Safety of Sampled-Data Systems with Control Barrier Functions via Approximate Discrete Time Models

Andrew J. Taylor[1], Victor D. Dorobantu[1], Ryan K. Cosner[1], Yisong Yue, and Aaron D. Ames

***Abstract*—Control Barrier Functions (CBFs) have been demonstrated to be a powerful tool for safety-critical controller design for nonlinear systems. Existing design paradigms do not address the gap between theory (controller design with continuous time models) and practice (the discrete time sampled implementation of the resulting controllers); this can lead to poor performance and violations of safety for hardware instantiations. We propose an approach to close this gap by synthesizing sampled-data counterparts to these CBF-based controllers using approximate discrete time models and *Sampled-Data Control Barrier Functions (SD-CBFs)*. Using properties of a system's continuous time model, we establish a relationship between SD-CBFs and a notion of *practical safety* for sampled-data systems. Furthermore, we construct convex optimization-based controllers that formally endow nonlinear systems with safety guarantees in practice. We demonstrate the efficacy of these controllers in simulation.**

I. Introduction

Nonlinear control methods offer promising solutions to many modern safety-critical engineering applications. However, theoretically sound controller designs often fail to meet safety requirements when deployed on real systems. Thus, it is critical to understand the discrepancies between theoretical design and practical implementation mathematically, and to design controllers that close these gaps. Specifically, we address the challenges in designing safety-critical controllers for continuous time systems for which controllers are realized with discrete time sampling implementations, known as the sampled-data control problem [1].

Control Barrier Functions (CBFs) have become a popular tool for constructively synthesizing controllers that endow nonlinear systems with rigorous safety guarantees [2], [3]. While originally posed for continuous time systems, they have similarly been developed for discrete time systems [4] and sampled-data systems [5]–[13]. These existing works take an *emulative* approach to sampled-data control, in which continuous time safety conditions are met more conservatively to ensure that a system remains safe throughout a sample period. The approaches in [6], [7], [10]–[13] achieve this by adding a margin term to the standard CBF derivative condition that captures possible changes in the dynamics and CBF during the inter-sample period. This margin term often directly incorporates an exponential of Lipschitz constants and the sample period, requiring exceptionally high sample rates to overcome conservativeness, as studied in [10]. The work in [9] takes a computationally intensive approach to reduce conservatism by propagating sensitivity functions, which may be difficult for high-dimensional systems.

[1]Authors contributed equally. A.J. Taylor, V.D. Dorobantu, Ryan K. Cosner, Y. Yue, and A.D. Ames are with the Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA 91125, USA, {ajtaylor, vdoroban, rkcosner, yyue, ames}@caltech.edu. Y. Yue is affiliated with Argo AI, Pittsburgh, PA.

While the aforementioned results have focused on safety for sampled-data nonlinear systems, there exists a significant body of literature on stabilization of sampled-data nonlinear systems through discrete time design using *approximate models*. Motivated by the challenge of finding exact representations of the discrete time sampled-data dynamics of nonlinear systems, the work in [14], [15] proposed a framework for achieving a type of *practical stability* using approximations of the discrete time sampled-data dynamics. Subsequently, a number of standard nonlinear stabilization techniques such as backstepping [16], model predictive control [17], Lyapunov-redesign [18], and optimization based control via Control Lyapunov Functions [19], were extended to use approximate models of discrete-time dynamics. These approaches often yielded significant improvements over their continuous time counterparts, even at relatively slow sample rates [20]. Notably, a similar framework for achieving safety has yet to be proposed.

In this work we propose a novel approach for achieving safety of sampled-data nonlinear systems via approximate models of discrete time sampled-data dynamics. In Section II we describe the sampled-data control setting and establish a *consistency* result on how accurately sampled-data dynamics of a nonlinear system can be captured by a Runge-Kutta approximation. In Section III we propose a novel definition of *practical safety* for sampled-data systems. Our definition mirrors the notion of practical stability developed in [14], such that a system is practically safe if its state can be kept arbitrarily close to a safe set at sample times through sufficiently high sample rates. This leads to the unification of discrete time Barrier Functions [4] with regularity properties developed in [14], wherein we formulate *Sampled-Data Barrier Functions (SD-BFs)* and their control counterparts, *Sampled-Data Control Barrier Functions (SD-CBFs)*. We establish properties of this new class of CBFs and relate them to Lyapunov functions.

The main contribution of this paper, given in Section IV, establishes the practical safety of sampled-data systems through SD-BFs. We achieve this by unifying the key properties of SD-BFs with the accuracy guarantees provided by consistent approximations of the discrete sampled-data dynamics. This result is used to inform controller synthesis in Section V, where we explore how appropriately designed SD-CBFs and Runge-Kutta approximations of systems with higher-order relative degrees preserves convexity with respect to the input of the SD-CBF difference constraint. This allows for SD-CBFs to be directly incorporated into a convex optimization based controller that achieves practical safety. We demonstrate this controller in simulation, illustrating the role that sample rate plays in sample-data systems in the context of practical safety. The proof of the main result is presented in the text, with all other proofs in the appendix.

II. Sampled-Data Control

Throughout this work, we will consider the nonlinear control system governed by the differential equation:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{u}, \tag{1}$$

for state signal $\mathbf{x}$ and control input signal $\mathbf{u}$ taking values in $\mathbb{R}^n$ and $\mathbb{R}^m$, respectively, drift dynamics $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$, and actuation matrix function $\mathbf{g} : \mathbb{R}^n \to \mathbb{R}^{n\times m}$. Consider an open subset $\mathcal{Z} \subseteq \mathbb{R}^n \times \mathbb{R}^m$ and its projection onto the state space $\mathcal{X} \triangleq \{\mathbf{x} \in \mathbb{R}^n \mid \exists\ \mathbf{u} \in \mathbb{R}^m \text{ s.t. } (\mathbf{x}, \mathbf{u}) \in \mathcal{Z}\} \subseteq \mathbb{R}^n$. Assume there exists $T_{\max} \in \mathbb{R}_{++}$ (the strictly positive reals) such that for every state-input pair $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$, there exists a unique solution $\boldsymbol{\varphi} : [0, T_{\max}] \to \mathbb{R}^n$ satisfying:

$$\dot{\boldsymbol{\varphi}}(t) = \mathbf{f}(\boldsymbol{\varphi}(t)) + \mathbf{g}(\boldsymbol{\varphi}(t))\mathbf{u}, \quad \boldsymbol{\varphi}(0) = \mathbf{x}. \tag{2}$$

for all $t \in (0, T_{\max})$. Given an $h \in (0, T_{\max}]$, we define a controller $\mathbf{k} : \mathcal{X} \to \mathbb{R}^m$ as *h-admissible* if for any state $\mathbf{x} \in \mathcal{X}$, the state-input pair $(\mathbf{x}, \mathbf{k}(\mathbf{x}))$ satisfies $(\mathbf{x}, \mathbf{k}(\mathbf{x})) \in \mathcal{Z}$ and the corresponding solution $\boldsymbol{\varphi}$ satisfies $\boldsymbol{\varphi}(t) \in \mathcal{X}$ for all $t \in [0, h]$.

Remark 1. This requirement on h-admissible controllers will ensure that in the sampled-data context, the closed-loop system is forward complete and its evolution may be described by iterative solutions to (2). Though verifying h-admissibility of a controller may be intractable, assuming that a controller is h-admissible and renders the set $\mathcal{X}$ invariant is relatively weak as $\mathcal{X}$ is defined to ensure the continued existence of solutions rather than reflecting a task-specific set.

The preceding construction of solutions and admissible controllers describes the sampled-data control setting, in which inputs are applied to the system with a zero-order hold over a sample period. More precisely, the set of possible sample periods is given by $I = (0, T_{\max}]$. Given a sample period $h \in I$ and an h-admissible controller $\mathbf{k} : \mathcal{X} \to \mathbb{R}^m$, the state and control input signals in (1) satisfy:

$$\mathbf{u}(t) = \mathbf{k}(\mathbf{x}(t_k)) \quad \forall t \in [t_k, t_{k+1}), \tag{3}$$

with sample times satisfying $t_{k+1} - t_k = h$ for all $k \in \mathbb{Z}_+$ (the non-negative integers). In general, the evolution of the system over a sample period is given by the *exact map* $\mathbf{F}^e_h : \mathcal{Z} \to \mathbb{R}^n$:

$$\mathbf{F}^e_h(\mathbf{x}, \mathbf{u}) = \mathbf{x} + \int_0^h \left[\mathbf{f}(\boldsymbol{\varphi}(\tau)) + \mathbf{g}(\boldsymbol{\varphi}(\tau))\mathbf{u}\right] \mathrm{d}\tau, \tag{4}$$

for all state-input pairs $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$. We call $\{\mathbf{k}_h : \mathcal{X} \to \mathbb{R}^m \mid h \in I\}$ a *family of admissible controllers* if there is an $h^* \in I$ such that for each $h \in (0, h^*)$, $\mathbf{k}_h$ is h-admissible. This enables the following definition:

Definition 1 (*Exact Family*)**.** We define the *exact family of maps* $\{\mathbf{F}^e_h \mid h \in I\}$, and for a family of admissible controllers $\{\mathbf{k}_h \mid h \in I\}$, we define the *exact family of controller-map pairs* $\{(\mathbf{k}_h, \mathbf{F}^e_h) \mid h \in I\}$.

For all $h \in I$ such that $\mathbf{k}_h$ is h-admissible, the recursion $\mathbf{x}_{k+1} = \mathbf{F}^e_h(\mathbf{x}_k, \mathbf{k}_h(\mathbf{x}_k)) \in \mathcal{X}$ is well-defined for all $\mathbf{x}_0 \in \mathcal{X}$ and $k \in \mathbb{Z}_+$. In practice, closed-form expressions for the exact family of maps are rarely obtainable, suggesting the use of approximations in the control synthesis process. While there are many approaches to approximating this family of maps, we will use the following common class of approximations:

Definition 2 (*Runge-Kutta Approximation Family*)**.** Let $p \in \mathbb{N}$. We define the *Runge-Kutta approximation family of maps* $\{\mathbf{F}^{a,p}_h \mid h \in I\}$, where for every sample period $h \in I$, define $\mathbf{F}^{a,p}_h : \mathcal{Z} \to \mathbb{R}^n$ recursively as:

$$\mathbf{F}^{a,p}_h(\mathbf{x}, \mathbf{u}) = \mathbf{x} + h\sum_{i=1}^{p} b_i(\mathbf{f}(\mathbf{z}_i) + \mathbf{g}(\mathbf{z}_i)\mathbf{u}), \tag{5}$$

$$\mathbf{z}_i = \mathbf{x} + h\sum_{j=1}^{i-1} a_{i,j}(\mathbf{f}(\mathbf{z}_j) + \mathbf{g}(\mathbf{z}_j)\mathbf{u}), \tag{6}$$

for all pairs $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$, with $\mathbf{z}_1 = \mathbf{x}$. Here, $b_1, \ldots, b_p \in \mathbb{R}_+$ satisfy $\sum_{i=}^{p} b_i = 1$ and $a_{i,j} \in \mathbb{R}$ for each $i \in \{1, \ldots p\}$ and $j \in \{1, \ldots, i-1\}$. For a family of admissible controllers $\{\mathbf{k}_h \mid h \in I\}$, we may define the *Runge-Kutta approximation family of controller-map pairs* $\{(\mathbf{k}_h, \mathbf{F}^{a,p}_h) \mid h \in I\}$.

