A Forward Reachability Perspective on Robust Control Invariance and Discount Factors in Reachability Analysis

Jason J. Choi*, Donggun Lee*, Boyang Li, Jonathan P. How, Koushil Sreenath, Sylvia L. Herbert, and Claire J. Tomlin

***Abstract*— Control invariant sets are crucial for various methods that aim to design safe control policies for systems whose state constraints must be satisfied over an indefinite time horizon. In this article, we explore the connections among reachability, control invariance, and Control Barrier Functions (CBFs) by examining the forward reachability problem associated with control invariant sets. We present the notion of an "inevitable Forward Reachable Tube" (FRT) as an analysis tool for the verification of control invariant sets with differentiable boundaries. Our findings show that the inevitable FRT of a robust control invariant set with a differentiable boundary is the set itself. We highlight the importance of the differentiability of the boundary through numerical examples. We also formulate a zero-sum differential game between the control and disturbance, where the inevitable FRT is characterized by the zero-superlevel set of the value function. By incorporating a discount factor in the cost function of the game, the barrier constraint of the CBF naturally arises as the constraint that is imposed on the optimal control policy. As a result, the value function serves as a CBF-like function. Conversely, any valid CBF is also a forward reachability value function inside the control invariant set. As such, our work establishes a strong link between reachability, control invariance, and CBFs, filling a gap that prior formulations based on backward reachability were unable to bridge.**

I. Introduction

Safety guarantees are essential for control design in many applications. In this article, we focus on safety problems that can be represented by ensuring that system states satisfy specific constraints over an indefinite time horizon. An effective strategy to maintain state trajectories within the desired constraint region involves identifying a subset in which the trajectory can remain indefinitely. Then, the control policy that renders the trajectories invariant within this set will ensure that the system remains safe. Sets exhibiting these properties are referred to as *control invariant sets* [1], and are key to various methods for designing safe control policies in the literature [2]. As such, the theoretical analysis of control invariance offers valuable insights for the development of safe control policies.

A typical way of characterizing a control invariant set is by using a scalar function whose zero-superlevel set defines the invariant set, known as the barrier certificate [3]. This concept has evolved into the notion of a *control barrier function* (CBF) [4], which mandates that the function satisfies a particular differential inequality condition. Control policies generated by imposing this condition not only maintain safety on the boundary of the set, but additionally enforce that trajectories approaching the boundary "brake" smoothly. The condition will be called the *barrier constraint* in this article.

This paper presents the analysis of control invariance and the barrier constraint through the lens of reachability analysis. Reachability analysis, in fact, forms the basis for many methods that construct control invariant sets using dynamic programming principles [5]–[7]. In these methods, a value function is computed by solving an optimal control problem, whose level sets characterize the invariant sets, similarly to the CBFs. An attempt to bring in the idea of the barrier constraint into the reachability formulations was made in [8], however, it was limited to finite-horizon problems. We will discuss in Section V how this formulation struggles to extend to infinite-horizon problems when considering control invariance. This article works toward developing a new reachability formulation that resolves the issues that arose in [8] for its infinite-horizon extension.

The key idea of our new formulation is to use the forward reachability concept, instead of the backward reachability concept that was employed in previous literature on reachability for control invariance [5]–[10]. Forward reachability focuses on the set of states that an initial set reaches in the future, whereas backward reachability pertains to the set of states that reaches a terminal set from the past. In the previous works, one typically verifies control invariant sets by identifying and eliminating states that will inevitably reach unsafe regions, which corresponds to the backward reachability problem.

In contrast, we take the perspective of forward reachability. Forward reachability concepts have also been employed in safety control and verification literature. Rather than producing a control invariant set, application of forward reachability typically focuses on determining the set that encompasses all possible forward trajectory evolutions from an initial set and verifying whether this set intersects with any unsafe regions. Such a set is known as the *maximal* forward reachable tube (FRT) [11], and has been the primary focus of forward reachability applied for safety applications [12]–[14].

Little attention has been paid to the *minimal* FRT, which only includes states that are *inevitably* reached from the initial set [11]. The study in [11] enumerates various combinations of reachable set concepts, including backward versus forward and minimal versus maximal variations. That work dismissed the utility of minimal FRTs for safety by demonstrating that trajectories from an initial set whose minimal FRT does not intersect with an unsafe set may still inevitably reach the unsafe set.

In this work, we present minimal FRTs as an analysis tool for the verification of control invariant sets with differentiable boundaries, and their corresponding CBFs. We consider nonlinear systems with disturbances, which leads us to first present the extended notion of control invariance, termed robust control invariance, as defined in [10], [15]. We then redefine the term minimal FRT as *inevitable* FRT to accommodate systems with disturbances. The first theoretical finding presented in this paper concerns the verification of conditions under which the inevitable FRT remains identical to the initial set. We determine that the inevitable FRT remains unchanged when the initial set is robustly control invariant and has a differentiable boundary.

Next, we introduce a differential game formulation that characterizes the inevitable FRT as the zero-superlevel set of the value function capturing the game between the control and disturbance. The crux of our formulation is the incorporation of a discount factor in the cost function of the value function. First, it induces a contraction mapping in the Bellman operator of the value function, allowing the value function to be continuous and characterized as a

*The first two authors contributed equally to this work. J. J. Choi, K. Sreenath, and C. J. Tomlin are with University of California, Berkeley. D. Lee is with North Carolina State University, and J. P. How is with the Department of Aeronautics and Astronautics, Massachusetts Institute of Technology. Boyang Li and Sylvia L. Herbert are with University of California, San Diego. Contact info: jason.choi, koushils, tomlin@berkeley.edu, donggun_lee@ncsu.edu, jhow@mit.edu, bol025, sherbert@ucsd.edu

TABLE I

COMPARISON OF REACHABILITY METHODS WITH RESPECT TO PROPERTIES OF CONTROL-BARRIER FUNCTIONS.

Value function	Diff. Inequality in HJ-PDE	Matching CBF constraint	Boundedness	Continuity	Sol. Unique. of HJ-PDE
BRT (Viability Kernel) w/o discount [7] $V(x) := \inf_{\xi_d} \sup_{\mathrm{u}} \inf_{t\in[0,\infty)} h_S(\mathrm{x}(t))$	$\max_{u\in U}\min_{d\in D} \frac{\partial V}{\partial x}\cdot f(x,u,d) \geq 0$	no	**yes**	no	no
Discounted BRT [9], [10] $V(x) := \inf_{\xi_d} \sup_{\mathrm{u}} \inf_{t\in[0,\infty)} e^{-\gamma t} h_S(\mathrm{x}(t))$	$\max_{u\in U}\min_{d\in D} \frac{\partial V}{\partial x}\cdot f(x,u,d) - \gamma V \geq 0$	no	**yes**	**yes**	**yes**
CBVF [8] + Extension to infinite horizon [16] $V(x) := \inf_{\xi_d} \sup_{\mathrm{u}} \inf_{t\in[0,\infty)} e^{\gamma t} h_S(\mathrm{x}(t))$	$\max_{u\in U}\min_{d\in D} \frac{\partial V}{\partial x}\cdot f(x,u,d) + \gamma V \geq 0$	**yes**	no	no	no
Discounted FRT (Ours) $V(x) := \sup_{\xi_d} \inf_{\mathrm{u}} \sup_{t\in(-\infty,0]} e^{\gamma t} h_S(\mathrm{x}(t))$	$\max_{u\in U}\min_{d\in D} \frac{\partial V}{\partial x}\cdot f(x,u,d) + \gamma V \geq 0$	**yes**	**yes**	**yes**	**yes**

unique viscosity solution [17] to a particular Hamilton-Jacobi partial differential equation (HJ PDE) called the Hamilton-Jacobi forward reachable tube variational inequality (HJ-FRT-VI).

Most importantly, this formulation establishes a connection between reachability and control barrier functions. The barrier constraint arises as the constraint that the optimal control policy of the discounted FRT value function abides by. Thus, the value function serves as a CBF-like function in that it satisfies the barrier constraint almost everywhere. Conversely, we discover that any valid CBF is also a valid viscosity solution to the HJ-FRT-VI inside the control invariant set and can therefore be interpreted as a forward reachability value function. These findings constitute the main contribution of this article.

We highlight that prior formulations relying on backward reachability, introduced in [7]–[10], were unable to establish this connection between reachability, control invariance, and CBFs (Table I). Consequently, by adopting a forward reachability approach to control invariant sets in a manner not previously explored in the literature, our work becomes the first to create a strong link between these three concepts. The discount factor plays a critical role in this process, as it shapes the value function to satisfy the barrier constraint through an induced contraction.

The rest of the article is organized as follows. In Section II, we review the concepts of control invariance and CBFs, extending these notions to systems with disturbances, which leads to the definitions of robust control invariance and robust CBFs. Additionally, we provide a geometric interpretation of robust control invariant sets, which is used in the subsequent analyses throughout the paper. In Section III, we introduce the definitions of forward reachable tubes and present an analysis of their application to robust control invariant sets. In Section IV, we detail the Hamilton-Jacobi formulation of the FRT discussed in Section III and establish a connection to CBFs. Section V offers a comparison between our formulation and reachability formulations from prior work that have been applied to characterize control invariant sets. Finally, we conclude the article with closing remarks and directions for future work in Section VI.

Notation: $\|\cdot\|$ indicates the l^2 norm in the Euclidean space. For two same dimensional vectors a and b, $a\cdot b$ denotes the inner product. For a set A, $\overline{A}$ and $\mathrm{Int}(A)$ denote the closure and the interior, respectively. For a point $x \in \mathbb{R}^n$ and $r > 0$, we define $B_r(x)$ as the hypersphere centered at x with radius r, $B_r(x) := \{y \in \mathbb{R}^n \mid \|y - x\| \leq r\}$. For $\varepsilon > 0$ and a set A, $A + B_\varepsilon := \bigcup_{x\in A} B_\varepsilon(x)$, and $A - B_\varepsilon := A \setminus \bigcup_{x\in A^c} B_\varepsilon(x)$.

II. CONTROL INVARIANCE AND CONTROL BARRIER FUNCTIONS

We will be concerned with a general nonlinear time-invariant system represented by an ODE

$$\dot{\mathrm{x}}(t) = f(\mathrm{x}(t), \mathrm{u}(t)) \text{ for } t > 0, \qquad \mathrm{x}(0) = x, \tag{1}$$

where $x \in \mathbb{R}^n$ is an initial state, $\mathrm{x} : [0,\infty) \to \mathbb{R}^n$ is the solution to the ODE, and $\mathrm{u} : [0,\infty) \to U$ is a Lebesgue measurable control signal with $U \subset \mathbb{R}^{m_u}$. We use $\mathcal{U}$ to denote the set of Lebesgue measurable control signals:

$$\mathcal{U} := \{\mathrm{u} : [0,\infty) \to U \mid \mathrm{u} \text{ is Lebesgue measurable.}\} \tag{2}$$

We assume that the control input set U is compact, which holds for most physical systems whose actuation limit is bounded. Also, we assume that the system (1) satisfies the following conditions.

Assumption 1 (on vector field of (1))**.**

1) $f : \mathbb{R}^n \times U \to \mathbb{R}^n$ is uniformly continuous,
2) $f(\cdot, u)$ is Lipschitz continuous in $x \in \mathbb{R}^n$ for each $u \in U$,
3) $\exists M > 0$ such that $\|f(x,u)\| \leq M\ \forall x \in \mathbb{R}^n, u \in U$,

Under the above conditions, the solution to the ODE dynamics (1) is unique for any $\mathrm{u} \in \mathcal{U}$ and initial state $x \in \mathbb{R}^n$. We will call the solution x the *(forward) trajectory* of the initial state x.

A. Control Invariance

Let $X \subset \mathbb{R}^n$ be the constraint set, i.e. the set that the system must remain within to maintain safety. The main challenge of finding a control signal $\mathrm{u} \in \mathcal{U}$ such that for given $\mathrm{x}(0) \in X$, $\mathrm{x}(t) \in X$ for all $t \geq 0$ (i.e. $\mathrm{x}(\cdot)$ remaining safe) is that there may be some states in X from which exiting the set X is inevitable regardless of the choice of a control signal. An effective way of ruling out these failure states is to consider a subset of X that is control invariant.

Definition 1 ((Forward) control invariant [1])**.** A set $S \subset \mathbb{R}^n$ in the state space is *(forward) control invariant* under the dynamics (1) if for all $x \in S$, there exists a control signal $\mathrm{u} \in \mathcal{U}$ such that $\mathrm{x}(t) \in S$ for all $t \geq 0$. We also say that such u renders the trajectory x *forward invariant* in S.

By the above definition, a trajectory starting inside a control invariant set S that is a subset of X can remain within S for all time, and therefore can stay safe in X. One method for determining if a set is control invariant is by analyzing the evolution of trajectories within the tangent cone.

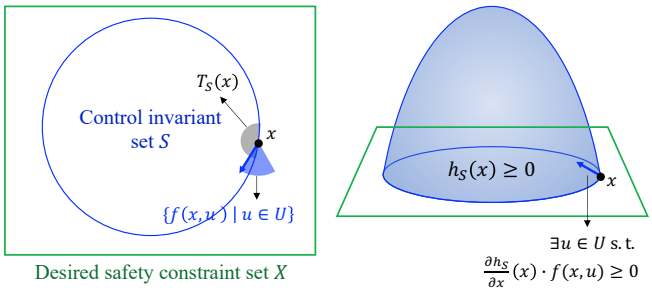

Fig. 1. A control invariant set $\boldsymbol{S}$ is a subset of the constraint set $\boldsymbol{X}$. In general, $\boldsymbol{S}$ is a strict subset. A trajectory starting inside a control invariant set $\boldsymbol{S} \in \boldsymbol{X}$ can remain within $\boldsymbol{S}$ for all time, and therefore can stay safe in $\boldsymbol{X}$. Geometric characterization of the control invariant set $\boldsymbol{S}$ based on the condition at its boundary is provided in Lemmas 1 and 2, by the usage of the tangent cone, and a distance-like function of $\boldsymbol{S}$, $\boldsymbol{h_S}$, respectively.

Definition 2 ((Bouligand's) tangent cone [18])**.** Given a closed set $S \subset \mathbb{R}^n$, the tangent cone to S at $x \in \mathbb{R}^n$ is defined as

$$T_S(x) := \left\{ z \in \mathbb{R}^n \mid \liminf_{\tau \to 0} \frac{\text{dist}(x + \tau z, S)}{\tau} = 0 \right\}, \tag{3}$$

where $\text{dist}(y, S) := \min_{z \in S} \|y - z\|$.

Lemma 1. (Tangential characterization of closed control invariant sets [19, Theorem 11.3.4]) Let the dynamics (1) satisfy Assumption 1. Then, a closed set $S \subset \mathbb{R}^n$ is (forward) control invariant under the dynamics (1) if and only if for all $x \in \partial S$,

$$\exists u \in U \text{ such that } f(x,u) \in T_S(x). \tag{4}$$

A pictorial description of this lemma is provided in Figure 1, left. Verifying the tangent cone everywhere along the boundary of a set is practically infeasible. A modification of the lemma can be made in a special case when the set S has a differentiable boundary (Assumption 2), by introducing a scalar function $h_S : \mathbb{R}^n \to \mathbb{R}$ that satisfies Assumption 3.

