Interval-valued Markov Chain Abstraction of Stochastic Systems using Barrier Functions

Maxence Dutreix[1], Cesar Santoyo[2], Matthew Abate[3] and Samuel Coogan[4]

***Abstract*— This paper presents a stochastic barrier function-based abstraction technique for discrete-time stochastic systems. Recent works have shown the potential of Interval-valued Markov Chain abstractions for conducting efficient verification of continuous-state, discrete-time stochastic systems against complex objectives, as well as efficient synthesis for finite-mode switched stochastic systems. Such Markovian abstractions allow for a range of transition probabilities between its states. In this work, we address the problem of constructing Interval-valued Markov Chain abstractions for polynomial systems using stochastic barrier functions. Stochastic barrier functions serve as Lyapunov-like probabilistic certificates of forward set invariance. Specifically, given a finite partition of the system's domain, we show that bounds on the probability of transition between any two elements of the partition are found by generating stochastic barrier functions via optimization procedures in the form of Sum-of-Squares programs. We present an algorithm for solving these optimization problems whose implementation is demonstrated in a verification and a synthesis case study.**

I. INTRODUCTION

Dynamical systems with complex objectives—such as autonomous vehicles and industrial robotics—subject to random disturbances pose challenges for verification and controller synthesis. Efforts have been dedicated to stability analysis of stochastic systems via stochastic Lyapunov functions [1]. Recent literature has extended stochastic system verification and synthesis to more complex system properties expressed using symbolic temporal logics [2], [3].

However, verification and synthesis for complex temporal logic specifications in discrete time are, in general, undecidable or intractable to solve and require resorting to approximation methods [3], [4]. These methods typically involve the discretization of the system's domain into a finite number of discrete states which are converted to a finite stochastic transition system. This transition system serves as a finite-state abstraction of the continuous-state dynamics. Performing verification or synthesis on this abstraction is generally more tractable and yields bounded-error probabilistic guarantees with respect to the original system states.

This work was supported in part by the NSF under project #1749357. C. Santoyo was supported by the NSF Graduate Research Fellowship Program under Grant No. DGE-1650044

[1]M. Dutreix and [2]C. Santoyo are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA maxdutreix@gatech.edu , csantoyo@gatech.edu

[3]M. Abate is with the School of Mechanical Engineering and the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA matt.abate@gatech.edu

[4]S. Coogan is with the School of Electrical and Computer Engineering and the School of Civil and Environmental Engineering, Georgia Institute of Technology, Atlanta, GA, USA sam.coogan@gatech.edu

Several types of stochastic abstractions, such as approximate Markov Chains [5], have been put forth in the literature. Abstractions by way of *Interval-valued Markov Chains* (IMC) [6] were shown to be an effective means for verification and synthesis of stochastic systems [2], [7], [8]. Individual states of an IMC abstraction encapsulate the collective behavior of all its abstracted continuous states by imposing their transition probabilities to lie within some interval. While IMC abstractions have proven to be efficient verification and synthesis tools for discrete-time stochastic systems, little work has been conducted on the computation of such abstractions. An abstraction algorithm for linear systems with additive noise and polytopic domain partition is introduced in [9]. In [10], an IMC abstraction technique scaling linearly with the number of dimensions is presented for mixed monotone systems. To the best of our knowledge, other classes of systems for which correct and non-trivial IMC abstractions can be constructed have not been discussed.

Stochastic barrier functions have emerged as promising instruments for providing probabilistic guarantees amenable to IMC abstractions. Stochastic barrier functions are used as a probabilistic certificate of set invariance for stochastic dynamical systems. Specifically, one can derive an upper bound on the probability that a system will reach some region of the domain if one can show the existence of a barrier function satisfying certain value constraints over the domain. The works in [11] and [12] derive set invariance bounds for discrete-time, finite-time horizon stochastic systems, while [13] focuses on infinite-time horizon guarantees.

In this work, we utilize stochastic barrier functions to construct IMC abstractions of discrete-time polynomial systems. These abstractions enable verification and synthesis for such systems against specifications from the expressive class of ω-*regular properties*, which is an improvement from existing techniques. State-of-the-art tools such as FAUST^2 [14] and StocHy [15] cannot perform synthesis for arbitrary stochastic polynomial systems against all ω-regular specifications.

The contributions of this paper are as follows: we present an IMC abstraction method for discrete-time stochastic polynomial systems; to construct such abstractions, we use a discrete-time formulation of the stochastic barrier function framework over a single transition where two barrier functions are computed; by means of this formulation, an IMC abstraction of stochastic polynomial systems is created from a finite partition of its domain by finding two stochastic barrier functions per transition. The barrier functions are calculated via *Sum-of-Squares* (SOS) optimization programs.

The paper is organized as follows: Section II introduces

the problem formulation; Section III discusses the theory of stochastic barrier functions; Section IV shows how stochastic barrier functions can be used for computing IMC abstractions of polynomial stochastic systems; Section V presents a verification and synthesis case study where our abstraction method is applied; Section VI concludes this work.

