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 unstructured uncertainties such as modeling error and external disturbances. Typical robust safety methods achieve their guarantees by always assuming that the worst-case disturbance will occur. In contrast, this paper utilizes Freedman's inequality in the context of discrete-time control barrier functions (DTCBFs) and c-martingales 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 does not require the barrier function to be upper-bounded, which makes the resulting safety probability bounds more useful for intuitive safety constraints 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 stronger. Finally, we present simulation examples, including a bipedal walking robot, that demonstrate the utility and tightness of our safety guarantee.**

***Index Terms*— Constrained control, Lyapunov methods, robotics, stochastic systems, uncertain systems**

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. Historically, control theory has treated the problem of safety under uncertainty using deterministic methods, often seeking safety guarantees in the presence of bounded disturbances. This problem has been studied using a variety of safe control approaches including control barrier functions (CBFs) [2], backwards Hamilton-Jacobi (HJ) reachability [3], and state-constrained model-predictive control (MPC) [4]. However, this worst-case analysis often leads to conservative performance since it ensures robustness to adversarial disturbances which are uncommon in practice.

Stochastic methods provide an alternative to the worst-case bounding approach. Instead of a conservative uncertainty bound, these methods consider a distribution of possible disturbances. Although they do not provide absolute, risk-free safety guarantees, they allow for smooth degradation of safety via variable, risk-aware levels of conservatism. A wide variety of stochastic safety methods exist including: reachability-based optimal safety [6], [7], constrained coherent risk measures [8], sampling-based general risk measures [9], and martingale-based methods [10], [11] amongst many others. In this work, we will focus on martingale-based methods due to their ability to generate trajectory-long guarantees and their relative simplicity as a method which relies primarily on only a distribution's first-moment.

Continuous-time martingale-based stochastic safety methods have successfully achieved strong probabilistic safety guarantees [12]–[14], [15], but generally require controllers with functionally infinite bandwidth, a strong assumption for real-world systems with discrete-time sensing and actuation. Alternatively, discrete-time methods have shown success while also capturing the sampled-data complexities of most real-world systems [10], [16]–[18]. In this work we focus on ex-

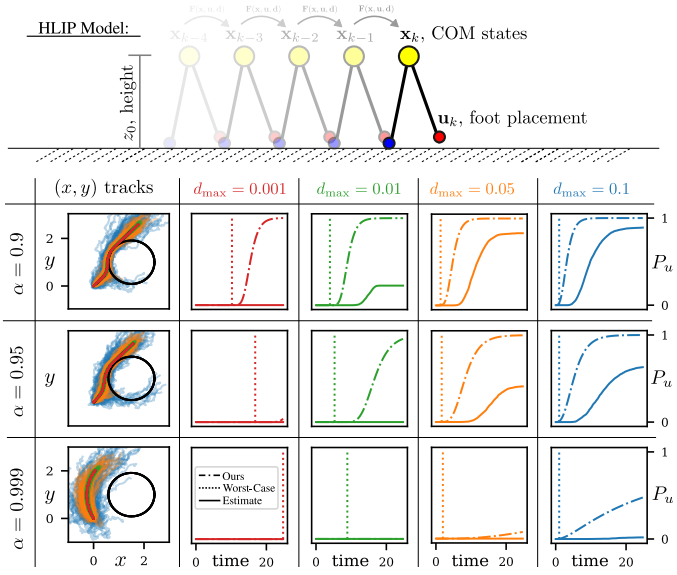

Fig. 1. Safety results for a bipedal robot navigating around an obstacle using our method. Details are provided in Section IV. **(Top)** Visualization of the Hybrid Linear Inverted Pendulum (HLIP) model. Yellow indicates the center-of-mass (COM), blue is the stance foot, and red is the swing foot. The states $\mathbf{x}_k$ are the global COM position, the relative COM position, and COM velocity, and the input is the relative position of the feet at impact. **(Bottom)** A table with variable maximum disturbance value ($d_{\max}$) and controller parameter (α) shows our (dashed lines) theoretical bound on safety failure from Thm. 3, (dotted lines) the shortest first-violation time based on the worst-case disturbance approximation, and (solid lines) approximated probabilities from 5000 trials (lower is safer). On the left, the trajectories of the COM are shown walking from bottom left towards the top right while avoiding the obstacle with each color corresponding to a different $d_{\max}$. The robot attempts to avoid the obstacle (black). Code to reproduce this plot can be found at [5].

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.

tending the theory of discrete-time martingale-based stochastic safety involving discrete-time control barrier functions (DTCBFs) and c-martingales.

The stochastic distrete-time martingale-based stochastic safety literature has shown significant theoretical success [10], [11], [14], [16], [18] in generating risk-based safety guarantees and in deploying these guarantees to real-world systems [19]. In this work we seek to extend these existing martingale-based safety techniques by utilizing a different (and often stronger) concentration inequality that can provide sharper safety probability bounds. Where other works have traditionally relied on Ville's inequality [20], we instead turn to Freedman's inequality [21]. By additionally assuming that the martingale differences and predictable quadratic variation are bounded, this inequality relaxes the nonnegativity assumption required by Ville's inequality while also providing generally tighter bounds that degrade smoothly with increasing uncertainty.

This paper combines discrete-time martingale-based safety techniques with Freedman's inequality to obtain tighter bounds on stochastic safety. We make three key contributions: (1) introducing Freedman-based safety probabilities for DTCBFs and c-martingales, (2) providing a range of parameter values where our bound is tighter than existing discrete-time martingale-based safety results, and (3) validating our method in simulation. We apply our results to a bipedal obstacle avoidance scenario (Fig. 1), using a reduced-order model of the step-to-step dynamics. This case study shows the utility of our probability bounds, which decay smoothly with increasing uncertainty and enable non-conservative, stochastic collision avoidance for bipedal locomotion.

II. Background

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

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

where $\mathbf{x}_k \in \mathbb{R}^n$ is the state, $\mathbf{u}_k \in \mathbb{R}^m$ is the input, $\mathbf{d}_k$ is an $\mathscr{F}_{k+1}$ measurable random disturbance which takes values in $\mathbb{R}^\ell$, 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 $\mathbf{k} : \mathbb{R}^n \to \mathbb{R}^m$:

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

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 user-defined "safe set", $\mathcal{C} \subset \mathbb{R}^n$, as is common in the robotics and control literature [1], [3], [4], [22].

Definition 1 (Forward Invariance and Safety[1])**.** *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" with respect to $\mathcal{C}$ 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 a continuous 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) [23])**.** *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[2]. On the other hand, they are similar in their ability to create *safety filters* for nominal controllers $\mathbf{k}_{\text{nom}} : \mathbb{R}^n \times \mathbb{Z} \to \mathbb{R}^m$ of the form:

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

Assuming feasibility, [3] $\mathbf{k}(\mathbf{x})$ guarantees safety for the undisturbed system by selecting inputs that satisfy (4) [23, Prop. 1].

For deterministic systems, infinite-horizon safety guarantees are common. However, for discrete-time stochastic systems, when the disturbance is bounded, infinite horizon guarantees fail to capture the nuances of variable risk levels and, when the disturbance is unbounded, infinite-horizon guarantees can be impossible to achieve[4] [27, Sec. IV]. In order to provide an achievable risk-based guarantee we choose to analyze finite-time safety probabilities as in [10], [11], [14], [15] instead of infinite-time safety guarantees.

Definition 3 (K-step Exit Probability)**.** *For any $K \in \mathbb{N}_1$ 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:*

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

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

[1] For this work we will focus on the safety of (2) exclusively at samples times as in [4] and [23]. We refer to [24] for an analysis of intersample safety.

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

[3] If infeasible, a slack variable can be added to recover feasibility and its effect on safety can be analyzed using the ISSf framework [2]. Additionally, unlike the affine inequality constraint that arises with continuous-time CBFs [1], the optimization problem (5) is not necessarily convex. To ameliorate this issue, it is often assumed that $h \circ \mathbf{F}$ is concave with respect to $\mathbf{u}$ [23], [25], [26].

[4] Consider the system: $\mathbf{x}_{k+1} = \mathbf{u}_k + \mathbf{d}_k$, where $\mathbf{x} \in \mathbb{R}$, $\mathbf{u} \in \mathbb{R}$, $\mathbf{d} \sim \mathcal{N}(0, 1)$, and $\mathcal{C} = \{\mathbf{x} \in \mathbb{R} \mid |\mathbf{x}| < 1\}$. At every time step, $\mathbb{P}\{\mathbf{x}_{k+1} \in \mathcal{C}\}$ is maximized with $\mathbf{u}_k = 0$, but then even over a single discrete step, there is at least 30% chance of failure. As time continues, this constant risk of failure at every step makes infinite horizon guarantees impossible to achieve.