Remark 2. There may be an $h \in I$ such that the controller $\mathbf{k}_h$ is h-admissible but the recursion $\mathbf{x}_{k+1} = \mathbf{F}^{a,p}_h(\mathbf{x}_k, \mathbf{k}_h(\mathbf{x}_k))$ is not well-defined for all $\mathbf{x}_0 \in \mathcal{X}$ and $k \in \mathbb{Z}_+$. This is due to this map enabling $\mathbf{x}_k \notin \mathcal{X}$ for some $k > 0$. While our results do not need this recursion to be well-defined, this can be achieved by extending the domain of $\mathbf{k}_h$ to $\mathbb{R}^n$.

Defining class $\mathcal{K}$ ($\mathcal{K}_\infty$) and $\mathcal{K}^e$ ($\mathcal{K}^e_\infty$) comparison functions as in [21] and [3], the following definition characterizes how accurately an approximate map captures the exact map:

Definition 3 (*One-Step Consistency*)**.** A family $\{(\mathbf{k}_h, \mathbf{F}_h) : h \in I\}$ is *one-step consistent* with $\{(\mathbf{k}_h, \mathbf{F}^e_h) \mid h \in I\}$ over a set $A \subseteq \mathcal{X}$ if there exist a function $\rho \in \mathcal{K}_\infty$ and $h^* \in I$ such that for all $\mathbf{x} \in A$ and $h \in (0, h^*)$, we have:

$$\|\mathbf{F}^e_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) - \mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))\| \leq h\rho(h). \tag{7}$$

Before establishing a relationship between a Runge-Kutta approximation family and one-step consistency, we state the following lemma we will use throughout this work:

Lemma 1. *For any compact set $K \subset \mathcal{X}$, there is an $\varepsilon \in \mathbb{R}_{++}$ such that $K \oplus \overline{B}_\varepsilon \subset \mathcal{X}$, where $\overline{B}_\varepsilon$ is the closed norm-ball of radius ε and $\oplus$ denotes the Minkowski sum. Moreover, $K \oplus \overline{B}_\varepsilon$ is compact.*

We now provide our first contribution by showing how properties of the dynamics and a family of controllers can be used to establish one-step consistency of the Runge-Kutta approximation family of controller-map pairs with the exact family of controller-map pairs:

Theorem 1. *Suppose $\mathbf{f}$ and $\mathbf{g}$ are locally Lipschitz continuous over $\mathcal{X}$. Let $K \subset \mathcal{X}$ be compact, consider a family of admissible controllers $\{\mathbf{k}_h \mid h \in I\}$, and suppose there exists $h_1 \in I$ and a bound $M_K \in \mathbb{R}_+$ such that for every sample period $h \in (0, h_1)$, the controller $\mathbf{k}_h$ is bounded by M_K over K. Then the family $\{(\mathbf{k}_h, \mathbf{F}^{a,p}_h) \mid h \in I\}$ is one-step consistent with $\{(\mathbf{k}_h, \mathbf{F}^e_h) \mid h \in I\}$ over the set K.*

III. Sampled-Data Control Barrier Functions

In this section we develop a notion of *practical safety* for sampled-data systems, and define *Sampled-Data Control*

Barrier Functions (SD-CBFs) as a tool for safety-critical sampled-data control synthesis. Lastly, we highlight familiar settings which satisfy the properties required by SD-CBFs.

We begin with the following definition relating the evolution of a sampled-data system and a set:

Definition 4 (*Forward Invariance*)**.** A set $\mathcal{C} \subseteq \mathcal{X}$ is *forward invariant* for a controller-map pair $(\mathbf{k}, \mathbf{F})$ if for every $\mathbf{x} \in \mathcal{C}$ and number of steps $k \in \mathbb{Z}_+$, the recursion $\mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k))$ is well-defined and satisfies $\mathbf{x}_k \in \mathcal{C}$.

Remark 3. This definition of forward invariance requires that the system state be contained in the set $\mathcal{C}$ at sample times, which is aligned with the notion of stability for sampled-data systems presented in [14]. This differs from the standard definition of forward invariance used in the existing sampled-data safety literature, which additionally requires that the solution remain in the set $\mathcal{C}$ between sample times, i.e. $\boldsymbol{\varphi}(t) \in \mathcal{C}$ for $t \in [t_k, t_{k+1}]$. As seen in this literature, requiring inter-sample safety typically requires selecting control actions that meet a robustified continuous time barrier derivative condition. This robust condition typically depends on parameters of the system that are difficult to estimate, and using over-approximations may produce very conservative behavior [10]. Reducing this conservativeness usually amounts to operating at exceedingly high sample rates, which may not be practical, and which may excite unmodeled features of the system dynamics. Moreover, in practice, inter-sample safety violations at high sample rates can be inconsequential (and may not even be detectable).

We often do not have a closed-form expression for the exact family of maps and will need to design controllers using an approximate family of maps. The following definition will be used to describe the safety properties of the exact family of controller-map pairs when design is done with approximations:

Definition 5 (*Practical Safety*)**.** A family $\{(\mathbf{k}_h, \mathbf{F}_h) : h \in I\}$ is *practically safe* with respect to a set $\mathcal{C} \subseteq \mathcal{X}$ if for each $R \in \mathbb{R}_{++}$, there exists an $h^* \in I$ such that for each sample period $h \in (0, h^*)$, there is a corresponding set $\mathcal{C}_h \subseteq \mathcal{X}$ that is forward invariant for the controller-map pair $(\mathbf{k}_h, \mathbf{F}_h)$ and satisfies $\mathcal{C} \subseteq \mathcal{C}_h \subseteq \mathcal{C} \oplus \overline{B}_R$.

Remark 4. This definition is posed to mirror that of practical stability for sampled-data systems proposed in [14]. In particular, the burden of proof lies with small values of R. If $R' \geq R$ and $\mathcal{C}_h$ is a forward invariant subset of $\mathcal{C} \oplus \overline{B}_R$, then it is automatically a forward invariant subset of $\mathcal{C} \oplus \overline{B}_{R'}$.

Before defining Sampled-Data Control Barrier Functions, for a non-empty set $\mathcal{C} \subseteq \mathcal{X}$, we denote $d_{\mathcal{C}}(\mathbf{x}) = \inf_{\mathbf{y} \in \mathcal{C}} \|\mathbf{y} - \mathbf{x}\|$ for all $\mathbf{x} \in \mathcal{X}$. We now define Sampled-Data Barrier Functions and Sampled-Data Control Barrier Functions:

Definition 6 (*Sampled-Data Barrier Function Candidate*)**.** Consider a set $\mathcal{C} \subseteq \mathcal{X}$. A collection of functions $\{\mathbf{s}_h \mid h \in I\}$ is a *family of Sampled-Data Barrier Function Candidates* on $\mathcal{C}$ if there exist $h^* \in I$, a function $\alpha \in \mathcal{K}^e$, a radius $\varepsilon \in \mathbb{R}_{++}$, and a Lipschitz constant $M \in \mathbb{R}_{++}$ such that:

$$\mathbf{s}_h(\mathbf{x}_1) > 0, \quad \mathbf{s}_h(\mathbf{x}_2) = 0, \quad \mathbf{s}_h(\mathbf{x}_3) < 0, \tag{8}$$

$$h\alpha(\mathbf{s}_h(\mathbf{x}_4)) \leq \mathbf{s}_h(\mathbf{x}_4), \tag{9}$$

$$|\mathbf{s}_h(\mathbf{x}_5) - \mathbf{s}_h(\mathbf{x}_6)| \leq M\|\mathbf{x}_5 - \mathbf{x}_6\|, \tag{10}$$

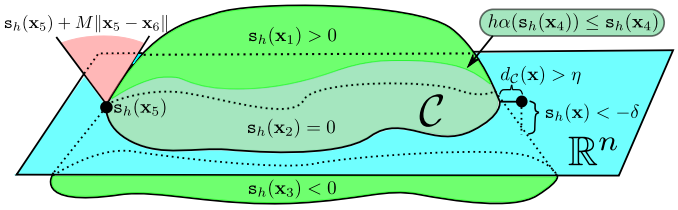

Fig. 1. Visualizing the properties (8, 9, 10, 11) of SD-BF Candidates. The dark green region represents the lower bound $h\alpha(\mathbf{s}_h(\mathbf{x}_4))$ and $\mathbf{s}_h(\mathbf{x}_6)$ cannot be in the red region due to the Lipschitz bound.

for all states $\mathbf{x}_1 \in \text{Int}(\mathcal{C})$, $\mathbf{x}_2 \in \partial\mathcal{C}$, $\mathbf{x}_3 \in \mathcal{X} \setminus \mathcal{C}$, $\mathbf{x}_4 \in \mathcal{C}$, $\mathbf{x}_5, \mathbf{x}_6 \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_\varepsilon)$, and sample periods $h \in (0, h^*)$, and for each $\eta \in \mathbb{R}_{++}$ there exists a $\delta \in \mathbb{R}_{++}$ such that[1]:

$$d_{\mathcal{C}}(\mathbf{x}) > \eta \implies \mathbf{s}_h(\mathbf{x}) < -\delta, \tag{11}$$

for all states $\mathbf{x} \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_\varepsilon)$ and sample periods $h \in (0, h^*)$.

