2021 60th IEEE Conference on Decision and Control (CDC)
December 13-15, 2021. Austin, Texas

2021 60th IEEE Conference on Decision and Control (CDC) | 978-1-6654-3659-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CDC45484.2021.9683085

Robust Control Barrier–Value Functions for Safety-Critical Control

Jason J. Choi, Donggun Lee, Koushil Sreenath, Claire J. Tomlin, and Sylvia L. Herbert

Abstract— **This paper works towards unifying two popular approaches in the safety control community: Hamilton-Jacobi (HJ) reachability and Control Barrier Functions (CBFs). HJ Reachability has methods for direct construction of value functions that provide safety guarantees and safe controllers, however the online implementation can be overly conservative and/or rely on chattering bang-bang control. The CBF community has methods for safe-guarding controllers in the form of point-wise optimization using quadratic programs (CBF-QP), where the CBF-based safety certificate is used as a constraint. However, finding a valid CBF for a general dynamical system is challenging. This paper unifies these two methods by introducing a new reachability formulation inspired by the structure of CBFs to construct a Control Barrier-Value Function (CBVF). We verify that CBVF is a viscosity solution to a novel Hamilton-Jacobi-Isaacs Variational Inequality and preserves the same safety guarantee as the original reachability formulation. Finally, inspired by the CBF-QP, we propose a QP-based online control synthesis for systems affine in control and disturbance, whose solution is always the CBVF's optimal control signal robust to bounded disturbance. We demonstrate the benefit of using the CBVFs for double-integrator and Dubins car systems by comparing it to previous methods.**

I. Introduction

A. Motivation & Related Work

Value function-based approaches are common techniques for solving safe control problems. Two such methods are Hamilton-Jacobi (HJ) reachability analysis and Control Barrier Functions (CBFs). HJ reachability analysis formulates the reachability of a target set as an optimal control problem, and has long been used as a formal theoretical tool for safety analysis and synthesis of safe controllers [1], [2]. HJ reachability-based value functions can be solved numerically by using the dynamic programming principle [3]. The zero-superlevel set of the value function describes the safe set, and the optimal safety controller can be synthesized based on the gradient of the function. Moreover, the safe control can be robust to disturbances [2].

The main drawbacks of HJ reachability analysis are twofold. First, although there have been recent advances to improve computational efficiency [4], [5], [6], most numerical methods to construct the value function suffer from the curse of dimensionality [7]. Secondly, the resulting safe optimal control policy is generally overly conservative when applied directly. A popular remedy for reducing conservativeness is to use a least-restrictive hybrid controller–the optimal control is only applied when the system is very close to the safe boundary. However, this switching-based control law often results in undesirable jerky behaviors.

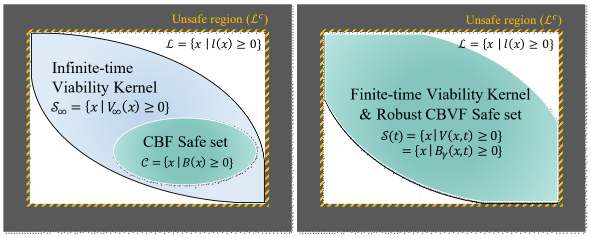
Unsafe region ($\mathcal{L}^c$)
$\mathcal{L} = \{x \mid l(x) \geq 0\}$
Infinite-time
Viability Kernel
$\mathcal{S}_\infty = \{x \mid V_\infty(x) \geq 0\}$
CBF Safe set
$\mathcal{C} = \{x \mid B(x) \geq 0\}$
Unsafe region ($\mathcal{L}^c$)
$\mathcal{L} = \{x \mid l(x) \geq 0\}$
Finite-time Viability Kernel
& Robust CBVF Safe set
$\mathcal{S}(t) = \{x \mid V(x,t) \geq 0\}$
$= \{x \mid B_\gamma(x,t) \geq 0\}$

Fig. 1. Illustrative diagram of the viability kernel and the zero-superlevel sets of the functions presented in the paper. The gray region represents the failure set that should not be entered. The constraint set $\mathcal{L}$ is seen in white. On the left, the infinite-time viability kernel generated by HJ reachability is shown in blue, with the CBF safe set being a guaranteed under-approximation. On the right, the finite-time viability kernel is generally larger than the infinite-time version, as there exists more states that can be safe for only a finite time horizon. The zero-superlevel set of the proposed Robust CBVF B_γ matches the viability kernel, the maximal robust safe set.

Recently, Control Barrier Functions (CBFs) have gained popularity among the controls and robotics community as a convenient way of solving safe control problems [8], [9]. CBFs are Lyapunov-like functions that impose certain state-dependent constraints on the control input. The constraint results in control invariance of the zero-superlevel set of CBFs, and this property can be used to ensure that the system stays within a desired safe region. The main benefit of using a CBF for safety control is that for control-affine systems, the CBF constraint can be incorporated in an online min-norm optimization based controller, namely the CBF-based Quadratic Program (CBF-QP). The fact that this controller can be applied in real-time for high-dimensional systems makes it attractive for many applications [10], [11], [12]. Also, it can be used as an automatic safety filter (as opposed to using least-restrictive control) [13], [14], [15].

The main drawback of CBF-based approaches is that they lack general methods of constructing a valid CBF, which results in using hand-designed or application-specific CBFs [10], [12]. This may restrict the system to stay only in a conservative safe region defined by a CBF's zero-superlevel set. Another problem arises when the system has control input bounds: the CBF may be invalid under these bounds, causing the CBF-QP to become infeasible anytime. A new QP formulation proposed recently provides pointwise feasibility but not persistent feasibility [16].

In summary, HJ reachability analysis and CBF-based safety control are complementary in many ways. HJ reachability provides constructive methods for the value functions, whereas the CBF community usually has to deal with handcrafting a valid CBF. Also, HJ-based value functions

This research is supported in part by the DARPA Assured Autonomy program, National Science Foundation Grant CMMI-1931853 and UCSD.
Jason Choi, Donggun Lee, Koushil Sreenath, and Claire Tomlin are with University of California, Berkeley, and Sylvia Herbert is with University of California, San Diego. Contact info: {jason.choi, donggun_lee, koushils, tomlin}@berkeley.edu, sherbert@ucsd.edu

result in the maximal safe region for a desired safety constraint, whereas CBFs often can only provide a conservative estimate of safe region. On the other hand, online CBF-based safety controllers like the CBF-QP are a powerful tool to apply CBFs to high-dimensions systems in real-time applications, whereas HJ reachability suffers from the curse of dimensionality and its value function's online deployment is not straightforward due to the optimal policy's restrictive behavior. A recent paper uses HJ reachability functions as CBFs [13], but a theoretical understanding of the relationship between the two methods is still lacking.

B. Paper Organization and Contributions

In light of the fact that reachability-based value functions and CBFs are tackling a similar problem in complementary ways, we unify the two functions theoretically. First, in Sec. II we briefly summarize and compare the concept of a value function from HJ reachability and CBFs.

In Sec. III we introduce the notion of a *Robust Control Barrier-Value function* (CBVF) that merges reachability-based value functions and CBFs into one function. This function (a) can be used for finite-time safety guarantees, (b) is robust to bounded disturbances, (c) recovers the maximal safe set for a desired safety constraint, and (d) leads to a safety control that satisfies the control bound everywhere inside the safe set. The main theoretical contribution is a verification that the CBVF is a viscosity solution of a particular Hamilton-Jacobi-Isaacs variational inequality (HJI-VI), and this can be used to numerically construct a valid CBVF. This constructive method does not naturally scale well, but can benefit from methods from the reachability community that enhance scalability [4], [5], [17].

In Sec. IV, we introduce the optimal control policy corresponding to the CBVF. This controller is less conservative than that from the original HJ reachability, and is less jerky than using the least-restrictive controller that is commonly applied in HJ reachability. For systems affine in control and disturbance, we show that such an optimal controller can be obtained by solving a QP, namely the *Robust CBVF-QP*. In Sec. V, we demonstrate this findings on numerical examples by comparing the CBVF-based safety control with the original HJ reachability and CBF-based methods.