B. Existing Martingale-based Safety Methods

In this work, we will generate bounds on K-step exit probabilities 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 [28], [10]). *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 W_k that is adapted to the filtration and is integrable at each k is a martingale if*

$$\mathbb{E}[\ W_{k+1} \mid \mathscr{F}_k\ ] = W_k, \quad \forall k \in \mathbb{Z} \quad \text{(a.s.)} \tag{7}$$

Additionally, if W_k satisfies:

$$\mathbb{E}[\ W_{k+1} \mid \mathscr{F}_k\ ] \leq W_k + c, \quad \forall k \in \mathbb{Z} \quad \text{(a.s.)}, \tag{8}$$

with $c = 0$ then it is a supermartingale and if it satisfies (8) with $c \geq 0$ then it is a $c-$martingale.

Many concentration inequalities can be used to bound the spread of a martingale over time. One particularly useful bound is Ville's [20] which bounds the probability that a supermartingale W_k rises above a threshold $\lambda > 0$.

Lemma 1 (Ville's Inequality [20]). *If W_k is a nonnegative supermartingale, then for all $\lambda > 0$,*

$$\mathbb{P}\left\{\sup_{k\in\mathbb{Z}} W_k > \lambda\right\} \leq \frac{\mathbb{E}[W_0]}{\lambda} \tag{9}$$

Critically, Ville's inequality assumes *nonnegativity* which manifests as a requirement that h be upper-bounded, e.g. (10). 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

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

for some $\alpha \in (0, 1)$ or $c \geq 0$. In this case, we can achieve the following bound on the K-step exit probability, $P_u(K, \mathbf{x}_0)$:

Theorem 1 (Safety using Ville's Inequality[5], [10], [11], [14], [16]). *If, for some $B > 0$ and $K \in \mathbb{N}_1$, the function $h : \mathbb{R}^n \to \mathbb{R}$ satisfies:*

$$h(\mathbf{x}) \leq B, \quad \text{for all } \mathbf{x} \in \mathbb{R}^n, \tag{10}$$

then:
$$P_u(K, \mathbf{x}_0) \leq 1 - \frac{\lambda}{B}, \tag{11}$$

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

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

[5] See Appx. C for a discussion notational differences between this presentation of Thm. 1 and that in [17] and [10]. Also, see [16, Thm. 5] for probability bounds associated with the general condition $\mathbb{E}[h(\mathbf{F}(\mathbf{x}_k, \mathbf{k}(\mathbf{x}_k), \mathbf{d}_k)) \mid \mathscr{F}_k] \geq \alpha h(\mathbf{x}_k) - c$ using Ville's inequality.

III. Safety Guarantees using Freedman's Inequality

This section presents our main result: K-step exit probability bounds for DTCBFs and c-martingales generated using Freedman's inequality, a particularly strong martingale concentration inequality. Here, we use the simpler, historical version as presented by Freedman [21]; see [29] for historical context and a new, tighter alternative which could also be used. After presenting this result, this section explores comparisons with existing Ville's-based methods and input-to-state safety.

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) [28]). *The PQV of a martingale W_k at $K \in \mathbb{N}_1$ is:*

$$\langle W \rangle_K \triangleq \textstyle\sum_{i=1}^{K} \mathbb{E}[(W_i - W_{i-1})^2 \mid \mathscr{F}_{i-1}] \tag{12}$$

Unlike Ville's inequality, Freedman's inequality does not require nonnegativity of the martingale W_k, thus removing the upper-bound requirement (10) on h. 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 (i.e. $W_{k+1} - W_k \leq 1$, similar to Azuma-Hoeffding methods [28]).*

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

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

Theorem 2 (Freedman's Inequality [21, Thm. 4.1]). *If, for some $K \in \mathbb{N}_1$ and $\xi > 0$, W_k is a supermartingale with $W_0 = 0$ such that:*

$$(W_k - W_{k-1}) \leq 1 \quad \text{for all } k \leq K, \quad \text{(Assumption 1)}$$
$$\langle W \rangle_K \leq \xi^2, \quad \text{(Assumption 2)}$$

then, for any $\lambda \geq 0$,

$$\mathbb{P}\left\{\max_{k\leq K} W_k \geq \lambda\right\} \leq H(\lambda, \xi) \triangleq \left(\frac{\xi^2}{\lambda + \xi^2}\right)^{\lambda+\xi^2} e^{\lambda}. \tag{13}$$

See [30, Appx.] D for a restatement of Freedman's proof.

A. Main Result: Freedman's Inequality for Safety

Next we present the key contribution of this paper: the application of Freedman's inequality to systems which satisfy the DTCBF or c-martingale conditions.

Theorem 3. *If, for some $K \in \mathbb{N}_1, \sigma > 0$, and $\delta > 0$, the following bounds[6] on the difference[7] between the true and predictable update (14) and the conditional variance (15) hold for all $k \leq K$:*

$$\mathbb{E}[\ h(\mathbf{x}_k) \mid \mathscr{F}_{k-1}\ ] - h(\mathbf{x}_k) \leq \delta, \tag{14}$$
$$\text{Var}(\ h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k\ ) \leq \sigma^2, \tag{15}$$

[6] Only upper-bounds on δ and σ^2 are required for (16) to hold and this guarantee is robust to changes in distribution that still satisfy (14) and (15). For real-world systems, distribution-learning can be employed, similar to [19].

[7] See Appx. G for a constructive method for determining δ and σ.

then the K-step exit probability is bounded as:

$$P_u(K, \mathbf{x}_0) \leq H\left(\tfrac{\lambda}{\delta}, \tfrac{\sigma\sqrt{K}}{\delta}\right), \tag{16}$$

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

To apply Thm. 2 to achieve Thm. 3 we follow this proof structure: **(Step 1)** normalize h and use it to construct a candidate supermartingale W_k, **(Step 2)** verify that W_k is indeed a supermartingale with $W_0 = 0$, **(Step 3)** use Doob's decomposition [28, Thm 12.1.10] to produce a martingale M_k from W_k in order to remove the negative effect of safe, predictable jumps from the PQV, **(Step 4)** verify that M_k satisfies Assp.s 1 and 2, **(Step 5)** choose $\lambda \geq 0$ such that a safety failure implies $\{\max_{k\leq K} W_k \geq \lambda\}$ as in (13), and **(Step 6)** specialize to specific values of α and c for each case.

Proof. **(Step 1)** Consider the case, for $\tilde{\alpha} \in (0, 1]$ and $\tilde{c} \geq 0$,

$$\text{where } \mathbb{E}[h(\mathbf{x}_{k+1})|\mathscr{F}_k] \geq \tilde{\alpha} h(\mathbf{x}_k) - \tilde{c}, \quad \text{for all } k \leq K. \tag{17}$$

First, define the normalized safety function $\eta(\mathbf{x}) \triangleq \frac{h(\mathbf{x})}{\delta}$ to ensure that the martingale differences will be bounded by 1. Next, use η to define the candidate supermartingale[8]

$$W_k \triangleq -\tilde{\alpha}^{K-k}\eta(\mathbf{x}_k) + \tilde{\alpha}^K \eta(\mathbf{x}_0) - \textstyle\sum_{i=1}^k \tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta} \tag{18}$$

(Step 2) This satisfies[9] $W_0 = 0$ and is a supermartingale:

$$\begin{aligned} &\mathbb{E}[W_{k+1}|\mathscr{F}_k] \\ &= -\tilde{\alpha}^{K-(k+1)}\mathbb{E}[\eta(\mathbf{x}_{k+1})|\mathscr{F}_k] + \tilde{\alpha}^K\eta(\mathbf{x}_0) - \textstyle\sum_{i=1}^{k+1}\tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta}, \\ &\leq -\tilde{\alpha}^{K-k}\eta(\mathbf{x}_k) + \tilde{\alpha}^K\eta(\mathbf{x}_0) - \textstyle\sum_{i=1}^{k}\tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta} = W_k. \end{aligned} \tag{19}$$

which can be seen by applying the bound from (17).
(Step 3) The martingale from Doob's decomposition is:

$$\begin{aligned} M_k &\triangleq W_k + \textstyle\sum_{i=1}^k (W_{i-1} - \mathbb{E}[W_i|\mathscr{F}_{i-1}]), \\ &= W_k + \textstyle\sum_{i=1}^k \underbrace{\frac{\tilde{\alpha}^{K-i}}{\delta}(\mathbb{E}[h(\mathbf{x}_i)|\mathscr{F}_{i-1}] - \tilde{\alpha}h(\mathbf{x}_{i-1}) + \tilde{c})}_{\geq 0} \geq W_k \end{aligned} \tag{20}$$

where the bound comes from (17) and positivity of $\tilde{\alpha}$ and δ.
(Step 4) Furthermore, M_k satisfies Assp. 1:

$$M_k - M_{k-1} = W_k - \mathbb{E}[W_k|\mathscr{F}_{k-1}], \tag{21}$$

$$= \tilde{\alpha}^{K-k}(\mathbb{E}[\eta(\mathbf{x}_k)|\mathscr{F}_{k-1}] - \eta(\mathbf{x}_k)) \leq \tilde{\alpha}^{K-k}\tfrac{\delta}{\delta} \leq 1, \tag{22}$$

since we assume in (14) that $\mathbb{E}[h(\mathbf{x}_k) \mid \mathscr{F}_{k-1}] - h(\mathbf{x}_k) \leq \delta$.