Definition 7 (*Sampled-Data Barrier Control Barrier Functions*)**.** A family of Sampled-Data Barrier Function Candidates $\{\mathbf{s}_h \mid h \in I\}$ is a *family of Sampled-Data Control Barrier Functions* on $\mathcal{C}$ for $\{\mathbf{F}_h \mid h \in I\}$ if for each state $\mathbf{x} \in \mathcal{X}$ and sample time $h \in (0, h^*)$, there exists a corresponding input $\mathbf{u} \in \mathbb{R}^m$ such that $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$ and:

$$\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{u})) - \mathbf{s}_h(\mathbf{x}) \geq -h\alpha(\mathbf{s}_h(\mathbf{x})). \tag{12}$$

Definition 8 (*Sampled-Data Barrier Function*)**.** Given a family of admissible controllers $\{\mathbf{k}_h \mid h \in I\}$, a family of Sampled-Data Barrier Function Candidates $\{\mathbf{s}_h \mid h \in I\}$ is a *family of Sampled-Data Barrier Functions* on $\mathcal{C}$ for $\{(\mathbf{k}_h, \mathbf{F}_h) \mid h \in I\}$ if:

$$\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{x}) \geq -h\alpha(\mathbf{s}_h(\mathbf{x})), \tag{13}$$

for all states $\mathbf{x} \in \mathcal{X}$ and sample times $h \in (0, h^*)$.

Remark 5. We note that the conditions in (8)-(9) are standard conditions required by barrier functions for discrete systems [4]. The inequalities in (8) imply that for each $h \in (0, h^*)$, $\mathcal{C}$ is the 0-superlevel set of $\mathbf{s}_h$. The inequality in (9) places a requirement on the SD-BF decrement through (13) that implies that for each $h \in (0, h^*)$, $\mathcal{C}$ is forward invariant for $(\mathbf{k}_h, \mathbf{F}_h)$. The condition in (10) requires the SD-BF to be Lipschitz continuous over a slightly larger set than $\mathcal{C}$ with a Lipschitz constant that is uniform in the sample period, and will be used to relate exact and approximate families through one-step consistency. The implication in (11) resembles a *coercivity* condition, requiring the SD-BF value to decrease locally outside of the set $\mathcal{C}$ in a way that is uniform in the sample-period. This property will be critical for producing forward invariant sets contained in $\mathcal{C} \oplus \overline{B}_R$ for arbitrarily small values of R. The distinction between the conditions in (13) and (12) are that the former applies as a *certificate* for a closed-loop system, while the latter condition states the possibility of safe control synthesis for an open-loop system.

To more clearly understand the nature of the properties (8)-(12) we will discuss some familiar settings in which they are implied. We first note that as in the continuous time Control

[1]See Theorem 2 for how this property relates to regular values.

Barrier Function literature [3], a continuously differentiable function $\mathbf{s} : \mathcal{X} \to \mathbb{R}$ has $c \in \mathbb{R}$ as a *regular value* if $\mathbf{s}(\mathbf{x}) = c$ implies $\nabla \mathbf{s}(\mathbf{x}) \neq \mathbf{0}$ for all states $\mathbf{x} \in \mathcal{X}$. The following result makes a connection between regular values and ensuring that the property in (11) is satisfied:

Theorem 2. *Suppose that $\mathbf{s} : \mathcal{X} \to \mathbb{R}$ is twice continuously differentiable with a compact 0-superlevel set $\mathcal{C}$ and 0 as a regular value. There is an $\varepsilon \in \mathbb{R}_{++}$ such that each $\eta \in \mathbb{R}_{++}$ corresponds to a $\delta \in \mathbb{R}_{++}$ satisfying:*

$$d_{\mathcal{C}}(\mathbf{x}) > \eta \implies \mathbf{s}(\mathbf{x}) < -\delta. \tag{14}$$

for all states $\mathbf{x} \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\varepsilon})$.

Our next result shows how Lyapunov functions used for practical stability of sampled-data systems [14], [19] yield Sampled-Data Control Barrier Functions:

Theorem 3. *Consider a family of controller map pairs $\{(\mathbf{k}_h, \mathbf{F}_h) \mid h \in I\}$ for which the corresponding family of controllers is admissible. Suppose that for a locally Lipschitz continuous function $V : \mathbb{R}^n \to \mathbb{R}_+$, there exist $\alpha_1, \alpha_2 \in \mathcal{K}_\infty$, $\alpha_3 \in \mathcal{K}$ and $h^* \in I$ such that:*

$$\alpha_1(\|\mathbf{x}_1\|) \leq V(\mathbf{x}_1) \leq \alpha_2(\|\mathbf{x}_1\|), \tag{15}$$

$$V(\mathbf{F}_h(\mathbf{x}_2, \mathbf{k}_h(\mathbf{x}_2))) - V(\mathbf{x}_2) \leq -h\alpha_3(\|\mathbf{x}_2\|), \tag{16}$$

for all $\mathbf{x}_1 \in \mathbb{R}^n$, $\mathbf{x}_2 \in \mathcal{X}$, and sample periods $h \in (0, h^*)$. For any $c \in \mathbb{R}$, define $\Gamma : \mathbb{R} \to \mathcal{P}(\mathcal{X})$ as:

$$\Gamma(c) = \{\mathbf{x} \in \mathcal{X} : V(\mathbf{x}) \leq c\}, \tag{17}$$

for all $c \in \mathbb{R}$. If for some $c^* \in \mathbb{R}_{++}$, $\Gamma(c^*)$ is compact, then for any $c \in (0, c^*)$, the family $\{\mathbf{s}_h : \mathcal{X} \to \mathbb{R} \mid h \in I\}$ satisfying:

$$\mathbf{s}_h(\mathbf{x}) = c - V(\mathbf{x}), \tag{18}$$

for all $\mathbf{x} \in \mathcal{X}$ and $h \in I$ is a family of Sampled-Data Control Barrier Functions on $\Gamma(c)$ for the family $\{\mathbf{F}_h \mid h \in I\}$.

We note that if $\mathcal{X} = \mathbb{R}^n$, the compactness assumption for $\Gamma(c^*)$ is redundant. The lower bound on V in (15) shows that if $\mathbf{x} \in \Gamma(c^*)$, then $\|\mathbf{x}\| \leq \alpha^{-1}(V(\mathbf{x})) \leq \alpha^{-1}(c^*)$, implying $\Gamma(c^*)$ is bounded, and $\Gamma(c^*)$ is closed since it is the preimage of the closed interval $[0, c^*]$ under the continuous function V.

IV. Practical Safety

In this section we establish our main contribution by connecting practical safety and Sampled-Data Barrier Functions.

The following result establishes how a family of SD-BFs for an approximate family of controller-map pairs can be used to ensure the practical safety of the exact family of controller-map pairs via one-step consistency:

Theorem 4. *Consider a set $\mathcal{C} \subseteq \mathcal{X}$ and a family of admissible controllers $\{\mathbf{k}_h \mid h \in I\}$. Suppose that:*

1) *There exists a family of Sampled-Data Barrier Functions on $\mathcal{C}$ for a family $\{(\mathbf{k}_h, \mathbf{F}_h) \mid h \in I\}$.*
2) *There exists an $\varepsilon' \in \mathbb{R}_{++}$ such that the family $\{(\mathbf{k}_h, \mathbf{F}_h) \mid h \in I\}$ is one-step consistent with the exact family $\{(\mathbf{k}_h, \mathbf{F}^e_h) \mid h \in I\}$ over the set $\mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\varepsilon'})$.*

Then the exact family $\{(\mathbf{k}_h, \mathbf{F}^e_h) \mid h \in I\}$ is practically safe with respect to $\mathcal{C}$.

Proof. Let h_1^*, α, ε, and M be defined as in Definition 6. By assumption, there exists an $h_2^* \in I$ and $\rho \in \mathcal{K}$ such that (7) holds for all $\mathbf{x} \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\varepsilon'})$ and $h \in (0, h_2^*)$. Since the family of controllers is assumed to be admissible, there is an $h_3^* \in I$ such that $\mathbf{k}_h$ is h-admissible for each $h \in (0, h_3^*)$.

Let $R \in \mathbb{R}_{++}$, and pick $R' \in \mathbb{R}_{++}$ such that $R' \leq \min\{\varepsilon, \varepsilon', R\}$. By (11), there exist $\delta, \Delta \in \mathbb{R}_{++}$ such that:

$$d_{\mathcal{C}}(\mathbf{x}) > R'/2 \implies s_h(\mathbf{x}) < -\delta, \tag{19}$$

$$d_{\mathcal{C}}(\mathbf{x}) > \delta/(2M) \implies s_h(\mathbf{x}) < -\Delta, \tag{20}$$

for all $\mathbf{x} \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\varepsilon})$. Let $h \in I$ with $h < \min\{h_1^*, h_2^*, h_3^*\}$. For any $c \in \mathbb{R}$, we denote the c-superlevel set of $\mathbf{s}_h$ as:

$$\Omega_{c,h} = \{\mathbf{x} \in \mathcal{X} \mid \mathbf{s}_h(\mathbf{x}) \geq c\}. \tag{21}$$

For any state $\mathbf{x} \in \Omega_{-\delta,h}$, we have $d_{\mathcal{C}}(\mathbf{x}) \leq R'/2$, and thus $\mathcal{C} \subseteq \Omega_{-\delta,h} \subseteq \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{R'/2}) \subseteq \mathcal{C} \oplus \overline{B}_R$.

We will prove that for small enough h, the set $\Omega_{-\delta,h}$ is forward invariant for the controller-map pair $(\mathbf{k}_h, \mathbf{F}^e_h)$. We denote three cases, considering a state $\mathbf{x} \in \mathcal{X}$ such that either **(1)** $\mathbf{x} \in \mathcal{C}$, **(2)** $\mathbf{x} \in \Omega_{-\delta,h} \setminus \mathcal{C}$ and $d_{\mathcal{C}}(\mathbf{x}) \leq \delta/(2M)$, or **(3)** $\mathbf{x} \in \Omega_{-\delta,h} \setminus \mathcal{C}$ and $d_{\mathcal{C}}(\mathbf{x}) > \delta/(2M)$.

Case 1: Suppose $\mathbf{x} \in \mathcal{C}$. From (13) and (9), we have:

$$\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{x}) \geq -h\alpha(\mathbf{s}_h(\mathbf{x})) \geq -\mathbf{s}_h(\mathbf{x}), \tag{22}$$

so $\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) \geq 0$, or $\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \mathcal{C}$. By one-step consistency, we have:

$$\|\mathbf{F}^e_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) - \mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))\| \leq h\rho(h), \tag{23}$$

so if $h\rho(h) \leq \varepsilon$, then $\mathbf{F}^e_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\varepsilon})$. Thus:

$$|\mathbf{s}_h(\mathbf{F}^e_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})))| \leq Mh\rho(h), \tag{24}$$

and if $Mh\rho(h) \leq \delta$ as well, then:

$$\mathbf{s}_h(\mathbf{F}^e_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) \geq \mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - Mh\rho(h) \geq -\delta, \tag{25}$$

giving us $\mathbf{F}^e_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \Omega_{-\delta,h}$. The analysis of this case gives us the requirement $h\rho(h) \leq \min\{\varepsilon, \delta/M\}$.