Assumption 2. S is a closed set whose interior is not empty, and the boundary of S, ∂S, *is continuously differentiable*.[1]

Assumption 3. Given a closed set S, $h_S : \mathbb{R}^n \to \mathbb{R}$ is a function whose zero-superlevel set is S, $S = \{x \in \mathbb{R}^{n_x} \mid h_S(x) \geq 0\}$, and satisfies the following conditions:

1)
$$\begin{aligned} \text{Int}(S) &= \{x \in \mathbb{R}^n \mid h_S(x) > 0\}, \\ \partial S &= \{x \in \mathbb{R}^n \mid h_S(x) = 0\}. \end{aligned} \tag{5}$$

2) (Differentiability and boundedness) h_S is uniformly continuously differentiable and both upper and lower bounded.
3) (Regularity) $\exists \varepsilon > 0$ such that

$$\frac{\partial h_S}{\partial x}(x) \neq 0 \quad \forall x \in \partial S + B_\varepsilon. \tag{6}$$

Lemma 2. Let the dynamics (1) satisfy Assumption 1 and for a given closed set $S \subset \mathbb{R}^n$ satisfying Assumption 2, let $h_S : \mathbb{R}^n \to \mathbb{R}$ satisfy Assumption 3. Then, S is (forward) control invariant under the dynamics (1) if and only if for all $x \in \partial S$,

$$\exists u \in U \text{ such that } \frac{\partial h_S}{\partial x}(x) \cdot f(x,u) \geq 0. \tag{7}$$

[1]For each point $x \in \partial S$, there exists $r > 0$ and a C^1 function $\eta : \mathbb{R}^{n-1} \to \mathbb{R}$ such that $S \cap B_r(x) = \{x \in B_r(x) \mid x_n \geq \eta(x_1, ..., x_{n-1})\}$, where relabeling and reorienting the coordinates axes are allowed [20].

Proof. This is a corollary of Lemma 1 by noticing that for $x \in \partial S$,

$$T_S(x) = \left\{ z \in \mathbb{R}^n | \frac{\partial h_S}{\partial x} \cdot z \geq 0 \right\}, \tag{8}$$

when Assumptions 2 and 3 hold. □

Remark 1. An h_S satisfying Assumption 3 always exists for the set S satisfying Assumption 2, by selecting a regularized distance function for S [21, Theorem 2.1].

In other words, if h_S is differentiable, at the boundary of the set where $h_S(x) = 0$, there must exist a control input $u \in U$ such that $\frac{\partial h_S}{\partial x}(x) \cdot f(x,u) \geq 0$. If this condition is met, the resulting vector field points inward into the set so that the value of $h_S(x)$ stays non-negative. This is shown in Figure 1, right. The lemma is known as Nagumo's theorem for autonomous systems [22].

Remark 2. For a given S that is control invariant, the condition (7) holds for any h_S satisfying Assumption 3. Thus, the specific choice of h_S does not affect the condition (7).

Remark 3. Note that a control invariant set does not necessarily have a differentiable boundary. In general, the maximal control invariant set contained in the desired safety constraint set X, might have a non-differentiable boundary [19]. However, the differentiability of the boundary will render a few noticeable differences in the theory that will be developed in Section III.

B. Control Barrier Functions

Lemma 2 implies that a safe control input on the boundary of the set S can render the trajectory x forward invariant in S. In the modern control theory, control barrier functions (CBFs), first introduced in [4], also impose conditions on the control input when the trajectory is strictly inside the set before reaching the boundary, which enables the trajectories to "smoothly brake" as they approach the boundary of the safe set. More formally, it is defined as below.

Definition 3. A function $h_S : \mathbb{R}^n \to \mathbb{R}$ that satisfies Assumption 3 for a closed set S is a *control barrier function* for the dynamics (1) if there exists an extended class $\mathcal{K}$ function α such that, for all $x \in S$,

$$\max_{u \in U} \frac{\partial h_S}{\partial x}(x) \cdot f(x,u) + \alpha\left(h_S(x)\right) \geq 0. \tag{9}$$

Here, $\alpha : \mathbb{R} \to \mathbb{R}$ is an extended class $\mathcal{K}$ function if it is continuous and strictly increasing and satisfies $\alpha(0) = 0$. We say the *barrier constraint is feasible at* x if the condition (9) holds for x.

This paper considers a particular class $\mathcal{K}$ function $\alpha(y) = \gamma y$ for a constant $\gamma > 0$, as in [23], [24],

$$\max_{u \in U} \frac{\partial h_S}{\partial x}(x) \cdot f(x,u) + \gamma h_S(x) \geq 0. \tag{10}$$

This is the most common choice of class $\mathcal{K}$ function used in the CBF literature, and enables us to make a connection between CBFs and reachability value functions where γ will play the role of a discount factor in the reachability formulation.

Intuitively, the inequality (10) ensures that $h_S(\mathrm{x}(t))$ does not decay faster than the exponentially decaying curve $\dot{h}_S(\mathrm{x}(t)) = -\gamma h_S(\mathrm{x}(t))$. This induces the "smooth braking" mechanism to any trajectory x approaching the boundary of S. If (10) is satisfied, (7) is trivially satisfied at $x \in \partial S$ where $h_S(x) = 0$. Thus, according to Lemma 2, the existence of the CBF h_S is a sufficient condition for S being control invariant. For control-affine systems, min-norm controllers like the CBF quadratic program (CBF-QP) have been

proposed as examples of the feedback policies that produce safe control signals that satisfy the barrier constraint [4].

Remark 4. If (7) in Lemma 2 holds with *strict* inequality for a compact and control invariant set S, any function h_S satisfying Assumption 3 can is a CBF with large enough γ [4, Lemma 2].

C. Robust control invariance for systems with disturbance

We introduce the concepts of control invariance and control barrier functions extended to systems with disturbance. Plenty of literature presents various notions of robustness with respect to disturbances or uncertainties in system dynamics [25]–[27], however, in this paper, we employ the differential game-based formulation that interprets the disturbance as an adversarial agent playing against the control input [28], as commonly done in the Hamilton-Jacobi reachability-based safety analysis for systems with bounded disturbance [7], [10], [15].

For this, we consider the system dynamics

$$\dot{\mathrm{x}}(t) = f(\mathrm{x}(t), \mathrm{u}(t), \mathrm{d}(t)) \text{ for } t > 0, \qquad \mathrm{x}(0) = x, \qquad (1_\mathrm{d})$$

where $\mathrm{d} : [0, \infty) \to D$ is a Lebesgue measurable disturbance signal and $D \subset \mathbb{R}^{m_d}$ is a compact set. We use $\mathcal{D}$ to denote the set of Lebesgue measurable disturbance signals. We assume conditions on the dynamics, similar to Assumption 1:

Assumption 4 (on vector field of (1_d))**.**

1) $f : \mathbb{R}^n \times U \times D \to \mathbb{R}^n$ is uniformly continuous,
2) $f(\cdot, u, d)$ is Lipschitz continuous in $x \in \mathbb{R}^n$ for each $(u, d) \in U \times D$,
3) $\exists M > 0$ such that $\|f(x, u, d)\| \leq M \ \forall x \in \mathcal{X}, (u, d) \in U \times D$,

so that under the above conditions, the solution to the ODE (1_d) is unique for any pair of $(\mathrm{u}, \mathrm{d}) \in \mathcal{U} \times \mathcal{D}$ and initial state $x \in \mathbb{R}^n$ [28].

To ensure safety under the most adversarial disturbance, we assume that the disturbance can use the control signal's current and previous information, whereas the control is not aware of the current disturbance input. To formulate this, we recall the definition of the *non-anticipative strategies* [28]:

$$\begin{aligned} \xi_d \in \Xi_d \coloneqq \{\xi_d : \mathcal{U} \to \mathcal{D} \mid \forall s \in [0, \infty) \text{ and } \mathrm{u}, \bar{\mathrm{u}} \in \mathcal{U}, \\ \text{if } \mathrm{u}(\tau) = \bar{\mathrm{u}}(\tau) \text{ a.e. } \tau \in [0, s], \\ \text{then } \xi_d[\mathrm{u}](\tau) = \xi_d[\bar{\mathrm{u}}](\tau) \text{ a.e. } \tau \in [0, s]\}. \end{aligned} \qquad (11)$$

Using the notion of non-anticipative strategies, we define the robust control invariant set under the dynamics (1_d).

Definition 4 (Robustly (forward) control invariant [10], [15])**.** A set $S \subset \mathbb{R}^n$ is *robustly (forward) control invariant* (under the dynamics (1_d)) if, for all $x \in S$, $\xi_d \in \Xi_d$, for any $\varepsilon > 0$ and $T > 0$, there exists a control signal $\mathrm{u}(\cdot) \in \mathcal{U}$ such that $\mathrm{x}(t) \in S + B_\varepsilon$ for all $t \in [0, T]$.

We provide a brief remark on the necessity of ε and T in the definition. First, if S is an open set, the notion of ε and T can be dropped, that is, if S is robustly control invariant, for all $x \in S$, $\xi_d \in \Xi_d$, there exists a control signal $\mathrm{u}(\cdot) \in \mathcal{U}$ such that $\mathrm{x}(t) \in S$ for all $t \geq 0$. However, at the boundary of a closed set S, the disturbance can react to the current control input to drive the system outside of S. Thus, x might not stay in S for all time although the trajectory x will stay in $S + B_\varepsilon$ for any small ε. To clarify this subtlety, we recall the example in [15]. Consider $\dot{\mathrm{x}}(t) = \mathrm{u}(t) + \mathrm{d}(t)$, $S = \{0\}$, and $U = D = [-1, 1]$. Then, for all disturbances, there is no control signal u that satisfies $\mathrm{x}(t) = 0$ for all $t \in [0, \infty)$. This is because for any control signal, $\dot{\mathrm{x}}(t)$ cannot be 0 almost everywhere in $(0, \infty)$ under the following non-anticipative strategy

$$\xi_d[\mathrm{u}](t) = \begin{cases} \mathrm{u}(t), & \text{if } \mathrm{u}(t) \neq 0, \\ 1, & \text{if } \mathrm{u}(t) = 0. \end{cases}$$

Thus, Definition 4 captures cases where, under the worst-case disturbance, there exists a control signal that "almost" never leaves the set S "almost" indefinitely (by choosing ε arbitrarily small and T sufficiently large).

Remark 5. Note that there exist different definitions of robust control invariance in the literature, for instance in [1].

Similar to Lemma 2, robustly control invariant sets can be verified by examining the vector field of the dynamics at the boundary of the sets. More formally, the following lemma holds.

Lemma 3. (Tangential characterization of robustly control invariant sets) Let the dynamics (1_d) satisfy Assumption 4 and let $S \subset \mathbb{R}^n$ and $h_S : \mathbb{R}^n \to \mathbb{R}$ satisfy Assumptions 2 and 3, respectively. Then, S is robustly (forward) control invariant under the dynamics (1_d) if and only if for all $x \in \partial S$,

$$\exists u \in U \text{ such that } \frac{\partial h_S}{\partial x}(x) \cdot f(x, u, d) \geq 0 \ \forall d \in D. \qquad (12)$$

Proof. The lemma results from [15, Theorem 2.3], and (8) which holds under Assumptions 2 and 3. □

We can also extend the definition of the control barrier function associated with the barrier constraint to the dynamics with disturbance (1_d).

Definition 5 (Robust Control Barrier Function)**.** A function $h_S : \mathbb{R}^n \to \mathbb{R}$ that satisfies Assumption 3 for a closed set S is a *robust control barrier function* for the dynamics (1_d) if there exists an extended class $\mathcal{K}$ function α such that, for all $x \in S$,

$$\max_{u \in U} \min_{d \in D} \frac{\partial h_S}{\partial x}(x) \cdot f(x, u, d) + \alpha\left(h_S(x)\right) \geq 0. \qquad (13)$$

By Lemma 3, it is again straightforward that the existence of the robust CBF h_S is a sufficient condition for S that is satisfying Assumption 2 to be robustly control invariant, since when $x \in \partial S$ (meaning that $h_S(x) = 0$), (13) indicates (12):

Proposition 1. Let the dynamics (1_d) satisfy Assumption 4 and let $S \subseteq \mathbb{R}^n$ satisfy Assumption 2. Then if the robust CBF h_S exists, the set S is robustly control invariant.

Remark 6. Another common concept of the CBF in the literature that is robust to disturbance is the notion of input-to-state safe (ISSf) CBF [26], [29]. The zero-superlevel set of an ISSf CBF is not necessarily robustly control invariant, however, one can verify a negative superlevel set that can be rendered robustly control invariant under the control signal satisfying the original barrier constraint (9). This means that while the margin that will be infiltrated by the disturbance has to be considered in the process of the design of the CBF, a controller that is blind to disturbance can be deployed safely as long as it satisfies (9). On the other hand, the robust CBF in Definition 5 allows the zero-superlevel set of h_S to be robustly control invariant as stated in Proposition 1. However, in order to render the set robustly forward invariant, the controller has to address the worst-case effect of the disturbance proactively, as in (13).

III. Forward Reachability of Control Invariant Sets

In this section, we apply forward reachability analysis to control invariant sets. In order to do so, we first provide background on the

forward reachability of a set and introduce definitions of forward reachable tubes.

A. Forward Reachability

Forward reachability analyzes a set's evolution in the future; its purpose is to identify the states that trajectories from an initial set $C \subset \mathbb{R}^n$ reach forward in time. The forward reachable tube (FRT) of a set, roughly speaking, encompasses states that are reached by trajectories departed from the initial set. This concept is illustrated in Figure 2. For autonomous systems (e.g. $\dot{\mathrm{x}}(t) = f(\mathrm{x}(t))$) whose trajectory is uniquely determined for each initial state, the evolution of a set is also uniquely determined, therefore, its forward reachable tube is unique (Fig 2 (a)). However, for systems with control and/or disturbance inputs like (1) and (1_d), the trajectory is determined by the choice of control and disturbance signals. Thus, the forward reachable tube can be shaped in various ways based on the choice of the controller and the disturbance assumptions.

Consider the dynamics of a controlled system satisfying (1) first. At one extreme, the control can use its best effort to get further away from the original set C, and at the other extreme, the control works to stay as close to C as possible. The former would render the FRT to expand maximally covering all the states such that from C, reaching them is viable, and the latter would induce the FRT to grow minimally, encapsulating only the states which inevitably must have evolved from C. From this intuition, we are able to define the viable and inevitable FRTs of a set C under the dynamics (1).

To introduce their formal definitions, we use a separate notation for the solution of the ODE (dynamics) whose terminal state is specified as x (as opposed to initial states being specified as x in (1)):

$$\dot{\mathrm{x}}^-(t) = f(\mathrm{x}^-(t), \mathrm{u}^-(t)) \text{ for } t < 0, \quad \mathrm{x}^-(0) = x, \qquad (1^-)$$

where $\mathrm{u}^- : (-\infty, 0] \to U$ is a measurable backward control signal. We will call x^- the *backward trajectory of (terminal state)* x. We will also denote $\mathcal{U}^-$ as a set of measurable backward control signals. Evaluating whether x^- reaches the set C if the time flows backward will tell us whether x belongs to a forward reachable tube of C. Using this, we define the viable and the inevitable FRTs:

Definition 6 (Viable FRT)**.** The *viable FRT* of an initial set $C \subset \mathbb{R}^n$ under the dynamics (1) for a time horizon $T > 0$ is defined as

$$\begin{aligned}\mathrm{FRT}'(C;T) \coloneqq \{x \in \mathbb{R}^n \mid \exists \mathrm{u}^- \in \mathcal{U}^-, \exists t \in [-T, 0] \\ \text{s.t. } \mathrm{x}^-(t) \in C, \text{ where } \mathrm{x}^- \text{ solves } (1^-).\}\end{aligned} \qquad (14)$$

We also define the *infinite-horizon viable FRT* of C as

$$\begin{aligned}\mathrm{FRT}'(C) \coloneqq \{x \in \mathbb{R}^n \mid \exists \mathrm{u}^- \in \mathcal{U}^-, \exists t \in (-\infty, 0] \\ \text{s.t. } \mathrm{x}^-(t) \in C, \text{ where } \mathrm{x}^- \text{ solves } (1^-).\}\end{aligned} \qquad (15)$$

In plain words, $\mathrm{FRT}'(C)$ is a collection of states that can be reached forward in time from trajectories that departed from C in the past. Note that for control systems, the viable FRT is the maximal FRT achievable by selecting an appropriate control signal (Figure 2 (b)) [11]. Viable FRTs have often been used in literature as means of safety verification, by evaluating safety of all possible trajectories in the future [12], [30]. In contrast, this paper focuses on the *inevitable* FRT, introduced next.