Next, $\tilde{\alpha} \in (0, 1]$ and (15) ensure that M_k satsifes Assp. 2:

$$\begin{aligned} \langle M\rangle_K &= \textstyle\sum_{i=1}^K \mathbb{E}[\tilde{\alpha}^{2(K-i)}(\eta(\mathbf{x}_i) - \mathbb{E}[\eta(\mathbf{x}_i)|\mathscr{F}_{i-1}])^2|\mathscr{F}_{i-1}] \\ &= \textstyle\sum_{i=1}^K \frac{\tilde{\alpha}^{2(K-i)}}{\delta^2}\mathrm{Var}(h(\mathbf{x}_i)|\mathscr{F}_{i-1}) \leq \sum_{i=1}^K \tilde{\alpha}^{2(K-i)}\frac{\sigma^2}{\delta^2} \quad (23) \\ &\leq \tfrac{\sigma^2 K}{\delta^2}. \quad (24) \end{aligned}$$

[8]We use the "empty sum" convention that $\sum_{i=1}^0 \rho = 0$ for any $\rho \in \mathbb{R}$.
[9]$W_0 = 0$ since $\mathbf{x}_0$ is known and randomness first enters through $\mathbf{d}_0$.

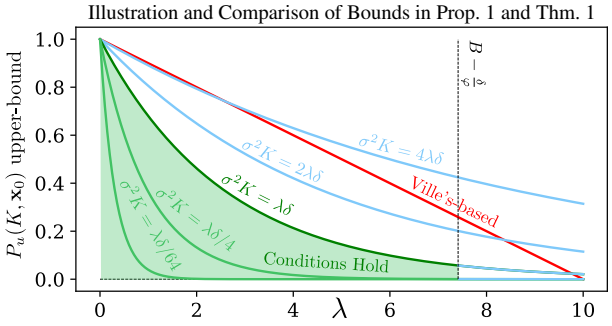

Fig. 2. Comparison for Prop. 1 with $B = 10, K = 100, \delta = 1$, and varying σ and λ. The Freedman-based bounds are shown in green when the conditions of Prop. 1 hold and blue when they do not. The Ville's-based bound is shown in red. Code to reproduce this plot can be found at [5]

(Step 5) Now, to relate the unsafe event $\{\min_{k\leq K} h(\mathbf{x}_k) < 0\}$ to our martingale M_k we consider the implications:

$$\min_{k\leq K} h(\mathbf{x}_k) < 0 \implies \min_{k\leq K} h(\mathbf{x}_k) \leq 0 \tag{25}$$

$$\iff \max_{k\leq K} -\tilde{\alpha}^{K-k}\eta(\mathbf{x}_k) \geq 0, \quad \text{since } \tilde{\alpha} > 0, \delta > 0 \tag{26}$$

$$\iff \max_{k\leq K} W_k \geq \tilde{\alpha}^K\eta(\mathbf{x}_0) - \textstyle\sum_{i=1}^k \tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta} \tag{27}$$

$$\implies \max_{k\leq K} M_k \geq \tilde{\alpha}^K\eta(\mathbf{x}_0) - \textstyle\sum_{i=1}^k \tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta} \tag{28}$$

$$\implies \max_{k\leq K} M_k \geq \tilde{\alpha}^K\eta(\mathbf{x}_0) - \textstyle\sum_{i=1}^K \tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta}, \tag{29}$$

where (26) is due to multiplication by a value strictly less than zero, (27) is due to adding zero, (28) is due to $M_k \geq W_k$ as in (20), and (29) is due to $k \leq K$ and the nonnegativity of α, δ, and $\tilde{c}$. Thus, the unsafe event satisfies the containment:

$$\left\{\min_{k\leq K} h(\mathbf{x}_k) < 0\right\} \subseteq \left\{\max_{k\leq K} M_k \geq \tilde{\alpha}^K\eta(\mathbf{x}_0) - \sum_{i=1}^K \tilde{\alpha}^{K-i}\frac{\tilde{c}}{\delta}\right\}$$

Since M_k satisfies $M_0 = 0$, $M_k - M_{k-1} \leq 1\ \forall k \leq K$, and $\langle M\rangle_K \leq \frac{\sigma^2 K}{\delta^2}$, we can apply Thm. 2 (Freedman's Ineq.) with $\lambda = \frac{\tilde{\alpha}^K h(\mathbf{x}_0) - \sum_{i=1}^K \tilde{\alpha}^{K-i}\tilde{c}}{\delta}$ to achieve the probability bound[10]: $P_u(K, \mathbf{x}_0) \leq H\left(\frac{\tilde{\alpha}^K h(\mathbf{x}_0) - \sum_{i=1}^K \tilde{\alpha}^{K-i}\tilde{c}}{\delta}, \frac{\sigma\sqrt{K}}{\delta}\right)$.
(Step 6) If the system satisfies the DTCBF condition, then (17) holds with $(\tilde{\alpha} = \alpha, \tilde{c} = 0)$ so the desired bound is achieved with $\lambda = \alpha^K h(\mathbf{x}_0)/\delta$ and if the system satisfies the c-mart. condition then (17) holds with $(\tilde{\alpha} = 1, \tilde{c} = c)$ so the desired bound is achieved with $\lambda = h(\mathbf{x}_0)/\delta - Kc$. □

B. Bound Tightness Comparison

We now relate the Freedman-based safety of Thm. 3 to the Ville's-based safety of Thm. 1. For systems that have an upper-bound h (10), a lower-bounded error (14), and a bounded conditional variance (15), we provide a range of values for σ, δ, K, B, and λ for which Thm. 3 is stronger. This Prop. provides a direct theoretical comparison (after changing notation) to the Ville's-based bounds in [10], [11], [14], [16].

Proposition 1. *For some $\sigma, \delta, B > 0$, $\lambda \geq 0$ and $K \in \mathbb{N}_1$, consider the conditions*

$$\lambda\delta \geq \sigma^2 K, \qquad \lambda \leq B - \tfrac{\delta}{\varphi}, \tag{30}$$

[10]The proof can end after Step 5 and can be applied to any system satisfying (17). We specialize to DTCBFs and c-martingales for clarity.

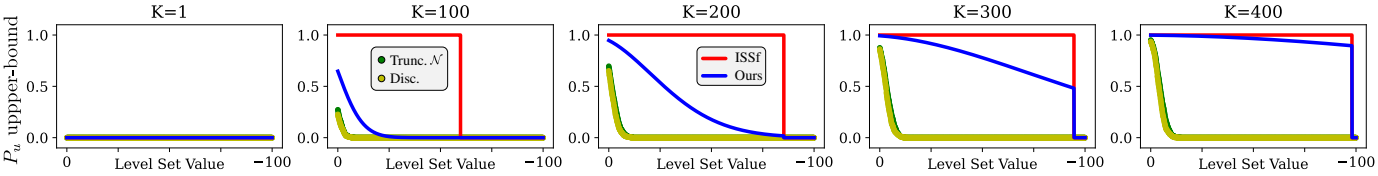

Fig. 3. Probability that the system is unsafe: our bound from Cor. 1 (blue), ISSf bound (red). The x-axis is the level set expansion $-\epsilon$ and the y-axis is the failure probability (lower is better). The plots from left to right indicate safety for $K = 1, 100, 200, 300$, and 400 steps. Simulations where $\mathbb{E}[h(\mathbf{x}_k)|\mathscr{F}_{k-1}] = \alpha h(\mathbf{x}_k)$ and approximate probabilities from 1000 samples are shown for simulations where $h(\mathbf{x}_k)$ is sampled from 3 different conditional distributions: uniform (pink), truncated Gaussian (green), and a categorical (yellow) all which satisfy Cor. 1. Code for these plots is can be found at [5].

