Graphical Abstract

Finite-time Safety and Reach-avoid Verification of Stochastic Discrete-time Systems

Bai Xue

This paper studies finite-time safety and reach-avoid verification for stochastic discrete-time dynamical systems. The aim is to ascertain lower and upper bounds of the probability that, within a predefined finite-time horizon, a system starting from an initial state in a safe set will either exit the safe set (safety verification) or reach a target set while remaining within the safe set until the first encounter with the target (reach-avoid verification). We introduce novel barrier-like sufficient conditions for characterizing these bounds, which either complement existing ones or fill gaps. Finally, we demonstrate the efficacy of these conditions on two simple examples.

Highlights

Finite-time Safety and Reach-avoid Verification of Stochastic Discrete-time Systems

Bai Xue

- This work studies the finite-time safety and reach-avoid verification of stochastic discrete-time systems. Compared with existing works, which merely offered upper bounds on the relevant probabilities, this work goes beyond by providing both lower and upper bounds. These bounds deepen our understanding of the system's characteristics and yield a more accurate estimation of the true probability, thus enhancing the overall rigour and precision of the finite-time safety and reach-avoid analysis.
- The proposed barrier-like conditions for upper bounding the probabilities complement existing ones, facilitating the gain of sharper upper bounds for some systems.
- Unlike the approach in [38], our proposed barrier-like conditions for bounding probabilities in finite-time safety verification eliminate the need for the strong invariance assumption. Additionally, this work extends these barrier-like conditions to finite-time reach-avoid verification, providing both lower and upper probability bounds.

Finite-time Safety and Reach-avoid Verification of Stochastic Discrete-time Systems

Bai Xue

[a]*Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China, 100190, China*
Email: xuebai@ios.ac.cn

Abstract

This paper studies finite-time safety and reach-avoid verification for stochastic discrete-time dynamical systems. The aim is to ascertain lower and upper bounds of the probability that, within a predefined finite-time horizon, a system starting from an initial state in a safe set will either exit the safe set (safety verification) or reach a target set while remaining within the safe set until the first encounter with the target (reach-avoid verification). We introduce novel barrier-like sufficient conditions for characterizing these bounds, which either complement existing ones or fill gaps. Finally, we demonstrate the efficacy of these conditions on two simple examples.

Keywords: Stochastic Discrete-time Systems, Finite-time Safety Verification, Finite-time Reach-avoid Verification, Barrier-like Conditions, Lower and Upper Probability Bounds

1. Introduction

Temporal verification plays a pivotal role in modern systems analysis, especially in the realm of complex systems where temporal behavior holds utmost significance [25]. It entails a rigorous scrutiny of a system's compliance with temporal properties, including safety and reach-avoid guarantees, to ensure desired outcomes while circumventing undesirable events. Formal methods such as model checking [10, 3] and theorem proving [19] serve as indispensable tools in this endeavor, enabling precise and thorough analysis of temporal specifications.

Barrier certificates were initially proposed for deterministic systems as a popular formal approach to temporal verification in [23]. They offer Lyapunov-like assurances regarding system behavior, with the mere existence of a barrier function being sufficient to establish the satisfiability of safety and/or reachability specifications in [25]. Subsequent efforts have focused on adapting and enhancing deterministic barrier functions, as well as broadening their applications [4, 29, 35]. However, many real-world applications are susceptible to stochastic disturbances and are thus modeled as stochastic systems. In the stochastic setting, safety verification over the infinite time horizon via barrier certificates was introduced alongside its deterministic counterpart in [24]. Utilizing Ville's Inequality [30], [24] constructed a non-negative barrier function and provided a sufficient condition for upper bounding the probability of eventually entering an unsafe region from a given initial state while remaining within a state constraint set. More recently, a new barrier function, constructed by relaxing a set of equations, was proposed for lower bounding the probability of eventually entering an unsafe or desired region from an initial state while adhering to state constraints in [34, 36]. These barrier functions were further extended to determine the lower and upper bounds of the safety probability over the infinite time horizon for a specified safe set and set of initial states in [37]. Furthermore, by formulating barrier certificates via a relaxation of Bellman equations, [33] established necessary and sufficient conditions for lower and upper bounds the safety and reach-avoid probabilities of stochastic discrete-time systems over the infinite time horizon. In addition, under the assumption that a robust invariant set exists and the system evolves within this robust invariant set, [39] proposed a new barrier certificate, termed reach-avoid supermartingale, to guarantee satisfaction of reach-avoid specifications as well as facilitate reach-avoid controllers. Barrier certificates have also been extended to infinite-time horizon probabilistic program analysis, where they verify properties such as (positive) almost-sure termination, probabilistic termination, assertion violations, and reachability (e.g., [6, 21, 22, 15, 9, 7, 18, 32, 28]). Specially, the probabilistic termination analysis discussed in [9, 7, 18] exhibits interesting connections with classical analysis for stochastic discrete-time systems. When seeking a lower bound for termination probability, this analysis shares conceptual similarities with classical reach-avoid analysis. This connection arises because the termination probability essentially measures the likelihood that a program, beginning from a specific initial state, will eventually reach terminal states while preserving a stochastic invariant set throughout its execution prior to

termination. Conversely, the probabilistic termination analysis presented in [18], which focuses on establishing upper bounds for termination probability, parallels classical safety analysis in stochastic discrete-time systems. In this case, the termination probability represents the chance that a program will eventually violate (escape from) a stochastic invariant set (which excludes the terminal state) when starting from a given initial state. Moreover, the application of barrier certificates has been expanded to encompass both qualitative and quantitative analysis of ω-regular properties [11, 1, 2, 12].

On the other hand, finite-time temporal verification holds greater practical significance as most real-world systems operate within well-defined time constraints. Drawing inspiration from [17], the concept of a c-martingale was introduced in [27] for stochastic continuous-time systems modelled by stochastic differential equations, enabling a controlled increase in the expected certificate value at each time step and offering an upper bound on the exit probability of leaving safe sets within bounded time horizons. Afterwards, [20] proposed a computational method to find a c-martingale expressed by neural networks for finite-time safety verification of stochastic discrete-time systems. The c-martingales in [20] are a typical case of the proposed barrier function in the present work. Under the assumption that the system evolves within a robust invariant set, [13] extended the c-martingale framework to address temporal logic verification for discrete-time systems, and later, [14] synthesized control policies for discrete-time stochastic control systems together with a lower bound on the probability that the systems satisfy complex temporal properties. [26] utilized barrier-like results introduced in [17] to address the challenges of finite-time safety verification and the synthesis of safe controllers for stochastic discrete-time systems, employing semi-definite programming techniques. The detailed description of the verification problem in [26] and its relationship with the verification problem are illustrated in Remark 3. On the other hand, the aforementioned works on finite-time temporal verification offer only upper bounds of the probability of reaching undesirable sets (equivalently, lower bounds of the probability of staying within desirable sets). Such works do not provide the lower bounds. This work will offer both types of bounds. Recent work by [38] introduced barrier functions for bounding probabilistic safety (lower and upper bounds) across infinite and finite time horizons. Its analysis, similar to [13, 14], relies on the assumption that system evolution remains within a robust invariant set. However, as critically examined in [37], this strong invariance requirement constitutes a significant limitation. In contrast, the current work de-

velops new barrier functions that eliminate the need for such a restrictive assumption. Similar to the infinite-time case, barrier certificates have also been extended to the analysis of probabilistic programs within bounded time horizons (e.g., [9, 16, 8]). [9] (e.g., Lemma 3) presented a sufficient condition based on an ϵ-repulsing supermartingale supported by a pure invariant, utilizing Azuma's and Hoeffding's inequalities to derive an upper bound for programs that reach a specified set exactly at a given step. Afterward, in the context where programs terminate almost surely, [16] proposed a sufficient condition for establishing lower bounds on program termination within bounded time horizons; [31] developed lower and upper bounds for the tail bound problem which can also be employed to bound the probability that programs terminate within bounded time horizons. Recently, in conjunction with stochastic invariants [9], [8] investigated the tail bound problem for programs that do not necessarily terminate almost surely. This approach can also be employed to establish lower bounds on the probability that programs terminate within bounded time horizons.

This paper investigates the finite-time safety and reach-avoid verification of stochastic discrete-time systems. The finite-time safety verification problem aims to compute both lower and upper bounds of the probability that a system, starting from an initial state in a safe set, will exit the safe set throughout a given bounded time interval. From a reachability perspective, it involves computing lower and upper bounds on the probability of reaching the complement of the safe set within the specified bounded time interval. Thus, it exclusively addresses safety or reachability concerns. In contrast, finite-time reach-avoid verification integrates guarantees of safety and reachability. It seeks to establish lower and upper bounds on the probability that a system, starting from an initial state in a safe set, will reach a target set within a designated bounded time interval while ensuring it remains within the safe set before reaching the target set. Although these two problems are interconnected, they differ fundamentally in essence, as we will elaborate on in the preliminaries section. We propose novel barrier-like conditions to address these two problems. These conditions either complement existing ones or fill gaps, facilitating the attainment of tight probability bounds for some systems. Finally, we demonstrate the effectiveness of the proposed conditions on two numerical examples, utilizing semi-definite programming tools.

The main contributions of this work are summarized below.

1. This work studies the finite-time safety and reach-avoid verification

of stochastic discrete-time systems. Compared with existing works [26, 20, 17], which merely offered upper bounds on the relevant probabilities, our contribution goes beyond by providing both lower and upper bounds. These bounds deepen our understanding of the system's characteristics and yield a more accurate estimation of the true probability, thus enhancing the overall rigour and precision of the finite-time safety and reach-avoid analysis. In addition, obtaining both lower and upper bounds also facilitates evaluating their mutual tightness in practice.

2. The proposed barrier-like conditions for upper bounding the probabilities complement existing ones in [20, 17], facilitating the gain of sharper upper bounds for some systems.
3. Unlike the approach in [38], our proposed barrier-like conditions for bounding probabilities in finite-time safety verification eliminate the need for the strong invariance assumption. Additionally, this work extends these barrier-like conditions to finite-time reach-avoid verification, providing both lower and upper probability bounds.

