Reach-avoid Analysis for Stochastic Discrete-time Systems

Bai Xue[1], Renjue Li[1], Naijun Zhan[1] and Martin Fränzle[2]

***Abstract*— Stochastic discrete-time systems, i.e., discrete-time dynamic systems subject to stochastic disturbances, are an essential modelling tool for many engineering systems, and reach-avoid analysis is able to guarantee safety (i.e., via avoiding unsafe sets) and progress (i.e., via reaching target sets). In this paper we study the reach-avoid problem of stochastic discrete-time systems over open (i.e., not bounded a priori) time horizons. The stochastic discrete-time system of interest is modeled by iterative polynomial maps with stochastic disturbances, and the problem addressed is to effectively compute an inner approximation of its *p*-reach-avoid set. The *p*-reach-avoid set collects those initial states that give rise to a bundle of trajectories which with probability being larger than *p* eventually hits a designated set of target states while remaining inside a set of safe states before the first hit. The computation of the *p*-reach-avoid set is first reduced to the computation of a corresponding strict *p*-super-level set and is then inner-approximated by solving a semi-definite programming problem obtained from a relaxation of the definition of the super-level set. Two examples demonstrate the proposed approach.**

I. Introduction

Since the development of digital computers, the discrete-time perspective on system dynamics plays an important role in the control theory [12]. Discrete time differs from a continuous time view in that the signals take the form of sequences of samples. Such discrete-time systems arise as the result of sampling from a continuous-time system or when only discrete data are available [13]. Due to the inherent noise in sensors and other measurement errors, as well as due to partly unknown dynamics of the system, uncertainties in the samples and signals arise, which can conveniently be modelled in a probabilistic way using random variables and stochastic processes. This leads to discrete-time systems with stochastic disturbances (i.e., stochastic discrete-time systems). Stochastic discrete-time systems have obtained considerable attention among both control and computer scientists due to their capabilities for modeling many real-life systems.

Dynamic properties of interest, generally posed as system verification obligations, are the stability of an equilibrium, the invariance of a set, or controllability and observability [7]. This system verification perspective has recently been broadened, using formal methods [2], towards checking richer specifications of temporal behavior. An important instance is reach-avoid properties covering both safety (i.e., via avoiding unsafe sets) and progress (i.e., via reaching target sets). Such reach-avoid analysis has been applied in several domains such as motion planning in robotics [10], spacecraft docking [8] and autonomous surveillance [5]. In its *qualitative* form, it induces the problem of computing the maximal set of initial states such that the system starting from them is guaranteed to (eventually or within a given time horizon) reach a target set while avoiding an unsafe set till the target hit.

The verification of stochastic discrete-time systems, in contrast, induces a more complex *quantitative reach-avoid analysis* problem. Given an acceptance threshold in form of a probability p, it calls for assuring probabilistic success of the reach-avoid objective with at least the desired likelihood p, i.e., accepts initial states from which the probability of (eventually or within a given duration) reaching the target while avoiding the unsafe set exceeds p. Established methods for computationally solving this problem rely on dynamic programming [1], [14] and thus are computationally intractable for even moderately sized systems due to the gridding of both the state and disturbance spaces that is necessary to obtain a finite dynamic program. Recent work has focused on alternatives to dynamic programming, including approximate dynamic programming [6], semi-definite programs [3], and Lagrangian techniques [4]. These works are generally confined to reach-avoid problems of stochastic discrete-time systems over *bounded time horizons*.

This paper studies the reach-avoid problem of polynomial stochastic discrete-time dynamical systems over open time horizons and resolves it computationally within the framework of semi-definite programming. The reach-avoid problem of interest in this paper is to inner-approximate the *p*-reach-avoid set, which is the maximal set of initial states that each gives rise to a set of trajectories which, with a probability being larger than *p*, hit the target set in finite time while remaining inside the safe set beforehand. In our approach, a bounded value function whose strict *p* super-level set equals the *p*-reach-avoid set of interest is first constructed. The description of the super-level set then is reduced to a solution of a system of equations. Finally, via relaxing the equations to a system of inequalities and encoding the resulting inequalities into semi-definite constraints based on the sum-of-squares decomposition for multivariate polynomials, a semi-definite program is derived whose solutions approximate the *p*-reach-avoid set safely from the inner, i.e., represent a reliable subset of the proper initial states. Two examples demonstrate the proposed method.

The contributions of this paper thus are twofold:

1) We investigate the reach-avoid problem of stochastic discrete-time systems modeled by iterative polynomial

1 State Key Lab. of Computer Science, Institute of Software, CAS, and Univ. of Chinese Academy of Sciences, Beijing, China {xuebai,lirj19,znj}@ios.ac.cn

2 Carl von Ossietzky Universität Oldenburg, Oldenburg, Germany fraenzle@uni-oldenburg.de

maps subject to stochastic disturbances over open time horizons. Their p-reach-avoid sets are reduced to the strict p super-level set of a solution to a system of equations, which is an extension of our previous work [16] to a quantitative-verification setting: [16] in contrast studied the qualitative reach-avoid analysis for discrete-time polynomial systems free of disturbances.

2) A reduction to a semi-definite program is proposed to inner-approximate the above super-level set. The resultant semi-definite program falls within the convex-programming category and can be solved efficiently via interior point methods in polynomial time. Thus, the proposed method reduces an overall non-convex problem of computing p-reach-avoid sets to a problem of solving a single convex program.

This paper is structured as follows. In Section II we introduce stochastic discrete-time systems and the p-reach-avoid problem. After elaborating the reduction to semi-definite programming problems in Section III, we demonstrate it on two examples. Section V provides conclusions.

II. Preliminaries

We start our exposition by a formal introduction of discrete-time systems subject to stochastic disturbances and the corresponding p-reach-avoid sets of interest. Before posing the problem studied, let us introduce some basic notions used throughout this paper: $\mathbb{N}$ denotes the set of nonnegative integers. For a set Δ, Δ^c and $\partial\Delta$ denote the complement and the boundary of the set Δ, respectively. $\mathbb{R}[\cdot]$ denotes the ring of polynomials in variables given by the argument. Vectors are denoted by boldface letters. $\sum[\boldsymbol{x}]$ is used to represent the set of sum-of-squares polynomials over variables $\boldsymbol{x}$, i.e.,

$$\sum[\boldsymbol{x}] = \{q' \in \mathbb{R}[\boldsymbol{x}] \mid q' = \sum_{i=1}^{k'} q_i^2, q_i \in \mathbb{R}[\boldsymbol{x}], i = 1, \dots, k'\}.$$

In this paper we restrict our attention to the class of discrete-time systems subject to stochastic disturbances that can be modeled by iterative probabilistic maps of the following form:

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

where $\boldsymbol{x}(\cdot) : \mathbb{N} \to \mathcal{R}^n$ are states, and $\boldsymbol{\theta}(\cdot) : \mathbb{N} \to \Theta$ with $\Theta \subseteq \mathbb{R}^m$ are stochastic disturbances. In addition, suppose that $\boldsymbol{\theta}(0), \boldsymbol{\theta}(1), \dots$, are independent and identically distributed (i.i.d) random variables on a probability space $(\Theta, \mathcal{F}, \mathbb{P})$, and take values in Θ with the following probability distribution: for any measurable set $B \subseteq \Theta$,

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

$E[\cdot]$ is the expectation induced by the probability distribution $\mathbb{P}$. Also, we assume that $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})$ is polynomial over $\boldsymbol{x} \in \mathbb{R}^n$, and is measurable on Θ for each fixed $\boldsymbol{x}$.