II. Background

A. Problem Formulation

Consider a state trajectory of the continuous-time time-invariant controlled system with disturbance, solving

$$\dot{\mathrm{x}}(s) = f(\mathrm{x}(s), u(s), d(s)), \;\; s \in [t, t'], \quad \text{and } \mathrm{x}(t) = x, \quad (1)$$

where t and x are the initial time and state, respectively. $u \in U \subset \mathbb{R}^m$ is the control input, $d \in D \subset \mathbb{R}^w$ is the disturbance where U, D are compact and convex sets, and $f : \mathbb{R}^n \times U \times D \to \mathbb{R}^n$ is Lipschitz continuous in the state and bounded. Let $\mathcal{U}_{[t,t']}$, $\mathcal{D}_{[t,t']}$ be a set of Lebesgue measurable functions from the time interval $[t, t']$ to U and D, respectively. For simplicity, we set the final time as 0. For every initial time $t \leq 0$, initial state $x \in \mathbb{R}^n$, $u(\cdot) \in \mathcal{U}_{[t,0]}$, and $d(\cdot) \in \mathcal{D}_{[t,0]}$, system (1) admits a unique solution trajectory. We denote this *trajectory* as $\mathrm{x}(s)$, and will say that "$\mathrm{x}(\cdot)$ solves (1) for (x, t, u, d)" with a slight abuse of notation.

Throughout the paper, we assume that the disturbance signal $d(\cdot)$ can be determined in reaction to the control signal in a form of a strategy $\xi_d : \mathcal{U}_{[t,0]} \to \mathcal{D}_{[t,0]}$. However, we restrict it to draw only from *nonanticipative strategies* with respect to $u(\cdot)$, denoted as $\xi_d \in \Xi_{[t,0]}$. The nonanticipative strategy prohibits the use of future information of the control signal to make a decision of the disturbance at each time [18].

Now consider a set $\mathcal{L}$ defined as a zero-superlevel set of a bounded Lipschitz continuous function $l : \mathbb{R}^n \to \mathbb{R}$:

$$\mathcal{L} = \{x : l(x) \geq 0\}. \quad (2)$$

The objective of the safety control is to guarantee the trajectory to stay in $\mathcal{L}$ for $s \in [t, 0]$ under the worst case disturbance. We refer to $l(x)$ as the *safety target function*. More formally, we are interested in the following problems:

- **Computing the viability kernel $\mathcal{S}(t)$ [1] for $\mathcal{L}$:** Verify $\mathcal{S}(t) := \{x \in \mathcal{L} : \forall \xi_d \in \Xi_{[t,0]}, \exists u(\cdot) \in \mathcal{U}_{[t,0]} \text{ s.t. } \forall s \in [t, 0], \mathrm{x}(s) \in \mathcal{L} \text{ where } \mathrm{x}(s) \text{ solves (1) for } (x, t, u, \xi_d)\}$ for $t < 0$. $\mathcal{S}(t)$ is the set of all the initial states at time t in $\mathcal{L}$ from which there exists an admissible control signal that keeps the system safe under the worst-case disturbance.
- **Computing a robust safe control $u(\cdot)$ for $\mathcal{L}$:** For each $x \in \mathcal{S}(t)$, verify a control signal $u(\cdot) \in \mathcal{U}_{[t,0]}$ that renders the trajectory safe for $s \in [t, 0]$, under the worst-case disturbance.

B. Hamilton-Jacobi Reachability Analysis

It has been verified that solving for the viability kernel and the robust safe control signal can be posed as an optimal control problem, which can be solved using HJ reachability analysis [1], [2], [19]. First, we define a cost function as

$$J(x, t, u(\cdot), d(\cdot)) := \min_{s \in [t,0]} l(\mathrm{x}(s)), \quad (3)$$

which captures the minimal value of $l(\cdot)$ along the trajectory $\mathrm{x}(\cdot)$ that solves (1) for (x, t, u, d). If $\exists s \in [t, 0]$ such that $J(x, t, u(s), d(s)) < 0$, it means that the trajectory was violating the safety constraint at some point in the time horizon (obtaining a negative value of l), and is therefore unsafe. The objective of the safety control is to make J as big as possible, whereas under the worst case, the disturbance would act in a direction of decreasing J as much as it can. Based on this, we can define the value function $V : \mathbb{R}^n \times (-\infty, 0] \to \mathbb{R}$ as

$$V(x, t) := \min_{\xi_d \in \Xi_{[t,0]}} \max_{u \in \mathcal{U}_{[t,0]}} J(x, t, u(\cdot), \xi_d[u](\cdot)), \quad (4)$$

Then, by the following proposition, the viability kernel for $\mathcal{L}$ is $\mathcal{S}(t) = \{x \in \mathbb{R}^n : V(x, t) \geq 0\}$. Note that the minimum and maximum in $\Xi_{[t,0]}$,$\mathcal{U}_{[t,0]}$ always exists because U and D are compact and convex [20].

Proposition 1. For all $t \leq 0$, the viability kernel for $\mathcal{L}$, $\mathcal{S}(t)$, always is $\{x \in \mathbb{R}^n : V(x, t) \geq 0\}$.

Proof. This is directly from the definition of V and $\mathcal{S}(t)$. □

Note that if $\mathcal{S}(t)$ is empty, safety can never be guaranteed under the worst-case disturbance. In the complement of $\mathcal{S}(t)$, the value function $V(x,t)$ is negative, therefore, for any admissible control, the trajectory is unsafe under the worst-case disturbance. This set $\mathcal{S}(t)^c$ describes what is known in the HJ Reachability community as a *Backward Reachable Tube* of the unsafe set.

The value function $V(x,t)$ is the viscosity solution to the following Hamilton-Jacobi-Isaacs Variational Inequality (HJI-VI) [19]:

$$0 = \min\Big\{ l(x) - V(x,t), \quad D_t V(x,t) + \max_{u\in U}\min_{d\in D} D_x V(x,t)\cdot f(x,u,d) \Big\} \tag{5}$$

with the terminal condition $V(x,0) = l(x)$. This means that $V(x,t)$ can be computed directly using dynamic programming backwards in time by applying the HJI-VI at each point in the state space.

Remark 1. The viscosity solution $V(x,t)$ is a weak solution to (5): $V(x,t)$ is not differentiable for some (x,t). Under the Lipschitz assumptions for the dynamics (f) and the cost (l) in the state, $V(x,t)$ is Lipschitz continuous, which is differentiable almost everywhere (a.e.) in (x,t)-space [18, Th.3.2.][21].

When the viability kernel $\mathcal{S}(t)$ is non-empty, from any element in $\mathcal{S}(t)$, we can synthesize a robust safe control signal from the optimal control policy. Based on whether the left or the right term in the minimum of (5) is *active*, the optimal policy $\pi^*_V(x,t): \mathbb{R}^n \times (-\infty, 0] \to U$ is determined in a different way. That is, when $V(x,t) < l(x)$,

$$\pi^*_V(x,t) = \arg\max_{u\in U}\min_{d\in D} D_x V(x,t)\cdot f(x,u,d), \tag{6}$$

and the right term of (5) is 0. Second, when $V(x,t) = l(x)$, any element of

$$K_V(x,t) := \{u \in U : D_t V(x,t) + \min_{d\in D} D_x V(x,t)\cdot f(x,u,d) \geq 0\} \tag{7}$$

can be used as $\pi^*_V(x,t)$. Therefore, the second case may allow multiple options for the optimal control. In either case, for any $d \in D$,

$$\begin{aligned}\dot{V}(\mathrm{x}(t),t) &= D_t V(\mathrm{x}(t),t) \\ &\quad + D_x V(\mathrm{x}(t),t)\cdot f(\mathrm{x}(t), \pi^*_V(\mathrm{x}(t),t), d) \geq 0,\end{aligned}$$

where $\mathrm{x}(\cdot)$ is an instantaneous trajectory of (1) at t with $\mathrm{x}(t) = x$, control $\pi^*_V(x,t)$ and disturbance d. Therefore, this implies that for any initial state $x \in \mathcal{S}(t)$, for any $\xi_d \in \Xi_{[t,0]}$, along the optimal trajectory $\mathrm{x}^*(\cdot)$ which solves (1) for $(x, t, \pi^*_V, \xi_d[\pi^*_V])$, the value function $V(\mathrm{x}^*(s), s)$ will never decrease. Since V is non-negative at the initial time t, it is always kept non-negative under π^*_V for $s \in [t, 0]$, which means the trajectory is rendered safe.