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

$$H\left(\tfrac{\lambda}{\delta}, \tfrac{\sigma\sqrt{K}}{\delta}\right) \leq 1 - \tfrac{\lambda}{B}. \tag{31}$$

Proof of this Proposition is is provided in the Appendix.

Intuitively, conditions (30) stipulate that the conditional variance σ^2 and number of steps K must be limited by $\lambda\delta$, which is a function of the initial condition times the maximum single-step disturbance to $h(\mathbf{x}_k)$. Additionally, the initial condition must be less than the maximum safety bound B by an amount proportional to δ. The exact value of φ is a result of the first assumption ($\lambda\delta \geq \sigma^2 K$) and alternative values can be found by changing this assumption; for clarity of presentation, we leave exploration of these alternative assumptions to 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.

C. Extending Input-to-State Safety

Since Thm. 3 assumes that h has lower-bounded errors (14), we can directly compare our method with Input-to-State Safety (ISSf) [2], which provides almost-sure safety guarantees.

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

Proposition 2 (Input-to-State Safety)**.** *If the closed-loop system* (2) *satisfies the DTCBF condition and the bounded-jump condition* (14) *(a.s) for some* $\alpha \in [0, 1)$ *and* $\delta > 0$*, then* $h(\mathbf{x}_k) \geq \alpha^k h(\mathbf{x}_0) - \sum_{i=0}^{k-1} \alpha^i \delta$ *for all* $k \geq 0$ *and* $\mathcal{C}_\delta = \left\{\mathbf{x} \in \mathbb{R}^n \mid h(\mathbf{x}) \geq \frac{-\delta}{1-\alpha}\right\}$ *is safe (a.s.).*

Proof. By combining the bounds (DTCBF) and (14):

$$h(\mathbf{x}_{k+1}) \geq \mathbb{E}[h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] - \delta \geq \alpha h(\mathbf{x}_k) - \delta \text{ (a.s.)} \tag{32}$$

Thus, for all $k \in \mathbb{Z}$, we have the lower-bound $h(\mathbf{x}_k) \geq \alpha^k h(\mathbf{x}_0) - \sum_{i=0}^{k-1} \alpha^i \delta$ (a.s). 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 (a.s.). □

To compare with ISSf's worst-case safe set $\mathcal{C}_\delta$, we wish to use Thm. 3 to bound the probability that our system leaves some expanded safe set $\mathcal{C}_\epsilon = \{\mathbf{x} \in \mathbb{R}^n | h(\mathbf{x}) \geq -\epsilon\}$ with $\epsilon \geq 0$ in finite time.

Corollary 1. *If the hypotheses of Theorem 3 are satisfied and* (2) *satisfies the DTCBF for some* $\alpha \in (0, 1)$*, then for any value* $\epsilon \geq 0$ *and any* $K \in \mathbb{N}_1$*,*

$$P\left\{\min_{k \leq K} h(\mathbf{x}_k) < -\epsilon\right\} \tag{33}$$
$$\leq H\left(\lambda, \tfrac{\sigma}{\delta}\left(\tfrac{1-\alpha^{2K}}{1-\alpha^2}\right)^{\frac{1}{2}}\right) \mathbb{1}_{\left\{-\epsilon \geq \alpha^K h(\mathbf{x}_0) - \sum_{i=0}^{K-1} \alpha^i \delta\right\}}$$

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

Proof. The DTCBF condition ensures that, for any $\epsilon \geq 0$:

$$\mathbb{E}[\, h(\mathbf{x}_{k+1}) + \epsilon \mid \mathscr{F}_k \,] \geq \alpha(h(\mathbf{x}_k) + \epsilon) + \epsilon(1 - \alpha) \tag{34}$$
$$\geq \alpha(h(\mathbf{x}_k) + \epsilon) \tag{35}$$

We apply the same proof as Thm. 3 starting at (18) with $(\eta(\mathbf{x}_k) = \frac{h(\mathbf{x}_k)+\epsilon}{\delta}, \tilde{\alpha} = \alpha, \tilde{c} = 0)$. Choosing $\lambda = \alpha^K \eta(\mathbf{x}_0)$ and bounding[11] $\langle M \rangle_K \leq \sum_{i=1}^{K} \alpha^{2(K-i)} \frac{\sigma^2}{\delta^2} = \frac{\sigma^2(1-\alpha^{2K})}{\delta^2(1-\alpha^2)}$ as in (23) yields the desired bound without the indicator function by applying Thm. 2. The indicator function is a result of applying the lower bound on the safety value from Prop. 1, i.e. $h(\mathbf{x}_k) \geq \alpha^k h(\mathbf{x}_0) - \sum_{i=0}^{k-1} \alpha^i \delta$ (a.s.) for $k \in \mathbb{Z}$. □

A comparison of Prop. 1 and Cor. 2 and Monte Carlo approximations for various ϵ and a variety of distributions[12] is shown in Fig. 3 where we can see that our method successfully upper-bounds the sampled safety probabilities with risk-sensitive guarantees that are much less conservative than the worst-case bounds provided by ISSf.

For these simulations, we use the simple system:

$$\mathbf{x}_{k+1} = \alpha \mathbf{x}_k + \mathbf{d}_k \tag{36}$$

for $\mathbf{x} \in \mathbb{R}^1$, $\alpha = 0.99$, and zero-mean disturbances $\mathbf{d}_k$ sampled from a variety of distributions for up to $K = 400$ steps. This system naturally satisfies the DTCBF constraint:

$$\mathbb{E}[h(\mathbf{x}_{k+1})|\mathscr{F}_k] \geq \alpha h(\mathbf{x}_k) \text{ with } h(\mathbf{x}) = \mathbf{x}, \tag{37}$$

so we seek to provide guarantees of its inherent safety probabilities. In particular, in three different experiments we consider $\mathbf{d}_k$ sampled from one of three zero-mean distributions that all satisfy $|\mathbf{d}| \leq 1$ and $\sigma \leq \frac{1}{3}$: a uniform distribution $\mathcal{U}_{[-1,1]}$, a standard normal distribution truncated at -1 and 1, and a categorical distribution where $\mathbb{P}\{\mathbf{d} = -1\} = \frac{1}{6}$ and $\mathbb{P}\{\mathbf{d} = \frac{1}{5}\} = \frac{5}{6}$ to ensure 0 mean.

These simulations show that although our method is conservative compared to the Monte-Carlo approximations, it provides useful risk-based safety probabilities for a variety of $\mathcal{C}_\epsilon$ level sets whereas ISSf only provides a worst-case almost-surely bound.

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 Linear Inverted Pendulum (HLIP) model [31] approximates a bipedal

[11] This bound on $\langle M \rangle_K$ uses the finite geometric series identity and can also be applied for a tighter Thm. 3 and Prop. 1.

[12] Code for these simulations can be found at [5]

robot as an inverted pendulum with a fixed center of mass (COM) height $z_0 \in \mathbb{R}_{>0}$. 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 z_0 and gait parameters including the stance and swing phase periods. The HLIP model with an added disturbance matrix $\mathbf{D} \in \mathbb{R}^{6\times 4}$ and disturbance $\mathbf{d} \in \mathbb{R}^4$ affecting position and velocity 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 $\mathbf{x}_k = \begin{bmatrix}\mathbf{p}_k^\top & \mathbf{c}_k^\top & \mathbf{v}_k^\top\end{bmatrix}^\top$. We augment the standard HLIP model and assume that $\mathbf{d}$ enters linearly and $\mathcal{D}$ is a 4-dimensional, 0-mean uniform distribution[13] with $\|\mathbf{d}\| \leq d_{\max}$.

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

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

$$h(\mathbf{x}_{k+1}) \geq \widehat{\mathbf{e}}(\mathbf{p}_k)^\top (\mathbf{p}_{k+1} - \boldsymbol{\rho}) - r \triangleq \bar{h}(\mathbf{x}_{k+1}), \tag{38}$$

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

$$\begin{aligned} \mathbf{u}^* = \min_{\mathbf{u}\in\mathbb{R}^2} \quad & \|\mathbf{u} - \mathbf{k}_{\text{nom}}(\mathbf{x}_k)\| \\ \text{s.t.} \quad & \mathbb{E}\left[\, \bar{h}(\mathbf{x}_{k+1}) \mid \mathscr{F}_k \,\right] \geq \alpha \bar{h}(\mathbf{x}_k) \end{aligned} \tag{39}$$

with $\alpha \in (0, 1]$ and where $\mathbf{k}_{\text{nom}}$ 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 [5].