This paper is structured as follows: in Section 2, we formulate the finite-time safety and reach-avoid verification problems. In Sections 3 and 4, we introduce our barrier-like conditions for addressing these two problems, respectively. After demonstrating the performance of proposed conditions on two examples in Section 5, we conclude this paper in Section 6.

2. Preliminaries

We start the exposition by a formal introduction of discrete-time systems subject to stochastic disturbances and finite-time safety/reach-avoid verification problems of interest. Before posing the problem studied, let me introduce some basic notions used throughout this paper: $\mathbb{R}$ denotes the set of real values; $\mathbb{N}$ denotes the set of nonnegative integers; $\mathbb{N}_{\leq k}$ is the set of nonnegative integers being less than or equal to k; for sets Δ_1 and Δ_2, $\Delta_1 \setminus \Delta_2$ denotes the difference of sets Δ_1 and Δ_2, which is the set of all elements in Δ_1 that are not in Δ_2; $1_A(\boldsymbol{x})$ denotes the indicator function in the set A, where, if $\boldsymbol{x} \in A$, then $1_A(\boldsymbol{x}) = 1$ and if $\boldsymbol{x} \notin A$, $1_A(\boldsymbol{x}) = 0$.

This paper considers stochastic discrete-time systems that are modeled by stochastic difference equations of the following form:

$$\boldsymbol{x}(l+1) = \boldsymbol{f}(\boldsymbol{x}(l), \boldsymbol{\theta}(l)), \forall l \in \mathbb{N}, \tag{1}$$

where $\boldsymbol{x}(l) \in \mathbb{R}^n$ is the state at time l and $\boldsymbol{\theta}(l) \in \Theta$ with $\Theta \subseteq \mathbb{R}^m$ is the stochastic disturbance at time l. In addition, let $\boldsymbol{\theta}(0), \boldsymbol{\theta}(1), \ldots$ be i.i.d. (independent and identically distributed) random vectors on a probability space $(\Theta, \mathcal{F}, \mathbb{P})$, and take values in Θ with the following probability distribution: for any measurable set $B \subseteq \Theta$,

$$\text{Prob}(\boldsymbol{\theta}(l) \in B) = \mathbb{P}(B), \quad \forall l \in \mathbb{N}.$$

The expectation $\mathbb{E}[\cdot]$ is defined with respect to the probability measure $\mathbb{P}$.

Before defining trajectories of system (1), we define a disturbance signal.

Definition 1. *A disturbance signal π is a sample path of the stochastic process $\{\boldsymbol{\theta}(i)\colon \Theta \to \Theta, i \in \mathbb{N}\}$, which is defined on the canonical sample space Θ^∞, endowed with its product topology $\mathcal{B}(\Theta^\infty)$, with the probability measure $\mathbb{P}^\infty$. The expectation associated with the probability measure $\mathbb{P}^\infty$ is denoted by $\mathbb{E}^\infty[\cdot]$.*

A disturbance signal π together with an initial state $\boldsymbol{x}_0 \in \mathbb{R}^n$ induces a unique discrete-time trajectory as follows.

Definition 2. *Given a disturbance signal π and an initial state $\boldsymbol{x}_0 \in \mathbb{R}^n$, a trajectory of system (1) is denoted as $\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(\cdot)\colon \mathbb{N} \to \mathbb{R}^n$ with $\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(0) = \boldsymbol{x}_0$, i.e., $\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l+1) = \boldsymbol{f}(\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l), \boldsymbol{\theta}(l)), \forall l \in \mathbb{N}$.*

In this study, we address two verification problems for the system governed by (1) with a finite time horizon $[0, N]$, where $N \in \mathbb{N}$. The first problem pertains to a finite-time safety verification problem, examining the likelihood of the system exiting the safe set $\mathcal{X}$ throughout its evolution over $[0, N]$, starting from $\boldsymbol{x}_0 \subseteq \mathcal{X}$. The second one involves a finite-time reach-avoid task, focusing on the probability that the system enters the target set $\mathcal{X}_r \subset \mathcal{X}$ safely within the time horizon $[0, N]$, given an initial state $\boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r$.

Problem 1 (Finite-time Safety Verification)**.** *Given a finite time interval $[0, N]$ with $N \in \mathbb{N}$, a safe set $\mathcal{X}$, and an initial state $\boldsymbol{x}_0 \in \mathcal{X}$, the finite-time safety verification problem is to compute $\epsilon_1 \in [0, 1]$ and $\epsilon_2 \in [0, 1]$ which are respectively the lower and upper bounds of the exit probability, with which system (1) starting from $\boldsymbol{x}_0$ will exit the safe set $\mathcal{X}$ within $[0, N]$, i.e.,*

$$\epsilon_1 \leq \mathbb{P}^\infty \left(\exists k \in \mathbb{N}_{\leq N}. \boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \notin \mathcal{X} \middle| \boldsymbol{x}_0 \in \mathcal{X} \right) \leq \epsilon_2.$$

Problem 2 (Finite-time Reach-avoid Verification)**.** *Given a finite time interval* $[0, N]$ *with* $N \in \mathbb{N}$*, a safe set* $\mathcal{X}$*, a target set* $\mathcal{X}_r \subseteq \mathcal{X}$*, and an initial state* $\boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r$*, the finite-time reach-avoid verification problem is to compute* $\epsilon_1 \in [0, 1]$ *and* $\epsilon_2 \in [0, 1]$ *which are respectively the lower and upper bounds of the reach-avoid probability, with which system* (1) *starting from* $\boldsymbol{x}_0$ *will enter the target set* $\mathcal{X}_r$ *within* $[0, N]$ *while staying inside the set* $\mathcal{X}$ *before the first target hitting time, i.e.,*

$$\epsilon_1 \leq \mathbb{P}^{\infty}\left(\begin{matrix}\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \\ \wedge\, \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(l) \in \mathcal{X}\end{matrix}\middle| \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\right) \leq \epsilon_2.$$

Like stochastic barrier functions based methods, which formulate sufficient conditions for mainly computing upper bounds of the probability of reaching unsafe sets eventually, we in this paper will propose barrier-like conditions for addressing Problem 1 and 2.

It is noteworthy to mention that by treating system (1) within an extended domain $\widehat{\mathcal{X}}$, which includes the safe set $\mathcal{X}$ and all one-step reachable states from $\mathcal{X}$, and interpreting $\widehat{\mathcal{X}} \setminus \mathcal{X}$ as a target region as shown in the sequel, the conditions derived for Problem 2 can be adapted to tackle Problem 1 since $\mathbb{P}^{\infty}(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \notin \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}) = \mathbb{P}^{\infty}(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widehat{\mathcal{X}} \setminus \mathcal{X} \wedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(l) \in \widehat{\mathcal{X}} \mid \boldsymbol{x}_0 \in \mathcal{X})$. However, Problem 1 and 2 are different. From a reachability perspective, the discrepancy arises from whether the target set is contained within the safe set $\mathcal{X}$ or not. When the target set is outside the safe set, as in the safety verification problem in Problem 1, reaching the target set $\widehat{\mathcal{X}} \setminus \mathcal{X}$ is equivalent to exiting the safe set $\mathcal{X}$. However, this does not hold for the reach-avoid problem in Problem 2. Consequently, the conditions derived for Problem 2 should be refined to address Problem 1. Thus, to underscore the improvements and maintain clarity, we treat these problems as separate entities in this paper.

3. Finite-time Safety Verification

In this section, we present our sufficient conditions for characterizing upper and lower bounds on the probability in Problem 1. The sufficient condition for lower bounds is formulated in Subsection 3.1 and the one for upper bounds is introduced in Subsection 3.2.

In accordance with the methodology in [37], we define a switched system that is constructed by freezing the dynamics of system (1) upon exiting the

safe set $\mathcal{X}$. This switched system will facilitate the construction of sufficient conditions for lower and upper bounding the exit probability in the sequel.

Definition 3. *The switched stochastic discrete-time system, which is built upon system* (1)*, is a quadruple* $(\widetilde{\mathcal{L}}, \widetilde{\mathcal{X}}, \boldsymbol{x}_0, \widetilde{\boldsymbol{f}})$ *with the following components:*

- $\widetilde{\mathcal{L}} = \{1, 2\}$ *is a set of two locations;*
- $\widetilde{\mathcal{X}} \subseteq \mathbb{R}^n$ *is the state constraint set;*
- $\boldsymbol{x}_0 \in \widetilde{\mathcal{X}}$ *is the initial state;*
- $\widetilde{\boldsymbol{f}}(\cdot,\cdot)\colon \mathbb{R}^n \times \Theta \to \mathbb{R}^n$*, where*

$$\widetilde{\boldsymbol{f}}(\boldsymbol{x}, \boldsymbol{\theta}) = \sum_{i=1}^{2} 1_{\widetilde{\mathcal{X}}_i}(\boldsymbol{x}) \widetilde{\boldsymbol{f}}_i(\boldsymbol{x}, \boldsymbol{\theta})$$

with $\widetilde{\boldsymbol{f}}_1(\boldsymbol{x}, \boldsymbol{\theta}) = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})$ *and* $\widetilde{\boldsymbol{f}}_2(\boldsymbol{x}, \boldsymbol{\theta}) = \boldsymbol{x}$*, and* $1_{\widetilde{\mathcal{X}}_i}(\boldsymbol{x})$ *is the indicator function of the set* $\widetilde{\mathcal{X}}_i$*, i.e.,* $1_{\widetilde{\mathcal{X}}_i}(\boldsymbol{x}) = 1$ *if* $\boldsymbol{x} \in \widetilde{\mathcal{X}}_i$*; otherwise,* $1_{\widetilde{\mathcal{X}}_i}(\boldsymbol{x}) = 0$*,*

where

1. $\widetilde{\mathcal{X}}$ *is a set satisfying* $\widetilde{\Omega} \subset \widetilde{\mathcal{X}}$*, where* $\widetilde{\Omega}$ *is the union of* $\mathcal{X}$ *and all reachable states starting from* $\mathcal{X}$ *in one step, i.e.,*

$$\widetilde{\Omega} = \{\boldsymbol{x}' \in \mathbb{R}^n \mid \boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta}), \boldsymbol{x} \in \mathcal{X}, \boldsymbol{\theta} \in \Theta\} \cup \mathcal{X};$$

2. $\widetilde{\mathcal{X}}_1 = \mathcal{X}$*;*
3. $\widetilde{\mathcal{X}}_2 = \widetilde{\mathcal{X}} \setminus \mathcal{X}$*.*

The evolution of the state of this system is governed by the iterative map

$$\begin{aligned} &\boldsymbol{x}(l+1) = \widetilde{\boldsymbol{f}}(\boldsymbol{x}(l), \boldsymbol{\theta}(l)), \forall l \in \mathbb{N}, \\ &\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \widetilde{\mathcal{X}}. \end{aligned} \tag{2}$$

The trajectory of system (2), induced by initial state $\boldsymbol{x}_0 \in \widetilde{\mathcal{X}}$ and disturbance policy π, is denoted by $\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(\cdot)\colon \mathbb{N} \to \mathbb{R}^n$.

