Bounding Stochastic Safety: Leveraging Freedman's Inequality with Discrete-Time Control Barrier Functions

Ryan K. Cosner, Preston Culbertson, and Aaron D. Ames

***Abstract*—When deployed in the real world, safe control methods must be robust to the unstructured uncertainties such as modeling error and external disturbances. Typical disturbance mitigation approaches either leverage worst-case uncertainty bounds to provide safety guarantees for an expanded (overly conservative) safe set or sythesize controllers that always assume the worst-case disturbance will occur. In contrast, this paper utilizes Freedman's inequality in the context of discrete-time control barrier functions (DTCBFs) to provide stronger (less conservative) safety guarantees for stochastic systems. Our approach accounts for the underlying disturbance distribution instead of relying exclusively on its worst-case bound and, unlike other martingale-based safety methods, does not require the barrier function to be upper-bounded. The resulting bounds on stochastic safety are more directly applicable to intuitive safety metrics such as signed distance. We compare our results with existing safety guarantees, such as Input-to-State-Safety (ISSf) and martingale results that rely on Ville's inequality. When the assumptions for all methods hold, we provide a range of parameters for which our guarantee is less conservative. Finally, we present simulation examples, including a bipedal walking robot, which demonstrate the utility and tightness of our safety guarantee.**

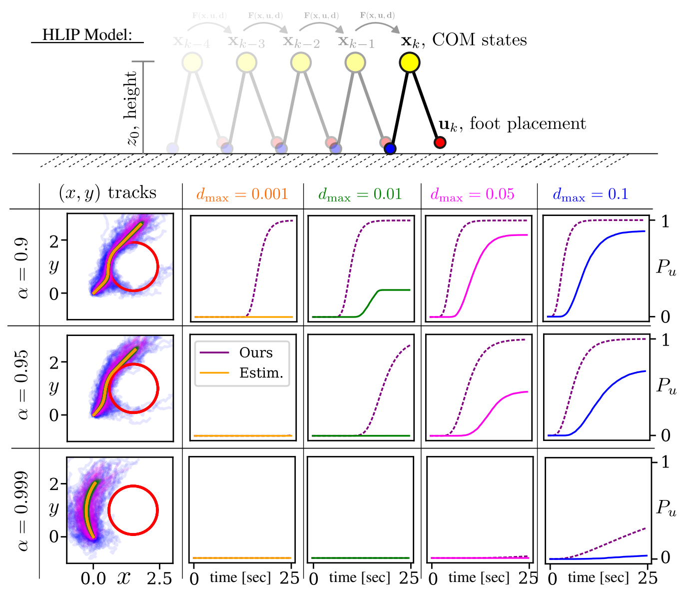

Fig. 1. Safety results for a bipedal robot navigating around an obstacle using our method. Details are provided in Section IV. **(Top)** Visualization of the Hybrid passive Linear Inverted Pendulum (HLIP) model. Yellow indicates the center-of-mass (COM), blue is the stance foot, and red is the swing foot. The states $\mathbf{x}_k$ are the COM position and velocity, and the input is the relative position of the feet at impact. This model gives us an approximate discrete-time model for walking. **(Bottom)** A table with variable maximum disturbance value ($d_{\max}$) and controller parameter (α) shows our theoretical bound from Thm. 3 as a dotted line and approximated probabilities from 5000 trials as solid colored lines. On the left, the (x, y) trajectories of the COM are shown from above with each color corresponding to a different $d_{\max}$. The robot attempts to walk around and avoid the obstacle (red).

I. Introduction

Safety—typically characterized as the forward-invariance of a safe set [1]—has become a popular area of study within control theory, with broad applications to autonomous vehicles, medical and assistive robotics, aerospace systems, and beyond. Ensuring safety for these systems requires one to account for unpredictable, real-world effects. Controllers must be designed to ensure robust safety which degrades smoothly with increasing uncertainty. Historically, control theory has treated the problem of safety under uncertainty using deterministic methods, often by providing safety assurances in the presence of bounded disturbances. Popular safety assurance methods such as Control Barrier Functions (CBFs), backwards Hamilton-Jacobi (HJ) reachability, and state-constrained model-predictive control (MPC) have experienced significant advancements in their robustness to bounded disturbance [2], [3], [4]. Yet, in achieving this, these robustness methods see sharp degradation of performance since they conservatively reject the worst-case disturbances at all times.

Stochastic methods have appeared as an alternative to the worst-case bounding approach. Instead of a conservative over-approximation of uncertainty's effect on safety, these methods consider the entire distribution of possible disturbances. Although they do not share the absolute safety guarantees of the worst-case bounding methods, they allow for smooth degradation of safety via variable, risk-based levels of conservatism. By relying on the unbounded bandwidth of a continuous-time controller, continuous-time stochastic safety methods have achieved significant success [5], [6], [7]. Alternatively, discrete-time methods, have also shown success while capturing the sampled-data complexities of most real-world systems [8], [9], [10], [11]. In this work we will focus in particular on extending the theory of stochastic safety involving Discrete-Time Control Barrier Functions (DTCBFs).

The stochastic DTCBF literature can, in general, be divided into two main categories: firstly, risk-based constraint enforcement which can be extended using the union bound [12], [13], [14] and secondly, martingale-based techniques which develop trajectory-long safety guarantees [5], [15], [10], [11], [8]. Both the first [16] and second [17] class of methods have been demonstrated on real-world robotic systems. We focus this work on martingale-based methods due to their popularity, trajectory-long guarantees, and distributional robustness. In particular, extend the existing martingale-based stochastic DTCBF techniques by utilizing a martingale concentration inequality which has yet to be studied in this context. Traditionally, other works rely on Ville's inequality [18]. Instead, we

The authors are with the Department of Mechanical and Civil Engineering at the California Institute of Technology, Pasadena, CA 91125, USA. {rkcosner, pbulbert, ames}@caltech.edu
This work was supported by BP and NSF CPS Award #1932091.

turn to Freedman's inequality (sometimes called "Hoeffding's inequality for supermartingales") as presented in [19] which additionally assumes bounded martingale jumps and known predictable quadratic variation, but generally provides a tighter bound and relaxes the upper boundedness assumption required by methods based on Ville's inequality.

This paper combines DTCBFs with Freedman's inequality to obtained tight bounds on stochastic safety. This is achieved through three main contributions: (1) we present new Freedman-based probabilistic safety bounds for DTCBFs and c-martingales, (2) when the assumptions of our method and previous methods hold, we provide a range of parameters for which our bound is tighter previous bounds, and (3) we demonstrate the proposed bound in simulation and compare to existing probabilistic and worst-case bounds. To demonstrate the practical applicability of the developed bounds on stochastic safety, we apply them to the use case of obstacle avoidance with a bipedal robot (see Fig. 1), wherein reduced order (HSLIP) models are considered with discrete-time dynamics dictated by the step-to-step dynamics, and a DTCBF is synthesized encoding the distance to an obstacle. We demonstrate that the main result of the paper, and associated probability bounds, hold in this case leading to bounded stochastic collision avoidance in bipedal locomotion.

II. Background

Let $(\Omega, \mathscr{F}, \mathbb{P})$ be a probability space and let $\mathscr{F}_0 \subset \mathscr{F}_1 \cdots \subset \mathscr{F}$ be a filtration of $\mathscr{F}$. Consider discrete-time dynamical systems of the form:

$$\mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k, \mathbf{u}_k, \mathbf{d}_k), \quad \forall k \in \mathbb{N} \tag{1}$$

where $\mathbf{x}_k \in \mathbb{R}^n$ is the state, $\mathbf{u}_k \in \mathbb{R}^m$ is the input, $\mathbf{d}_k$ taking values in $\mathbb{R}^\ell$ and adapted to the filtration is a random disturbance to the system, and $\mathbf{F} : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^\ell \to \mathbb{R}^n$ is the dynamics. Throughout this work we assume that all random variables and functions of random variables are integrable.

