 . Let \mathcal{U} encode the set of allowable control inputs, herein called the *control set*, and assume that \mathcal{U} is compact and convex and contains the zero vector. Assume that f , g_1 , g_2 , and u are sufficiently regular that trajectories of (1) exist and are unique for all times $t \in \mathcal{T} = [t_0, t_f)$, where t_f is possibly ∞ . Note that the model (1) includes Euler-Lagrange systems, where $n_1 = n_2$, as in [2], [14], [27], but is also more general.

C. Safety Definitions

A principal requirement of any autonomous system should be to at all times satisfy certain operation constraints. Specifically, suppose we are given several *constraint functions* $\kappa_i : \mathbb{R}^{n_1} \rightarrow \mathbb{R}$, $\kappa_i \in \mathcal{C}^2$, $i \in [N_1]$ and $\eta_j : \mathbb{R}^{n_2} \rightarrow \mathbb{R}$, $\eta_j \in \mathcal{C}^1$, $j \in [N_2]$, which each generate a *constraint set*:

$$\mathcal{Q}_i \triangleq \{q \in \mathbb{R}^{n_1} \mid \kappa_i(q) \leq 0\}, \quad (2)$$

$$\mathcal{V}_j \triangleq \{v \in \mathbb{R}^{n_2} \mid \eta_j(v) \leq 0\}. \quad (3)$$

We call the composition of all the constraint sets the *safe set* \mathcal{S} , and say that the system is *safe* at time t if $x(t) \in \mathcal{S}$:

$$\mathcal{S} \triangleq \left(\bigcap_{i \in [N_1]} \mathcal{Q}_i \right) \times \left(\bigcap_{j \in [N_2]} \mathcal{V}_j \right). \quad (4)$$

That is, we allow for both position constraints κ_i and velocity constraints η_j , but assume that these constraints are encoded separately. This implies that each κ_i is of relative-degree 2 along (1) and each η_j is of relative-degree 1 along (1). This separation of \mathcal{Q}_i and \mathcal{V}_j is not necessary, but is greatly simplifying, as will be explained in Remark 2.

We now introduce two notions of CBF.

Definition 1. Let $\mathcal{X} \subseteq \mathcal{S}$ and $\mathcal{Y} \subseteq \mathcal{U}$. A function $h : \mathbb{R}^{n_1+n_2} \rightarrow \mathbb{R}$, $h \in \mathcal{C}^1$ is a control barrier function (CBF) for $(\mathcal{X}, \mathcal{Y})$ if there exists $\alpha \in \mathcal{K}$ such that the set

$$\boldsymbol{\mu}(q, v, \mathcal{Y}) \triangleq \{u \in \mathcal{Y} \mid \dot{h}(q, v, u) \leq \alpha(-h(q, v))\} \quad (5)$$

is nonempty for all $(q, v) \in \mathcal{H} \cap \mathcal{X}$, where

$$\mathcal{H} \triangleq \{(q, v) \in \mathbb{R}^{n_1+n_2} \mid h(q, v) \leq 0\}. \quad (6)$$

We call \mathcal{H} the CBF induced set, or simply CBF set.

Note that under the dynamics (1), \dot{h} is affine in u ,

$$\dot{h}(q, v, u) = \nabla_q h(q, v)g_1(q)v + \nabla_v h(q, v)g_2(q)u, \quad (7)$$

so if \mathcal{Y} is convex, then the set $\boldsymbol{\mu}$ in (5) is also convex.

Definition 2. Let $\mathcal{X} \subseteq \mathcal{S}$ and $\mathcal{Y} \subseteq \mathcal{U}$. A function $h : \mathbb{R}^{n_1+n_2} \rightarrow \mathbb{R}$, $h \in \mathcal{C}^1$ is a simple control barrier function (SCBF) for $(\mathcal{X}, \mathcal{Y})$ if 1) h is a CBF for $(\mathcal{X}, \mathcal{Y})$, and 2) the set

$$\boldsymbol{\mu}^s(q, v, \mathcal{Y}) \triangleq \{u \in \boldsymbol{\mu}(q, v, \mathcal{Y}) \mid \exists c \geq 0 : u = -c[\nabla_v h(q, v)g_2(q)]^T\} \quad (8)$$

is nonempty for all $(q, v) \in \mathcal{H} \cap \mathcal{X}$.

That is, h is an SCBF if the condition $\dot{h}(q, v, u) \leq \alpha(-h(q, v))$ can always be satisfied for a control input

u anti-parallel to the vector $\nabla_v h(q, v)g_2(q)$. We introduce the notion of SCBF because it allows for slightly less conservative viability domain computations, as we will show in Section III. SCBFs arise naturally in many practical applications. Note that if $\mathcal{Y} = \{u \in \mathbb{R}^m \mid \|u\|_2 \leq u_{\max}\}$, then any CBF for $(\mathcal{X}, \mathcal{Y})$ is automatically an SCBF for $(\mathcal{X}, \mathcal{Y})$ too. Next, we recall the definition of *viability domain*.

Definition 3 ([18, Eq. 7]). *A set $\mathcal{A} \subseteq \mathcal{S}$ is called a viability domain if for every point $x(t_0) \in \mathcal{A}$, there exists a control signal $u(t) \in \mathcal{U}, t \in \mathcal{T}$ such that the trajectory $x(\cdot)$ of (1) satisfies $x(t) \in \mathcal{A}$ for all $t \in \mathcal{T}$.*

Note that if 1) h is a CBF for $(\mathcal{S}, \mathcal{U})$ and 2) $\mathcal{H} \subseteq \mathcal{S}$, then it follows from Definition 1 and [1, Thm. 2] that \mathcal{H} is a viability domain. This is useful because generally \mathcal{S} in (4) is not a viability domain, but we can use CBFs to describe subsets of \mathcal{S} that are viability domains. However, in this paper, we assume that \mathcal{S} is sufficiently complex that it is difficult to find a single CBF h for which $\mathcal{H} \subseteq \mathcal{S}$, thus motivating the following extensions of [1, Thm. 2].

D. Safe Quadratic Program Control

The heart of safety-critical control is Nagumo's theorem:

Lemma 1 ([28, Thm. 3.1]). *Let $\mathcal{A} \subseteq \mathbb{R}^n$ be a closed convex set, and let $\mathcal{A}^T(x)$ be the tangent cone of \mathcal{A} at $x \in \mathbb{R}^n$. Then \mathcal{A} is forward invariant under (1) if and only if $\dot{x} \in \mathcal{A}^T(x)$ for all $x \in \mathcal{A}$.*

Note that if $x \in \text{int}(\mathcal{A})$, then $\mathcal{A}^T(x) = \mathbb{R}^n$, so Lemma 1 in effect only depends on the flow \dot{x} when $x \in \partial\mathcal{A}$. We use this fact in Lemma 3 below.

Given multiple constraint functions $\kappa_i, i \in [N_1]$ and $\eta_j, j \in [N_2]$, it is common [9], [10], [29] to construct multiple CBFs $h_k, k \in [M]$. These can then be used for safe control according to the following lemma, which follows immediately from [1, Thm. 2].

Lemma 2. *Given functions $\{h_k\}_{k \in [M]}$, with \mathcal{H}_k as in (6), denote $\mathcal{H}_{\text{all}} = \bigcap_{k \in [M]} \mathcal{H}_k$. Assume that each h_k is a CBF for $(\mathcal{H}_{\text{all}}, \mathcal{U})$. Then any control law $u : \mathbb{R}^{n_1+n_2} \rightarrow \mathcal{U}$ satisfying*

$$u(q, v) \in \boldsymbol{\mu}_{\text{all}}(q, v) \triangleq \bigcap_{k \in [M]} \boldsymbol{\mu}_k(q, v, \mathcal{U}) \quad (9)$$

for all $(q, v) \in \mathcal{H}_{\text{all}}$ will render \mathcal{H}_{all} forward invariant.