Before continuing to cases 2 and 3, we establish some additional properties. First, note that the superlevel sets have the containment property $\Omega_{-\delta/2,h} \subseteq \Omega_{-\delta,h}$. Next, for any $\eta \in \mathbb{R}_{++}$ and any $\mathbf{x} \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\varepsilon})$ with $\mathbf{x} \notin \mathcal{C}$, there is a point $\mathbf{y} \in \mathcal{C}$ such that $\|\mathbf{x} - \mathbf{y}\| < d_{\mathcal{C}}(\mathbf{x}) + \eta$. Therefore:

$$\mathbf{s}_h(\mathbf{x}) \geq \mathbf{s}_h(\mathbf{y}) - M\|\mathbf{x} - \mathbf{y}\| \geq -Md_{\mathcal{C}}(\mathbf{x}) - M\eta, \tag{26}$$

since $\mathbf{s}_h(\mathbf{y}) \geq 0$. Since η can be chosen arbitrarily small, we

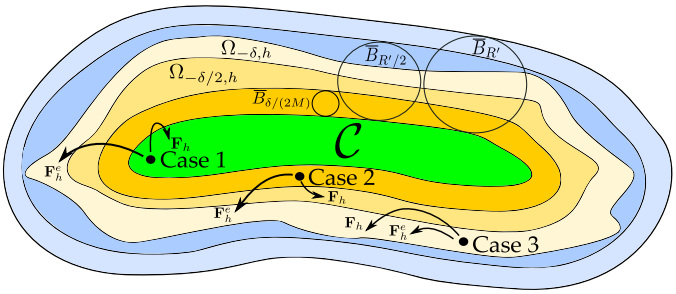

Fig. 2. A visual representation of the main sets and three cases discussed in the proof of Theorem 4.

have $\mathbf{s}_h(\mathbf{x}) \geq -Md_{\mathcal{C}}(\mathbf{x})$. If $d_{\mathcal{C}}(\mathbf{x}) \leq \delta/(2M)$, then $\mathbf{s}_h(\mathbf{x}) \geq -\delta/2$ and so $\mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\delta/(2M)}) \subseteq \Omega_{-\delta/2,h} \subseteq \Omega_{-\delta,h}$.

Next, consider $\mathbf{x} \in \Omega_{-\delta,h} \setminus \mathcal{C}$. Since $\mathbf{x} \notin \mathcal{C}$, meaning $\mathbf{s}_h(\mathbf{x}) < 0$ and thus $\alpha(\mathbf{s}_h(\mathbf{x})) < 0$, we have from (13) that:

$$\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) \geq \mathbf{s}_h(\mathbf{x}) - h\alpha(\mathbf{s}_h(\mathbf{x})) > -\delta. \tag{27}$$

Thus $\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \Omega_{-\delta,h} \subseteq \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{R'/2})$ so we can apply one step consistency to achieve:

$$\|\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) - \mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))\| \leq h\rho(h). \tag{28}$$

If $h\rho(h) \leq R'/2$, then $\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{R'})$, in which case the Lipschitz property of $\mathbf{s}_h$ yields the bound:

$$|\mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})))| \leq Mh\rho(h). \tag{29}$$

Note that because $R'/2 < \varepsilon$, the requirement from Case 1 can be replaced by $h\rho(h) \leq \min\{R'/2, \delta/M\}$.

Case 2: Suppose $\mathbf{x} \in \Omega_{-\delta,h} \setminus \mathcal{C}$ and $d_{\mathcal{C}}(\mathbf{x}) \leq \delta/(2M)$. Since $\mathbf{x} \notin \mathcal{C}$ and $\mathcal{X} \cap (\mathcal{C} \oplus \overline{B}_{\delta/(2M)}) \subseteq \Omega_{-\delta/2,h}$, we have $-\delta/2 \leq \mathbf{s}_h(\mathbf{x}) < 0$. Therefore:

$$\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) \geq \mathbf{s}_h(\mathbf{x}) - h\alpha(\mathbf{s}_h(\mathbf{x})) \geq -\delta/2, \tag{30}$$

so $\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \Omega_{-\delta/2,h}$. By adding and subtracting $\mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})))$ and using (29), we have:

$$\mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) \geq -Mh\rho(h) - \delta/2, \tag{31}$$

when $h\rho(h) \leq R'/2$. If $Mh\rho(h) \leq \delta/2$ as well, then $\mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) \geq -\delta$, or $\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \Omega_{-\delta,h}$. Thus we update the requirements to be $h\rho(h) \leq \min\{R'/2, \delta/(2M)\}$.

Case 3: Suppose $\mathbf{x} \in \Omega_{-\delta,h} \setminus \mathcal{C}$ and $d_{\mathcal{C}}(\mathbf{x}) > \delta/(2M)$. From (20), we have:

$$\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{x}) > -h\alpha(-\Delta). \tag{32}$$

Adding and subtracting $\mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})))$ and (29) yields:

$$\begin{aligned} \mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) &> \mathbf{s}_h(\mathbf{x}) - Mh\rho(h) - h\alpha(-\Delta), &(33)\\ &= \mathbf{s}_h(\mathbf{x}) - h(M\rho(h) + \alpha(-\Delta)), &(34)\end{aligned}$$

when $h\rho(h) \leq R'/2$. If $M\rho(h) \leq -\alpha(-\Delta)$ as well, then $\mathbf{s}_h(\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) > \mathbf{s}_h(\mathbf{x}) \geq -\delta$, or $\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \in \Omega_{-\delta,h}$.

To conclude, if both:

1) $h < \min\left\{h_1^*, h_2^*, h_3^*, \rho^{-1}(-\alpha(-\Delta)/M)\right\}$,
2) $h\rho(h) \leq \min\{R'/2, \delta/(2M)\}$,

then the set $\mathcal{C}_h \triangleq \Omega_{-\delta,h} \subseteq \mathcal{C} \oplus \overline{B}_R$ is forward invariant for the controller-map pair $(\mathbf{k}_h, \mathbf{F}_h^e)$, and thus the family $\{(\mathbf{k}_h, \mathbf{F}_h^e) \mid h \in I\}$ is practically safe with respect to $\mathcal{C}$. □

V. Control Synthesis & Simulation

In this section we present a result on the convexity of the CBF decrement condition, and define an optimization-based controller via an SD-CBF for achieving practical safety. We deploy this controller in simulation on an inverted and double inverted pendulum.

The following result establishes how for a system with a block integrator structure, a Runge-Kutta approximation family of maps of the appropriate order can preserve a convexity property of a family $\{\mathbf{s}_h \mid h \in I\}$:

Theorem 5. *Consider $\ell, \gamma \in \mathbb{N}$ such that $n = \ell\gamma$. Suppose the system dynamics have the form:*

$$\dot{\mathbf{x}} = \underbrace{\begin{bmatrix} \mathbf{0} & \mathbf{I} & & \\ & \ddots & \ddots & \\ & & \mathbf{0} & \mathbf{I} \\ & & & \mathbf{0} \end{bmatrix}}_{\mathbf{A}} \mathbf{x} + \underbrace{\begin{bmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{f}_\gamma(\mathbf{x}) + \mathbf{g}_\gamma(\mathbf{x})\mathbf{u} \end{bmatrix}}_{\mathbf{r}(\mathbf{x},\mathbf{u})}, \tag{35}$$

where $\mathbf{f}_\gamma : \mathbb{R}^n \to \mathbb{R}^\ell$ and $\mathbf{g}_\gamma : \mathbb{R}^n \to \mathbb{R}^{\ell \times m}$. For each $h \in I$, consider a function $\mathbf{s}_h : \mathbb{R}^n \to \mathbb{R}$, and suppose there exists a function $\tilde{\mathbf{s}}_h : (\mathbb{R}^\ell)^q \to \mathbb{R}$ satisfying:

$$\mathbf{s}_h(\mathbf{x}) = \tilde{\mathbf{s}}_h(\boldsymbol{\zeta}_1, \ldots, \boldsymbol{\zeta}_q), \tag{36}$$

for all $\mathbf{x} = (\boldsymbol{\zeta}_1, \ldots, \boldsymbol{\zeta}_\gamma) \in (\mathbb{R}^\ell)^\gamma \simeq \mathbb{R}^n$. If the function $\tilde{\mathbf{s}}_h$ is concave with respect to its last argument and $\mathbf{F}_h^{a,p} : \mathcal{Z} \to \mathbb{R}^n$ is a Runge-Kutta Approximation map with $p = \gamma - q + 1$, then for $\alpha \in \mathcal{K}^e$, then the function $\phi_h : \mathcal{Z} \to \mathbb{R}$ defined as:

$$\phi_h(\mathbf{x}, \mathbf{u}) = -\mathbf{s}_h(\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u})) + \mathbf{s}_h(\mathbf{x}) - h\alpha(\mathbf{s}_h(\mathbf{x})), \tag{37}$$

is convex in its second argument.

The synthesis of safety-critical controllers using Control Barrier Functions is frequently achieved using convex optimization (typically quadratic programs) [3]. The following result highlights how we may similarly synthesize a family of controllers that achieve practical safety through optimization:

Theorem 6. *Let $\{\mathbf{s}_h \mid h \in I\}$ be a family of SD-CBFs on $\mathcal{C}$ for a family $\{\mathbf{F}_h^{a,p} \mid h \in I\}$ such that the set:*

$$\mathcal{F}(\mathbf{x}) = \{\mathbf{u} \in \mathbb{R}^m \mid (\mathbf{x}, \mathbf{u}) \in \mathcal{Z} \text{ and } \phi_h(\mathbf{x}, \mathbf{u}) \geq 0\}, \tag{38}$$

is closed and convex for each $h \in I$ and $\mathbf{x} \in \mathcal{X}$. Consider a set of controllers $\{\mathbf{k}_h \mid h \in I\}$ satisfying:

$$\begin{aligned} \mathbf{k}_h(\mathbf{x}) = \underset{\mathbf{u} \in \mathbb{R}^m}{\operatorname{argmin}} \ & \frac{1}{2}\|\mathbf{u} - \mathbf{k}_d(\mathbf{x})\|_2^2 && \text{(SD-CBF-OP)}\\ \text{s.t. } & \mathbf{s}_h(\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u})) - \mathbf{s}_h(\mathbf{x}) \geq -h\alpha(\mathbf{s}_h(\mathbf{x})), \end{aligned}$$

for each $\mathbf{x} \in \mathcal{X}$ and $h \in (0, h^*)$, where $\mathbf{k}_d : \mathcal{X} \to \mathbb{R}^m$ is a nominal controller. If $\{\mathbf{k}_h \mid h \in I\}$ is a family of admissible controllers, then $\{\mathbf{s}_h \mid h \in I\}$ is a family of Sampled-Data Barrier Functions on $\mathcal{C}$ for $\{(\mathbf{k}_h, \mathbf{F}_h^{a,p}) \mid h \in I\}$.