Remark 2. Note that for the second case of π^*_V, for any optimal $u \in K_V(x,t)$ and any $d \in D$,

$$\dot{l}(\mathrm{x}(t)) = \dot{V}(\mathrm{x}(t),t) \geq 0, \tag{8}$$

where $\mathrm{x}(\cdot)$ is an instantaneous trajectory of (1) at t with $\mathrm{x}(t) = x$, control u and disturbance d. This means that for the second case, π^*_V requires l to increase, in other words, it never allows the trajectory to get closer to the safety boundary. Therefore, such optimal control policy is often too restrictive to be used as a safety filter for a reference control signal. In the reachability community, to remedy this, a common practice is to switch from the reference control to the safe optimal control only when $V(\mathrm{x}(s), s)$ is close to 0, so called least-restrictive control law [17], [22], [23]. The resulting control system with such switching law may give undesirable jerky behaviors and is prone to errors in numerically computed $D_x V$.

C. Control Barrier Functions

An alternative approach for achieving the safety control objective is to use Control Barrier Functions (CBFs). The theory of CBFs is developed upon viability theory and Lyapunov-based stability theory [9].

Definition 1. Let $\mathcal{C}$ be a zero-superlevel set of a continuously differentiable function $B: \mathbb{R}^n \to \mathbb{R}$. Consider a Lipschitz continuous controlled system without disturbance, $f = f(\mathrm{x}(s), u(s))$. Then B is a *Control Barrier Function* for this system if there exists an extended class $\mathcal{K}_\infty$ function α such that for all $x \in \mathcal{C}$,

$$\max_{u\in U} D_x B(x)\cdot f(x,u) \geq -\alpha(B(x)). \tag{9}$$

Introducing $-\alpha(B(x))$ on the right hand side of (9) is inspired by the condition that Control Lyapunov Functions (CLFs) should satisfy in order to provide exponential stabilizability [9]. In practice, a linear function γz ($\gamma > 0$) is often used as $\alpha(z)$. In this case, γ serves as a *maximal discount rate* of $B(\mathrm{x}(s))$. Informally, this means that $B(\mathrm{x}(s))$ is not allowed to decay faster than the exponentially decaying curve $\dot{B}(\mathrm{x}(s)) = -\gamma B(\mathrm{x}(s))$, therefore potential unsafe behaviors smooth out as it approaches the safe boundary. More formally, the following holds:

Theorem 1. [9, Corollary 2] For such B and its zero-superlevel set $\mathcal{C}$, any Lipschitz continuous controller $\pi : \mathcal{C} \to U$ such that $\pi(x) \in K_B(x)$ where

$$K_B(x) := \{u \in U : D_x B(x)\cdot f(x,u) \geq -\alpha(B(x))\}, \tag{10}$$

will render the set $\mathcal{C}$ forward invariant [9]. In other words, $\mathcal{C}$ is control invariant.

Condition (9) can be incorporated in an online optimization based controller that minimizes the norm of the difference between u and the reference control u_{ref}. For control-affine systems, this can become a Quadratic Program, namely Control Barrier Function-based Quadratic Program (CBF-QP) [9], and can be used as an online safety filter for any reference control signal u_{ref}.

D. Comparison between HJ reachability and CBF

In this subsection, we restrict our interest to systems without disturbance, $f = f(\mathrm{x}(s), u(s))$, for the comparison between value function from the reachability V and CBF B. Note that by extending the definition of V to infinite-time horizon as $V_\infty(x) := \lim_{t\to-\infty} V(x,t)$, we can get a time-invariant value function [24] whose zero-superlevel set $\mathcal{S}_\infty := \{x : V_\infty(x) \geq 0\}$ is a maximal control invariant set contained in $\mathcal{L}$. The latter results from extending Proposition 1 to infinite horizon.

The geometric connection between the zero-superlevel set of the CBF B, $\mathcal{C}$, and the zero-superlevel set of V_∞, $\mathcal{S}_\infty$, is that $\mathcal{C}$ is always a subset of $\mathcal{S}_\infty$. This is because in order to use B for our safety objective (2), the control invariant set $\mathcal{C}$ should be a subset of $\mathcal{L}$, as shown in Fig. 1. Since $\mathcal{S}_\infty$ is the maximal control invariant set in $\mathcal{L}$, $\mathcal{C} \subseteq \mathcal{S}_\infty$.

Also, note that V_∞ satisfies the CBF condition (9) for any extended class $\mathcal{K}_\infty$ function α where the gradient $D_x V_\infty$ exists, from the fact, $D_t V_\infty = 0$, and the HJI-VI (5):

$$\max_{u\in U} D_x V_\infty(x) \cdot f(x,u) \geq 0 \geq -\alpha(V_\infty(x)).$$

This implies that if V_∞ is differentiable in $\mathcal{S}_\infty$, then setting $B = V_\infty$ works as a valid CBF with $\mathcal{C} = \mathcal{S}_\infty$. However, if it is not the case, it is hard to devise a CBF such that its zero-superlevel set recovers the maximal control invariant set in $\mathcal{L}$ without relaxing its differentiability condition. Note that choosing $B = l$, which makes $\mathcal{C} = \mathcal{L}$, would not be a valid CBF in general. In many cases, a valid handcrafted CBF results in its zero-superlevel set C strictly smaller than $\mathcal{S}_\infty$.

III. Robust Control Barrier-Value Function and Hamilton-Jacobi-based Verification

Note that the condition the CBF-based safe control should satisfy, $D_x B(x) \cdot f(x,u) \geq -\alpha(B(x))$, from Theorem 1, is less restrictive than the condition the optimal control for V should satisfy, $\min_{d\in D} D_x V(x,s) \cdot f(x,u,d) \geq 0$. This is mainly because of the introduction of $-\alpha(\cdot)$ on the right hand side of (9). Inspired by this and the fact that when $\alpha(B(x)) \equiv \gamma B(x)$, γ serves as the maximal discount rate of B, we define the following new value function.

Definition 2. A Robust Control Barrier-Value Function (CBVF) $B_\gamma : \mathbb{R}^n \times (-\infty, 0] \to \mathbb{R}$ is defined as

$$B_\gamma(x,t) := \min_{\xi_d \in \Xi_{[t,0]}} \max_{u\in\mathcal{U}_{[t,0]}} \min_{s\in[t,0]} e^{\gamma(s-t)} l(\mathrm{x}(s)), \tag{11}$$

where $\mathrm{x}(\cdot)$ solves for $(x,t,u,\xi_d[u])$, for some $\gamma \geq 0$ and $\forall t \leq 0$. At $t = 0$, we get terminal condition $B_\gamma(x,0) = l(x)$.

Note that B_γ is defined for each fixed value of $\gamma \geq 0$. Now, consider the case $\gamma = 0$. For this case, the definition of B_0 in (11) matches with the definition of the original reachability-based value function in (4). This is not surprising because (11) should be regarded as a *special case of the reachability problem*, whose target function is exponentially decaying backward in time.

Since (11) is an optimal control problem under a differential game setting, Bellman's principle of optimality can be applied to derive the dynamic programming principle for B_γ.