It is observed that if system (1) starting from $\boldsymbol{x}_0 \in \mathcal{X}$ enters the set $\widetilde{\mathcal{X}} \setminus \mathcal{X}$ initially at time $i \in \mathbb{N}$, system (2) starting from $\boldsymbol{x}_0 \in \mathcal{X}$ will also enter it for the first time at this time instant, and vice versa. Furthermore, when system (2) transitions into the set $\widetilde{\mathcal{X}} \setminus \mathcal{X}$, it remains there indefinitely. Thus, the set $\widetilde{\mathcal{X}}$ is a robust invariant for system (2) [37], that is, trajectories of system (2) originating from the set $\widetilde{\mathcal{X}}$ will never leave it. Consequently, the probability of system (2) entering $\widetilde{\mathcal{X}} \setminus \mathcal{X}$ at time $t = i$ is equal to the probability of system (1) entering this set up to time $t = i$.

Lemma 1. *For* $i \in \mathbb{N}$, $\mathbb{P}^{\infty}(\exists k \in \mathbb{N}_{\leq i}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}) = \mathbb{P}^{\infty}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(i) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X})$. *Thus,* $\mathbb{P}^{\infty}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(i) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}) \leq \mathbb{P}^{\infty}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(j) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X})$ *if* $i \leq j$.

3.1. Sufficient Conditions for Upper Bounds

In this subsection, we present our sufficient condition for upper bounding the probability of exiting the safe set $\mathcal{X}$ over the time horizon $[0, N]$ in Problem 1.

The sufficient condition requires the existence of a non-negative function $v(\boldsymbol{x}) : \widetilde{\mathcal{X}} \to \mathbb{R}$ defined on the set $\widetilde{\mathcal{X}}$ that satisfies two key properties: (1) it must be greater than or equal to one on the subset $\widetilde{\mathcal{X}} \setminus \mathcal{X}$, and (2) its α-scaled expected value at the next step along the system dynamics described in (1) should not increase by more than $\alpha\beta$ relative to its current value for $\boldsymbol{x} \in \mathcal{X}$, where $\alpha \in (0, 1]$ and $\beta \in (-\infty, 1]$. The upper bounds derivation proceeds as follows: Lemma 1 establishes that the probability of system (2) entering $\widetilde{\mathcal{X}} \setminus \mathcal{X}$ at time $t = N$ is equal to the probability of system (1) entering this set up to time $t = N$. Then, we derive upper bounds using system (2) by analyzing α and β. Relying on the fact that the system in (2) remains stationary when starting from $\widetilde{\mathcal{X}} \setminus \mathcal{X}$, which implies $\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}$, we reformulate the constraint over the function $v(\boldsymbol{x}) : \widetilde{\mathcal{X}} \to \mathbb{R}$ using system (2), requiring that the α-scaled expected value of $v(\boldsymbol{x})$ at the next step along the system (2) grows by at most $\alpha\beta$ relative to its current value $v(\boldsymbol{x})$ over the whole set $\widetilde{\mathcal{X}}$ when $\alpha \in (0, 1]$ and $\beta\alpha - (\alpha - 1) \in [0, 1]$. Upper bounds follow from recursive application of this reformulated constraint; when $\alpha \in (0, 1]$ and $\beta\alpha - (\alpha - 1) \in (-\infty, 0)$, the constraint is modified to require that the expected value of $v(\boldsymbol{x})$ at the next step along the system (2) grows by at most β, relative to the $(1-\beta)$-weighted current value $v(\boldsymbol{x})$. The upper bound again emerges through recursive application of this reformulated constraint.

Theorem 1. *If there exist a function* $v(\boldsymbol{x})\colon \widetilde{\mathcal{X}} \to \mathbb{R}$, *and* $\alpha \in (0, 1]$ *and* $\beta \in (-\infty, 1]$ *such that*

$$\begin{cases} \mathbb{E}^{\infty}[v(\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \\ v(\boldsymbol{x}) \geq 0, & \forall \boldsymbol{x} \in \mathcal{X}, \end{cases} \tag{3}$$

then $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) = \mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in$

$\mathcal{X}) \leq$

$$\begin{cases} v(\boldsymbol{x}_0) + \beta N, & \text{if } \alpha = 1 \wedge \gamma \in [0,1], \\ v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha-1}, & \text{if } \alpha \in (0,1) \wedge \gamma \in [0,1], \\ 1 - (1 - v(\boldsymbol{x}_0))(1-\beta)^N, & \text{if } \alpha \in (0,1] \wedge \gamma \in (-\infty, 0), \end{cases}$$

where $\gamma = \beta\alpha - (\alpha - 1)$.

Proof. 1) We first prove the case of $\alpha \in (0,1) \wedge \gamma \in [0,1]$.

Since $\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}$, we can obtain

$$\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] - \frac{1}{\alpha}v(\boldsymbol{x}) = (1 - \frac{1}{\alpha})v(\boldsymbol{x}), \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}.$$

Therefore,

$$\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] - \frac{1}{\alpha}v(\boldsymbol{x}) \leq \beta, \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X},$$

which can be justified based on the facts that $v(\boldsymbol{x}) \geq 1$ for $\boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}$, $\alpha \in (0,1)$ and $\gamma \in [0,1]$. Therefore, if $v(\boldsymbol{x})$ satisfies (3), it will satisfy

$$\begin{cases} \mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}, \\ v(\boldsymbol{x}) \geq 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\boldsymbol{x}), & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}. \end{cases} \tag{4}$$

According to (4), we have

$$\begin{aligned} & v(\boldsymbol{x}_0) \geq 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\boldsymbol{x}_0), \\ & \alpha^{-1}v(\boldsymbol{x}_0) + \beta \geq \mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))] \geq \mathbb{E}^{\infty}[1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))], \\ & \ldots, \\ & \alpha^{-N}v(\boldsymbol{x}_0) + \beta \sum_{i=0}^{N-1} \alpha^{-i} \geq \mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))] \geq \mathbb{E}^{\infty}[1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))]. \end{aligned}$$

Therefore, $\mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) = \mathbb{E}^{\infty}[1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))] \leq \alpha^{-N}v(\boldsymbol{x}_0) + \alpha\beta\frac{(1-\alpha^{-N})}{\alpha-1}$. According to Lemma 1, we have the conclusion.

2) The conclusion for the case of $\alpha = 1 \wedge \gamma \in [0,1]$ can be justified via following the proof of the above one.

3) We will show the case of $\alpha \in (0,1] \wedge \gamma \in (-\infty, 0)$.

Since $\beta < 1 - \frac{1}{\alpha}$, thus $\frac{1}{\alpha} < 1 - \beta$. Consequently, $1 - \beta > 0$. Thus, we conclude that if $v(\boldsymbol{x})$ satisfies (3), it will satisfy

$$\begin{cases} \mathbb{E}^{\infty}[v(\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1))] \leq v(\boldsymbol{x})(1-\beta) + \beta, & \forall \boldsymbol{x} \in \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \\ v(\boldsymbol{x}) \geq 0, & \forall \boldsymbol{x} \in \mathcal{X}, \end{cases}$$

and thus it satisfies

$$\begin{cases} \mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] \leq (1-\beta)v(\boldsymbol{x}) + \beta, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}, \\ v(\boldsymbol{x}) \geq 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\boldsymbol{x}), & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}. \end{cases}$$

Therefore, following the proof for the case $\alpha \in (0, 1] \wedge \gamma \in [0, 1]$, we will have the conclusion.

The proof is completed. □

In Theorem 1, the parameter β is practically constrained to be less than or equal to one. This restriction is necessary to ensure the practical utility of the upper bounds $v(\boldsymbol{x}_0) + \beta N$ and $v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha-1}$. Assigning a value greater than one to β would lead to these two bounds exceeding unity when $N \geq 1$, rendering them ineffective.

If $\alpha = 1$ and $\beta = 0$, Theorem 1 is equivalent to Proposition 3 in [37], which formulates a sufficient condition for determining an upper bound of the probability of exiting the safe set $\mathcal{X}$ eventually (i.e., $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big)$). The upper bound is $v(\boldsymbol{x}_0)$, which is also an upper bound of the exit probability $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big)$. On the other hand, when $\alpha \in (0, 1)$ and $\gamma \in (-\infty, 0)$, if $v(\boldsymbol{x}_0) < 1$, $\lim_{N \to +\infty} 1 - (1 - v(\boldsymbol{x}_0))(1-\beta)^N = -\infty$ holds, implying $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) = 0$ and $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) = 0$.

Theorem 1 extends the conclusion drawn in [17], as it allows for a value of α within the interval $(0, 1)$, in contrast to the requirement of $\alpha \geq 1$ in the cited work. For convenience of reference, we present the related result in [17] here, which corresponds to Theorem 3 in Chapter 3 in [17].