To create a closed-loop system, we add a state-feedback controller $\mathbf{k} : \mathbb{R}^n \to \mathbb{R}^m$:

$$\mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k), \mathbf{d}_k), \quad \forall k \in \mathbb{N} \tag{2}$$

The goal of this work is to provide probabilisic safety guarantees for this closed-loop system.

A. Safety and Discrete-Time Control Barrier Functions

To make guarantees regarding the safety of system (2), we first formalize our notion of safety as the forward invariance of a "safe set", $\mathcal{C} \subset \mathbb{R}^n$, as is common in the robotics and control literature [1], [3], [4], [20].

Definition 1 (Forward Invariance and Safety)**.** *A set $\mathcal{C} \subset \mathbb{R}^n$ is forward invariant for system* (2) *if $\mathbf{x}_0 \in \mathcal{C} \implies \mathbf{x}_k \in \mathcal{C}$ for all $k \in \mathbb{N}$. We define "safety" as the forward invariance of $\mathcal{C}$.*

One method for ensuring safety is through the use of Discrete-Time Control Barrier Functions (DTCBFs). For DTCBFs, we consider safe sets that are 0-superlevel sets [1] of some function $h : \mathbb{R}^n \to \mathbb{R}$:

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n \mid h(\mathbf{x}) \geq 0\}. \tag{3}$$

In particular the DTCBF is defined as:

Definition 2 (Discrete-Time Control Barrier Function (DT-CBF) [21])**.** *Let $\mathcal{C} \subset \mathbb{R}^n$ be the 0-superlevel set of some function $h : \mathbb{R}^n \to \mathbb{R}$. The function h is a DTCBF for $\mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k, \mathbf{u}, \mathbf{0})$ if there exists an $\alpha \in [0, 1]$ such that:*

$$\sup_{\mathbf{u} \in \mathbb{R}^m} h(\mathbf{F}(\mathbf{x}, \mathbf{u}, \mathbf{0})) > \alpha h(\mathbf{x}), \qquad \forall \mathbf{x} \in \mathcal{C} \tag{4}$$

DTCBFs differ from their continuous-time counterparts in that they satisfy an inequality constraint on their *finite difference* instead of their derivative[1]. On the other hand, they are similar in their ability to create *safety filters* for nominal controllers $\mathbf{k}_{\text{nom}} : \mathbb{R}^N \times \mathbb{N} \to \mathbb{R}^m$:

$$\begin{aligned} \mathbf{k}(\mathbf{x}) = \underset{\mathbf{u} \in \mathbb{R}^m}{\operatorname{argmin}} \quad & \|\mathbf{u} - \mathbf{k}_{\text{nom}}(\mathbf{x}, k)\|^2 \\ \text{s.t.} \quad & h(\mathbf{F}(\mathbf{x}, \mathbf{u}, \mathbf{0})) \geq \alpha h(\mathbf{x}). \end{aligned} \tag{5}$$

Assuming that this opimization problem is feasible[2], $\mathbf{k}(\mathbf{x})$ guarantees safety of the undisturbed system by selecting inputs that satisfy condition (4) [21, Prop. 1]. .

For deterministic systems, infinite-horizon safety guarantees are common for CBF-based controllers such as (5). However, such guarantees for discrete-time stochastic systems fail to capture the nuances of the disturbance distribution and, at times, can be impossible to achieve [24, Sec. IV]. We therefore choose to instead analyze finite-time safety probabilities.

Definition 3 (K-step Exit Probability)**.** *For any $K \in \mathbb{N}$ and initial condition $\mathbf{x}_0 \in \mathbb{R}^n$, the K-step exit probability of the set $\mathcal{C}$ for the closed-loop system* (2) *is:*

$$P_u(K, \mathbf{x}_0) = \mathbb{P}\left\{\mathbf{x}_k \notin \mathcal{C} \text{ for some } k \in \{0, \ldots, K\}\right\} \tag{6}$$

This describes the probability that the system will leave the safe set $\mathcal{C}$ within K time steps given that it started at $\mathbf{x}_0$.

B. Existing Martingale-based Safety Methods

In this work, we will generate bounds for the K-step exit probability for systems with stochastic dynamics using martingale-based concetration inequalities. Martingales are a class of stochastic processes which satisfy a relationship between their mean and previous value.

Definition 4 (Martingale [25])**.** *Let $(\Omega, \mathscr{F}, \mathbb{P})$ be a probability space with a filtration $\{\mathscr{F}_0, \mathscr{F}_1, \ldots \mathscr{F}\}$. A stochastic process R_k that is adapted to the filtration and is integrable at each k is a martingale if*

$$\mathbb{E}[R_{k+1} \mid \mathscr{F}_k] = R_k, \quad \forall k \in \mathbb{N} \quad \text{a.s.} \tag{7}$$

Additionally, R_k is a supermartingale if it instead satisfies:

$$\mathbb{E}[R_{k+1} \mid \mathscr{F}_k] \leq R_k, \quad \forall k \in \mathbb{N} \quad \text{a.s.} \tag{8}$$

[1]The standard continuous-time CBF condition $\dot{h}(\mathbf{x}) \leq -\overline{\gamma} h(\mathbf{x})$ for $\overline{\gamma} > 0$ becomes $\Delta h(\mathbf{x}_k) = h(\mathbf{x}_{k+1}) - h(\mathbf{x}_k) \geq -\gamma h(\mathbf{x}_k)$ for $\gamma \in [0, 1]$, defining $\alpha = 1 - \gamma$ and rearranging terms recovers condition (4).

[2]Unlike the affine inequality constraint that arises with continuous-time CBFs [1], the optimization problem (5) is not necessarily convex. To solve this issue, it is often assumed that $h \circ \mathbf{F}$ is concave with respect to $\mathbf{u}$ [22], [21], [14]. In general, the assumption that $\mathbf{F}$ is affine with respect to $\mathbf{u}$ is well-motivated for systems with fast sampling rates [23]. If $\mathbf{F}$ is affine in $\mathbf{u}$ and h is concave then $h \circ \mathbf{F}$ is concave and (5) is a convex program.

Many concentration inequalities can be used to bound the spread of a martingale over time. One inequality that has been central to many proofs of stochastic safety is Ville's inequality [18] which relates the probability that the supermartingale R_k ever rises above a threshold $\lambda > 0$ to its initial expectation.

Lemma 1 (Ville's Inequality [18]). *Let R_k be a nonnegative supermartingale. Then for all $\lambda > 0$,*

$$\mathbb{P}\left\{\sup_{k\in\mathbb{N}} R_k > \lambda\right\} \leq \frac{\mathbb{E}[R_0]}{\lambda} \tag{9}$$

Critically, Ville's inequality assumes that R_k is nonnegative. This manifests as an upper bound requirement on h. A proof of Ville's inequality can be found in Appendix A

For safety applications of Ville's inequality, we consider the case where $h(\mathbf{x}_k)$ is upper bounded by $B > 0$ and satisfies one of the following expectation conditions:

$$\mathbb{E}[\ h(\mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k), \mathbf{d}_k))\ |\ \mathscr{F}_k\ ] \geq \alpha h(\mathbf{x}_k), \tag{DTCBF}$$
$$\mathbb{E}[\ h(\mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k), \mathbf{d}_k))\ |\ \mathscr{F}_k\ ] \geq h(\mathbf{x}_k) - c, \tag{c-mart.}$$

for some $\alpha \in (0, 1)$ or $c \geq 0$. The first case is an expectation-based DTCBF condition [8] and the second is the c-martingale condition [10]. In this case, we can achieve the following bound on the K-step exit probability, $P_u(K, \mathbf{x}_0)$:

Theorem 1 (DTCBF Safety using Ville's Inequality, Thm. 5 [8], [10]). *Let $h : \mathbb{R}^n \to \mathbb{R}$ have an upper bound $B > 0$. If the closed loop system* (2) *satisfies the* (DTCBF) *condition or the* (c-mart.) *condition for all $\mathbf{x} \in \mathcal{C}$, then for any $K \in \mathbb{N}$:*

$$P_u(K, \mathbf{x}_0) \leq 1 - \frac{\lambda}{B}, \tag{10}$$

$$\text{where } \lambda = \begin{cases} \alpha^K h(\mathbf{x}_0), & \text{if system (2) satisfies (DTCBF)}, \\ h(\mathbf{x}_0) - cK, & \text{if system (2) satisfies (c-mart.)}. \end{cases}$$

This theorem guarantees that the risk of the process becoming unsafe is upper bounded by a function which decays to 1 geometrically or linearly in time and which is a function of the initial safety "fraction", $h(\mathbf{x}_0)/B$, of the system. A proof of this Theorem can be found in Appendix B.

III. Safety Guarantees using Freedman's Inequality

This section presents the main result of this paper: maximal bounds on DTCBFs and c-martingales, which are then related back to input-to-state safety. This is achieved utilizing Freedman's inequality, which is a particularly strong, well-studied concentration inequality for martingales. For this work, we utilize the simpler, historical version of the bound as presented by Freedman [26]; see also [19] for historical context and a new tighter alternative which could also be used.

Before presenting Freedman's inequality, we must define the predictable quadratic variation (PQV) of a process which is a generalization of variance for stochastic processes.

Definition 5 (Predictable Quadratic Variation (PQV) [25]). *The predictable quadratic variation (PQV) of R_k is:*

$$\langle R\rangle_k \triangleq \sum_{i=1}^{k} \mathbb{E}[(R_k - R_{k-1})^2 \mid \mathscr{F}_{k-1}] \tag{11}$$

Unlike Ville's inequality, Freedman's inequality will no longer require the martingale R_k to be lower bounded, thus removing the upper bound requirement on h. Instead, in place of nonnegativity, we require two alternative assumptions:

Assumption 1 (Upper-Bounded Differences). *We assume that the martingale differences are upper-bounded by* 1.

Assumption 2 (Bounded PQV). *We assume that the PQV is upper-bounded by $\sigma^2 > 0$.*

Given the PQV of the process, Freedman's inequality provides the following bound:

Theorem 2 (Freedman's Inequality [19]). *Assume that R_k is a martingale satisfying $(R_k - R_{k-1}) \leq 1$ and $\langle R\rangle_K \leq \sigma^2$ for some $\sigma > 0$ and $K \in \mathbb{N}$. Then, for any $\lambda \geq 0$,*

$$\mathbb{P}\left\{\max_{k\leq K} R_k \geq \lambda\right\} \leq H(\lambda, \sigma) \triangleq \left(\frac{\sigma^2}{\lambda + \sigma^2}\right)^{\lambda+\sigma^2} e^{\lambda}. \tag{12}$$

To apply (12) to systems governed by the DTCBF or c-mart. condition, we require an upper bound on the PQV of a supermartingale created from $h(\mathbf{x}_k)$. However, naively calculating the PQV for this process may cause safe, predictable control actions to harm the probabilistic guarantee by increasing $\langle h(\mathbf{x})\rangle_k$. Essentially, we wish to remove the effect of the nominal controller from our safety guarantee. In order to do this we decompose our supermartingale into a decreasing predictable process A_k and a martingale M_k. Doob's decomposition theorem [25, Thm 12.1.10] ensures the existence and uniqueness (a.s.) of this decomposition.

Instead of applying the Freedman's inequality to the original supermartingale, we can remove the predictable effects of the controller from the PQV by applying it to M_k. This allows us to consider a smaller quadratic variation that grows only with respect to the the unpredictable randomness of $h(\mathbf{x}_k)$.

A. Main Result: Freedman's Inequality for DTCBFs

We first present the key contribution of this paper: the application of Freedman's Inequality (Thm. 2) to systems which satisfy the DTCBF condition.

Theorem 3. *If, for some $K \in \mathbb{N}$, $\alpha \in (0, 1]$ and $\delta > 0$, the following bounds hold for all $k \leq K$ on the conditional expectation* (DTCBF)*, the difference between the true and predictable update* (13)*, and the conditional variance* (14)*:*

$$\mathbb{E}[\ h(\overbrace{\mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k), \mathbf{d}_k)}^{\mathbf{x}_{k+1}=})\ |\ \mathscr{F}_k\ ] \geq \alpha h(\mathbf{x}_k), \tag{DTCBF}$$
$$h(\mathbf{x}_{k+1}) - \mathbb{E}[h(\mathbf{x}_{k+1})\ |\ \mathscr{F}_k\ ] \geq -\delta, \tag{13}$$
$$\mathrm{Var}(\ h(\mathbf{x}_{k+1})\ |\ \mathscr{F}_k\ ) \leq \sigma^2, \tag{14}$$

then the K-step exit probability is bounded as:

$$P_u(K, \mathbf{x}_0) \leq H_K\left(\frac{\alpha^K h(\mathbf{x}_0)}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right). \tag{15}$$

Proof. First, we define the normalized safety function

$$\eta(\mathbf{x}) \triangleq h(\mathbf{x})/\delta \tag{16}$$

to ensure that the martingale differences will be bounded by 1. We then use η to define the candidate supermartingale

$$R_k \triangleq -\alpha^{K-k}\eta(\mathbf{x}_k) + \alpha^K \eta(\mathbf{x}_0). \tag{17}$$

This function has zero as an initial condition, $R_0 = 0$, and is a supermartingale:

$$\begin{aligned}\mathbb{E}[R_{k+1}|\mathscr{F}_k] &= -\alpha^{K-(k+1)}\mathbb{E}[\eta(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] + \alpha^K\eta(\mathbf{x}_0),\\ &\leq -\alpha^{K-(k+1)}\alpha\eta(\mathbf{x}_k) + \alpha^K\eta(\mathbf{x}_0) = R_k.\end{aligned}$$

The martingale from Doob's decomposition of R_k is:

$$\begin{aligned}M_k &\triangleq R_k + \sum_{i=1}^{k}(R_{i-1} - \mathbb{E}[R_i|\mathscr{F}_{i-1}]), \qquad (18)\\ &= R_k + \sum_{i=1}^{k}\underbrace{\frac{\alpha^{K-i}}{\delta}(\mathbb{E}[h(\mathbf{x}_i)|\mathscr{F}_{i-1}] - \alpha h(\mathbf{x}_{i-1}))}_{\geq \frac{\alpha^{K-i}}{\delta}\geq 0} \geq R_k\end{aligned}$$

where the bound $M_k \geq R_k$ comes from the DTCBF condition (DTCBF). Furthermore, M_k has differences that are upper-bounded by 1, thus satisfying Assumption 1:

$$\begin{aligned}M_k - M_{k-1} &= R_k - \mathbb{E}[R_k|F_{k-1}], &(19)\\ &= -\alpha^{K-k}\eta(\mathbf{x}_k) + \alpha^{K-k}\mathbb{E}[\eta(\mathbf{x})_k|\mathscr{F}_{k-1}], &(20)\\ &\leq \alpha^{K-k}\frac{\delta}{\delta} \leq 1, &(21)\end{aligned}$$

since we assume in (13) that $\delta \geq \mathbb{E}[h(\mathbf{x}_k) \mid \mathscr{F}_{k-1}] - h(\mathbf{x}_k)$.