Theorem 2. (Dynamic Programming Optimality Condition) For the Robust CBVF B_γ in Definition 2, for each $t < t + \delta \leq 0$, the following is satisfied.

$$B_\gamma(x,t) = \min_{\xi_d\in\Xi_{[t,0]}} \max_{u\in\mathcal{U}_{[t,0]}} \min\Big\{ \min_{s\in[t,t+\delta]} e^{\gamma(s-t)} l(\mathrm{x}(s)), \\ e^{\gamma\delta} B_\gamma(\mathrm{x}(t+\delta), t+\delta) \Big\} \tag{12}$$

where $\mathrm{x}(\cdot)$ solves (1) for (x,t,u,ξ_d).

Proof. See Appendix. □

Theorem 2 leads to the derivation of the following theorem, which is the main theoretical result of this paper, showing that B_γ can be obtained by solving a particular variational inequality that has the form of HJI-VI.

Theorem 3. The Robust CBVF B_γ is a Lipschitz continuous unique viscosity solution of the CBVF variational inequality (CBVF-VI) below with the terminal condition $B_\gamma(x,0) = l(x)$:

$$0 = \min\Big\{ l(x) - B_\gamma(x,t), \tag{13}$$

$$D_t B_\gamma(x,t) + \max_{u\in U} \min_{d\in D} D_x B_\gamma(x,t) \cdot f(x,u,d) + \gamma B_\gamma(x,t) \Big\}.$$

Proof. See Appendix. □

The following proposition shows that like the original reachability-based value function V from (4), B_γ can also be used to verify the viability kernel $\mathcal{S}(t)$. In other words, the zero-superlevel set of the Robust CBVF contains every initial state from which robust safety guarantee is possible for a chosen time span. This is in sharp contrast to the CBFs, since the safe invariant set from a given CBF is only guaranteed to be a subset of the maximal control invariant set. Moreover, since CBVF is concerned with safety for finite-time horizon, the obtained safe set can be much bigger than the control invariant set from CBFs. Therefore, in addition to the fact that the CBVF is constructive, the main benefit of using the CBVF is that it recovers the biggest permissible region for the system for maintaining safety (Fig. 1).

Proposition 2. For each $t \leq 0$, define $\mathcal{C}_\gamma(t) := \{x \in \mathbb{R}^n : B_\gamma(x,t) \geq 0\}$. Then, $\forall t \leq 0$, $\mathcal{C}_\gamma(t) = \mathcal{S}(t)$.

Proof. For each $t \in (-\infty, 0]$, consider x such that $B_\gamma(x,t) \geq 0$. For $\forall \xi_d \in \Xi_{[t,0]}$, there exists $u \in \mathcal{U}_{[t,0]}$ such that $\min_{s\in[t,0]} e^{\gamma(s-t)} l(\mathrm{x}(s)) \geq 0$. Therefore, x belongs to $\mathcal{S}(t)$.

Consider $x \in \mathcal{S}(t)$. For all $\xi_d \in \Xi_{[t,0]}$, there exists $u \in \mathcal{U}_{[t,0]}$ such that $l(\mathrm{x}(s))$ is non-negative for all $s \in [t,0]$. Thus, $\max_{u\in\mathcal{U}_{[t,0]}} \min_{s\in[t,0]} e^{\gamma(s-t)} l(\mathrm{x}(s))$ is non-negative for all ξ_d, and $B_\gamma(x,t) \geq 0$. □

Finally, since V can be used to verify the viability kernel $\mathcal{S}(t)$, readers might wonder the additional benefit of introducing B_γ. In the next section, we explain why using B_γ would be preferable to using the original value function V.

IV. Optimal Control Policy of the CBVF

A. Evaluation of the optimal control policy of the CBVF

The main benefit of using the optimal controller from the new formulation of CBVF B_γ instead of the original reachability-based optimal controller π_V^* is that it can significantly reduce the conservativeness of π_V^* (Remark 2).

First recall how the optimal policy π_V^* of V is verified: 1) when $V(x,t) < l(x)$, it is determined by (6), and 2) when $V(x,t) = l(x)$, any element of (7) is optimal.

From the CBVF-VI (13), we can verify the optimal control policy with respect to B_γ similarly. For the first case, when $B_\gamma(x,t) < l(x)$, the second term of (13) must be zero; therefore the optimal control must be given by

$$\pi_{B_\gamma}^*(x,t) = \arg\max_{u\in U} \min_{d\in D} D_x B_\gamma(x,t) \cdot f(x,u,d), \tag{14}$$

which is similar to the first case of π^*_V. Also, the CBVF-VI (13) implies that for this case,

$$D_tB_\gamma(x,t)+\min_{d\in D}D_xB_\gamma(x,t)\cdot f(x,\pi^*_{B_\gamma}(x,t),d)+\gamma B_\gamma(x,t) = \dot{B}_\gamma(\mathrm{x}(t),t)+\gamma B_\gamma(\mathrm{x}(t),t)=0. \tag{15}$$

For the second case, when $B_\gamma(x,t)=l(x)$, any element of

$$K_{B_\gamma}(x,t)\!:=\!\{u\in U\!: D_tB_\gamma(x,t)+\min_{d\in D}D_xB_\gamma(x,t)\cdot f(x,u,d) + \gamma B_\gamma(x,t)\geq 0\} \tag{16}$$

is optimal with respect to B_γ and can be used as $\pi^*_{B_\gamma}$. For this case, $K_{B_\gamma}(x,t)$ is always non-empty because the second term of (13) is greater or equal to 0, and for any $u\in K_{B_\gamma}(x,t)$ and any $d\in D$,

$$\dot{l}(\mathrm{x}(t))=\dot{B}_\gamma(\mathrm{x}(t),t)\geq-\gamma B_\gamma(\mathrm{x}(t),t)=-\gamma l(\mathrm{x}(t)), \tag{17}$$

where $\mathrm{x}(\cdot)$ solves (1) for (x,t,u,d).

It is crucial to note the difference between (8) and (17). Speaking informally, both second cases of the optimal control policies with respect to V and B_γ occur when the state is not at stake of violating safety, therefore, the user is allowed to choose any u from K_V and K_{B_γ} as π^*_V and $\pi^*_{B_\gamma}$, respectively. However, as Remark 2 explains, π^*_V still never allows the state to get closer to the safety boundary. On the other hand, $\pi^*_{B_\gamma}$ allows l to decrease as long as it satisfies (17), which is a very similar property that CBFs have. Therefore, $\pi^*_{B_\gamma}$ allows for more control authority than π^*_V, while achieving the same safety objective.

This benefit of B_γ over V can be regarded as CBF's property of becoming less conservative instilled in the HJ reachability formulation. In the next section, we will numerically demonstrate that the optimal trajectories from $\pi^*_{B_\gamma}$ actually behave less conservative than the optimal trajectories from π^*_V, especially with higher value of γ.

B. Online optimal policy synthesis for control-affine systems

We end this section by proposing a specific way of synthesizing $\pi^*_{B_\gamma}$ for systems affine in control and disturbance:

$$\dot{\mathrm{x}}(s)\!=\!f(\mathrm{x}(s),u(s),d(s)) = p(\mathrm{x}(s))\!+\!q(\mathrm{x}(s))u(s)\!+\!r(\mathrm{x}(s))d(s), \tag{18}$$

where $p:\mathbb{R}^n\to\mathbb{R}^n$, $q:\mathbb{R}^n\to\mathbb{R}^{n\times m}$, and $r:\mathbb{R}^n\to\mathbb{R}^{n\times w}$.

Note that $u=\pi^*_{B_\gamma}(x,t)$ should satisfy

$$D_tB_\gamma(x,t)+\min_{d\in D}D_xB_\gamma(x,t)\cdot f(x,u,d)+\gamma B_\gamma(x,t)\geq 0$$

from (15) and (16). Similarly to the CBF-QP, we can incorporate this as a linear inequality constraint in a min-norm optimization based controller. When the input bound U is polytopic, the optimization becomes a QP as well:

Robust CBVF-QP:

$$\pi_{QP}(x,t)=\operatorname*{arg\,min}_{u\in U}\quad (u-u_{ref})^T(u-u_{ref}) \tag{19a}$$

$$\text{s.t.}\quad a(x,t)+D_xB_\gamma(x,t)\cdot q(x)u+\gamma B_\gamma(x,t)\geq 0, \tag{19b}$$

$$\text{where } a(x,t)=D_tB_\gamma(x,t)+D_xB_\gamma(x,t)\cdot p(x) + \min_{d\in D}D_xB_\gamma(x,t)\cdot r(x)d. \tag{19c}$$

Note that a similar formulation is proposed in a previous work that introduces a concept of Robust CBF [25].