Let $\Theta \times \Theta = \Theta^2$. Then, the twofold composition of the stochastic dynamical system, denoted by $\boldsymbol{f}^2 : \mathbb{R}^n \times \Theta^2 \to \mathbb{R}^n$, is given by

$$\boldsymbol{x}(l+2) = \boldsymbol{f}(\boldsymbol{f}(\boldsymbol{x}(l), \boldsymbol{\theta}(l)), \boldsymbol{\theta}(l+1)) := \boldsymbol{f}^2(\boldsymbol{x}(l), \boldsymbol{\theta}_l^{l+1}),$$

where $\boldsymbol{\theta}_l^{l+1} \in \Theta^2$. Since the sequence of random vectors $\{\boldsymbol{\theta}(l)\}$ is assumed i.i.d, the probability measure on Θ^2 will simply be the product measure, i.e., $\mathbb{P} \times \mathbb{P} := \mathbb{P}^2$. Similarly, the $(l+1)$-times composition, $\boldsymbol{f}^{l+1} : \mathbb{R}^n \times \Theta^{l+1} \to \mathbb{R}^n$, is denoted by $\boldsymbol{x}(l+1) = \boldsymbol{f}^{l+1}(\boldsymbol{x}(0), \boldsymbol{\theta}_0^l)$, where $\boldsymbol{\theta}_0^l \in \Theta^{l+1}$ with probability measure $\mathbb{P}^{l+1}$.

Before defining the trajectory of system (1), we define a disturbance policy controlling it.

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

A disturbance policy 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 policy π and an initial state $\boldsymbol{x}_0 \in \mathbb{R}^n$, a trajectory of system (1) is denoted as $\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(\cdot) : \mathbb{N} \to \mathbb{R}^n$ with $\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(0) = \boldsymbol{x}_0$, i.e.,

$$\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l+1) = \boldsymbol{f}(\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l), \boldsymbol{\theta}(l)), \forall l \in \mathbb{N}.$$

Given the safe set

$$\mathcal{X} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) < 0\}$$

and the target set

$$\mathcal{T} = \{\boldsymbol{x} \in \mathbb{R}^n \mid g(\boldsymbol{x}) \le 1\}$$

with $h(\boldsymbol{x}), g(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ and $\mathcal{T} \subseteq \mathcal{X}$, we define the p-reach-avoid set below.

Definition 3: The p-reach-avoid set RA_p is the set of all initial states that each gives rise to a set of trajectories which, with a probability being larger than $p \in [0,1)$, eventually enter the target set $\mathcal{T}$ while remaining inside the safe set $\mathcal{X}$ until the target hit, i.e.,

$$\mathrm{RA}_p = \left\{ \boldsymbol{x}_0 \in \mathcal{X} \;\middle|\; \begin{aligned} &\mathbb{P}^\infty \Big(\exists k \in \mathbb{N}. \boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{T} \bigwedge \\ &\qquad \forall l \in [0,k] \cap \mathbb{N}. \boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \Big) > p \end{aligned} \right\}.$$

An inner-approximation is a subset of the set RA_p.

Remark 1: The 0-reach-avoid set RA_0 is the set of all initial states that each gives rise to a set of trajectories which will enter the target set $\mathcal{T}$ in finite time while remaining inside the safe set $\mathcal{X}$ preceding the target hitting time with a probability being larger than 0. That is, there exists a non-empty set of disturbance policies $\pi \in \Pi$ such that system (1) originating from RA_0 will enter the target set $\mathcal{T}$ in finite time while remaining inside the safe set $\mathcal{X}$ preceding the target hitting time. *If the disturbance policy is replaced by the control policy, the set* RA_0 *is an inner-approximation of a controllable reach-avoid set.* This inner-approximation, however, requires a positive measure of the control set.

III. Inner-Approximating Reach-Avoid Sets

In this section we elucidate our semi-definite programming method for inner-approximating the p-reach-avoid set RA_p. The semi-definite program originates from a system of equations, which is obtained based on a bounded value function whose strict p super level set equals the set RA_p.

Similar to [16], we define a switched system, whose trajectories play a fundamental role in defining the bounded value function, for obtaining the bounded value function aforementioned whose strict p super-level set is equal to the p-reach-avoid set RA_p.

Definition 4: The switched discrete-time stochastic system (or, **SDSS**), 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;
- $\widehat{\boldsymbol{f}}(\cdot,\cdot) : \mathbb{R}^n \times \Theta \to \mathbb{R}^n$, 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) $\widehat{\mathcal{X}} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h_0(\boldsymbol{x}) \leq 0\}$ is a set satisfying $\widehat{\Omega} \subset \widehat{\mathcal{X}}$, where $h_0(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ and
$$\widehat{\Omega} = \{\boldsymbol{x} \in \mathbb{R}^n \mid \boldsymbol{x} = \boldsymbol{f}(\boldsymbol{x}_0,\boldsymbol{\theta}), \boldsymbol{x}_0 \in \mathcal{X}, \boldsymbol{\theta} \in \Theta\} \cup \mathcal{X};$$
2) $\widehat{\mathcal{X}}_1 = \mathcal{X} \setminus \mathcal{T} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) < 0 \wedge 1 - g(\boldsymbol{x}) < 0\}$;
3) $\widehat{\mathcal{X}}_2 = \mathcal{T} = \{\boldsymbol{x} \in \mathbb{R}^n \mid 1 - g(\boldsymbol{x}) \geq 0\}$;
4) $\widehat{\mathcal{X}}_3 = \widehat{\mathcal{X}} \setminus \mathcal{X} = \{\boldsymbol{x} \in \mathbb{R}^n \mid h(\boldsymbol{x}) \geq 0 \wedge h_0(\boldsymbol{x}) \leq 0\}$.