II. PROBLEM FORMULATION

We consider the discrete-time, continuous-state stochastic system

$$x[k+1] = \mathcal{F}(x[k], w[k]) \ , \tag{1}$$

where $x[k] \in D \subset \mathbb{R}^n$ is the state of the system and $w[k] \in W \subset \mathbb{R}^p$ is a random disturbance at time k, and $\mathcal{F} : D \times W \to D$ is a continuous map. At each time-step k, the random disturbance $w[k]$ is sampled from a probability distribution with density function $f_w : \mathbb{R}^p \to \mathbb{R}_{\geq 0}$. Associated with (1) is a labeling function $L : D \to \Sigma$, where Σ is a finite alphabet. An infinite path $\pi = x[0]x[1]x[2]\dots$ generated by (1) induces a trace $\mathcal{L}(\pi) = L(x[0])L(x[1])L(x[2])\dots$

We denote by Ψ an arbitrary *ω-regular property* [16] over alphabet Σ. In particular, all properties defined by a *Linear Temporal Logic* (LTL) formula are ω-regular. We define a probability operator $\mathcal{P}_{\bowtie p_{sat}}[\Psi]$ over ω-regular properties, with $\bowtie \in \{\leq, <, \geq, >\}$, $p_{sat} \in [0,1]$. For any initial state $x \in D$, we define the satisfaction relation $\models$ where $x \models \mathcal{P}_{\bowtie p_{sat}}[\Psi] \ \Leftrightarrow \ p^x_\Psi \bowtie p_{sat}$, with p^x_Ψ being the probability that the trace generated by a random path starting at x satisfies property Ψ (for a rigorous formalization, see, e.g., [5]). We concentrate on formulas of the type $\phi = \mathcal{P}_{\bowtie p_{sat}}[\Psi]$. Given a formula ϕ of this form, *the verification problem* requires sorting all initial states of system (1) into those that satisfy property ϕ and those that do not satisfy property ϕ.

We additionally consider switched stochastic systems

$$x[k+1] = \mathcal{F}_a(x[k], w_a[k]) \ , \tag{2}$$

with $a \in A$ and A is a finite set of *modes*, and everything is defined as in (1) for a fixed mode a. At each time-step k, a mode a is chosen and a transition occurs according to the dynamics of $\mathcal{F}_a$ subject to the disturbance w_a. A finite sequence of states $\pi = x[0]x[1]\dots x[m]$ in (2) is called a finite path and the set of all finite paths of (2) is denoted by $Paths_{fin}$. A function $\mu : Paths_{fin} \to A$ assigning a mode to each finite path in (2) is called a *switching policy* and the set of all switching policies of (2) is denoted by $\mathcal{U}$. Given an ω-regular property Ψ, the *synthesis problem* asks for a switching policy $\breve{\mu}_\Psi$ or $\widehat{\mu}_\Psi$ that respectively minimizes or maximizes the probability of satisfying Ψ and are such that

$$\breve{\mu}_\Psi = \arg\min_{\mu \in \mathcal{U}} (p^x_\Psi)_\mu \quad , \quad \widehat{\mu}_\Psi = \arg\max_{\mu \in \mathcal{U}} (p^x_\Psi)_\mu$$

for any initial state $x \in D$, with $(p^x_\Psi)_\mu$ being the probability that the trace generated by a random path starting at x satisfies property Ψ under policy μ. Recent works have shown that these verification and synthesis problems cannot, in general, be solved exactly [3], [4]. Instead, they are addressed via approximation techniques by first generating a finite partition P of the system domain D.

Definition 1 (Partition): A *partition* P of $D \subset \mathbb{R}^n$ is a collection of states $P = \{Q_j\}_{j=1}^m$, $Q_j \subset D$, satisfying $\bigcup_{j=1}^m Q_j = D$ and $\mathbf{int}(Q_j) \cap \mathbf{int}(Q_\ell) = \emptyset \ \ \forall j, \ell, \ j \neq \ell$, where $\mathbf{int}(Q_j)$ denotes the interior of Q_j. For any continuous state x belonging to a state Q_j, we write $x \in Q_j$.

The discrete states of P, which are collections of continuous states of D, serve as a basis for finite-state abstractions of (1) and (2) by means of stochastic transition systems. In this paper, the abstractions of choice for (1) are Interval-valued Markov Chains (IMC) [6], while (2) is abstracted by Bounded-parameter Markov Decision Processes (BMDP) [17], which are finite collections of IMCs.

Definition 2 (Bounded-parameter Markov Decision Process): A *Bounded-parameter Markov Decision Process (BMDP)* [17] is a 6-tuple $\mathcal{B} = (Q, Act, \breve{T}, \widehat{T}, \Sigma, L)$ where:

- Q is a finite set of states,
- Act is a finite set of actions,
- $\breve{T} : Q \times Act \times Q \to [0,1]$ maps pairs of states and an action to a lower transition bound,
- $\widehat{T} : Q \times Act \times Q \to [0,1]$ maps pairs of states and an action to an upper transition bound,
- Σ is a finite set of atomic propositions,
- $L : Q \to \Sigma$ is a labeling function from states to Σ.

Definition 3 (Interval-valued Markov Chain): An *Interval-valued Markov Chain* (IMC) $\mathcal{I} = (Q, \breve{T}, \widehat{T}, \Sigma, L)$ is defined similarly to a BDMP with the difference that a single action (omitted in the defining tuple) is available.

Techniques for performing verification of IMCs and synthesis for BMDPs against ω-regular specifications are presented in [7] and [18] and are not the focus of this work. Here, we seek to determine bounds on the probabilities of transition between any two states in the partition P so as to construct IMC and BMDP abstractions of (1) and (2).