We use this controller in simulation on fully-actuated single and double inverted pendulums, with dynamics given by:

$$\mathbf{D}(\mathbf{q})\ddot{\mathbf{q}} + \mathbf{C}(\mathbf{q}, \dot{\mathbf{q}})\dot{\mathbf{q}} + \mathbf{G}(\mathbf{q}) = \mathbf{u} \tag{39}$$

where $\mathbf{D}$, $\mathbf{C}$, and $\mathbf{G}$ are functions encoding inertia, Coriolis, and gravity terms, $\mathbf{q}, \dot{\mathbf{q}} \in \mathbb{R}^m$ are configuration and velocity vectors, and $\mathbf{u} \in \mathbb{R}^m$ is a torque vector. These terms are detailed in Table I. With state vector $\mathbf{x} = (\mathbf{q}, \dot{\mathbf{q}}) \in \mathbb{R}^n$, the dynamics in (39) can be expressed in the form (35), where $\ell = m$ and $\gamma = 2$. For the single inverted pendulum we use safe sets with the form of a Lyapunov sublevel set ($\mathbf{s}_h(\mathbf{x}) = 1 - \mathbf{x}^\top \mathbf{P}\mathbf{x}$ with $\mathbf{P} \in \mathbb{S}_{++}^2$ obtained from feedback linearization), a configuration ellipsoid ($\tilde{\mathbf{s}}_h(\theta) = 1 - \theta^2$), and a halfspace ($\tilde{\mathbf{s}}_h(\theta) = \theta + 0.1$). For the double inverted pendulum we enforce safety of a configuration ellipsoid ($\tilde{\mathbf{s}}(\mathbf{q}) = 1 - \|\mathbf{q}\|_2^2$). We use a Runge-Kutta approximation with

System	$\mathbf{q}$	$\mathbf{D} : \mathbb{R}^m \to \mathbb{S}^m_{++}$	$\mathbf{C} : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}^{m\times m}$	$\mathbf{G} : \mathbb{R}^m \to \mathbb{R}^m$
Single	θ	1	0	$-\sin\theta$
Double	$\begin{bmatrix}\theta_1\\ \theta_2\end{bmatrix}$	$\begin{bmatrix}3+2\cos\theta_2 & 1+\cos\theta_2\\ 1+\cos\theta_2 & 1\end{bmatrix}$	$\begin{bmatrix}0 & -(2\dot\theta_1+\dot\theta_2)\sin\theta_2\\ \frac{1}{2}(2\dot\theta_1+\dot\theta_2)\sin\theta_2 & -\frac{1}{2}\dot\theta\sin\theta_2\end{bmatrix}$	$\begin{bmatrix}-2\sin\theta_1-\sin(\theta_1+\theta_2)\\ -\sin(\theta_1+\theta_2)\end{bmatrix}$

TABLE I. Terms in pendulum dynamics given by 39. Angles are taken clockwise from upright, and θ_2 is taken relative to θ_1.

$p = 1$ (forward Euler) for the Lyapunov sublevel set and $p = 2$ (midpoint rule) for the other settings. Controllers of the form (SD-CBF-OP) are employed; for the Lyapunov sublevel set, $\mathbf{k}_d$ is a feedback linearizing controller with auxiliary PD control, and for the other settings, $\mathbf{k}_d$ is a zero (constant) controller. With 11 sample periods spaced logarithmically between 0.05 and 0.5 seconds and initial conditions sampled from each safe set, the closed-loop systems are simulated for 10 seconds. For the inverted pendulum, 500 initial states are sampled uniformly from the Lyapunov sublevel set, and 41×41 grids of initial states cover $[-1, 1]\times[-5, 5]$ for the configuration ellipsoid and $[-0.1, 1] \times [-5, 5]$ for the halfspace. For the double inverted pendulum, 500 initial states are drawn with configurations sampled uniformly from the unit Euclidean ball in $\mathbb{R}^2$ and velocities sampled uniformly from $[-1, 1]^2$. The worst-case distances from the safe sets are reported as a function of sample period in Fig. 3. These distances decrease with sample period for the inverted pendulum, and decrease for sufficiently small sample periods for the double inverted pendulum.

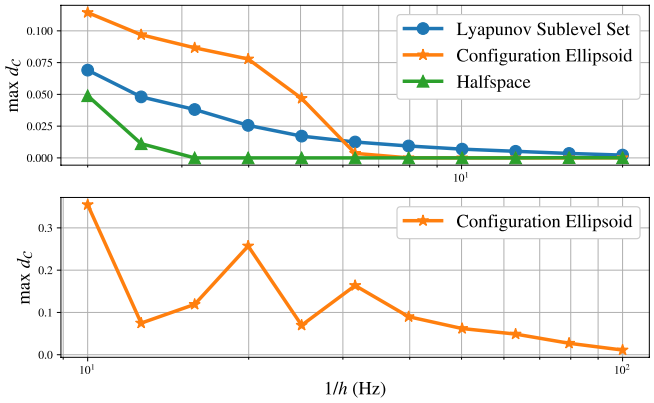

Fig. 3. The maximum distance from the safe set $\mathcal{C}$ (lower is better) achieved during trials vs. the the sampling frequency. The simulations and corresponding animations be found at https://bit.ly/CBF-OP and https://vimeo.com/690803272. **Top:** The inverted pendulum for 3 different safe sets. **Bottom:** The double inverted pendulum.

VI. Conclusion

In this work we have developed a novel approach for safety-critical sampled-data control through approximate discrete time models. Our main contribution, Sampled-Data Control Barrier Functions, provides a tool for designing practically safe controllers. Future work will study the relationship between approximation maps and control methods like backstepping.

References

[1] S. Monaco and D. Normand-Cyrot, "Advanced tools for nonlinear sampled-data systems' analysis and control," in *2007 European Control Conference (ECC)*, 2007, pp. 1155–1158.

[2] A. Ames, J. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *Conference on Decision & Control (CDC)*. IEEE, 2014, pp. 6271–6278.

[3] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *European Control Conference (ECC)*. IEEE, 2019, pp. 3420–3431.

[4] A. Agrawal and K. Sreenath, "Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation." in *Robotics: Science and Systems (RSS)*, vol. 13. Cambridge, MA, USA, 2017.

[5] A. Ghaffari, I. Abel, D. Ricketts, S. Lerner, and M. Krstić, "Safety verification using barrier certificates with application to double integrator with input saturation and zero-order hold," in *American Control Conference (ACC)*. IEEE, 2018, pp. 4664–4669.

[6] W. S. Cortez, D. Oetomo, C. Manzie, and P. Choong, "Control barrier functions for mechanical systems: Theory and application to robotic grasping," *Transactions on Control Systems Technology*, 2019.

[7] T. Gurriet, P. Nilsson, A. Singletary, and A. D. Ames, "Realizable set invariance conditions for cyber-physical systems," in *American Control Conference (ACC)*. IEEE, 2019, pp. 3642–3649.

[8] G. Yang, C. Belta, and R. Tron, "Self-triggered control for safety critical systems using control barrier functions," in *American Control Conference (ACC)*. IEEE, 2019, pp. 4454–4459.

[9] A. Singletary, Y. Chen, and A. D. Ames, "Control barrier functions for sampled-data systems with input delays," in *Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 804–809.

[10] J. Breeden, K. Garg, and D. Panagou, "Control barrier functions in sampled-data systems," *Control Systems Letters*, 2021.

[11] J. Usevitch and D. Panagou, "Adversarial resilience for sampled-data systems using control barrier function methods," in *American Control Conference (ACC)*. IEEE, 2021, pp. 758–763.

[12] L. Niu, H. Zhang, and A. Clark, "Safety-critical control synthesis for unknown sampled-data systems via control barrier functions," *arXiv preprint arXiv:2109.13415*, 2021.

[13] Y. Zhang, S. Walters, and X. Xu, "Control barrier function meets interval analysis: Safety-critical control with measurement and actuation uncertainties," *arXiv preprint arXiv:2110.00915*, 2021.

[14] D. Nešić, A. R. Teel, and P. V. Kokotović, "Sufficient conditions for stabilization of sampled-data nonlinear systems via discrete-time approximations," *Systems & Control Letters*, vol. 38, no. 4-5, pp. 259–270, 1999.

[15] D. Nesic and A. R. Teel, "A framework for stabilization of nonlinear sampled-data systems based on their approximate discrete-time models," *Transactions on Automatic Control*, vol. 49, no. 7, pp. 1103–1122, 2004.

[16] ——, "Backstepping on the euler approximate model for stabilization of sampled-data nonlinear systems," in *Conference on Decision and Control (CDC)*, vol. 2. IEEE, 2001, pp. 1737–1742.

[17] L. Grüne and D. Nesic, "Optimization-based stabilization of sampled-data nonlinear systems via their approximate discrete-time models," *SIAM Journal on Control and Optimization*, vol. 42, no. 1, pp. 98–122, 2003.

[18] D. Nešić and L. Grüne, "Lyapunov-based continuous-time nonlinear controller redesign for sampled-data implementation," *Automatica*, vol. 41, no. 7, pp. 1143–1156, 2005.

[19] A. J. Taylor, V. D. Dorobantu, Y. Yue, P. Tabuada, and A. D. Ames, "Sampled-data stabilization with control lyapunov functions via quadratically constrained quadratic programs," *Control Systems Letters*, vol. 6, pp. 680–685, 2022.

[20] D. S. Laila and D. Nešić, "Changing supply rates for input–output to state stable discrete-time nonlinear systems with applications," *Automatica*, vol. 39, no. 5, pp. 821–835, 2003.

[21] C. M. Kellett, "A compendium of comparison function results," *Mathematics of Control, Signals, and Systems*, vol. 26, no. 3, pp. 339–374, 2014.