Finally, $\alpha \in (0, 1]$ and $k \leq K$ together with our bounded variance assumption (14) ensure that $\langle M\rangle_K$ is bounded:

$$\begin{aligned}\langle M\rangle_k &= \sum_{i=1}^{k}\mathbb{E}[\alpha^{2(K-i)}(\eta(\mathbf{x}_i) - \mathbb{E}[\eta(\mathbf{x}_i)|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}]\\ &= \sum_{i=1}^{k}\frac{\alpha^{2(K-i)}}{\delta^2}\mathrm{Var}(h(\mathbf{x}_i)|\mathscr{F}_{i-1}) \leq \sum_{i=1}^{k}\alpha^{2(K-i)}\frac{\sigma^2}{\delta^2} \leq \frac{\sigma^2 K}{\delta^2}.\end{aligned}$$

Now to relate the unsafe event $\{\exists k \leq K \text{ s.t. } h(\mathbf{x}_k) < 0\}$ to our martingale M_k we consider the implications:

$$\begin{aligned}&\exists k \leq K \text{ s.t. } h(\mathbf{x}_k) < 0 \implies \exists k \leq K \text{ s.t. } h(\mathbf{x}_k) \leq 0 &(22)\\ &\iff \max_{k\leq K} -\alpha^{K-k}\eta(\mathbf{x}_k) \geq 0, \quad \text{since } \alpha > 0, \delta > 0 &(23)\\ &\iff \max_{k\leq K} -\alpha^{K-k}\eta(\mathbf{x}_k) + \alpha^K\eta(\mathbf{x}_0) \geq \alpha^K\eta(\mathbf{x}_0) &(24)\\ &\iff \max_{k\leq K} R_k \geq \alpha^K\eta(\mathbf{x}_0) \implies \max_{k\leq K} M_k \geq \alpha^K\eta(\mathbf{x}_0) &(25)\end{aligned}$$

where the second line is due to multiplication by a value strictly less than zero, the third line is due to adding zero, and the fourth line is due to subtracting the predictable differences to bound R_k with M_k as in equation (18). Thus the unsafe event satisfies the containment:

$$\left\{\min_{k\leq K} h(\mathbf{x}_k) < 0\right\} \subseteq \left\{\max_{k\leq K} M_k \geq \frac{\alpha^K}{\delta}h(\mathbf{x}_0)\right\} \tag{26}$$

Since M_K is a martingale with differences upper-bounded by 1 and $\langle M\rangle_K \leq \frac{\sigma^2 K}{\delta^2}$, we can apply Theorem 2 with $\lambda = \frac{\alpha^K h(\mathbf{x}_0)}{\delta}$ to achieve the desired probability bound: $P_u(K, \mathbf{x}_0) \leq H\left(\frac{\alpha^K h(\mathbf{x}_0)}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right)$. $\square$

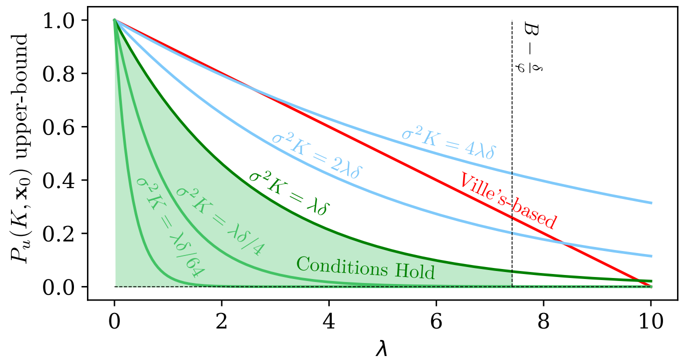

Fig. 2. Comparison for Prop. 1 with $B = 10, K = 100, \delta = 1$, and varying $\sigma$and λ (lower is stronger). The bounds from Freedman's inequality are shown in green when the conditions of Thm. 1 hold and blue when they do not. The bound from Ville's inequality is shown in red. This validates the theorem and shows that it is conservative.

B. Maximal Azuma-Hoeffding Bounds for c-martingales

Next we apply the same bound to c-martingales.

Theorem 4. *Assume for some $K \in \mathbb{N}$, $c \geq 0$ and $\delta > 0$, the following bounds hold for all $k \leq K$. If $h(\mathbf{x}_k)$ satisfies* (13), (14)*, and:*

$$\mathbb{E}[\ h(\mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k), \mathbf{d}_k)) \mid \mathscr{F}_{k-1}\ ] \geq h(\mathbf{x}_k) - c, \quad (c\text{-mart.})$$

then the K-step exit probability is bounded as:

$$P_u(K, \mathbf{x}_0) \leq H_K\left(\frac{h(\mathbf{x}_0) - Kc}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right). \tag{27}$$

The proof but with the supermartingale $R_k = \frac{1}{\delta}(-h(\mathbf{x}_k) - kc + h(\mathbf{x}_0))$ and can be found in Appendix C.

C. Bound Tightness of Ville's and Hoeffding's Inequalities

To show the utility of Theorems 3 and 4 we now provide a range of parameters for which Freedman's bound (12) generates a better safety guarantee than Ville's bound (10) when the assumptions of both theorems are satisfied. This relationship will allow us to directly compare safety guarantees by setting $\lambda = \alpha^K h(\mathbf{x}_0)$ for systems satisfying the DTCBF condition and $\lambda = h(\mathbf{x}_0) - Kc$ for systems satisfying c-mart. condition.

Proposition 1. *For some $\sigma, \delta, B > 0$, $\lambda \geq 0$ and $K \in \mathbb{N}$, consider the conditions*

$$\lambda\delta \geq \sigma^2 K, \qquad\qquad \lambda \leq B - \frac{\delta}{\varphi}, \tag{28}$$

where $\varphi = 2\ln(2) - 1$. If these conditions hold, then:

$$H\left(\frac{\lambda}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right) \leq 1 - \frac{\lambda}{B}. \tag{29}$$

Proof of this Proposition is is provided in Appendix F.

Intuitively, the conditions of this theorem stipulate that the predictable variance σ and number of steps K must be limited by $\lambda\delta$ which is a function of the initial condition and the maximum single-step disturbance. Additionally, the initial condition must be less than the safety bound B by some amount that is proportional to the maximum disturbance δ. The exact value of φ is a result of the first assumption

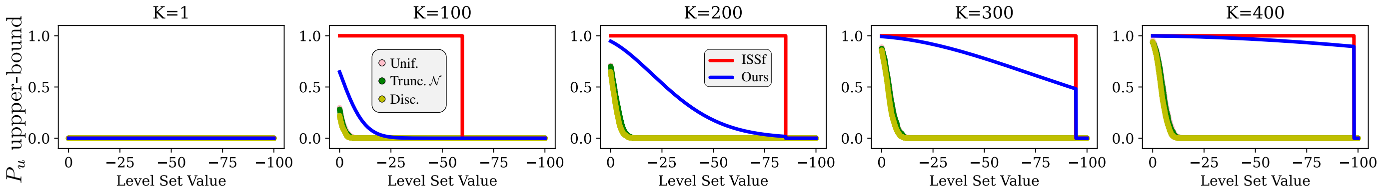

Fig. 3. Probability that the system is unsafe: our bound from Cor. 1 (blue), ISSf bound (red). The x-axis is the level set expansion $-\epsilon$ and the y-axis is the failure probability. The plots from left to right indicate safety through for $K = 1, 100, 200, 300$, and 400 steps. Simulations where $\mathbb{E}[h(\mathbf{x}_k)|\mathscr{F}_{k-1}] = \alpha h(\mathbf{x}_k)$ are shown where $h(\mathbf{x}_k)$ is sampled from a distribution; approximate probabilities from 1000 samples are shown for 3 different distributions: uniform (pink), truncated Gaussian (green), and a discrete (yellow) all which satisfy Cor. 1. Code for these plots can be found here.