Proposition 3. For the Robust CBVF B_γ, and for the system (18) with linear control bound U, the Robust CBVF-QP (19) is feasible everywhere $(x,t)\in\mathbb{R}^n\times(-\infty,0]$ where the gradient $D_xB_\gamma(x,t)$ exists, and its solution is always an optimal policy with respect to B_γ.

Proof. For the first case, when $B_\gamma(x,t)<l(x)$, the constraint of the QP (19b) is satisfied but only under the equality condition since

$$D_tB_\gamma(x,t)+\max_{u\in U}\min_{d\in D}D_xB_\gamma(x,t)\cdot f(x,u,d)+\gamma B_\gamma(x,t)=0$$

from (15). Any $u\in U$ that satisfies the equality condition is optimal. For the second case, when $B_\gamma(x,t)=l(x)$, K_{B_γ} is exactly the feasible set of the Robust CBVF-QP. □

Remark 3. Note that any reference control signal u_{ref} can be used in (19), since Proposition 3 holds for every feasible solution. Therefore, (19) is not only an optimal controller for B_γ, it also can be used as a safety filter for any kind of performance controller. As we explained in Sec. IV-A, this new safety filter is much less restrictive than the original optimal control policy of V. Also, compared to applying a least-restrictive safety filter explained in Remark 2 which utilizes value function only at the boundary, the filter (19) can be applied globally inside $\mathcal{S}(t)$, and the optimization automatically adjusts u_{ref} to make it safe.

Remark 4. When the differential D_xB_γ does not exist, since B_γ is Lipschitz continuous, either one of superdifferential or subdifferential always exists. The optimal control is determined by the same rule (16) where the differential $D_xB_\gamma(x,t)$ is replaced by the superdifferential $D_x\varphi(x,t)\in D_xB^+_\gamma(x,t)$ or subdifferential $D_x\varphi(x,t)\in D_xB^-_\gamma(x,t)$ [26, Ch.3.2.5].

V. Numerical Examples

In the following numerical examples, standard numerical methods for computing the reachability-based value functions [3], [19] are used to compute B_γ.

A. Double Integrator Example

The running example in this subsection will be a simple 2D double integrator. Its system dynamics are $\dot{z}=v+d$, $\dot{v}=u$, with states position z and velocity v, disturbance $d\in[-0.2,0.2]$ and control $u\in[-0.5,0.5]$. Figure 2 shows a comparison of the functions, zero level sets, trajectories, and control signals for three different values of γ. On the top in orange is the standard HJ VI computation (i.e. $\gamma=0$). The other rows show computations for $\gamma=0.2$ (middle, blue), and $\gamma=0.5$ (bottom, cyan). The new formulation is also robust to bounded disturbances. Figure 3 shows a comparison of trajectories under different disturbance conditions. Even under worst-case disturbances (blue), the online trajectory is guaranteed to remain in the safe set.

B. Dubins Car Example

In this subsection we demonstrate a comparison between using the original reachability-based controllers and the CBVF-QP, and a comparison between the CBF-QP and the CBVF-QP. We use a Dubins car model: $\dot{x}=v\cos(\theta)$, $\dot{y}=v\sin(\theta)$, $\dot{\theta}=u$, where x,y are positions, θ is heading, v

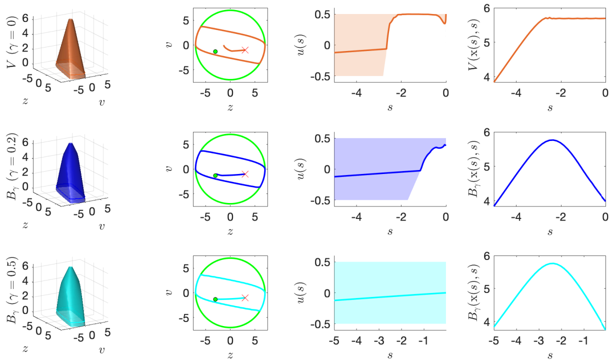

Fig. 2. From left to right: 1. Comparison between $V(x,t)$ (top) and $B_\gamma(x,t)$ with $\gamma = 0.2$ (middle) and 0.5 (bottom), $t = -5$. Note that when $\gamma = 0$, $B_\gamma(x,t) = V(x,t)$. 2. The optimal trajectories in the state space initiated at $x = [3, -1]$ (red cross) and the zero-level sets of $l(x)$ (green) and $B_\gamma(x,t)$. 3. The corresponding optimal control signals. The control is synthesized using the Robust-CBVF-QP, where u_{ref} is a simple PD control for the target point (green dot), and the shaded regions indicate feasible solutions of the QP ($K_{B_\gamma}(\mathrm{x}(s), s)$). 4. Profiles of B_γ along the trajectories. The optimal policy is less conservative with larger γ (allowing B_γ to decrease more) and is able to reach the target when $\gamma = 0.5$.

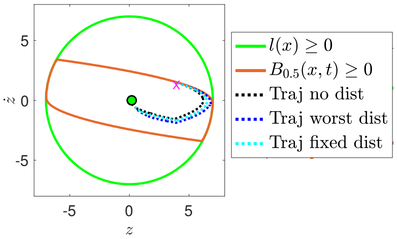

Fig. 3. Trajectories under different online disturbance conditions. All trajectories start from $x = [4, 1.5]$ (red cross). Conditions shown are no disturbance (black), a fixed disturbance of 0.1 m/s (cyan), and worst-case disturbance (blue). By starting in the safe set (orange boundary) the system remains within the constraint set (green boundary) even under worst-case disturbance.

is a fixed speed, and $u \in [-3, 3]$ is rotational velocity. We use $\gamma = 10$. In Fig. 4, the system navigates around an obstacle to a goal using least-restrictive control (top) and the CBVF-QP (bottom). The CBVF-QP is able to use a smoother control signal and still reach the goal within the time horizon.

In Fig. 5, the time stamps are shown for a system using a CBVF-QP (which is time-varying) and a CBF-QP (which is time-invariant) controller. For the CBF, $B = V_\infty$ is used to maximize its safe set $\mathcal{C}$ as $\mathcal{S}_\infty$. Although V_∞ has non-differentiable points for the Dubins car system in general, the trajectory resulting from the CBF-QP in Fig. 5 does not intersect with such points. The CBF-QP maintains safety, however, because of its safety concern for infinite-time horizon, the system is unable to reach the goal. In contrast, the time-varying CBVF-QP allows the system to safely reach the goal within the finite-time horizon. This formulation can be used for scenarios that require safety only for a fixed time [27], [28], for example, a hybrid system like legged robots that requires the system to stay safe only until it reaches the goal.

VI. Conclusion

This paper has introduced the notion of a Control Barrier-Value Function (CBVF) by unifying ideas from HJ reachability and Control Barrier Functions. To the best of our knowledge, this is the first constructive method for the CBF community that provides the maximal safe set for a desired safety constraint which also can handle bounded control and disturbances, however, this comes with a cost of bearing the curse of dimensionality. We also introduce the Robust CBVF-QP for online control and demonstrate its usage as a safety filter in a double-integrator and Dubins car system. This provides a new systematic way of designing the safety filter for the reachability community. We believe the introduction of CBVFs is an important step towards bridging the gap between the CBF-based and reachability-based safety control frameworks. We plan to extend this analysis to Control Lyapunov Functions, similarly to [29], and to reach-avoid problems [19].