The evolution of the state of system **SDSS** is governed by the iterative map
$$\begin{aligned} &\boldsymbol{x}(l+1) = \widehat{\boldsymbol{f}}(\boldsymbol{x}(l), \boldsymbol{\theta}(l)), \forall l \in \mathbb{N}, \\ &\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \widehat{\mathcal{X}}. \end{aligned} \tag{2}$$

The trajectory of system **SDSS**, induced by initial state $\boldsymbol{x}_0 \in \widehat{\mathcal{X}}$ and disturbance policy $\pi \in \Omega$, is denoted by $\boldsymbol{\psi}_\pi^{\boldsymbol{x}_0}(\cdot) : [0,\infty) \to \mathbb{R}^n$. The set $\widehat{\mathcal{X}}$ is invariant for system **SDSS**, that is, trajectories of system **SDSS** originating from the set $\widehat{\mathcal{X}}$ will never leave it.

Corollary 1: If $\boldsymbol{x}_0 \in \widehat{\mathcal{X}}$ and $\pi \in \Omega$,
$$\boldsymbol{\psi}_\pi^{\boldsymbol{x}_0}(l) \in \widehat{\mathcal{X}}$$
for $l \in \mathbb{N}$ and $\pi \in \Omega$.

Proof: Since the sets $\widehat{\mathcal{X}}_2$ and $\widehat{\mathcal{X}}_3$ are positively invariant for system **SDSS**, and trajectories originating from the set $\mathcal{X} \setminus \mathcal{T}$ will hit either the set $\widehat{\mathcal{X}}_2$ or the set $\widehat{\mathcal{X}}_3$ if they would leave the set $\mathcal{X} \setminus \mathcal{T}$, it is easy to obtain the conclusion. ■

Clearly, the p-reach-avoid set RA_p is equal to the set of initial states enabling system **SDSS** to hit the target set $\mathcal{T}$ in finite time with a probability being larger than p. Given $\boldsymbol{x} \in \widehat{\mathcal{X}}$, let $t_{\mathcal{T}}^{\boldsymbol{x}}(\pi)$ be the hitting time of the target set $\mathcal{T}$ for the trajectory $\boldsymbol{\psi}_\pi^{\boldsymbol{x}}(\cdot) : [0,\infty) \to \mathbb{R}^n$, i.e.,
$$t_{\mathcal{T}}^{\boldsymbol{x}}(\pi) = \inf\{k \in \mathbb{N} \mid \boldsymbol{\psi}_\pi^{\boldsymbol{x}}(k) \in \mathcal{T}\}.$$

The p-reach-avoid set is the set of initial states rendering the hitting time $t_{\mathcal{T}}^{\boldsymbol{x}}$ less than ∞ with a probability being larger than p. This is formally stated in Lemma 1.

Lemma 1: $\mathrm{RA}_p = \{\boldsymbol{x} \in \mathcal{X} \mid \mathbb{P}^\infty(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi) < \infty) > p\}$, where RA_p is the p-reach-avoid set.

Proof: We just need to show that
$$\mathrm{RA}_p \setminus \mathcal{T} = \{\boldsymbol{x} \in \mathcal{X} \mid \mathbb{P}^\infty(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi) < \infty) > p\} \setminus \mathcal{T},$$
since $\boldsymbol{x} \in \mathcal{T}$ implies $\boldsymbol{\phi}_\pi^{\boldsymbol{x}}(0) = \boldsymbol{\psi}_\pi^{\boldsymbol{x}}(0) \in \mathcal{T}$ and thus
$$\begin{aligned} &\mathbb{P}^\infty(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi) < \infty) \\ &= \mathbb{P}^\infty(\exists k \in \mathbb{N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}}(k) \in \mathcal{T} \bigwedge \forall l \in [0,k] \cap \mathbb{N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}}(l) \in \mathcal{X}) \\ &= 1 > p. \end{aligned}$$

Let $\boldsymbol{x}_0 \in \mathrm{RA}_p \setminus \mathcal{T}$. According to Definition 3, we have that $\mathbb{P}^\infty(A) > p$, where
$$A = \left\{\pi \in \Omega \,\middle|\, \begin{aligned} &\exists k \in \mathbb{N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{T} \bigwedge \\ &\forall l \in [0,k] \cap \mathbb{N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \end{aligned}\right\}.$$
Let $B = \{\pi \in \Omega \mid t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) < \infty\}$.

Let $\pi \in A$ and
$$\widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) = \inf\left\{k \in \mathbb{N} \,\middle|\, \begin{aligned} &\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(k) \in \mathcal{T} \bigwedge \\ &\forall l \in [0,k] \cap \mathbb{N}.\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \end{aligned}\right\}.$$
Obviously, $\widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) < \infty$. We next show $t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) = \widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)$.

Since
$$\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \setminus \mathcal{T}, \forall l \in [0, \widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)) \cap \mathbb{N}$$
holds, according to Definition 4 we have that
$$\boldsymbol{\psi}_\pi^{\boldsymbol{x}_0}(l) = \boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \setminus \mathcal{T}, \forall l \in [0, \widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)) \cap \mathbb{N}.$$
Thus, $\widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) \leq t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)$.

On the other hand,
$$\boldsymbol{\psi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \setminus \mathcal{T}, \forall l \in [0, t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)) \cap \mathbb{N}.$$
According to Definition 4 we have that
$$\boldsymbol{\phi}_\pi^{\boldsymbol{x}_0}(l) = \boldsymbol{\psi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \setminus \mathcal{T}, \forall l \in [0, t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)) \cap \mathbb{N}.$$
Thus, $t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) \leq \widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)$.