Definition 7 (Inevitable FRT)**.** The *inevitable FRT* of an initial set $C \subset \mathbb{R}^n$ under the dynamic (1) for a time horizon $T > 0$ is defined as

$$\begin{aligned}\mathrm{FRT}(C;T) \coloneqq \{x \in \mathbb{R}^n \mid \forall \mathrm{u}^- \in \mathcal{U}^-, \exists t \in [-T, 0] \\ \text{s.t. } \mathrm{x}^-(t) \in C, \text{ where } \mathrm{x}^- \text{ solves } (1^-).\}\end{aligned} \qquad (16)$$

We also define the *infinite-horizon inevitable FRT* of C as

$$\begin{aligned}\mathrm{FRT}(C) \coloneqq \{x \in \mathbb{R}^n \mid \exists T > 0 \text{ s.t. } \forall \mathrm{u}^- \in \mathcal{U}^-, \exists t \in [-T, 0] \\ \text{s.t. } \mathrm{x}^-(t) \in C, \text{ where } \mathrm{x}^- \text{ solves } (1^-).\}\end{aligned} \qquad (17)$$

Note that $\mathrm{FRT}(\cdot)$ can be also interpreted as a set mapping, $\mathrm{FRT} : 2^{\mathbb{R}^n} \to 2^{\mathbb{R}^n}$.

In plain words, $\mathrm{FRT}(C)$ is a collection of states such that *every* trajectory reaching it forward in time must have passed through C at some point in the past (Figure 2 (c)). For control systems, the inevitable FRT is minimal [11] since it excludes any state that can be reached by a trajectory that does not evolve from C.

Next, we extend the definition of forward reachable tubes to systems with disturbance (1_d). Because of the interaction between control and disturbance, we cannot trivially extend Definitions 6 and 7 by simply adding a disturbance term. Complexity is introduced due to the interplay between the disturbance strategies (e.g. (11)) and the choice of a control signal (which similarly makes Definition 4 more complicated than Definition 1). This work introduces only a particular type of robust FRT that is the equivalent of the infinite-horizon inevitable FRT (17) for systems with disturbance, which we will focus on throughout the rest of the paper. This FRT is shaped by the control aiming to restrain the growth of the FRT, whereas the disturbance is assumed to act adversarially and attempts to grow the FRT.

To formally define this, consider again the *backward trajectory* x^- solving

$$\dot{\mathrm{x}}^-(t) = f(\mathrm{x}^-(t), \mathrm{u}^-(t), \xi_d^-[\mathrm{u}^-](t)), t < 0, \quad \mathrm{x}^-(0) = x, \quad (1_\mathrm{d}^-)$$

where $\mathcal{D}^-$ denotes a set of measurable backward disturbance signals $\mathrm{d}^- : (-\infty, 0] \to D$, and ξ_d^- is a non-anticipative strategy for the disturbance in the sense of backward in time

$$\begin{aligned}\xi_d^- \in \Xi_d^- \coloneqq \{\xi_d^- : \mathcal{U}^- \to \mathcal{D}^- \mid \forall s \in (-\infty, 0] \text{ and } \mathrm{u}^-, \bar{\mathrm{u}}^- \in \mathcal{U}^-, \\ \text{if } \mathrm{u}^-(\tau) = \bar{\mathrm{u}}^-(\tau) \text{ a.e. } \tau \in [s, 0], \\ \text{then } \xi_d^-[\mathrm{u}^-](\tau) = \xi_d^-[\bar{\mathrm{u}}^-](\tau) \text{ a.e. } \tau \in [s, 0]\}.\end{aligned}$$

In the backward ODE dynamics (1_d^-), at each time $t < 0$, the control $\mathrm{u}^-(t)$ is forced to play first, and then the disturbance $\xi_d^-[\mathrm{u}^-](t)$ counters.

Definition 8. For a given initial set $C \subset \mathbb{R}^n$ which is an open set, we define the (infinite-horizon inevitable) FRT of C as the following set.

$$\begin{aligned}\mathrm{FRT}(C) \coloneqq \Big\{x \in \mathbb{R}^n \;\Big|\; \exists \xi_d \in \Xi_d, T > 0 \text{ s.t.} \\ \forall \mathrm{u} \in \mathcal{U}^-, \exists t \in [-T, 0] \text{ s.t. } \mathrm{x}^-(t) \in C, \\ \text{where } \mathrm{x}^- \text{ solves } (1_\mathrm{d}^-).\Big\}\end{aligned} \qquad (17_\mathrm{d})$$

Note that for systems with disturbance, the inevitable FRT is not necessarily minimal since the disturbance strategy attempts to grow the FRT.

B. Forward Reachable Tubes of control invariant sets

We are now ready to apply the forward reachability analysis to control invariant sets. The main theorem of the section is as follows:

Theorem 1. Suppose f satisfies Assumption 1 (or Assumption 4). Then, a set S satisfying Assumption 2 is control invariant under (1) (or robustly control invariant under (1_d)) if and only if $\mathrm{FRT}(\mathrm{Int}(S)) = \mathrm{Int}(S)$.

Proof. See Appendix A. □

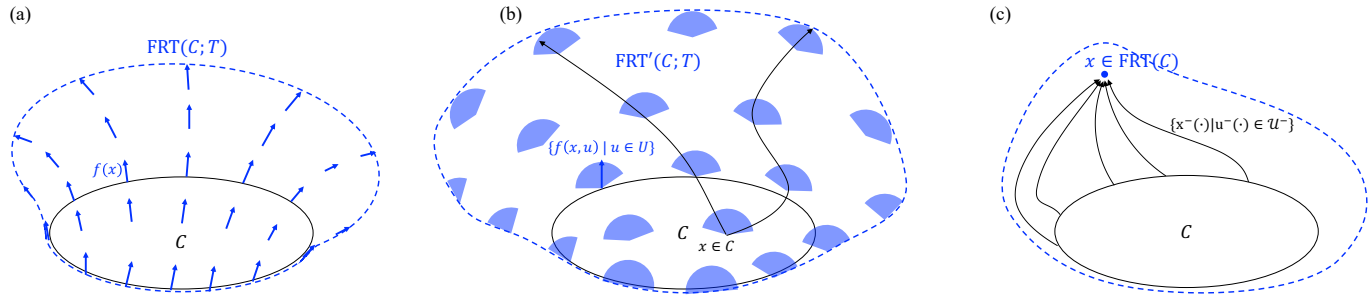

Fig. 2. (a) For an autonomous system $\dot{\mathbf{x}}(\boldsymbol{t}) = \boldsymbol{f}(\mathbf{x}(\boldsymbol{t}))$, the forward reachable tube (FRT) of $\boldsymbol{C}$ is a union of the set $\boldsymbol{C}$'s forward evolution and it is uniquely determined. (b) For control systems, the viable FRT, $\mathbf{FRT'}(\boldsymbol{C})$, is the collection of all possible trajectories departed from $\boldsymbol{C}$. (c) On the other hand, the inevitable FRT, $\mathbf{FRT}(\boldsymbol{C})$, is a collection of a state such that every trajectory reaching it must have passed through $\boldsymbol{C}$ at some point in the past.

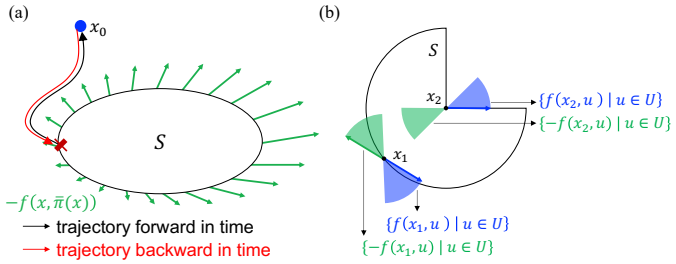

Fig. 3. (a) Illustration of why Theorem 1 holds for smooth control invariant set $\boldsymbol{S}$. (b) Illustration of the importance of the boundary of $\boldsymbol{S}$ being differentiable (Assumption 2) for Theorem 1.

The theorem states that the (inevitable) forward reachable tube of the interior of a (robust) control invariant set with a differentiable boundary is identical to the interior of the set itself. Another interpretation of the theorem is that the interior of any control invariant set with a differentiable boundary is a fixed point of $\mathrm{FRT}(\cdot)$. However, control invariant sets with nondifferentiable boundaries are not fixed points of $\mathrm{FRT}(\cdot)$ in general, and Theorem 1 does not hold for them. In the rest of this section, we mainly describe how the differentiable and nondifferentiable cases render different results. To simplify the explanation, we only consider the control system (1) without disturbance, and the system with disturbance is considered in the full proof of Theorem 1 in Appendix A.

First, when S satisfies Assumption 2 and h_S satisfies Assumption 3, Lemmas 1 and 2 imply that at any state x on the boundary ∂S of the control invariant set S, there exists a control $\bar{\pi}(x) \in U$ such that the dynamic flow points inward or tangential to S:

$$f(x, \bar{\pi}(x)) \in T_S(x), \tag{18}$$

and equivalently,

$$\frac{\partial h_S}{\partial x}(x) \cdot f(x, \bar{\pi}(x) \geq 0. \tag{19}$$

Equation (19) implies that the backward dynamic flow $-f(x, \bar{\pi}(x))$ must point either outward from or tangential to S (as the green vector fields in Figure 3a:

$$\frac{\partial h_S}{\partial x}(x) \cdot (-f(x, \bar{\pi}(x)) \leq 0,$$

or equivalently,

$$-f(x, \bar{\pi}(x)) \in T_{\mathrm{Int}(S)^c}(x), \tag{20}$$

by noting that $h_{\mathrm{Int}(S)^c} := -h_S$ also satisfies Assumption 3 and thus,

$$T_{\mathrm{Int}(S)^c}(x) = \{z \in \mathbb{R}^n | -\frac{\partial h_S}{\partial x} \cdot z \geq 0\}, \tag{21}$$

for $x \in \partial S$.

We will now discuss $\mathrm{Int}(S) = \mathrm{FRT}(\mathrm{Int}(S))$ under these conditions for smooth control invariant sets. First note that by Definition 7, $\mathrm{Int}(S) \subseteq \mathrm{FRT}(\mathrm{Int}(S))$. Therefore it is only left to check that there does not exist any state $x_0 \in \mathrm{FRT}(\mathrm{Int}(S))$ such that $x_0 \notin \mathrm{Int}(S)$. This hypothetical state x_0 is plotted in Figure 3a.

The definition of FRT requires that all trajectories reaching x_0 have departed from the interior of S at some point in the past. Reversing the flow of time, all backward trajectories x^- that start from x_0 and follow the backward dynamic flow should enter the interior of S at some point. However, from (20), one can see that this is not possible for the backward trajectory under the control signal satisfying $\mathrm{u}^-(t) = \bar{\pi}(\mathrm{x}^-(t))$ where $\mathrm{x}^-(t)$ is on the boundary of S, because $\bar{\pi}$ pushes the backward trajectory away from the interior of S. This is visualized in Figure 3a, where the backward trajectory (red) cannot enter the set S due to the flow field shown in green. Thus, this results in a contradiction and such a x_0 cannot exist.

It is important to note that Assumption 2 is crucial for establishing the equivalence between (18) and (20), which results from (8) and (21). The geometric interpretation of this equivalence is that the existence of the forward dynamic flow that keeps the set S invariant on its boundary should imply the existence of the backward dynamic flow that keeps the set S^c invariant (when the time flows backward) and vice versa. Figure 3b illustrates this relationship at the state x_1 which is on the smooth boundary of S.

One might consider the same equivalence relationship at the nonsmooth boundary of S when Assumption 2 does not hold. However, x_2 in Figure 3b highlights that this is not necessarily true. In particular, even if there exists a control input $u \in U$ such that the resulting forward dynamic flow keeps the set S invariant (by the flow pointing inward or tangential to S), all possible backward dynamic flow might still point inward to S and there might not exist any $u \in U$ such that the backward dynamic flow keeps the set S^c invariant if the time flows backward. In other words, even if (18) hold, (20) might not hold. In this case, the forward trajectory can be inevitably "leaked" from the interior of S, leading to the expansion of $\mathrm{FRT}(\mathrm{Int}(S))$ to a strict superset of $\mathrm{Int}(S)$. An example of this incident is introduced in the next subsection (Figure 4b).

In summary, it is important to note that the differentiability of the boundary of S is a crucial prerequisite condition for the equivalence between S being robustly control invariant and $\mathrm{Int}(S)$ being a fixed point of $\mathrm{FRT}(\cdot)$. This crucial gap between the smooth and nonsmooth cases, informally, is due to the fact that the tangent cone of a set on its boundary is locally symmetric to the tangent cone of the complement of the set only when it is on the smooth boundary.

C. Running example: Double Integrator

A running example we use in this subsection is a simple double integrator system with the system dynamics, $\dot{p} = v, \dot{v} = u$, with state $x = [p\ v]^T$, and control input u, with control bound $u \in [-1, 1]$. We compute the (inevitable) forward reachable tube defined in (17) for four specific sets S (Figure 4, first row). Note that in the state domain where $v > 0$, a curve $p = c - \frac{1}{2}v^2$ characterizes a trajectory that is decelerating from a positive velocity with the saturated input, $u = -1$, which stops at $p = c$. In the state domain where $v < 0$, a curve $p = c + \frac{1}{2}v^2$ characterizes a trajectory that is accelerating from a negative velocity with the saturated input, $u = 1$.

The descriptions of each choice of S are enlisted below:

(a) S is defined as the circular region with radius r centered at the origin. This set S satisfies Assumption 2 but is not control invariant.

(b) S is formed by five curves, $p = -p_1 + \frac{1}{2}v^2$, $p = p_1 - \frac{1}{2}v^2$, $p = p_2 - \frac{1}{2}v^2$, $p = -p_2 + \frac{1}{2}v^2$, $p = -\frac{1}{2}v^2$, and the p-axis, as shown in Figure 4(b). This set does not satisfy Assumption 2, but is control invariant.

(c) S is formed by two curves, $p = -p_1 + \frac{1}{2}v^2$, and $p = p_1 - \frac{1}{2}v^2$. This set also does not satisfy Assumption 2 but is control invariant.

(d) S is formed by two curves, $p = -p_1 + \frac{1}{2}v^2$ and $p = p_1 - \frac{1}{2}v^2$ ($p_1 > 1$), and two arcs whose radius is $r = -1 + 2\sqrt{p_1}$ that are tangential to the curves whose centers are positioned at $(-p_1 + r, 0), (p_1 - r, 0)$, respectively. This set satisfies Assumption 2 and is also control invariant.

The FRT of each $\mathrm{Int}(S)$ is visualized in the second row of Figure 4. The first case demonstrates that $\mathrm{FRT}(\mathrm{Int}(S))$ can be a strict superset of $\mathrm{Int}(S)$ when the set S is not control invariant. Note that the resulting $\mathrm{FRT}(\mathrm{Int}(S))$ is still not control invariant since the trajectory is bounded to escape the set at points A and B. This example reveals a challenge in constructing a control invariant set with forward reachability, when the initial set that is used is not control invariant. In the second and third cases, the control invariance of S can be checked analytically. The second case shows that $\mathrm{FRT}(\mathrm{Int}(S))$ can be a strict superset of $\mathrm{Int}(S)$ if Assumption 2 is not met. Note that point C is where (18) holds but (20) does not hold. In the third case, due to the fact that (20) holds at both points D and E, where ∂S is not smooth, $\mathrm{FRT}(\mathrm{Int}(S)) = \mathrm{Int}(S)$. Finally, the set S in the last case satisfies Assumption 2 and is also control invariant. Thus, according to Theorem 1, $\mathrm{FRT}(\mathrm{Int}(S))$ remains the same as $\mathrm{Int}(S)$.

