k-Inductive Barrier Certificates for Stochastic Dynamical Systems

Mahathi Anand
LMU Munich
Munich, Germany
mahathi.anand@lmu.de

Vishnu Murali
University of Colorado, Boulder
Boulder, USA
vishnu.murali@colorado.edu

Ashutosh Trivedi
University of Colorado, Boulder
Boulder, USA
ashutosh.trivedi@colorado.edu

Majid Zamani
University of Colorado Boulder
Boulder, USA
majid.zamani@colorado.edu

ABSTRACT

Barrier certificates are inductive invariants that provide guarantees on the safety and reachability behaviors of continuous dynamical systems. For stochastic dynamical systems, barrier certificates take the form of inductive "expectation" invariants. In this context, a barrier certificate is a non-negative real-valued function over the state space of the system satisfying a strong *supermartingale* condition: it decreases in expectation as the system evolves. The existence of barrier certificates, then, provides lower bounds on the probability of satisfaction of safety or reachability specifications over *unbounded-time horizons*. Unfortunately, establishing supermartingale conditions on barrier certificates can often be restrictive. In practice, we strive to overcome this challenge by utilizing a weaker condition called c-martingale that permits a bounded increment in expectation at every time step; unfortunately this only guarantees the property of interest for a bounded time horizon.

The idea of k-inductive invariants, often utilized in software verification, relaxes the need for the invariant to be inductive with every transition of the system to requiring that the invariant holds in the next step if it holds for the last k steps. This paper synthesizes the idea of k-inductive invariants with barrier certificates. These refinements that we dub as *k-inductive barrier certificates* relax the supermartingale requirements at each time step to supermartingale requirements in k-steps with potential c-martingale requirements at each step, while still providing unbounded-time horizon probabilistic guarantees. We characterize a notion of k-inductive barrier certificates for safety and two distinct notions of k-inductive barrier certificates for reachability. Correspondingly, utilizing such k-inductive barrier certificates, we obtain probabilistic lower bounds on the satisfaction of safety and reachability specifications, respectively. We present a computational method based on sum-of-squares (SOS) programming to synthesize suitable k-inductive barrier certificates and, demonstrate the effectiveness of the proposed methods via some case studies.

HSCC '22, May 4–6, 2022, Milan, Italy

ACM ISBN 978-1-4503-9196-2/22/05.
https://doi.org/10.1145/3501710.3519532

KEYWORDS

Barrier certificates, Stochastic dynamical systems, Safety specification, Reachability specification, k-Induction

ACM Reference Format:
Mahathi Anand, Vishnu Murali, Ashutosh Trivedi, and Majid Zamani. 2022. k-Inductive Barrier Certificates for Stochastic Dynamical Systems. In *25th ACM International Conference on Hybrid Systems: Computation and Control (HSCC '22), May 4–6, 2022, Milan, Italy.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3501710.3519532

1 INTRODUCTION

Structural induction is a versatile approach to verify properties of hardware, software, and cyber-physical systems. A crucial element to the success of induction based approaches to verification is the idea of *inductive invariants*: a property of the states of the system that holds on the initial states and is closed under transition structure of the system. Barrier certificates, a quantitative analog of inductive invariants, are typically real-valued functions of the state space that decrease along the trajectories of the system. The existence of barrier certificates provide safety guarantees if the value of the barrier function for the unsafe states is greater than that of initial states. This approach can also be harnessed to establish reachability guarantees. For stochastic dynamical systems, barrier certificates take the form of expectation invariants [1]: they employ *supermartingale* conditions to ensure that they are non-increasing in expectation at each time step, which can provide lower bounds for the probabilities of satisfying safety and reachability properties over potentially *unbounded* time horizons.

The strong supermartingale requirement on barrier certificates makes their discovery hard. The notion of c-martingales [2] aims to alleviate this problem by permitting a bounded increase in the expected value of the certificate at each time step. However, this flexibility comes at the cost that the probabilistic guarantees can only be established for *bounded* time horizons. The notion of k-inductive invariants, used in software verification [3, 4], also aims to relax the strict inductive invariant requirements by requiring that the invariant is inductive for k-compositions of the transition relation for a given bound k. The k-induction principle has been effectively generalized to non-stochastic continuous systems as t-barrier [5] and k-inductive barrier functions [6, 7] and has been successfully demonstrated to improve the search for barrier certificates. These success stories prompt several questions in the context of stochastic systems:

(1) What are the counterparts of k-inductive barrier certificates for stochastic dynamical systems?
(2) Can they be used to provide guarantees for unbounded time-horizon safety and reachability properties? and
(3) Do they mitigate the search for barrier certificates?

Contributions. This paper answers aforementioned questions by presenting three notions of k-inductive barrier certificates.

(1) The first notion strengthens the standard conditions for safety properties in [8] via k-induction such that a larger class of functions can behave as k-inductive barrier certificates and still provides probabilistic safety guarantees for unbounded time horizons.
(2) We present two notions of k-inductive barrier certificates for reachability properties over unbounded time horizons. While the first one allows us to compute a lower bound for the probability of satisfying reachability, the second one (if existing) can be utilized to guarantee almost sure reachabilty.
(3) As expected, we show that our definitions and probability bounds for k-inductive barrier certificates coincide with those of standard barrier certificates when $k = 1$, in the case of both safety and reachability.
(4) We demonstrate the utility of the proposed notions over simple illustrative examples (cf. Example 7 and 20) showing the existence of systems that may not admit standard barrier certificates but do admit k-inductive barrier certificates.
(5) Under some mild assumptions on the underlying dynamics, we provide a computational method based on sum-of-squares (SOS) optimization to obtain appropriate k-inductive barrier certificates for safety and reachability properties.
(6) Finally, we demonstrate the effectiveness of our proposed approaches over two case studies.

Related Work. Verification of safety and reachability properties for discrete systems have been extensively studied and can either be performed by model checking [9] or by utilizing deductive verification techniques [10]. Typical model checking techniques rely on computing graph reachability of finite-state models, whereas deductive verification approaches rely on mathematical proof rules and logical inferences that guarantee safety or reachability properties. Model checking approaches may also be extended to continuous-state systems by means of abstraction techniques [11, 12]. There are several results in the literature that tackle the verification and synthesis problem for stochastic systems against safety and reachability specifications by utilizing abstraction-based techniques. Results in this direction include those providing probabilistic guarantees for stochastic hybrid automata for safety and reachability specifications [13], game-based abstraction framework for reachability verification and synthesis for hybrid automata [14, 15], and reach-and-avoid verification via reachable set computations [16, 17]. Unfortunately, these techniques rely on discretizing state sets and suffer from the curse of dimensionality, i.e. the number of discrete states grows exponentially with the dimension of the system.

More recently, abstraction-free techniques via barrier certificates [8] have gained considerable attentions. Barrier certificates are non-negative real valued functions that are analogous to inductive invariants [18, 19] in deductive verification approaches for software verification. Barrier certificates were first proposed for the verification of safety specifications in the context of non-stochastic dynamical systems in [20] and were later extended to reachability specifications in [21, 22]. These approaches have also been extended to stochastic dynamical systems [8, 23] by utilizing supermartingale conditions to provide probabilistic guarantees for unbounded time horizons. These conditions have been relaxed by utilizing c-martingales in [2, 24, 25] but at the cost of providing only bounded time horizons guarantees.

A generalization of barrier certificates utilizing the k-induction principle was first proposed in [5], but in the context of non-stochastic continuous-time systems and relies on time-bounded backward reachability analysis to verify safety. As such, a similar idea cannot be extended to stochastic systems without relying on over-approximations of backward reachable sets. The k-inductive barrier certificate approaches were also utilized for non-stochastic systems in [6, 7]; however, to the best of our knowledge, the present submission is the first attempt to verify stochastic dynamical systems via k-inductive barrier certificates.

We should add that the two standard (a.k.a. 1-inductive) barrier certificate definitions for reachability used in our paper are adapted from [21] and [26], respectively. In particular, the first definition (cf. Definition 15) is a stochastic version of the one used in [21]. The second definition (cf. Definition 18) is akin to the additive supermartingale ranking functions [26] used to provide almost-sure termination guarantees for program verification.

Organization. Section 2 discusses the key problems we study. In Section 3, we present safety verification via barrier certificates. First, we review the classical barrier certificates used for safety, and then submit key theoretical result of our paper by proposing k-inductive barrier certificates for safety properties. Section 4 extends the standard barrier certificate-based approaches to reachability and presents the second result of our paper concerning k-inductive barrier certificates for reachability. An implementation of the proposed techniques is discussed in Section 5, followed by case studies in Section 6. Note that all proofs can be found in the Appendix.

2 PROBLEM DEFINITION

We use $\mathbb{R}$, $\mathbb{R}_{>0}$ and $\mathbb{R}_{\geq 0}$ to denote the set of reals, positive reals, and non-negative reals, respectively. Similarly, we use $\mathbb{N}$ and $\mathbb{N}_{\geq 1}$ for the set of non-negative and positive integers, respectively. Given sets A and B, a function $f : A \to B$ is a mapping from A to B. We use $\varnothing$ to denote the empty set. For a set $A \subseteq \mathbb{R}^n$, we write ∂A and $\overline{A}$ for its boundary and topological closure, respectively.

We consider the probability space $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$ where Ω is the sample space, $\mathcal{F}_\Omega$ is the sigma-algebra on Ω comprising the subsets of Ω as events in the probability space and $\mathbb{P}_\Omega$ is the probability measure assigned to those events. We consider random variables to be measurable functions of the form $X : (\Omega, \mathcal{F}_\Omega) \to (S_X, \mathcal{F}_X)$, and each random variable X is associated with a probability measure on $(S_X, \mathcal{F}_X)$ as $Prob\{A\} = \mathbb{P}_\Omega\{X^{-1}(A)\}$ for any $A \in \mathcal{F}_X$.

The topological space S is a Borel space if it is homeomorphic to a Borel subset of a separable and completely metrizable space. We denote by $B(S)$ the Borel sigma-algebra generated from the Borel space S, and the map $f : S \to Y$ is said to be measurable when it is Borel measurable.