V. Conclusion

Despite the relative tightness guarantee of Prop. 1, the probability guarantees of our 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 further tightening. Additionally, the case study shown in Section IV presents an immediate direction for future work which may involving a hardware demonstration of this method.

Appendix

A. Proof of Ville's Inequality

Proof. Fix $\lambda > 0$ and define the stopping time $\tau \triangleq \inf\{k \in \mathbb{N} \mid W_k > \lambda\}$ with $\tau = +\infty$ if $W_k \leq \lambda$ for all time. Since W_k is a nonnegative supermartingale, the stopped process $W_{k\wedge\tau}$ is also a nonnegative supermartingale where

$$\mathbb{E}[W_{k\wedge\tau}] \leq \mathbb{E}[W_0] \text{ and } \liminf_{k\to\infty} \mathbb{E}[W_{k\wedge\tau}] \leq \mathbb{E}[W_0]. \tag{40}$$

[13] See Appx. H for bounds for δ and σ given this problem structure.

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

$$\begin{aligned} \mathbb{E}[W_0] &\geq \liminf_{k\to\infty} \mathbb{E}[W_{k\wedge\tau}\mathbb{1}_{\{\tau<\infty\}}] && (41)\\ &\geq \mathbb{E}[\liminf_{k\to\infty} W_{k\wedge\tau}\mathbb{1}_{\{\tau<\infty\}}] && (42)\\ &> \mathbb{E}[\lambda\mathbb{1}_{\tau<\infty}] = \lambda\mathbb{P}\{\tau<\infty\} = \lambda\mathbb{P}\left\{\sup_{k\in\mathbb{N}} W_k > \lambda\right\}. \end{aligned}$$

The first inequality is by the nonegativity of W_k, the second inequality is by Fatou's Lemma [28], and the third is by the definition of τ. Rearranging terms completes the proof. □

B. Proof of Theorem 1

Proof. We prove the two cases separately:

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

$$\begin{aligned} W_k &= \alpha^{-K}B - \alpha^{-k}h(\mathbf{x}_k) \geq \alpha^{-k}(B - h(\mathbf{x}_k)) \geq 0\\ \mathbb{E}[W_{k+1}|\mathscr{F}_k] &= \alpha^{-K}B - \alpha^{-(k+1)}\mathbb{E}[h(\mathbf{x}_{k+1})|\mathscr{F}_k]\\ &\leq \alpha^{-K}B - \alpha^{-k}h(\mathbf{x}_k) = W_k. \end{aligned} \tag{43}$$

  Apply Ville's inequality (1) to W_k to find:

$$\mathbb{P}\left\{\max_{k\leq K} W_k > \lambda\right\} \leq \frac{\mathbb{E}[W_0]}{\lambda}. \tag{44}$$

  Next note that the implication:

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

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

$$P_u(K, \mathbf{x}_0) \leq \frac{\alpha^{-K}B - h(\mathbf{x}_0)}{\alpha^{-K}B} = 1 - \frac{h(\mathbf{x}_0)}{B}\alpha^K \tag{45}$$

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

$$\begin{aligned} W_k^c &= B - h(\mathbf{x}_k) + (K-k)c \geq 0 && (46)\\ \mathbb{E}[W_{k+1}^c \mid \mathscr{F}_k] &= B - \mathbb{E}[h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k] + (K-k-1)c\\ &\leq B - h(\mathbf{x}_k) + c + (K-k-1)c && (47)\\ &= B - h(\mathbf{x}_k) + (K-k)c = W_k^c && (48) \end{aligned}$$

  Apply Ville's inequality (1) to W_k^c to find:

$$\mathbb{P}\left\{\max_{k\leq K} W_k^c > \lambda\right\} \leq \frac{\mathbb{E}[W_0^c]}{\lambda} \tag{49}$$

  Next note that the implication:

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

  ensure that $P_u(K, \mathbf{x}_0) \leq \mathbb{P}\{\max_{k\leq K} W_k^c > \lambda\}$. 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. Ville's-based Safety Theorems from [11] and [10]

To show how Prop. 1 can be used to compare with existing literature, we restate [11, Thm. 2] which contains [10, Thm, 2.3]. In particular, using the transformation, $h(\mathbf{x}) = B(1 - b_s(\mathbf{x}))$ where $b_s(\mathbf{x})$ is the relevant safety function from [11], [11, Thm. 2] can be rewritten as:

Theorem 4 ([11, Thm. 2]). *Given the closed-loop dynamics* (2) *and the sets* $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_0 \subset \text{Int}(\mathcal{C})$. *Suppose there exists a twice differentiable function* h *such that*

$$h(\mathbf{x}) \leq B, \quad \forall \mathbf{x} \in \mathcal{X}, \tag{50}$$

$$\mathbb{E}[h(\mathbf{F}(\mathbf{x}_k)) \mid \mathbf{x}_k] \leq \alpha h(\mathbf{x}_k) - c, \quad \forall \mathbf{x} \in \mathcal{C} \tag{51}$$

for some $\alpha \in (0, 1], c \in [B(\alpha - 1), \alpha)$, $\gamma \in [B, 0)$. *Then,*

$$\text{if } \alpha \in (0,1] \text{ and } c \leq 0,\ P_u(\mathbf{x}_0) \leq 1 - \tfrac{h(\mathbf{x}_0)}{B}\left(\tfrac{\alpha B - c}{B}\right)^K \tag{52}$$

$$\text{if } \alpha \in (0,1] \text{ and } c > 0,$$

$$P_u(\mathbf{x}_0, K) \leq 1 - \tfrac{\alpha^K h(\mathbf{x}_0)}{(1-\alpha)}\left(\tfrac{c + (1-\alpha)B}{B}\right) \tag{53}$$

$$\text{if } \alpha \in (0,1] \text{ and } c = 0,\ P_u(\mathbf{x}_0, K) \leq 1 - \frac{\alpha^K h(\mathbf{x}_0)}{B} \tag{54}$$

$$\text{if } \alpha = 1,\ P_u(\mathbf{x}_0, K) \leq 1 - \frac{h(\mathbf{x}_0) - cK}{B}. \tag{55}$$

One minor difference between these methods is that we consider a state $\mathbf{x}$ to be safe if $\mathbf{x} \in \mathcal{C}$ and in [11] they consider a state to be safe if it is in $\text{Int}(\mathcal{C})$. Ultimately, this makes very little difference for the bound because $\mathbf{x} \notin \mathcal{C} \implies \mathbf{x} \notin \text{Int}(\mathcal{C})$ and because $\mathcal{C} \setminus \text{Int}(\mathcal{C})$ is generally a set of zero measure.

D. Proof of Freedman's Inequality, (Theorem 2)

Here we represent the proof as given in [21] for reference.

First, Freedman presents the following bound on the exponential function. We refer to [21, Lem. 3.1 and Cor. 3.2] for the original calculus.

Lemma 2 ([21, Cor. 3.2]). *For* $\varphi(\gamma) \triangleq (e^\gamma - 1 - \gamma)$

$$e^{\gamma x} \leq 1 + \gamma x + x^2 \varphi(\gamma), \text{ for all } \gamma \geq 0, x \leq 1. \tag{56}$$

Freedman then uses this construction to bound the moment generating function of supermartingale differences to find the following bound from which the main theorem will follow almost immediately.