Note that Lemma 2 does not include the safe set \mathcal{S} from (4), so safety is only guaranteed if $\mathcal{H}_{\text{all}} \subseteq \mathcal{S}$. We next introduce a modified version of Lemma 2 to handle the possibility that $\mathcal{H}_{\text{all}} \not\subseteq \mathcal{S}$, as frequently occurs when using High Order CBFs (e.g. [4, Thm. 5], [5, Lemma 7]).

Lemma 3. *Given functions $\{h_k\}_{k \in [M]}$, with \mathcal{H}_k as in (6), denote $\mathcal{H}_{\text{all}} = \bigcap_{k \in [M]} \mathcal{H}_k$ and $\mathcal{A} = \mathcal{H}_{\text{all}} \cap \mathcal{S}$. Assume that each h_k is a CBF for $(\mathcal{A}, \mathcal{U})$. Let $u : \mathbb{R}^{n_1+n_2} \rightarrow \mathcal{U}$ be a control law. For every $i \in [N_1]$, $j \in [N_2]$, and all $(q, v) \in \text{int}(\mathcal{H}_{\text{all}})$, assume that $\kappa_i(q) = 0 \implies \dot{\kappa}_i(q, v) \leq 0$ and that $\eta_j(v) = 0 \implies \dot{\eta}_j(q, v, u(q, v)) \leq 0$. If u satisfies (9) for all $(q, v) \in \mathcal{A}$, then u will render \mathcal{A} forward invariant.*

Note that $\kappa_i(q) = 0 \implies \dot{\kappa}_i(q, v) \leq 0$ is equivalent to Nagumo's necessary condition in Lemma 1. Thus, Lemma 3 highlights how one purpose of the CBFs h_k is to construct a set $\mathcal{A} \subseteq \mathcal{S}$ that excludes all the states in \mathcal{S} where Nagumo's necessary condition does not hold for any $u \in \mathcal{U}$. This idea is the central motivation for the algorithm in Section III-C.

Finally, given a collection of constraints κ_i, η_j and CBFs h_k satisfying the conditions of Lemma 3, it is common to construct control laws $u : \mathbb{R}^{n_1+n_2} \rightarrow \mathcal{U}$ of the form [1, Sec. II-C]

$$u(q, v) = \arg \min_{u \in \mathcal{U}} \|u - u_{\text{nom}}(q, v)\|_2^2 \quad (10a)$$

$$\text{s.t. } \dot{h}_k(q, v, u) \leq \alpha_k(-h_k(q, v)), \forall k \in [M] \quad (10b)$$

where α_k comes from (5), u_{nom} is any control law, and (10b) is affine due to (7). If u in (10) always exists, i.e. if $\boldsymbol{\mu}_{\text{all}}$ in (9) is nonempty for all $(q, v) \in \mathcal{A}$, then it follows from Lemma 3 that the set \mathcal{A} in Lemma 3 is a viability domain. However, if there exists $(q, v) \in \mathcal{A}$ for which $\boldsymbol{\mu}_{\text{all}}(q, v)$ is empty, then trajectories originating at (q, v) might exit the safe set \mathcal{S} . Thus, the goal of this paper is to present tools to ensure that \mathcal{A} is a viability domain, so that the related controller (12) (to be introduced) is always feasible.

Problem 1. *Determine a set of CBFs $\{h_k\}_{k \in [M]}$ such that the set \mathcal{A} in Lemma 3 is a viability domain.*

E. Assumptions and Motivating Example

The principal challenge addressed in this paper is the problem of multi-CBF compositions. For this reason, we assume that the single-CBF problem is sufficiently solved.

Assumption 1. *Given sets $\mathcal{X} \subseteq \mathcal{S}$ and $\mathcal{Y} \subseteq \mathcal{U}$, focus on any single constraint function κ_i (or η_j). Denote $\mathcal{O} = \mathcal{Q}_i \times \mathbb{R}^{n_2}$ (or $\mathcal{O} = \mathbb{R}^{n_1} \times \mathcal{V}_j$). Consider the set $\mathcal{Z} = \mathcal{X} \cap (\text{int}(\mathcal{X}) \cup \partial\mathcal{O})$. Assume that there exists an algorithm (e.g. [1]–[5]) to derive one or more functions $\{h_k\}_{k=k_1}^{k_2}$, each a CBF for $(\mathcal{X}, \mathcal{Y})$, such that $\kappa_i(q) = 0 \implies \dot{\kappa}_i(q, v) \leq 0$ (or $\eta_j(v) = 0 \implies \dot{\eta}_j(q, v, u) \leq 0$) for all $(q, v) \in (\mathcal{Z} \cap (\bigcap_{k=k_1}^{k_2} \text{int}(\mathcal{H}_k)))$ and all $u \in \mathcal{U}$, where \mathcal{H}_k is as in (6). That is, for each constraint function, assume that we can find one or more CBFs that prevents state trajectories from violating that particular constraint function.*

Remark 1. *In practice, for the relative-degree 1 constraint functions η_j , we can often choose a CBF h_k so that $h_k = \eta_j$. In this case, the set $\mathcal{Z} \cap \text{int}(\mathcal{H}_k)$ in Assumption 1 has empty intersection with the set $\{(q, v) \in \mathcal{X} \mid \eta_j(v) = 0\}$, so the condition “ $\eta_j(v) = 0 \implies \dot{\eta}_j(q, v, u) \leq 0$ for all $(q, v) \in (\mathcal{Z} \cap \text{int}(\mathcal{H}_k)), u \in \mathcal{U}$ ” is automatically satisfied. Therefore, the “all $u \in \mathcal{U}$ ” part of Assumption 1 is a rarely used technicality. One only needs to check this technicality if one chooses a CBF h_k such that there exists $(q, v) \in \mathcal{H}_k$ where $\eta_j(v) > 0$. The authors are unaware of a practical example where this occurs for a relative degree 1 constraint function η_j , though such a choice of h_k is common for relative-degree 2 constraint functions κ_i , e.g. [5].*

Successive application of Assumption 1 to every constraint function one-at-a-time then produces a collection of CBFs $\{h_k\}_{k \in [M]}$ satisfying the assumptions of Lemma 3. However, this still does not imply joint feasibility of all the CBFs h_k , as we illustrate with the following example.

Example 1. Consider the 2D double integrator $\dot{q} = v, \dot{v} = u$, $q = (q_1, q_2) \in \mathbb{R}^2, v = (v_1, v_2) \in \mathbb{R}^2, u = (u_1, u_2) \in \mathcal{U} = [-1, 1] \times [-1, 1]$ subject to two constraint functions $\kappa_1(q) = q_1 + \gamma q_2$ and $\kappa_2(q) = q_1 - \gamma q_2$ for some constant $\gamma > 0$, resulting in the safe set $\mathcal{S} = (\mathcal{Q}_1 \cap \mathcal{Q}_2) \times \mathbb{R}^2$, pictured in Fig. 1. From [4], [5], one can derive CBFs h_1, h_2 for $(\mathcal{S}, \mathcal{U})$, where $h_i(q, v) = \kappa_i(q, v) - \sqrt{-2(1 + \gamma)\kappa_i(q)}$, that satisfy the conditions of Lemma 3. Denote $\mathcal{A} = \mathcal{H}_1 \cap \mathcal{H}_2 \cap \mathcal{S}$ and let $x_0 = (q, v) = (-\frac{1}{2(1+\gamma)}, 0, 1, 0) \in \partial \mathcal{A}$. Then there is no $u \in \mathcal{U}$ that renders \mathcal{A} forward invariant from x_0 (see the right side of Fig. 1). That is, Nagumo's necessary condition (Lemma 1) for forward invariance of \mathcal{A} is violated at x_0 .