[22] 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.

[23] C. D. Aliprantis and K. C. Border, *Infinite dimensional analysis: A Hitchhiker's Guide*. Springer, 2006.

APPENDIX

A. Proof of Lemma 1

Proof. Since $\mathcal{X}$ is open, for every $\mathbf{x} \in K$, there is a corresponding open ball centered at $\mathbf{x}$ that is contained in $\mathcal{X}$; let $\delta_{\mathbf{x}} \in \mathbb{R}_{++}$ denote the radius of this ball, and let $B_{\mathbf{x}} \subset \mathcal{X}$ denote the open ball centered at $\mathbf{x}$ of radius $\delta_{\mathbf{x}}/2$. Consider the collection $\{B_{\mathbf{x}} : \mathbf{x} \in K\}$. This collection is an open cover for the compact set K, implying some finite sub-collection also covers K. Suppose this finite subcover is $B_{\mathbf{x}_1}, \ldots, B_{\mathbf{x}_N}$ for some $\mathbf{x}_1, \ldots, \mathbf{x}_N \in K$, respectively. Let $\delta = \min_i \delta_{\mathbf{x}_i}$, and consider any $\mathbf{z} \in K \oplus \overline{B}_{\delta/4}$. There is some $\mathbf{x} \in K$ such that $\|\mathbf{z} - \mathbf{x}\| \leq \delta/4$. Moreover, there is some $i \in \{1, \ldots, N\}$ such that $\|\mathbf{x} - \mathbf{x}_i\| < \delta_{\mathbf{x}_i}/2$. By the triangle inequality, $\|\mathbf{z} - \mathbf{x}_i\| < \delta/4 + \delta_{\mathbf{x}_i}/2 < \delta_{\mathbf{x}_i}$, implying that $\mathbf{z} \in \mathcal{X}$. Since $\mathbf{z}$ was arbitrary, $K \oplus \overline{B}_{\delta/4} \subseteq \mathcal{X}$, so pick $\varepsilon \leq \delta/4$. To see that $K \oplus \overline{B}_{\varepsilon}$ is compact, note that the product $K \times \overline{B}_{\varepsilon}$ is compact and the map $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} + \mathbf{y}$ is continuous. □

B. Proof of Theorem 1

Proof. Consider a compact set $K \subset \mathcal{X}$ and corresponding $h_1 \in I$ and $M_K \in \mathbb{R}_{++}$, and fix a sample period $h \in (0, h_1)$. By Lemma 1, there exists an $\varepsilon \in \mathbb{R}_{++}$ such that the compact set $N = K \oplus \overline{B}_{\varepsilon}$ satisfies $N \subset \mathcal{X}$. By assumption, $\mathbf{k}_h$ is bounded on K, and since $\mathbf{f}$ and $\mathbf{g}$ are continuous, $\mathbf{f}$ and $\mathbf{g}$ are bounded on N, implying there exists an $M \in \mathbb{R}_{++}$ such that:

$$\|\mathbf{f}(\mathbf{z}) + \mathbf{g}(\mathbf{z})\mathbf{k}_h(\mathbf{y})\| \leq M, \tag{40}$$

for all $\mathbf{y} \in K$ and $\mathbf{z} \in N$. As $\mathbf{f}$ and $\mathbf{g}$ are locally Lipschitz continuous over $\mathcal{X}$, it follows that $\mathbf{f}$ and $\mathbf{g}$ are globally Lipschitz continuous over N. Therefore:

$$\begin{aligned} &\|\mathbf{f}(\mathbf{z}) + \mathbf{g}(\mathbf{z})\mathbf{k}_h(\mathbf{y}) - \mathbf{f}(\mathbf{y}) + \mathbf{g}(\mathbf{y})\mathbf{k}_h(\mathbf{y}))\| \\ &\quad \leq \|\mathbf{f}(\mathbf{z}) - \mathbf{f}(\mathbf{y})\| + \|\mathbf{g}(\mathbf{z}) - \mathbf{g}(\mathbf{y})\|\|\mathbf{k}_h(\mathbf{y})\| \\ &\quad \leq (L_{\mathbf{f}} + L_{\mathbf{g}} M_k)\|\mathbf{z} - \mathbf{y}\| = \rho(\|\mathbf{z} - \mathbf{y}\|), \end{aligned} \tag{41}$$

for all states $\mathbf{y} \in K$ and $\mathbf{z} \in N$, where $L_{\mathbf{f}}, L_{\mathbf{g}} \in \mathbb{R}_{++}$ are Lipschitz constants for $\mathbf{f}$ and $\mathbf{g}$, respectively, and $\rho \in \mathcal{K}_\infty$ satisfies $\rho(r) = (L_{\mathbf{f}} + L_{\mathbf{g}} M_k) r$ for all $r \in \mathbb{R}_+$. Let $\mathbf{x} \in K$. We then have that:

$$\begin{aligned} &\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) - \mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) \\ &= \int_0^h [\mathbf{f}(\boldsymbol{\varphi}(t)) + \mathbf{g}(\boldsymbol{\varphi}(t))\mathbf{k}_h(\mathbf{x})] \, \mathrm{d}t \\ &\qquad - h \sum_{i=1}^p b_i (\mathbf{f}(\mathbf{z}_i) + \mathbf{g}(\mathbf{z}_i)\mathbf{k}_h(\mathbf{x})) \\ &= \int_0^h [\mathbf{f}(\boldsymbol{\varphi}(t)) + \mathbf{g}(\boldsymbol{\varphi}(t))\mathbf{k}_h(\mathbf{x}) - (\mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{k}_h(\mathbf{x}))] \, \mathrm{d}t \\ &\quad + h \sum_{i=1}^p b_i [\mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x})\mathbf{k}_h(\mathbf{x}) - (\mathbf{f}(\mathbf{z}_i) + \mathbf{g}(\mathbf{z}_i)\mathbf{k}_h(\mathbf{x}))], \end{aligned} \tag{42}$$

where we make use of the fact $\sum_{i=1}^p b_i = 1$.

To bound the first term in (42), let $h_2 \in (0, h_1)$ satisfy $h_2 < \varepsilon/M$. By continuity of $\boldsymbol{\varphi}$, if $\boldsymbol{\varphi}(t_0) \notin N$ for any $t_0 \in I$, then there is a minimal time $t^* \in (0, t_0)$ such that $\|\boldsymbol{\varphi}(t) - \mathbf{x}\| < \varepsilon$ for all $t \in [0, t^*)$ and $\|\boldsymbol{\varphi}(t^*) - \mathbf{x}\| = \varepsilon$. We have:

$$\|\boldsymbol{\varphi}(t) - \mathbf{x}\| \leq \int_0^t \|\mathbf{f}(\boldsymbol{\varphi}(s)) + \mathbf{g}(\boldsymbol{\varphi}(s))\mathbf{k}_h(\mathbf{x})\| \, \mathrm{d}s \leq Mt, \tag{43}$$

for all $t \in [0, t^*]$. Since $\varepsilon = \|\boldsymbol{\varphi}(t^*) - \mathbf{x}\| \leq Mt^*$, we know that $t^* \geq \varepsilon/M > h_2$. Thus if $h \in (0, h_2)$, then:

$$\|\boldsymbol{\varphi}(t) - \mathbf{x}\| \leq Mt \leq Mh < Mh_2 < \varepsilon, \tag{44}$$

for all $t \in [0, h]$, implying $\boldsymbol{\varphi}(t) \in N$ for all $t \in [0, h]$.

To bound the second term in (42), we show by induction that if h is sufficiently small, then $\mathbf{z}_i \in N$ for all $i \in \{1, \ldots, p\}$. First, since $\mathbf{z}_1 = \mathbf{x}$, we have $\mathbf{z}_1 \in N$. Next, for $i \in \{1, \ldots, p\}$, suppose $\mathbf{z}_j \in N$ for all $j \in \{1, \ldots, i-1\}$. Considering the definition of $\mathbf{z}_i$ in (6) and the bound (40), we have that:

$$\begin{aligned} \|\mathbf{z}_i - \mathbf{x}\| &\leq h \sum_{j=1}^{i-1} |a_{i,j}| \|\mathbf{f}(\mathbf{z}_j) + \mathbf{g}(\mathbf{z}_j)\mathbf{k}_h(\mathbf{x})\| \\ &\leq Mh \sum_{j=1}^{i-1} |a_{i,j}| \leq Mh(p-1) \max_{j,k} |a_{j,k}| \triangleq Lh \end{aligned} \tag{45}$$

Let $h^* \in (0, h_2)$ satisfy $h^* < \varepsilon/L$. Then for $h \in (0, h^*)$, we have $\|\mathbf{z}_i - \mathbf{x}\| < \varepsilon$, or $\mathbf{z}_i \in N$. Since this choice of h^* does not depend on i, we can conclude by induction that if $h \in (0, h^*)$, then $\mathbf{z}_i \in N$ for all $i \in \{1, \ldots, p\}$.

We have shown that if $h \in (0, h^*)$, then $\boldsymbol{\varphi}(t) \in N$ for all $t \in [0, h]$, and $\mathbf{z}_i \in N$ for $i \in \{1, \ldots, p\}$. Thus using the bound (41) in (42), we have that:

$$\begin{aligned} &\|\mathbf{F}_h^e(\mathbf{x}, \mathbf{k}_h(\mathbf{x})) - \mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))\| \\ &\quad \leq \int_0^h \rho(\|\boldsymbol{\varphi}(t) - \mathbf{x}\|) \, \mathrm{d}t + h \sum_{i=1}^p b_i \rho(\|\mathbf{z}_i - \mathbf{x}\|) \\ &\quad \leq h\rho(Mh) + h \sum_{i=1}^p b_i \rho(Lh) \\ &\quad = h\rho(Mh) + h\rho(Lh) \leq h\tilde{\rho}(h) \end{aligned} \tag{46}$$

where $\tilde{\rho} \in \mathcal{K}$ is defined as:

$$\tilde{\rho}(r) = \rho(Mr) + \rho(Lr) \tag{47}$$

for all $r \in \mathbb{R}_+$. □

C. Proof of Theorem 2

Proof. The boundary $\partial\mathcal{C}$ is a closed subset of the compact set $\mathcal{C}$ and is therefore compact. Thus, there is a lower bound $\sigma \in \mathbb{R}_+$ with $\min_{\mathbf{x} \in \partial\mathcal{C}} \|\nabla \mathbf{s}(\mathbf{x})\|_2 = \sigma$, and since 0 is a regular value, $\sigma > 0$. By Lemma 1, there is an $\varepsilon' \in \mathbb{R}_{++}$ with $\mathcal{C} \oplus \overline{B}_{\varepsilon'} \subset \mathcal{X}$ and $\mathcal{C} \oplus \overline{B}_{\varepsilon'}$ compact.