$(\lambda\delta \geq \sigma^2 K)$ and alternative values can be used by changing this assumption; for clarity of presentation, we leave this optimization for future work. The safety bounds for various λ and σ are shown in Fig. 2 where it is clear that these conditions provide a *conservative* set of parameters over which this proposition holds.

D. Extending Input-to-State Safety

Given the lower-bounded disturbance required in Assumption 1, we next look to compare our stochastic bounds to the worst-case bounds common in Input-to-State Safety (ISSf) [2].

In the context of our stochastic, discrete time problem formulation, the ISSf property can be reformulated as:

Proposition 2 (Input-to-State Safety)**.** *If the system satisfies the DTCBF condition and the bounded-jump condition* (13) *for some* $\alpha \in [0, 1)$ *and* $\delta \geq 0$*, then* $h(\mathbf{x}_k) \geq \alpha^k h(\mathbf{x}_0) - \sum_{i=0}^{k-1} \alpha^i \delta$ *for* $k < \infty$ *and* $\mathcal{C}_\delta = \left\{ \mathbf{x} \mid h(\mathbf{x}) \geq \frac{-\delta}{1-\alpha} \right\}$ *is safe.*

with a proof provided in Appendix D.

To compare with ISSf, we wish to use Theorem 2 to bound the probability that our system reaches the expanded safe set $\mathcal{C}_\epsilon = \{\mathbf{x} | h(\mathbf{x}) \geq -\epsilon\}$ for any $\epsilon \geq 0$ in finite time.

Corollary 1. *If the hypotheses of Theorem 3 are satisfied, then for any value* $\epsilon \geq 0$ *and any* $K < \infty$*,*

$$P\left\{ \min_{k \leq K} h(\mathbf{x}_k) < -\epsilon \right\} \tag{30}$$

$$\leq H\left(\lambda, \sigma \left(\sum_{i=1}^{K} \frac{\alpha^{2(K-i)}}{\delta^2} \right)^{\frac{1}{2}} \right) \mathbb{1}_{\left\{ -\epsilon \geq \alpha^K h(\mathbf{x}_0) - \sum_{i=0}^{K-1} \alpha^i \delta \right\}}$$

where $\lambda = \frac{\alpha^K}{\delta}(h(\mathbf{x}_0) + \epsilon)$.

The proof of Cor. 1 can be found in Appendix E and applies the same method as Thm. 3, but for the supermartingale $R_k = -\alpha^{K-k}(h(\mathbf{x}_k) + \epsilon)/\delta + \alpha^K(h(\mathbf{x}_0) + \epsilon)/\delta + \sum_{i=1}^{k} \alpha^{K-i}\epsilon(1 - \alpha)/\delta$ and then utilizes the finite-horizon guarantee of Thm. 2 to produce the indicator function. A comparison of these bounds and Monte Carlo approximations for various level sets and distributions over time is shown in Fig. 3.

IV. Case Study: Bipedal Obstacle Avoidance

In this section we apply our method to a simplified model of a bipedal walking robot. In particular, the Hybrid passive Linear Inverted Pendulum (HLIP) model [27] approximates a bipedal robot as an inverted pendulum with a fixed center of mass (COM) height $z_0 \in \mathbb{R}$. Its states are the planar position, relative COM-to-stance foot position, and COM velocity $\mathbf{p}, \mathbf{c}, \mathbf{v} \in \mathbb{R}^2$. The step-to-step dynamics are linear and the input is the relative foot placement, $\mathbf{u}_k \in \mathbb{R}^2$. The matrices $\mathbf{A} \in \mathbb{R}^{6\times 6}$ and $\mathbf{B} \in \mathbb{R}^{6\times 2}$ are determined by gait parameters including the stance, swing phase periods, and z_0. The HLIP model with an added disturbance term, $\mathbf{d}$ is:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{D}\mathbf{d}_k, \quad \mathbf{d}_k \sim \mathcal{D}.$$

where $\mathbf{x}_{k+1} = \begin{bmatrix} \mathbf{p}_{k+1} & \mathbf{c}_{k+1} & \mathbf{v}_{k+1} \end{bmatrix}^\top$. We augment the standard HLIP model and assume that $\mathbf{d}$ enters the system linearly and $\mathcal{D}$ is a 4-dimensional 0-mean truncated Gaussian.

We define safety for this system as avoiding a circular obstacle of radius $r > 0$ located at $\boldsymbol{\rho} \in \mathbb{R}^2$, so $h(\mathbf{x}) = \|\mathbf{p} - \boldsymbol{\rho}\|_2 - r$. Notably, this function has no upper bound and therefore the Ville's-based bounds of Theorem 1 do not apply.

Since $h(\mathbf{x})$ is not convex, we use a conservative halfspace convexification instead:

$$h(\mathbf{x}_{k+1}) \geq \widehat{\mathbf{e}}(\mathbf{p}_k)^\top (\mathbf{p}_{k+1} - \boldsymbol{\rho}) - r \triangleq \bar{h}(\mathbf{x}_{k+1}), \tag{31}$$

where $\widehat{\mathbf{e}}(\mathbf{p}) = \frac{(\mathbf{p}-\boldsymbol{\rho})}{\|\mathbf{p}-\boldsymbol{\rho}\|}$ and we apply the controller:

$$\begin{aligned} \mathbf{u}^* = \min_{\mathbf{u}\in\mathbb{R}^2} \quad & \|\mathbf{u} - \mathbf{k}_{\text{nom}}(\mathbf{x}_k)\| \\ \text{s.t.} \quad & \mathbb{E}\left[\ \bar{h}(\mathbf{x}_{k+1}) \mid \mathscr{F}_k\ \right] \geq \alpha \bar{h}(\mathbf{x}_k) \end{aligned} \tag{32}$$

where $\alpha \in (0, 1]$ and $\mathbf{k}_{\text{nom}}$ tracks a desired velocity.

We ran 5000 trials with 3 steps per second and compared against the theoretical bound from Thm. 3. Those values and planar pose trajectories can be seen in Fig. 1. Exact values and code for this and all other plots can be found in this repository.

V. Conclusion

Despite the tightness guarantee of Theorem 1, the probability guarantees of this method are not necessarily tight as can be seen in Fig. 3. Optimization of h without changing $\mathcal{C}$ as in [10] is a promising direction for future work and further tightening of our bound. Additionally, the example shown in Section IV presents an immediate direction for future work which may involve learning the real-life disturbance distribution using a similar method to [17] on a humanoid robot such as [28].