Therefore, $\widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) = t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) < \infty$ and thus $\pi \in B$. Consequently, we have $A \subseteq B$, implying that $\mathbb{P}^\infty(B) > p$ and thus
$$\mathrm{RA}_p \setminus \mathcal{T} \subseteq \{\boldsymbol{x} \in \mathcal{X} \mid \mathbb{P}^\infty(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi) < \infty) > p\} \setminus \mathcal{T}.$$

Let $\boldsymbol{x}_0 \in \{\boldsymbol{x} \in \mathcal{X} \mid \mathbb{P}^\infty(\widehat{t}_{\mathcal{T}}^{\boldsymbol{x}}(\pi) < \infty) > p\} \setminus \mathcal{T}$ and $\pi \in B$. Therefore,
$$\boldsymbol{\psi}_\pi^{\boldsymbol{x}_0}(l) \in \mathcal{X} \setminus \mathcal{T}, \forall l \in [0, t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)) \cap \mathbb{N}.$$
Similar to the above proof, we obtain
$$\widehat{t}_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi) = t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi).$$
Thus, $B \subseteq A$, implying that $\mathbb{P}^\infty(A) > p$ and thus
$$\{\boldsymbol{x} \in \mathcal{X} \mid \mathbb{P}^\infty(t_{\mathcal{T}}^{\boldsymbol{x}}(\boldsymbol{w}) < \infty) > p\} \setminus \mathcal{T} \subseteq \mathrm{RA}_p \setminus \mathcal{T}.$$

Thus, $\mathrm{RA}_p = \{\boldsymbol{x} \in \mathcal{X} \mid \mathbb{P}^\infty(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi) < \infty) > p\}$ holds. ■

Now we define the value function $V(\boldsymbol{x}):\widehat{\mathcal{X}}\to\mathbb{R}$, whose strict p super-level set, i.e., $\{\boldsymbol{x}\in\mathcal{X}\mid V(\boldsymbol{x})>p\}$, is equal to the p-reach-avoid set RA_p.

$$V(\boldsymbol{x}):=\liminf_{k\to\infty}\frac{E^{\infty}[\sum_{i=0}^{k}1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}}(i))]}{k+1},\qquad(3)$$

where $1_{\mathcal{T}}(\boldsymbol{x})$ is the indicator function of the set $\mathcal{T}$.

Lemma 2: $\mathrm{RA}_p=\{\boldsymbol{x}\in\mathcal{X}\mid V(\boldsymbol{x})>p\}$, where $V(\cdot):\widehat{\mathcal{X}}\to[0,1]$ is the value function in (3).

Proof: According to Lemma 1, we just need to prove that $V(\boldsymbol{x})=\mathbb{P}^{\infty}(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi)<\infty)$ for $\boldsymbol{x}\in\mathcal{X}$.

For $k\in\mathbb{N}$, we have

$$\frac{E^{\infty}[\sum_{i=0}^{k}1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}}(i))]}{k+1}=\frac{\sum_{i=0}^{k}\mathbb{P}^{\infty}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}}(i)\in\mathcal{T})}{k+1}.$$

Therefore, $V(\boldsymbol{x})=\lim_{k\to\infty}\inf\frac{\sum_{i=0}^{k}\mathbb{P}^{\infty}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}}(i)\in\mathcal{T})}{k+1}$. According to Lemma 3, which is shown below, we have that

$$\lim_{k\to\infty}\mathbb{P}^{\infty}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}}(k)\in\mathcal{T})=\mathbb{P}^{\infty}(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi)<\infty).$$

Consequently, $V(\boldsymbol{x})=\mathbb{P}^{\infty}(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi)<\infty)$ and thus $\mathrm{RA}_p=\{\boldsymbol{x}\in\mathcal{X}\mid V(\boldsymbol{x})>p\}$ according to Lemma 1. ■

Lemma 3: If $\boldsymbol{x}\in\mathcal{X}$, then

$$\lim_{l\to\infty}\mathbb{P}^{\infty}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}}(l)\in\mathcal{T})=\mathbb{P}^{\infty}(t_{\mathcal{T}}^{\boldsymbol{x}}(\pi)<\infty).$$

Proof: We first prove that

$$\mathbb{P}^{\infty}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l)\in\mathcal{T})=\mathbb{P}^{\infty}(t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)\leq l)$$

with $l\in\mathbb{N}$.

Let $A_l=\{\pi\in\Omega\mid\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l)\in\mathcal{T}\}$ and $B_l=\{\pi\in\Omega\mid t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)\leq l\}$. If $A_l=B_l$, $\mathbb{P}^{\infty}(A_l)=\mathbb{P}^{\infty}(B_l)$ holds. We just need to prove that $A_l=B_l$.

Obviously, if $\pi\in A_l$, we have that

$$\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l)\in\mathcal{T}$$

and

$$\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(k)\in\mathcal{X},\forall k\in[0,l]\cap\mathbb{N}.$$

Thus, $t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)\leq l$, implying that $\pi\in B_l$ and further $A_l\subseteq B_l$.

If $\pi\in B_l$, $t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)\leq l$ and thus $\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l)\in\mathcal{T}$. Therefore, $\pi\in A_l$ and thus $B_l\subseteq A_l$.

Consequently, $A_l=B_l$ and thus $\mathbb{P}^{\infty}(A_l)=\mathbb{P}^{\infty}(B_l)$.

Also, since $A_{l_2}\subseteq A_{l_1}$ and $B_{l_2}\subseteq B_{l_1}$ for $0\leq l_2\leq l_1$, according to the Monotone Convergence Theorem for measurable sets we have $\lim_{l\to\infty}\mathbb{P}^{\infty}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l)\in\mathcal{T})=\mathbb{P}^{\infty}(t_{\mathcal{T}}^{\boldsymbol{x}_0}(\pi)<\infty)$. The proof is completed. ■

According to Lemma 2 we conclude that the exact p-reach-avoid set RA_p can be obtained if the bounded value function $V(\boldsymbol{x})$ in (3) is computed. In the following we show that the bounded value function $V(\boldsymbol{x})$ in (3) could be the unique bounded solution to a system of equations.

Theorem 1: If there exist bounded functions $v(\boldsymbol{x}):\widehat{\mathcal{X}}\to\mathbb{R}$ and $w(\boldsymbol{x}):\widehat{\mathcal{X}}\to\mathbb{R}$ such that for $\boldsymbol{x}\in\widehat{\mathcal{X}}$,

$$\int_{\Theta}v(\widehat{\boldsymbol{f}}(\boldsymbol{x},\boldsymbol{\theta}))d\mathbb{P}(\boldsymbol{\theta})-v(\boldsymbol{x})=0,\qquad(4)$$

$$v(\boldsymbol{x})=1_{\mathcal{T}}(\boldsymbol{x})+\int_{\Theta}w(\widehat{\boldsymbol{f}}(\boldsymbol{x},\boldsymbol{\theta}))d\mathbb{P}(\boldsymbol{\theta})-w(\boldsymbol{x}),\qquad(5)$$

then $v(\boldsymbol{x})=V(\boldsymbol{x})$ for $\boldsymbol{x}\in\mathcal{X}$ and thus $\mathrm{RA}_p=\{\boldsymbol{x}\in\mathcal{X}\mid v(\boldsymbol{x})>p\}$, where $V(\cdot):\widehat{\mathcal{X}}\to[0,1]$ is the function (3).