Consider a state $\mathbf{x} \in \mathcal{C} \oplus \overline{B}_{\varepsilon'}$ with $\mathbf{x} \notin \mathcal{C}$. There exists a $\mathbf{y} \in \partial\mathcal{C}$ such $d_{\mathcal{C}}(\mathbf{x}) = \|\mathbf{y} - \mathbf{x}\|$. Since $\mathbf{s}$ has 0 as a regular value, by [22, Proposition 1.1.9] we have that:

$$\nabla \mathbf{s}(\mathbf{y}) = -\|\nabla \mathbf{s}(\mathbf{y})\|_2 \frac{\mathbf{x} - \mathbf{y}}{\|\mathbf{x} - \mathbf{y}\|_2}. \tag{48}$$

As $\overline{B}_{\varepsilon'}$ is convex, we have that $(1 - \lambda)\mathbf{y} + \lambda\mathbf{x} \in \mathcal{C} \oplus \overline{B}_{\varepsilon'}$ for all $\lambda \in [0, 1]$. For some $\lambda^* \in (0, 1)$, the state $\boldsymbol{\xi} \triangleq (1 -$

$\lambda^*)\mathbf{y} + \lambda^*\mathbf{x}$ satisfies:

$$\begin{aligned}\mathbf{s}(\mathbf{x}) &= \mathbf{s}(\mathbf{y}) + (\mathbf{x}-\mathbf{y})^\top \nabla \mathbf{s}(\mathbf{y}) \\ &\quad + \frac{1}{2}(\mathbf{x}-\mathbf{y})^\top \nabla^2 \mathbf{s}(\boldsymbol{\xi})(\mathbf{x}-\mathbf{y}) \quad (49)\\ &= -\|\nabla \mathbf{s}(\mathbf{y})\|_2 \|\mathbf{x}-\mathbf{y}\|_2 + \frac{1}{2}(\mathbf{x}-\mathbf{y})^\top \nabla^2 \mathbf{s}(\boldsymbol{\xi})(\mathbf{x}-\mathbf{y}). \quad (50)\end{aligned}$$

Since $\mathcal{C} \oplus \overline{B}_{\varepsilon'}$ is compact, there is an upper bound $\mu \in \mathbb{R}_+$ such that $\max_{\mathbf{z} \in \mathcal{C} \oplus \overline{B}_{\varepsilon'}} \|\nabla^2 \mathbf{s}(\mathbf{z})\|_2 = \mu$, we have:

$$\begin{aligned}\mathbf{s}(\mathbf{x}) &\leq -\sigma \|\mathbf{x}-\mathbf{y}\|_2 + \frac{1}{2}\mu \|\mathbf{x}-\mathbf{y}\|_2^2 \quad (51)\\ &= -(\sigma - \frac{\mu}{2}\|\mathbf{x}-\mathbf{y}\|_2)\|\mathbf{x}-\mathbf{y}\|_2. \quad (52)\end{aligned}$$

Since norms are equivalent in finite dimensions, we have coefficients $c_1, c_2 \in \mathbb{R}_{++}$ with $c_1 \leq c_2$ such that:

$$c_1 \|\mathbf{x}-\mathbf{y}\| \leq \|\mathbf{x}-\mathbf{y}\|_2 \leq c_2 \|\mathbf{x}-\mathbf{y}\|. \quad (53)$$

If $\|\mathbf{x}-\mathbf{y}\|_2 \leq \sigma/\mu$, then:

$$\mathbf{s}(\mathbf{x}) \leq -\frac{\sigma}{2}\|\mathbf{x}-\mathbf{y}\|_2 \leq -\frac{c_1\sigma}{2}\|\mathbf{x}-\mathbf{y}\| = -\frac{c_1\sigma}{2} d_{\mathcal{C}}(\mathbf{x}). \quad (54)$$

Finally, we pick $\varepsilon \in \mathbb{R}_{++}$ such that $\varepsilon \leq \min\{\varepsilon', \sigma/(\mu c_2)\}$, and for any $\eta \in \mathbb{R}_{++}$, we pick $\delta \in \mathbb{R}_{++}$ such that $\delta < c_1\sigma\eta/2$. □

D. Proof of Theorem 3

Before proving this result, we review the following continuity definition for set-valued maps:

Definition 9 (*Upper Hemicontinuity* [23])**.** Consider a set-valued function $\Gamma : \mathbb{R} \to \mathcal{P}(\mathcal{X})$; that is, for any $a \in \mathbb{R}$, $\Gamma(a)$ is a subset of $\mathcal{X}$. For some $a \in \mathbb{R}$, if $\Gamma(a) \subseteq \mathcal{X}$ is compact, then Γ is *upper hemicontinuous* at a when the following equivalent conditions are satisfied:

1) For any open set $V \subseteq \mathcal{X}$ with $\Gamma(a) \subseteq V$, there is an open set $U \subseteq \mathbb{R}$ with $\Gamma(a') \subseteq V$ for all $a' \in U$,
2) For any real-valued sequence $\{a_n \in \mathbb{R} \mid n \in \mathbb{N}\}$ converging to a and any state-valued sequence $\{\mathbf{x}_n \in \mathcal{X} \mid n \in \mathbb{N}\}$ with $\mathbf{x}_n \in \Gamma(a_n)$ for all $n \in \mathbb{N}$, there is a subsequence of the state-valued sequence converging to a limit in $\Gamma(a)$.

The equivalence of these conditions is established in [23, Theorem 17.20]. We now proceed to prove Theorem 3:

Proof. For all sample periods $h \in I$, (8) is satisfied by construction. For a sample period $h \in (0, h^*)$, we have:

$$\begin{aligned}&\mathbf{s}_h(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{x}) = -V(\mathbf{F}_h(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) + V(\mathbf{x}) \\ &\quad \geq h\alpha_3(\|\mathbf{x}\|) \geq h\alpha_3(\alpha_2^{-1}(V(\mathbf{x}))), \quad (55)\end{aligned}$$

for all $\mathbf{x} \in \mathcal{X}$. Note that $\alpha_3 \circ \alpha_2^{-1} \in \mathcal{K}$. Pick any $\gamma \in \mathbb{R}_{++}$, and define $\alpha_e \in \mathcal{K}^e$ as:

$$\alpha_e(r) = \begin{cases} \gamma r & r \geq 0, \\ -\alpha_3(\alpha_2^{-1}(-r)) & r < 0, \end{cases} \quad (56)$$

for all $r \in \mathbb{R}$. Fix a state $\mathbf{x} \in \mathcal{X}$. If $\mathbf{s}_h(\mathbf{x}) \geq 0$, then:

$$\alpha_3(\alpha_2^{-1}(V(\mathbf{x}))) \geq 0 \geq -\gamma \mathbf{s}_h(\mathbf{x}) = -\alpha_e(\mathbf{s}_h(\mathbf{x})). \quad (57)$$

Otherwise, if $\mathbf{s}_h(\mathbf{x}) < 0$, then $V(\mathbf{x}) > c$, so:

$$\begin{aligned}\alpha_3(\alpha_2^{-1}(V(\mathbf{x}))) &\geq \alpha_3(\alpha_2^{-1}(V(\mathbf{x}) - c)) \quad (58)\\ &= \alpha_3(\alpha_2^{-1}(-\mathbf{s}_h(\mathbf{x}))) = -\alpha_e(\mathbf{s}_h(\mathbf{x})). \quad (59)\end{aligned}$$

Thus (13) holds using α_e, and $\mathbf{k}_h(\mathbf{x})$ can be used in (12). Moreover, we have that (9) holds for all $h \leq 1/\gamma$.

Since $\Gamma(c) \subseteq \Gamma(c^*)$, we have that $\Gamma(c)$ is bounded, and $\Gamma(c)$ is closed since it is the preimage of the closed interval $[0, c]$ under the continuous function V. Therefore, $\Gamma(c)$ is compact, and Lemma 1 implies there is an $\varepsilon \in \mathbb{R}_{++}$ such that $\Gamma(c) \oplus \overline{B}_\varepsilon \subset \mathcal{X}$ and $\Gamma(c) \oplus \overline{B}_\varepsilon$ is compact. Since V is locally Lipschitz continuous on $\mathcal{X}$, we can choose a global Lipschitz constant over $\Gamma(c) \oplus \overline{B}_\varepsilon$, such that (10) holds.

To show that (11) holds, consider a real-valued sequence $\{c_n \in \mathbb{R} \mid n \in \mathbb{N}\}$ converging to c and a state-valued sequence $\{\mathbf{x}_n \in \mathcal{X} \mid n \in \mathbb{N}\}$ with $\mathbf{x}_n \in \Gamma(c_n)$. For any $\varepsilon' \in \mathbb{R}_{++}$ with $c + \varepsilon' < c^*$, there is a corresponding $N_{\varepsilon'} \in \mathbb{N}$ such that $|c - c_n| < \varepsilon'$ for all $n \in \mathbb{N}$ with $n \geq N_{\varepsilon'}$. This means:

$$V(\mathbf{x}_n) \leq c + \varepsilon' < c^*, \quad (60)$$

or $\mathbf{x}_n \in \Gamma(c^*)$ for all $n \in \mathbb{N}$ with $n \geq N_{\varepsilon'}$. Since $\Gamma(c^*)$ is compact, there is a state-valued subsequence converging to a limit in $\Gamma(c^*)$; denote this subsequence by $\{\mathbf{x}_{n_k} \mid k \in \mathbb{N}\}$ and denote its limit by $\mathbf{x} \in \Gamma(c^*)$. For any $\varepsilon' \in \mathbb{R}_{++}$, there is a corresponding $K_{\varepsilon'} \in \mathbb{N}$ such that:

$$V(\mathbf{x}_{n_k}) \leq c + \varepsilon', \quad (61)$$

for all $k \in \mathbb{N}$ with $k \geq K_{\varepsilon'}$. Since ε' was arbitrary and V is continuous, $V(\mathbf{x}) \leq c$, or $\mathbf{x} \in \Gamma(c)$.