IV. FRT VALUE FUNCTION AND CBF

In this section, by taking the Hamilton-Jacobi approach to the forward reachability problem, we pose the computation of forward reachable tubes as a differential game. The forward reachable tube is characterized by the value function proposed in Section IV-A. This value function is the unique solution to the HJ-PDE proposed in Section IV-B. When the initial set is control invariant and has a differentiable boundary, we establish a connection between the proposed value function and the CBFs in Section IV-C. Importantly, this provides an interpretation of any valid CBF as a forward reachability value function.

A. FRT Value function

For a closed set S, by noting that h_S satisfying Assumption 3 serves as a distance-like metric to the boundary of S and its sign serves as an indicator of the inclusion in S, we can rewrite the definition of the infinite-horizon inevitable FRT in (17_d) as follows:

$$\begin{aligned}\mathrm{FRT}(\mathrm{Int}(S)) \coloneqq \Big\{ & x \in \mathbb{R}^n \mid \exists \xi_d \in \Xi_d, \exists T > 0 \text{ s.t. } \forall \mathrm{u}^- \in \mathcal{U}^-, \\ & \exists t \in [-T, 0] \text{ s.t. } \mathrm{x}^-(t) \in \mathrm{Int}(S), \text{ where } \mathrm{x}^- \text{ solves } (1_\mathrm{d}^-). \Big\} \\ = & \left\{ x \in \mathbb{R}^n \mid \exists \xi_d \in \Xi_d, \forall \mathrm{u}^- \in \mathcal{U}^-, \sup_{t \in (-\infty, 0]} h_S(\mathrm{x}^-(t)) > 0 \right\} \\ = & \left\{ x \in \mathbb{R}^n \mid \sup_{\xi_d^- \in \Xi_d^-} \inf_{\mathrm{u}^- \in \mathcal{U}^-} \sup_{t \in (-\infty, 0]} h_S(\mathrm{x}^-(t)) > 0 \right\}.\end{aligned}$$

Since rescaling $h_S(\mathrm{x}^-(t))$ with a positive constant at any time t does not change its sign, the following holds:

$$\mathrm{FRT}(\mathrm{Int}(S)) = \left\{ x \in \mathbb{R}^n \mid \sup_{\xi_d^- \in \Xi_d^-} \inf_{\mathrm{u}^- \in \mathcal{U}^-} \sup_{t \in (-\infty, 0]} e^{\gamma t} h_S(\mathrm{x}^-(t)) > 0 \right\},$$

where at each time $t \in (-\infty, 0]$, $h_S(\mathrm{x}^-(t))$ is rescaled by $e^{\gamma t}$. Thus, by defining the FRT value function of S, $V_\gamma : \mathbb{R}^n \to \mathbb{R}$, as

$$V_\gamma(x) \coloneqq \sup_{\xi_d^- \in \Xi_d^-} \inf_{\mathrm{u}^- \in \mathcal{U}^-} J_\gamma(x, \mathrm{u}^-, \Xi_d^-) \tag{22}$$

with the cost functional $J_\gamma : \mathbb{R}^n \times \mathcal{U}^- \times \Xi_d^- \to \mathbb{R}$ defined as

$$J_\gamma(x, \mathrm{u}^-, \xi_d^-) = \sup_{t \in (-\infty, 0]} e^{\gamma t} h_S(\mathrm{x}^-(t)), \tag{23}$$

where x^- solves (1_d^-) and x is the terminal state of x^-, the following holds.

Lemma 4. Suppose $S \in \mathbb{R}^n$ is a closed set, f satisfies Assumption 4, and a bounded function h_S satisfies Assumption 3-1). $V_\gamma(x)$ is positive if and only if x belongs to the FRT of the interior of S:

$$\mathrm{FRT}(\mathrm{Int}(S)) = \{x \mid V_\gamma(x) > 0\}. \tag{24}$$

Proof. See Appendix B. □

The value function (22) captures a differential game between the control and the disturbance, wherein the optimal control signal of this game is verifying the existence of a trajectory that reaches x without passing through $\mathrm{Int}(S)$ in the past under the worst-case disturbance. If such a trajectory does not exist, $V_\gamma(x)$ is positive and x is inside $\mathrm{FRT}(\mathrm{Int}(S))$.

We now discuss the effect of introducing γ to the cost function. When we choose $\gamma > 0$, rescaling by $e^{\gamma t}$ discounts the measure h_S backward in time exponentially, thus, (22) defines a differential game problem with a discounted supremum-over-time cost function. More importantly, the value of the discount factor would also affect the resulting optimal control policy. Whereas the optimal control always has to try its best to maintain the value of h_S when there is no discount, the non-zero discount factor alleviates this conservativeness and allows the optimal control to decay the value of h_S. The discount factor attenuates the "degree of retrospection" in evaluating the worst-case in the past ($\sup_{t \in [-T, 0]}$); larger γ will recognize the value of h_S at the current time more than the value in the past.

As such, the discount factor introduces the "game-of-degree" aspect to the reachability problem. In this "game-of-degree," the parameter γ serves as a knob that adjusts how conservative the resulting optimal policy will be. However, the fundamental nature of the reachability problem—what is called the "game-of-kind" [15], [31]—remains consistent. In this aspect, whether or not the state is inside the FRT of $\mathrm{Int}(S)$ can still be determined by checking if $V_\gamma(x)$ is positive, as equation (24) holds for any value of γ.

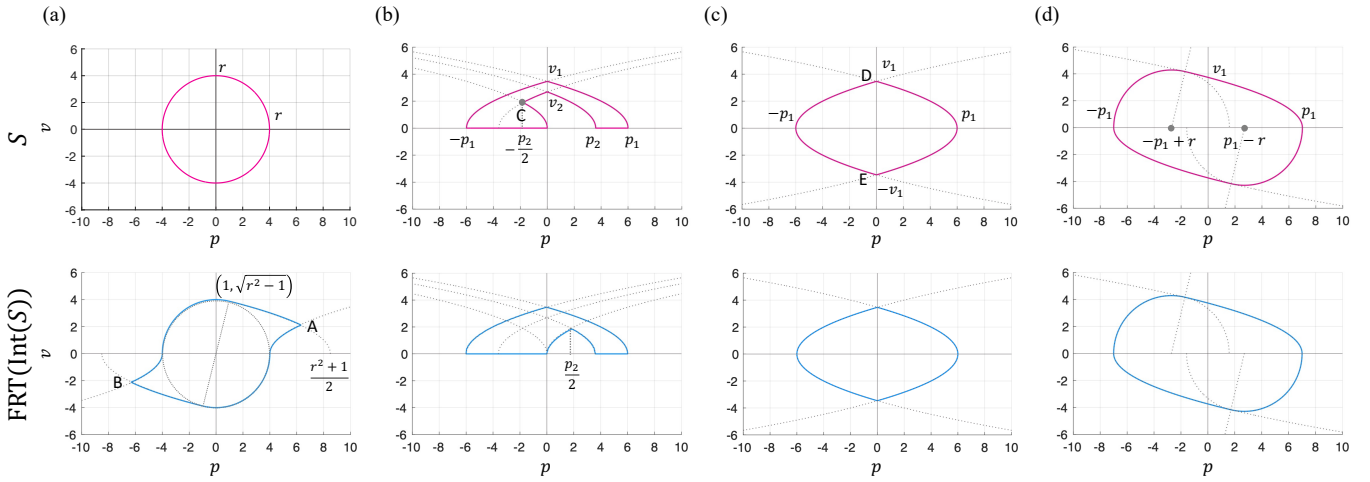

Fig. 4. Forward reachable tubes under double integrator dynamics for various shapes of $\boldsymbol{S}$. In the first row, $\boldsymbol{S}$ is visualized as the interior of the pink level curve. The interior of the blue level curve in the second row is $\mathbf{FRT}(\mathbf{Int}(\boldsymbol{S}))$ for each case. (a) Smooth $\boldsymbol{S}$ that is not control invariant, resulting in $\mathbf{FRT}(\mathbf{Int}(\boldsymbol{S})) \neq \mathbf{Int}(\boldsymbol{S})$. The FRT is still not control invariant. (b, c) Nonsmooth sets $\boldsymbol{S}$ that are control invariant; in case (b), $\mathbf{FRT}(\mathbf{Int}(\boldsymbol{S})) \neq \mathbf{Int}(\boldsymbol{S})$, and in case (c), $\mathbf{FRT}(\mathbf{Int}(\boldsymbol{S})) = \mathbf{Int}(\boldsymbol{S})$. This shows that Assumption 2 is required for Theorem 1 to hold. (d) Smooth control invariant $\boldsymbol{S}$ that results in $\mathbf{FRT}(\mathbf{Int}(\boldsymbol{S})) = \mathbf{Int}(\boldsymbol{S})$ according to Theorem 1.

The idea of introducing the discount to (23) is similar to the idea of introducing the discount factor to an infinite-horizon sum-over-time cost in optimal control problems [17]. In fact, many favorable properties of the value function resulting from the discount like its Lipschitz continuity, and the contraction of the corresponding Bellman backup operator hold similarly in both types of problems.

Proposition 2 (Lipschitz Continuity)**.** Suppose f satisfies Assumption 4 and h_S is Lipschitz continuous. V_γ is Lipschitz continuous in $\mathbb{R}^n$ if $L_f < \gamma$, where L_f is the Lipschitz constant of f.

Proof. See Appendix C. □

The condition $L_f < \gamma$ implies that the discount factor has to be large enough to suppress the effect of the vector field in prohibiting continuity. Under this condition, since the value function is Lipschitz continuous, it is differentiable almost everywhere by Rademacher's Theorem [20, Ch.5.8.3]. Other infinite-horizon value functions in backward reachability formulations [7], [8] do not have Lipschitz continuity and can even be discontinuous, which prohibits the usage of a differential inequality-based condition like the barrier constraint to derive safe control policies from the value function.

The contraction property of the Bellman backup will be discussed next after introducing the dynamic programming principle and the HJ-PDE characterization for FRT value function V_γ.

B. Hamilton-Jacobi characterization of the value function

This section provides a computational machinery for the computation of the value function V_γ using the Hamilton-Jacobi analysis. First, we apply Bellman's principle of optimality to (22):

Theorem 2 (Dynamic Programming principle)**.** Suppose $\gamma > 0$. For $x \in \mathbb{R}^n$,

$$V_\gamma(x) = \sup_{\xi_d^- \in \Xi_d^-} \inf_{\mathrm{u}^- \in \mathcal{U}^-} \max \Big\{ \max_{t \in [-T,0]} e^{\gamma t} h_S\left(\mathrm{x}^-(t)\right), \; e^{-\gamma T} V_\gamma\left(\mathrm{x}^-(-T)\right) \Big\} \tag{25}$$

for any $T > 0$, where x^- solves (1_{d}^-).

Proof. See Appendix D. □

Building on Theorem 2, Theorem 3 presents the Hamilton-Jacobi variational inequality for V_γ. For the definition of the viscosity solution in the theorem, see the proof of the theorem and [17] for more details.

Theorem 3. Suppose h_S is a bounded and Lipschitz continuous function, and $\gamma > 0$. V_γ in (22) is a unique viscosity solution in $\mathbb{R}^n$ of the following Hamilton-Jacobi PDE, called forward reachable tube Hamilton-Jacobi variational inequality (FRT-HJ-VI):

$$0 = \min \Big\{ V_\gamma(x) - h_S(x), \max_u \min_d \frac{\partial V_\gamma}{\partial x} \cdot f(x,u,d) + \gamma V_\gamma(x) \Big\}. \tag{26}$$

Proof. See Appendix E. □

For non-positive values of γ, V_γ might be unbounded and the FRT-HJ-VI might have multiple solutions. In contrast, a strictly positive value of γ guarantees the boundedness and the uniqueness of the solution of the FRT-HJ-VI. (An example in Appendix J illustrates these outcomes.) In fact, the uniqueness property follows from the contraction property of the Bellman backup associated with the dynamic programming principle of V_γ in (25).

To see this, we define a Bellman backup operator $B_T : \mathrm{BUC}(\mathbb{R}^n) \to \mathrm{BUC}(\mathbb{R}^n)$ for $T > 0$, where $\mathrm{BUC}(\mathbb{R}^n)$ represents a set of bounded and uniformly continuous functions: $\mathbb{R}^n \to \mathbb{R}$, as

$$B_T[V](x) \coloneqq \sup_{\xi_d^- \in \Xi_d^-} \inf_{\mathrm{u}^- \in \mathcal{U}^-} \max \Big\{ \max_{t \in [-T,0]} e^{\gamma t} h_S(\mathrm{x}(t)), \; e^{-\gamma T} V(\mathrm{x}^-(-T)) \Big\}. \tag{27}$$

Then, the following holds.

Theorem 4 (Contraction mapping)**.** For $V^1, V^2 \in \mathrm{BUC}(\mathbb{R}^n)$,

$$\|B_T[V^1] - B_T[V^2]\|_\infty \leq e^{-\gamma T} \|V^1 - V^2\|_\infty, \tag{28}$$

and the FRT value function V_γ in (22) is the unique fixed-point solution to $V_\gamma = B_T[V_\gamma]$ for each $T > 0$. Also, for any $V \in \mathrm{BUC}(\mathbb{R}^n)$,

$$\lim_{T \to \infty} B_T[V] = V_\gamma, \tag{29}$$

Proof. See Appendix F. □

The theorem provides us various methods to compute the FRT value function V_γ using the operation $B_T[\cdot]$, which does not require any assumptions for the initial guess of the value function, besides

the boundedness and uniform continuity in $\mathbb{R}^n$. For instance, the following lemma presents a finite-horizon HJ equation for this computation.

Lemma 5. For a given initial value function candidate $V^0 \in \mathrm{BUC}(\mathbb{R}^n)$, let $W : [0,T] \times \mathbb{R}^n \to \mathbb{R}$ be the unique viscosity solution to the following initial-value HJ-PDE

$$W(0,x) = \max\{h_S(x), V^0(x)\}, \text{ for } x \in \mathbb{R}^n, \tag{30}$$

$$0 = \min\left\{W(t,x) - h_S(x), \frac{\partial W}{\partial t} + \max_u \min_d \frac{\partial W}{\partial x} \cdot f(x,u,d) + \gamma W(t,x)\right\} \tag{31}$$

for $(t,x) \in (0,T) \times \mathbb{R}^n$. Then, $W(T,x) \equiv B_T[V^0](x)$.

Proof. See Appendix G. □

In Lemma 5, any $V^0 \in \mathrm{BUC}(\mathbb{R}^n)$ works for the computation of V_γ; for instance, a straightforward choice of V^0 can be h_S. As $T \to \infty$, $\frac{\partial W}{\partial t}$ vanishes to 0 for all $x \in \mathbb{R}^n$.

Combining Theorem 4 and Lemma 5, we have

$$\lim_{T\to\infty} B_T[V^0] = \lim_{T\to\infty} W(T,x) = V_\gamma(x). \tag{32}$$

The PDE (31) can be numerically solved forward in time from the initial condition (30), by using well-established time-dependent level-set methods [32].

Theorem 4 also enables other numerical schemes that are based on time-discretization, like value iteration, to produce an accurate approximate solution of V_γ. The following corollary of Theorem 4 provides the guarantee that the value iteration with any initial guess of $V^0 \in \mathrm{BUC}(\mathbb{R}^n)$ will converge to V_γ with a Q-linear convergence rate specified by (33). For a given time step size Δt, the semi-Lagrangian approximation can be applied to the exact Bellman backup operator in (27) for its numerical approximation, and the resulting value function will converge to V_γ when $\Delta t \to 0$ [9].