Proof: From (4), we have that

$$v(\boldsymbol{x}_0)=E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))],\forall i\in\mathbb{N}.\qquad(6)$$

From (5) we have that for $i\in\mathbb{N}$,

$$\begin{aligned}v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))=&1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))\\&+\int_{\Theta}w(\widehat{\boldsymbol{f}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i),\boldsymbol{\theta}))d\mathbb{P}(\boldsymbol{\theta})-w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i)).\end{aligned}$$

Thus, we can obtain that

$$\begin{aligned}&E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]=E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]\\&+E^{\infty}[\int_{\Theta}w(\widehat{\boldsymbol{f}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i),\boldsymbol{\theta}))d\mathbb{P}(\boldsymbol{\theta})]-E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]\end{aligned}$$

and further

$$\begin{aligned}E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]&=E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]\\&+E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i+1))]-E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]\end{aligned}$$

which implies that

$$\begin{aligned}&\sum_{i=0}^{l}E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]=\sum_{i=0}^{l}E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]\\&\quad+\sum_{i=0}^{l}\big(E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i+1))]-E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]\big).\end{aligned}$$

Combining (6), we have that for $l\in\mathbb{N}$,

$$\begin{aligned}v(\boldsymbol{x}_0)=&\frac{\sum_{i=0}^{l}E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]}{l+1}\\&+\frac{E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l+1))]-w(\boldsymbol{x}_0)}{l+1}\end{aligned}$$

and thus $v(\boldsymbol{x}_0)=\lim_{l\to\infty}\frac{E^{\infty}[\sum_{i=0}^{l}1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]}{l+1}=V(\boldsymbol{x}_0)$. As an immediate consequence, we have that $\mathrm{RA}_p=\{\boldsymbol{x}\in\mathcal{X}\mid v(\boldsymbol{x})>p\}$ from Lemma 2. ■

Theorem 1 tells that the set RA_p could be computed by solving the system of equations (4) and (5). However, it is challenging, even impossible for solving them. In order to circumvent the challenge of solving them directly, in the following we show that an inner-approximation of the set RA_p could be obtained by solving a system of inequalities, which is generated via relaxing the equations (4) and (5).

Corollary 2: If there exist bounded functions $v(\boldsymbol{x}):\widehat{\mathcal{X}}\to\mathbb{R}$ and $u(\boldsymbol{x}):\widehat{\mathcal{X}}\to\mathbb{R}$ such that for $\boldsymbol{x}\in\widehat{\mathcal{X}}$,

$$\int_{\Theta}v(\widehat{\boldsymbol{f}}(\boldsymbol{x},\boldsymbol{\theta}))d\mathbb{P}(\boldsymbol{\theta})-v(\boldsymbol{x})\geq 0,\qquad(7)$$

$$v(\boldsymbol{x})\leq 1_{\mathcal{T}}(\boldsymbol{x})+\int_{\Theta}w(\widehat{\boldsymbol{f}}(\boldsymbol{x},\boldsymbol{\theta}))d\mathbb{P}(\boldsymbol{\theta})-w(\boldsymbol{x}),\qquad(8)$$

then $\{\boldsymbol{x}\in\mathcal{X}\mid v(\boldsymbol{x})>p\}\subseteq\mathrm{RA}_p$ is an inner-approximation of the p-reach-avoid set RA_p.

Proof: Assume that $\boldsymbol{x}_0\in\mathcal{X}$. From (7), we have that

$$v(\boldsymbol{x}_0)\leq E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))],\forall i\in\mathbb{N}.\qquad(9)$$

From (8) we have that for $i \in \mathbb{N}$,

$$v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i)) \leq 1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i)) + \int_{\Theta} w(\widehat{\boldsymbol{f}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i), \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i)).$$

Thus,

$$E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))] \leq E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))] + E^{\infty}[\int_{\Theta} w(\widehat{\boldsymbol{f}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i), \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta})] - E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]$$

and further

$$E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))] \leq E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))] + E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i+1))] - E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))],$$

which implies that

$$\sum_{i=0}^{l} E^{\infty}[v(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))] \leq \sum_{i=0}^{l} E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))] + E^{\infty}[\sum_{i=0}^{l} w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i+1))] - E^{\infty}[\sum_{i=0}^{l} w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))],$$

Combining (9), we have that for $l \in \mathbb{N}$,

$$v(\boldsymbol{x}_0) \leq \frac{\sum_{i=0}^{l} E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]}{l+1} + \frac{E^{\infty}[w(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(l+1))] - w(\boldsymbol{x}_0)}{l+1},$$

and thus $v(\boldsymbol{x}_0) \leq \liminf_{l \to \infty} \frac{\sum_{i=0}^{l} E^{\infty}[1_{\mathcal{T}}(\boldsymbol{\psi}_{\pi}^{\boldsymbol{x}_0}(i))]}{l+1} = V(\boldsymbol{x}_0)$. Therefore, $\{\boldsymbol{x} \in \mathcal{X} \mid v(\boldsymbol{x}) > p\} \subseteq \mathrm{RA}_p$. ■

Corollary 2 uncovers that an inner-approximation of the p-reach-avoid set RA_p comes with one solution $v(\boldsymbol{x}) : \widehat{\mathcal{X}} \to \mathbb{R}$ to the system of inequalities (7) and (8). Constraints (7) and (8) can be equivalently reformulated below:

$$\begin{aligned} &[\int_{\Theta} v(\widehat{\boldsymbol{f}}_1(\boldsymbol{x}, \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \widehat{\mathcal{X}}_1] \wedge \\ &\bigwedge_{i=1}^{3} [-v(\boldsymbol{x}) + 1_{\mathcal{T}}(\boldsymbol{x}) + w'(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \widehat{\mathcal{X}}_i], \end{aligned} \tag{10}$$

with $w'(\boldsymbol{x}) = \int_{\Theta} w(\widehat{\boldsymbol{f}}_i(\boldsymbol{x}, \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - w(\boldsymbol{x})$, which can be further reduced to

$$\begin{aligned} &\int_{\Theta} v(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{T}, \\ &- v(\boldsymbol{x}) + \int_{\Theta} w(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - w(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{T}, \\ &- v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}, \\ &1 - v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \mathcal{T}. \end{aligned} \tag{11}$$

If the functions $v(\boldsymbol{x})$ and $w(\boldsymbol{x})$ in (11) are polynomials over $\boldsymbol{x} \in \mathbb{R}^n$, we can encode the system of inequalities (11) into semi-definite constraints using the sum-of-squares decomposition for multivariate polynomials, and then construct a semi-definite program (12) for inner-approximating the p-reach-avoid set RA_p.