Definition 4 (Exact Transition Bounds): Let P be a partition of the domain D of (1). For all $Q_i, Q_j \in P$, the *exact* transition lower bound $\breve{T}_{ex}(Q_i, Q_j)$ and upper bound $\widehat{T}_{ex}(Q_i, Q_j)$ on the transition from Q_i to Q_j are given by

$$\breve{T}_{ex}(Q_i, Q_j) = \inf_{x \in Q_i} Pr(\mathcal{F}(x, w) \in Q_j),$$
$$\widehat{T}_{ex}(Q_i, Q_j) = \sup_{x \in Q_i} Pr(\mathcal{F}(x, w) \in Q_j),$$

where $Pr(\mathcal{F}(x, w) \in Q_j \mid x)$ for fixed x is the probability that (1) transitions from x to some $x' = F(x, w)$ in Q_j.

Definition 5 (IMC and BMDP Abstractions): Let P be a partition of the domain D of (1). An interval-valued Markov Chain $\mathcal{I} = (Q, \breve{T}, \widehat{T}, \Sigma, L)$ is an *abstraction* of (1) if $Q = P$; for all $Q_j \in P$ and for any two $x_i, x_\ell \in Q_j$, it holds that

$L(Q_j) := L(x_i) = L(x_\ell)$; and, for all $Q_i, Q_j \in P$,

$$\breve{T}(Q_i, Q_j) \leq \breve{T}_{ex}(Q_i, Q_j) \leq \widehat{T}_{ex}(Q_i, Q_j) \leq \widehat{T}(Q_i, Q_j) \ .$$

A BMDP abstraction $\mathcal{B} = (Q, Act, \breve{T}, \widehat{T}, \Sigma, L)$ of (2) is defined similarly by letting each action $a \in Act$ induce an IMC abstraction of (2) under mode a.

The tractibility of finding non-trivial transition intervals, i.e., not ranging from 0 to 1, depends on the system of interest and the geometry of its domain partition. Here, we focus on systems with polynomial dynamics in x and w.

Assumption 1: The function $\mathcal{F}$ in (1) is a polynomial in x and w.

For system (2), we assume that every mode a induces an equation of the form (1) under Assumption 1. Consequently, a method for constructing an IMC abstraction of (1) allows us to build an IMC abstraction for all modes of (2), which is equivalent to a BMDP abstraction. Thus, the main problem of this work consists in devising an IMC abstraction procedure for (1).

Problem: *Given a system of the form* (1) *under Assumption 1 and a partition P of its domain D, construct a non-trivial IMC abstraction of* (1)*.*

III. STOCHASTIC BARRIER FUNCTIONS

In order to propose a solution to the main problem, we first introduce the concept of stochastic barrier function.

Stochastic barrier functions are utilized as a probabilistic certificate of set invariance for stochastic systems. By showing the existence of a function satisfying a particular set of constraints over the domain of the system, one can ensure that the probability of reaching a given set of states from a set of initial conditions is less than some bound. Here, we study stochastic barrier functions in a discrete-time framework over a time horizon of one transition. Consider a stochastic system (1) over a continuous domain $\mathcal{X} \subset \mathbb{R}^n$. Let $\mathcal{X}_0 \subseteq \mathcal{X}$ be a set of initial conditions, and $\mathcal{X}_1 \subseteq \mathcal{X}$ be a compact set of the domain. The probability of reaching set $\mathcal{X}_1$ from any initial state $x_0 \in \mathcal{X}_0$ in one time-step can be upper-bounded by finding a function $B(x)$ fulfilling specific value constraints on $\mathcal{X}$, $\mathcal{X}_0$ and $\mathcal{X}_1$ as formalized below.

Theorem 1: Given the stochastic differential equation in (1) and the sets $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_0 \subseteq \mathcal{X}, \mathcal{X}_1 \subseteq \mathcal{X}$. Consider the process $x[k]$ evolving according to (1). Suppose that there exists a function $B : \mathcal{X} \to \mathbb{R}$, such that

$$B(x) \geq 1 \ \forall x \in \mathcal{X}_1 \ , \tag{3}$$

$$B(x) \geq 0 \ \forall x \in \mathcal{X} \ , \tag{4}$$

$$\mathbb{E}_w\Big[B(\mathcal{F}(x,w)) \mid x\Big] \leq \alpha \quad \forall x \in \mathcal{X}_0 \tag{5}$$

for some $\alpha \geq 0$, where $\mathbb{E}_w$ denotes the expectation with respect to w. Given $x_0 := x[0]$, define $\rho_u(x_0) := Pr\{x[1] \in \mathcal{X}_1 \mid x_0\}$. Then, for any initial state $x_0 \in \mathcal{X}_0$,

$$\rho_u(x_0) \leq Pr\left\{B(x[1]) \geq 1 \mid x_0\right\} \leq \alpha \ . \tag{6}$$

Proof: This theorem follows from Markov's inequality, as $Pr\left\{B(x[1]) \geq 1 \mid x_0\right\} \leq \frac{\mathbb{E}_w\left[B(\mathcal{F}(x_0,w)) \mid x_0\right]}{1}$. ∎

The function B in the above theorem serve as a stochastic barrier function for general systems of the form (1). Numerical procedures for finding a function B satisfying the conditions of Theorem 1 for particular polynomial systems under Assumption 1 are developed in the next section.