III. METHODOLOGY

It is clear from Example 1 that possessing a collection of CBFs for $(\mathcal{S}, \mathcal{U})$ is not sufficient to solve Problem 1. Thus, our first strategy is to identify other control sets \mathcal{Y} , for which possessing CBFs for $(\mathcal{S}, \mathcal{Y})$ is sufficient to solve Problem 1. That is, if we restrict w_1, w_2 in Fig. 1 to a smaller set $\mathcal{Y} \subset \mathcal{U}$ when designing our CBFs, then under certain conditions, presented in Section III-A, we can ensure that several CBFs will be concurrently feasible over the full control set \mathcal{U} . When this strategy fails to yield a full solution to Problem 1, we then present a more typical iterative algorithm in Section III-C to remove the remaining infeasible states in \mathcal{S} . We also present a brief remark on QP controllers in Section III-B.

A. When All CBFs are Non-Interfering

Some properties we will need are as follows:

Definition 4. Two CBFs h_i and h_j are called non-interfering on \mathcal{X} if $(\nabla_v h_i(q, v)g_2(q)) \cdot (\nabla_v h_j(q, v)g_2(q)) \geq 0$ for all $(q, v) \in \mathcal{X}$. A collection of CBFs $\{h_k\}_{k \in [M]}$ is called non-interfering if every pair of CBFs is non-interfering.

Definition 5. Given a set $\mathcal{U}' \subset \mathcal{U}$, let $\{w_i\}_{i \in [m]}$ be a set of m vectors $w_i \in \mathcal{U}'$ satisfying $w_i \cdot w_j \geq 0, \forall i \in [m], j \in [m]$. Let $\{y_i\}_{i \in [m]}$ be the set of orthogonal projections $y_i = w_i - \text{proj}_{\{w_j\}_{j \in [i-1]}} w_i$ (or $y_i = w_i$ if $\{w_i\}_{i \in [m]}$ are orthogonal). The set \mathcal{U}' has the orthogonal extension property (OEP) with respect to \mathcal{U} if for every such set $\{w_i\}_{i \in [m]}$, the point $z = \sum_{i \in [m]} y_i$ belongs to \mathcal{U} .

Definition 6. Given a set $\mathcal{U}' \subset \mathcal{U}$, let $\{\mathcal{P}_i\}_{i \in [m]}$ be a set of m orthogonal hyperplanes in \mathbb{R}^m satisfying $\mathcal{P}_i \cap \mathcal{U}' \neq \emptyset, \forall i \in [m]$. Let p be the point where all m hyperplanes intersect (where p is guaranteed to exist because $\{\mathcal{P}_i\}_{i \in [m]}$ are orthogonal). The set \mathcal{U}' has the quadrant extension property (QEP) with respect to \mathcal{U} if for every such set $\{\mathcal{P}_i\}_{i \in [m]}$, the point p belongs to \mathcal{U} .

Examples of sets satisfying Definitions 5-6 are as follows:

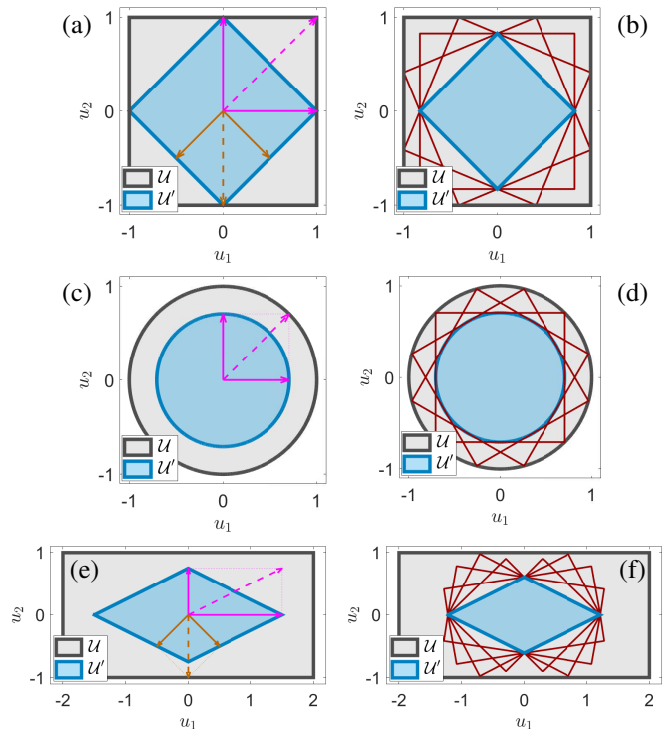


Fig. 3: Given three different control sets \mathcal{U} (gray), the above illustrates possible choices of set \mathcal{U}' (blue) that: left) have the OEP with respect to \mathcal{U} , and right) have the QEP with respect to \mathcal{U} , as in Definitions 5-6. The left plots also show how given two orthogonal vectors (solid arrows) in \mathcal{U}' , their sum (dashed arrow) must by construction belong to \mathcal{U} . The right plots also show various choices of orthogonal hyperplanes (i.e. lines in \mathbb{R}^2) whose intersections (the red right angles) by construction must belong to \mathcal{U} .

Example 2. Given various prescribed input bounds \mathcal{U} , the following sets \mathcal{U}' possess the OEP or QEP with respect to \mathcal{U} . Note that these choices of \mathcal{U}' are not unique.

- 1) If $\mathcal{U} = \{u \in \mathbb{R}^m \mid \|u\|_\infty \leq \gamma\}$, then one possible set with the OEP is $\mathcal{U}' = \{u \in \mathbb{R}^m \mid \|u\|_1 \leq \gamma\}$ (Fig. 3a). One possible set with the QEP is $\mathcal{U}' = \{u \in \mathbb{R}^m \mid \|u\|_1 \leq \gamma^*\}$ (Fig. 3b), where γ^* must be computed. If $m = 2$, then $\gamma^* = \frac{2\gamma}{1+\sqrt{2}}$.
- 2) If $\mathcal{U} = \{u \in \mathbb{R}^m \mid \|u\|_1 \leq \gamma\}$, then one possible set with the OEP is $\mathcal{U}' = \{u \in \mathbb{R}^m \mid \|u\|_\infty \leq \frac{\gamma}{m}\}$. One possible set with the QEP is $\mathcal{U}' = \{u \in \mathbb{R}^m \mid \|u\|_\infty \leq \frac{\gamma^*}{m}\}$, where γ^* is as in the prior case.
- 3) If $\mathcal{U} = \{u \in \mathbb{R}^m \mid \|u\|_2 \leq \gamma\}$, then one possible set with the OEP (Fig. 3c) and QEP (Fig. 3d) is $\mathcal{U}' = \{u \in \mathbb{R}^m \mid \|u\|_2 \leq \frac{\gamma}{\sqrt{m}}\}$.
- 4) If $\mathcal{U} = \{u \in \mathbb{R}^m \mid \max_i |a_i u_i| \leq \gamma\}$ for constants $\{a_1, \dots, a_m\}$, then one possible set with the OEP is $\mathcal{U}' = \{u \in \mathbb{R}^m \mid \sum_i |a_i u_i| \leq \gamma^*\}$ (Fig. 3e), where $\gamma^* \leq \gamma$ must be computed. A set with the QEP can be constructed similarly (Fig. 3f).

The core idea of this subsection is that given a set \mathcal{U}' with the OEP or QEP, if we design our CBFs $\{h_k\}_{k \in [M]}$ one-at-a-time for $(\mathcal{S}, \mathcal{U}')$, then, subject to an additional condition on the CBF gradients, we can guarantee a priori that $\{h_k\}_{k \in [M]}$ will have jointly feasible CBF conditions. To show this, we

begin with several lemmas about the geometry of the OEP and QEP, first for two constraints, and then for M constraints.