$$\begin{aligned} &\max \boldsymbol{c}^{\top} \cdot \hat{\boldsymbol{w}} \\ &\text{s.t.} \\ &\int_{\Theta} v(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - v(\boldsymbol{x}) + s_0(\boldsymbol{x}) h(\boldsymbol{x}) \\ &\qquad - s_1(\boldsymbol{x})(g(\boldsymbol{x}) - 1) \in \sum[\boldsymbol{x}], \\ &- v(\boldsymbol{x}) + \int_{\Theta} w(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) d\mathbb{P}(\boldsymbol{\theta}) - w(\boldsymbol{x}) \\ &\qquad + s_2(\boldsymbol{x}) h(\boldsymbol{x}) - s_3(\boldsymbol{x})(g(\boldsymbol{x}) - 1) \in \sum[\boldsymbol{x}], \\ &- v(\boldsymbol{x}) + s_4(\boldsymbol{x}) h_0(\boldsymbol{x}) - s_5(\boldsymbol{x}) h(\boldsymbol{x}) \in \sum[\boldsymbol{x}], \\ &1 - v(\boldsymbol{x}) - s_6(\boldsymbol{x})(1 - g(\boldsymbol{x})) \in \sum[\boldsymbol{x}], \end{aligned} \tag{12}$$

where $\boldsymbol{c}^{\top} \cdot \hat{\boldsymbol{w}} = \int_{\widehat{\mathcal{X}}} v(\boldsymbol{x}) d\boldsymbol{x}$, $\hat{\boldsymbol{w}}$ is the constant vector computed by integrating the monomials in $v(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ over $\widehat{\mathcal{X}}$, $\boldsymbol{c}$ is the vector composed of unknown coefficients in $v(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$; $w(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$, and $s_i(\boldsymbol{x}) \in \sum[\boldsymbol{x}]$, $i = 0, \ldots, 6$.

Theorem 2: If a function $v(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ satisfies the semi-definite program (12), the set $\{\boldsymbol{x} \in \mathcal{X} \mid v(\boldsymbol{x}) > p\}$ is an inner approximation of the p-reach-avoid set RA_p.

Remark 2: A robust inner-approximation of the qualitative *reach-avoid set* RA *can also be obtained via solving a semi-definite program derived from the semi-definite program* (12) *if* $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta}) \in \mathbb{R}[\boldsymbol{x}, \boldsymbol{\theta}]$ *and the set* $\Theta = \{\boldsymbol{\theta} \in \mathbb{R}^m \mid r(\boldsymbol{\theta}) \leq 0\}$ *with* $r(\boldsymbol{\theta}) \in \mathbb{R}[\boldsymbol{\theta}]$*. The reach-avoid set* RA *is the set of all initial states letting system* (1) *hit the target set* $\mathcal{T}$ *in finite time while remaining inside the safe set* $\mathcal{X}$ *till the hit irrespective of disturbances. That is,*

$$\mathrm{RA} = \left\{ \boldsymbol{x}_0 \in \mathcal{X} \,\middle|\, \begin{array}{r} \forall \pi \in \Omega. \exists k \in \mathbb{N}. \boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(k) \in \mathcal{T} \bigwedge \\ \forall l \in [0, k] \cap \mathbb{N}. \boldsymbol{\phi}_{\pi}^{\boldsymbol{x}_0}(l) \in \mathcal{X} \end{array} \right\}.$$

The semi-definite program is presented below.

$$\begin{aligned} &\max \boldsymbol{c}^{\top} \cdot \hat{\boldsymbol{w}} \\ &\text{s.t.} \\ &v(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) - v(\boldsymbol{x}) + s_0(\boldsymbol{x}, \boldsymbol{\theta}) h(\boldsymbol{x}) \\ &\quad - s_1(\boldsymbol{x}, \boldsymbol{\theta})(g(\boldsymbol{x}) - 1) + s_2(\boldsymbol{x}, \boldsymbol{\theta}) r(\boldsymbol{\theta}) \in \sum[\boldsymbol{x}, \boldsymbol{\theta}], \\ &- v(\boldsymbol{x}) + w(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) - w(\boldsymbol{x}) + s_3(\boldsymbol{x}, \boldsymbol{\theta}) h(\boldsymbol{x}) \\ &\quad - s_4(\boldsymbol{x}, \boldsymbol{\theta})(g(\boldsymbol{x}) - 1) + s_5(\boldsymbol{x}, \boldsymbol{\theta}) r(\boldsymbol{\theta}) \in \sum[\boldsymbol{x}, \boldsymbol{\theta}], \\ &- v(\boldsymbol{x}) + s_6(\boldsymbol{x}) h_0(\boldsymbol{x}) - s_7(\boldsymbol{x}) h(\boldsymbol{x}) \in \sum[\boldsymbol{x}], \end{aligned} \tag{13}$$

where $\boldsymbol{c}^{\top} \cdot \hat{\boldsymbol{w}} = \int_{\widehat{\mathcal{X}}} v(\boldsymbol{x}) d\boldsymbol{x}$, $\hat{\boldsymbol{w}}$ is the constant vector computed by integrating the monomials in $v(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ over $\widehat{\mathcal{X}}$, $\boldsymbol{c}$ is the vector composed of unknown coefficients in $v(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$; $w(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$, and $s_i(\boldsymbol{x}, \boldsymbol{\theta}) \in \sum[\boldsymbol{x}, \boldsymbol{\theta}]$, $i = 0, \ldots, 5$, and $s_i(\boldsymbol{x}) \in \sum[\boldsymbol{x}]$, $i = 6, 7$.

Theorem 3: If a function $v(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ *satisfies the semi-definite program* (13)*, the set* $\{\boldsymbol{x} \in \mathcal{X} \mid v(\boldsymbol{x}) > 0\}$ *is an inner-approximation of the reach-avoid set* RA.

Ex.	SDP (12)			
	d_v	d_w	d_s	T
1	10	10	12	3.53
2	14	14	16	3.71

TABLE I

PARAMETERS OF OUR IMPLEMENTATIONS ON (12) FOR EXAMPLES 1 AND 2. d_v AND d_w: DEGREE OF POLYNOMIALS v AND w IN (12), RESPECTIVELY; d_s : DEGREE OF POLYNOMIALS s_i IN (12), RESPECTIVELY, $i = 0, \dots, 6$; T: COMPUTATIONAL TIME(SECONDS)

Proof: The constraints in the semi-definite program (13) imply that

$$v(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) - v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{T}, \forall \boldsymbol{\theta} \in \Theta, \quad (14)$$

$$v(\boldsymbol{x}) \leq w(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{\theta})) - w(\boldsymbol{x}), \forall \boldsymbol{x} \in \mathcal{X} \setminus \mathcal{T}, \forall \boldsymbol{\theta} \in \Theta, \quad (15)$$

$$-v(\boldsymbol{x}) \geq 0, \forall \boldsymbol{x} \in \widehat{\mathcal{X}} \setminus \mathcal{X}, \quad (16)$$

Assume that $\boldsymbol{x}_0 \in \{\boldsymbol{x} \in \mathcal{X} \mid v(\boldsymbol{x}) > 0\}$ and $\boldsymbol{x}_0 \notin \mathrm{RA}$. Consequently, either

$$\exists \pi_0 \in \Omega. \forall l \in \mathbb{N}. \boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l) \in \mathcal{X} \setminus \mathcal{T} \quad (17)$$

or

$$\exists \pi_0 \in \Omega. \exists l \in \mathbb{N}. \boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l) \notin \mathcal{X} \wedge \bigwedge_{i \in [0,l) \cap \mathbb{N}} \boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(i) \in \mathcal{X} \setminus \mathcal{T} \quad (18)$$

holds.