Proposition 1. *If there exists a continuous nonnegative function* $v(\cdot) : \widetilde{\mathcal{X}} \to$

$\mathbb{R}$ *satisfying*

$$\begin{cases} v(\boldsymbol{x}_0) < 1, & \\ \mathbb{E}^{\infty}[v(\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \\ v(\boldsymbol{x}) \geq 0, & \forall \boldsymbol{x} \in \mathcal{X}, \end{cases} \tag{5}$$

where $\alpha \geq 1$ *and* $\beta \geq 0$*, then* $\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) \leq$

$$\begin{cases} 1 - (1 - v(\boldsymbol{x}_0))(1-\beta)^N, & \text{if } \alpha > 1 \wedge \gamma \in (-\infty, 0], \\ v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha - 1}, & \text{if } \alpha > 1 \wedge \gamma \in (0, \infty), \\ v(\boldsymbol{x}_0) + \beta N, & \text{if } \alpha = 1 \wedge \gamma \in (0, \infty), \end{cases}$$

where $\gamma = \alpha\beta - (\alpha - 1)$*.*

Since $\boldsymbol{x}_0 \in \{\boldsymbol{x} \in \widetilde{\mathcal{X}} \mid v(\boldsymbol{x}) < 1\}$ and $\widetilde{\mathcal{X}} \setminus \mathcal{X} \subseteq \{\boldsymbol{x} \in \widetilde{\mathcal{X}} \mid v(\boldsymbol{x}) \geq 1\}$, according to Theorem 3 in Chapter 3 in [17], the above statement holds. Similarly, the parameter β in (5) should be less than or equal to one. When $\gamma \leq 0$ and $\alpha > 1$, $\beta \leq 1 - \frac{1}{\alpha}$ holds and thus $\beta \leq 1$ holds. For the case with $\gamma > 0$, when $\beta > 1$ and $N \geq 1$, $v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha-1} > 1$ and $v(\boldsymbol{x}_0) + \beta N > 1$ hold, which are ineffective upper bounds.

When comparing constraints (3) and (5), it becomes apparent that if there exists a function $v(\boldsymbol{x})$ along with $\alpha > 1$ and $\beta \in [0, 1]$ satisfying (5), the same function $v(\boldsymbol{x})$ with $\frac{1}{\alpha}$ and $\beta \in [0, 1]$ will satisfy (3). In addition, it is observed that the barrier function in [20], referred to as c-martingales, is just a function that satisfies constraint (3) with $\alpha = 1$ and $\beta \geq 0$.

3.2. Sufficient Conditions for Lower Bounds

In this subsection, we present our sufficient condition for lower bounding the probability of exiting the safe set over the time horizon $[0, N]$ in Problem 1, which is inspired by [34, 36].

The sufficient condition requires the existence of a function $v(\boldsymbol{x})$ defined on the set $\widetilde{\mathcal{X}}$ that satisfies three key properties: (1) it admits a finite upper bound over $\widetilde{\mathcal{X}}$, (2) it is less than or equal to one on the subset $\widetilde{\mathcal{X}} \setminus \mathcal{X}$, and (3) its expected value at the next step along the system dynamics described in (1) increases over its α-scaled current value by more than β for $\boldsymbol{x} \in \mathcal{X}$, where $\alpha \in [1, \infty)$, and $\beta \in (1-\alpha, \infty)$. The lower bounds derivation proceeds as follows: Lemma 1 establishes that the probability of system (2) entering

$\widetilde{\mathcal{X}} \setminus \mathcal{X}$ at time $t = N$ is equal to the probability of system (1) entering this set up to time $t = N$. Then, we derive the lower bounds using system (2) by analyzing α. Relying on the fact that the system in (2) remains stationary when starting from $\widetilde{\mathcal{X}} \setminus \mathcal{X}$, which implies $\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}$, and noting that $v(\boldsymbol{x})$ is less than or equal to one on this subset, we reformulate the constraint on $v(\boldsymbol{x})$. Specifically, using system (2), we require that the expected value of $v(\boldsymbol{x})$ at the next step grows at least by $\beta - (\alpha - 1 + \beta)1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(\boldsymbol{x})$ over its α-scaled current value $v(\boldsymbol{x})$, for all $\boldsymbol{x} \in \widetilde{\mathcal{X}}$. For $\alpha > 1$ and $\alpha = 1$, the lower bounds are subsequently obtained through recursive application of the reformulated constraint, in conjunction with the upper bound on the function $v(\boldsymbol{x}) : \widetilde{\mathcal{X}} \to \mathbb{R}$.

Theorem 2. *If there exist a function* $v(\boldsymbol{x})\colon \widetilde{\mathcal{X}} \to \mathbb{R}$ *with* $\sup_{\boldsymbol{x}\in\widetilde{\mathcal{X}}} v(\boldsymbol{x}) \leq M$*,* $\alpha \in [1, \infty)$*, and* $\beta \in (1 - \alpha, \infty)$ *such that*

$$\begin{cases} \beta + \alpha v(\boldsymbol{x}) \leq \mathbb{E}^{\infty}[v(\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1))], & \forall \boldsymbol{x} \in \mathcal{X}, \\ v(\boldsymbol{x}) \leq 1, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases} \tag{6}$$

then $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) = \mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) \geq$

$$\begin{cases} \frac{(\alpha^{N+1}v(\boldsymbol{x}_0)-M)(\alpha-1)+\beta(\alpha^{N+1}-1)}{(\alpha+\beta-1)(\alpha^{N+1}-1)}, & \text{if } \alpha > 1, \\ 1 + \frac{v(\boldsymbol{x}_0)-M}{\beta(N+1)}, & \text{if } \alpha = 1. \end{cases}$$

Proof. 1) We first prove the case of $\alpha > 1$.

Since $\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}$, we conclude that if $v(\boldsymbol{x})$ satisfies (6), it will satisfy

$$(\alpha - 1 + \beta)1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(\boldsymbol{x}) + \mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] \geq \alpha v(\boldsymbol{x}) + \beta, \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}.$$

Consequently, for $\boldsymbol{x}_0 \in \mathcal{X}$, we have

$$\begin{aligned} &\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))] - \alpha v(\boldsymbol{x}_0) \geq \beta + (1 - \alpha - \beta)1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(\boldsymbol{x}_0), \\ &\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(2))] - \alpha\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))] \geq \beta + (1 - \alpha - \beta)\mathbb{E}^{\infty}[1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))], \\ &\dots, \\ &\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N+1))] - \alpha\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))] \geq \beta + (1 - \alpha - \beta)\mathbb{E}^{\infty}[1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))]. \end{aligned}$$

Thus, we obtain

$$\begin{aligned}
&\mathbb{E}^{\infty}[v(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N+1))] - \alpha^{N+1} v(\boldsymbol{x}_0) \\
&\geq \beta \sum_{i=0}^{N} \alpha^i + (1-\alpha-\beta) \sum_{i=0}^{N} \alpha^{N-i} \mathbb{E}^{\infty}[1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(i))] \\
&\geq \beta \frac{1-\alpha^{N+1}}{1-\alpha} + (1-\alpha-\beta) \frac{1-\alpha^{N+1}}{1-\alpha} \times \mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big)
\end{aligned}.$$

The last inequality is obtained according to Lemma 1, which states $\mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) \geq \mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(i) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big)$ for $i \leq N$, and the fact that $1-\alpha-\beta < 0$.

Consequently,

$$\mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) \geq \frac{(\alpha^{N+1} v(\boldsymbol{x}_0) - M)(\alpha - 1) + \beta(\alpha^{N+1} - 1)}{(\alpha + \beta - 1)(\alpha^{N+1} - 1)}.$$

2) The conclusion for the case of $\alpha = 1$ can be justified via following the proof of the above one.

The proof is completed. □

It is worth noting here that if there exists a bounded function $v(\boldsymbol{x})\colon \widetilde{\mathcal{X}} \to \mathbb{R}$ satisfying (6) with $\alpha = 1$, then system (1), starting from $\boldsymbol{x}_0 \in \mathcal{X}$, will exit the safe set $\mathcal{X}$ eventually with the probability of one, since $\lim_{N \to +\infty} 1 + \frac{v(\boldsymbol{x}_0) - M}{\beta(N+1)} = 1$. Therefore, if system (1) does not feature this property, $\alpha = 1$ cannot be used to perform computations.

Remark 1. *When $\alpha = 1$, the constraint $v(\boldsymbol{x}) \leq 1, \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}$ in (6) is redundant and can be removed.*

Remark 2. *One may wonder whether a sufficient condition for lower bounding the probability of exiting the safe set $\mathcal{X}$ over the time horizon $[0, N]$ in Problem 1 can be constructed by directly reversing the sign in constraint (3) in Theorem 1. We will give a brief explanation here that the condition constructed in this manner will consistently yield zero as lower bounds.*

If there exists a function $v(\boldsymbol{x})\colon \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases}
\mathbb{E}^{\infty}[v(\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1))] \geq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \mathcal{X}, \\
v(\boldsymbol{x}) \leq 1, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \\
v(\boldsymbol{x}) \leq 0, & \forall \boldsymbol{x} \in \mathcal{X},
\end{cases} \tag{7}$$

then $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) = \mathbb{P}^{\infty}\big(\widetilde{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\big) \geq$

$$\begin{cases} v(\boldsymbol{x}_0) + \beta N, & \text{if } \alpha = 1 \wedge \gamma \in (-\infty, 0), \\ v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha-1}, & \text{if } \alpha \in (0,1) \wedge \gamma \in (-\infty, 0), \\ 1 - (1 - v(\boldsymbol{x}_0))\alpha^{-N}, & \text{if } \alpha \in (0,1] \wedge \gamma \in [0, \infty), \end{cases}$$

where $\gamma = \beta\alpha - (\alpha - 1)$. *This conclusion can be justified by following the proof of Theorem 1. However, via* $\gamma = \beta\alpha - (\alpha - 1) < 0$ *and* $\alpha \in (0, 1]$, *we have* $\beta < 0$. *Also, since* $v(\boldsymbol{x}) \leq 0$ *for* $\boldsymbol{x} \in \mathcal{X}$, $v(\boldsymbol{x}_0) \leq 0$ *holds. Thus,* $v(\boldsymbol{x}_0) + \beta N \leq 0$, $v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha-1} \leq 0$, *and* $1 - (1 - v(\boldsymbol{x}_0))\alpha^{-N} \leq 0$ *hold.*

4. Finite-time Reach-avoid Verification

In this section, we present our sufficient conditions for characterizing upper and lower bounds of the reach-avoid probability in Problem 2. The sufficient condition for upper bounds is formulated in Subsection 4.1 and the one for lower bounds is introduced in Subsection 4.2.