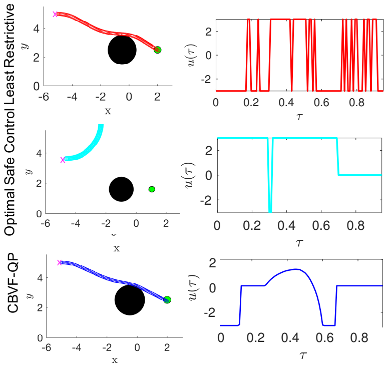

Fig. 4. Comparison between the least-restrictive controller (top), the optimal controller from the original HJ reachability (middle), and the CBVF-QP controller (bottom).

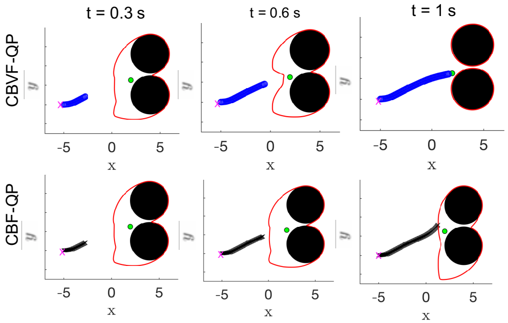

Fig. 5. Comparison of trajectories using a CBVF-QP (top) vs. a CBF-QP (bottom).The red set represents the boundary of the x-y slice of the zero-superlevel sets of B_γ and B at current θ. Note that these sets appear to rotate over time because we are visualizing the 2D slice at the current value of θ. On the top, the system is able to reach a goal while avoiding obstacles within the prescribed time horizon. On the bottom, the system must stay safe for an infinite time horizon, and is therefore unable to reach the goal (video: `https://youtu.be/wGg7rfyXCTs`).

Acknowledgements

We would like to thank Zhichao Li, Somil Bansal, Andrea Bajcsy, and Jaime Fisac for the insightful discussions.

Appendix

The following **proofs of Theorem 2 and 3** inherit the structure from the standard proof of viscosity solution of HJI Partial Differential Equation (HJI-PDE) [18]. Note that the proofs hold for compact U, D without convexity condition. Here, we use notation $\psi_{x,t}^{u,d} \equiv \mathrm{x} : [t, 0] \to \mathbb{R}^n$, where $\mathrm{x}(\cdot)$ solves (1) for (x, t, u, d), instead of $\mathrm{x}(\cdot)$, to specify control and disturbance signal. We use $\Xi_t := \Xi_{[t,0]}$, $\mathcal{U}_t := \mathcal{U}_{[t,0]}$.

Proof. **(Proof of Theorem 2)**

Define $W(x,t)$ as the right hand side of (12). For $\forall\varepsilon>0$, $\exists\eta\in\Xi_t$ such that $\forall u\in\mathcal{U}_t$

$$W(x,t)\geq\min\Big\{\inf_{s\in[t,t+\delta]}e^{\gamma(s-t)}l(\psi_{x,t}^{u,\eta[u]}(s)),\\ e^{\gamma\delta}B_\gamma(\psi_{x,t}^{u,\eta[u]}(t+\delta),t+\delta)\Big\}-\varepsilon \tag{20}$$

From the definition of B_γ, for each $y\in\mathbb{R}^n$,

$$B_\gamma(y,t+\delta)=\inf_{\xi_d\in\Xi_{t+\delta}}\sup_{u\in\mathcal{U}_{t+\delta}}\inf_{s\in[t+\delta,0]}e^{\gamma(s-(t+\delta))}l(\psi_{y,t+\delta}^{u,\xi_d[u]}(s)).$$

Therefore, $\forall\varepsilon_1>0$, $\exists\eta_y\in\Xi_{t+\delta}$ such that for $\forall u\in\mathcal{U}_{t+\delta}$

$$B_\gamma(y,t+\delta)\geq\inf_{s\in[t+\delta,0]}e^{\gamma(s-(t+\delta))}l(\psi_{y,t+\delta}^{u,\eta_y[u]}(s))-\varepsilon_1. \tag{21}$$

With $y:=\psi_{x,t}^{u,\eta[u]}(t+\delta)$, define

$$\xi_d[u]:=\begin{cases}\eta[u](s) & \text{for} \quad t\leq s\leq t+\delta\\ \eta_y[u](s) & \text{for} \quad t+\delta<s\leq 0\end{cases}$$

Then, from (20) and (21), for $\forall u\in\mathcal{U}_t$,

$$W(x,t)\geq\inf_{s\in[t,0]}e^{\gamma(s-t)}l(\psi_{x,t}^{u,\xi_d[u]}(s))-2\varepsilon \text{ by taking } \varepsilon_1=e^{-\gamma\delta}\varepsilon.$$

Therefore,

$$W(x,t)\geq B_\gamma(x,t)-2\varepsilon \quad \forall\varepsilon>0. \tag{22}$$

On the other hand, by definitions of B_γ and W, for $\forall\varepsilon>0$, $\exists\eta\in\Xi_t$ such that for $\forall u\in\mathcal{U}_t$

$$\inf_{s\in[t,0]}e^{\gamma(s-t)}l(\psi_{x,t}^{u,\eta[u]}(s))\leq B_\gamma(x,t)+\varepsilon \tag{23}$$

$$W(x,t)\leq\sup_{u\in\mathcal{U}_t}\min\Big\{\inf_{s\in[t,t+\delta]}e^{\gamma(s-t)}l(\psi_{x,t}^{u,\eta[u]}(s)),\\ e^{\gamma\delta}B_\gamma(\psi_{x,t}^{u,\eta[u]}(t+\delta),t+\delta)\Big\},$$

Therefore, $\exists u_0\in\mathcal{U}_t$ such that

$$W(x,t)\leq\min\Big\{\inf_{s\in[t,t+\delta]}e^{\gamma(s-t)}l(\psi_{x,t}^{u_0,\eta[u_0]}(s)),\\ e^{\gamma\delta}B_\gamma(\psi_{x,t}^{u_0,\eta[u_0]}(t+\delta),t+\delta)\Big\}+\varepsilon \tag{24}$$

For $\forall u\in\mathcal{U}_{t+\delta}$, define

$$\bar{u}(s):=\begin{cases}u_0(s) & \text{for} \quad t\leq s\leq t+\delta\\ u(s) & \text{for} \quad t+\delta<s\leq 0,\end{cases}$$

and define $\bar{\eta}\in\Xi_{t+\delta}$ by $\bar{\eta}[u](s)=\eta[\bar{u}](s)$ for $s\in[t+\delta,0]$. Then, with $y:=\psi_{x,t}^{\bar{u},\eta[\bar{u}]}(t+\delta)$, by definition of B_γ,

$$B_\gamma(y,t+\delta)\leq\sup_{u\in\mathcal{U}_{t+\delta}}\inf_{s\in[t+\delta,0]}e^{\gamma(s-(t+\delta))}l(\psi_{y,t+\delta}^{u,\bar{\eta}[u]}(s)).$$

Therefore, $\forall\varepsilon_2>0$, $\exists u_1\in\mathcal{U}_{t+\delta}$ such that

$$B_\gamma(y,t+\delta)\leq\inf_{s\in[t+\delta,0]}e^{\gamma(s-(t+\delta))}l(\psi_{y,t+\delta}^{u_1,\bar{\eta}[u_1]}(s))+\varepsilon_2. \tag{25}$$

Selecting $\bar{u}\in\mathcal{U}_t$ with $u_1\in\mathcal{U}_{t+\delta}$, (24) and (25) yields

$$W(x,t)\leq\inf_{s\in[t,0]}e^{\gamma(s-t)}l(\psi_{x,t}^{u,\eta[u]}(s))+2\varepsilon \text{ by taking } \varepsilon_2=e^{-\gamma\delta}\varepsilon.$$

Therefore, from (23),

$$W(x,t)\leq B_\gamma(x,t)+3\varepsilon \quad \forall\varepsilon>0. \tag{26}$$

The proof is done from (22) and (26). □

Proof. **(Proof of Theorem 3)**

According to the definition of viscosity solution [26], Theorem 3 is equivalent to B_γ satisfying the following statements.