If (17) holds, according to constraint (14) we have that

$$v(\boldsymbol{x}_0) \leq v(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l)), \forall l \in \mathbb{N}. \quad (19)$$

Further, constraint (15) implies that

$$v(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l)) \leq w(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l+1)) - w(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l)), \forall l \in \mathbb{N}$$

and thus for $l \in \mathbb{N}$,

$$\sum_{i=0}^{l} v(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(i)) \leq \sum_{i=0}^{l} (w(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(i+1)) - w(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(i))). \quad (20)$$

Inequalities (19) and (20) tell that

$$v(\boldsymbol{x}_0) \leq \frac{w(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l+1)) - w(\boldsymbol{x}_0)}{l+1}, \forall l \in \mathbb{N}.$$

Also, since $w(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ and the safe set $\mathcal{X}$ is bounded, $\lim_{l \to \infty} \frac{w(\boldsymbol{\phi}_{\pi_0}^{\boldsymbol{x}_0}(l+1)) - w(\boldsymbol{x}_0)}{l+1} = 0$ and thus $v(\boldsymbol{x}_0) \leq 0$, contradicting the fact that $v(\boldsymbol{x}_0) > 0$.

The fact that $v(\boldsymbol{x}_0) > 0$, together with constraints (14) and (16), indicates that (18) does not hold.

Consequently, $\{\boldsymbol{x} \in \mathcal{X} \mid v(\boldsymbol{x}) > 0\} \subseteq \mathrm{RA}$. ■

IV. EXAMPLES

In this section we demonstrate our semi-definite programming approach on two examples. All computations were performed on an i7-7500U 2.70GHz CPU with 32GB RAM running Windows 10, where the Matlab toolboxes YALMIP for sum-of-squares decomposition [9] and Mosek for semi-definite programs [11] are used to implement (12).

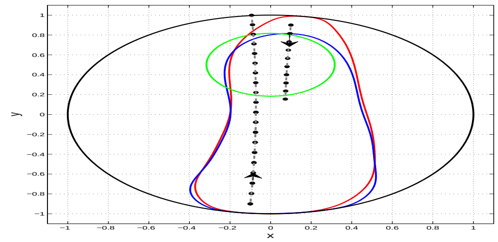

Fig. 1. An illustration of computed inner-approximations of 0-reach-avoid sets for Example 1. The black curve denotes the boundary of the safe set $\mathcal{X}$. The red and blue curves denote computed inner-approximations of 0-reach-avoid sets with $\Theta = [-10, 10]$ and $\Theta = [-5, 5]$ respectively. The gray-black curves denote the trajectories starting from $(0.1, 0.9)^\top$ with $\theta(l) \equiv -5$ and $(-0.1, -0.9)^\top$ with $\theta(l) \equiv 5$ respectively.

Example 1: In this example we consider a computer-based model of the following ordinary differential equation:

$$\begin{cases} \dot{x}(t) = -0.5x(t) - 0.5y(t) + 0.5x(t)y(t) \\ \dot{y}(t) = -0.5y(t) + 1 + \theta(t) \end{cases}$$

where $\theta(\cdot) : [0, \infty) \to \Theta$ with Θ being a set in $\mathbb{R}$.

When performing computer simulations, Euler's method is often used to analyze an ordinary differential equation, which employs the idea of a linear extrapolation along the local derivative. When the simulation step is 0.01, the resulting discrete-time system is of the following from:

$$\begin{cases} x(l+1) = x(l) + 0.01(-0.5x(l) - 0.5y(l) + 0.5x(l)y(l)) \\ y(l+1) = y(l) + 0.01(-0.5y(l) + 1 + \theta(l)) \end{cases}$$

Assume that $\mathcal{X} = \{(x, y)^\top \mid x^2 + y^2 - 1 < 0\}$ and $\mathcal{T} = \{(x, y)^\top \mid 10x^2 + 10(y - 0.5)^2 \leq 1\}$.

The random vector $\theta(l)$ for $l \in \mathbb{N}$ has the uniform distribution on the set Θ. We consider the following two cases with different disturbance sets Θ. The set $\widehat{\mathcal{X}} = \{(x, y)^\top \mid x^2 + y^2 - 1.1 \leq 0\}$, which is computed by solving a semi-definite program as in [16], is applicable for these two cases.

1) $\Theta = [-5, 5]$: an inner-approximation of the set RA_0, which is computed by solving (12) with parameters in Table I, is illustrated in Fig. 1. The computed inner-approximations of p-reach-avoid sets with $p = 0.25, 0.5$ and 0.75 are illustrated in Fig. 2.
2) $\Theta = [-10, 10]$: an inner-approximation of the set RA_0, which is computed by solving (12) with parameters listed in Table I, is also illustrated in Fig. 1. Meanwhile, the computed inner-approximations of p-reach-avoid sets with $p = 0.25, 0.5$ and 0.75 are illustrated in Fig. 2 as well.

Note that in both cases we obtain correct but useless robust inner approximations of the *qualitative* reach-avoid set, which are empty, via solving the program (13). This shows that the p-reach-avoid set is a useful generalization.