Similar to [34], we define a switched system, which facilitates the transformation of the reach-avoid problem in Problem 2 to a mere reachability problem. The switched system is constructed by freezing the dynamics of system (1) upon either exiting the safe set $\mathcal{X}$ or reaching the target set $\mathcal{X}_r$.

Definition 4. *The switched stochastic discrete-time system, which is built upon system* (1), *is a quadruple* $(\widehat{\mathcal{L}}, \widehat{\mathcal{X}}, \boldsymbol{x}_0, \widehat{\boldsymbol{f}})$ *with the following components:*

- $\widehat{\mathcal{L}} = \{1, 2, 3\}$ *is a set of three locations;*
- $\widehat{\mathcal{X}} \subseteq \mathbb{R}^n$ *is the state constraint set;*
- $\boldsymbol{x}_0 \in \widehat{\mathcal{X}}$ *is the initial state;*
- $\widehat{\boldsymbol{f}}(\cdot,\cdot)\colon \mathbb{R}^n \times \Theta \to \mathbb{R}^n$, *where*

$$\widehat{\boldsymbol{f}}(\boldsymbol{x}, \boldsymbol{\theta}) = \sum_{i=1}^{3} 1_{\widehat{\mathcal{X}}_i}(\boldsymbol{x})\widehat{\boldsymbol{f}}_i(\boldsymbol{x}, \boldsymbol{\theta})$$

with $\widehat{\boldsymbol{f}}_1(\boldsymbol{x}, \boldsymbol{\theta}) = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})$, $\widehat{\boldsymbol{f}}_2(\boldsymbol{x}, \boldsymbol{\theta}) = \boldsymbol{x}$ *and* $\widehat{\boldsymbol{f}}_3(\boldsymbol{x}, \boldsymbol{\theta}) = \boldsymbol{x}$, *and* $1_{\widehat{\mathcal{X}}_i}(\boldsymbol{x})$ *is the indicator function of the set* $\widehat{\mathcal{X}}_i$, *i.e.,* $1_{\widehat{\mathcal{X}}_i}(\boldsymbol{x}) = 1$ *if* $\boldsymbol{x} \in \widehat{\mathcal{X}}_i$; *otherwise,* $1_{\widehat{\mathcal{X}}_i}(\boldsymbol{x}) = 0$,

where

1. $\widehat{\mathcal{X}}$ *is a set satisfying* $\widehat{\Omega} \subset \widehat{\mathcal{X}}$*, where*

$$\widehat{\Omega} = \{\boldsymbol{x}' \in \mathbb{R}^n \mid \boldsymbol{x}' = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta}), \boldsymbol{x} \in \mathcal{X}, \boldsymbol{\theta} \in \Theta\} \cup \mathcal{X};$$

2. $\widehat{\mathcal{X}}_1 = \mathcal{X} \setminus \mathcal{X}_r$*;*
3. $\widehat{\mathcal{X}}_2 = \mathcal{X}_r$*;*
4. $\widehat{\mathcal{X}}_3 = \widehat{\mathcal{X}} \setminus \mathcal{X}$*.*

The evolution of the state of this switched system is governed by the iterative map

$$\begin{aligned} &\boldsymbol{x}(l+1) = \widehat{\boldsymbol{f}}(\boldsymbol{x}(l), \boldsymbol{\theta}(l)), \forall l \in \mathbb{N}, \\ &\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \widehat{\mathcal{X}}. \end{aligned} \tag{8}$$

The trajectory of system (8), induced by initial state $\boldsymbol{x}_0 \in \widehat{\mathcal{X}}$ and disturbance policy π, is denoted by $\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(\cdot)\colon \mathbb{N} \to \mathbb{R}^n$.

When system (1), initialized at $\boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r$, enters the region $\mathcal{X}_r$ for the first time at time $i \in \mathbb{N}$ without leaving the safe set $\mathcal{X}$ beforehand, system (8) starting from $\boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r$ also experiences its initial entry at this time, and vice versa. Further, when entering $\mathcal{X}_r$ and $\widehat{\mathcal{X}} \setminus \mathcal{X}$, system (8) will remain confined indefinitely. Thus, the set $\widehat{\mathcal{X}}$ is a robust invariant for system (8) [34], that is, trajectories of system (8) originating from the set $\widehat{\mathcal{X}}$ will never leave it. Consequently, the probability of system (8) entering $\mathcal{X}_r$ at time $t = i$ aligns with the cumulative probability of system (1) entering this target set up to time i without exiting $\mathcal{X}$ until the target hitting event occurs.

Lemma 2. *For* $i \in \mathbb{N}$, $\mathbb{P}^\infty(\exists k \in \mathbb{N}_{\leq i}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r) = \mathbb{P}^\infty(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r)$*. Thus,* $\mathbb{P}^\infty(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r) \leq \mathbb{P}^\infty(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(j) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r)$ *if* $i \leq j$*.*

4.1. Sufficient Conditions for Upper Bounds

In this subsection, we introduce our sufficient condition for upper bounding the probability in Problem 2.

The sufficient condition requires the existence of a non-negative function $v(\boldsymbol{x})$ defined on the set $\widehat{\mathcal{X}}$ that satisfies two key properties: (1) it must be greater than or equal to one on the target set $\mathcal{X}_r$, and (2) its α-scaled expected value at the next step under the dynamics in (1) should increase by

at most $\alpha\beta$ relative to its current value for $\boldsymbol{x} \in \mathcal{X} \setminus \mathcal{X}_r$, where $\alpha \in (0,1]$, and $\beta \in [0,1]$. Upper bounds are derived as follows. Lemma 2 equates the probability of system (8) entering $\mathcal{X}_r$ at $t = N$ with the cumulative probability of system (1) reaching $\mathcal{X}_r$ by time N without leaving $\mathcal{X}$ before hitting the target. Then, we derive upper bounds using system (8) by analyzing α. Since system (8) remains stationary when starting from $\widehat{\mathcal{X}} \setminus \mathcal{X}$ and $\mathcal{X}_r$, implying $\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in (\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r$, we reformulate the constraint on $v(\boldsymbol{x})$ using system (8): its α-scaled expected value at the next step along (8) grows by at most $\alpha\beta$ relative to its current value across the entire set $\widehat{\mathcal{X}}$. For $\alpha \in (0,1)$ and $\alpha = 1$, the upper bounds follow from recursively applying this reformulated constraint.

Theorem 3. *If there exist a function* $v(\boldsymbol{x})\colon \widehat{\mathcal{X}} \to \mathbb{R}$, $\alpha \in (0,1]$, *and* $\beta \in [0,1]$ *such that*

$$\begin{cases} \mathbb{E}^{\infty}[v(\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{X}_r, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \mathcal{X}_r, \\ v(\boldsymbol{x}) \geq 0, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}_r, \end{cases} \tag{9}$$

then $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) = \mathbb{P}^{\infty}\big(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) \leq$

$$\begin{cases} v(\boldsymbol{x}_0) + \beta N, & \text{if } \alpha = 1 \wedge \beta \in [0,1], \\ v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha - 1}, & \text{if } \alpha \in (0,1) \wedge \beta \in [0,1]. \end{cases}$$

Proof. 1) We first justify the case of $\alpha \in (0,1) \wedge \beta \in [0,1]$.

Since $\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in (\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r$, we can obtain

$$\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] - \frac{1}{\alpha}v(\boldsymbol{x}) = (1 - \frac{1}{\alpha})v(\boldsymbol{x}), \forall \boldsymbol{x} \in (\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r.$$

Therefore,

$$\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] - \frac{1}{\alpha}v(\boldsymbol{x}) \leq 0 \leq \beta, \forall \boldsymbol{x} \in (\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r,$$

which can be justified based on the facts that $v(\boldsymbol{x}) \geq 0$ for $\boldsymbol{x} \in \widehat{\mathcal{X}}$, $\alpha \in (0,1)$ and $\beta \in [0,1]$. Therefore, if $v(\boldsymbol{x})$ satisfies (9), it will satisfy

$$\begin{cases} \mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}}, \\ v(\boldsymbol{x}) \geq 1_{\mathcal{X}_r}(\boldsymbol{x}), & \forall \boldsymbol{x} \in \widehat{\mathcal{X}}. \end{cases} \tag{10}$$

According to (10), we have

$$
\begin{aligned}
&v(\boldsymbol{x}_0) \geq 1_{\mathcal{X}_r}(\boldsymbol{x}_0),\\
&\alpha^{-1}v(\boldsymbol{x}_0) + \beta \geq \mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))] \geq \mathbb{E}^{\infty}[1_{\mathcal{X}_r}(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))],\\
&\cdots,\\
&\alpha^{-N}v(\boldsymbol{x}_0) + \beta\sum_{i=0}^{N-1}\alpha^{-i} \geq \mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))] \geq \mathbb{E}^{\infty}[1_{\mathcal{X}_r}(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))].
\end{aligned}
$$

Thus,

$$
\begin{aligned}
&\mathbb{P}^{\infty}\big(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X}\setminus\mathcal{X}_r\big) = \mathbb{E}^{\infty}[1_{\mathcal{X}_r}(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))]\\
&\leq \alpha^{-N}v(\boldsymbol{x}_0) + \alpha\beta\frac{(1-\alpha^{-N})}{\alpha-1}.
\end{aligned}
$$

According to Lemma 2, we have the conclusion.

2) The conclusion on the case of $\alpha = 1 \wedge \beta \in [0,1]$ can be justified by following the proof for the above one.

The proof is completed. □

Similar to the analysis for the parameter β in Theorem 1, the parameter β in Theorem 3 is also required to be less than or equal to 1, which is subject to a practical restriction. Assigning a value greater than one to β would result in bounds exceeding unity when $N \geq 1$, rendering them ineffective.

On the other hand, the analysis for the upper bounds in Theorem 3 is similar to the one in Theorem 1. When $\alpha = 1$ and $\beta = 0$, the upper bound is $v(\boldsymbol{x}_0)$. It is an upper bound of the probability $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \wedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}\setminus\mathcal{X}_r\big)$, which is the probability of reaching the target set $\mathcal{X}_r$ eventually while staying within the safe set $\mathcal{X}$ before the first target hitting time.