Proposition 3 ([21, Prop. 3.3]). *If* $W_k = \sum_{i=0}^k X_k$ *is a supermartingale with stopping time* τ *where* $W_k - W_{k-1} \leq 1$ (a.e.) *for all* $k \in \mathbb{N}_1$ *and any* $\gamma \geq 0$, *then*

$$\int_{\{\tau < \infty\}} e^{\gamma W_\tau - \varphi(\gamma)\langle W \rangle_\tau} d\mathbb{P} \leq 1. \tag{57}$$

Proof. Let $p_x(x)$ be the probability distribution of a random variable X with $X \leq 1$ (a.e.) and $\mathbb{E}[X] \leq 0$ (a.e.). Choose probability distributions $p_0(x)$ on $(-\infty, 1]$ and $p_-(x)$ on $(-\infty, 0)$ such that

$$\mathbb{E}_0[X] = \int_{(-\infty,\infty)} x p_0(x) dx = 0, \tag{58}$$

$$p_x(x) = \theta p_0(x) + (1-\theta) p_-(x). \tag{59}$$

Next we bound the moment generating function $\mathbb{E}\left[e^{\gamma X}\right]$,

$$\mathbb{E}\left[e^{\gamma X}\right] = \int_{(-\infty,1]} e^{\gamma x}(\theta p_0(x) + (1-\theta)p_-(x))dx \tag{60}$$

$$= \theta \mathbb{E}_0[e^{\gamma X}] + (1-\theta)\int_{(-\infty,0)} e^{\gamma x} p_-(x) dx \tag{61}$$

$$\leq \theta \int_{(-\infty,1]} e^{\gamma x} p_0(x) dx + (1-\theta) \tag{62}$$

$$\leq \theta \int_{(\infty,1]} (1 + \gamma x + x^2 \varphi(\gamma)) p_0(x) dx + (1-\theta) \tag{63}$$

$$= \theta(1 + 0 + \mathbb{E}_0[X^2]\varphi(\gamma)) + (1-\theta) \tag{64}$$

$$\leq \theta(1 + \mathbb{E}_0[X^2]\varphi(\gamma)) + (1-\theta)(1 + \varphi(\gamma)\text{Var}_-(X)) \tag{65}$$

$$\leq 1 + \varphi(\gamma)\left(\mathbb{E}[X^2] - (1-\theta)^2 \mathbb{E}_-[X]^2\right) \tag{66}$$

$$= 1 + \varphi(\gamma)\left(\mathbb{E}[X^2] - \mathbb{E}[X]^2\right) = 1 + \varphi(\gamma)\text{Var}(X), \tag{67}$$

$$\leq e^{\varphi(\gamma)\text{Var}(X)} \implies \mathbb{E}[e^{\gamma X - \varphi(\gamma)\text{Var}(X)}] \leq 1 \tag{68}$$

where (62) is attained by bounding $e^{\gamma x} \leq 1$ since $\gamma \geq 0$ and $x \in (-\infty, 0)$ and then using the fact that p_- is a probability distribution, (63) is attained by using of Lem. 2, (65) is attained by noting that $\varphi(\gamma) \geq 0$ and $\text{Var}_-(X) \geq 0$, (66) is attained by noting that $\mathbb{E}[X^2] = \theta\mathbb{E}_0[X^2] + (1-\theta)\mathbb{E}_-[X^2]$ and that $(1-\theta) \in [0,1]$ and $\mathbb{E}_-[X]^2 \geq 0$, (67) holds with equality since $\mathbb{E}_0[X] = 0$, and (68) holds due to the bound $1 + x \leq e^x$ for $x \geq 0$.

This allows us to establish that $Q_k \triangleq e^{\gamma W_k - \varphi(\gamma)\langle W \rangle_k}$ is a supermartingale since:

$$\mathbb{E}[Q_{k+1} \mid \mathscr{F}_k] = \mathbb{E}[e^{\gamma W_{k+1} - \varphi(\gamma)\langle W \rangle_{k+1}} \mid \mathscr{F}_k] \tag{69}$$

$$= Q_k \mathbb{E}\left[e^{\gamma(W_{k+1} - W_k) - \varphi(\gamma)(\langle W \rangle_{k+1} - \langle W \rangle_k)} \mid \mathscr{F}_k\right] \leq Q_k$$

which holds since $X \triangleq W_{k+1} - W_k$ given $\mathscr{F}_k$ satisfies 68.

Next we note that $Q_0 = 1$ and $Q_{k\wedge\tau}$ is also a positive supermartingale, so

$$1 \geq \liminf_{\tau\to\infty} \mathbb{E}[Q_{k\wedge\tau}] \geq \liminf_{\tau\to\infty} \mathbb{E}[Q_{k\wedge\tau} \mathbb{1}_{\{\tau<\infty\}}] \tag{70}$$

$$\geq \mathbb{E}[\liminf_{\tau\to\infty} Q_{k\wedge\tau}] = \mathbb{E}[Q_\tau \mathbb{1}_{\{\tau<\infty\}}], \tag{71}$$

where (as in [32, Proof of Thm. 2.3]) the indicator decreases the expectation because $Q_{k\wedge\tau}$ is positive, Fatou's lemma [28] justifies the third inequality, and the fact that $\tau < \infty$ for the indicator event yields the final equality which is equivalent to (57) as desired. □

Theorem (Freedman's Inequality [21, Thm. 4.1]). *If, for some* $K \in \mathbb{N}_1$ *and* $\xi > 0$, W_k *is a supermartingale with* $W_0 = 0$ *such that:*

$$(W_k - W_{k-1}) \leq 1 \quad \text{for all } k \leq K, \qquad \text{(Assumption 1)}$$

$$\langle W \rangle_K \leq \xi^2, \qquad \text{(Assumption 2)}$$

then, for any $\lambda \geq 0$,

$$\mathbb{P}\left\{\max_{k \leq K} W_k \geq \lambda\right\} \leq H(\lambda, \xi) \triangleq \left(\frac{\xi^2}{\lambda + \xi^2}\right)^{\lambda + \xi^2} e^\lambda. \tag{72}$$

Proof. Define the stopping time τ as the smallest $k \leq K$ such that $W_k \geq \lambda$, and $\tau = \infty$ if $W_k < \lambda$ for all $k \leq K$. Also

define the event $A \triangleq \{W_k \geq \lambda \text{ and } \tau < \infty \text{ for some } k \leq K\}$.

Next, we continue by bounding using any γ:

$$1 \geq \int_A \exp\{\gamma W_\tau - (e^\gamma - 1 - \gamma)\langle W_k \rangle\} d\mathbb{P} \tag{73}$$

$$\geq \int_A \exp\{\gamma\lambda - (e^\gamma - 1 - \gamma)\xi^2\} d\mathbb{P} \tag{74}$$

$$= \mathbb{P}\{A\} \exp\{\gamma\lambda - (e^\gamma - 1 - \gamma)\xi^2\} \tag{75}$$

$$\implies \mathbb{P}\{A\} \leq \exp\{(e^\gamma - 1 - \gamma)\xi^2 - \gamma\lambda\} \tag{76}$$

From here we choose $\gamma = \ln\left(\frac{\lambda+\xi^2}{\xi^2}\right)$ to minimize this probability bound and achieve the desired result (72). □

E. Proof of Proposition 1

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

If $\Delta(\lambda, B, \sigma, K, \delta) \geq 0$, then (31) must hold. We first show Δ is monotonically decreasing in σ^2. Consider[14] $\frac{\partial\Delta}{\partial(\sigma^2)} = a(\lambda, \sigma, K, \delta) b(\lambda, \sigma, K, \delta)$ where

$$a(\lambda, \sigma, K, \delta) \triangleq \frac{-e^{\frac{\lambda}{\delta}}}{\delta^2\sigma^2}\left(\frac{\sigma^2 K}{\lambda\delta+\sigma^2 K}\right)^{\frac{(\lambda\delta+\sigma^2 K)}{\delta^2}} < 0, \tag{77}$$

$$b(\lambda, \sigma, K, \delta) \triangleq \left(\sigma^2 K \ln\left(\frac{\sigma^2 K}{\lambda\delta+\sigma^2 K}\right) + \lambda\delta\right). \tag{78}$$

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

$$b(\lambda, \sigma, K, \delta) \geq \sigma^2 K\left(1 - \frac{\lambda\delta+\sigma^2 K}{\sigma^2 K}\right) + \lambda\delta = 0. \tag{79}$$

Since $a < 0$ and $b \geq 0$, $\Delta(\lambda, B, \sigma, K, \delta)$ is monotonically decreasing with respect to σ^2, so we can use the assumption $\sigma^2 K \leq \lambda\delta$ to lower bound Δ as:

$$\Delta(\lambda, B, \sigma, K, \delta) \geq 1 - \frac{\lambda}{B} - \left(\tfrac{1}{2}\right)^{2\frac{\lambda}{\delta}} e^{\frac{\lambda}{\delta}} \tag{80}$$

$$= 1 - \frac{\lambda}{B} - e^{(1-2\ln(2))\frac{\lambda}{\delta}} \triangleq 1 - \frac{\lambda}{B} - e^{-\varphi\frac{\lambda}{\delta}} \triangleq \Delta_1(\lambda, B, \delta)$$

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

Next, we show that $\Delta_1(\lambda, B, \delta) \geq 0$ for[15] $\lambda \in \left[0, B - \frac{\delta}{\varphi}\right]$. 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.

(1) Nonnegativity at $\lambda = 0$: $\Delta_1(0, B, \delta) = 0$.

(2) Nonnegativity at $\lambda = B - \frac{\delta}{\varphi}$:

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

$$\geq \frac{\delta}{\varphi B} - \frac{\delta}{\varphi B} = 0, \tag{81}$$

where the inequality in line (81) 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 for $r = \frac{\delta}{B\varphi} > 0$ since $B, \delta, \varphi > 0$.