Corollary 1. For any $V^0 \in \mathrm{BUC}(\mathbb{R}^n)$ and a time step $\Delta t > 0$, define the sequence $\{V^k\}_{k=0}^\infty$ by an iteration $V^k := B_{\Delta t}[V^{k-1}]$ for $k \in \mathbb{N}$. Then,

$$\frac{\|V^{k+1} - V_\gamma\|_\infty}{\|V^k - V_\gamma\|_\infty} = e^{-\gamma \Delta t} < 1, \tag{33}$$

and thus, $\lim_{k\to\infty} V^k = V_\gamma$.

Proof. This is a direct outcome of Theorem 4. □

C. FRT Value Functions for control invariant sets

We now revisit the forward reachability for control invariant sets, by extending from the analysis presented in Section III-B, and draw a connection between the FRT value function V_γ and robust CBFs.

First, when S has a differentiable boundary and is robustly control invariant where Theorem 1 holds, the following holds:

Proposition 3. Under Assumptions 3, 4, and 2, S is robustly control invariant if and only if

$$\mathrm{FRT}(\mathrm{Int}(S)) = \mathrm{Int}(S) = \{x \mid V_\gamma(x) > 0\}, \tag{34}$$

$$\mathrm{Int}(S)^c = \{x \mid V_\gamma(x) = 0\}, \tag{35}$$

where V_γ is defined as (22).

Proof. The proposition holds from Theorem 1 and Lemma 4. □

When Proposition 3 holds, the control invariant set $\mathrm{Int}(S)$ is characterized as a strict zero-superlevel of V_γ. This enables the synthesis of a control policy using V_γ to maintain forward invariance of trajectories within $\mathrm{Int}(S)$. To see this, we derive an optimal policy of V_γ from the FRT-HJ-VI (26).

Proposition 4. Under the assumptions in Theorem 3, we define the set-valued map policy $K_\gamma : S \to 2^U$ as

$$K_\gamma(x) := \left\{u \in U : \min_{d\in D} \frac{\partial V_\gamma}{\partial x} \cdot f(x,u,d) + \gamma V_\gamma(x) \geq 0\right\}, \tag{36}$$

where V_γ is defined as (22). Then, $K_\gamma(x)$ is non-empty for every $x \in \mathrm{Int}(S)$ where $\frac{\partial V_\gamma}{\partial x}$ exists. In addition, if V_γ is differentiable, any element of $K_\gamma(x)$ is an optimal control input with respect to V_γ in (22), and under Assumptions 3, 4, and 2, if S is robustly control invariant, the trajectory under $K_\gamma(x)$ remains forward invariant in S under the worst-case disturbance.

Proof. See Appendix H □

The full proof is deferred to the appendix, however, the non-emptiness of $K_\gamma(x)$ is derived from V_γ satisfying the FRT-HJ-VI (26). By noting that the second term of the minimum in (26) has to be non-negative for (26) to hold, we get that

$$\max_{u\in U} \min_{d\in D} \frac{\partial V_\gamma}{\partial x} \cdot f(x,u,d) + \gamma V_\gamma(x) \geq 0 \tag{37}$$

at every $x \in \mathbb{R}^n$ where V_γ is differentiable. This corresponds to the barrier constraint in (13), where we consider a particular extended class $\mathcal{K}$ function $\alpha(y) = \gamma y$ for $y \in \mathbb{R}$.

Since the value function is Lipschitz continuous and differentiable almost everywhere by Proposition 2, V_γ satisfies (37) almost everywhere in $\mathrm{Int}(S) \subset \mathbb{R}^n$. Note that since V_γ is 0 everywhere outside $\mathrm{Int}(S)$, (37) also holds trivially for $x \in \mathrm{Int}(S)^c$. If V_γ is differentiable in $\mathrm{Int}(S)$, (37) is satisfied everywhere in $\mathrm{Int}(S) \subset \mathbb{R}^n$, which constitutes the definition of the robust CBF in Definition 5:

Corollary 2. If V_γ is continuously differentiable in $\mathrm{Int}(S)$, $V_\gamma : S \to \mathbb{R}$ is a robust CBF.

Proof. Proposition 4 implies that the barrier constraint holds at any state in the interior of S. As we constrain the domain of V_γ to S, the gradient of V_γ at any state on the boundary, $x \in \partial S$, is defined as $\lim_{y\to x} \frac{\partial V_\gamma}{\partial x}$. Since V_γ is continuously differentiable, this limit exists and $K_\gamma(x)$ in (36) is nonempty by Proposition 4. Thus, the statement holds by the definition of robust CBF in Def. 5. □

More importantly, any valid robust CBF h itself is the FRT value function in $\mathrm{Int}(S)$:

Theorem 5. Assume Assumptions 4 and 2. Let $h : \mathbb{R}^n \to \mathbb{R}$ be a differentiable function that satisfies Assumption 3 and is a robust CBF for a closed set S, satisfying

$$\max_{u\in U} \min_{d\in D} \frac{\partial h}{\partial x} \cdot f(x,u,d) + \gamma h(x) \geq 0, \tag{38}$$

for all $x \in S$ and some $\gamma > 0$. Then,

$$V_\gamma(x) = \max\{0, h(x)\} \tag{39}$$

is the unique viscosity solution of the FRT-HJ-VI (26) with $h_S(x) = h(x)$.

Proof. See Appendix I. □

Corollary 2 and Theorem 5 establishes a tight theoretical linkage between HJ reachability analysis and CBFs, wherein the role of discount factor is crucial. By introducing the discount factor to the reachability formulation, the value function becomes a CBF-like function in a sense that it satisfies the barrier constraint almost everywhere in the set S, and in the best case when it is differentiable,

it becomes the CBF. On the other hand, by Theorem 5, any CBF can be interpreted as an FRT value function with a discount factor. The barrier constraint naturally emerges as a discounted optimal control policy of the value function. Thus, this reveals that any CBF and a policy that satisfies the barrier constraint is *inverse optimal* for a forward reachability problem. The inverse optimality of CBF-based min-norm controllers has been investigated in [27], however, we believe that this is the first work that establishes the inverse optimality of the CBF itself.

Remark 7. Our findings reveal a significant correlation between the differentiability of the value function and the discount factor. Although viscosity solutions are generally non-differentiable, according to Theorem 5, under specific conditions, the value function (39) is differentiable in $\mathrm{Int}(S)$. As discussed in Remark 4, any h that characterizes the robust control invariant set is a CBF for sufficiently large γ. Under this condition, V_γ is identical to h in $\mathrm{Int}(S)$ and 0 in $\mathrm{Int}(S)^c$, thus, V_γ is differentiable in $\mathrm{Int}(S)$. Conversely, when the value of γ is smaller (i.e., indicating slower braking), V_γ may become non-differentiable even within $\mathrm{Int}(S)$. As will be demonstrated in the simulations presented in Section IV-D, we employ numerical gradients when the value function is computed numerically, but this method could allow violation of safety and the barrier constraint near states where the value function is not differentiable. To resolve these issues, further research is necessary, including our work, to explore Hamilton-Jacobi analysis with viscosity solutions in identifying optimal or robust controls at non-differentiable states.

D. Running example

We present an example of a pendulum system subjected to disturbance where we demonstrate the robustness of the safety control derived from Proposition 4. We use Proposition 4 to design the following robust safety filter:

Robust min-norm safety filter

$$\pi_S(x,t) = \arg\min_{u\in U} \left\|u - u_{ref}(t)\right\| \tag{40a}$$

$$\text{s.t.} \quad \min_{d\in D} \frac{\partial h}{\partial x}\cdot f(x,u,d) + \gamma h(x) \geq 0, \tag{40b}$$

where h is the chosen CBF. The controller (40) filters a reference control signal $u_{ref}(t)$—in case $u_{ref}(t)$ does not satisfy the barrier constraint, it selects a control input $u \in U$ that is closest to $u_{ref}(t)$ that satisfies (40b). Note that from Proposition 4, if we use an FRT value function V_γ that is differentiable for h, the filter is always feasible for $x \in \mathrm{Int}(S)$, and will render the trajectory forward invariant in $\mathrm{Int}(S)$. In the case when the system is affine in control input and disturbance, this safety filter can be implemented as a quadratic program [4], [8].

The dynamics of the pendulum system is given as

$$\begin{bmatrix}\dot{x_1}\\ \dot{x_2}\end{bmatrix} = \begin{bmatrix}x_2\\ -\sin x_1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix} u + \begin{bmatrix}0\\ \cos x_1\end{bmatrix} d, \tag{41}$$

where $x_1 = \theta$, $x_2 = \dot{\theta}$ are the angle and the angular rate of the pendulum, respectively, u is the applied torque, the control input, and d is the horizontal acceleration applied to the base of the pendulum, the disturbance to the system. $x_1 = 0$ at the released configuration. The desired safety constraint is $X = \{x \mid 0.5\pi \leq x_1 \leq 2\pi, |x_2| \leq 1\}$, constraining both the range of angle and the angular rate of the pendulum. We set the maximum torque $\bar{u} = \sin\frac{\pi}{3}$, so that the maximum torque cannot resist the torque produced by the gravity in the range of $\theta \in [\frac{\pi}{3}, \frac{2\pi}{3}]$ and $\theta \in [\frac{4\pi}{3}, \frac{5\pi}{3}]$. Then U is set as $[-\bar{u}, \bar{u}]$, and D is set as $[-0.1, 0.1]$.

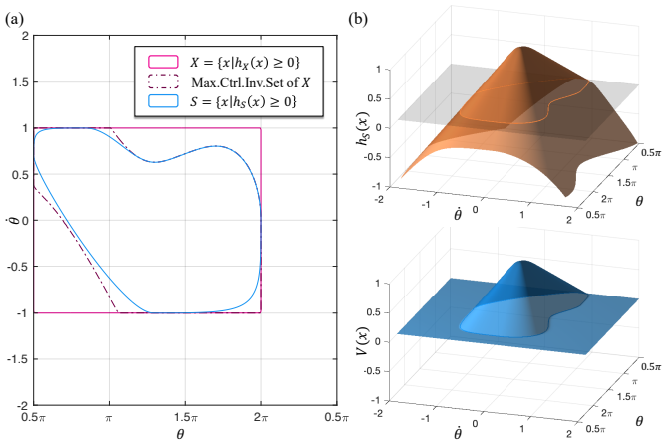

Fig. 5. (a) The desired safety constraint for the pendulum example is set to be $\boldsymbol{X = \{x | 0.5\pi \leq \theta \leq 2\pi, |\dot{\theta}| \leq 1\}}$. The robust control invariant set $\boldsymbol{S}$ for the computation of the FRT value function is designed by a bezier fitting to the maximal control invariant set of $\boldsymbol{X}$, computed from the backward reachability analysis. (b) The corresponding target function $\boldsymbol{h_S(X)}$ and the computed value function $\boldsymbol{V_\gamma(x)}$ with $\boldsymbol{\gamma = 5}$.

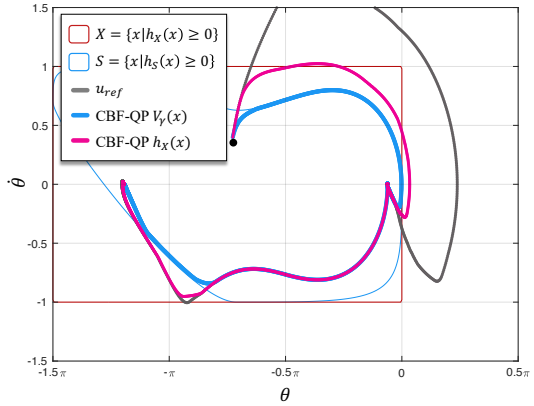

Fig. 6. Trajectories from a sampled initial state $\mathbf{x(0)} = [\mathbf{4\ 0.4}]^{\boldsymbol{T}}$ of the pendulum system under 1) the reference control signal $\boldsymbol{u_{ref}}$ that stabilizes to $\boldsymbol{(-0.2, 0)}$ for $\boldsymbol{t \in [0, 8]}$ and $\boldsymbol{(\pi - 0.6, 0)}$ for $\boldsymbol{t > 8}$ (grey), 2) the safety filter that uses the FRT value function $\boldsymbol{V_\gamma}$ as robust CBF (blue), and 3) the safety filter that uses the distance function of $\boldsymbol{X}$, $\boldsymbol{h_X}$ as robust CBF (red).

The reference control signal is produced by a clipped feedback linearization controller $u_{ref}(t) = \pi_{ref}(\mathrm{x}(t))$, given as

$$\pi_{ref}(x) = \min\left\{\max\{\sin x_1 - k_1(x_1 - x_{1,\text{target}}) - k_2 x_2, -\bar{u}\}, \bar{u}\right\}.$$

The desired target angle $x_{1,\text{target}}$ is set as -0.2 for $t \in [0, 8]$ and $\pi - 0.6$ for $t > 8$.

For the design of the target function h_S, we first verify the maximal control invariant set contained in X, using the backward reachability analysis, presented in [7], [10]. Then, a control invariant set with a differentiable boundary, S, and its distance function h_S, is designed by applying Bezier curve fitting [33] to the maximal control invariant set. The resulting S and h_S are visualized in Figure 5. We then compute the FRT value function V_γ. The result when $\gamma = 5$ is presented in Figure 5, which is differentiable in $\mathrm{Int}(S)$.

Next we demonstrate the robust min-norm safety filter (40) under the worst-case disturbances for various initial states. The phase plot

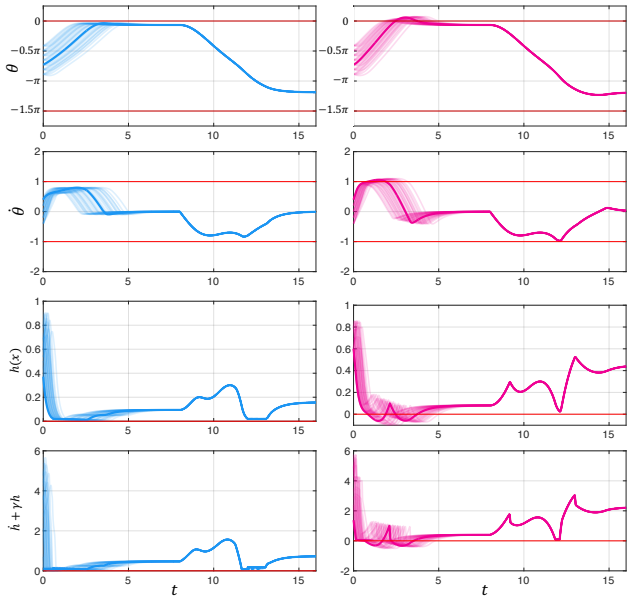

Fig. 7. Trajectories from multiple initial states under worst-case disturbance and the safety filter that uses the FRT value function $\boldsymbol{V_\gamma}$ as robust CBF (blue), and 3) the safety filter that uses the distance function of $\boldsymbol{X}$, $\boldsymbol{h_X}$ as robust CBF (red). The first and the second rows are states, the third row is the value of CBF, and the fourth row is the value of the left hand side of (40b), in time. The trajectories highlighted by thick lines are the trajectories in Figure 6

of the trajectories with the initial state $\mathrm{x}(0) = [4\ 0.4]^T$ is plotted in Figure 6. The state $\mathrm{x}(\cdot)$, control input $\mathrm{u}(\cdot)$ and the resulting CBF value $h(\mathrm{x}(\cdot))$ is plotted in time for various initial states in Figure 7. The trajectories under the desired control signal always exit X and violate safety. When the computed V_γ is used as the CBF h in (40), the trajectories under the safety filter remains safe in S, while always ensuring the feasibility of (40b). In contrast, for comparison, when a signed distance function h_X is used as the CBF h in (40), the feasibility of (40b) is not guaranteed. Even under the best control effort, i.e. $u = \max_{u\in U} \min_{d\in D} \frac{\partial h}{\partial x} \cdot f(x,u,d)$, applied in the case of infeasibility, the trajectories often violate safety. The worst-case disturbance in both cases is produced at each sampling time, by taking $\min_{d\in D} \frac{\partial h}{\partial x} \cdot f(x,u,d)$ for the chosen h.