Appendix

A. Proof of Ville's Inequality

Proof. Fix $\lambda > 0$ and define the stopping time $\tau \triangleq \inf\{k \in \mathbb{N} \mid R_k > \lambda\}$ with $\tau = +\infty$ if $R_k \leq \lambda$ for all time. Since R_k

is a nonnegative supermartingale, the stopped process $R_{k\wedge\tau}$ is also a nonnegative supermartingale where

$$\mathbb{E}[R_{k\wedge\tau}] \leq \mathbb{E}[R_0] \text{ and } \liminf_{k\to\infty} \mathbb{E}[R_{k\wedge\tau}] \leq \mathbb{E}[R_0]. \tag{33}$$

We can further bound this in the case that τ is finite:

$$\begin{aligned}\mathbb{E}[R_0] &\geq \liminf_{k\to\infty} \mathbb{E}[R_{k\wedge\tau}\mathbb{1}_{\{\tau<\infty\}}] && (34)\\ &\geq \mathbb{E}[\liminf_{k\to\infty} R_{k\wedge\tau}\mathbb{1}_{\{\tau<\infty\}}] && (35)\\ &> \mathbb{E}[\lambda\mathbb{1}_{\tau<\infty}] = \lambda\mathbb{P}\{\tau<\infty\} = \lambda\mathbb{P}\left\{\sup_{k\in\mathbb{N}} W_k > \lambda\right\}.\end{aligned}$$

The first inequality is by the nonegativity of W_k, the second inequality is by Fatou's Lemma [25], and the third is by the definition of τ. Rearranging terms completes the proof. □

B. Proof of Theorem 1

Proof. We first prove the case when (DTCBF) is satisfied. Let $R_k \triangleq B\alpha^{-K} - \alpha^{-k}h(\mathbf{x}_k)$. This is a nonnegative supermartingale for $k \leq K$:

$$R_k = \alpha^{-K}B - \alpha^{-k}h(\mathbf{x}_k) \geq \alpha^{-k}(B - h(\mathbf{x}_k)) \geq 0 \tag{36}$$

$$\begin{aligned}\mathbb{E}[R_{k+1}|\mathscr{F}_k] &= \alpha^{-K}B - \alpha^{-(k+1)}\mathbb{E}[h(\mathbf{x}_{k+1})|\mathscr{F}_k] && (37)\\ &\leq \alpha^{-K}B - \alpha^{-k}h(\mathbf{x}_k) = \mathbb{R}_k. && (38)\end{aligned}$$

Apply Ville's inequality 1 to R_k to find:

$$\mathbb{P}\left\{\max_{k\leq K} R_k \leq \lambda\right\} \leq \frac{\mathbb{E}[R_0]}{\lambda}. \tag{39}$$

Next note that the implications:

$$\exists k \leq K \text{ s.t. } h(\mathbf{x}_k) < 0 \implies \exists k \leq K \text{ s.t. } R_k > \alpha^{-K}B$$

ensure that $P_u(K, \mathbf{x}_0) \leq \mathbb{P}\left\{\max_{k\leq K} R_k > \alpha^{-K}\right\}$. Choose $\lambda = \alpha^{-K}B$ to achieve:

$$P_u(K, \mathbf{x}_0) \leq \frac{\alpha^{-K}B - h(\mathbf{x}_0)}{\alpha^{-K}B} = 1 - \frac{h(\mathbf{x}_0)}{B}\alpha^K \tag{40}$$

Next we prove the case when (c-mart.) is satisfied. Let $R^c_k \triangleq B - h(\mathbf{x_k}) + (K-k)c$. This is a non-negative supermartingale for $k \leq K$:

$$\begin{aligned}R^c_k &= B - h(\mathbf{x}_k) + (K-k)c \geq 0 && (41)\\ \mathbb{E}[R^c_{k+1} \mid \mathscr{F}_k] &= B - \mathbb{E}[h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] + (K-k-1)c\\ &\leq B - h(\mathbf{x}_k) + c + (K-k-1)c && (42)\\ &= B - h(\mathbf{x}_k) + (K-k)c = R^c_k && (43)\end{aligned}$$

Apply Ville's inequality 1 to R^c_k to find:

$$\mathbb{P}\left\{\max_{k\leq K} R^c_k \leq \lambda\right\} \leq \frac{\mathbb{E}[R^c_0]}{\lambda} \tag{44}$$

Next note that the implication:

$$\exists k \leq K \text{ s.t. } h(\mathbf{x}_k) < 0 \implies \exists k \leq K \text{ s.t. } R^c_k > B \tag{45}$$

ensure that $P_u(K, \mathbf{x}_0) \leq \mathbb{P}\{\max_{k\leq K} R^c_k \leq \lambda\}$. Choose $\lambda = M$ to achieve:

$$P_u(K, \mathbf{x}_0) \leq \frac{B - h(\mathbf{x}_0) + Kc}{B} = 1 - \frac{h(\mathbf{x}_0) - Kc}{B}.$$

□

C. Proof of Theorem 4

Proof. First we define the normalized safety function

$$\eta(\mathbf{x}) \triangleq h(\mathbf{x})/\delta \tag{46}$$

to ensure that the martingale differences will be bounded by 1. We then use η to define the candidate supermartingale $R_k = -\eta(\mathbf{x}_k) - \frac{kc}{\delta} + \eta(\mathbf{x}_0)$, which satisfies $R_0 = 0$ and is a supermartingale:

$$\begin{aligned}\mathbb{E}[R_{k+1} \mid \mathscr{F}_k] &= \mathbb{E}[-\eta(\mathbf{x}_{k+1})|\mathscr{F}_k] - (k+1)\frac{c}{\delta} + \eta(\mathbf{x}_0)\\ &\leq -\eta(\mathbf{x}_k) - k\frac{c}{\delta} + \eta(\mathbf{x}_0) = R_k. && (47)\end{aligned}$$

Consider the Doob's decomposition of this supermartingale. The resulting martingale is:

$$\begin{aligned}M_k &= R_k - \sum_{i=1}^{k}(\mathbb{E}[R_i \mid \mathscr{F}_{i-1}] - R_{i-1}) && (48)\\ &= R_k + \sum_{i=1}^{k}\left(\mathbb{E}[\eta_i|\mathscr{F}_{i-1}] - \eta_{i-1} + \frac{c}{\delta}\right) \geq R_k && (49)\end{aligned}$$

The martingale difference is given by:

$$\begin{aligned}M_k - M_{k-1} &= R_k - \mathbb{E}[R_k \mid \mathscr{F}_{k-1}] && (50)\\ &= -\eta(\mathbf{x}_k) + \mathbb{E}[\eta(\mathbf{x}_k) \mid \mathscr{F}_{k-1}] \leq \frac{\delta}{\delta} = 1 && (51)\end{aligned}$$

Finally, we must ensure that $\langle M\rangle_K$ is bounded:

$$\begin{aligned}\langle M\rangle_K &= \sum_{i=1}^{K}\mathbb{E}[(M_i - \mathbb{E}[M_i|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] && (52)\\ &= \sum_{i=1}^{K}\frac{1}{\delta^2}\mathrm{Var}(h(\mathbf{x}_i)|\mathscr{F}_{i-1}) \leq K\frac{\sigma^2}{\delta^2} && (53)\end{aligned}$$

Now we consider the inequalities:

$$\begin{aligned}&\max_{k\leq K} -\eta(\mathbf{x}_k) - K\frac{c}{\delta} + \eta(\mathbf{x}_0) \leq \max_{k\leq K}\eta(\mathbf{x}_k) - k\frac{c}{\delta} + \eta(\mathbf{x}_0)\\ &= \max_{k\leq K} R_k \leq \max_{k\leq K} M_k. && (54)\end{aligned}$$

Consider the case when $\lambda^* = -K\frac{c}{\delta} + \eta(\mathbf{x}_0)$. Then the safety event satisfies the containment:

$$\left\{\min_{k\leq K} h(\mathbf{x}_k) < 0\right\} \subset \left\{\max_{k\leq K} R_k \geq \lambda^*\right\} \subseteq \left\{\sup_{k\leq K} M_k \geq \lambda^*\right\}.$$

Applying the probability bound from Theorem 2 results in the desired probability bound:

$$P_u(K, \mathbf{x}_0) \leq H\left(\frac{-Kc + h(\mathbf{x}_0)}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right) \tag{55}$$

□

D. Proof of Proposition 2

Proof. By combining the bounds (DTCBF) and (13):

$$h(\mathbf{x}_{k+1}) \geq \mathbb{E}[h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] - \delta \geq \alpha h(\mathbf{x}_k) - \delta \tag{56}$$