IV. BARRIER FUNCTION-BASED IMC ABSTRACTION

We next present a stochastic barrier function-based approach to the IMC abstraction problem for general systems of the form (1). Consider two states Q_i and Q_j from a partition P of the domain D of (1). Our goal is to determine a lower bound $\breve{T}(Q_i, Q_j)$ and an upper bound $\widehat{T}(Q_i, Q_j)$ on the probability of transitioning from any continuous state in Q_i to a state in Q_j. Then, an IMC abstraction of (1) is constructed by applying this methodology to all pairs of states in P. We assume henceforth that an over-approximation and an under-approximation of any discrete state in P can be represented as the zero-superlevel set of some polynomial function.

Assumption 2: For any state Q_i in a partition P of domain D, there exists an over-approximation $\widehat{\mathcal{X}}_{Q_i} \supset Q_i$ and an under-approximation $\breve{\mathcal{X}}_{Q_i} \subset Q_i$ such that $\widehat{\mathcal{X}}_{Q_i} = \{x \in \mathbb{R}^n \mid s_{\widehat{\mathcal{X}}_{Q_i}}(x) \geq 0\}$ and $\breve{\mathcal{X}}_{Q_i} = \{x \in \mathbb{R}^n \mid s_{\breve{\mathcal{X}}_{Q_i}}(x) \geq 0\}$, where $s_{\widehat{\mathcal{X}}_{Q_i}}$ and $s_{\breve{\mathcal{X}}_{Q_i}}$ are polynomials. Also, there exists an over-approximation $\widehat{\mathcal{X}} \supset D$ of D such that $\widehat{\mathcal{X}} = \{x \in \mathbb{R}^n \mid s_{\widehat{\mathcal{X}}}(x) \geq 0\}$, where $s_{\widehat{\mathcal{X}}}$ is a polynomial.

Finding bounds on the probability of making a transition from Q_i to Q_j in one time-step can be converted to two reachability problems over a one time-step time horizon. Indeed, by viewing Q_i as the set $\mathcal{X}_0$ in Theorem 1, determining upper bounds on the probability of reaching $\mathcal{X}_1 = Q_j$ and $\mathcal{X}_1 = D \setminus Q_j$ induces an interval on the probability of making a transition from Q_i to Q_j. We formalize this in terms of the over and under-approximation representations of these states in the following lemma.

Lemma 1: Let $\mathcal{X}_0$ and $\mathcal{X}_1$ be the sets defined in Theorem 1. Recall the exact bounds on the probability of transition from Q_i to Q_j are $\breve{T}_{ex}(Q_i, Q_j)$ and $\widehat{T}_{ex}(Q_i, Q_j)$, where Q_i and Q_j are states in partition P. Let $\widehat{\rho}_u$ be an upper bound on the probability for system (1) to reach $\mathcal{X}_1$ when $\mathcal{X}_0 = \widehat{\mathcal{X}}_{Q_i}$ and $\mathcal{X}_1 = \widehat{\mathcal{X}}_{Q_j}$, and let $\breve{\rho}_u$ be a similarly defined upper bound when $\mathcal{X}_0 = \breve{\mathcal{X}}_{Q_i}$ and $\mathcal{X}_1 = D \setminus \breve{\mathcal{X}}_{Q_j}$. Then,

$$\widehat{\rho}_u \geq \widehat{T}_{ex}(Q_i, Q_j) \ , \tag{7}$$

$$1 - \breve{\rho}_u \leq \breve{T}_{ex}(Q_i, Q_j) \ . \tag{8}$$

Proof: By assumption, the probability of making a transition to $\widehat{\mathcal{X}}_{Q_j}$ from any state $x \in \widehat{\mathcal{X}}_{Q_i}$ in one time-step is upper bounded by $\widehat{\rho}_u$. Since $Q_j \subset \widehat{\mathcal{X}}_{Q_j}$, the probability of transitioning from $\widehat{\mathcal{X}}_{Q_i}$ to Q_j cannot be greater than $\widehat{\rho}_u$. As $Q_i \subset \widehat{\mathcal{X}}_{Q_i}$, the latter also holds true for all $x \in Q_i$, proving (7). Then, the probability of transitioning to $D \setminus \breve{\mathcal{X}}_{Q_j}$ from any state $x \in \widehat{\mathcal{X}}_{Q_i}$ in one time-step is upper bounded by $\breve{\rho}_u$. Therefore, the probability of transitioning to $\breve{\mathcal{X}}_{Q_j}$ is at least $1 - \breve{\rho}_u$. Since $\breve{\mathcal{X}}_{Q_j} \subset Q_j$, the probability of transitioning to Q_j from $\widehat{\mathcal{X}}_{Q_i}$ cannot be less than $1 - \breve{\rho}_u$. As $Q_i \subset \widehat{\mathcal{X}}_{Q_i}$, the latter also holds true for all $x \in Q_i$, proving (8). ■

First, we describe a numerical procedure for computing polynomial barrier functions fulfilling the requirements of Theorem 1 for polynomial systems satisfying Assumption 1. Next, we discuss an approach for constructing tight polynomial superlevel sets that under- and over-approximate every state in partitions where all states are hyperrectangles.