Lemma 4. *Let \mathcal{U}' have the OEP with respect to \mathcal{U} . Given two row vectors $A_1, A_2 \in \mathbb{R}^{1 \times m}$ and two scalars $b_1, b_2 \in \mathbb{R}$, if $A_1 \cdot A_2 \geq 0$ and there exists $w_1, w_2 \in \mathcal{U}'$ such that 1) $A_1 w_1 \leq b_1$, 2) $A_2 w_2 \leq b_2$, 3) $A_1 \cdot w_1 = -\|A_1\|_2 \|w_1\|_2$, and 4) $A_2 \cdot w_2 = -\|A_2\|_2 \|w_2\|_2$, then there exists $z \in \mathcal{U}$ such that $A_1 z \leq b_1$ and $A_2 z \leq b_2$.*

Proof. Note that conditions 3 and 4 imply that either 1) w_1 is parallel and opposite to A_1 when $b_1 < 0$, or 2) that $w_1 = 0$ when $b_1 \geq 0$, and similarly for A_2, b_2, w_2 . Without loss of generality, assume that $\|w_1\|_2 \geq \|w_2\|_2$. Let $w^* = w_2 - \frac{w_2 \cdot w_1}{w_1 \cdot w_1} w_1$. Then $z = w_1 + w^*$ satisfies $A_1 z = A_1 w_1 \leq b_1$ since w^* is orthogonal to w_1 and A_1 , and

$$A_2 z = A_2 w_2 + \underbrace{A_2 w_1}_{\leq 0} \left(1 - \underbrace{\frac{w_2 \cdot w_1}{w_1 \cdot w_1}}_{\leq 1}\right) \leq A_2 w_2 \leq b_2.$$

By the OEP, $z \in \mathcal{U}$. ■

Lemma 5. *Let \mathcal{U}' have the OEP with respect to \mathcal{U} . Given M row vectors $\{A_k\}_{k \in [M]}$ and scalars $\{b_k\}_{k \in [M]}$ with $A_k \in \mathbb{R}^{1 \times m}$, if 1) $A_i \cdot A_j \geq 0$ for all $i \in [M], j \in [M]$, 2) there exists $w_k \in \mathcal{U}'$ such that $A_k w_k \leq b_k$ for all $k \in [M]$, and 3) $A_k w_k = -\|A_k\|_2 \|w_k\|_2$ for all $k \in [M]$, then there exists $z \in \mathcal{U}$ such that $A_k z \leq b_k$ for all $k \in [M]$.*

Proof. The proof follows from that of Lemma 4. Assume that the vectors are ordered by decreasing $\|w_k\|_2$. If $M \leq m$, then use orthogonal projections to construct a vector $z = \sum_{i \in [M]} (w_i - \text{proj}_{\{w_j\}_{j \in [i-1]}} w_i)$ that satisfies all M constraints $A_k z \leq b_k$ simultaneously. By the OEP, $z \in \mathcal{U}$. If $M > m$, then because $A_i \cdot A_j \geq 0$ for all i, j , the set $\mathcal{W} = \{u \in \mathbb{R}^m \mid A_k u \leq b_k, \forall k \in [M]\}$ must contain a complete orthant $\mathbb{O} = \{u \in \mathbb{R}^m \mid O_k u \leq O_k y, \forall k \in [m]\} \subseteq \mathcal{W}$ for some orthogonal set $\{O_k\}_{k \in [m]}$, $O_k \in \mathbb{R}^{1 \times m}$ and some point $y \in \mathbb{R}^m$. Therefore, at least $l_0 = M - m$ of the constraints $A_k z \leq b_k$ must be redundant, i.e. $l \geq l_0$ of the constraints must be automatically satisfied if the remaining constraints are satisfied. Use the remaining $M - l$ constraints as in the prior case to construct a vector $z \in \mathcal{U}$ satisfying all M inequalities simultaneously. ■

Lemma 6. *Let \mathcal{U}' have the QEP with respect to \mathcal{U} . Given two row vectors $A_1, A_2 \in \mathbb{R}^{1 \times m}$ and two scalars $b_1, b_2 \in \mathbb{R}$, if $A_1 \cdot A_2 \geq 0$ and there exists $w_1, w_2 \in \mathcal{U}'$ such that $A_1 w_1 \leq b_1$ and $A_2 w_2 \leq b_2$, then there exists $p \in \mathcal{U}$ such that $A_1 p \leq b_1$ and $A_2 p \leq b_2$.*

Proof. Consider the following figure:

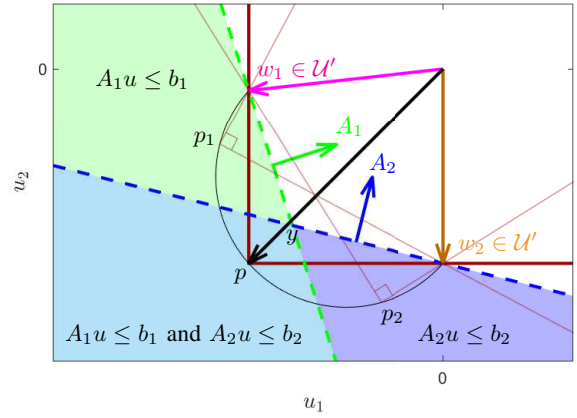


Fig. 4: Visualization for Lemma 6 proof.

Since $w_1, w_2 \in \mathcal{U}'$, by the QEP, any two orthogonal lines (i.e. hyperplanes in \mathbb{R}^2) that intersect w_1 and w_2 (i.e. intersect points in \mathcal{U}') must meet at a point in \mathcal{U} , such as the points p, p_1, p_2 above. That is, every point on the black arc must belong to \mathcal{U} . Next, since $A_1 \cdot A_2$ is at least zero, the point y where the hyperplanes $\{u \mid A_1 u = b_1\}$ and $\{u \mid A_2 u = b_2\}$ (dashed lines) intersect must be enclosed by the black arc. It follows that at least one point, above labeled p , on this arc must satisfy both inequalities simultaneously. ■

Lemma 7. *Let \mathcal{U}' have the QEP with respect to \mathcal{U} . Given M row vectors $\{A_k\}_{k \in [M]}$ and scalars $\{b_k\}_{k \in [M]}$ with $A_k \in \mathbb{R}^{1 \times m}$, if $A_i \cdot A_j \geq 0$ for all $i \in [M], j \in [M]$ and there exists $w_k \in \mathcal{U}'$ such that $A_k w_k \leq b_k$ for all $k \in [M]$, then there exists $p \in \mathcal{U}$ such that $A_k p \leq b_k$ for all $k \in [M]$.*

Proof. The argument is similar to that in Lemma 6, now extended to higher dimension. Let $\{\mathcal{P}_k\}_{k \in [m]}$ be a set of orthogonal hyperplanes in \mathbb{R}^m that meet at some point $p \in \mathbb{R}^m$ and satisfy $\mathcal{P}_k \cap \mathcal{U}' \neq \emptyset, \forall k \in [m]$. Let $\mathbb{P} = \{u \in \mathbb{R}^m \mid P_k u \leq P_k p, \forall k \in [m]\}$ be the orthant of \mathbb{R}^m originating from p and enclosed by $\{\mathcal{P}_k\}_{k \in [m]}$, for appropriate vectors $\{P_k\}_{k \in [m]}$, $P_k \in \mathbb{R}^{1 \times m}$. As in Lemma 5, there are at most m non-redundant constraints. Let \mathcal{N} be the set of indices of these non-redundant constraints, and construct \mathbb{P} so that $w_k \in \partial \mathbb{P}, \forall k \in \mathcal{N}$, analogous to how the solid red lines ($\partial \mathbb{P}$) intersect the vectors w_1, w_2 in Fig. 4. Then the point p will lie on the boundary of an m -hypersphere \mathbb{S} analogous to the black arc in Fig. 4, and all possible choices of p must lie in \mathcal{U} by the QEP. Let $y \in \mathbb{R}^m$ satisfy $A_k y = b_k, \forall k \in \mathcal{N}$. By the same argument as in Lemma 6, \mathbb{S} must enclose at least one such y . Thus, there exists at least one $p \in \mathbb{S} \subseteq \mathcal{U}$ that satisfies all M inequalities simultaneously. ■

We now apply the above geometric observations to the concurrent feasibility of several SCBFs or CBFs as follows.