Thus Γ is upper hemicontinuous by the second condition of Definition 9. Consider any $\eta \in \mathbb{R}_{++}$. Letting B_η denote the open ball of radius η, the set $\Gamma(c) \oplus B_\eta$ is an open subset of $\mathbb{R}^n$ since it can be represented as a union of open balls, so $\mathcal{X} \cap (\Gamma(c) \oplus B_\eta)$ is an open subset of $\mathcal{X}$ containing $\Gamma(c)$. The equivalent first condition of upper hemicontinuity shows that for any $\eta \in \mathbb{R}_{++}$, there is a corresponding $\delta \in \mathbb{R}_{++}$ such that $\Gamma(c') \subseteq \mathcal{X} \cap (\Gamma(c) \oplus B_\eta)$ for all $c' \in (c - 2\delta, c + 2\delta)$. For any $\mathbf{x} \in \mathcal{X}$, if $V(\mathbf{x}) \leq c + \delta$, then $d_{\Gamma(c)}(\mathbf{x}) \leq \eta$. Therefore, if $d_{\Gamma(c)}(\mathbf{x}) > \eta$, then $V(\mathbf{x}) > c + \delta$. This means:

$$d_{\Gamma(c)}(\mathbf{x}) > \eta \implies \mathbf{s}_h(\mathbf{x}) < -\delta. \quad (62)$$

for all $\mathbf{x} \in \mathcal{X}$, implying that (11) is satisfied. □

E. Proof of Theorem 5

Proof. For all $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$, denote:

$$\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u}) = ((\mathbf{F}_1)_h^{a,p}(\mathbf{x}, \mathbf{u}), \ldots, (\mathbf{F}_\gamma)_h^{a,p}(\mathbf{x}, \mathbf{u})), \quad (63)$$

where $(\mathbf{F}_i)_h^{a,p} : \mathcal{Z} \to \mathbb{R}^\ell$ for all $i \in \{1, \ldots, \gamma\}$. For $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$ and degree $d \in \{0, \ldots, \gamma - 1\}$, the block vector $\mathbf{r}(\mathbf{x}, \mathbf{u})$ can be nonzero only in the last (γth) block. Noting the block chain-of-integrators structure of $\mathbf{A}$, we see the block vector $\mathbf{A}^d \mathbf{r}(\mathbf{x}, \mathbf{u})$ can be nonzero only in the $(\gamma - d)$th block, and for a degree d polynomial ρ_d, the block vector $\rho_d(\mathbf{A})\mathbf{r}(\mathbf{x}, \mathbf{u})$ can be nonzero only in the last $d + 1$ blocks (that is, blocks $\gamma - d$ through γ).

Consider a state-input pair $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$. We have:

$$\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u}) = \mathbf{x} + h \sum_{i=1}^{p} b_i(\mathbf{A}\mathbf{z}_i + \mathbf{r}(\mathbf{z}_i, \mathbf{u})), \tag{64}$$

$$\mathbf{z}_i = \mathbf{x} + h \sum_{j=1}^{i-1} a_{i,j}(\mathbf{A}\mathbf{z}_j + \mathbf{r}(\mathbf{z}_j, \mathbf{u})), \tag{65}$$

with $\mathbf{z}_1 = \mathbf{x}$. By induction, for any $i \in \{1, \dots, p\}$, we can show that:

$$\mathbf{z}_i = \rho_{i,i-1}(\mathbf{A})\mathbf{x} + \sum_{j=1}^{i-1} \sigma_{i,i-j-1}(\mathbf{A})\mathbf{r}(\mathbf{z}_j, \mathbf{u}), \tag{66}$$

where $\rho_{i,i-1}$ is a degree $i-1$ polynomial, and for $j \in \{1, \dots, i-1\}$, $\sigma_{i,i-j-1}$ is a degree $i-j-1$ polynomial. Indeed, $\mathbf{z}_1 = \mathbf{I}\mathbf{x}$, and assuming (66) is true for $0, \dots, i-1$, substituting (66) into (65) yields the following:

$$\begin{aligned}\mathbf{z}_i = \underbrace{\overbrace{\left(\mathbf{I} + h \sum_{j=1}^{i-1} a_{i,j} \overbrace{\mathbf{A}\rho_{j,j-1}(\mathbf{A})}^{\text{degree } j}\right)}^{\text{degree } i-1} \mathbf{x}}_{\triangleq \rho_{i,i-1}(\mathbf{A})} + h \sum_{j=1}^{i-1} a_{i,j}\mathbf{r}(\mathbf{z}_j, \mathbf{u}) \\ + h \sum_{k=1}^{i-1} \sum_{j=1}^{k-1} a_{i,k}\mathbf{A}\sigma_{k,k-j-1}(\mathbf{A})\mathbf{r}(\mathbf{z}_j, \mathbf{u}),\end{aligned} \tag{67}$$

which we may further manipulate to obtain:

$$\begin{aligned}&\mathbf{z}_i - \rho_{i,i-1}(\mathbf{A})\mathbf{x} \\ &= \sum_{j=1}^{i-1} \underbrace{h\left(a_{i,j} + \sum_{k=j+1}^{i-1} a_{i,k} \underbrace{\mathbf{A}\sigma_{k,k-j-1}(\mathbf{A})}_{\text{degree } k-j}\right)}_{\text{degree } i-j-1} \mathbf{r}(\mathbf{z}_j, \mathbf{u}), \quad (68) \\ &\triangleq \sum_{j=1}^{i-1} \sigma_{i,i-j-1}(\mathbf{A})\mathbf{r}(\mathbf{z}_j, \mathbf{u}), \quad (69)\end{aligned}$$

establishing (66) holds for i. Substituting the expression (66) into (64) and following a similar sequence of steps, we find a degree p polynomial $\tilde{\rho}_p$, and for each $i \in \{1, \dots, p\}$, a degree $p-i$ polynomial $\tilde{\sigma}_{p-i}$ such that:

$$\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u}) = \tilde{\rho}_p(\mathbf{A})\mathbf{x} + \sum_{i=1}^{p} \tilde{\sigma}_{p-i}(\mathbf{A})\mathbf{r}(\mathbf{z}_i, \mathbf{u}). \tag{70}$$

For $i \in \{1, \dots, p\}$, the term $\tilde{\sigma}_{p-i}(\mathbf{A})\mathbf{r}(\mathbf{z}_i, \mathbf{u})$ can be nonzero only in blocks $\gamma - (p-i) = q + i - 1$ through γ. The highest-order polynomial multiplying the block vectors $\mathbf{r}(\mathbf{z}_1, \mathbf{u}), \dots, \mathbf{r}(\mathbf{z}_p, \mathbf{u})$ is $\tilde{\sigma}_{p-1} = \tilde{\sigma}_{\gamma-q}$. Therefore, the functions $(\mathbf{F}_1)_h^{a,p}, \dots, (\mathbf{F}_{q-1})_h^{a,p}$ are independent of their second argument (they depend only on state). Moreover, $(\mathbf{F}_q)_h^{a,p}(\mathbf{x}, \mathbf{u})$ depends on the block vector $\mathbf{r}(\mathbf{z}_1, \mathbf{u}) = \mathbf{r}(\mathbf{x}, \mathbf{u})$, which depends on $\mathbf{u}$ affinely, and does not depend on the block vectors $\mathbf{r}(\mathbf{z}_2, \mathbf{u}), \dots, \mathbf{r}(\mathbf{z}_p, \mathbf{u})$, which may depend on $\mathbf{u}$ nonlinearly.

The function $\mathbf{s}_h \circ \mathbf{F}_h^{a,p} : \mathcal{Z} \to \mathbb{R}$ satisfies:

$$\mathbf{s}_h(\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u})) = \tilde{\mathbf{s}}_h((\mathbf{F}_1)_h^{a,p}(\mathbf{x}, \mathbf{u}), \cdots, (\mathbf{F}_q)_h^{a,p}(\mathbf{x}, \mathbf{u})),$$

for all $(\mathbf{x}, \mathbf{u}) \in \mathcal{Z}$, and since the composition of a concave function and an affine function is concave, $\mathbf{s}_h \circ \mathbf{F}_h^{a,p}$ is concave with respect to its second argument. Thus we have ϕ_h as defined in (37) is a convex function of its second argument. □

F. Proof of Theorem 6

Proof. Let $h \in I$ and $\mathbf{x} \in \mathcal{X}$. As $\mathbf{s}_h$ is a SD-CBF on $\mathcal{C}$, there exists a $\mathbf{u}' \in \mathbb{R}^m$ such that $(\mathbf{x}, \mathbf{u}') \in \mathcal{Z}$ and:

$$\mathbf{s}_h(\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{u}')) - \mathbf{s}_h(\mathbf{x}) \geq -h\alpha(\mathbf{s}_h(\mathbf{x})), \tag{71}$$

implying that $\mathbf{u}' \in \mathcal{F}(\mathbf{x})$. Thus the optimization problem in (SD-CBF-OP) is feasible. Define the compact, convex set:

$$A = \left\{ \mathbf{u} \in \mathbb{R}^m \;\middle|\; \frac{1}{2}\|\mathbf{u} - \mathbf{k}_d(\mathbf{x})\|_2^2 \leq \frac{1}{2}\|\mathbf{u}' - \mathbf{k}_d(\mathbf{x})\|_2^2 \right\}. \tag{72}$$

As the set $\mathcal{F}(\mathbf{x})$ is closed and convex, the set $A \cap \mathcal{F}(\mathbf{x})$ is compact and convex. As the cost of the optimization problem is continuous and strictly convex with respect to $\mathbf{u}$, there exists a unique minimizer $\mathbf{u}^* \in A \cap \mathcal{F}(\mathbf{x})$, and by the definition of A, we have that $\frac{1}{2}\|\mathbf{u}^* - \mathbf{k}_d(\mathbf{x})\|_2^2 < \frac{1}{2}\|\mathbf{u} - \mathbf{k}_d(\mathbf{x})\|_2^2$ for all $\mathbf{u} \in \mathcal{F}(\mathbf{x}) \setminus A$, implying $\mathbf{u}^*$ is the unique minimizer in $\mathcal{F}(\mathbf{x})$. Moreover, as $\mathbf{u}^* \in \mathcal{F}(\mathbf{x})$, we have that:

$$\mathbf{s}_h(\mathbf{F}_h^{a,p}(\mathbf{x}, \mathbf{k}_h(\mathbf{x}))) - \mathbf{s}_h(\mathbf{x}) \geq -h\alpha(\mathbf{s}_h(\mathbf{x})), \tag{73}$$

and as $\mathbf{x}$ was arbitrary, we have that $\mathbf{s}_h$ is a SD-BF for the controller-map pair $(\mathbf{k}_h, \mathbf{F}_h^{a,p})$. As h was arbitrary, we may extended this result to the respective families. □