(3) Concavity for $\lambda \in [0, B - \frac{\delta}{\varphi}]$: Since $\frac{\varphi}{\delta} > 0$, the second derivative of Δ_1 with respect to λ is negative:

$$\frac{\partial^2\Delta_1}{\partial\lambda^2} = -\left(\frac{\varphi}{\delta}\right)^2 e^{-\varphi\frac{\lambda}{\delta}} < 0. \tag{82}$$

[14]The derivation of this derivative is given after the proof.

[15]This interval is non-empty since $\lambda \geq 0$ and $B \geq \lambda + \frac{\delta}{\varphi}$ implies $B \geq \frac{\delta}{\varphi}$.

Thus, Δ_1 is concave with respect to λ. Since, $\Delta_1(0, B, \delta) \geq 0$, $\Delta_1\left(B - \frac{\delta}{\varphi}, B, \delta\right) \geq 0$, and $\Delta_1(\lambda, B, \delta)$ is concave for all $\delta > 0$ and $B \geq \frac{\delta}{\varphi}$, 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 (31). □

F. Derivative of $\frac{\partial\Delta}{\partial(\sigma^2)}$

E Here we show the derivation of the derivative given in (E). For reference, the complete function is:

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

with the partial derivative with respect to σ^2:

$$\frac{\partial\Delta}{\partial(\sigma^2)} = -e^{\frac{\lambda}{\delta^2}} \frac{\partial}{\partial(\sigma^2)}\left[u(\sigma^2)^{v(\sigma)}\right] \tag{83}$$

$$= -e^{\frac{\lambda}{\delta^2}} \frac{u(\sigma^2)^{v(\sigma^2)}}{u(\sigma^2)^{v(\sigma^2)}} \frac{\partial}{\partial(\sigma^2)}\left[u(\sigma^2)^{v(\sigma^2)}\right] \tag{84}$$

$$= -e^{\frac{\lambda}{\delta^2}} u(\sigma^2)^{v(\sigma^2)} \frac{\partial}{\partial(\sigma^2)}\left[\ln\left(u(\sigma^2)^{v(\sigma^2)}\right)\right] \tag{85}$$

$$= -e^{\frac{\lambda}{\delta^2}} u(\sigma^2)^{v(\sigma^2)} \frac{\partial}{\partial(\sigma^2)}\left[\ln\left(u(\sigma^2)\right) v(\sigma^2)\right] \tag{86}$$

$$= -e^{\frac{\lambda}{\delta^2}} u(\sigma^2)^{v(\sigma^2)} \left[\frac{v(\sigma^2)}{u(\sigma^2)}\frac{\partial u}{\partial(\sigma^2)} + \ln(u(\sigma^2))\frac{\partial v}{\partial(\sigma^2)}\right]$$

$$= -e^{\frac{\lambda}{\delta^2}} u(\sigma^2)^{v(\sigma^2)} \left[\frac{\lambda}{\delta\sigma^2} + \ln(u(\sigma^2))\frac{K}{\delta^2}\right]$$

$$= \underbrace{-\frac{e^{\frac{\lambda}{\delta^2}}}{\delta^2\sigma^2} u(\sigma^2)^{v(\sigma^2)}}_{\triangleq a(\lambda,\sigma,K,\delta)} \underbrace{\left[\lambda\delta + \sigma^2 K \ln(u(\sigma^2))\right]}_{\triangleq b(\lambda,\sigma,K,\delta)} \tag{87}$$

where introduce the following functions for clarity:

$$u(\sigma^2) \triangleq \frac{\sigma^2 K}{\delta\lambda + \sigma^2 K}, \qquad v(\sigma^2) \triangleq \frac{1}{\delta^2}(\lambda\delta + \sigma^2 K). \tag{88}$$

Critically, this proof multiplies by 1 in line (84) (which is well defined since $\sigma, \delta, K > 0$), then applies the product rule in reverse (85), and then uses the properties of the logarithm function (86). The derivation is finished by applying the product rule and rearranging terms.

G. Sufficient Conditions for Constructively Bounding δ and σ

Here we provide sufficient conditions for which bounds on δ and σ in Theorem 3's assumptions (14) and (15) are constructive.

Proposition 4. *If*

$$\mathbf{d} \sim \mathcal{D} \text{ satisfies } \|\mathbf{d}\| \leq d_{\max} \text{ for some } d_{\max} \geq 0, \tag{89}$$

$$h : \mathbb{R}^n \to \mathbb{R} \text{ is globally Lipschitz with } \mathcal{L}_h \geq 0, \tag{90}$$

$$\mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k) + \mathbf{d}_k, \text{ for some } \mathbf{F} : \mathbb{R}^n \to \mathbb{R}^n, \tag{91}$$

then

$$\mathbb{E}[h(\mathbf{x}_k) \mid \mathscr{F}_{k-1}] - h(\mathbf{x}_k) \leq 2\mathcal{L}_h d_{\max} \triangleq \delta, \tag{92}$$

$$\text{Var}(h(\mathbf{x}_{k+1}) \mid \mathscr{F}_k) \leq \mathcal{L}_h^2 d_{\max}^2 \triangleq \sigma^2 \tag{93}$$

Proof. First we bound δ:

$$\begin{aligned}
&\mathbb{E}[h(\mathbf{x}_k) \mid \mathscr{F}_{k-1}] - h(\mathbf{x}_k) && (94)\\
&= \mathbb{E}[h(\mathbf{F}(\mathbf{x}_{k-1}) + \mathbf{d}_{k-1}) \mid \mathscr{F}_{k-1}] - h(\mathbf{F}(\mathbf{x}_{k-1}) + \mathbf{d}_{k-1})\\
&\leq \mathbb{E}[h(\mathbf{F}(\mathbf{x}_{k-1})) + \mathcal{L}_h\|\mathbf{d}_{k-1}\| \mid \mathscr{F}_{k-1}] && (95)\\
&\qquad - h(\mathbf{F}(\mathbf{x}_{k-1})) + \mathcal{L}_h\|\mathbf{d}_{k-1}\|\\
&= h(\mathbf{F}(\mathbf{x}_{k-1})) - h(\mathbf{F}(\mathbf{x}_{k-1})) + \mathcal{L}_h\mathbb{E}[\|\mathbf{d}_{k-1}\|] + \mathcal{L}_h\|\mathbf{d}_{k-1}\|\\
&\leq \mathcal{L}_h\mathbb{E}[d_{\max}] + \mathcal{L}_h d_{\max} = 2\mathcal{L}_h d_{\max} \triangleq \delta && (96)
\end{aligned}$$

To bound σ^2, note that boundedness of $\mathcal{D}$ and Lipschitz continuity of h implies that:

$$h(\mathbf{F}(\mathbf{x}_k)) - \mathcal{L}_h d_{\max} \leq h(\mathbf{F}(\mathbf{x}_k) + \mathbf{d}_k) \leq h(\mathbf{F}(\mathbf{x}_k)) + \mathcal{L}d_{\max}.$$

Thus, the distribution of $h(\mathbf{F}(\mathbf{x}_k) + \mathbf{d}_k)$ is bounded at $\mathscr{F}_k$, so we can use Popoviciu's inequality on variances [33] to achieve:

$$\text{Var}(h(\mathbf{F}(\mathbf{x}_k) + \mathbf{d} \mid \mathscr{F}_{k-1}) \leq \mathcal{L}_h^2 d_{\max}^2 \triangleq \sigma^2 \tag{97}$$

□

H. Bounding δ and σ^2 in the Example

The bound (14) can be obtained for the example in Section IV by using the given assumptions that $\mathcal{D}$ is uniform on the ball of radius $d_{\max}$ and that the matrices $\mathbf{C}$ and $\mathbf{D}$ reflect the fact that safety is defined only with respect to position and that the global position and the center-of-mass (COM) position are coupled. These facts give $\mathbf{C}$ and $\mathbf{D}$ this structure:

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{D} = \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{98}$$