Thus, for $K < \infty$, we can lower bound $h(\mathbf{x}_k) \geq \alpha^k h(\mathbf{x}_0) - \sum_{i=0}^{k-1}\alpha^i\delta$. Furthermore, for all time, $h(\mathbf{x}_k) \geq \frac{-\delta}{1-\alpha} \implies h(\mathbf{x}_{k+1}) \geq \frac{-\delta}{1-\alpha}$, so $\mathcal{C}_\delta$ is safe. □

E. Proof of Corollary 1

Proof. First define $\eta(\mathbf{x}) = \frac{h(\mathbf{x})+\epsilon}{\delta}$ and $R_k = -\alpha^{K-k}\eta(\mathbf{x}_k) + \alpha^K \eta(\mathbf{x}_0) + \sum_{i=1}^k \alpha^{K-i}\frac{\epsilon}{\delta}(1-\alpha)$. First note that h_k satisfies:

$$E[\eta(\mathbf{x}_k)|\mathscr{F}_{k-1}] \geq \alpha(\eta_{k-1}) + \frac{\epsilon}{\delta}(1-\alpha) \tag{57}$$

Note that R_k satisfies $R_0 = 0$ and is a supermartingale:

$$\mathbb{E}[R_{k+1}|\mathscr{F}_k] \tag{58}$$

$$= -\alpha^{K-(k+1)}\mathbb{E}[\eta_{k+1}|\mathscr{F}_k] + \alpha^K\eta_0 + \sum_{i=1}^{k+1}\alpha^{K-i}\epsilon(1-\alpha)/\delta$$

$$\leq -\alpha^{K-k}\eta_k + \alpha^K\eta_0 + \sum_{i=1}^{k}\alpha^{K-i}\epsilon(1-\alpha)/\delta = R_k. \tag{59}$$

Next, we take the Doob's decomposition and consider the martingale:

$$M_k = R_k + \sum_{i=1}^k (R_{i-1} - \mathbb{E}[R_i|\mathscr{F}_{i-1}]) \tag{60}$$

$$= R_k + \sum_{i=1}^k \alpha^{K-i}\left(\mathbb{E}[\eta(\mathbf{x}_i)|\mathscr{F}_{i-1}] - \alpha\eta_{i-1} + \frac{\epsilon}{\delta}(1-\alpha)\right)$$

$$\leq R_k \tag{61}$$

Since the predictable quadratic variation $\langle h(\mathbf{x})\rangle_k$ is bounded, so is $\langle M\rangle_k$:

$$\langle M\rangle_k = \sum_{i=1}^k \mathbb{E}[(W_i - \mathbb{E}[W_i|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \tag{62}$$

$$= \sum_{i=1}^k \alpha^{2(K-i)}\mathbb{E}[(\eta(\mathbf{x}_k) - \mathbb{E}[\eta(\mathbf{x}_i)|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \tag{63}$$

$$= \sum_{i=1}^k \frac{\alpha^{2(K-i)}}{\delta^2}\mathbb{E}[(h(\mathbf{x}_k) - \mathbb{E}[h(\mathbf{x}_i)|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \tag{64}$$

$$\leq \sum_{i=1}^k \frac{\alpha^{2(K-i)}}{\delta^2}\sigma^2 \leq \frac{K\sigma^2}{\delta^2} \tag{65}$$

Next we consider the implications:

$$\min_{k\leq K}\eta(\mathbf{x}_k) < 0 \implies \min_{1\leq k\leq K}\eta(\mathbf{x}_k) \leq 0 \tag{66}$$

$$\implies \max_{1\leq k\leq K} W_k \geq \alpha^K\eta(\mathbf{x}_0) \implies \max_{1\leq k\leq K} M_k \geq \alpha^K\eta(\mathbf{x}_0)$$

Considering the case when $\lambda^* = \alpha^K\eta(\mathbf{x}_0)$ ensures that:

$$P_u(K, \mathbf{x}_0) \leq H\left(\alpha^K\eta(\mathbf{x}_0), \frac{\sigma\sqrt{k}}{\delta}\right) \tag{67}$$

Finally we can bound h as in Proposition 2 to find that:

$$h(\mathbf{x}_k) \geq \alpha^K h(\mathbf{x}_0) - \sum_{i=0}^{K-1}\alpha^i\delta \quad \text{(a.s.)} \tag{68}$$

to achieve the indicator probability:

$$P_u(K, \mathbf{x}_0) \leq \mathbb{1}_{\left\{-\epsilon \geq \alpha^K h(\mathbf{x}_0) - \sum_{i=0}^{K-1}\alpha^i\delta\right\}} \tag{69}$$

and take the smaller bound between (67) and (69) via multiplication, to obtain the desired bound in (30). □

F. Proof of Theorem 1

Proof. Define

$$\Delta(\lambda, B, \sigma, K, \delta) \triangleq 1 - \frac{\lambda}{B} - H\left(\frac{\lambda}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right). \tag{70}$$

Thus, if $\Delta(\lambda, B, \sigma, K, \delta) \geq 0$, then the desired bound (29) is true.

We first prove that Δ is monotonically decreasing in σ^2. Consider $\frac{\partial\Delta}{\partial(\sigma^2)}$:

$$\frac{\partial\Delta}{\partial(\sigma^2)} = a(\lambda, \sigma, K, \delta)b(\lambda, \sigma, K, \delta) \tag{71}$$

$$a(\lambda, \sigma, K, \delta) \triangleq -\frac{e^{\frac{\lambda}{\delta}}}{\delta^2\sigma^2}\left(\frac{\sigma^2 K}{\lambda\delta + \sigma^2 K}\right)^{\frac{(\lambda\delta+\sigma^2 K)}{\delta^2}} \leq 0, \tag{72}$$

$$b(\lambda, \sigma, K, \delta) \triangleq \left(\sigma^2 K\ln\left(\frac{\sigma^2 K}{\lambda\delta + \sigma^2 K}\right) + \lambda\delta\right). \tag{73}$$

The function $a(\lambda, \sigma, K, \delta)$ is nonpositive since $\lambda, \delta, \sigma, K \geq 0$. For b, the logarithm bound $\ln(r) \geq 1 - 1/r$ ensures that:

$$b(\lambda, \sigma, K, \delta) \geq \sigma^2 K\left(1 - \frac{\lambda\delta + \sigma^2 K}{\sigma^2 K}\right) + \lambda\delta = 0. \tag{74}$$

Thus $\Delta(\lambda, B, \sigma, K, \delta)$ is monotonically decreasing with respect to σ^2, so we can use the assumption[3] $\sigma^2 K \leq \lambda\delta$ to lower bound Δ as:

$$\Delta(\lambda, B, \sigma, K, \delta) \geq 1 - \frac{\lambda}{B} - \left(\frac{1}{2}\right)^{2\frac{\lambda}{\delta}} e^{\frac{\lambda}{\delta}} \tag{75}$$

$$= 1 - \frac{\lambda}{B} - e^{(1-2\ln(2))\frac{\lambda}{\delta}} \tag{76}$$

$$= 1 - \frac{\lambda}{B} - e^{-\varphi\frac{\lambda}{\delta}} \triangleq \Delta_1(\lambda, B, \delta) \tag{77}$$

where $\varphi \triangleq 2\ln(2) - 1 > 0$.

Next, to show that $\Delta_1(\lambda, B, \delta) \geq 0$ for $\lambda \in \left[0, B - \frac{\delta}{\varphi}\right]$ which is non-empty since $\lambda \geq 0$ and $B \geq \lambda + \frac{\delta}{\varphi}$ implies that $B \geq \frac{\delta}{\varphi}$. We prove this by showing that $\Delta_1(\lambda, B, \delta) \geq 0$ for $\lambda = \left\{0, B - \frac{\delta}{\varphi}\right\}$ and that Δ_1 is concave with respect to λ.