2.1 Discrete-Time Stochastic Systems

Definition 1. A discrete-time stochastic dynamical system (dt-SS) is a tuple

$$\mathfrak{S} = (X, \varsigma, f), \tag{1}$$

where

- $X \subseteq \mathbb{R}^n$ is a Borel space as the state space of the system. The tuple $(X, B(X))$ is the measurable state space where $B(X)$ denotes the Borel sigma-algebra on the state space;
- $\varsigma := \{\varsigma(k) : \Omega \to \mathcal{V}_\varsigma,\ k \in \mathbb{N}\}$ is a sequence of independent and identically distributed (i.i.d.) random variables from a sample space Ω to the measurable space $(\mathcal{V}_\varsigma, \mathcal{F}_\varsigma)$; and
- $f : X \times V_\varsigma \to X$ is a measurable function that describes the state evolution of $\mathfrak{S}$.

For a given initial condition $x(0) \in X$, the state evolution of $\mathfrak{S}$ can be described by the following stochastic difference equation:

$$x(t+1) = f(x(t), \varsigma(t)), \quad t \in \mathbb{N}. \tag{2}$$

We denote the solution process generated by $\mathfrak{S}$ starting from initial state $x(0) = x_0$ by a sequence of states $\mathbf{x}_{x_0} = (x(0), x(1), \ldots)$.

Given a set of initial states X_0 and a set of unsafe states X_u, a solution process $\mathbf{x}_{x_0}$ starting from $x_0 \in X_0$ is *safe* if it never visits the states in X_u, *i.e.*, we have that $\mathbf{x}_{x_0}(t) \notin X_u$, for all time $t \in \mathbb{N}$. In other words, a system satisfies the safety property if its solution processes never visit the unsafe set X_u.

Similarly, given a set of initial states X_0 and a set of target states X_R, a solution process $\mathbf{x}_{x_0}$ of the dt-SS $\mathfrak{S}$ starting from some state $x_0 \in X_0$ is said to *reach* X_R if it eventually visits some states in X_R, *i.e.* we have that $\mathbf{x}_{x_0}(t) \in X_R$, for some time $t \in \mathbb{N}$. Correspondingly a system satisfies the reachability property if its solution processes reach the target set X_R at some point in the future.

We are concerned with obtaining probabilistic guarantees over the satisfaction of safety and reachability properties for a given stochastic dynamical system $\mathfrak{S}$. In particular, one would like to compute a tight lower bound on the probability of satisfying safety and reachability specifications. To do so, we first present the definition of probabilistic satisfaction of safety specification.

Definition 2 (Safety Probability). For a dt-SS $\mathfrak{S}$, let X_0 and X_u be the set of initial and unsafe states respectively. Then, we say that $\mathfrak{S}$ satisfies safety with a probability bound of λ if the solution processes of $\mathfrak{S}$ starting from some state $x_0 \in X_0$ do not visit X_u with a probability of at least λ, *i.e.*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0 \in X_0\} \geq \lambda.$$

We now formalize the first problem studied in this paper, which is to obtain the probability bound with which the dt-SS $\mathfrak{S}$ satisfies the safety specification.

Problem 1 (Safety Verification). *Given a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ with dynamics as in (2), the sets of initial and unsafe states X_0 and X_u, respectively, compute a constant $0 \leq \lambda \leq 1$ such that the system is safe with a probability bound of λ.*

The other problem we consider is the probabilistic satisfaction of reachability properties defined as follows.

Definition 3 (Reachability Probability). For a dt-SS $\mathfrak{S}$, let X_0 and X_R be the set of initial and target states, respectively. Then, we say that $\mathfrak{S}$ satisfies reachability with a probability bound of λ if the solution processes of $\mathfrak{S}$ starting from some state $x_0 \in X_0$ eventually reach X_R with a probability of at least λ, *i.e.*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0 \in X_0\} \geq \lambda.$$

With that, the reachability verification problem for dt-SS can formally be expressed as the following.

Problem 2 (Reachability Verification). *Given a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ with dynamics as in (2), the sets of initial and target states X_0 and X_R, respectively, compute a constant $0 \leq \lambda \leq 1$ such that the system reaches X_R with a probability bound of λ.*

2.2 The k-Induction Principle

Mathematical induction can sometimes be employed to prove safety and reachability properties. The inductive proof for a property P comprises of a base case, an inductive hypothesis and an inductive step. In the case of standard induction, one utilizes the inductive hypothesis that the property P holds at any given time step to imply that the property also holds in the subsequent time step. Formally, an inductive proof for the property P is written as follows:

$$\Big(P(0) \wedge \underset{t\in\mathbb{N}}{\forall} (P(t) \implies P(t{+}1))\Big) \implies \underset{t\in\mathbb{N}}{\forall} P(t).$$

On the other hand, the inductive hypothesis of k-induction assumes that the property P holds at all steps until the kth step. The stronger inductive hypothesis weakens the need to enforce the consequent due to the availability of additional information. Mathematically, a k-inductive proof for property P is described as:

$$\left(\bigwedge_{0\leq i<k} P(i) \wedge \underset{t\in\mathbb{N}}{\forall} \left(\bigwedge_{0\leq i<k} \big(P(t{+}i)\big) \implies P(t{+}k)\right)\right) \implies \underset{t\in\mathbb{N}}{\forall} P(t).$$

In k-induction, the base case requires the property to be shown to hold true in the first k steps. The inductive step then allows us to show that if the property P holds true in k consecutive steps, then consequently it holds true in the $(k+1)$th step as well and so it must hold true for any time step.

3 SAFETY VERIFICATION

3.1 Barrier Certificates for Safety

A supermartingale is a sequence of random variables for which the conditional expectation of the next value in the sequence is smaller than the present value irrespective of the prior values. The barrier certificates [8] for stochastic systems are non-negative real valued functions over the state set that satisfy the *supermartingale* property, *i.e.*, the expected value of the function remains non-increasing at every time step.

Definition 4. We say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a *barrier certificate* for the dt-SS $\mathfrak{S}$ with respect to a set of initial states $X_0 \subseteq X$, a set of unsafe states $X_u \subseteq X$ if there exists a constant $0 \leq \varepsilon \leq 1$ such that the following conditions hold:

$$\mathcal{B}(x) \leq \varepsilon, \qquad \text{for all } x \in X_0, \tag{3}$$

$$\mathcal{B}(x) \geq 1, \qquad \text{for all } x \in X_u, \text{ and} \tag{4}$$

$$\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] - \mathcal{B}(x) \leq 0, \qquad \text{for all } x \in X. \tag{5}$$

Definition 4 can then be utilized to obtain the lower bound on the probability that the dt-SS $\mathfrak{S}$ satisfies the safety specification.

Theorem 5. *[8] Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$. Let $\mathcal{B}$ be a barrier certificate satisfying conditions* (3)-(5) *for some $0 \leq \varepsilon \leq 1$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ does not reach unsafe region X_u is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0\} \geq 1 - \varepsilon. \tag{6}$$

From Theorem 5, it can be easily inferred that the existence of a barrier certificate according to Definition 4 guarantees a solution to Problem 1 with a probability of $\lambda = 1 - \varepsilon$. Our goal is to find the tight lower bound on probability λ, which requires us to find the minimal value of ε that guarantees the existence of the barrier certificate satisfying conditions (3)-(5).

Remark 6. *Observe that if $X_0 \cap X_u \neq \emptyset$, there does not exist a barrier certificate as in Definition 4 that guarantees safety due to the conflict between conditions* (3) *and* (4). *In such a case, the solution processes can start from the unsafe regions and will trivially violate the safety property. Therefore, throughout the paper, we work with the case where $X_0 \cap X_u = \emptyset$.*

The search for a barrier certificate is usually performed by restricting barrier certificates to a certain parametric form (e.g. polynomial functions) and utilizing suitable search techniques such as sum-of-squares (SOS) optimization [27] or satisfiability modulo theory (SMT) solvers [28]. However, the supermartingale condition (5) can be quite restrictive as it requires the expected value of the barrier certificate to be non-increasing for all time steps. Due to this, in many cases, one may fail to find an appropriate barrier certificate as in Definition 4. Then, one may have to replace the probability λ with a trivial value of 0, and the approach fails to give a non-trivial probability. We now illustrate with an example that the barrier certificate approach fails to provide non-trivial probabilistic guarantees even when the system is safe with a high probability for a fixed template of barrier certificates.

Example 7. Consider a Markov chain shown in Figure 1 as a finite state stochastic system $\mathfrak{S}$ with $x \in X = \{0, 0.1, 0.2, 0.3, 0.5, 6, 10\}$ as states of the system, $x = 0.2$ as the initial state and $x = 10$ as the unsafe state. By utilizing barrier certificates, we want to provide a tight lower bound on the probability that the solution processes do not reach unsafe regions. As it can be seen from the figure, the probability that the system remains safe is 0.99. However, by choosing a linear barrier certificate according to Definition 4, we cannot provide a non-trivial probabilistic lower bound on the satisfaction of safety.

Consider $\mathcal{B}(x) = ax + b$. According to condition (3), since $x = 0.2$ is the initial state, we have $0.2x + b \leq \varepsilon$, for some $0 \leq \varepsilon \leq 1$. Moreover, by applying the supermartingale condition (5) at $x = 0.2$, we get $\mathbb{E}[\mathcal{B}(f(x)) \mid x = 0.2] - \mathcal{B}(x) = 0.2a \leq 0$, implying that $a \leq 0$. However, due to condition (4) and the fact that $x = 10$ is the unsafe state, we have $10x + b \geq 1$. Then, $a \leq 0$ would lead to contradiction between conditions conditions (3) and (4). Therefore, there does not exist a linear barrier certificate for any value of ε.

A practical approach to tackle this issue is to relax condition (5) by utilizing a *c-martingale* [2] instead of a supermartingale, at

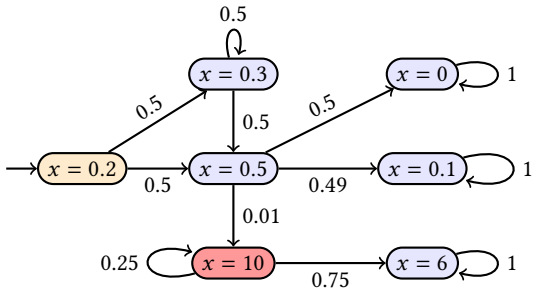


Figure 1: Finite Markov chain $\mathfrak{S}$ for Example 7. The initial state is denoted in yellow and the unsafe state in red.

the cost of providing guarantees over *bounded-time* horizons. We provide the definition of a *c*-martingale barrier certificate as follows:

Definition 8. We say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a *c*-martingale barrier certificate for the dt-SS $\mathfrak{S}$ with respect to a set of initial states $X_0 \subseteq X$ and a set of unsafe states $X_u \subseteq X$ if there exist constants $0 \leq \varepsilon \leq 1$ and $c \geq 0$ such that the following conditions hold:

$$\mathcal{B}(x) \leq \varepsilon, \qquad \text{for all } x \in X_0, \tag{7}$$

$$\mathcal{B}(x) \geq 1, \qquad \text{for all } x \in X_u, \tag{8}$$

$$\mathbb{E}[\mathcal{B}(f(x, \varsigma)) \mid x] - \mathcal{B}(x) \leq c, \qquad \text{for all } x \in X. \tag{9}$$

Condition (9), unlike the supermartingale condition (5), does not require the barrier certificate to be non-increasing at every time step. Instead, it ensures that the barrier certificate is a *c*-martingale, meaning that the expected value of the barrier certificate can increase at every time step as long as it is bounded by a constant c. This condition allows the barrier certificate to increase slowly in expectation such that it takes a *long* time to reach the unsafe regions of the state space. We obtain the following theorem as a direct consequence of [24, Theorem 1].