In this case we can calculate δ as:

$$\begin{aligned}
&\mathbb{E}[h(\mathbf{x}_k) \mid \mathscr{F}_{k-1}] - h(\mathbf{x}_k) && (99)\\
&= \mathbb{E}[h(\mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{D}\mathbf{d}_{k-1})] \mid \mathscr{F}_{k-1}] && (100)\\
&\qquad - h(\mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{D}\mathbf{d}_{k-1}))\\
&= \mathbb{E}[\|\mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{D}\mathbf{d}_{k-1} - \boldsymbol{\rho}\|] \mid \mathscr{F}_{k-1}] && (101)\\
&\qquad - \|\mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{D}\mathbf{d}_{k-1} - \boldsymbol{\rho}\|\\
&\leq \|\mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1}) - \boldsymbol{\rho}\| + \mathbb{E}[\|\mathbf{C}\mathbf{D}\mathbf{d}_{k-1}\|]] && (102)\\
&\qquad - \|\mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} - \boldsymbol{\rho})\| + \|\mathbf{C}\mathbf{D}\mathbf{d}_{k-1}\|\\
&= \mathbf{E}[\|\mathbf{C}\mathbf{D}\mathbf{d}_{k-1}\|] + \|\mathbf{C}\mathbf{D}\mathbf{d}_{k-1}\| && (103)\\
&\leq \mathbf{E}[\|\mathbf{C}\mathbf{D}\mathbf{d}_{k-1}\|] + d_{\max} && (104)\\
&= \int_{\mathcal{B}_{d_{\max}}(0)} \frac{1}{\pi d_{\max}^2}\|\mathbf{C}\mathbf{D}\mathbf{d}_{k-1}\| d\mathbf{d}_{k-1} + d_{\max} && (105)\\
&= \int_0^{2\pi}\int_0^{d_{\max}} \frac{r^2}{\pi d_{\max}^2} dt d\theta + d_{\max} = \frac{2}{3}d_{\max} + d_{\max} && (106)\\
&= \frac{5}{3}d_{\max} \triangleq \delta. && (107)
\end{aligned}$$

where we use the triangle inequality and then calculate the expectation in (104) exactly on the ball $\mathcal{B}_{d_{\max}}(0) \subset \mathbb{R}^2$ using a coordinate transform to produce a less conservative bound.

Next, to bound σ^2 consider some constant vector $\mathbf{a} \in \mathbb{R}^2$ and random vector $\mathbf{b} \in \mathbb{R}^2$ that is uniformly distributed on the ball of radius $\mathbf{d}_{\max}$, i.e. $\mathcal{B}_{d_{\max}}(0)$.

First, we will lower-bound $\mathbb{E}[\|\mathbf{a} - \mathbf{b}\|]^2$ using Jensen's inequality given the convexity of the 2-norm:

$$\mathbb{E}[\|\mathbf{a} - \mathbf{b}\|] \geq \|\mathbf{a} - \mathbb{E}[\mathbf{b}]\| = \|\mathbf{a}\| \geq 0 \tag{108}$$

$$\implies \mathbb{E}[\|\mathbf{a} - \mathbf{b}\|]^2 \geq \|\mathbf{a}\|^2 \tag{109}$$

Next, we will bound $\mathbb{E}[\|\mathbf{a} - \mathbf{b}\|^2]$ by using the definition of the 2-norm squared and the linearity of the expectation,

$$\begin{aligned}
&\mathbb{E}[\|\mathbf{a} - \mathbf{b}\|^2] = \mathbb{E}[(\mathbf{a} - \mathbf{b})^\top(\mathbf{a} - \mathbf{b})] && (110)\\
&= \mathbb{E}[\mathbf{a}^\top\mathbf{a} - 2\mathbf{a}^\top\mathbf{b} + \mathbf{b}^\top\mathbf{b}] && (111)\\
&= \|\mathbf{a}\|^2 - 2\mathbf{a}^\top\mathbb{E}[\mathbf{b}] + \mathbb{E}[\|\mathbf{b}\|^2] = \|\mathbf{a}\|^2 + \mathbb{E}[\|\mathbf{b}\|^2] && (112)
\end{aligned}$$

We then use these two bounds, along with a coordinate transform, to calculate the variance.

$$\begin{aligned}
\text{Var}(\|\mathbf{a} - \mathbf{b}\|) &= \mathbb{E}[\|\mathbf{a} - \mathbf{b}\|^2] - \mathbb{E}[\|\mathbf{a} - \mathbf{b}\|]^2 && (113)\\
&\leq \mathbb{E}[\|\mathbf{a} - \mathbf{b}\|^2] - \|\mathbf{a}\|^2 = \|\mathbf{a}\|^2 + \mathbb{E}[\|\mathbf{b}\|^2] - \|\mathbf{a}\|^2\\
&= \int_0^{2\pi}\int_0^{d_{\max}} \frac{r^3}{\pi d_{\max}^2} dr d\theta = \frac{2\pi d_{\max}^4}{4\pi d_{\max}^2} = \frac{1}{2}d_{\max}^2 \triangleq \sigma^2
\end{aligned}$$

To find the value for σ^2 define $\mathbf{a} \triangleq \mathbf{C}(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}(\mathbf{u}_{k-1}) - \boldsymbol{\rho})$ and $\mathbf{b} \triangleq \mathbf{C}\mathbf{D}\mathbf{d}_{k-1}$ where $\mathbf{d}_{k-1} \sim \mathcal{D}$ and note that variance is translationally invariant allowing us to reintroduce r and set $\sigma^2 = \frac{1}{2}d_{\max}^2$.

Thus, given the structure of the example problem in Section IV we have found values $\delta = \frac{5}{3}d_{\max}$ and $\sigma^2 = \frac{d_{\max}^2}{2}$ which satisfy the conditions of Thm. 3.

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, Jan. 2019.

[3] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017.

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

[5] Code *Repository for this work:*. https://github.com/rkcosner/freedman.git.

[6] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, 2008.

[7] M. Fränzle, E. M. Hahn, H. Hermanns, N. Wolovick, and L. Zhang, "Measurability and safety verification for stochastic hybrid systems," 2011. 14th Conference on Hybrid systems: computation and control.

[8] M. P. Chapman, R. Bonalli, K. M. Smith, I. Yang, M. Pavone, and C. J. Tomlin, "Risk-sensitive safety analysis using conditional value-at-risk," *IEEE Transactions on Automatic Control*, vol. 67, 2021.

[9] L. Lindemann, N. Matni, and G. J. Pappas, "Stl robustness risk over discrete-time stochastic processes," in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 1329–1335, IEEE, 2021.

[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] 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.

[12] O. So, A. Clark, and C. Fan, "Almost-sure safety guarantees of stochastic zero-control barrier functions do not hold," 2023. arXiv:2312.02430.

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

[14] H. Kushner, "Stochastic Stability and Control.," 1967. Academic Press.

[15] S. Prajna, A. Jadbabaie, and G. J. Pappas, "Stochastic safety verification using barrier certificates," in *2004 43rd IEEE conference on decision and control (CDC)*, vol. 1, pp. 929–934, IEEE, 2004.

[16] R. Cosner, P. Culbertson, A. Taylor, and A. Ames, "Robust Safety under Stochastic Uncertainty with Discrete-Time Control Barrier Functions," in *Proceedings of Robotics: Science and Systems*, 2023.

[17] C. Santoyo, M. Dutreix, and S. Coogan, "Verification and control for finite-time safety of stochastic systems via barrier functions," in *IEEE Conference on Control Technology and Applications (CCTA)*, 2019.

[18] 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," in *2023 62nd IEEE Conference on Decision and Control (CDC)*, pp. 3073–3080, 2023.

[19] 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.

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

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

[22] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots," *The international journal of robotics research*, 1986.

[23] 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*, July 2017.

[24] J. Breeden, K. Garg, and D. Panagou, "Control Barrier Functions in Sampled-Data Systems," *IEEE Control Systems Letters*, vol. 6, pp. 367–372, 2022. Conference Name: IEEE Control Systems Letters.

[25] 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.

[26] 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 Conference on Decision and Control (CDC)*.

[27] P. Culbertson, R. K. Cosner, M. Tucker, and A. D. Ames, "Input-to-State Stability in Probability," 2023. IEEE Conference on Decision and Control (CDC).

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

[29] X. Fan, I. Grama, and Q. Liu, "Hoeffding's inequality for supermartingales," *Stochastic Processes and their Applications*, 2012.

[30] R. K. Cosner, P. Culbertson, and A. D. Ames. Extended version of this paper: https://arxiv.org/pdf/2403.05745.pdf.

[31] X. Xiong and A. Ames, "3-d underactuated bipedal walking via h-lip based gait synthesis and stepping stabilization," *IEEE Transactions on Robotics*, vol. 38, no. 4, pp. 2405–2425, 2022.

[32] J. Tropp, "Freedman's inequality for matrix martingales," *Electronic Communications in Probability*, vol. 16, no. none, pp. 262 – 270, 2011.

[33] T. Popoviciu, "Sur les équations algébriques ayant toutes leurs racines réelles," *Mathematica*, vol. 9, no. 129-145, p. 20, 1935.