Theorem 1. *Let \mathcal{U}' be any set with the OEP with respect to \mathcal{U} . Let $\{h_k\}_{k \in [M]}$ each be an SCBF for $(\mathcal{S}, \mathcal{U}')$. If $\{h_k\}_{k \in [M]}$ are non-interfering on \mathcal{S} as in Definition 4, then the set μ_{all} in (9) is nonempty for all $(q, v) \in \mathcal{S} \cap (\cap_{k \in [M]} \mathcal{H}_k)$.*

Proof. Let $A_k = \nabla_v h_k(q, v) g_2(q)$ and $b_k = \alpha_k(-h_k(q, v)) - \nabla_q h_k(q, v) g_1(q)$ for all $k \in [M]$, where α_k each come

from (5). It follows from Definition 4 that $A_i \cdot A_j \geq 0$ for all $i \in [M], j \in [M]$ everywhere in \mathcal{S} . It follows from Definition 2 that for each $k \in [M]$, there exists $w_k \in \mathcal{U}'$ such that $A_k w_k \leq b_k$ and w_k is anti-parallel to A_k . Lemma 5 then implies that these M inequalities are simultaneously feasible for some u in the full set \mathcal{U} , which is equivalent to the sets $\{\mu_k\}_{k \in [M]}$ having a nonempty intersection μ_{all} . ■

Theorem 2. *Let \mathcal{U}' be any set with the QEP with respect to \mathcal{U} . Let $\{h_k\}_{k \in [M]}$ each be a CBF for $(\mathcal{S}, \mathcal{U}')$. If $\{h_k\}_{k \in [M]}$ are non-interfering on \mathcal{S} as in Definition 4, then the set μ_{all} in (9) is nonempty for all $(q, v) \in \mathcal{S} \cap (\cap_{k \in [M]} \mathcal{H}_k)$.*

Proof. The proof is identical to that of Theorem 1, except that h_k are CBFs instead of SCBFs, so each w_k is not guaranteed to be anti-parallel to each A_k , respectively. Thus, we apply Lemma 7 instead of Lemma 5. ■

Theorems 1-2 constitute our first method for ensuring concurrent feasibility of multiple CBFs. Note that we provide theorems under both the OEP and QEP separately, because as shown in Fig. 3, the OEP is less conservative (i.e. allows for larger \mathcal{U}'), but is only applicable when the stricter SCBF condition (8) holds (which is often the case in practice). We also note the following remark about the computation of the gradients of the CBFs h_k for Definition 4 and Theorems 1-2.

Remark 2. *If κ is a High Order CBF as in [4], then there exists a function $\phi \in \mathcal{K}$ such that $h(q, v) = \dot{\kappa}(q, v) - \phi(-\kappa(q))$ is a CBF as in Definition 1. Moreover, $\dot{\kappa}(q, v) = \nabla_q \kappa(q) g_1(q) v$, so $\nabla_v h(q, v) \equiv \nabla_q \kappa(q) g_1(q) g_2(q)$. That is, $\nabla_v h(q, v)$ 1) is independent of v and 2) does not depend on the function ϕ . Thus, Definition 4 can be checked using only the gradients of the constraint functions κ_i, κ_j and the dynamics (1) without knowing the exact CBFs (i.e. the choices of ϕ).*

Referring to Example 1, Theorems 1-2 address the problem of determining a viability domain \mathcal{A} when $\gamma \in (0, 1]$. However, how to address Example 1 when $\gamma > 1$ still needs to be determined, as is done in Section III-C.

Example 3. *Consider the problem in Example 1 with $\gamma = 0.75$. The set $\mathcal{U}' = \{u \in \mathbb{R}^2 \mid \|u\|_1 \leq \frac{2}{1+\sqrt{2}}\}$ has the QEP with respect to \mathcal{U} as in Example 1. Using the new set \mathcal{U}' as the assumed allowable input bounds, the method in [4], [5] yields the CBFs $h_i(q, v) = \dot{\kappa}_i(q) - \sqrt{-\frac{4}{1+\sqrt{2}} \kappa_i(q)}$. Unlike in Example 1, the new set $\mathcal{A} = \mathcal{S} \cap \mathcal{H}_1 \cap \mathcal{H}_2$ is indeed a viability domain. The impact of constructing the CBFs for $(\mathcal{S}, \mathcal{U}')$ instead of $(\mathcal{S}, \mathcal{U})$ is visualized in the left half of Fig. 5.*

B. Modifying the Quadratic Program

The work in the prior section required Definition 4 to apply to all states in \mathcal{S} . Now, recall that Lemma 1 is effectively only a condition on the boundary of the invariant set \mathcal{A} . Noting this, in Section III-C, we will focus only on the boundary of \mathcal{A} , so unlike in Section III-A we will no longer be able to guarantee that $\mu_{\text{all}}(q, v)$ is nonempty for $(q, v) \in \text{int}(\mathcal{A})$.

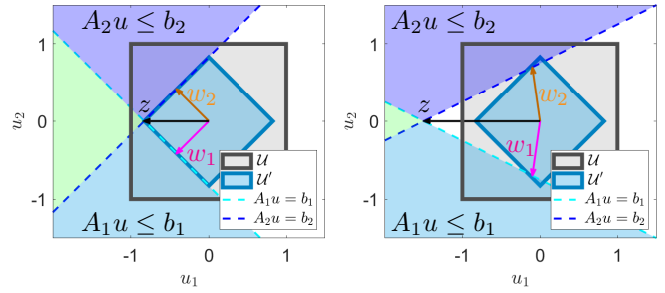


Fig. 5: Left: Visualization of the control space at a point $x_0 \in \partial \mathcal{H}_1 \cap \partial \mathcal{H}_2$ using $\mathcal{H}_1, \mathcal{H}_2$ as in Example 3. Compared to Fig. 1, the CBFs are now designed over \mathcal{U}' (the blue diamond) instead of \mathcal{U} , so there exists $z \in \mathcal{U}$ satisfying both $A_1 z \leq b_1$ and $A_2 z \leq b_2$. Right: Visualization of the control space at the point x_0 in Example 4. Because the CBFs h_1, h_2 do not satisfy Definition 4, it may be the case that every point z satisfying both inequalities $A_k z \leq b_k$ lies outside the set \mathcal{U} , so x_0 should not lie in the viability domain.