Theorem 9. *Consider a dt-SS $\mathfrak{S}$. Suppose $\mathcal{B}$ is a c-martingale barrier certificate for $\mathfrak{S}$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ does not reach unsafe region X_u within a finite time horizon $T \in \mathbb{N}$ is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \leq T \mid x_0\} \geq 1 - (\varepsilon + cT). \tag{10}$$

It is apparent from the above discussion that relaxing the conservative supermartingale condition (5) to the *c*-martingale condition (9) restricts the verification problem to bounded-time domains. Due to the dependency of the time horizon while computing the probability of satisfaction, one may only obtain a high probability of satisfaction for short time horizons. However, for reactive systems, such as medical devices and power grids, it is vital to provide long-term or even unbounded-time safety guarantees. Therefore, it becomes necessary to be able to relax the supermartingale requirement of barrier certificates while still providing probabilistic safety guarantees over unbounded-time horizons.

Standard notion of barrier certificates for safety as in Definition 4 are analogous to standard inductive proofs. The definition of barrier certificates is similar to the inductive proofs that yield expectation invariants [26]. Particularly, via conditions (3) and (5),

the expectation of barrier certificate at any time instant is bounded by ε. This allows one to view condition (3) as the base case, while the supermartingale condition (5) is the inductive step.

We show that we can effectively weaken the supermartingale conditions for safety by leveraging the k-induction principle, often utilized in the context of software verification [3, 4], which results in less conservative conditions for barrier certificates that are easier to satisfy. These barrier certificates, which we dub as *k-inductive barrier certificates*, can still provide probabilistic guarantees for the satisfaction of safety over unbounded-time horizons. Therefore, a dt-SS $\mathfrak{S}$ that does not admit the standard notion of barrier certificates for safety may admit a k-inductive barrier certificate, while still providing unbounded-time horizon guarantees.

3.2 k-Inductive Barrier for Safety

This section presents the main results concerning probabilistic safety verification via k-inductive barrier certificates. Our approach relies on looking at the behavior of the stochastic system in future time instances, such as after i time steps rather than at every time step. We obtain such behavior by simply utilizing recursive application of the function f defined in (2). In particular, for a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ with dynamics as in (2), the value of the solution process after the i^{th} time step, $i \geq 1$ is obtained as

$$x(t+i) = f_i(x(t), \varsigma_i(t)), \tag{11}$$

where $\varsigma_i(t) = [\varsigma(t); \ldots; \varsigma(t+i-1)]$ is the vector containing all the noise terms from time t to time $t+i-1$, and we define f_i recursively, where $f_i(x(t), \varsigma_i(t)) = f(x(t), \varsigma(t))$, if $i = 1$, and $f_i(x(t), \varsigma_i(t)) = f(f_{i-1}(x(t), \varsigma_{i-1}(t)), \varsigma(t+i-1))$ for all $i > 1$.

To provide probabilistic safety guarantees over unbounded-time horizons, one can simply extend the notion of c-martingale barrier certificates and leverage the k-induction principle. We define k-inductive barrier certificates for safety as follows.

Definition 10. Consider a dt-SS $\mathfrak{S}$. We say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a k-inductive barrier certificate for $\mathfrak{S}$ with respect to a set of initial states X_0 and an unsafe set X_u if there exist constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$ and $c \geq 0$ such that the following holds:

$$\mathcal{B}(x) \leq \varepsilon, \qquad \text{for all } x \in X_0, \tag{12}$$
$$\mathcal{B}(x) \geq 1, \qquad \text{for all } x \in X_u, \tag{13}$$
$$\mathbb{E}[\mathcal{B}(f(x, \varsigma)) \mid x] - \mathcal{B}(x) \leq c, \qquad \text{for all } x \in X, \tag{14}$$
$$\mathbb{E}[\mathcal{B}(f_k(x, \varsigma_k)) \mid x] - \mathcal{B}(x) \leq 0, \qquad \text{for all } x \in X. \tag{15}$$

Note that condition (14) requires the barrier certificate to be a c-martingale at every time step and condition (15) requires the barrier certificate sampled after every kth step to be a supermartingale. We now present the first key result of our paper based on this definition of k-inductive barrier certificates.

Theorem 11. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (12)-(15) *with some $0 \leq \varepsilon \leq 1$, $c \geq 0$, and $k \in \mathbb{N}_{\geq 1}$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ does not reach the unsafe region X_u is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0\} \geq 1 - k\varepsilon - \frac{k(k-1)c}{2}. \tag{16}$$

x	$\mathcal{B}(x)$	$\mathbb{E}[\mathcal{B}(f(x,\varsigma))\|x]$	$\mathbb{E}[\mathcal{B}(f_2(x,\varsigma_2))\|x]$	$\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3))\|x]$
0.2	0.03	0.05	0.03745	0.029675
0.3	0.04	0.05	0.03745	0.029675
0.5	0.06	0.0249	0.0219	0.02115
0	0.01	0.01	0.01	0.01
0.1	0.02	0.02	0.02	0.02
6	0.61	0.61	0.61	0.61
10	1.01	0.71	0.635	0.61625

Table 1: The values of $\mathbb{E}[\mathcal{B}(f_i(x,\varsigma_i)) \mid x]$ for all $i \in \{1,2,3\}$ and all $x \in X$ for Example 7. Note that $\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3)) \mid x] - \mathcal{B}(x) \leq 0$ for all $x \in X$.

Remark 12. *Note that, in order to obtain meaningful probabilities, the value of k in inequality* (16) *is bounded by*

$$1 \leq k \leq \frac{(c - 2\varepsilon) + \sqrt{4\varepsilon^2 + c^2 - 4c(2+\varepsilon)}}{2c}.$$

One can readily observe that k-inductive barrier certificates as in Definition 10 also lead to expectation invariants, as the expected value of the barrier certificate remains bounded in the set $\mathbb{E}[\mathcal{B}(\mathbf{x}_{x_0}(t)) \mid x_0] \leq \varepsilon + (k-1)c$ for all $t \in \mathbb{N}$ due to the bounded increase of $\mathbb{E}[\mathcal{B}(\mathbf{x}_{x_0}(t)) \mid x_0]$ at every time step via conditions (14) and (15). Note that, when $k = 1$ and $c = 0$, conditions (12)-(15) reduce to standard barrier certificate conditions (3)-(5). Moreover, one immediately observes that the probability bounds in (16) also converge to those in (6) under the same conditions. Therefore, any barrier certificate satisfying conditions (3)-(5) is also a 1-inductive barrier certificate as in Definition 10. However, the converse may not hold true since conditions (12)-(15) are more relaxed. We now illustrate k-inductive barrier certificates as in Definition 10 with the Markov chain considered in Example 7.

Example 7 (Continued). Let us consider the finite Markov chain $\mathfrak{S}$ presented in Figure 1. For this system, we already showed that there exists no linear barrier certificate satisfying conditions (3)-(5) for any $0 \leq \varepsilon < 1$ which leads to trivial probabilistic bounds for the satisfaction of safety. Now, we show that by using k-inductive barrier certificates as in Definition 10, we get more reliable probabilistic bounds for the satisfaction of safety.

Consider $\mathcal{B}(x) = 0.1x + 0.01$, constants $\varepsilon = 0.05$ and $c = 0.02$, and $k = 3$. The enumerated values of $\mathcal{B}(x), \mathbb{E}[\mathcal{B}(f(x,\varsigma) \mid x]$, $\mathbb{E}[\mathcal{B}(f_2(x,\varsigma_2)) \mid x]$, and $\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3)) \mid x]$ for all states $x \in X$ are provided in Table 1. We immediately see that condition (12) is satisfied for the initial state $x = 0.2$ and similarly, condition (13) holds for the unsafe state $x = 10$. Moreover, conditions (14) and (15) also hold for all $x \in X$. Therefore, $\mathcal{B}(x) = 0.1x + 0.01$ is indeed a linear 3-inductive barrier certificate for $\mathfrak{S}$. We now apply Theorem 11 to obtain lower bound on the probability of safety as

$\mathbb{P}\{x_{x_0}(t) \notin X_u = \{10\} \text{ for all } t \in \mathbb{N} \mid x_0 = \{0.2\}\} \geq 0.79$.

Figure 2 shows how the probability bounds for safety in (16) is affected for different values of $k \leq 10$ and $\varepsilon \leq 0.1$, for a fixed value of c for $k > 1$ (for $k = 0$, we have $c = 0$). Ideally, to obtain a high probability bound for safety, one requires $k = 1$ and ε to be as small as possible. However, due to the restrictive nature of barrier certificate conditions when $k = 1$, the minimal obtained value of ε, even if exists, may be high. In such cases, by considering $k > 1$, one is still able to relax the barrier certificate conditions, allowing to further reduce the value of ε such that a higher and a more reliable, less conservative probability is obtained.

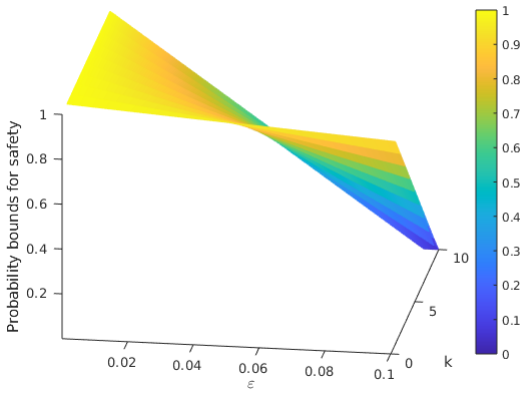


Figure 2: Variation of probability bounds for safety with respect to k and ε values

4 REACHABILITY VERIFICATION

4.1 Barrier Certificates for Reachability

The barrier certificates can be used to provide probabilistic guarantees for reachability properties under the following assumption that renders the system to be forward invariant in X.