Remark 3. *In Theorem 3, α is limited to be in $(0,1]$. We can obtain upper bounds for the case with $\alpha > 1$ according to Theorem 3 in Chapter 3 in [17] or Proposition 1 in Section 3, as shown in Corollary 1.*

Corollary 1. *If there exist a continuous non-negative function $v(\boldsymbol{x})\colon \widehat{\mathcal{X}} \to$*

$\mathbb{R}$, $\alpha \in [1,\infty)$, *and* $\beta \in [0,1]$ *such that*

$$\begin{cases} v(\boldsymbol{x}_0) < 1, & \\ \mathbb{E}^\infty[v(\boldsymbol{\phi}_\pi^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{X}_r, \\ (1-\frac{1}{\alpha})v(\boldsymbol{x}) - \beta \leq 0, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \mathcal{X}_r, \\ v(\boldsymbol{x}) \geq 0, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}}, \end{cases} \tag{11}$$

then $\mathbb{P}^\infty\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) \leq$

$$\begin{cases} v(\boldsymbol{x}_0) + \beta N, & \text{if } \alpha = 1, \\ v(\boldsymbol{x}_0)\alpha^{-N} + \frac{(1-\alpha^{-N})\alpha\beta}{\alpha-1}, & \text{if } \alpha > 1 \wedge \frac{\beta\alpha}{\alpha-1} > 1, \\ 1 - (1 - v(\boldsymbol{x}_0))(1-\beta)^N, & \text{if } \alpha > 1 \wedge \frac{\beta\alpha}{\alpha-1} \leq 1. \end{cases} \tag{12}$$

Proof. Like in [26], consider the stopped version of the stochastic process satisfying (1), which ceases evolving upon exiting the set $\mathcal{X}$. Given a disturbance signal π, the trajectory of the stopped process, starting from $\boldsymbol{x}_0$, is denoted by $\{\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i)\}_{i\in\mathbb{N}}$, which satisfies

$$\begin{cases} \bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i+1) = 1_{\widehat{\mathcal{X}}\setminus\mathcal{X}}(\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i)) + 1_{\mathcal{X}}(\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i))\boldsymbol{f}(\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(i), \boldsymbol{\theta}(i)), \\ \bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(0) = \boldsymbol{x}_0. \end{cases}$$

It is easy to conclude that any sample trajectory for the stopped process starting from any state in $\widehat{\mathcal{X}}$ cannot leave the set $\widehat{\mathcal{X}}$, and $\{\pi \mid \exists k \in \mathbb{N}_{\leq N}.\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r\}$=$\{\pi \mid \exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X}\}$ for $\boldsymbol{x}_0 \in \widehat{\mathcal{X}} \setminus \mathcal{X}$. Therefore, the probability $\mathbb{P}^\infty\big(\exists k \in \mathbb{N}_{\leq N}.\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big)$ of reaching $\mathcal{X}_r$ for the stopped process is equivalent to the reach-avoid probability $\mathbb{P}^\infty\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big)$.

According to Theorem 3 in Chapter 3 in [17] (or, Proposition 1 in Section 3), we have that if there exist a continuous non-negative function $v(\boldsymbol{x})\colon \widehat{\mathcal{X}} \to \mathbb{R}$, $\alpha \in [1,\infty)$, and $\beta \in [0,1]$ such that

$$\begin{cases} v(\boldsymbol{x}_0) < 1, & \\ \mathbb{E}^\infty[v(\bar{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}}(1))] \leq \frac{v(\boldsymbol{x})}{\alpha} + \beta, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}_r, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \mathcal{X}_r, \\ v(\boldsymbol{x}) \geq 0, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}}, \end{cases} \tag{13}$$

then $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\bar{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r\big)$ has upper bounds in (12), and thus $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big)$ has upper bounds in (12).

On the other hand, since $\bar{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1) = \boldsymbol{x}, \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}, \forall \pi$, and $\bar{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}}(1) = \boldsymbol{\phi}_{\pi}^{\boldsymbol{x}}(1)$, $\forall \boldsymbol{x} \in \mathcal{X}, \forall \pi$, we obtain that constraint (13) is equivalent to (11). Thus, the conclusion holds and the proof is completed. □

Following the comparison between constraints (3) *and* (5)*, we conclude that if there exist a function* $v(\boldsymbol{x})$*,* $\alpha \geq 1$*, and* $\beta \in [0, 1]$ *satisfying* (11)*, then the same function* $v(\boldsymbol{x})$ *with* $\frac{1}{\alpha}$ *and* $\beta \in [0, 1]$ *will satisfy* (9)*. Additionally, it is noted that a similar constraint, associated with the same upper bounds in* (12)*, has been presented in Proposition 2 of [26], which is also derived from Theorem 3 in Chapter 3 of [17] (or, Proposition 1). [26] utilized this constraint to determine upper bounds of the probability of reaching the set* $\mathcal{X}_r$ *for stopped processes that cease evolving upon exiting the interior of the set* $\mathcal{X}$*. The stopped process is the same as the one in the proof of Corollary 1 when the set* $\mathcal{X}$ *is open. As shown in the proof of Corollary 1, the probability of reaching* $\mathcal{X}_r$ *for the stopped process in [26] is equivalent to the reach-avoid probability* $\mathbb{P}^{\infty}\big(\exists k \in \mathbb{N}_{\leq N}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\leq k}.\boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big)$ *when the set* $\mathcal{X}$ *is open. This indicates that the safety verification problem in [26] for stopped processes is actually a reach-avoid verification problem for the original process in the present work. Although the constraint in [26] and the one* (11) *are constructed based on the same stopped process (when the set* $\mathcal{X}$ *is open) and Theorem 3 in Chapter 3 of [17], constraint* (11) *is more stringent than the one in [26], including additional conditions of* $(1 - \frac{1}{\alpha})v(\boldsymbol{x}) - \beta \leq 0, \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}$ *and* $v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}$*. To the best of my knowledge, I believe that these additional constraints are necessary and cannot be omitted according to Theorem 3 in Chapter 3 of [17] (or, Proposition 1).*

Remark 4. *Under the assumption that* $\boldsymbol{f}(\cdot, \cdot) \colon \mathcal{X} \times \Theta \to \mathcal{X}$ *(i.e.,* $\mathcal{X}$ *is a robust invariant set* [1] *for system* (1)*), the c-martingale was employed in [13] to certify upper bounds of the probability with which system* (1) *starting from* $\boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r$ *will reach the set* $\mathcal{X}_r$ *within a specified bounded time horizon. Under this strong assumption, c-martingale satisfies* (9) *in Theorem 3 with*

[1] Generally, a robust invariant set is fundamentally challenging, even impossible to compute even if it exists.

$\alpha = 1$. *This assumption is also imposed in [38]. It is worth noting that* $\widehat{\mathcal{X}}$ *in our conditions is not needed if* $\boldsymbol{f}(\cdot,\cdot)\colon \mathcal{X} \times \Theta \to \mathcal{X}$ *holds.*

4.2. Sufficient Conditions for Lower Bounds

In this subsection, we introduce our sufficient condition for lower bounding the probability in Definition 2.

The sufficient condition requires a function $v(\boldsymbol{x}) : \widehat{\mathcal{X}} \to \mathbb{R}$ satisfying four key properties: (1) its admits a finite upper bound over $\widehat{\mathcal{X}}$, (2) it is less than or equal to one on the target set $\mathcal{X}_r$, (3) its expected value at the next step under the dynamics in (1) exceeds its α-scaled value by at least β for $\boldsymbol{x} \in \mathcal{X} \setminus \mathcal{X}_r$, and (4) it is less than or equal to $-\frac{\beta}{\alpha-1}$ over the set $\widehat{\mathcal{X}} \setminus \mathcal{X}$, where $\alpha \in (1,\infty)$ and $\beta \in (1-\alpha,\infty)$. Lower bounds are derived as follows. Lemma 2 equates the probability of system (8) entering $\mathcal{X}_r$ at $t = N$ with the cumulative probability of system (1) reaching $\mathcal{X}_r$ by time N without leaving $\mathcal{X}$ before hitting the target. Then, we derive a lower bound using system (8). System (8) remains stationary for initial states in $(\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r$, implying $\mathbb{E}^\infty[v(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in (\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r$. Given that $v(\boldsymbol{x}) \le 1$ on $\mathcal{X}_r$ and $v(\boldsymbol{x}) \le -\frac{\beta}{\alpha-1}$ over $\widehat{\mathcal{X}} \setminus \mathcal{X}$, we reformulate the constraint over $v(\boldsymbol{x})$ using system (8): its expected value at the next step should grow by at least $\beta - (\alpha - 1 + \beta)1_{\widehat{\mathcal{X}}\setminus\mathcal{X}}(\boldsymbol{x})$ relative to its α-scaled current value $v(\boldsymbol{x})$ for $\boldsymbol{x} \in \widehat{\mathcal{X}}$. Recursively applying this reformulated constraint, together with the upper bound on v, yields a lower bound.