1) For $\forall\varphi(x,t)\in C^1(\mathbb{R}^n\times(-\infty,0])$ such that $B_\gamma-\varphi$ has a *local maximum* 0 at $(x_0,t_0)\in\mathbb{R}^n\times(-\infty,0]$,

$$0\leq\min\Big\{l(x_0)-\varphi(x_0,t_0), \tag{27}\\ D_t\varphi(x_0,t_0)+\max_{u\in U}\min_{d\in D}D_x\varphi(x_0,t_0)\cdot f(x_0,u,d)+\gamma\varphi(x_0,t_0)\Big\}.$$

2) For $\forall\varphi(x,t)\in C^1(\mathbb{R}^n\times(-\infty,0])$ such that $B_\gamma-\varphi$ has a *local minimum* 0 at $(x_0,t_0)\in\mathbb{R}^n\times(-\infty,0]$,

$$0\geq\min\Big\{l(x_0)-\varphi(x_0,t_0), \tag{28}\\ D_t\varphi(x_0,t_0)+\max_{u\in U}\min_{d\in D}D_x\varphi(x_0,t_0)\cdot f(x_0,u,d)+\gamma\varphi(x_0,t_0)\Big\}.$$

We use the following lemma to prove 1) and 2).

Lemma 1. For $\varphi(x,t)\in C^1(\mathbb{R}^n\times(-\infty,0])$, define

$$\Lambda_\varphi(x,t,u,d):=D_t\varphi(x,t)+D_x\varphi(x,t)\cdot f(x,u,d)+\gamma\varphi(x,t). \tag{29}$$

(a) If $\exists\theta>0$, $\exists(x_0,t_0)\in\mathbb{R}^n\times(-\infty,0]$ such that $\max_{u\in U}\min_{d\in D}\Lambda_\varphi(x_0,t_0,u,d)\leq-\theta$, there exists a small enough $\delta>0$, $\exists\xi_d\in\Xi_{t_0}$ such that $\forall u\in\mathcal{U}_{t_0}$,

$$e^{\gamma\delta}\varphi(\psi_{x_0,t_0}^{u,\xi_d[u]}(t_0+\delta),t_0+\delta)-\varphi(x_0,t_0)\leq-\frac{\theta}{2}\delta. \tag{30}$$

(b) If $\exists\theta>0$, $\exists(x_0,t_0)\in\mathbb{R}^n\times(-\infty,0]$ such that $\max_{u\in U}\min_{d\in D}\Lambda_\varphi(x_0,t_0,u,d)\geq\theta$, there exists a small enough $\delta>0$, $\forall\xi_d\in\Xi_{t_0}$, $\exists u\in\mathcal{U}_{t_0}$ such that

$$e^{\gamma\delta}\varphi(\psi_{x_0,t_0}^{u,\xi_d[u]}(t_0+\delta),t_0+\delta)-\varphi(x_0,t_0)\geq\frac{\theta}{2}\delta. \tag{31}$$

Lemma 1 is a modification of [18, Lemma 4.3.] for general HJI-PDE to CBVF-VI. For its proof, please refer to [18].

Proof of 1). Let (27) be false. Then one of the followings should hold.

$$\exists\theta_1>0 \text{ s.t. } l(x_0)-\varphi(x_0,t_0)\leq-\theta_1 \tag{32a}$$

$$\exists\theta_2>0 \text{ s.t. } D_t\varphi(x_0,t_0)+\max_{u\in U}\min_{d\in D}D_x\varphi(x_0,t_0)\cdot f(x_0,u,d)\\ +\gamma\varphi(x_0,t_0)\leq-\theta_2 \tag{32b}$$

If (32a) is true, by continuity of l in the state and ψ in time, $\exists\delta>0$ such that for all $u\in\mathcal{U}_{t_0}$, $\xi_d\in\Xi_{t_0}$, $s\in[t_0,t_0+\delta]$,

$$\Big|e^{\gamma(s-t_0)}l(\psi_{x_0,t_0}^{u,\xi_d[u]}(s))-l(x_0)\Big|\leq\frac{\theta_1}{2}.$$

$$\Rightarrow e^{\gamma(s-t_0)}l(\psi_{x_0,t_0}^{u,\xi_d[u]}(s))\leq l(x_0)+\frac{\theta_1}{2}\leq B_\gamma(x_0,t_0)-\frac{\theta_1}{2}.$$

Plugging this into the dynamic programming principle (12),

$$B_\gamma(x_0,t_0)\leq\inf_{\xi_d\in\Xi_{t_0}}\sup_{u\in\mathcal{U}_{t_0}}\inf_{s\in[t_0,t_0+\delta]}e^{\gamma(s-t_0)}l(\psi_{x_0,t_0}^{u,\xi_d[u]}(s))\\ \leq B_\gamma(x_0,t_0)-\frac{\theta_1}{2}.$$

This is a contradiction, therefore, (32a) is false.

Next, if (32b) is true, from Lemma 1.a, for small enough $\delta>0$, $\exists\eta\in\Xi_{t_0}$ such that for all $u\in\mathcal{U}_{t_0}$,

$$e^{\gamma\delta}\varphi(\psi_{x_0,t_0}^{u,\eta[u]}(t_0+\delta),t_0+\delta)-\varphi(x_0,t_0)\leq-\frac{\theta_2}{2}\delta.$$

Since $B_\gamma-\varphi$ has local maximum 0 at (x_0,t_0),

$$B_\gamma(\psi_{x_0,t_0}^{u,\eta[u]}(t_0+\delta),t_0+\delta)-\varphi(\psi_{x_0,t_0}^{u,\eta[u]}(t_0+\delta),t_0+\delta)\leq 0.$$

$$\begin{aligned}\Rightarrow e^{\gamma\delta} B_\gamma(\psi_{x_0,t_0}^{u,\eta[u]}(t_0{+}\delta), t_0{+}\delta) &\le e^{\gamma\delta}\varphi(\psi_{x_0,t_0}^{u,\eta[u]}(t_0{+}\delta), t_0{+}\delta)\\ &\le \varphi(x_0,t_0) - \frac{\theta_2}{2}\delta = B_\gamma(x_0,t_0) - \frac{\theta_2}{2}\delta.\end{aligned}$$

Finally, from (12), we get,

$$\begin{aligned}B_\gamma(x_0,t_0) \le \sup_{u\in\mathcal{U}_{t_0}} \min\Big\{&\inf_{s\in[t_0,t_0+\delta]} e^{\gamma(s-t_0)} l(\psi_{x_0,t_0}^{u,\eta[u]}(s)),\\ &e^{\gamma\delta} B_\gamma(\psi_{x_0,t_0}^{u,\eta[u]}(t_0{+}\delta), t_0{+}\delta)\Big\}\\ \le & B_\gamma(x_0,t_0) - \frac{\theta_2}{2}\delta,\end{aligned}$$

which is a contradiction. Therefore, (32b) is false. □

Proof of 2). Let (28) be false. Then both of the followings should hold.

$$\exists\theta_1 > 0 \text{ s.t. } l(x_0) - \varphi(x_0,t_0) \ge \theta_1 \tag{33a}$$

$$\begin{aligned}\exists\theta_2 > 0 \text{ s.t. } & D_t\varphi(x_0,t_0) + \max_{u\in U}\min_{d\in D} D_x\varphi(x_0,t_0)\cdot f(x_0,u,d)\\ &+ \gamma\varphi(x_0,t_0) \ge \theta_2\end{aligned} \tag{33b}$$

From (33a), by continuity of l and ψ, $\exists\delta_1 > 0$ such that for all $u\in\mathcal{U}_{t_0}$, $\xi_d\in\Xi_{t_0}$, $s\in[t_0, t_0+\delta_1]$,

$$\left|e^{\gamma(s-t_0)} l(\psi_{x_0,t_0}^{u,\xi_d[u]}(s)) - l(x_0)\right| \le \frac{\theta_1}{2}.$$

$$\Rightarrow e^{\gamma(s-t_0)} l(\psi_{x_0,t_0}^{u,\xi_d[u]}(s)) \ge l(x_0) - \frac{\theta_1}{2} \ge B_\gamma(x_0,t_0) + \frac{\theta_1}{2}. \tag{34}$$