Assumption 13. *For any solution process $\mathbf{x}_{x_0}$ of dt-SS $\mathfrak{S}$ starting from some initial state $x_0 \in X$, we have $\mathbf{x}_{x_0}(t) \in X$ for all $t \in \mathbb{N}$.*

Remark 14. *Assumption 13 can be supported by analyzing an auxiliary "stopped" process (see, e.g., [29]). Given a solution process $\mathbf{x}_{x_0}$ of dt-SS $\mathfrak{S}$, we define a stopped process $\bar{\mathbf{x}}_{x_0}$ as*

$$\bar{\mathbf{x}}_{x_0}(t) = \begin{cases} \mathbf{x}_{x_0}(t), & \text{for } t < \tau, \\ \mathbf{x}_{x_0}(\tau - 1), & \text{for } t \geq \tau, \end{cases}$$

where $\tau \in \mathbb{N}$ is the first exit time of $\mathbf{x}_{x_0}$ from X. Note that the relevance of such an assumption has been demonstrated in [30]. Intuitively, this assumption is natural in many physical applications where state variables are naturally constrained to a compact set and do not leave this set in their operating envelope.

We present two definitions of barrier certificates for reachability with the help of Assumption 13. The first definition is a stochastic version of the one presented in [21, Theorem 3.5].

Definition 15. Consider a dt-SS $\mathfrak{S}$ that satisfies Assumption 13. Then, we say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a *barrier certificate* for a dt-SS $\mathfrak{S}$ with respect to a set of initial states $X_0 \subseteq X$ and a set of target states $X_R \subseteq X$ if there exist constants $0 \leq \varepsilon \leq 1$ and $\delta > 0$ such that the following conditions hold:

$$\mathcal{B}(x) \leq \varepsilon, \qquad \text{for all } x \in X_0, \tag{17}$$

$$\mathcal{B}(x) \geq 1, \qquad \text{for all } x \in \partial X \setminus \partial X_R, \tag{18}$$

$$\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] - \mathcal{B}(x) \leq -\delta, \qquad \text{for all } x \in \overline{X \setminus X_R}. \tag{19}$$

This definition can then be utilized to obtain a lower bound on the probability that a dt-SS $\mathfrak{S}$ satisfies the reachability specification over *unbounded-time* horizons.

Theorem 16. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (17)-(19) *with some $0 \leq \varepsilon \leq 1$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ reaches the target region X_R is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} \geq 1 - \varepsilon. \tag{20}$$

Remark 17. *Note that barrier certificates as in Definition 15 provide reach-while-avoid guarantees. They ensure that the system avoids the set $\partial X \setminus \partial X_R$ while reaching the set X_R with a probability of at least $1 - \varepsilon$. Given a set of unsafe states $X_u \subseteq X$, one can replace $\partial X \setminus \partial X_R$ with X_u in condition* (18) *to give a probabilistic guarantee of reaching the target set of states X_R while avoiding X_u.*

We next formulate another definition of barrier certificates for reachability when no unsafe region to avoid is provided. This formulation can provide stronger almost-sure guarantees and is analogous to supermartingale ranking functions used in [26, Definition 4.3.2].

Definition 18. Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 13 holds for $\mathfrak{S}$. Then, we say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a *barrier certificate* for $\mathfrak{S}$ with respect to a set of initial states $X \setminus X_R$ and a set of target states $X_R \subseteq X$ if there exist constants $\varepsilon, \delta > 0$, such that the following conditions hold:

$$\mathcal{B}(x) \geq \varepsilon, \qquad \text{for all } x \in X \setminus X_R, \tag{21}$$

$$\mathcal{B}(x) < \varepsilon, \qquad \text{for all } x \in X_R \text{ and} \tag{22}$$

$$\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] - \mathcal{B}(x) \leq -\delta, \qquad \text{for all } x \in X \setminus X_R. \tag{23}$$

Definition 18 can then be utilized to show that the dt-SS $\mathfrak{S}$ satisfies reachability specification with probability 1.

Theorem 19. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (21)-(23) *with some $\varepsilon > 0$. Then a solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X \setminus X_R$ reaches the target region X_R with probability* 1*, i.e.,*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} = 1. \tag{24}$$

The set of initial states for a system admitting barrier certificates as in Definition 18 can be anywhere within the set X. If a solution process starts in X_R, the system trivially satisfies the reachability specification. For a solution process that starts in $X \setminus X_R$, the existence of a barrier certificate guarantees convergence and reachability into X_R. However, in the case of barrier certificates as defined in Definition 15, one requires condition $X_0 \cap (\partial X \setminus \partial X_R) \neq \emptyset$. The reasoning for this is similar to that of Remark 6. It is also important to note that conditions (19) and (23) in Definitions 15 and 18, respectively, impose a stronger supermartingale condition than the one in Definition 4 for safety. The conditions (19) and (23) require a strict decrease in barrier certificate values. This ensures the convergence of barrier certificate so that it eventually reaches the target set.

Similar to the computation of barrier certificates for safety, one may search for barrier certificates for reachability according to Definitions 15 and 18 by restricting the barrier certificates to a certain parametric form and utilizing techniques such as SOS optimization or SMT solvers. Since conditions (19) and (23) requires the expected value of the barrier certificate to be strictly decreasing at every time

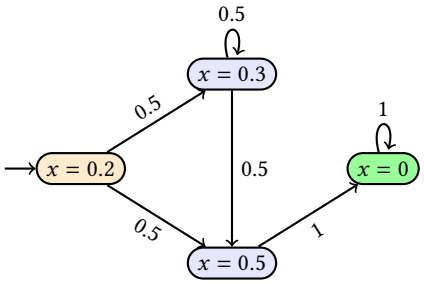


Figure 3: Finite Markov chain $\mathfrak{S}'$ for Example 20. The initial state is denoted in yellow and the target state in green.

step, it can be quite restrictive and one may fail to find appropriate barrier certificates even if the system satisfies the reachability specification. We now illustrate with an example that the barrier certificate approach fails to provide non-trivial probabilistic guarantees for a fixed template of barrier certificates even when the system satisfies the reachability almost surely.

Example 20. Consider a Markov chain shown in Figure 3 as a finite state stochastic system $\mathfrak{S}'$ with $x \in X = \{0, 0.2, 0.3, 0.5\}$ as states of the system, $x = 0.2$ as the initial state and $x = 0$ as the target state. It can be immediately seen that the solution processes of $\mathfrak{S}$ reach the target state with probability 1. However, we want to provide a barrier certificate of a fixed template to guarantee the satisfaction of the reachability specification with a non-trivial probability bound via Definition 15.

Consider a linear barrier certificate $\mathcal{B}(x) = ax + b$. Note that in the context of finite systems, if there are no states to avoid, we do not need to ensure condition (18) for any state in X. Now, according to condition (17), since $x = 0.2$ is the initial state, we get $0.2a + b \leq \varepsilon$. By applying the supermartingale condition (19) at $x = 0.2$, we get $\mathbb{E}[\mathcal{B}(f(x)) \mid x = 0.2] - \mathcal{B}(x) = 0.2a < -\delta$, implying that $a < 0$. Similarly, applying condition (19) at $x = 0.5$, we get $\mathbb{E}[\mathcal{B}(f(x)) \mid x = 0.5] - \mathcal{B}(x) = -0.5a < -\delta$ implying that $a > 0$, which results in a contradiction. Therefore there exists no linear barrier certificate satisfying conditions (17)-(19) for any value of ε and we cannot give a non-trivial probability of reachability with a linear barrier certificate as in Definition 15.

Similarly, consider a linear barrier certificate as in Definition 18. Note that condition (23) is the same as condition (19) for finite systems. So it also follows that there exists no linear barrier certificate satisfying condition (23) and we cannot ensure reachability with a linear barrier certificate as in Definition 18 as well.

The barrier certificates for reachability via Definitions 15 and 18 are also analogous to standard induction where conditions (17) and (19) as well as conditions (21) and (23) act as base cases and inductive steps for Definitions 15 and 18, respectively. Next, we consider k-inductive barrier certificates for reachability and show that they still provide unbounded-time guarantees.

4.2 k-Inductive Barrier for Reachability

In this section, we leverage k-inductive barrier certificates to obtain probabilistic guarantees for reachability specifications over unbounded-time horizons. To do this, one can relax the supermartingale condition imposed at every time step to a supermartingale requirement after k time steps, while necessitating a c-martingale condition at every time step. We first consider k-inductive barrier certificates based on Definition 15 as follows:

Definition 21. Consider a dt-SS $\mathfrak{S}$ that satisfies Assumption 13. We say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a k-inductive barrier certificate for dt-SS $\mathfrak{S}$ with respect to a set of initial states X_0 and a set of target states X_R if there exists constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$, $c \geq 0$ and $\delta > 0$ such that the following conditions hold:

$$\mathcal{B}(x) \leq \varepsilon, \qquad \text{for all } x \in X_0, \tag{25}$$

$$\mathcal{B}(x) \geq 1, \qquad \text{for all } x \in \partial X \setminus \partial X_R, \tag{26}$$

$$\mathbb{E}[\mathcal{B}(f(x, \varsigma)) \mid x] - \mathcal{B}(x) \leq c, \qquad \text{for all } x \in \overline{X \setminus X_R}, \tag{27}$$

$$\mathbb{E}[\mathcal{B}(f_k(x, \varsigma_k)) \mid x] - \mathcal{B}(x) \leq -\delta, \qquad \text{for all } x \in \overline{X \setminus X_R}. \tag{28}$$

Note that condition (27) requires the barrier certificate to be a c-martingale at every time step and condition (28) requires the barrier certificate sampled after every kth step to be decreasing in expectation for all states not in the set of target states.

Now, we present the second key result of our paper based on this definition of k-inductive barrier certificates.

Theorem 22. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (25)-(28) *with some $0 \leq \varepsilon \leq 1$, $c \geq 0$, $\delta > 0$ and $k \in \mathbb{N}_{\geq 1}$. Then the probability the the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ reaches the target region X_R is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} \geq 1 - k\varepsilon - \frac{k(k-1)c}{2}. \tag{29}$$

Note again that, when $k = 1$ and $c = 0$, conditions (25)-(28) converge to standard barrier certificate conditions (17)-(19). One then also observes that the probability bounds in (29) converge to those in (20) under the same conditions. Therefore, any barrier certificate satisfying conditions (17)-(19) is also a 1-inductive barrier certificate as in Definition 21.