A. Numerical Procedure for Barrier Function Computation

This section proposes a numerical algorithm based on the equations in Theorem 1 for computing the bounds discussed in Lemma 1. In this subsection, we assume the dynamics of the system under consideration to satisfy Assumption 1. As we wish to find transition bounds that are as tight as possible, we formulate an optimization problem that minimizes the computed upper bound probability of system (1) transitioning to a set $\mathcal{X}_1$ in one time-step as established in Theorem 1. Specifically, for a given initial set $\mathcal{X}_0$ and a set $\mathcal{X}_1$, we are interested in finding the minimum upper bound α on ρ_u such that a barrier function B satisfying conditions (3) – (5) exists. Imposing the restriction that B is a polynomial function, this problem is converted to a *Sum-of-Squares Program* (SOSP) as defined below.

Definition 6 (Sum-of-Squares Polynomial): Define $\mathbb{R}[x]$ as the set of all polynomials in $x \in \mathbb{R}^n$. Then

$$\Sigma[x] := \left\{ s(x) \in \mathbb{R}[x] : s(x) = \sum_{i=1}^{m} g_i(x)^2, g_i(x) \in \mathbb{R}[x] \right\}$$

is the set of SOS polynomials. It is noted that if $s(x) \in \Sigma[x]$ then $s(x) \geq 0 \ \forall \ x$.

Definition 7 (Sum-of-Squares Program): Given $p_i(x) \in \mathbb{R}[x]$ for $i = 0, \ldots, m$, the problem of finding $q_i(x) \in \Sigma[x]$ for $i = 1, \ldots, \hat{m}$ and $q_i(x) \in \mathbb{R}[x]$ for $i = \hat{m}+1, \ldots, m$ such that

$$p_0(x) + \sum_{i=1}^{m} p_i(x) q_i(x) \in \Sigma[x]$$

is a sum-of-squares program (SOSP). SOSPs are converted to semidefinite programs with tools such as SOSTOOLS [19].

Finding an SOS polynomial barrier functions B fulfilling constraints (4) – (6) over the sets $\mathcal{X}_0$ and $\mathcal{X}_1$ can be encoded as an SOSP: assume $\mathcal{X}_0 = \{x \in \mathbb{R}^n \mid s_{\mathcal{X}_0}(x) \geq 0\}$, $\mathcal{X}_1 = \{x \in \mathbb{R}^n \mid s_{\mathcal{X}_1}(x) \geq 0\}$ and $\mathcal{X} = \{x \in \mathbb{R}^n \mid s_{\mathcal{X}}(x) \geq 0\}$, where $s_{\mathcal{X}_0}$, $s_{\mathcal{X}_1}$ and $s_{\mathcal{X}}$ are polynomials. The SOSP $S(s_{\mathcal{X}_0}, s_{\mathcal{X}_1}, s_{\mathcal{X}})$ in Algorithm 1 finds an upper bound on the probability of making a transition from $\mathcal{X}_0$ to $\mathcal{X}_1$ in one time-step by setting α to be the objective function to minimize.

Algorithm 1 Upper-bounding SOSP $\mathcal{S}(s_{\mathcal{X}_0}, s_{\mathcal{X}_1}, s_{\mathcal{X}})$

1: **Input**: Polynomial representations $s_{\mathcal{X}_0}, s_{\mathcal{X}_1}, s_{\mathcal{X}}$ of regions $\mathcal{X}_0$, $\mathcal{X}_1$ and domain D
2: **Output**: Upper bound α^* on the probability of making a transition from $\mathcal{X}_0$ to $\mathcal{X}_1$ in one time-step
3: Solve
$$\alpha^* = \min_{\substack{\alpha,\, B(x),\\ \lambda_{\mathcal{X}}(x),\, \lambda_{\mathcal{X}_0}(x),\, \lambda_{\mathcal{X}_1}(x)}} \alpha$$
subject to
$$\begin{aligned} B(x) - \lambda_{\mathcal{X}}(x) s_{\mathcal{X}}(x) &\in \Sigma[x] \\ B(x) - \lambda_{\mathcal{X}_1}(x) s_{\mathcal{X}_1}(x) - 1 &\in \Sigma[x] \\ -\mathbb{E}_w[B(\mathcal{F}(x,w)) \mid x] + \alpha - \lambda_{\mathcal{X}_0}(x) s_{\mathcal{X}_0}(x) &\in \Sigma[x] \\ \lambda_{\mathcal{X}}(x),\ \lambda_{\mathcal{X}_0}(x),\ \lambda_{\mathcal{X}_1}(x) &\in \Sigma[x] \end{aligned}$$
4: **return** α^*

The constraints of the SOSPs are derived from the *Positivstellensatz condition* for converting constraints on sets to SOSPs as detailed in [19]. The expectation term in the SOSP is computed by expanding $B(\mathcal{F}(x,w))$ and determining the moments of the noise terms, which results in a polynomial in x when $\mathcal{F}$ is a polynomial. An important hyperparameter of this algorithm is the degree of the barrier and λ polynomials. Searching for high degree polynomials allows to find tighter bounds, at a cost of increased computational complexity.

According to Lemma 1, an upper and lower bound on the probability of transition between any two states in a partition P of the domain D can be found using function $\mathcal{S}$. Algorithm 2 summarizes the IMC abstraction procedure for system (1) with a given domain partition P.

Theorem 2: Given a system of the form (1) and partition P of its domain D, an IMC abstraction of (1) is computed via Algorithm 2.