From (33b), by Lemma 1.b, for small enough $\delta_2 > 0$, $\forall\xi_d\in\Xi_{t_0}$, $\exists u_2\in\mathcal{U}_{t_0}$ such that

$$e^{\gamma\delta_2}\varphi(\psi_{x_0,t_0}^{u_2,\xi_d[u_2]}(t_0{+}\delta_2), t_0{+}\delta_2) - \varphi(x_0,t_0) \ge \frac{\theta_2}{2}\delta_2. \tag{35}$$

Since $B_\gamma - \varphi$ has a local minimum 0 at (x_0,t_0),

$$\begin{aligned}&e^{\gamma\delta_2} B_\gamma(\psi_{x_0,t_0}^{u_2,\xi_d[u]}(t_0{+}\delta_2), t_0{+}\delta_2)\\ &\quad\ge e^{\gamma\delta_2}\varphi(\psi_{x_0,t_0}^{u_2,\xi_d[u]}(t_0{+}\delta_2), t_0{+}\delta_2)\\ &\quad\ge \varphi(x_0,t_0) + \frac{\theta_2}{2}\delta_2 = B(x_0,t_0) + \frac{\theta_2}{2}\delta_2.\end{aligned} \tag{36}$$

Take $\delta = \min(\delta_1,\delta_2)$ and plugging (34) and (36) into (12),

$$\begin{aligned}B_\gamma(x_0,t_0) \ge \inf_{\xi_d\in\Xi_{t_0}} \min\Big\{&\inf_{s\in[t_0,t_0+\delta]} e^{\gamma(s-t_0)} l(\psi_{x_0,t_0}^{u_2,\xi_d[u_2]}(s)),\\ &e^{\gamma\delta} B_\gamma(\psi_{x_0,t_0}^{u_2,\xi_d[u_2]}(t_0{+}\delta), t_0{+}\delta)\Big\}\\ \ge\ & B_\gamma(x_0,t_0) + \min\left\{\frac{\theta_2}{2}\delta, \frac{\theta_1}{2}\right\}.\end{aligned}$$

This is a contradiction. □

Note that since B_γ satisfies both 1) and 2), uniqueness and Lipschitz continuity of B_γ can be derived similarly to [30, Th.4.2] and [18, Th.3.2.], respectively.

References

[1] J. Lygeros, "On reachability and minimum cost optimal control," *Automatica*, 2004.

[2] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE TAC*, July 2005.

[3] I. M. Mitchell and J. A. Templeton, "A toolbox of Hamilton-Jacobi solvers for analysis of nondeterministic continuous and hybrid systems," in *Hybrid Systems: Computation and Control*, 2005.

[4] S. L. Herbert, S. Bansal, S. Ghosh, and C. J. Tomlin, "Reachability-based safety guarantees using efficient initializations," in *IEEE CDC*, 2019.

[5] S. Bansal and C. J. Tomlin, "Deepreach: A deep learning approach to high-dimensional reachability," in *IEEE ICRA*, 2021.

[6] M. Chen, S. L. Herbert, M. S. Vashishtha, S. Bansal, and C. J. Tomlin, "Decomposition of reachable sets and tubes for a class of nonlinear systems," *IEEE TAC*, 2018.

[7] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-Jacobi reachability: A brief overview and recent advances," in *IEEE CDC*, 2017.

[8] P. Wieland and F. Allgöwer, "Constructive safety using control barrier functions," *IFAC Proceedings Volumes*, vol. 40, no. 12, pp. 462–467, 2007, 7th IFAC Symposium on Nonlinear Control Systems.

[9] A. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE TAC*, 2017.

[10] Q. Nguyen and K. Sreenath, "Optimal robust time-varying safety-critical control with application to dynamic walking on moving stepping stones," *ASME Dynamic Sys. and Control Conf.*, 2016.

[11] L. Wang, A. Ames, and M. Egerstedt, "Safety barrier certificates for collisions-free multirobot systems," *IEEE Trans. on Robotics*, 2017.

[12] E. Squires, P. Pierpaoli, and M. Egerstedt, "Constructive barrier certificates with applications to fixed-wing aircraft collision avoidance," in *IEEE Conference on Control Technology and Applications*, 2018.

[13] T. Gurriet, A. Singletary, J. Reher, L. Ciarletta, E. Feron, and A. Ames, "Towards a framework for realizable safety critical control through active set invariance," in *ACM/IEEE International Conference on Cyber-Physical Systems*, 2018, pp. 98–106.

[14] R. Cheng, G. Orosz, R. M. Murray, and J. W. Burdick, "End-to-end safe reinforcement learning through barrier functions for safety-critical continuous control tasks," in *AAAI Conf. on AI*, 2019.

[15] A. Taylor, A. Singletary, Y. Yue, and A. Ames, "Learning for safety-critical control with control barrier functions," in *Conference on Learning for Dynamics and Control*, 2020.

[16] J. Zeng, B. Zhang, Z. Li, and K. Sreenath, "Safety-critical control using optimal-decay control barrier function with guaranteed point-wise feasibility," in *American Control Conference*, 2021.

[17] S. Herbert, J. J. Choi, S. Sanjeev, M. Gibson, K. Sreenath, and C. J. Tomlin, "Scalable learning of safety guarantees for autonomous systems using Hamilton-Jacobi reachability," in *IEEE ICRA*, 2021.

[18] L. C. Evans and P. E. Souganidis, "Differential games and representation formulas for solutions of Hamilton-Jacobi-Isaacs equations," *Indiana University Mathematics Journal*, 1984.

[19] J. F. Fisac, M. Chen, C. J. Tomlin, and S. S. Sastry, "Reach-avoid problems with time-varying dynamics, targets and constraints," in *Hybrid Systems: Computation and Control*. ACM, 2015.

[20] A. Altarovici, O. Bokanowski, and H. Zidani, "A general Hamilton-Jacobi framework for non-linear state-constrained control problems," *ESAIM: Control, Optimisation and Calculus of Variations*, 2013.

[21] L. C. Evans and R. F. Gariepy, *Measure theory and fine properties of functions*. CRC press, 2015.

[22] M. Chen, S. Herbert, H. Hu, Y. Pu, J. Fernandez Fisac, S. Bansal, S. Han, and C. J. Tomlin, "Fastrack: a modular framework for real-time motion planning and guaranteed safe tracking," *IEEE TAC*, 2021.

[23] A. Bajcsy, S. Bansal, E. Bronstein, V. Tolani, and C. J. Tomlin, "An efficient reachability-based framework for provably safe autonomous navigation in unknown environments," in *IEEE CDC*, 2019.

[24] I. J. Fialho and T. T. Georgiou, "Worst case analysis of nonlinear systems," *IEEE TAC*, 1999.

[25] M. Jankovic, "Robust control barrier functions for constrained stabilization of nonlinear systems," *Automatica*, 2018.

[26] M. Bardi and I. Capuzzo-Dolcetta, *Optimal control and viscosity solutions of Hamilton-Jacobi-Bellman equations*. Springer, 2008.

[27] K. Garg, R. K. Cosner, U. Rosolia, A. D. Ames, and D. Panagou, "Multi-rate control design under input constraints via fixed-time barrier functions," *arXiv preprint arXiv:2103.03695*, 2021.

[28] M. Ohnishi, G. Notomista, M. Sugiyama, and M. Egerstedt, "Constraint learning for control tasks with limited duration barrier functions," *Automatica*, 2021.

[29] F. Camilli, L. Grüne, and F. Wirth, "Control Lyapunov functions and Zubov's method," *SIAM Journal on Control and Optimization*, 2008.

[30] E. Barron and H. Ishii, "The Bellman equation for minimizing the maximum cost," *Nonlinear Analysis: Theory, Methods & Applications*, 1989.