<u>**(1)** At $\lambda = 0$:</u> $\Delta_1(0, B, \delta) = 1 - 0 - e^0 = 0$

<u>**(2)** At $\lambda = B - \frac{\delta}{\varphi}$:</u>

$$\Delta_1\left(B - \frac{\delta}{\varphi}, B, \delta\right) = \frac{\delta}{\varphi B} - e^{-\left(B - \frac{\delta}{\varphi}\right)\frac{\varphi}{\delta}} = \frac{\delta}{\varphi B} - e^{\left(1 - \frac{B\varphi}{\delta}\right)}$$

$$\geq \frac{\delta}{\varphi B} - \frac{\delta}{\varphi B} = 0. \tag{78}$$

Where the inequality in line (78) is due to the previously used log inequality: $\ln(r) \geq 1 - \frac{1}{r} \iff r \geq e^{\left(1-\frac{1}{r}\right)}$ which holds since for $r = \frac{\delta}{B\varphi}$ since $B, \delta, \varphi > 0$.

<u>**(3)** Concavity for $\lambda \in \left[0, B - \frac{\delta}{\varphi}\right]$:</u> Consider the second derivative of Δ_1 with respect to λ,

$$\frac{\partial^2\Delta_1}{\partial\lambda^2} = -\left(\frac{\varphi}{\delta}\right)^2 e^{-\varphi\frac{\lambda}{\delta}} < 0. \tag{79}$$

[3]Tighter bounds can be found by further optimizing the inequality $\sigma^2 K \leq \rho\lambda\delta$ for some $\rho \neq 1$.

Thus, Δ_1 is concave with respect to λ. Since, for all $\delta > 0$, $\Delta_1(0, B, \delta) \geq 0$, $\Delta_1\left(B - \frac{\delta}{\varphi}, B, \delta\right) \geq 0$, and $\Delta_1(\lambda, B, \delta)$ is concave, it follows from the definition of concavity that $\Delta_1(\lambda, B, \delta) \geq 0$ for all $\lambda \in \left[0, B - \frac{\delta}{\varphi}\right]$.

Using this lower bound for $\Delta_1(\lambda, B)$, we have $\Delta(\lambda, B, \sigma, K, \delta) \geq \Delta_1(\lambda, B) \geq 0$ which implies the desired inequality (29). $\square$

REFERENCES

[1] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control Barrier Function Based Quadratic Programs for Safety Critical Systems," *IEEE Transactions on Automatic Control*, vol. 62, pp. 3861–3876, Aug. 2017.

[2] S. Kolathaya and A. D. Ames, "Input-to-State Safety With Control Barrier Functions," *IEEE Control Systems Letters*, vol. 3, pp. 108–113, Jan. 2019. Conference Name: IEEE Control Systems Letters.

[3] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-Jacobi Reachability: A Brief Overview and Recent Advances," Sept. 2017. arXiv:1709.07523.

[4] F. Borrelli, A. Bemporad, and M. Morari, *Predictive control for linear and hybrid systems*. Cambridge University Press, 2017.

[5] O. So, A. Clark, and C. Fan, "Almost-sure safety guarantees of stochastic zero-control barrier functions do not hold," 2023.

[6] M. Black, G. Fainekos, B. Hoxha, D. Prokhorov, and D. Panagou, "Safety under uncertainty: Tight bounds with risk-aware control barrier functions," in *2023 IEEE International Conference on Robotics and Automation (ICRA)*, IEEE, May 2023.

[7] H. J. Kushner, "Stochastic Stability and Control.," Jan. 1967. NTRS Author Affiliations: NTRS Document ID: 19680034059 NTRS Research Center: Legacy CDMS (CDMS).

[8] R. K. Cosner, P. Culbertson, A. J. Taylor, and A. D. Ames, "Robust Safety under Stochastic Uncertainty with Discrete-Time Control Barrier Functions," Feb. 2023. arXiv:2302.07469.

[9] C. Santoyo, M. Dutreix, and S. Coogan, "Verification and Control for Finite-Time Safety of Stochastic Systems via Barrier Functions," May 2019. arXiv:1905.12077 [cs].

[10] J. Steinhardt and R. Tedrake, "Finite-time regional verification of stochastic non-linear systems," *The International Journal of Robotics Research*, vol. 31, pp. 901–923, June 2012.

[11] F. B. Mathiesen, L. Romao, S. C. Calvert, A. Abate, and L. Laurenti, "Inner approximations of stochastic programs for data-driven stochastic barrier function design," *arXiv preprint arXiv:2304.04505*, 2023.

[12] V. K. Sharma and S. Sivaranjani, "Safe control design through risk-tunable control barrier functions," in *2023 62nd IEEE Conference on Decision and Control (CDC)*, pp. 4393–4398, IEEE, 2023.

[13] A. Singletary, M. Ahmadi, and A. D. Ames, "Safe Control for Nonlinear Systems with Stochastic Uncertainty via Risk Control Barrier Functions," Mar. 2022. arXiv:2203.15892.

[14] M. Ahmadi, A. Singletary, J. W. Burdick, and A. D. Ames, "Safe Policy Synthesis in Multi-Agent POMDPs via Discrete-Time Barrier Functions," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, pp. 4797–4803, Dec. 2019. ISSN: 2576-2370.

[15] C. Santoyo, M. Dutreix, and S. Coogan, "A barrier function approach to finite-time stochastic system verification and control," *Automatica*, vol. 125, p. 109439, Mar. 2021.

[16] M. Vahs, C. Pek, and J. Tumova, "Belief control barrier functions for risk-aware control," *IEEE Robotics and Automation Letters*, 2023.

[17] R. K. Cosner, I. Sadalski, J. K. Woo, P. Culbertson, and A. D. Ames, "Generative modeling of residuals for real-time risk-sensitive safety with discrete-time control barrier functions," May 2023.

[18] J. Ville, "Etude critique de la notion de collectif," 1939.

[19] X. Fan, I. Grama, and Q. Liu, "Hoeffding's inequality for supermartingales," *Stochastic Processes and their Applications*, vol. 122, no. 10, pp. 3545–3559, 2012.

[20] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots," *The international journal of robotics research*, vol. 5, no. 1, pp. 90–98, 1986.

[21] 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 XIII*, Robotics: Science and Systems Foundation, July 2017.

[22] J. Zeng, B. Zhang, and K. Sreenath, "Safety-Critical Model Predictive Control with Discrete-Time Control Barrier Function," in *2021 American Control Conference (ACC)*, pp. 3882–3889, IEEE, May 2021.

[23] A. J. Taylor, V. D. Dorobantu, R. K. Cosner, Y. Yue, and A. D. Ames, "Safety of Sampled-Data Systems with Control Barrier Functions via Approximate Discrete Time Models," June 2022. arXiv:2203.11470.

[24] P. Culbertson, R. K. Cosner, M. Tucker, and A. D. Ames, "Input-to-State Stability in Probability," Apr. 2023. arXiv:2304.14578 [cs, eess].

[25] G. Grimmett and D. Stirzaker, *Probability and Random Processes*. Oxford University Press, July 2020.

[26] D. A. Freedman, "On tail probabilities for martingales," *the Annals of Probability*, pp. 100–118, 1975.

[27] X. Xiong and A. D. Ames, "Orbit characterization, stabilization and composition on 3d underactuated bipedal walking via hybrid passive linear inverted pendulum model," in *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp. 4644–4651, IEEE, 2019.

[28] A. B. Ghansah, J. Kim, M. Tucker, and A. D. Ames, "Humanoid robot co-design: Coupling hardware design with gait generation via hybrid zero dynamics," in *2023 62nd IEEE Conference on Decision and Control (CDC)*, pp. 1879–1885, IEEE, 2023.