Proof: For any states Q_i and Q_j of a partition P of the domain D of (1), Algorithm 2 computes an upper bound and a lower bound on the probability of making a transition from any continuous state in Q_i to Q_j in line 6 to 10, from Lemma 1. Moreover, Algorithm 2 applies this bounding procedure to every pair of states in P, proving the theorem. ■

B. Polynomial Under and Over-Approximation of Boxes

Algorithm 2 requires the computation of polynomial over- and under-approximation representations of the sets of interest. In this subsection, we derive a procedure for constructing tight representations of box states arising from a rectangular partition of the domain. Let Q_i denote a hyperrectangular region of the state-space, i.e., $Q_i = \{x \mid \underline{q} \leq x \leq \overline{q}\}$ for some $\underline{q}$, $\overline{q} \in \mathbb{R}^n$ satisfying $\underline{q} \leq \overline{q}$, where all inequalities are interpreted element-wise. We aim to compute an under and over-approximation of Q_i as the super-zero level sets of two polynomials, i.e, we seek to generate polynomials $s_{\widehat{\mathcal{X}}_{Q_i}}(x)$, $s_{\breve{\mathcal{X}}_{Q_i}}(x) \in \mathbb{R}[x]$ such that, for all $x \in Q_i$ we have

Algorithm 2 Barrier function-based IMC Abstraction

Input: Domain D, Domain partition P
Output: IMC Abstraction $\mathcal{I}$
Compute an over-approximation representation $s_{\widehat{\mathcal{X}}}$ of D
for $Q_i \in P$ **do**
  for $Q_j \in P$ **do**
    Compute the over and under-approximation representations $s_{\widehat{\mathcal{X}}_{Q_i}}$, $s_{\widehat{\mathcal{X}}_{Q_j}}$ and $s_{D\setminus\breve{\mathcal{X}}_{Q_j}}$
    $\widehat{\rho} := \mathcal{S}(s_{\widehat{\mathcal{X}}_{Q_i}}, s_{\widehat{\mathcal{X}}_{Q_j}}, s_{\widehat{\mathcal{X}}})$, $\breve{\rho} := \mathcal{S}(s_{\widehat{\mathcal{X}}_{Q_i}}, s_{D\setminus\breve{\mathcal{X}}_{Q_j}}, s_{\widehat{\mathcal{X}}})$
    $\widehat{T}(Q_i, Q_j) := \widehat{\rho}$, $\breve{T}(Q_i, Q_j) := 1 - \breve{\rho}$
  end for
end for
return $\mathcal{I}$

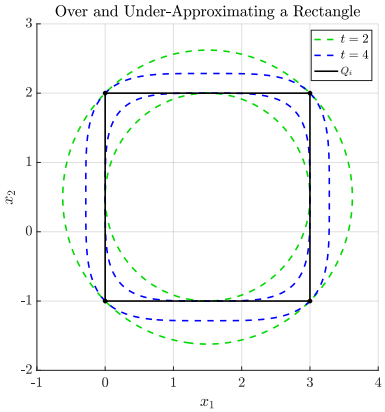

Fig. 1. Generating over and under-approximations for the rectangle $Q_i = [0,3] \times [-1,2] \subset \mathbb{R}^2$. Rectangle Q_i is shown in black, 2nd and 4th order polynomials approximations are shown in green and blue, respectively.

$s_{\widehat{\mathcal{X}}_{Q_i}}(x) \geq 0$, and, for all $x \notin Q_i$ we have $s_{\breve{\mathcal{X}}_{Q_i}}(x) < 0$. We solve this problem by employing a modified p-norm based approach, where we define the p-norm of a vector $x \in \mathbb{R}^n$ to be $||x||_p = \sqrt[p]{x_1^p + \cdots + x_n^p}$. The level sets of the function $||x||_p$ are known to be convex and to better approximate the shape of a rectangle as p increases.

Proposition 1: Given a positive even integer t, define

$$\begin{aligned} \underline{p}(x) &= \left(\tfrac{1}{2}\right)^t - x_1^t - \cdots - x_n^t \ , \\ \overline{p}(x) &= n\left(\tfrac{1}{2}\right)^t - x_1^t - \cdots - x_n^t \ . \end{aligned} \tag{9}$$

Additionally, define $q^m = \frac{1}{2}(\underline{q} + \overline{q})$ and $\widetilde{q} = \overline{q} - \underline{q}$. Then the polynomial pair $s_{\breve{\mathcal{X}}_{Q_i}}(x) := \underline{p}\big(y(x)\big)$ and $s_{\widehat{\mathcal{X}}_{Q_i}}(x) := \overline{p}\big(y(x)\big)$ respectively under- and over-approximate Q_i, where $y(x) \in \mathbb{R}^n$ is defined along each dimension by

$$y_j(x_j) = \frac{x_j - q_j^m}{\widetilde{q}_j} \ . \tag{10}$$

Proof: Define $\mathcal{C} \subset \mathbb{R}^n$ to be the rectangular region centered at the origin and with unit side length, that is, $\mathcal{C} := \left[-\frac{1}{2}\mathbb{1}_n, \ \frac{1}{2}\mathbb{1}_n\right]$, where $\mathbb{1}_n \in \mathbb{R}^n$ denotes a vector fully populated with ones. We first show that the super-zero levelsets of $\underline{p}(x), \overline{p}(x) \in \mathbb{R}[x]$ (as defined by (9)) are over- and under-approximations for $\mathcal{C}$, respectively; that is, we show $\underline{\mathcal{C}} \subseteq \mathcal{C} \subseteq \overline{\mathcal{C}}$, where we define $\underline{\mathcal{C}}, \overline{\mathcal{C}} \subset \mathbb{R}^n$ by $\underline{\mathcal{C}} := \{z \in \mathbb{R}^n \,|\, \underline{p}(z) \geq 0\}$ and $\overline{\mathcal{C}} := \{z \in \mathbb{R}^n \,|\, \overline{p}(z) \geq 0\}$.