V. Discussion

Although inspired by existing works that establish the connection between reachability and robust control invariance, our work is the first paper that connects *forward* reachability to the analysis of robust control invariance. Existing works have focused on backward reachability-based formulations that produce the largest robust control invariant set contained in a given desired safety region called the viability kernel. This is done by finding the inevitable (or minimal) backward reachable tube (BRT) [11] of the unsafe region, which becomes the complement of the viability kernel. Various value functions have been proposed to characterize the viability kernels based on computing the BRTs, both for finite time [6], [8], [34], [35] and infinite time [7], [9], [10], [16] but none of these functions are CBFs, as indicated in Table I.

The time-varying value functions that characterize finite-horizon BRTs are proposed in [6], [34], [35], where the discount factor is not necessary for the boundedness and continuity of the value function, and the solution uniqueness of the HJ-PDE. The work in [7] has extended these formulations to the infinite-horizon setting. However, the value function can be discontinuous and the corresponding HJ-PDE admits non-unique solutions [36]. The work in [9], [10] proposes formulations that resolve these issues for the infinite-horizon setting through the introduction of the discount factor. However, the differential inequality condition on the value function that emerges from the corresponding HJ-PDE differs from the barrier constraint (Table I). Moreover, the value function flattens to zero in the interior of the computed control invariant set, thus, there is no non-zero gradient of the value function inside the control invariant set that can be useful for the synthesis of safety control. On the other hand, another work [8] presents a formulation for the finite-horizon BRT wherein the differential inequality derived from the corresponding HJ-PDE matches the barrier constraint in the CBF definition. However, the extension of this formulation to infinite horizon might lead to an unbounded and discontinuous value function and non-unique solutions to the corresponding HJ-PDE.

Our formulation of forward reachability ensures compliance with the barrier constraint in the CBF definition. Additionally, the value function is both continuous and bounded in $\mathbb{R}^n$, while the corresponding HJ-PDE has a unique solution. The central idea behind our approach is the usage of the discount factor backward in time, as $e^{\gamma t}$ where $t < 0$, in the definition of the discounted FRT (22). In contrast to the discount in backward reachable tube formulations leading to the emergence of $-\gamma V_\gamma(x)$ in the corresponding HJ-PDEs, the usage of discount in this way leads to the emergence of positive $\gamma V_\gamma(x)$ term in the FRT-HJ-VI (26), and thus the satisfaction of the barrier constraint. Moreover, $e^{\gamma t}$ vanishes as t approaches $-\infty$, thereby ensuring continuous, bounded value functions and the solution uniqueness of the FRT-HJ-VI, resulting from the contraction mapping property outlined in Section IV-B.

An example in Appendix J illustrates the limitations of the previous approaches and compares our formulation to them using a simple one-dimensional system.

VI. Conclusions

In this study, we have presented a framework that establishes a strong linkage between reachability, control invariance, and Control Barrier Functions (CBFs) through a Hamilton-Jacobi differential game formulation. Two main aspects of our approach are the use of forward reachability concept in lieu of backward reachability, and the incorporation of a discount factor in the value function. These elements induce a contraction in the Bellman backup of the value function, thereby shaping it to satisfy the barrier constraint of the CBFs. Importantly, we note that prior formulations relying on backward reachability were unable to establish this connection between reachability, control invariance, and CBFs. Thus, our work fills a crucial gap in the existing literature, shedding new light on the interplay among these key concepts, which is vital for ensuring safety in control systems.

As we look toward future research avenues, several open questions and challenges emerge. One salient assumption underlying our study is the differentiability of the boundaries of control invariant sets. A deeper understanding of the implications and limitations of this assumption is crucial for broadening the applicability of our results. Also, the potential of forward reachability, especially in the context of inevitable FRT, has been discussed but not yet fully explored. Finally, our finding regarding the contraction mapping property has potential ramifications for learning-based approaches. Specifically, this property may pave the way for advancements in value-function-based approximate dynamic programming algorithms for safety control.

Appendix

A. Proof of Theorem 1

Before we present the proof, let us point out that control systems can be regarded as a special case of systems with disturbance when

the disturbance set D in (1_{d}) is set to a singleton (e.g. $D = \{0\}$ without loss of generality, which results in $\mathrm{d}(t) \equiv 0$). Under this point of view, it is easily checked that a set S is *robustly* control invariant if and only if it is control invariant by using Lemmas 7 and 12. As such, we will present the proof of Theorem 1 only in terms of systems with disturbance (1_{d}).

For the formal proof of Theorem 1, we have to reason about the backward flow of the dynamics, as in (1^-) and (1^-_{d}). In order to do so, we first consider the notion of backward control invariance, the mirrored version of the forward control invariance.

Definition 9 (Robustly *backward* control invariant)**.** A set $S \in \mathbb{R}^n$ is robustly *backward* control invariant (under (1_{d})) if for all $x \in S$, for all $\xi_d^- \in \Xi_d^-$, for any $\varepsilon > 0$ and time $T > 0$, there exists a backward control signal $\mathrm{u}^- \in \mathcal{U}^-$ such that $\mathrm{x}^-(t) \in S + B_\varepsilon$ for all $t \in [-T, 0]$, where x^- solves (1^-_{d}).

Put simply, backward control invariant sets are forward control invariant under the negated dynamics (where the time flows inversely). Thus, we can geometrically characterize the backward control invariant sets similarly to Lemma 3:

Corollary 3. Suppose Assumption 4 holds and let $S \subset \mathbb{R}^n$ and $h_S : \mathbb{R}^n \to \mathbb{R}$ satisfy Assumptions 2 and 3, respectively. Then, S is robustly backward control invariant if and only if for all $x \in \partial S$,

$$\exists u \in U \text{ such that } -\frac{\partial h_S}{\partial x}(x) \cdot f(x, u, d) \geq 0 \ \forall d \in D. \tag{42}$$

By combining Lemma 3 and Corollary 3, we draw a connection between forward and backward control invariant sets.

Lemma 6. Let $S \subset \mathbb{R}^n$ and $h_S : \mathbb{R}^n \to \mathbb{R}$ satisfy Assumptions 2 and 3, respectively. Under the dynamics (1_{d}) satisfying Assumption 4, S is robustly forward control invariant if and only if $\mathrm{Int}(S)^c$ is robustly backward control invariant.

Proof. By Lemma 3, S is robustly forward control invariant if and only if for all $x \in \partial S$, (12) is satisfied. Note that $\partial S = \partial \mathrm{Int}(S)^c$ and $\mathrm{Int}(S)^c$ and $h_{\mathrm{Int}(S)^c} := -h_S$ also satisfies Assumptions 2 and 3, respectively. Since $\frac{\partial h_{\mathrm{Int}(S)^c}}{\partial x}(x) = -\frac{\partial h_S}{\partial x}(x)$, (12) is equivalent to

$$\exists u \in U \text{ such that } \frac{\partial h_{\mathrm{Int}(S)^c}}{\partial x}(x) \cdot (-f(x, u, d)) \geq 0 \ \forall d \in D. \tag{43}$$

By applying Corollary 3, $\mathrm{Int}(S)^c$ is robustly backward control invariant if and only if for all $x \in \partial S$, (43) is satisfied. □

As remarked in Section III-B, ∂S being continuously differentiable in Assumption 2, is very important in Lemma 6. This assumption guarantees that, for a state x_1 on the boundary of S, if there exists a particular control u_1 such that $f(x_1, u_1, d)$ points inward to S for all $d \in D$, $-f(x_1, u_1, d)$ points outwards to S for all $d \in D$.

Next, we introduce the concept of a viability kernel under the backward dynamics:

Definition 10. A viability kernel of a closed set $C \subset \mathbb{R}^n$, under the backward dynamics (1^-_{d}), is defined as follows.

$$\begin{aligned}\mathrm{VK}_{-f}(C) \coloneqq \{x \in \mathbb{R}^n \mid \forall \xi_d^- \in \Xi_d^-, \varepsilon > 0, T > 0, \exists \mathrm{u}^- \in \mathcal{U}^- \text{ s.t.} \\ \forall t \in [-T, 0], \mathrm{x}^-(t) \in C + B_\varepsilon, \text{ where } \mathrm{x}^- \text{ solves } (1^-_{\mathrm{d}}).\}\end{aligned} \tag{44}$$

In words, it is a set of terminal states from which, for all backward disturbance strategies, a backward control signal exists such that the corresponding backward trajectory stays in $C + B_\varepsilon$ for all time. This definition applies the concept of *leadership kernel* in [15] to the backward dynamics.

Given any closed set $C \subset \mathbb{R}^n$, the $\mathrm{VK}_{-f}(C)$ is the largest negatively robustly invariant set in C. Thus, if C is negatively robustly control invariant, C is identical to its FVK.

Lemma 7. A closed set $C \subset \mathbb{R}^n$ is negatively robustly control invariant under (1_{d}) if and only if $\mathrm{VK}_{-f}(C) = C$.

Proof. This is straightforward from the definition of the robust backward control invariance and the viability kernel. □

According to Definitions 8 and 10, the FRT and the viability kernel under the backward dynamics have the following complement property.

Lemma 8. For any open set $C \subset \mathbb{R}^n$, the state space $\mathbb{R}^n$ can be partitioned into $\mathrm{FRT}(C)$ and $\mathrm{VK}_{-f}(C^c)$. In other words,

$$\{\mathrm{FRT}(C)\}^c = \mathrm{VK}_{-f}(C^c). \tag{45}$$

Furthermore, $\mathrm{VK}_{-f}(C)$ is always a closed set and $\mathrm{FRT}(C)$ is always an open set.

Proof. The complement relationship (45) follows directly from Definitions 8 and 10. That $\mathrm{VK}_{-f}(C)$ is a closed set is proven in [15], and $\mathrm{FRT}(C)$ being an open set follows directly from it being the complement of the closed set $\mathrm{VK}_{-f}(\mathrm{Int}(C)^c)$. □

Combining the lemmas above, we are now ready to present the proof of Theorem 1.

Proof of Theorem 1. S is positively robustly control invariant if and only if $\mathrm{Int}(S)^c$ is negatively robustly control invariant, by Lemma 6. By Lemma 7, $\mathrm{Int}(S)^c$ is negatively robustly control invariant if and only if $\mathrm{VK}_{-f}(\mathrm{Int}(S)^c) = \mathrm{Int}(S)^c$. By Lemma 8, $\mathrm{VK}_{-f}(\mathrm{Int}(S)^c) = \mathrm{FRT}(\mathrm{Int}(S))^c$. Thus, from the above statements, S is positively robustly control invariant if and only if $\mathrm{FRT}(\mathrm{Int}(S)) = \mathrm{Int}(S)$.

B. Proof of Lemma 4

Proof. We define two one-to-one functions: $\rho_{\mathrm{u}} : \mathcal{U} \to \mathcal{U}^-$:

$$\rho_{\mathrm{u}}(\mathrm{u})(-t) = \mathrm{u}(t), \quad \forall t \in [0, \infty); \tag{46}$$

and $\rho_{\xi_d} : \Xi_d \to \Xi_d^-$:

$$\rho_{\xi_d}(\xi_d)[\mathrm{u}^-](-t) = \xi_d[\rho_{\mathrm{u}}^{-1}(\mathrm{u}^-)](t), \tag{47}$$

for all $\mathrm{u}^- \in \mathcal{U}^-$ and $t \in [0, \infty)$. Then,

$$\mathrm{x}^-(-t) = \mathrm{x}(t) \quad \forall t \in [0, \infty), \tag{48}$$

where x^- solves (1^-_{d}), and x solves $\dot{\mathrm{x}}(t) = -f(\mathrm{x}(t), \rho_{\mathrm{u}}^{-1}(\mathrm{u}^-)(t), \rho_{\xi_d^-}^{-1}(\Xi_d^-)[\rho_{\mathrm{u}}^{-1}(\mathrm{u}^-)](t))$ for $t > 0$, and $\mathrm{x}(0) = x$. Since ρ_{u} and $\rho_{\xi_d^-}$ are one-to-one, the viability kernel of $\mathrm{Int}(S)^c$ under $-f$, defined in Definition 10, is equivalent to the following set:

$$\begin{aligned}\mathrm{VK}_{-f}(C) = \{x \in \mathbb{R}^n \mid \forall \xi_d \in \Xi_d, \varepsilon > 0, T > 0, \exists \mathrm{u} \in \mathcal{U} \text{ s.t.} \\ \forall t \in [0, T], \mathrm{x}(t) \in C + B_\varepsilon\},\end{aligned} \tag{49}$$

where x solves

$$\dot{\mathrm{x}}(t) = -f(\mathrm{x}(t), \mathrm{u}(t), \xi_d[\mathrm{u}](t)), \forall t > 0, \quad \mathrm{x}(0) = x. \tag{50}$$

By [10, Lemma 1], the viability kernel (49) of $\mathrm{Int}(S)^c$ is characterized by a particular value function:

$$\mathrm{VK}_{-f}(\mathrm{Int}(S)^c) = \left\{x \;\middle|\; \inf_{\xi_d \in \Xi_d} \sup_{\mathrm{u} \in \mathcal{U}} \inf_{t \in [0, \infty)} e^{-\gamma t}\Big(-h_S(\mathrm{x}(t))\Big) = 0\right\},$$

where x solves (50). By (48) and one-to-one properties of ρ_{u} and ρ_{ξ_d}, $\mathrm{VK}_{-f}(\mathrm{Int}(S)^c) = \{x \mid V_\gamma(x) = 0\}$. By Lemma 8,

$$\mathrm{FRT}(\mathrm{Int}(S)) = \{x \mid V_\gamma(x) \neq 0\}. \tag{51}$$

Since h_S is bounded,

$$V_\gamma(x) \geq \sup_{\xi_d^- \in \Xi_d^-} \inf_{\mathrm{u}^- \in \mathcal{U}^-} [e^{\gamma t} h_S(\mathrm{x}^-(t)) \mid t = \infty] = 0. \tag{52}$$

for all $x \in \mathbb{R}^n$. By combining (51) and (52), $\mathrm{FRT}(\mathrm{Int}(S)) = \{x \mid V_\gamma(x) > 0\}$. □

C. Proof of Proposition 2

Proof. For $x_1 \in \mathbb{R}^n$ and $\varepsilon > 0$, there exists $\hat{\xi}_d^- \in \Xi_d^-$ such that

$$V(x_1) \leq \inf_{\mathrm{u}^- \in \mathcal{U}^-} J_\gamma(x_1, \mathrm{u}^-, \hat{\xi}_d^-) + \varepsilon, \tag{53}$$

where J_γ is defined in (23). Hence,

$$V(x_1) \leq J_\gamma(x_1, \mathrm{u}^-, \hat{\xi}_d^-) + \varepsilon \tag{54}$$

for any $\mathrm{u}^- \in \mathcal{U}^-$. For x_2, there exists $\hat{\mathrm{u}}^- \in \mathcal{U}^-$ such that

$$V(x_2) \geq \inf_{\mathrm{u}^- \in \mathcal{U}^-} J_\gamma(x_2, \mathrm{u}^-, \hat{\xi}_d^-) \geq J_\gamma(x_2, \hat{\mathrm{u}}^-, \hat{\xi}_d^-) - \varepsilon. \tag{55}$$