Remark 23. *The probability bounds for reachability obtained in* (29) *are the same as the ones obtained for safety in* (16)*. This is due to the fact that we leverage the reach-while-avoid nature of conditions* (25)-(28)*, which ensure that the system avoids the set $\partial X \setminus \partial X_R$, and then utilizes Doob's martingale convergence [31] to ensure that the system reaches the target set X_R with a probability lower bound in* (29)*.*

We now illustrate k-inductive barrier certificates as in Definition 15 with the Markov Chain considered in Example 20.

Example 20 (Continued). Consider the finite Markov chain $\mathfrak{S}'$ of Figure 3. We already showed that there exists no linear barrier certificate as in Definition 15 for any $0 \leq \varepsilon < 1$. Now, we show that by using k-inductive barrier certificates as in Definition 21, we get more reliable probability bounds for the satisfaction of reachability.

Consider $\mathcal{B}(x) = 0.1x + 0.01$, constants $\varepsilon = 0.03$, $c = 0.02$, and $k = 3$. The enumerated values of $\mathcal{B}(x), \mathbb{E}[\mathcal{B}(f(x, \varsigma) \mid x]$, $\mathbb{E}[\mathcal{B}(f_2(x, \varsigma_2)) \mid x]$ and $\mathbb{E}[\mathcal{B}(f_3(x, \varsigma_3)) \mid x]$ for all states $x \in X$ are provided in Table 2. We immediately see that condition (25) is satisfied for the initial state $x = 0.2$. As we deal with a finite state system, and there are no states to avoid, there is no need to ensure the satisfaction of condition (18). It can be seen that conditions (27) and (28) also hold for all $x \in X$. Therefore, $\mathcal{B}(x) = 0.1x + 0.01$

x	$\mathcal{B}(x)$	$\mathbb{E}[\mathcal{B}(f(x,\varsigma))\,\vert x]$	$\mathbb{E}[\mathcal{B}(f_2(x,\varsigma_2))\,\vert x]$	$\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3))\,\vert x]$
0.2	0.03	0.05	0.03	0.02
0.3	0.04	0.05	0.03	0.02
0.5	0.06	0.01	0.01	0.01
0	0.01	0.01	0.01	0.01

Table 2: The values of $\mathbb{E}[\mathcal{B}(f_i(x,\varsigma_i)) \mid x]$ for all $i \in \{1,2,3\}$ and all $x \in X$ for Example 20. Note that $\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3)) \mid x] < \mathcal{B}(x)$ for all $x \in \overline{X \setminus X_R}$

x	$\mathcal{B}(x)$	$\mathbb{E}[\mathcal{B}(f(x,\varsigma))\,\vert x]$	$\mathbb{E}[\mathcal{B}(f_2(x,\varsigma_2))\,\vert x]$	$\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3))\,\vert x]$
0.2	0.29	0.49	0.29	0.19
0.3	0.39	0.49	0.29	0.19
0.5	0.59	0.09	0.09	0.09
0	0.09	0.09	0.09	0.09

Table 3: The values of $\mathbb{E}[\mathcal{B}(f_i(x,\varsigma_i)) \mid x]$ for all $i \in \{1,2,3\}$ and all $x \in X$ for Example 20. Note that $\mathbb{E}[\mathcal{B}(f_3(x,\varsigma_3)) \mid x] < \mathcal{B}(x)$ for all $x \in X \setminus X_R$.

is indeed a linear 3-inductive barrier certificate for $\mathfrak{S}$. We apply Theorem 22 to obtain lower bound on reachability probability as:

$$\mathbb{P}\{x_{x_0}(t) \in X_R = \{0\} \text{ for some } t \in \mathbb{N} \mid x_0 = \{0.2\}\} \geq 0.85,$$

which provides better guarantees than the linear barrier certificate.

We now extend barrier certificates for reachability as in Definition 18 to k-inductive barrier certificates presented below.

Definition 24. Consider a dt-SS $\mathfrak{S}$ that satisfies Assumption 13. We say that a function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is a k-inductive barrier certificate for $\mathfrak{S}$ with respect to a set of initial states $X \setminus X_R$ and a set of target states X_R if there exist constants $k \in \mathbb{N}_{\geq 1}$, $\varepsilon \geq 0$, $c \geq 0$ and $\delta > 0$ such that the following conditions hold:

$$\mathcal{B}(x) \geq \varepsilon, \qquad \text{for all } x \in X \setminus X_R, \tag{30}$$
$$\mathcal{B}(x) < \varepsilon, \qquad \text{for all } x \in X_R, \tag{31}$$
$$\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] - \mathcal{B}(x) \leq c \qquad \text{for all } x \in X \setminus X_R, \tag{32}$$
$$\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] - \mathcal{B}(x) \leq -\delta \qquad \text{for all } x \in X \setminus X_R. \tag{33}$$

Similar to Definition 18, condition (32) requires the barrier certificate to be a c-martingale at every time step and condition (33) requires the barrier certificate sampled after every kth step to be decreasing in expectation for those states not in the set of target states. We now present the third result of our paper based on this definition of k-inductive barrier certificates.

Theorem 25. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (30)-(33) *with some $\varepsilon, c \geq 0$, $\delta > 0$, and $k \in \mathbb{N}_{\geq 1}$. Then a solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X \setminus X_R$ reaches the target region X_R with probability* 1*, i.e.,*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} = 1. \tag{34}$$

Remark 26. *The existence of barrier certificates as in Definition 18 gives a probability of* 1 *for reachability. This bound is independent of the values of the constants k, ε, c and δ. Therefore these constants can be set to any value that is greater than* 0 *and still give an almost sure guarantee of reachability to the target set.*

Note that when $c < 0$ and $k = 1$, conditions (30)-(33) reduce to standard barrier conditions (21)-(23). Therefore any barrier certificate satisfying conditions (21)-(23) is also a 1-inductive barrier certificate as in Definition 18. However, the converse may not hold true, as conditions (30)-(33) are more relaxed. We now illustrate k-inductive barrier certificates as in Definition 24 with the Markov chain considered in Example 20.

Example 20 (Continued). We once again consider the finite Markov chain $\mathfrak{S}'$ presented in Figure 3. We show that by using k-inductive barrier certificates as in Definition 24, we get that $\mathfrak{S}'$ satisfies the reachability specification with probability 1. Consider $\mathcal{B}(x) = x + 0.09$, constants $\varepsilon = 0.1$, and $c = 0.2$, and $k = 3$. The enumerated values of $\mathcal{B}(x)$, $\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x]$ and $\mathbb{E}[\mathcal{B}(f_2(x,\varsigma_2)) \mid x]$ are provided in Table 3. We immediately observe that conditions (30) is satisfied for all states except $x = 0$ and similarly, condition (31) holds for the target state $x = 0$. Lastly conditions (32) and (33) also hold for all $x \in X \setminus X_R$. Therefore $\mathcal{B}(x) = x + 0.09$ is indeed a linear 3-inductive barrier certificate for $\mathfrak{S}'$. This allows one to conclude that the system reaches the state $x = 0$ with probability 1.

5 BARRIER COMPUTATION VIA SOS

In general, computation of k-inductive barrier certificates is a hard problem. However, under certain assumptions on the underlying dynamics as well as the safe, unsafe or target sets of the system, one can utilize existing computational methods to approach this problem. We provide an approach to synthesize k-inductive barrier certificates for stochastic dynamical systems by utilizing a sum-of-squares (SOS) programming approach. This approach can be adopted under the assumption that the underlying dynamics are polynomial and the regions of interest are semi-algebraic[32] and can be described by polynomials. We first state the required assumption that is used in the remainder of this section.

Assumption 27. *The dt-SS $\mathfrak{S}$ has a continuous state set X and the function $f : X \times V_\varsigma \to X$ is polynomial in the state variable x and noise variable ς. Moreover, the sets X, X_0, X_u and X_R are semi-algebraic.*

A semi-algebraic set $A \subseteq \mathbb{R}^n$ can be defined with the help of a vector of polynomials $h(x)$, *i.e.*, the set $A = \{x \in \mathbb{R}^n \mid h(x) \geq 0\}$ where the inequalities are presented element-wise. Under the assumption that X and X_R are semi-algebraic, we also have that the sets $\partial X \setminus \partial X_R$, $\overline{X \setminus X_R}$ and $X \setminus X_R$ are semi-algebraic. In the rest of this section, we consider the vector of polynomials $g(x), g_0(x)$, and $g_u(x)$ for the sets X, X_0, and X_u respectively, and use the vector of polynomials $g_r(x), g_b(x), g_c(x)$ and $g_z(x)$ for the sets $X_R, \partial X \setminus \partial X_R, \overline{X \setminus X_R}$, and $X \setminus X_R$ respectively.

5.1 SOS Optimization for Safety

For the synthesis of appropriate k-inductive barrier certificates for safety as in Definition 10, one can compile conditions (12)-(15) as a sum-of-squares optimization [27] problem under Assumption 27. The collection of sum-of-squares constraints corresponding to conditions (12)-(15) can be obtained by employing the following lemma.

Lemma 28. *Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 27 holds and there exists a sum-of-squares polynomial $\mathcal{B}(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$ and $c \geq 0$, and vectors of sum-of-squares polynomials*

$\lambda(x), \hat{\lambda}(x), \lambda_0(x)$, and $\lambda_u(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:

$$-\mathcal{B}(x) - \lambda_0^T(x)g_0(x) + \varepsilon, \tag{35}$$

$$\mathcal{B}(x) - \lambda_u^T(x)g_u(x) - 1, \tag{36}$$

$$-\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] + \mathcal{B}(x) - \lambda^T(x)g(x) + c, \tag{37}$$

$$-\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] + \mathcal{B}(x) - \hat{\lambda}^T(x)g(x). \tag{38}$$

Then the function $\mathcal{B}(x)$ is a k-inductive barrier certificate as in Definition 10 satisfying conditions (12)-(15).

5.2 SOS Optimization for Reachability

We now utilize Assumption 27 to formulate k-inductive barrier certificates for reachability as in Definition 21 as a collection of sum-of-squares constraints corresponding to conditions (25)-(28), which can be obtained by employing the following lemma.