To that end, let $z \in \mathcal{C}$ denote the center of one face of the unit box; in this case $z \in \mathbb{R}^n$ contains ± 0.5 in some position and is populated with zeros otherwise. By (9), we have $\underline{p}(z) = 0$. Therefore, the center of each face of the unit box must be contained inside $\underline{\mathcal{C}}$. Additionally $\underline{\mathcal{C}}$ is convex and symmetric in all dimensions. Thus, it holds that $\underline{\mathcal{C}} \subseteq \mathcal{C}$.

Now redefine $z \in \mathcal{C}$ to denote a corner of the unit box; in this case $z \in \mathbb{R}^n$ is defined to have ± 0.5 in every position. By (9), $\overline{p}(z) = 0$. Therefore, each corner of the unit square must be contained inside $\overline{\mathcal{C}}$. Additionally, $\overline{\mathcal{C}}$ is convex. Thus, it holds that $\mathcal{C} \subseteq \overline{\mathcal{C}}$. Following from (10), we have $x \in Q_i \iff y(x) \in \mathcal{C}$. Therefore, $x \in Q_i \iff s_{\widehat{\mathcal{X}}_{Q_i}}(x) := \overline{p}\big(y(x)\big) \geq 0$ and $x \notin Q_i \iff s_{\breve{\mathcal{X}}_{Q_i}}(x) := \underline{p}\big(y(x)\big) < 0$. ■

For p-norms, as the order of the polynomials increases, the over and under-approximations reduce in conservatism.

We illustrate the utility of Proposition 1 by calculating under and over-approximations of a rectangle in Fig. 1.

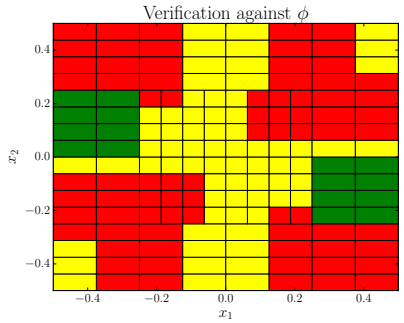

Fig. 2. Verification of system (11) against specification ϕ on a 160-state partition of D. States in green satisfy ϕ, states in red violate ϕ, and states in yellow are undecided.

V. CASE STUDY

We now demonstrate the machinery described in previous sections in a verification and synthesis case study. The code used to produce the following examples is found at `https://github.com/gtfactslab/ACCBarrier`.

A. Verification

We consider the 2-dimensional polynomial system

$$\begin{aligned} x_1[k+1] &= 6.0x_1^3 x_2 \\ x_2[k+1] &= 0.3x_1 x_2 + w \ , \end{aligned} \tag{11}$$

with domain $D = [-0.5, 0.5] \times [-0.5, 0.5]$ and Gaussian additive noise $w \sim \mathcal{N}(\mu = 0, \ \sigma = 0.18)$. The probability of transition outside of D is negligible, thus we ignore the possibility of transitioning outside of D[1]. We perform verification for these dynamics against the probabilistic specification

$$\phi = \mathcal{P}_{\geq 0.82}[\Box\neg B \wedge (\Diamond C \vee \bigcirc A \vee \bigcirc\bigcirc A)] \ ,$$

where the specification inside the probabilistic operator translates to "Never reach a B state and either eventually reach a

[1]Alternatively, a "sink" state can be used for all states outside of D.

C state or reach an A state in 2 time steps". The partition of the domain D is assumed to be as in Fig.1 and contains 160 states. The A states are located in $[-0.25, 0] \times [0.25, 0.5]$; the B states in $[-0.5, -0.25] \times [0.25, 0.5]$ and $[0.25, 0.5] \times [-0.5, -0.25]$; the C states in $[-0.5, -0.25] \times [0, 0.25]$ and $[0.25, 0.5] \times [-0.25, 0]$. We construct an IMC abstraction of the system using the procedure in Section IV-A. Given an IMC abstraction, formal techniques are applicable for verification with respect to ϕ [2]. Note that no SOS barrier function can ensure a transition upper bound of exactly zero. Thus, we apply a pre-processing step where states that are unreachable from one another have their upper bound probability of transition set to 0. To do so, we compute the range of reachable x_1 values for each state using the fact that the x_1 dynamics are locally monotone in the partition states, and identify the states lying outside this range. We search for SOS polynomials of degree 6 in the SOSP. To approximate each state with polynomial superlevel sets, we use shifted and scaled versions of 4th order polynomials, as detailed in Section IV-B. The result of verification is displayed in Fig. 2. States in green satisfy ϕ, states in red violate ϕ, and states in yellow are undecided. To reduce the volume of undecided states, refinement of the partition can be applied [7].