Example 2: Consider the following discrete-time Lotka-Volterra model:

$$\begin{cases} x(l+1) = rx(l) - ay(l)x(l) \\ y(l+1) = sy(l) + acy(l)x(l) \end{cases} \quad (21)$$

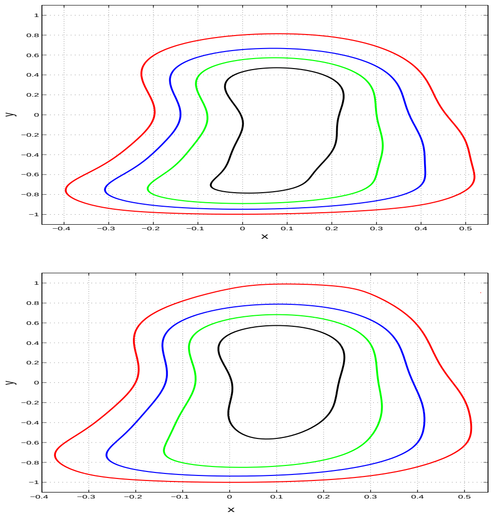

Fig. 2. An illustration of computed inner-approximations of p-reach-avoid sets for Example 1. Above ($\Theta = [-5, 5]$) and Below ($\Theta = [-10, 10]$): The red, blue, green and black curves denote the boundaries of computed inner-approximations of the 0.0-, 0.25-, 0.5- and 0.75-reach-avoid sets respectively.

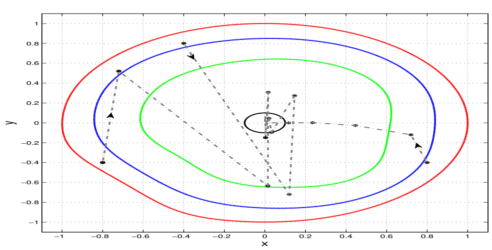

Fig. 3. An illustration of the computed p-reach-avoid sets for Example 2. The black curve denotes the boundary of the target set $\mathcal{T}$. The red, blue and green curves denote the boundaries of the computed inner-approximations of the 0.0-, 0.25-, and 0.6-reach-avoid sets respectively. The gray-black curves denote the trajectories starting from $(-0.8, -0.4)^\top$, $(-0.4, 0.8)^\top$ and $(0.8, -0.4)^\top$ with $\theta(l) \equiv 0$ respectively.

where $r = 0.5$, $a = 1$, $s = -0.5 + \theta(l)$ with $\theta(\cdot) : \mathbb{N} \to [-0.5, 0.5]$ and $c = 1$.

Assume that the random vector $\theta(l)$ for $l \in \mathbb{N}$ has the uniform distribution on the set $[-0.5, 0.5]$, $\mathcal{X} = \{(x, y)^\top \mid x^2 + y^2 - 1 < 0\}$ and $\mathcal{T} = \{(x, y)^\top \mid 100x^2 + 100y^2 \leq 1\}$. The set $\widehat{\mathcal{X}} = \{(x, y)^\top \mid x^2 + y^2 - 2.25 \leq 0\}$ is used. The computed inner-approximations of p-reach-avoid sets with $p = 0.0, 0.25$ and 0.6 are illustrated in Fig. 3.

Similar to Example 1, we obtain a correct but useless robust inner-approximation, which is empty, for this example via solving the semi-definite program (13) with parameters listed in Table I.

V. Conclusion

We have elaborated a computational method for under-approximating, i.e., approximating from the inner, the p-reach-avoid set over open time horizons of discrete-time systems given as iterative polynomial maps subject to stochastic disturbances. The method builds on a semi-definite-programming relaxation of the super-level set of a corresponding function and was demonstrated on two examples.

In future work we would extend the present method to reach-avoid reachability of random ordinary differential equations [15] and to the safe design of cyber-physical systems such as autonomous vehicles. Also, we would investigate the conservativeness of inner-approximations computed by the present semi-definite programming method.

Acknowledgments

This work has been supported through grants by NSFC under grant No. 61872341, 61836005, 61625206, 61732001, CAS Pioneer Hundred Talents Program, Natural Science Foundation of Guangdong Province, China (Grant No. 2019A1515011689), and Deutsche Forschungsgemeinschaft through the grants DFG GRK 1765 “System Correctness under Adverse Conditions” and FR 2715/4-1 “Integrated Socio-technical Models for Conflict Resolution and Causal Reasoning”.

References

[1] A. Abate, M. Prandini, J. Lygeros, and S. Sastry. Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. *Automatica*, 44(11):2724–2734, 2008.

[2] E. M. Clarke Jr, O. Grumberg, D. Kroening, D. Peled, and H. Veith. *Model checking*. MIT press, 2018.

[3] D. Drzajic, N. Kariotoglou, M. Kamgarpour, and J. Lygeros. A semidefinite programming approach to control synthesis for stochastic reach-avoid problems. In *ARCH@ CPSWeek*, pages 134–143, 2016.

[4] J. D. Gleason, A. P. Vinod, and M. M. Oishi. Underapproximation of reach-avoid sets for discrete-time stochastic systems via lagrangian methods. In *CDC*, pages 4283–4290. IEEE, 2017.

[5] N. Kariotoglou, D. M. Raimondo, S. Summers, and J. Lygeros. A stochastic reachability framework for autonomous surveillance with pan-tilt-zoom cameras. In *CDC-ECC*, pages 1411–1416. IEEE, 2011.

[6] N. Kariotoglou, S. Summers, T. Summers, M. Kamgarpour, and J. Lygeros. Approximate dynamic programming for stochastic reachability. In *ECC*, pages 584–589. IEEE, 2013.

[7] H. K. Khalil and J. W. Grizzle. *Nonlinear systems*, volume 3. Prentice hall Upper Saddle River, NJ, 2002.

[8] K. Lesser, M. Oishi, and R. S. Erwin. Stochastic reachability for control of spacecraft relative motion. In *CDC*, pages 4705–4712. IEEE, 2013.

[9] J. Lofberg. YALMIP: A toolbox for modeling and optimization in matlab. In *ICRA (IEEE Cat. No. 04CH37508)*, pages 284–289. IEEE, 2004.

[10] K. Margellos and J. Lygeros. Hamilton–jacobi formulation for reach–avoid differential games. *IEEE Transactions on Automatic Control*, 56(8):1849–1861, 2011.

[11] A. Mosek. The MOSEK optimization toolbox for matlab manual, 2015.

[12] K. Ogata et al. *Discrete-time control systems*, volume 2. Prentice Hall Englewood Cliffs, NJ, 1995.

[13] A. V. Oppenheim, J. R. Buck, and R. W. Schafer. *Discrete-time signal processing. Vol. 2*. Upper Saddle River, NJ: Prentice Hall, 2001.

[14] S. Summers and J. Lygeros. Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem. *Automatica*, 46(12):1951–1961, 2010.

[15] B. Xue, M. Fränzle, N. Zhan, S. Bogomolov, and B. Xia. Safety verification for random ordinary differential equations. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(11):4090–4101, 2020.

[16] B. Xue, N. Zhan, and M. Fränzle. Inner-approximating reach-avoid sets for discrete-time polynomial systems. In *CDC*, pages 867–873. IEEE, 2020.