Lemma 29. *Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 27 holds and there exists a sum-of-squares polynomial $\mathcal{B}(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$, $\delta > 0$, and $c \geq 0$, and vectors of sum-of-squares polynomials $\lambda_0(x), \lambda_b(x), \lambda_c(x)$ and $\hat{\lambda}_c(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$-\mathcal{B}(x) - \lambda_0^T(x)g_0(x) + \varepsilon, \tag{39}$$

$$\mathcal{B}(x) - \lambda_b^T(x)g_b(x) - 1, \tag{40}$$

$$-\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] + \mathcal{B}(x) - \lambda_c^T(x)g_c(x) + c, \tag{41}$$

$$-\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] + \mathcal{B}(x) - \hat{\lambda}_c^T(x)g_c(x) - \delta. \tag{42}$$

Then function $\mathcal{B}(x)$ is a k-inductive barrier certificate as in Definition 24 satisfying conditions (30)-(33).

Similarly one may use the following lemma to find k-inductive barrier certificates for reachability according to Definition 24.

Lemma 30. *Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 27 holds and there exists a sum-of-squares polynomial $\mathcal{B}(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$, $\delta > 0$, and $c \geq 0$, and vectors of sum-of-squares polynomials $\lambda_r(x), \lambda_c(x), \hat{\lambda}_c(x)$ and $\bar{\lambda}_c(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$\mathcal{B}(x) - \bar{\lambda}_c^T(x)g_z(x) - \varepsilon, \tag{43}$$

$$-\mathcal{B}(x) - \lambda_r^T(x)g_r(x) + \varepsilon - \epsilon, \tag{44}$$

$$-\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] + \mathcal{B}(x) - \lambda_c^T(x)g_z(x) + c, \tag{45}$$

$$-\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] + \mathcal{B}(x) - \hat{\lambda}_c^T(x)g_z(x) - \delta, \tag{46}$$

where ϵ is a small positive constant used to ensure the satisfaction of strict inequality (31). *Then the function $\mathcal{B}(x)$ is a k-inductive barrier certificate as in Definition 24 satisfying conditions* (30)-(33).

Remark 31. *The expected value $\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x]$ in Lemmas 28-30 can be evaluated when the probability distribution of the stochastic variable ς is known by considering all the monomials of the polynomial expression $\mathcal{B}(f_k(x,\varsigma_k))$ and utilizing the moments of the distribution of ς. For a Gaussian distribution, this can be done in linear time.*

Remark 32. *The SOS optimization problem is solved by fixing the degree d of the polynomial function $\mathcal{B}(x)$ along with the value of k. In general, if one cannot find a suitable function $\mathcal{B}(x)$ that satisfies the required constraints, one needs to solve the problem with a higher degree polynomial $\mathcal{B}(x)$ or a higher value of k. Note that for a fixed state dimension, the computational complexity grows polynomially with respect to d [27], and only linearly with k. Therefore, it would be more beneficial to use k-inductive barrier certificates with higher values of k than higher values of d.*

6 CASE STUDIES

6.1 Safety of an RLC circuit

In this case study, we study the safety property of a series RLC circuit. The dynamics of the dt-SS $\mathfrak{S}$ are given as

$$\mathfrak{S}: \begin{cases} i(t+1) = i(t) + \tau_s(-\frac{R}{L}i(t) + -\frac{1}{L}v(t)) + G\varsigma(t), \\ v(t+1) = v(t) + \tau_s\frac{1}{C}i(t), \end{cases} \tag{47}$$

where $i(t)$ denotes the current at time t, $v(t)$ is the voltage, $\tau_s = 0.5s$ is the sampling time, $R = 2\Omega$ is the series resistance, $L = 9$H is the series inductance, $C = 0.5$F is the capacitance of the circuit, and $G = 0.004$ is the noise coefficient. The state space of the system is given as $X = [-2, 2] \times [-4, 4]$, where the initial set $X_0 = [0, 0.5] \times [0, 1]$ and the unsafe set $X_u = [1, 2] \times [-4, 4]$.

We aim to utilize barrier certificates for safety as in Definition 4 to find the probability bound with which $\mathfrak{S}$ satisfies the safety property. To do so, we first consider the barrier certificate to be a polynomial of degree 6, and use the SOS programming toolbox YALMIP [33] version R20200930 along with SeDuMi [34] version 1.3 on MATLAB R2019b to search for a suitable barrier certificate satisfying conditions (3)-(5). However, we fail to find a supermartingale that achieves any meaningful probability of satisfaction.

We now compute a suitable polynomial k-inductive barrier certificate of degree 6 as in Definition 4 by reformulating conditions (12)-(15) as an SOS problem via Lemma 28. By considering $k = 2$, $\varepsilon = 0.029$ and $c = 10^{-4}$, we get a barrier certificate of degree 6 satisfying conditions (12)-(15). By Theorem 11, we can infer that the system $\mathfrak{S}$ satisfies the safety specification with a probability of at least 0.9419 for unbounded time. In comparison, by utilizing c-martingale barrier certificates as in Definition 8 for the same value of ε and c, by utilizing Theorem 9, one would obtain the probability of 0.9419 for a bounded time of 4564.5 seconds. Figures 4 shows the current and voltage for 50 representative solution processes starting from different initial conditions inside X_0. The computation time for this approach using the tools above is about 40 seconds on a machine running with Linux Ubuntu OS (Intel i7 − 8665U CPU with 32GB of RAM).

6.2 Reachability for Thermal Model of a Room

In this case study, we consider reachability specification for the temperature evolution of a room. The thermal model for the room is adapted from [24]. The dynamics of the dt-SS $\mathfrak{S}$ are given as

$$\mathfrak{S}: x(t+1) = (1 - \tau_s\alpha)x(t) + \tau_s\alpha T_e + G\varsigma(t),$$

where $\alpha = 0.01$ is the heat exchange coefficient, $T_e = 17$ is the ambient temperature, $\tau_s = 5$ minutes is the sampling time and $G = 0.05$ is the noise coefficient. The state space of the system

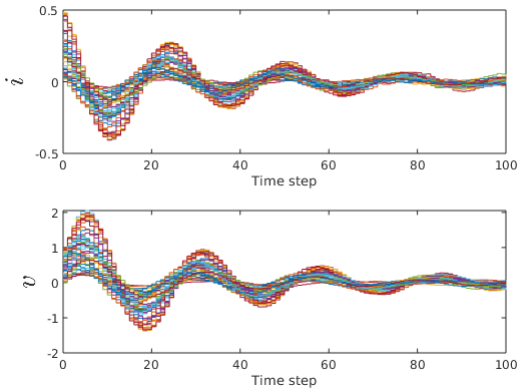
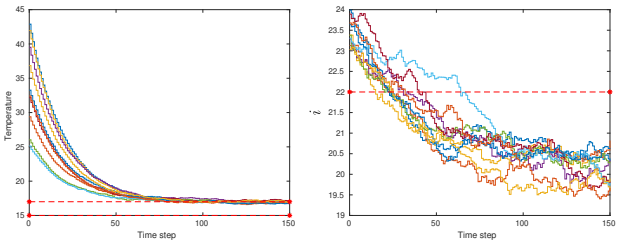


Figure 4: Solution processes of $\mathfrak{S}$ from Section 6.1 with respect to current i and voltage v from different initial states.



(a) **(b)**

Figure 5: (a) Solution processes of $\mathfrak{S}$ from Section 6.2, starting from different initial states in $X \setminus X_R$. (b) Solution processes of $\mathfrak{S}'$ from Section 6.2. In both figures, the set X_R is highlighted by red dashed lines

is given as $X = [15, 35]$, whereas the target set is specified as $X_R = [15, 17]$. We aim to utilize barrier certificates for reachability as in Definition 18 to verify whether $\mathfrak{S}$ satisfies reachability with probability 1. To do so, we first consider the barrier certificate to be a polynomial of degree 2, and search for a suitable barrier certificate satisfying conditions (21)-(23) by considering $X \setminus X_R = [17 + \vartheta, 35]$, where $\vartheta = 0.001$, and reformulating them into SOS constraints with tolerance parameters $\epsilon, \delta = 0.01$. However, we fail to find a suitable barrier certificate satisfying conditions (21)-(23). Therefore, using standard barrier certificates for reachability according to Definition 18, one cannot verify whether $\mathfrak{S}$ satisfies reachability with probability 1.

Instead, let us compute a suitable polynomial k-inductive barrier certificate of degree 2 as in Definition 24. We can reformulate conditions (30)-(33) as an SOS problem via Lemma 30. Setting $k = 11$, $\varepsilon = 1300$, $c = 0.001$, and $\delta = 0.01$, we obtain $\mathcal{B}(x) = 166.5118 + 34.7652x + 1.8769x^2$ as a k-inductive barrier certificate satisfying conditions (43)-(46) with a tolerance parameter $\epsilon = 0.01$. These computations take 15 seconds on our reference machine. From Lemma 30 and Theorem 25, it follows that the system $\mathfrak{S}$ indeed satisfies the reachability specification with probability 1. Figure 5a shows 10 representative solution processes starting from different initial conditions inside $X \setminus X_R$.

We now modify the parameters of the dynamics and consider a system $\mathfrak{S}'$ such that we can find standard barrier certificates satisfying Definition 15. Consider $\alpha = 0.004$, $T_e = 20$, $\tau_s = 5$ and $G = 0.08$ as the noise coefficient. The state space of the system is $X = [18, 45]$, the initial set of states $X_0 = [23, 24]$ and the target set $X_R = [18, 22]$. We first consider the barrier certificate to be a polynomial of degree 2 and search for a suitable barrier certificate satisfying conditions (17)-(19) by considering the sets $\partial X \setminus \partial X_R = [44 + \vartheta, 45]$, where $\vartheta = 0.01$, and $\overline{X \setminus X_R} = [22, 45]$, and reformulate them into SOS constraints with $\delta = 0.001$. We find a barrier certificate $\mathcal{B}(x) = 0.3658 - 0.05066x + 0.0018x^2$ satisfying conditions (17)-(28) for $\varepsilon = 0.24$. Thus, by utilizing Theorem 16, we get the lower bound on the probability of satisfying reachability as 0.76. We now consider a k-inductive barrier certificate as in Definition 21. For $k = 2$, $\varepsilon = 0.054$, $c = 0.0001$, and $\delta = 0.001$, we obtain $\mathcal{B}(x) = 1.1837 - 0.1196x + 0.003x^2$ as a k-inductive barrier certificate satisfying conditions (39)-(42). Then, by utilizing Theorem 22, we can say the system $\mathfrak{S}'$ satisfies the reachability specification with a probability of at least 0.89 which is greater than the lower bound obtained by using standard barrier certificates. This illustrates that even when standard barrier certificates exist, we may obtain more reliable probabilities for satisfaction with k-inductive barrier certificates (cf. Remark 23). Figure 5b shows 10 representative solution processes starting from X_0. The computation time for this approach is about 7 seconds with the mentioned tools and machine.