B. Synthesis

We now consider the two-mode system

$$\begin{aligned} x_1[k+1] &= a_i x_1^3 x_2 \\ x_2[k+1] &= b_i x_1 x_2 + w \ , \end{aligned}$$

for $i \in \{1, 2\}$, where $(a_1, b_1) = (6.0, 0.3)$ in the first mode, $(a_2, b_2) = (7.0, 0.2)$ in the second mode, and the domain D and noise term w are as in the verification case study.

Our goal is to find a switching policy minimizing the probability of satisfying the specification inside the probabilistic operator in ϕ. To do this, we build a BMDP abstraction of the system by constructing an IMC abstraction for each mode. Formal techniques can be utilized on this abstraction for controller synthesis [18]. The partition is the same as in the previous subsection. We check our results against Monte-Carlo simulations with initial state $x_0 = [0.15, -0.2]$. The computed switching policy guarantees a probability of satisfying the specification between [0, 0.81] from x_0, which is confirmed in simulations with a probability of 0.1008.

C. Discussion

The strength of our IMC and BMDP abstraction method lies in its applicability to the wide class of discrete-time polynomial stochastic systems. Such abstractions allow us to perform verification and synthesis for these systems against all ω-regular specifications. On the other hand, the computational complexity of this method, which depends heavily on the hyperparameters of the SOSP, varies greatly with the dynamics of interest. As all transitions computations are parallelizable, the viability of this technique for verification and synthesis relies on the available parallel computing capabilities. For instance, building the abstraction for the verification case study on a 2-core machine took 14 hours.

[2]For example, we propose such a technique in [7].

VI. CONCLUSIONS

This paper addressed the problem of generating IMC and BMDP abstractions for discrete-time polynomial stochastic systems. The construction of these IMCs and BMDPs was achieved by solving an SOSP for each transition bound in the abstraction. A technique for creating tight polynomial under and over-approximations of hyperrectangular states, required for the formulation of the SOSPs, was presented.

REFERENCES

[1] P. Florchinger, "Lyapunov-like techniques for stochastic stability," *SIAM Journal on Control and optimization*, vol. 33, no. 4, pp. 1151–1169, 1995.

[2] 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.

[3] A. Abate, J.-P. Katoen, J. Lygeros, and M. Prandini, "Approximate model checking of stochastic hybrid systems," *European Journal of Control*, vol. 16, no. 6, pp. 624–641, 2010.

[4] S. Summers and J. Lygeros, "Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem," *Automatica*, vol. 46, no. 12, pp. 1951–1961, 2010.

[5] A. Abate, A. D'Innocenzo, and M. D. Di Benedetto, "Approximate abstractions of stochastic hybrid systems," *IEEE Transactions on Automatic Control*, vol. 56, no. 11, pp. 2688–2694, 2011.

[6] I. O. Kozine and L. V. Utkin, "Interval-valued finite Markov chains," *Reliable computing*, vol. 8, no. 2, pp. 97–113, 2002.

[7] M. Dutreix and S. Coogan, "Specification-Guided Verification and Abstraction Refinement of Mixed-Monotone Stochastic Systems," *arXiv e-prints*, p. arXiv:1903.02191, Mar 2019.

[8] K. Chatterjee, K. Sen, and T. Henzinger, "Model-checking ω-regular properties of interval markov chains," *Foundations of Software Science and Computational Structures*, pp. 302–317, 2008.

[9] N. Cauchi, L. Laurenti, M. Lahijanian, A. Abate, M. Kwiatkowska, and L. Cardelli, "Efficiency through uncertainty: Scalable formal synthesis for stochastic hybrid systems," *arXiv:1901.01576*, 2019.

[10] M. Dutreix and S. Coogan, "Efficient verification for stochastic mixed monotone systems," in *International Conference on Cyber-Physical Systems*, 2018.

[11] C. Santoyo, M. Dutreix, and S. Coogan, "A Barrier Function Approach to Finite-Time Stochastic System Verification and Control," *arXiv e-prints*, p. arXiv:1909.05109, Sep 2019.

[12] J. Steinhardt and R. Tedrake, "Finite-time regional verification of stochastic non-linear systems," *The International Journal of Robotics Research*, vol. 31, no. 7, pp. 901–923, 2012.

[13] 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, no. 8, pp. 1415–1428, 2007.

[14] S. E. Z. Soudjani, C. Gevaerts, and A. Abate, "Faust 2: Formal abstractions of uncountable-state stochastic processes," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2015, pp. 272–286.

[15] N. Cauchi, K. Degiorgio, and A. Abate, "Stochy: automated verification and synthesis of stochastic processes," *arXiv preprint arXiv:1901.10287*, 2019.

[16] C. Baier, J.-P. Katoen, and K. G. Larsen, *Principles of model checking*. MIT press, 2008.

[17] R. Givan, S. Leach, and T. Dean, "Bounded-parameter Markov decision processes," *Artificial Intelligence*, vol. 122, no. 1-2, pp. 71–109, 2000.

[18] M. Dutreix, J. Huh, and S. Coogan, "Abstraction-based synthesis for stochastic systems with omega-regular objectives," 2020, arXiv:2001.09236.

[19] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo, "Sostools: Sum of squares optimization toolbox for matlab," *https://www.cds.caltech.edu/sostools/*, 2004, `http://arxiv.org/abs/1310.4716`.