Rather, we will only be able to guarantee that there exists $u \in \mathcal{U}$ such that $\dot{h}_k(q, v, u) \leq 0$ for all k in the active set

$$\mathcal{I}(q, v) = \{k \in [M] \mid h_k(q, v) = 0\}. \quad (11)$$

That is, after employing the algorithm in Section III-C, the condition $\dot{h}_k(q, v, u) \leq \alpha_k(-h_k(q, v))$ in (10b) will be feasible for all $k \in \mathcal{I}(q, v)$, but possibly not for $k \in [M] \setminus \mathcal{I}(q, v)$. By [30], if \mathcal{A} in Lemma 3 is a viability domain, then there exists a set of class- \mathcal{K} functions $\{\alpha_k^*\}_{k \in [M]}$, such that (10) is always feasible. Instead of computing such a set directly, we let $\alpha_k^*(\lambda) = \delta_k \alpha_k(\lambda)$, where δ_k is a free variable. We then let $J_k > 0$, and modify the QP (10) as in [26] to

$$u(q, v) = \arg \min_{u \in \mathcal{U}, \delta_k \geq 1} \|u - u_{\text{nom}}(q, v)\|_2^2 + \sum_{k \in [M]} J_k \delta_k \quad (12a)$$

$$\text{s.t. } \dot{h}_k(q, v, u) \leq \delta_k \alpha_k(-h_k(q, v)), \forall k \in [M] \quad (12b)$$

Proposition 1. *Suppose the conditions of Lemma 3 hold. Then 1) the control law (12) will render \mathcal{A} forward invariant for as long as (12) is feasible, 2) (12) is feasible for all $(q, v) \in \mathcal{A}$ for which $\mathcal{I}(q, v)$ has cardinality of 0 or 1, and 3) (12) is feasible for all $(q, v) \in \mathcal{A}$ if \mathcal{A} is a viability domain.*

C. When the CBFs are Interfering

Next, consider what happens in Example 3 if $\gamma > 1$.

Example 4. *Consider the problem in Example 3 for $\gamma = 1.25$. Using the same strategy as in Example 3 yields the new CBFs $h_i(q, v) = \dot{\kappa}_i(q, v) - \sqrt{-\frac{4\gamma}{1+\sqrt{2}} \kappa_i(q)}$. Denote $\mathcal{A} = \mathcal{S} \cap \mathcal{H}_1 \cap \mathcal{H}_2$ and let $x_0 = (q, v) = (-\frac{1+\sqrt{2}}{4\gamma}, 0, 1, 0) \in \partial \mathcal{A}$. From the right side of Fig. 5, we see that there is no $u \in \mathcal{U}$ that satisfies both CBF conditions at x_0 . That is, Nagumo's necessary condition for forward invariance of \mathcal{A} is violated at x_0 , so \mathcal{A} is not a viability domain.*

The difference between Example 3 and Example 4 is that in Example 4, the CBFs h_1, h_2 do not satisfy Definition 4, so Theorems 1-2 do not apply. Thus, we need additional tools to systematically remove states such as x_0 in Example 4 from

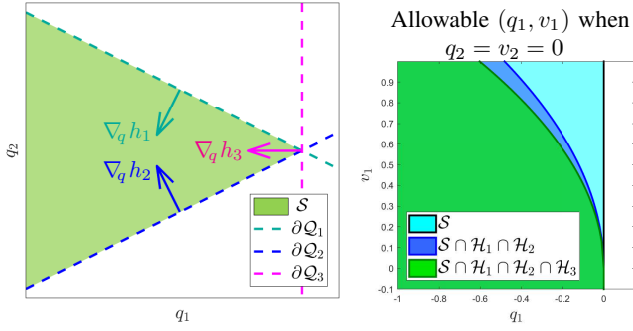


Fig. 6: Left: The CBFs h_1, h_2 do not satisfy Definition 4, so Theorems 1-2 do not apply. To remedy this, we add a third constraint κ_3 and associated CBF h_3 to remove the remaining states where (12) is infeasible. Right: Fixing $q_2 = v_2 = 0$, we show the allowable states (q_1, v_1) according to 1) the safe set (cyan), 2) the CBFs in Example 4 (blue), and 3) the CBFs in Example 5 (green).

Algorithm 1 Get Viability Domain

Require: \mathcal{S} in (4), \mathcal{U}' possessing QEP (or OEP) w.r.t. \mathcal{U} , CBFs (or SCBFs) $\{h_k\}_{k=1}^{M_0}$ for $(\mathcal{S}, \mathcal{U}')$ satisfying Lemma 3

- 1: $\mathcal{X} \leftarrow \mathcal{S} \cap (\bigcap_{k=1}^{M_0} \mathcal{H}_k)$
- 2: $\mathcal{D} = \bigcup_{i \in [M_0], j \in [M_0], i \neq j} (\partial \mathcal{H}_i \cap \partial \mathcal{H}_j)$
- 3: $M \leftarrow M_0$
- 4: $\mathcal{E} \leftarrow \text{getInfeasibleSet}(\mathcal{D})$
- 5: **while** $\mathcal{E} \neq \emptyset$ **do**
- 6: $\mathcal{E}_c \leftarrow \text{getCluster}(\mathcal{E})$
- 7: $h_{M+1} \leftarrow \text{getCBF}(\mathcal{E}_c, \mathcal{X}, \mathcal{U}')$
- 8: $\mathcal{X} \leftarrow \mathcal{X} \cap \mathcal{H}_{M+1}$
- 9: $M \leftarrow M + 1$
- 10: $\mathcal{D} = \bigcup_{i \in [M], j \in [M], i \neq j} (\partial \mathcal{H}_i \cap \partial \mathcal{H}_j)$
- 11: $\mathcal{E} \leftarrow \text{getInfeasibleSet}(\mathcal{D})$
- 12: **end while**
- 13: $\mathcal{A} \leftarrow \mathcal{X}$
- 14: **return** $\mathcal{A}, \{h_k\}_{k=1}^M$

\mathcal{A} in such cases. We begin by presenting a solution to this simple example before discussing a general algorithm.

Example 5. Consider the problem in Example 4. Introduce $\kappa_3(q) = q_1$, resulting in the constraint geometry in Fig. 6. Let \mathcal{H}_1 and \mathcal{H}_2 be as in Example 4, and using [4], [5], we can derive the CBF $h_3(q, v) = \dot{\kappa}_3(q, v) - \sqrt{-\frac{4}{1+\sqrt{2}}\kappa_3(q)}$. Then $\mathcal{A} = \mathcal{S} \cap \mathcal{H}_1 \cap \mathcal{H}_2 \cap \mathcal{H}_3$ is a viability domain for the sets \mathcal{S} and \mathcal{U} (see the green set on the right side of Fig. 6).

Example 5 improves upon Example 4 by further limiting the system's velocity v_1 so as to remove all the points where (12) is infeasible. This can be done either by adjusting h_1 and h_2 , or by adding the additional CBF h_3 . The first approach amounts to a joint tuning of all CBFs, which is challenging, so we instead focus on generalizing the latter strategy.

To this end, we propose Algorithm 1. Here, $\{h_k\}_{k \in [M]}$ is a working set of CBFs and \mathcal{X} is a working domain. Let \mathcal{D} be a set of candidate points where (12) could be infeasible, namely all points where at least two CBFs are active as in (11), as Proposition 1 guarantees feasibility of (12) at all other points. Next, let \mathcal{E} be the subset of \mathcal{D} where (12) is

actually infeasible, where \mathcal{E} is more expensive to compute than \mathcal{D} . Next, let $\text{getCluster}()$ be a function that divides all the points in \mathcal{E} into clusters (e.g. see Fig. 7), and then returns a single cluster $\mathcal{E}_c \subseteq \mathcal{E}$ for focus. Given this cluster, the function $\text{getCBF}()$ then determines a new CBF h_{M+1} for $(\mathcal{X}, \mathcal{U}')$ such that the cluster \mathcal{E}_c is entirely outside the CBF set \mathcal{H}_{M+1} . By Assumption 1, such a CBF h_{M+1} will always exist. Note also the use of the set \mathcal{U}' satisfying Definition 5 or 6 in $\text{getCBF}()$; this is done to reduce the number of points where h_{M+1} might conflict with the existing CBFs $\{h_k\}_{k \in [M]}$. Algorithm 1 then adds h_{M+1} to the working set of CBFs and shrinks the working domain to $\mathcal{X} \cap \mathcal{H}_{M+1}$ (e.g. see Fig. 6). The **while** block then repeats until either all the CBFs are jointly feasible or the domain \mathcal{X} becomes empty.