7 CONCLUSION

We introduce and study k-inductive barrier certificates to obtain probabilistic guarantees for the satisfaction of safety and reachability properties for discrete-time stochastic dynamical systems. We showed that one can relax the strong supermartingale condition of standard barrier certificates and still provide lower bounds on the probability of satisfaction for unbounded-time horizons. Using illustrative examples, we noted that k-inductive barrier certificates give reliable probabilities, even when standard barrier certificates of the same template fail to do so. We presented approaches to synthesize k-inductive barrier certificates using sum-of-squares programming and experimentally demonstrated their effectiveness. A potential next step is to investigate the utility of k-inductive barrier certificates in controller synthesis.

ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation (NSF) under grant ECCS-2015403 and in part by the German Research Foundation (DFG) through Research Training Group 2428.

REFERENCES

[1] A. Chakarov and S. Sankaranarayanan, "Expectation invariants for probabilistic program loops as fixed points," in *International Static Analysis Symposium*. Springer, 2014, pp. 85–100.
[2] J. Steinhardt and R. Tedrake, "Finite-time regional verification of stochastic nonlinear systems," *The International Journal of Robotics Research*, vol. 31, no. 7, pp. 901–923, 2012.
[3] A. F. Donaldson, L. Haller, D. Kroening, and P. Rümmer, "Software verification using k-induction," in *Static Analysis*, ser. Lecture Notes in Computer Science, 2011, pp. 351–368.

[4] M. Brain, S. Joshi, D. Kroening, and P. Schrammel, "Safety verification and refutation by k-Invariants and k-Induction," in *Static Analysis*, ser. Lecture Notes in Computer Science, 2015, pp. 145–161.

[5] S. Bak, "t-Barrier certificates: a continuous analogy to k-induction," in *6th IFAC Conference on Analysis and Design of Hybrid Systems*, 2018, pp. 145–150.

[6] S. Gao, J. Kapinski, J. Deshmukh, N. Roohi, A. Solar-Lezama, N. Arechiga, and S. Kong, "Numerically-robust inductive proof rules for continuous dynamical systems," in *Computer Aided Verification*, ser. Lecture Notes in Computer Science, 2019, pp. 137–154.

[7] M. Anand, V. Murali, A. Trivedi, and M. Zamani, "Safety verification of dynamical systems via k-inductive barrier certificates," in *60th Conference on Decision and Control*, 2021.

[8] 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*, vol. 52, pp. 1415–1428, 2007.

[9] C. Baier and J.-P. Katoen, *Principles of Model Checking*. MIT press, 2008.

[10] J.-C. Filliâtre, "Deductive software verification," *International Journal on Software Tools for Technology Transfer*, vol. 13, no. 5, p. 397, 2011. [Online]. Available: https://doi.org/10.1007/s10009-011-0211-0

[11] S. Soudjani, *Formal abstractions for automated verification and synthesis of stochastic systems*, ser. PhD thesis, Delft University of Technology, 2014.

[12] M. Lahijanian, S. B. Andersson, and C. Belta, "Formal verification and synthesis for discrete-time stochastic systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 8, pp. 2031–2045, 2015.

[13] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[14] M. Kattenbelt, M. Kwiatkowska, G. Norman, and D. Parker, "A game-based abstraction-refinement framework for Markov decision processes," *Formal Methods in System Design*, vol. 36, no. 3, pp. 246–280, 2010.

[15] E. Hahn, G. Norman, D. Parker, B. Wachter, and L. Zhang, "Game-based abstraction and controller synthesis for probabilistic hybrid systems," in *Eighth International Conference on Quantitative Evaluation of SysTems*, 2011, pp. 69–78.

[16] B. Xue, R. Li, N. Zhan, and M. Fränzle, "Reach-avoid analysis for stochastic discrete-time systems," in *American Control Conference*, 2021, pp. 4879–4885.

[17] B. Xue, N. Zhan, and M. Fränzle, "Inner-approximating reach-avoid sets for discrete-time polynomial systems," in *IEEE Conference on Decision and Control*, 2020, pp. 867–873.

[18] A. Tiwari, H. Rueß, H. Saïdi, and N. Shankar, "A technique for invariant generation," in *Proceedings of the 7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, 2001, p. 113–127.

[19] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*, 3rd ed. The MIT Press, 2009.

[20] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117–126, 2006.

[21] S. Prajna and A. Rantzer, "Convex programs for temporal verification of nonlinear dynamical systems," *SIAM Journal on Control and Optimization*, vol. 46, 2007.

[22] A. Kivilicim, O. Karabacak, and R. Wisniewski, "Safe reachability verification of nonlinear switched systems via a barrier density," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 2368–2372.

[23] C. Huang, X. Chen, W. Lin, Z. Yang, and X. Li, "Probabilistic safety verification of stochastic hybrid systems using barrier certificates," vol. 16, no. 5s, 2017.

[24] P. Jagtap, S. Soudjani, and M. Zamani, "Temporal logic verification of stochastic systems using barrier certificates," in *Proceedings of the International Symposium on Automated Technology for Verification and Analysis*, 2018, pp. 177–193.

[25] S. Yaghoubi, K. Majd, G. Fainekos, T. Yamaguchi, D. Prokhorov, and B. Hoxha, "Risk-bounded control using stochastic barrier functions," *IEEE Control Systems Letters*, vol. 5, pp. 1831–1836, 2021.

[26] A. Chakarov, *Deductive verification of infinite-state stochastic systems using martingales*, ser. PhD thesis, University of Colorado Boulder, 2016.

[27] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical Programming*, vol. 96, pp. 293–320, 2003.

[28] L. De Moura and N. Bjørner, "Satisfiability modulo theories: Introduction and applications," *Commun. ACM*, vol. 54, p. 69–77, 2011.

[29] H. J. Kushner, *Stochastic Stability and Control*, ser. Mathematics in Science and Engineering. Elsevier Science, 1967.

[30] J. P. Hespanha, "Modeling and analysis of networked control systems using stochastic hybrid systems," *Annual Reviews in Control*, vol. 38, no. 2, 2014.

[31] J. L. Doob, *Stochastic Processes*. John Wiley and Sons, 1953.

[32] J. Bochnak, M. Coste, and M.-F. Roy, *Real Algebraic Geometry*. Springer-Verlag, 1998.

[33] J. Löfberg, "Yalmip : A toolbox for modeling and optimization in matlab," in *IEEE International Conference on Robotics and Automation*, 2004, pp. 284–289.

[34] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization methods and software*, vol. 11, no. 1-4, pp. 625–653, 1999.

A APPENDIX

A.1 Proofs from Section 3

THEOREM 5. *[8] Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$. Let $\mathcal{B}$ be a barrier certificate satisfying conditions* (3)-(5) *for some $0 \leq \varepsilon \leq 1$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ does not reach unsafe region X_u is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0\} \geq 1 - \varepsilon. \tag{6}$$

PROOF. According to the condition (4), $X_u \subseteq \{x \in X \mid \mathcal{B}(x) \geq 1\}$. Therefore, it follows that

$$\mathbb{P}\{x(t) \in X_u \text{ for some } t \in \mathbb{N} \mid x_0\} \leq \mathbb{P}\{\sup_{t\in\mathbb{N}} \mathcal{B}(x(t)) \geq 1 \mid x_0\}. \tag{48}$$

Now, due to condition (5), we have that $\mathcal{B}$ is a non-negative supermartingale, and from [29, Theorem 12, Chapter II] it follows that

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_u \text{ for some } t \in \mathbb{N} \mid x_0\} \leq \varepsilon.$$

By means of complementation, we obtain the lower bound of (6). □

THEOREM 9. *Consider a dt-SS $\mathfrak{S}$. Suppose $\mathcal{B}$ is a c-martingale barrier certificate for $\mathfrak{S}$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ does not reach unsafe region X_u within a finite time horizon $T \in \mathbb{N}$ is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \leq T \mid x_0\} \geq 1 - (\varepsilon + cT). \tag{10}$$

PROOF. The probability bounds in (10) follows directly by applying [29, Theorem 3, Chapter III] to (48) and employing conditions (7) and (9). □

THEOREM 11. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (12)-(15) *with some $0 \leq \varepsilon \leq 1$, $c \geq 0$, and $k \in \mathbb{N}_{\geq 1}$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ does not reach the unsafe region X_u is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin X_u \text{ for all } t \in \mathbb{N} \mid x_0\} \geq 1 - k\varepsilon - \frac{k(k-1)c}{2}. \tag{16}$$

PROOF. According to condition (13), $X_u \subseteq \{x \in X \mid \mathcal{B}(x) \geq 1\}$. Therefore, it follows that

$$\mathbb{P}\{x(k) \in X_u \text{ for some } k \in \mathbb{N} \mid x_0\} \leq \mathbb{P}\{\sup_{k\in\mathbb{N}} \mathcal{B}(x(k)) \geq 1 \mid x_0\}. \tag{49}$$

Now, for the dt-SS $\mathfrak{S}$, consider k systems sampled after every k steps, each starting from initial conditions $x_0, x(1), \ldots, x(k-1)$, respectively. The dynamics of these systems are obtained as

$$\begin{aligned} x(t+k) &= f_k(x(t), \varsigma_k(t)), \\ x(t+k+1) &= f_k(x(t+1), \varsigma_k(t+1)), \\ &\vdots \\ x(t+2k-1) &= f_k(x(t+k-1), \varsigma_k(t+k-1)). \end{aligned}$$

Due to condition (15), the barrier certificate $\mathcal{B}$ satisfies the supermartingale condition (5) for each of these systems. Now, by means of Boole's inequality and Theorem 5, we obtain

$$\mathbb{P}\{\sup_{t\in\mathbb{N}} \mathcal{B}(x(t)) \geq 1 \mid x_0\} \leq \sum_{i=0}^{k-1} \mathbb{P}\{\sup_{t=jk, j\in\mathbb{N}} \mathcal{B}(x(i+t)) \geq 1 \mid x(i)\} \leq \sum_{i=0}^{k-1} \mathbb{E}(\mathcal{B}(x(i)).$$

Now, from condition (12), we have that $\mathcal{B}(x_0) \leq \varepsilon$. Moreover, by applying law of total expectation and condition (14) recursively for each term in the right hand side of the above inequality, we get