By combining (54) and (55), we have

$$\begin{aligned} V(x_1) - V(x_2) &\leq J_\gamma(x_1, \hat{\mathrm{u}}^-, \hat{\xi}_d^-) - J_\gamma(x_2, \hat{\mathrm{u}}^-, \hat{\xi}_d^-) + 2\varepsilon \quad (56)\\ &= \sup_{t \in (-\infty, 0]} e^{\gamma t} h_S(\mathrm{x}_1^-(t)) - \sup_{t \in (-\infty, 0]} e^{\gamma t} h_S(\mathrm{x}_2^-(t)) + 2\varepsilon, \end{aligned}$$

where x_1^- solves (1_{d}^-) for $(\hat{\mathrm{u}}^-, \hat{\xi}_d^-)$ with the terminal state x_1, and x_2^- solves (1_{d}^-) for $(\hat{\mathrm{u}}^-, \hat{\xi}_d^-)$ with the terminal state x_2. Since there exists $\hat{t} \in (-\infty, 0]$ such that

$$\sup_{t \in (-\infty, 0]} e^{\gamma t} h_S(\mathrm{x}_1^-(t)) \leq e^{\gamma \hat{t}} h_S(\mathrm{x}_1^-(\hat{t})) + \varepsilon, \tag{57}$$

(57) implies

$$\begin{aligned} V(x_1) - V(x_2) &\leq e^{\gamma \hat{t}} h_S(\mathrm{x}_1^-(\hat{t})) - e^{\gamma \hat{t}} h_S(\mathrm{x}_2^-(\hat{t})) + 3\varepsilon \quad (58)\\ &\leq L_{h_S} e^{\gamma \hat{t}} e^{-L_f \hat{t}} \|x_1 - x_2\| + 3\varepsilon \quad (59)\\ &\leq L_{h_S} \|x_1 - x_2\| + 3\varepsilon, \quad (60) \end{aligned}$$

where L_{h_S} is the Lipschitz constant of h_S. The second inequality is by Gronwall's inequality, and the third inequality is by the condition, $L_f < \gamma$. Using the similar argument, we can show $V(x_2) - V(x_1) \leq L_{h_S}\|x_1 - x_2\| + 3\varepsilon$, thus $|V(x_1) - V(x_2)| \leq L_{h_S}\|x_1 - x_2\| + 3\varepsilon$. Since the previous inequality holds for all $\varepsilon > 0$, $|V(x_1) - V(x_2)| \leq L_{h_S}\|x_1 - x_2\|$. □

D. Proof of Theorem 2

Proof. Similarly to Appendix B, using the one-to-one mappings ρ_{u} and $\rho_{\xi_d^-}$, the value function V_γ in (22) can be written as

$$V_\gamma(x) = \sup_{\xi_d \in \xi_d} \inf_{\mathrm{u} \in \mathcal{U}} \sup_{t \in [0, \infty)} e^{-\gamma t} h_S(\mathrm{x}(t)), \tag{61}$$

where x solves (50). [10, Lemma 3] proves that

$$V(x) = \sup_{\xi_d \in \Xi_d} \inf_{\mathrm{u} \in \mathcal{U}} \max\{\max_{t \in [0,T]} e^{-\gamma t} h_S(\mathrm{x}(t)), e^{-\gamma T} V(\mathrm{x}(T))\}. \tag{62}$$

Combining (62) with (46) and (47), we conclude (25). □

E. Proof of Theorem 3

Proof. Similarly to Appendix D, from (61), [10, Lemma 3] proves that V_γ is the unique viscosity solution to

$$0 = \min\{V_\gamma(x) - h_S(x), -\min_{u \in U} \max_{d \in D} \frac{\partial V_\gamma}{\partial x} \cdot (-f(x,u,d)) + \gamma V_\gamma(x)\}$$

in $\mathbb{R}^n$. This is equivalent to satisfying the following two conditions. First, for any smooth function $v \in C^\infty(\mathbb{R}^n)$ such that $V_\gamma - v$ has a local minimum at $x_0 \in \mathbb{R}^n$ and $V_\gamma(x_0) = v(x_0)$,

$$\begin{aligned} 0 &\leq \min\{v(x) - h_S(x), -\min_{u \in U} \max_{d \in D} \frac{\partial v}{\partial x} \cdot (-f(x,u,d)) + \gamma v(x)\}\\ &= \min\{v(x) - h_S(x), \max_{u \in U} \min_{d \in D} \frac{\partial v}{\partial x} \cdot f(x,u,d) + \gamma v(x)\}. \end{aligned}$$

Second, for any smooth function $v \in C^\infty(\mathbb{R}^n)$ such that $V_\gamma - v$ has a local maximum at $x_0 \in \mathbb{R}^n$ and $V(x_0) = v(x_0)$,

$$\begin{aligned} 0 &\geq \min\{v(x) - h_S(x), -\min_{u \in U} \max_{d \in D} \frac{\partial v}{\partial x} \cdot (-f(x,u,d)) + \gamma v(x)\}\\ &= \min\{v(x) - h_S(x), \max_{u \in U} \min_{d \in D} \frac{\partial v}{\partial x} \cdot f(x,u,d) + \gamma v(x)\}. \end{aligned}$$

□

F. Proof of Theorem 4

Proof. In the proof, we define

$$l(\xi_d, \mathrm{u}, x) \coloneqq \max_{t \in [-T, 0]} e^{\gamma t} h_S(\mathrm{x}(t)), \quad l^i(\xi_d, \mathrm{u}, x) \coloneqq e^{-\gamma T} V^i(\mathrm{x}(-T)),$$

for $i = 1, 2$, then

$$B_T[V^i i] = \sup_{\xi_d \in \Xi_d} \inf_{\mathrm{u} \in \mathcal{U}} \max\{l(\xi_d, \mathrm{u}), l^i(\xi_d, \mathrm{u})\}.$$

Without loss of generality, let $B_T[V^1](x) \geq B_T[V^2](x)$. For any $\varepsilon > 0$, there exists $\bar{\xi}_d$ such that $B_T[V^1] - \varepsilon < \inf_{\mathrm{u}} \max\{l(\bar{\xi}_d, \mathrm{u}), l^1(\bar{\xi}_d, \mathrm{u})\}$, and there exists $\bar{\mathrm{u}}$ such that $\inf_{\mathrm{u}} \max\{l(\bar{\xi}_d, \mathrm{u}), l^2(\bar{\xi}_d, \mathrm{u})\} + \varepsilon > \max\{l(\bar{\xi}_d, \bar{\mathrm{u}}), l^2(\bar{\xi}_d, \bar{\mathrm{u}})\}$. Then,

$$\begin{aligned} B_T[V^1](x) - B_T[V^2](x) &< 2\varepsilon + \max\{l(\bar{\xi}_d, \bar{\mathrm{u}}), l^1(\bar{\xi}_d, \bar{\mathrm{u}})\}\\ &\quad - \max\{l(\bar{\xi}_d, \bar{\mathrm{u}}), l^2(\bar{\xi}_d, \bar{\mathrm{u}})\}\\ &\leq 2\varepsilon + |l^1(\bar{\xi}_d, \bar{\mathrm{u}}) - l^2(\bar{\xi}_d, \bar{\mathrm{u}})|\\ &\leq 2\varepsilon + e^{-\gamma T} \max_{x \in \mathbb{R}^n} |V^1(x) - V^2(x)| \quad (63) \end{aligned}$$

The second inequality holds since, for all $a, b, c \in \mathbb{R}$, $|\max\{a,b\} - \max\{a,c\}| \leq |b - c|$. Since the above inequality holds for all $x \in \mathbb{R}^n$ and $\varepsilon > 0$,

$$\|B_T[V^1] - B_T[V^2]\|_{L^\infty(\mathbb{R}^n)} \leq e^{-\gamma T} \|V^1 - V^2\|_{L^\infty(\mathbb{R}^n)}$$

Since V_γ is a fixed-point solution for all $T > 0$, the Banach's contraction mapping theorem [20, Chapter 9.2] implies that V_γ is the unique fixed-point solution to $B_T[V_\gamma](x) = V_\gamma(x)$ for all $T > 0$. In addition, we have

$$\|B_T[V] - V_\gamma\|_{L^\infty(\mathbb{R}^n)} \leq e^{-\gamma T} \|V - V_\gamma\|_{L^\infty(\mathbb{R}^n)}$$

for all $V \in \mathrm{BUC}(\mathbb{R}^n)$, thus we conclude (29). □

G. Proof of Lemma 5

Proof. We will derive the HJ equation for another value function W^+ defined below, and then replace W^+ by W. Define $W^+ : [-T, 0] \times \mathbb{R}^n \to \mathbb{R}$

$$W^+(t,x) = \inf_{\xi_d \in \Xi_d} \sup_{\mathrm{u} \in \mathcal{U}} \min \Big\{ \min_{s \in [t,0]} e^{-\gamma(s-t)}(-h_S(\mathrm{x}(s))), e^{\gamma t}(-V_0(\mathrm{x}(0))) \Big\}, \tag{64}$$

where x solves (50). Then, $W(T,x) = -W^+(-T,x)$, and

$$W(t,x) = -W^+(-t,x), \frac{\partial W}{\partial t}(t,x) = \frac{\partial W^+}{\partial t}(-t,x), \\ \frac{\partial W}{\partial x}(t,x) = -\frac{\partial W^+}{\partial x}(-t,x), \forall (t,x) \in (0,T)\times\mathbb{R}^n. \tag{65}$$

In the rest of the proof, we will utilize the technique presented in [8]. The value function in [8] is

$$\inf_{\xi_d\in\xi_d}\sup_{\mathrm{u}}\min_{s\in[t,0]} e^{-\gamma(s-t)}(-h_S(\mathrm{x}(s))), \tag{66}$$

which is the exactly same as (64) except the second term of the minimization operation: $e^{\gamma t}(-V_0((\mathrm{x}(0)))$. This term affects the terminal condition of W^+ but not the dynamic programming principle. Thus, W^+ and the value function in [8] solves the same dynamic programming principle, but their terminal conditions are different. Note that we assume $\gamma > 0$, but [8] assumes $\gamma \le 0$. However, the sign of γ does not affect any arguments in [8]'s lemmas, theorems.

Using the similar arguments in the proof of [8, Theorem 2], we prove

$$W^+(t,x) = \inf_{\xi_d\in\Xi_d}\sup_{\mathrm{u}\in\mathcal{U}}\min\Big\{\min_{s\in[t,t+\delta]} e^{-\gamma(s-t)}(-h_S(\mathrm{x}(s))), \\ e^{-\gamma\delta}W^+(t+\delta,\mathrm{x}(t+\delta))\Big\}. \tag{67}$$

Then, [8, Theorem 3] implies that W^+ is the unique viscosity solution to the terminal-value HJ equation:

$$W^+(0,x) = -\max\{h_S(x), V_0(x)\} \quad \text{on } \{t=0\}\times\mathbb{R}^n, \tag{68}$$

$$0 = \min\Big\{-h_S(x) - W^+(t,x), \\ \frac{\partial W^+}{\partial t} + \max_u\min_d \frac{\partial W^+}{\partial x}\cdot(-f)(x,u,d) - \gamma W^+(t,x)\Big\}, \tag{69}$$

in $(-T,0)\times\mathbb{R}^n$. By applying (65), we get the conclusion that W is the unique viscosity solution to (31). □

H. Proof of Proposition 4

Proof. (i) At $x \in \mathrm{Int}(S)$ where V_γ is differentiable, the FRT-HJ-VI (26) implies that K_γ is non-empty.
(ii) For any control policy $\pi = \pi(x) \in K_\gamma(x)$, where V_γ is differentiable, consider the following equation for V_γ^π:

$$0 = \min\Big\{V_\gamma^\pi(x) - h_S(x), \min_d \frac{\partial V_\gamma}{\partial x}\cdot f(x,\pi(x),d) + \gamma V_\gamma^\pi(x)\Big\}. \tag{70}$$

For each $x\in\mathbb{R}^n$, $\min\{y - h_S(x), \min_d \frac{\partial V_\gamma}{\partial x}\cdot f(x,\pi(x),d) + \gamma y\}$ is monotonically increasing in $y\in\mathbb{R}$, so the equation (70) has a unique solution. Also, from the FRT-HJ-VI (26),

$$0 = \min\Big\{V_\gamma(x) - h_S(x), \max_u\min_d \frac{\partial V_\gamma}{\partial x}\cdot f(x,u,d) + \gamma V_\gamma(x)\Big\}, \\ \ge \min\Big\{V_\gamma(x) - h_S(x), \min_d \frac{\partial V_\gamma}{\partial x}\cdot f(x,\pi(x),d) + \gamma V_\gamma(x)\Big\} \ge 0. \tag{71}$$

The last inequality holds since $V_\gamma - h_S \ge 0$ by the FRT-HJ-VI (26) and $\min_d \frac{\partial V_\gamma}{\partial x}\cdot f(x,\pi(x),d) + \gamma V_\gamma(x) \ge 0$ since $\pi(x)\in K_\gamma(x)$. The equation (71) and the uniqueness of (70) imply $V_\gamma \equiv V_\gamma^\pi$ for any π. By replacing V_γ by V_γ^π in (70),

$$0 = \min\Big\{V_\gamma^\pi(x) - h_S(x), \min_d \frac{\partial V_\gamma^\pi}{\partial x}\cdot f(x,\pi(x),d) + \gamma V_\gamma^\pi(x)\Big\}. \tag{72}$$

The solution to (72) can be considered as the value function (23) under $\pi(x)$ and worst-case disturbance, and since $V_\gamma \equiv V_\gamma^\pi$, we conclude that any control $u\in K_\gamma(x)$ is an optimal control for the zero-sum game value V_γ in (22). □

I. Proof of Theorem 5

Proof. We will show the two statements as follows.

1) For any smooth function $v\in C^\infty(\mathbb{R}^n)$ such that $V_\gamma - v$ has a local minimum at $x_0\in\mathbb{R}^n$ and $V_\gamma(x_0) = v(x_0)$,

$$0 \le \min\Big\{v(x_0) - h(x_0), \max_{u\in U}\min_{d\in D}\frac{\partial v}{\partial x}(x_0)\cdot f(x_0,u,d) + \gamma v(x_0)\Big\}.$$

2) For any smooth function $v\in C^\infty(\mathbb{R}^n)$ such that $V_\gamma - v$ has a local maximum at $x_0\in\mathbb{R}^n$ and $V_\gamma(x_0) = v(x_0)$,

$$0 \ge \min\Big\{v(x_0) - h(x_0), \max_{u\in U}\min_{d\in D}\frac{\partial v}{\partial x}(x_0)\cdot f(x_0,u,d) + \gamma v(x_0)\Big\}.$$

Case 1. $V_\gamma(x_0) = h(x_0) > 0$: By the continuity of h, there exists $\varepsilon > 0$ such that $V_\gamma(y) = h(y)$ for all $y\in B_\varepsilon(x_0)$. Thus, the gradient of V_γ at x_0 exists: $\frac{\partial V_\gamma}{\partial x}(x_0) = \frac{\partial h}{\partial x}(x_0)$, so for any v such that $V_\gamma - v$ has either a local minimum or a local maximum at x_0, $\frac{\partial v}{\partial x}(x_0) = \frac{\partial h}{\partial x}(x_0)$. From (38),

$$\max_{u\in U}\min_{d\in D}\frac{\partial v}{\partial x}(x_0)\cdot f(x_0,u,d) + \gamma v(x_0) = 0. \tag{73}$$

Therefore, Statements 1) and 2) hold in this case.

Case 2. $V_\gamma(x_0) = 0 > h(x_0)$: By the continuity of h, there exists $\varepsilon > 0$ such that $V_\gamma(y) = 0$ for all $y\in B_\varepsilon(x_0)$. This implies that the gradient of V_γ at x_0 is $0\in\mathbb{R}^n$, so for any v such that $V_\gamma - v$ has either a local minimum or a local maximum at x_0, $\frac{\partial v}{\partial x}(x_0) = 0$. Thus, (73) holds. Therefore, Statements 1) and 2) hold in this case.