Theorem 4. *If there exist a function* $v(\boldsymbol{x})\colon \widehat{\mathcal{X}} \to \mathbb{R}$ *with* $\sup_{\boldsymbol{x}\in\widehat{\mathcal{X}}} v(\boldsymbol{x}) \le M$, $\alpha \in (1,\infty)$, *and* $\beta \in (1-\alpha,\infty)$ *such that*

$$\begin{cases} \beta + \alpha v(\boldsymbol{x}) \le \mathbb{E}^\infty[v(\boldsymbol{\phi}_\pi^{\boldsymbol{x}}(1))], & \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{X}_r, \\ v(\boldsymbol{x}) \le 1, & \forall \boldsymbol{x} \in \mathcal{X}_r, \\ (\alpha-1)v(\boldsymbol{x}) \le -\beta, & \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}, \end{cases} \tag{14}$$

then $\mathbb{P}^\infty\big(\exists k \in \mathbb{N}_{\le N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{X}_r \bigwedge \forall l \in \mathbb{N}_{\le k}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) = \mathbb{P}^\infty\big(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}_0}(N) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) \ge$

$$\frac{(\alpha^{N+1}v(\boldsymbol{x}_0) - M)(\alpha-1) + \beta(\alpha^{N+1}-1)}{(\alpha+\beta-1)(\alpha^{N+1}-1)}.$$

Proof. Since $\mathbb{E}^\infty[v(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}}(1))] = v(\boldsymbol{x})$ for $\boldsymbol{x} \in (\widehat{\mathcal{X}} \setminus \mathcal{X}) \cup \mathcal{X}_r$, we can obtain that if $v(\boldsymbol{x})$ satisfies (14), it will satisfy

$$(\alpha - 1 + \beta)1_{\mathcal{X}_r}(\boldsymbol{x}) + \mathbb{E}^\infty[v(\widehat{\boldsymbol{\phi}}_\pi^{\boldsymbol{x}}(1))] \ge \alpha v(\boldsymbol{x}) + \beta, \forall \boldsymbol{x} \in \widehat{\mathcal{X}}.$$

Thus, for $\boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r$, we have

$$
\begin{aligned}
&\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))] - \alpha v(\boldsymbol{x}_0) \geq \beta + (1-\alpha-\beta)1_{\mathcal{X}_r}(\boldsymbol{x}_0),\\
&\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(2))] - \alpha\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))] \geq \beta + (1-\alpha-\beta)\mathbb{E}^{\infty}[1_{\mathcal{X}_r}(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(1))],\\
&\cdots,\\
&\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N+1))] - \alpha\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))] \geq \beta + (1-\alpha-\beta)\mathbb{E}^{\infty}[1_{\mathcal{X}_r}(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N))].
\end{aligned}
$$

Thus, we can obtain

$$
\begin{aligned}
&\mathbb{E}^{\infty}[v(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N+1))] - \alpha^{N+1}v(\boldsymbol{x}_0)\\
&\geq \beta\sum_{i=0}^{N}\alpha^i + (1-\alpha-\beta)\sum_{i=0}^{N}\alpha^{N-i}\mathbb{E}^{\infty}[1_{\mathcal{X}_r}(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(i))]\\
&\geq \beta\frac{1-\alpha^{N+1}}{1-\alpha} + (1-\alpha-\beta)\frac{1-\alpha^{N+1}}{1-\alpha} \times \mathbb{P}^{\infty}\big(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big)
\end{aligned}.
$$

The last inequality is obtained via Lemma 2, which states $\mathbb{P}^{\infty}\big(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) \geq \mathbb{P}^{\infty}\big(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(i) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big)$ for $i \leq N$, and the fact that $1-\alpha-\beta < 0$.

Consequently,

$$
\mathbb{P}^{\infty}\big(\widehat{\boldsymbol{\phi}}_{\pi}^{\boldsymbol{x}_0}(N) \in \mathcal{X}_r \mid \boldsymbol{x}_0 \in \mathcal{X} \setminus \mathcal{X}_r\big) \geq \frac{(\alpha^{N+1}v(\boldsymbol{x}_0) - M)(\alpha-1) + \beta(\alpha^{N+1}-1)}{(\alpha+\beta-1)(\alpha^{N+1}-1)}.
$$

According to Lemma 2, we have the conclusion. The proof is completed. □

Remark 5. *Comparing Theorem 2 and 4, we observe that α cannot be equal to one in Theorem 4. Since if $\alpha = 1$, we have $\beta > 0$ from $\beta \in (1-\alpha, \infty)$. However, we have $\beta \leq 0$ from $(\alpha-1)v(\boldsymbol{x}) \leq -\beta, \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}$. This is a contradiction.*

5. Examples

In this section, we demonstrate the performance of the proposed conditions for safety and reach-avoid verification on two numerical examples, using the semi-definite programming tool Mosek [5].

Example 1. *Consider the following one-dimensional discrete-time system:*

$$x(l+1) = x(l) + d(l),$$

where $d(\cdot)\colon \mathbb{N} \to \Theta = [-0.1, 0.1]$, $\mathcal{X} = \{\, x \mid h(x) \leq 0 \,\}$ *with* $h(x) = x^2 - 1$, $\boldsymbol{x}_0 = 0.2$, $\mathcal{X}_r = \{\, x \mid (x-0.9)^2 - 10^{-4} \leq 0 \,\}$, *and* $N = 30$. *Besides, we assume that the probability distribution on* Θ *is the uniform distribution. The probabilities in Problem 1 and 2 obtained via Monte Carlo methods, which used* 10^4 *sample paths, are around 0.0085 and 0.0128, respectively.*

Given the small exact probabilities in Problems 1 and 2, we only estimate their upper bounds in this example. The set $\widetilde{\mathcal{X}} = \widehat{\mathcal{X}} = \{x \mid x^2 - 2 \leq 0\}$ *is employed in solving* (3), (5), (9), *and* (11). *To address these constraints, we encode them into semi-definite programs with sum of squares decomposition techniques for multivariate polynomials. Utilizing polynomials* $v(\boldsymbol{x})$ *of varying degrees, the computed upper bounds are summarized in Tables 1 and 2. Table 1 illustrates that the constraint* (3) *with* $\alpha = \frac{1}{1.1}$ *can yield tighter upper bounds for the probability in Problem 1 compared to* (3) *with* $\alpha = 1$ *(it also corresponds to the* $c-$*martingale in [20]) and* (5) *with* $\alpha = 1.1$. *Similarly, Table 2 shows that the constraint* (9) *with* $\alpha = \frac{1}{1.1}$ *outperforms* (9) *with* $\alpha = 1$ *and* (11) *with* $\alpha = 1.1$ *in providing tighter bounds for the probability in Problem 2. It is observed that employing higher-degree polynomials for computations facilitates the gain of tighter upper bounds of the probabilities in Problem 1 and 2.*

(5) with $\alpha = 1.1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.9795	0.9435	0.9427	0.9427	0.9427	0.9427	0.9427	0.9427	0.9427	0.9427
(3) with $\alpha = \frac{1}{1.1}$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.8166	0.1564	0.0650	0.0447	0.0404	0.0398	0.0398	0.0398	0.0398	0.0398
(3) with $\alpha = 1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.1351	0.1351	0.1351	0.1351	0.1351	0.1351	0.1351	0.1351	0.1351	0.1351

Table 1: Computed upper bounds of the probability in Problem 1 in Example 1 (d denotes the degree of the polynomial $v(\boldsymbol{x})$)

(11) with $\alpha = 1.1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.9943	0.9553	0.9428	0.9427	0.9427	0.9427	0.9427	0.9427	0.9427	0.9427
(9) with $\alpha = \frac{1}{1.1}$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1	0.2530	0.1260	0.0970	0.0906	0.0898	0.0897	0.0897	0.0897	0.0897
(9) with $\alpha = 1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.1736	0.1736	0.1736	0.1736	0.1736	0.1736	0.1736	0.1736	0.1736	0.1736

Table 2: Computed upper bounds of the probability in Problem 2 in Example 1 (d denotes the degree of the polynomial $v(\boldsymbol{x})$)

(5) with $\alpha = 1.01$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.8798	0.7694	0.7423	0.7302	0.6923	0.6663	0.6130	0.6127	0.5837	0.5830
(5) with $\alpha = 1.001$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.8169	0.6612	0.6041	0.5845	0.5316	0.4942	0.4131	0.4098	0.3615	0.3605
(3) with $\alpha = \frac{1}{1.01}$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1.0000	1.0000	0.9625	0.9235	0.8352	0.7731	0.6342	0.6236	0.5424	0.5397
(3) with $\alpha = \frac{1}{1.001}$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.8515	0.6877	0.6179	0.5929	0.5381	0.4983	0.4097	0.4027	0.3505	0.3488
(3) with $\alpha = 1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	0.8100	0.6542	0.5880	0.5643	0.5123	0.4745	0.3902	0.3835	0.3345	0.3322
(6) with $\alpha = 1.1$ and $\beta = 0$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_1	2.5096×10^{-14}	0.0279	0.0490	0.0502	0.0711	0.0735	0.0990	0.1064	0.1245	0.1289

Table 3: Computed lower and upper bounds of the probability in Problem 1 in Example 2 (d denotes the degree of the polynomial $v(\boldsymbol{x})$)

Example 2. *Consider the following one-dimensional discrete-time system from [37]:*

$$x(l+1) = (-0.5 + d(l))x(l),$$

(11) with $\alpha = 1.001$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1	0.9485	0.9388	0.9264	0.9117	0.8988	0.8832	0.8682	0.8579	0.8513
(11) with $\alpha = 1.0001$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1	0.9463	0.9360	0.9263	0.9077	0.8941	0.8780	0.8623	0.8515	0.8446
(11) with $\alpha = 1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1.0000	0.9460	0.9357	0.9259	0.9073	0.8936	0.8774	0.8617	0.8508	0.8439
(9) with $\alpha = \frac{1}{1.001}$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1.0000	0.9929	0.9827	0.9717	0.9524	0.9380	0.9208	0.9043	0.8932	0.8858
(9) with $\alpha = \frac{1}{1.0001}$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1.0000	0.9506	0.9403	0.9304	0.9117	0.8979	0.8816	0.8658	0.8550	0.8480
(9) with $\alpha = 1$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_2	1.0000	0.9460	0.9357	0.9259	0.9073	0.8936	0.8774	0.8617	0.8508	0.8439
(14) with $\alpha = 1.06$ and $\beta = 0$										
d	2	4	6	8	10	12	14	16	18	20
ϵ_1	0.1591	0.2824	0.3453	0.3669	0.4606	0.5218	0.5732	0.5778	0.6119	0.6128

Table 4: Computed lower and upper bounds of the probability in Problem 2 in Example 2 (d denotes the degree of the polynomial $v(\boldsymbol{x})$)

where $d(\cdot)\colon \mathbb{N} \to \Theta = [-1, 1]$, $\mathcal{X} = \{\, x \mid h(x) \leq 0 \,\}$ *with* $h(x) = x^2 - 1$, $\boldsymbol{x}_0 = -0.9$, $\mathcal{X}_r = \{\, x \mid x^2 - 0.36 \leq 0 \,\}$, *and* $N = 50$. *Besides, we assume that the probability distribution on* Θ *is the uniform distribution. The probabilities in Problem 1 and 2 obtained via Monte Carlo methods, which used* 10^4 *sample paths, are around 0.2321 and 0.7708, respectively.*