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_u \text{ for some } t \in \mathbb{N} \mid x_0\} \leq \varepsilon + \sum_{i=1}^{k-1}(\varepsilon + ic) = k\varepsilon + \frac{k(k-1)c}{2}.$$

By complementing the above, we obtain the bound (16) on the probability such that the system satisfies the safety specification. □

A.2 Proofs from Section 4

Theorem 16. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (17)-(19) *with some $0 \leq \varepsilon \leq 1$. Then the probability that the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ reaches the target region X_R is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} \geq 1 - \varepsilon. \tag{20}$$

Proof. The solution processes of $\mathfrak{S}$ may either reach the boundary $\partial X \setminus \partial X_R$ without entering X_R, or may never reach $\partial X \setminus \partial X_R$ after reaching X_R. Now, due to conditions (17)-(19) and Theorem 5 with $X_u = \partial X \setminus \partial X_R$, one has a lower bound on the probability that the solution process $\mathbf{x}_{x_0}$ starting from x_0 does not reach the boundary set $\partial X \setminus \partial X_R$ as

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin \partial X \setminus \partial X_R \text{ for all } t \in \mathbb{N} \mid x_0\} \geq 1 - \varepsilon. \tag{50}$$

Now, under the condition that the solution processes do not enter $\partial X \setminus \partial X_R$, we can provide an almost sure guarantee that the solution process reaches the target set X_R. This is due to condition (19), which imposes a stronger supermartingale condition which requires a strict decrease in the expected value of the barrier certificate. Since the barrier certificate is bounded below (due to non-negativity), by the virtue of Doob's martingale convergence theorem [31], we have that the barrier certificate convergences almost surely to a state x where $\mathcal{B}(x)$ reaches its minimum value. Let $x \in \overline{X \setminus X_R}$. Then by condition (19), the expected value of barrier certificate must strictly decrease. However, this is not possible, and therefore, $x \notin \overline{X \setminus X_R}$ and the solution process $\mathbf{x}_{x_0}$ must leave $\overline{X \setminus X_R}$. Since the probability of not leaving $\overline{X \setminus X_R}$ via the boundary set $\partial X \setminus \partial X_R$ is greater than $1 - \epsilon$, the solution process $\mathbf{x}_{x_0}$ must leave the set $\overline{X \setminus X_R}$ by entering X_R with probability greater than $1-\varepsilon$. Therefore, we obtain the probability bound of (20). □

Theorem 19. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (21)-(23) *with some $\varepsilon > 0$. Then a solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X \setminus X_R$ reaches the target region X_R with probability* 1*, i.e.,*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} = 1. \tag{24}$$

Proof. Since the barrier certificate $\mathcal{B}$ is a non-negative supermartingale that is strictly decreasing due to condition (23), from Doob's martingale convergence theorem [31] it follows that the barrier certificate almost surely converges to some state x such that $\mathcal{B}(x)$ reaches its minimum value. Moreover, due to Assumption 13 and conditions (21) and (22), we have $x \in X_R$. Therefore, we have that a solution process $\mathbf{x}_{x_0}$ starting from $x_0 \in X_0$ eventually reaches X_R almost surely, which implies that $\mathbf{x}_{x_0}(t) \in X_R$ for some $t \in \mathbb{N}$ with probability 1, as obtained in (24). □

Theorem 22. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (25)-(28) *with some $0 \leq \varepsilon \leq 1$, $c \geq 0$, $\delta > 0$ and $k \in \mathbb{N}_{\geq 1}$. Then the probability the the solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X_0$ reaches the target region X_R is bounded by*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} \geq 1 - k\varepsilon - \frac{k(k-1)c}{2}. \tag{29}$$

Proof. The proof for this theorem can be obtained by utilizing Theorem 11 and Theorem 16. From Theorem 11 with $X_u = \partial X \setminus \partial X_R$, one has the probability that a solution process $\mathbf{x}_{x_0}$ of $\mathfrak{S}$ starting from $x_0 \in X$ does not enter the boundary set $\partial X \setminus \partial X_R$ is

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \notin \partial X \setminus \partial X_R \text{ for all } t \in \mathbb{N} \mid x_0\} \geq 1 - k\varepsilon - \frac{k(k-1)c}{2}. \tag{51}$$

Now, for $\mathfrak{S}$, consider k-systems sampled after every k steps, each starting from initial conditions $x_0, x(1), \ldots, x(k-1)$. From condition (28), we have that each of these k systems satisfy the supermartingale requirement, and therefore, from Doob's martingale convergence, it must be the case that the value of barrier certificate must converge to its minimum. Now, by utilizing a similar argument to that of Theorem 16, under the condition that the solution process does not enter the set $\partial X \setminus \partial X_R$, we have that the solution process must almost surely enter the target set X_R. Therefore, solution process $\mathbf{x}_{x_0}$ starting from $x_0 \in X_0$ reaches the target set X_R over unbounded-time horizons with a probability as obtained in (29).

□

Theorem 25. *Consider a dt-SS $\mathfrak{S} = (X, \varsigma, f)$ satisfying Assumption 13. Let $\mathcal{B}$ be a barrier certificate for $\mathfrak{S}$ satisfying conditions* (30)-(33) *with some $\varepsilon, c \geq 0$, $\delta > 0$, and $k \in \mathbb{N}_{\geq 1}$. Then a solution process $\mathbf{x}_{x_0}$ starting from an initial condition $x_0 \in X \setminus X_R$ reaches the target region X_R with probability* 1*, i.e.,*

$$\mathbb{P}\{\mathbf{x}_{x_0}(t) \in X_R \text{ for some } t \in \mathbb{N} \mid x_0\} = 1. \tag{34}$$

Proof. For the dt-SS $\mathfrak{S}$, consider k systems sampled after every k steps starting from initial conditions $x_0, x(1), \ldots, x(k-1)$

respectively. The dynamics of these systems are obtained as

$$\begin{aligned} x(t+k) &= f_k(x(t), \varsigma_k(t)), \\ x(t+k+1) &= f_k(x(t+1), \varsigma_k(t+1)), \\ &\vdots \\ x(t+2k-1) &= f_k(x(t+k-1), \varsigma_k(t+k-1)). \end{aligned}$$

Due to condition (33), the barrier certificate $\mathcal{B}$ satisfies the supermartingale condition (32) for each of these systems. Therefore the probability of each of these systems eventually reaching some state in X_R is 1 by Theorem 19, *i.e.*, each of these system eventually reach some state in X_R with probability 1. This implies that $\mathfrak{S}$ must satisfy the reachability specification with probability 1, as obtained in (34). □

A.3 Proofs from Section 5

Lemma 28. *Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 27 holds and there exists a sum-of-squares polynomial $\mathcal{B}(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$ and $c \geq 0$, and vectors of sum-of-squares polynomials $\lambda(x), \hat{\lambda}(x), \lambda_0(x)$, and $\lambda_u(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$-\mathcal{B}(x) - \lambda_0^T(x) g_0(x) + \varepsilon, \tag{35}$$

$$\mathcal{B}(x) - \lambda_u^T(x) g_u(x) - 1, \tag{36}$$

$$-\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] + \mathcal{B}(x) - \lambda^T(x) g(x) + c, \tag{37}$$

$$-\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] + \mathcal{B}(x) - \hat{\lambda}^T(x) g(x). \tag{38}$$

Then the function $\mathcal{B}(x)$ is a k-inductive barrier certificate as in Definition 10 satisfying conditions (12)-(15).

Proof. Note that $\lambda_0(x)$ is an SOS polynomial and so we have that $\lambda_0^T(x) g_0(x)$ is non-negative over the set X_0. If (35) is an SOS polynomial, and therefore non-negative, it implies the satisfaction of condition (12). Similarly, equations (36)-(38) imply (13)-(15), respectively. □

Lemma 29. *Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 27 holds and there exists a sum-of-squares polynomial $\mathcal{B}(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$, $\delta > 0$, and $c \geq 0$, and vectors of sum-of-squares polynomials $\lambda_0(x), \lambda_b(x), \lambda_c(x)$ and $\hat{\lambda}_c(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$-\mathcal{B}(x) - \lambda_0^T(x) g_0(x) + \varepsilon, \tag{39}$$

$$\mathcal{B}(x) - \lambda_b^T(x) g_b(x) - 1, \tag{40}$$

$$-\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] + \mathcal{B}(x) - \lambda_c^T(x) g_c(x) + c, \tag{41}$$

$$-\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] + \mathcal{B}(x) - \hat{\lambda}_c^T(x) g_c(x) - \delta. \tag{42}$$

Then function $\mathcal{B}(x)$ is a k-inductive barrier certificate as in Definition 24 satisfying conditions (30)-(33).

Proof. Since $\lambda_0(x)$ is an SOS polynomial, we have $\lambda_0^T(x) g_0(x)$ is non-negative over the set X_0. Therefore, if (39) is an SOS polynomial, and therefore non-negative, it implies the satisfaction of condition (25). Similarly equations (40)-(42) imply (26)-(28), respectively. □

Lemma 30. *Consider a dt-SS $\mathfrak{S}$. Suppose Assumption 27 holds and there exists a sum-of-squares polynomial $\mathcal{B}(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $0 \leq \varepsilon \leq 1$, $\delta > 0$, and $c \geq 0$, and vectors of sum-of-squares polynomials $\lambda_r(x), \lambda_c(x), \hat{\lambda}_c(x)$ and $\bar{\lambda}_c(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$\mathcal{B}(x) - \bar{\lambda}_c^T(x) g_z(x) - \varepsilon, \tag{43}$$

$$-\mathcal{B}(x) - \lambda_r^T(x) g_r(x) + \varepsilon - \epsilon, \tag{44}$$

$$-\mathbb{E}[\mathcal{B}(f(x,\varsigma)) \mid x] + \mathcal{B}(x) - \lambda_c^T(x) g_z(x) + c, \tag{45}$$

$$-\mathbb{E}[\mathcal{B}(f_k(x,\varsigma_k)) \mid x] + \mathcal{B}(x) - \hat{\lambda}_c^T(x) g_z(x) - \delta, \tag{46}$$

where ϵ is a small positive constant used to ensure the satisfaction of strict inequality (31). *Then the function $\mathcal{B}(x)$ is a k-inductive barrier certificate as in Definition 24 satisfying conditions* (30)-(33).

Proof. The proof follows in a similar fashion to the two previous lemmas, where conditions (43)-(46) model conditions (30)-(33). □