Case 3. $V_\gamma(x_0) = 0 = h(x_0)$: From $v(x_0) - h(x_0) = 0$, it is trivial that 2) holds, and we focus on the proof of 1). Since $V_\gamma - v$ has a local minimum at x_0, $\frac{\partial v}{\partial x}(x_0)\in\partial^- V_\gamma(x_0)$, where $\partial^- V_\gamma(x_0)$ is the sub-differential, which is determined as

$$\partial^- V_\gamma(x_0) = \mathrm{conv}\left(\{0\}\cup\left\{\frac{\partial h}{\partial x}(x_0)\right\}\right),$$

where conv is a convex-hull operator. Thus, $\frac{\partial v}{\partial x}(x_0) = \alpha\frac{\partial h}{\partial x}(x_0)$ for some $\alpha\in[0,1]$. Thus, from (38) and $v(x_0) = 0$, (73) holds and therefore, 1) holds. □

J. 1D example: comparison of reachability methods in Table I

We consider a simple one-dimensional system described by

$$\dot{\mathrm{x}}(t) = \mathrm{x}(t) + \mathrm{u}(t), \mathrm{x}(0) = x, \tag{74}$$

where $u\in U = [-1,1]$. We consider the state domain $x\in[0,\infty)$. We consider the set $S = [0,2]$, and choose h_S as $h_S(x) = \max\{2-x,-2\}$. Basically, it is a distance function cut off at the absolute value of 2 (Figure 8 grey). For this example, we compare the results of the three backward reachability formulations studied in the previous literature [7]–[10], [16] with our forward reachability formulation, as summarized in Table I. We use $\gamma = 2$ in all formulations. Note that the chosen S is *not* control invariant, thus, the example is chosen not for the reachability analysis of control invariant sets, but to study the boundedness, continuity, and the solution uniqueness of the resulting value functions. The viability kernel of S, the maximal control invariant set contained in S, is $[0,1]$, since at $x = 1$, $\dot{x}$ can be maintained 0 by selecting the saturated control input $u = -1$, but for every x exceeding 1, $\dot{x} > 0$ for any admissible control input value. Also, we did not introduce disturbance for simplicity, thus, the readers may assume no effect of disturbance strategies ξ_d on the value functions defined in each formulation.

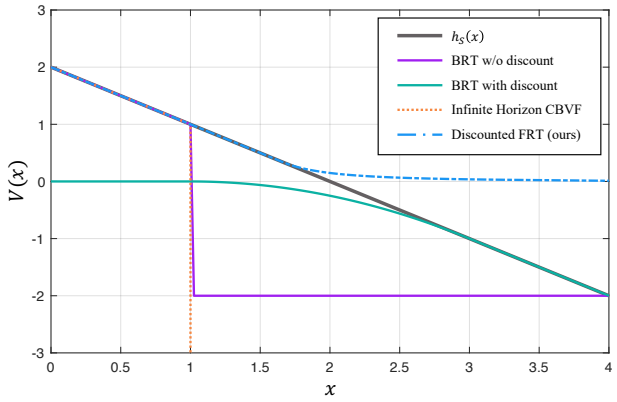

Fig. 8. Various reachability value functions, summarized in Table I, for the 1D example in (74). Only the formulations with the discounted factor (green and blue), including the one proposed in this work produce value functions that are bounded and continuous.

1) Backward Reachable Tube (BRT) without discount factor [7], [36]:

$$V(x) := \inf_{\xi_d \in \Xi_d} \sup_{\mathrm{u} \in \mathcal{U}} \inf_{t \in [0,\infty)} h_S(\mathrm{x}(t)), \tag{75}$$

which characterizes the viability kernel of S as $\{x | V(x) \geq 0\}$, which can be seen in Figure 8 (purple). The value function is discontinuous at $x = 1$. Moreover, the corresponding HJ-PDE, given as

$$0 = \min \left\{ h_S(x) - V(x), \max_u \min_d \frac{\partial V}{\partial x} \cdot f(x,u,d) \right\} \tag{76}$$

admits non-unique solutions, for instance, $V(x) \equiv -2$ in this example is also a valid viscosity solution to (76).

2) Discounted BRT with discount factor [9], [10]:

$$V(x) := \inf_{\xi_d \in \Xi_d} \sup_{\mathrm{u} \in \mathcal{U}} \inf_{t \in [0,\infty)} e^{-\gamma t} h_S(\mathrm{x}(t)). \tag{77}$$

In this case, as can be seen in Figure 8 (green), the value function is continuous and bounded. However, the main issue of this formulation is that the value function is flat inside the viability kernel, which is characterized as $\{x | V(x) = 0\}$.

3) Infinite horizon CBVF [8], [16]:

$$V(x) := \inf_{\xi_d \in \Xi_d} \sup_{\mathrm{u} \in \mathcal{U}} \inf_{t \in [0,\infty)} e^{\gamma t} h_S(\mathrm{x}(t)). \tag{78}$$

Notice the flip of sign in the factor of the exponential term, compared to (77). This formulation results in an HJ-PDE whose differential inequality matches the form of the barrier constraint. However, it results in discontinuity and unboundedness of the value function, as can be seen in Figure 8 (orange).

4) Our formulation: The value function is defined in (22), which is bounded and continuous, as can be seen in Figure 8 (blue). Also, this formulation admits a unique solution to the corresponding HJ-PDE in (26), and the differential inequality in the PDE matches the form of the barrier constraint. Note that in this example, $FRT(\mathrm{Int}(S))$ is $[0, \infty)$, thus, in Figure 8, $V(x) > 0$ everywhere.

References

[1] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[2] K. P. Wabersich, A. J. Taylor, J. J. Choi, K. Sreenath, C. J. Tomlin, A. D. Ames, and M. N. Zeilinger, "Data-driven safety filters: Hamilton-Jacobi reachability, control barrier functions, and predictive methods for uncertain systems," *Preprint*, 2023.

[3] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117–126, 2006.

[4] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Trans. on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[5] D. Bertsekas, "Infinite time reachability of state-space regions by using feedback control," *IEEE Trans. on Automatic Control*, vol. 17, no. 5, pp. 604–613, 1972.

[6] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, "A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games," *IEEE Trans. on Automatic Control*, vol. 50, no. 7, pp. 947–957, 2005.

[7] J. F. Fisac, A. K. Akametalu, M. N. Zeilinger, S. Kaynama, J. Gillula, and C. J. Tomlin, "A general safety framework for learning-based control in uncertain robotic systems," *IEEE Trans. on Automatic Control*, vol. 64, no. 7, pp. 2737–2752, 2019.

[8] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, "Robust control barrier–value functions for safety-critical control," in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 6814–6821.

[9] A. K. Akametalu, S. Ghosh, J. F. Fisac, and C. J. Tomlin, "A minimum discounted reward hamilton-jacobi formulation for computing reachable sets," *arXiv:1809.00706*, 2018.

[10] B. Xue, Q. Wang, N. Zhan, M. Fränzle, and S. Feng, "Reach-avoid differential games based on invariant generation," *arXiv:1811.03215*, 2018.

[11] I. M. Mitchell, "Comparing forward and backward reachability as tools for safety analysis," in *Hybrid Systems: Computation and Control: 10th International Workshop, HSCC 2007, Pisa, Italy, April 3-5, 2007. Proceedings 10*. Springer, 2007, pp. 428–443.

[12] M. Althoff and J. M. Dolan, "Online verification of automated road vehicles using reachability analysis," *IEEE Trans. on Robotics*, vol. 30, no. 4, pp. 903–918, 2014.

[13] S. Kousik, S. Vaskov, F. Bu, M. Johnson-Roberson, and R. Vasudevan, "Bridging the gap between safety and real-time performance in receding-horizon trajectory design for mobile robots," *The Int. J. of Robotics Research*, vol. 39, no. 12, pp. 1419–1469, 2020.

[14] M. Wetzlinger, N. Kochdumper, S. Bak, and M. Althoff, "Fully-automated verification of linear systems using inner-and outer-approximations of reachable sets," *arXiv preprint arXiv:2209.09321*, 2022.

[15] P. Cardaliaguet, "A differential game with two players and one target," *SIAM Journal on Control and Optimization*, vol. 34, no. 4, pp. 1441–1460, 1996.

[16] S. Tonkens and S. Herbert, "Refining control barrier functions through hamilton-jacobi reachability," in *2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2022, pp. 13 355–13 362.

[17] M. Bardi, I. C. Dolcetta *et al.*, *Optimal control and viscosity solutions of Hamilton-Jacobi-Bellman equations*. Springer, 1997, vol. 12.

[18] F. H. Clarke, Y. S. Ledyaev, R. J. Stern, and P. R. Wolenski, *Nonsmooth analysis and control theory*. Springer Science & Business Media, 2008, vol. 178.

[19] J.-P. Aubin, A. M. Bayen, and P. Saint-Pierre, *Viability theory: new directions*. Springer Science & Business Media, 2011.

[20] L. C. Evans, *Partial differential equations*. American Mathematical Soc., 2010, vol. 19.

[21] G. Lieberman, "Regularized distance and its applications," *Pacific journal of Mathematics*, vol. 117, no. 2, pp. 329–352, 1985.

[22] M. Nagumo, "Über die lage der integralkurven gewöhnlicher differentialgleichungen," *Proc. of the Physico-Mathematical Society of Japan. 3rd Series*, vol. 24, pp. 551–559, 1942.

[23] P. Ogren, A. Backlund, T. Harryson, L. Kristensson, and P. Stensson, "Autonomous ucav strike missions using behavior control lyapunov functions," in *AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2006, p. 6197.

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

[25] M. Jankovic, "Robust control barrier functions for constrained stabilization of nonlinear systems," *Automatica*, vol. 96, pp. 359–367, 2018.

[26] S. Kolathaya and A. D. Ames, "Input-to-state safety with control barrier functions," *IEEE Control Sys. Let.*, vol. 3, no. 1, pp. 108–113, 2018.

[27] M. Krstic, "Inverse optimal safety filters," *arXiv preprint arXiv:2112.08225*, 2021.

[28] L. C. Evans and P. E. Souganidis, "Differential games and representation formulas for solutions of hamilton-jacobi-isaacs equations," *Indiana University mathematics journal*, vol. 33, no. 5, pp. 773–797, 1984.

[29] A. Alan, A. J. Taylor, C. R. He, A. D. Ames, and G. Orosz, "Control barrier functions and input-to-state safety with application to automated vehicles," *arXiv:2206.03568*, 2022.
[30] S. Kousik, P. Holmes, and R. Vasudevan, "Safe, aggressive quadrotor flight via reachability-based trajectory design," in *Proc. ASME Dynamic Sys. and Control Conf. (DSCC)*, vol. 59162, Park City, UT, USA, 2019, p. V003T19A010.
[31] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *Proc. IEEE 56th Conf. on Decision and Control (CDC)*, Melbourne, VIC, Australia, 2017, pp. 2242–2253.
[32] I. M. Mitchell and J. A. Templeton, "A toolbox of hamilton-jacobi solvers for analysis of nondeterministic continuous and hybrid systems," in *Int. Work. on Hybrid Sys.: Computation and Control*. Springer, 2005, pp. 480–494.
[33] D. Mugnaini. (2023) Bezier curve with draggable control points. GitHub. Retrieved August 25, 2023. [Online]. Available: https://github.com/ducciomugnaini/Bezier-Curve-with-draggable-control-points/releases/tag/1.11.0.1
[34] J. Lygeros, "On reachability and minimum cost optimal control," *Automatica*, vol. 40, no. 6, pp. 917–927, 2004.
[35] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry, "Reach-avoid problems with time-varying dynamics, targets and constraints," in *Proc. of the 18th Int. Conf. on Hybrid Sys.: Computation and Control (HSCC)*, Seattle, WA, USA, 2015, pp. 11–20.
[36] S. L. Herbert, S. Bansal, S. Ghosh, and C. J. Tomlin, "Reachability-based safety guarantees using efficient initializations," in *Proc. IEEE 58th Conf. on Decision and Control (CDC)*, Nice, France, 2019, pp. 4810–4816.

Jason J. Choi (Student Member, IEEE) received the B.S. degree in mechanical engineering from Seoul National University in 2019. He is currently pursuing a Ph.D. degree at University of California Berkeley in mechanical engineering. His research interests center on optimal control theories for nonlinear and hybrid systems, data-driven methods for safe control, and their applications to robotics and autonomous mobility.

Donggun Lee is an Assistant Professor in the Department of Mechanical and Aerospace Engineering at North Carolina State University. He obtained his Ph.D. in Mechanical Engineering from UC Berkeley in 2016. Prior to that, he earned his B.S. and M.S. degrees in Mechanical Engineering from the Korea Advanced Institute of Science and Technology (KAIST) in Daejeon, Korea, in 2009 and 2011, respectively. His current focus lies in the field of control theory and robotics.

Boyang Li (bol025@ucsd.edu) received a B.S. degree in Mathematics and Physics (double major) from William & Mary in May 2022. He is currently pursing a Ph.D. degree in Mechanical Engineering at UC San Diego. Boyang is interested in developing control methodologies that possess both mathematical formality and versatility in application to various robotics systems, drawing ideas from optimization theory, dynamical systems, and deep learning.

Jonathan P. How (Fellow, IEEE) received the B.A.Sc. degree from the University of Toronto (1987), and the S.M. and Ph.D. degrees in aeronautics and astronautics from MIT (1990 and 1993). Prior to joining MIT in 2000, he was an Assistant Professor at Stanford University. He is currently the Richard C. Maclaurin Professor of aeronautics and astronautics at MIT. Some of his awards include the IEEE CSS Distinguished Member Award (2020), AIAA Intelligent Systems Award (2020), IROS Best Paper Award on Cognitive Robotics (2019), and the AIAA Best Paper in Conference Awards (2011, 2012, 2013). He was the Editor-in-chief of IEEE Control Systems Magazine (2015–2019), is a Fellow of AIAA, and was elected to the National Academy of Engineering in 2021.

Koushil Sreenath (Member, IEEE) is an associate professor of mechanical engineering, at UC Berkeley. He received a Ph.D. degree in electrical engineering and computer science and a M.S. degree in applied mathematics from the University of Michigan at Ann Arbor, MI, in 2011. He was a postdoctoral scholar at the GRASP Lab at University of Pennsylvania from 2011 to 2013 and an assistant professor at Carnegie Mellon University from 2013 to 2017. His research interest lies at the intersection of highly dynamic robotics and applied nonlinear control. He received the NSF CAREER, Hellman Fellow, Best Paper Award at the Robotics: Science and Systems (RSS), and the Google Faculty Research Award in Robotics.

Sylvia L. Herbert (sherbert@ucsd.edu) is an Assistant Professor at UC San Diego. She received her Ph.D. from UC Berkeley in Electrical Engineering and Computer Sciences in 2020. She works in the area of safe control for autonomous systems. She is the recipient of an ONR Young Investigator Award, the UC Berkeley Chancellor's Fellowship, and the Berkeley EECS Demetri Angelakos Memorial Achievement Award for Altruism.

Claire J. Tomlin (Fellow, IEEE) is the James and Katherine Lau Professor of Engineering and professor and chair of the Department of Electrical Engineering and Computer Sciences (EECS) at UC Berkeley. She was an assistant, associate, and full professor in aeronautics and astronautics at Stanford University from 1998 to 2007, and in 2005, she joined UC Berkeley. She works in the area of control theory and hybrid systems, with applications to air traffic management, UAV systems, energy, robotics, and systems biology. She is a MacArthur Foundation Fellow (2006), an IEEE Fellow (2010), and in 2017, she was awarded the IEEE Transportation Technologies Award. In 2019, Claire was elected to the National Academy of Engineering and the American Academy of Arts and Sciences.