The set $\widetilde{\mathcal{X}} = \widehat{\mathcal{X}} = \{\, x \mid x^2 - 2.25 \leq 0 \,\}$ *is used in solving* (3), (5), (6), (9), (11), *and* (14). *These constraints are addressed via encoding them into semi-definite programs with sum of squares decomposition techniques for multivariate polynomials. Utilizing polynomials* $v(\boldsymbol{x})$ *of varying degrees, the computed lower and upper bounds are summarized in Tables 3 and 4. It is evident from the results that employing higher-degree polynomials for*

computations leads to tighter lower and upper bounds of the probabilities in Problems 1 and 2, and the constraints (3) *and* (5) *can complement each other in providing upper bounds of the probability in Problem 1. However, the performance of the constraint* (11)*, with* $\alpha = \frac{1}{1.001}$*,* $\alpha = \frac{1}{1.0001}$*, marginally surpasses that of* (9)*, with* $\alpha = 1.001$*,* $\alpha = 1.0001$*, in yielding tighter upper bounds for the probability in Problem 2.*

In Example 1 and 2, we initially determine upper bounds by assigning pre-defined values to the parameter α in constraints (3), (5), (9) and (11), and lower bounds by assigning pre-defined values to the parameters α and β in (6) and (14), and employing convex optimization to solve them. This might yield conservative bounds. However, the automatic optimization of the function $v(\boldsymbol{x})$, α, and β to enhance these bounds constitutes a non-convex problem, which poses a significant challenge. Future work will address this issue, as it is beyond the scope of the current study. *Furthermore, this work does not concentrate on the design of efficient algorithms to solve the associated constraints. Instead, it leverages existing semi-definite programming tools to tackle these issues. Future work will address this gap by proposing efficient algorithms to effectively address these constraints.*

6. Conclusion

In this paper, we introduced novel sufficient conditions for the finite-time safety and reach-avoid verification of stochastic discrete-time dynamical systems. These conditions provide the lower and upper bounds of the probability that, within a predefined finite-time horizon, a system starting from an initial state in a safe set will either exit the safe set (safety verification) or reach a target set while remaining within the safe set until the first encounter with the target (reach-avoid verification). They complement existing criteria or bridge existing gaps in the literature. Finally, we demonstrated their performance in finite-time safety and reach-avoid verification on two numerical examples, utilizing semi-definite programming tools.

In the future, I would like to rigorously assess the conservativeness of the derived bounds through a necessity analysis of the proposed barrier-like conditions, extending the infinite-time framework developed in [33]. Furthermore, I would develop analysis methods for probabilistic programs by integrating these barrier-like conditions. For example, I intend to investigate termination analysis of probabilistic programs within bounded time horizons

and compare the results with state-of-the-art approaches, such as those presented in [8].

Acknowledgements

This work is funded by the CAS Pioneer Hundred Talents Program and Basic Research Program of Institute of Software, CAS (Grant No. ISCAS-JCMS-202302).

References

[1] A. Abate, M. Giacobbe, and D. Roy. Stochastic omega-regular verification and control with supermartingales. In *International Conference on Computer Aided Verification*, pages 395–419. Springer, 2024.

[2] A. Abate, M. Giacobbe, and D. Roy. Quantitative supermartingale certificates. *arXiv preprint arXiv:2504.05065*, 2025.

[3] A. Abate, J.-P. Katoen, J. Lygeros, and M. Prandini. Approximate model checking of stochastic hybrid systems. *European Journal of Control*, 16(6):624–641, 2010.

[4] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada. Control barrier functions: Theory and applications. In *2019 18th European control conference (ECC)*, pages 3420–3431. IEEE, 2019.

[5] M. ApS. Mosek optimization toolbox for matlab. *User's Guide and Reference Manual, Version*, 4(1), 2019.

[6] A. Chakarov and S. Sankaranarayanan. Probabilistic program analysis with martingales. In *Computer Aided Verification: 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings 25*, pages 511–526. Springer, 2013.

[7] K. Chatterjee, A. K. Goharshady, T. Meggendorfer, and Đ. Žikelić. Sound and complete certificates for quantitative termination analysis of probabilistic programs. In *International Conference on Computer Aided Verification*, pages 55–78. Springer, 2022.

[8] K. Chatterjee, A. K. Goharshady, T. Meggendorfer, and Đ. Žikelić. Quantitative bounds on resource usage of probabilistic programs. *Proceedings of the ACM on Programming Languages*, 8(OOPSLA1):362–391, 2024.

[9] K. Chatterjee, P. Novotnỳ, and Đ. Žikelić. Stochastic invariants for probabilistic termination. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, pages 145–160, 2017.

[10] E. M. Clarke. Model checking. In *Foundations of Software Technology and Theoretical Computer Science: 17th Conference Kharagpur, India, December 18–20, 1997 Proceedings 17*, pages 54–56. Springer, 1997.

[11] R. Dimitrova, L. M. Ferrer Fioriti, H. Hermanns, and R. Majumdar. Probabilistic ctl: the deductive way. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 280–296. Springer, 2016.

[12] T. A. Henzinger, K. Mallik, P. Sadeghi, and Đ. Žikelić. Supermartingale certificates for quantitative omega-regular verification and control. *arXiv preprint arXiv:2505.18833*, 2025.

[13] P. Jagtap, S. Soudjani, and M. Zamani. Temporal logic verification of stochastic systems using barrier certificates. In *International Symposium on Automated Technology for Verification and Analysis*, pages 177–193. Springer, 2018.

[14] P. Jagtap, S. Soudjani, and M. Zamani. Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, 66(7):3097–3110, 2020.

[15] A. Kenyon-Roberts and C.-H. L. Ong. Supermartingales, ranking functions and probabilistic lambda calculus. In *2021 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–13. IEEE, 2021.

[16] S. Kura, N. Urabe, and I. Hasuo. Tail probabilities for randomized program runtimes via martingales for higher moments. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 135–153. Springer, 2019.

[17] H. J. Kushner. Stochastic stability and control. 1967.

[18] R. Majumdar and V. Sathiyanarayana. Sound and complete proof rules for probabilistic termination. *Proceedings of the ACM on Programming Languages*, 9(POPL):1871–1902, 2025.

[19] Z. Manna and A. Pnueli. *Temporal verification of reactive systems: safety*. Springer Science & Business Media, 2012.

[20] F. B. Mathiesen, S. C. Calvert, and L. Laurenti. Safety certification for stochastic systems via neural barrier functions. *IEEE Control Systems Letters*, 7:973–978, 2022.

[21] A. McIver, C. Morgan, B. L. Kaminski, and J.-P. Katoen. A new proof rule for almost-sure termination. *Proceedings of the ACM on Programming Languages*, 2(POPL):1–28, 2017.

[22] M. Moosbrugger, E. Bartocci, J.-P. Katoen, and L. Kovács. Automated termination analysis of polynomial probabilistic programs. In *European Symposium on Programming*, pages 491–518. Springer International Publishing Cham, 2021.

[23] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

[24] S. Prajna, A. Jadbabaie, and G. J. Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

[25] S. Prajna and A. Rantzer. Convex programs for temporal verification of nonlinear dynamical systems. *SIAM Journal on Control and Optimization*, 46(3):999–1021, 2007.

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

[27] J. Steinhardt and R. Tedrake. Finite-time regional verification of stochastic non-linear systems. *The International Journal of Robotics Research*, 31(7):901–923, 2012.

[28] T. Takisaka, Y. Oyabu, N. Urabe, and I. Hasuo. Ranking and repulsing supermartingales for reachability in randomized programs. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 43(2):1–46, 2021.

[29] A. Taylor, A. Singletary, Y. Yue, and A. Ames. Learning for safety-critical control with control barrier functions. In *Learning for Dynamics and Control*, pages 708–717. PMLR, 2020.

[30] J. Ville. *Etude critique de la notion de collectif*. Gauthier-Villars Paris, 1939.

[31] D. Wang, J. Hoffmann, and T. Reps. Central moment analysis for cost accumulators in probabilistic programs. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, pages 559–573, 2021.

[32] J. Wang, Y. Sun, H. Fu, K. Chatterjee, and A. K. Goharshady. Quantitative analysis of assertion violations in probabilistic programs. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, pages 1171–1186, 2021.

[33] B. Xue. Sufficient and necessary barrier-like conditions for safety and reach-avoid verification of stochastic discrete-time systems. *arXiv preprint arXiv:2408.15572*, 2024.

[34] B. Xue, R. Li, N. Zhan, and M. Fränzle. Reach-avoid analysis for stochastic discrete-time systems. In *2021 American Control Conference (ACC)*, pages 4879–4885. IEEE, 2021.

[35] B. Xue, N. Zhan, M. Fränzle, J. Wang, and W. Liu. Reach-avoid verification based on convex optimization. *IEEE Transactions on Automatic Control*, 69(1):598–605, 2024.

[36] B. Xue, N. Zhan, and M. Fränzle. Reach-avoid analysis for polynomial stochastic differential equations. *IEEE Transactions on Automatic Control*, 69(3):1882–1889, 2024.

[37] Y. Yu, T. Wu, B. Xia, J. Wang, and B. Xue. Safe probabilistic invariance verification for stochastic discrete-time dynamical systems. In *2023 62nd*

IEEE Conference on Decision and Control (CDC), pages 5804–5811. IEEE, 2023.

[38] D. Zhi, P. Wang, S. Liu, C.-H. L. Ong, and M. Zhang. Unifying qualitative and quantitative safety verification of dnn-controlled systems. In *International Conference on Computer Aided Verification*, pages 401–426. Springer, 2024.

[39] Đ. Žikelić, M. Lechner, T. A. Henzinger, and K. Chatterjee. Learning control policies for stochastic systems with reach-avoid guarantees. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 37, pages 11926–11935, 2023.