Note that the exact mechanics of grouping points into clusters during $\text{getCluster}()$ and of generating CBFs during $\text{getCBF}()$ will be specific to the system under study. An example of these steps is described in Section IV.

Proposition 2. *If Algorithm 1 converges, then \mathcal{A} is a viability domain as in Definition 3 and the controller (12) is always feasible and renders \mathcal{A} forward invariant.*

Algorithm 1 is similar to typical viability domain computation algorithms [16]–[22], except that the set \mathcal{A} is parameterized by a collection of CBFs. Since these CBFs are defined for a control set \mathcal{U}' possessing the QEP (or OEP), we can reduce the number of points that we need to check for infeasibility to only the points where 1) multiple CBFs are active as in (11) and 2) the active CBFs violate the condition in Definition 4. We next illustrate the implementation of Algorithm 1 by example on a nonlinear system.

Remark 3. *The choice of the functions $\text{getCluster}()$ and $\text{getCBF}()$ in Algorithm 1 will also affect the conservativeness of the resulting set \mathcal{A} compared to the viability kernel, and the time of convergence of the algorithm. A very small cluster size could result in many added CBFs and an explosion in computation. Note also that Algorithm 1 can be either coded and run autonomously, or followed step-by-step “by hand” by a practiced engineer.*

IV. APPLICATION TO ORIENTATION CONTROL

Let $q \in \{q \in \mathbb{R}^4 \mid \|q\|_2 = 1\}$ be the quaternion describing the orientation of a spherically symmetric rigid body with unit moments of inertia, and let $\omega = (\omega_1, \omega_2, \omega_3) \in \mathbb{R}^3$ be the angular velocity of the body. The dynamics are

$$\dot{q} = \frac{1}{2} \begin{bmatrix} 0 & \omega_3 & -\omega_2 & \omega_1 \\ \omega_3 & 0 & \omega_1 & \omega_2 \\ \omega_2 & -\omega_1 & 0 & \omega_3 \\ -\omega_1 & -\omega_2 & -\omega_3 & 0 \end{bmatrix} q, \quad \dot{\omega} = u. \quad (13)$$

Suppose a sensitive instrument faces towards an axis \hat{a} fixed to the body, and must avoid pointing towards the fixed directions \hat{b}_1, \hat{b}_2 in Fig. 7 by angles θ_1, θ_2 (red cones in Fig. 7). These constraints can be expressed as $\kappa_1(q) = q^T P(\hat{a}, \hat{b}_1, \theta_1) q$ and $\kappa_2(q) = q^T P(\hat{a}, \hat{b}_2, \theta_2) q$, where P is constant with respect to the state (q, ω) and is constructed as in [31]. Let $\mathcal{U} = \{u \in \mathbb{R}^3 \mid \|u\|_\infty \leq u_{\max}\}$ for some

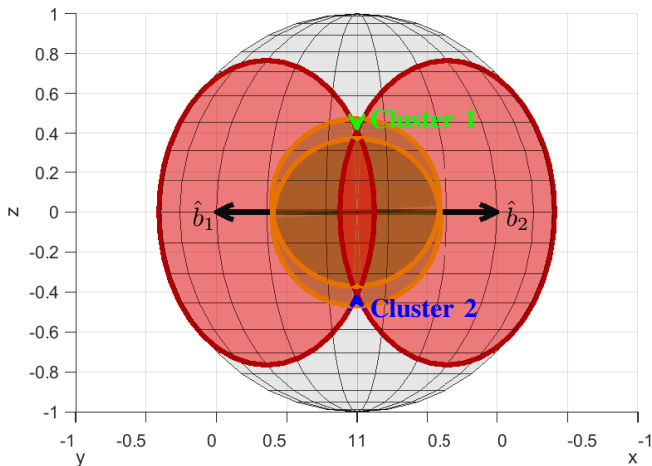


Fig. 7: Visualization of the constrained reorientation problem studied in Section IV. The large red cones are the initial unsafe states (where the body cannot point body-fixed vector \hat{a}), the two clusters are the states where (12b) is infeasible, and the brown cones are the states excluded by the new CBFs introduced by Algorithm 1.

u_{\max} . Assume the angular velocity is bounded by $\eta(\omega) = \|\omega\|_{\infty} - \omega_{\max}$, where the ∞ -norm can be expressed as 6 continuously differentiable constraint functions $\{\eta_j\}_{j \in [6]}$.

First, we find a set \mathcal{U}' with the OEP with respect to \mathcal{U} . Example 2 tells us that $\mathcal{U}' = \{u \in \mathbb{R}^3 \mid \|u\|_2 \leq \frac{u_{\max}}{\sqrt{3}}\}$ is one such set, from which we derive SCBFs $h_{\kappa,1}, h_{\kappa,2}$ for $(\mathcal{S}, \mathcal{U}')$ given by $h_{\kappa,i}(q, \omega) = \dot{\kappa}_i(q, \omega) - \sqrt{-\beta_i \kappa_i(q)}$ for some $\beta_i \in \mathbb{R}_{>0}$. We note that each η_j already satisfies the definition of an SCBF on $(\mathcal{S}, \mathcal{U}')$, so denote these SCBFs as $h_{\eta,j} \equiv \eta_j$. The eight SCBFs together satisfy the conditions of Lemma 3. We now focus only on the $h_{\kappa,1}, h_{\kappa,2}$ SCBFs. If the corresponding sets $\mathcal{H}_{\kappa,1}, \mathcal{H}_{\kappa,2}$ satisfy $\partial\mathcal{H}_{\kappa,1} \cap \partial\mathcal{H}_{\kappa,2} = \emptyset$, then \mathcal{A} in Lemma 3 is a viability domain and we are done. Here, we chose θ_1, θ_2 sufficiently large that this does not hold¹, as indicated by the intersection of the red cones in Fig. 7.

We then apply Algorithm 1. For this system, we coded `getCluster()` to return connected subsets of \mathcal{E} . In this case, `getInfeasibleSet()` returned states $(q, v) \in \mathbb{R}^7$ with quaternions q corresponding to the green and blue chevrons in Fig. 7, and `getCluster()` identified these points as two clusters. We then coded `getCBF()` to remove the cluster states by introducing a new constraint of the form $\kappa_{M+1}(q) = q^T P(\hat{a}, \hat{b}_{M+1}, \theta_{M+1}) q$, and computing an SCBF $h_{\kappa, M+1}$ of the same form as $h_{\kappa,1}$ and $h_{\kappa,2}$. The `getCBF()` function searched for the orientation \hat{b}_{M+1} and minimum angle θ_{M+1} that removed the entire cluster and that satisfied Definition 4 when paired with each of the existing SCBFs. Visually, for states with $\omega = 0$, the new SCBF $h_{\kappa, M+1}$ resulted in removing one of the brown cones in Fig. 7. After removing the first cluster, Algorithm 1 repeated for a second loop, and then completed and returned the two initial SCBFs (red cones) and two new SCBFs (brown cones) shown in Fig. 7.

One can also implement Algorithm 1 by hand as in

¹All code and parameters used can be found at <https://github.com/jbreeden-um/phd-code/tree/main/2023/ACCP2023>

Remark 3. For this system, a practiced engineer might instead decide that both clusters in Fig. 7 should be grouped into a single cluster, which can then be removed by adding a single new SCBF representing a larger cone.

Note that the computation time of Algorithm 1 depends most on the computation time of the `getInfeasibleSet()` step, which has to search a potentially large set for infeasibilities. However, this set is smaller than in typical verification algorithms, because we only have to consider states where the boundaries of two or more CBFs intersect. All other states already satisfy Lemma 1 because \mathcal{X} is parameterized by CBFs. Possible implementations of `getInfeasibleSet()` include [25], [29], and the wider viability theory literature. Since these are primarily sampling-based algorithms, the computation time is dependent on the sampling interval, which depends on the Lipschitz constants of h_k and the margin by which each h_k satisfies (5). The latter is equivalent to the chosen amount of conservatism with which the CBFs are implemented; more conservative margins (e.g. smaller β_i) will allow for sparser sampling and quicker computations. In this case, the results in Fig. 7 took 1052 seconds to compute, and results with a 10x coarser sampling took 0.30 seconds to compute, using a 3.5 GHz processor.

V. CONCLUSION

We have presented conditions under which multiple CBFs are guaranteed to be jointly feasible in the presence of prescribed input bounds, while allowing each CBF to be designed in a one-at-a-time fashion under more conservative assumptions on the available control authority. However, even under these assumptions, it is still possible for there to exist points where an optimization-based controller with multiple constraints may become infeasible. Thus, we also introduced an algorithm to iteratively remove such points from the allowable state set using additional CBFs until this set becomes a viability domain and the safe controller is always feasible. Future work in this area may include robust and sampled-data extensions of this framework, generalizations to other classes of systems, or extensions to relate this algorithm to the maximal viability kernel.

REFERENCES

- [1] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *18th Eur. Control Conf.*, 2019, pp. 3420–3431.
- [2] W. S. Cortez and D. V. Dimarogonas, "Correct-by-design control barrier functions for euler-lagrange systems with input constraints," in *Proc. Amer. Control Conf.*, 2020, pp. 950–955.
- [3] E. Squires, P. Pierpaoli, and M. Egerstedt, "Constructive barrier certificates with applications to fixed-wing aircraft collision avoidance," in *Proc. IEEE Conf. Control Technol. Appl.*, 2018, pp. 1656–1661.
- [4] W. Xiao and C. Belta, "Control barrier functions for systems with high relative degree," in *IEEE 58th Conference on Decision and Control*, 2019, pp. 474–479.
- [5] J. Breeden and D. Panagou, "Robust control barrier functions under high relative degree and input constraints for satellite trajectories," *arXiv*, 2021. [Online]. Available: <https://arxiv.org/abs/2107.04094v3>
- [6] L. Lindemann and D. V. Dimarogonas, "Control barrier functions for signal temporal logic tasks," *IEEE Control Syst. Lett.*, vol. 3, no. 1, pp. 96–101, 2019.

- [7] P. Glotfelter, J. Cortés, and M. Egerstedt, “Boolean composability of constraints and control synthesis for multi-robot systems via nonsmooth control barrier functions,” in *Proc. IEEE Conf. Control Technol. Appl.*, 2018, pp. 897–902.
- [8] M. Black and D. Panagou, “Adaptation for validation of a consolidated control barrier function based control synthesis,” *arXiv*, 2022. [Online]. Available: <https://arxiv.org/abs/2209.08170v1>
- [9] M. Rauscher, M. Kimmel, and S. Hirche, “Constrained robot control using control barrier functions,” in *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2016, pp. 279–285.
- [10] X. Xu, “Constrained control of input–output linearizable systems using control sharing barrier functions,” *Automatica*, vol. 87, pp. 195–201, 2018.
- [11] W. Jin, Z. Wang, Z. Yang, and S. Mou, “Neural certificates for safe control policies,” *arXiv*, 2020. [Online]. Available: <https://arxiv.org/abs/2006.08465v1>
- [12] A. Robey, H. Hu, L. Lindemann, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni, “Learning control barrier functions from expert demonstrations,” in *59th IEEE Conference on Decision and Control*, 2020, pp. 3717–3724.
- [13] W. Shaw Cortez, X. Tan, and D. V. Dimarogonas, “A robust, multiple control barrier function framework for input constrained systems,” *IEEE Control Syst. Lett.*, vol. 6, pp. 1742–1747, 2022.
- [14] W. Shaw Cortez and D. V. Dimarogonas, “Safe-by-design control for euler–lagrange systems,” *Automatica*, vol. 146, p. 110620, 2022.
- [15] J. Breeden and D. Panagou, “Guaranteed safe spacecraft docking with control barrier functions,” *IEEE Control Syst. Lett.*, vol. 6, pp. 2000–2005, 2022.
- [16] Y. Zhang, Y. Li, K. Tomsovic, S. M. Djouadi, and M. Yue, “Review on set-theoretic methods for safety verification and control of power system,” *IET Energy Syst. Integration*, vol. 2, no. 3, pp. 226–234, 2020.
- [17] F. Gruber and M. Althoff, “Computing safe sets of linear sampled-data systems,” *IEEE Control Syst. Lett.*, vol. 5, no. 2, pp. 385–390, 2021.
- [18] I. M. Mitchell, J. Budzisz, and A. Bolyachevets, “Invariant, viability and discriminating kernel under-approximation via zonotope scaling: Poster abstract,” in *Proc. of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*. New York, NY, USA: Association for Computing Machinery, 2019, p. 268–269.
- [19] N. Athanasopoulos, G. Bitsoris, and M. Lazar, “Construction of invariant polytopic sets with specified complexity,” *International Journal of Control*, vol. 87, no. 8, pp. 1681–1693, 2014.
- [20] S. V. Rakovic and M. Baric, “Parameterized robust control invariant sets for linear systems: Theoretical advances and computational remarks,” *IEEE Trans. Autom. Control*, vol. 55, no. 7, pp. 1599–1614, 2010.
- [21] M. A. Bouguerra, T. Fraichard, and M. Fezari, “Viability-based guaranteed safe robot navigation,” *Journal of Intelligent & Robotic Systems*, vol. 95, pp. 459–471, 2019.
- [22] L. Wang, D. Han, and M. Egerstedt, “Permissive barrier certificates for safe stabilization using sum-of-squares,” in *Proc. Amer. Control Conf.*, 2018, pp. 585–590.
- [23] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, “Robust control barrier–value functions for safety-critical control,” in *60th IEEE Conference on Decision and Control*, 2021, pp. 6814–6821.
- [24] B. Martin and O. Mullier, “Improving validated computation of viability kernels,” in *Proc. of the 21st International Conference on Hybrid Systems: Computation and Control*. New York, NY, USA: Association for Computing Machinery, 2018, p. 227–236.
- [25] K. Garg, A. A. Cardenas, and R. G. Sanfelice, “Sampling-based computation of viability domain to prevent safety violations by attackers,” in *2022 Proc. IEEE Conf. Control Technol. Appl.*, 2022, pp. 720–725.
- [26] J. Zeng, B. Zhang, Z. Li, and K. Sreenath, “Safety-critical control using optimal-decay control barrier function with guaranteed pointwise feasibility,” in *Proc. Amer. Control Conf.*, 2021, pp. 3856–3863.
- [27] A. Singletary, S. Kolathaya, and A. D. Ames, “Safety-critical kinematic control of robotic systems,” *IEEE Control Syst. Lett.*, vol. 6, pp. 139–144, 2022.
- [28] F. Blanchini, “Set invariance in control,” *Automatica*, vol. 35, no. 11, pp. 1747 – 1767, 1999.
- [29] X. Tan and D. V. Dimarogonas, “Compatibility checking of multiple control barrier functions for input constrained systems,” in *IEEE 61st Conference on Decision and Control*, 2022, pp. 939–944.
- [30] S. Prajna and A. Rantzer, “On the necessity of barrier certificates,” *IFAC Proceedings Volumes*, vol. 38, no. 1, pp. 526 – 531, 2005, 16th IFAC World Congress.
- [31] Y. Kim and M. Mesbahi, “Quadratically constrained attitude control via semidefinite programming,” *IEEE Trans. Autom. Control*, vol. 49, no. 5, pp. 731–735, May 2004.