

Data-Driven Strategy Synthesis for Stochastic Systems with Unknown Nonlinear Disturbances

Ibon Gracia

University of Colorado Boulder

IBON.GRACIA@COLORADO.EDU

Dimitris Boskos

Delft University of Technology

D.BOSKOS@TUDELFT.NL

Luca Laurenti

Delft University of Technology

L.LAURENTI@TUDELFT.NL

Morteza Lahijanian

University of Colorado Boulder

MORTEZA.LAHIJANIAN@COLORADO.EDU

Editors: A. Abate, M. C. A. K. Margellos, A. Papachristodoulou

Abstract

In this paper, we introduce a data-driven framework for synthesis of provably-correct controllers for general nonlinear switched systems under complex specifications. The focus is on systems with *unknown* disturbances whose effects on the dynamics of the system is nonlinear. The specification is assumed to be given as *linear temporal logic over finite traces* (LTL_f) formulas. Starting from observations of either the disturbance or the state of the system, we first learn an *ambiguity set* that contains the unknown distribution of the disturbances with a user-defined confidence. Next, we construct a *robust Markov decision process* (RMDP) as a finite abstraction of the system. By composing the RMDP with the automaton obtained from the LTL_f formula and performing optimal robust value iteration on the composed RMDP, we synthesize a strategy that yields a high probability that the uncertain system satisfies the specifications. Our empirical evaluations on systems with a wide variety of disturbances show that the strategies synthesized with our approach lead to high satisfaction probabilities and validate the theoretical guarantees.

Keywords: Formal synthesis, Switched stochastic systems, Robust Markov decision processes, Wasserstein distance, Data-driven control, Nonlinear Control, Nonlinear disturbances

1. Introduction

Stochastic dynamical systems are powerful mathematical models commonly employed to describe complex systems in many applications, ranging from autonomous systems (Kumar and Varaiya, 2015) to biological systems (Anderson and Kurtz, 2011). Many of these applications are *safety-critical*, and formal correctness guarantees are required to avoid fatal or costly accidents. Another common feature of these applications is that they are characterized by nonlinear dynamics and that the characteristics of the noise affecting the system dynamics are often uncertain and need to be estimated from data (Rahimian and Mehrotra, 2019). That is, the system is both characterized by *aleatoric* uncertainty (i.e., the uncertainty intrinsic in the system dynamics) and by *epistemic* uncertainty (i.e., the uncertainty due to the lack of knowledge of the system dynamics). A challenging research question that still remains open is *how to provide formal correctness guarantees for nonlinear stochastic systems whose noise distribution is unknown?* which is the focus of this work.

Formal guarantees of correctness for nonlinear stochastic systems are generally provided either via formal abstractions into a finite transition model, typically a variant of a Markov model

(Lahijanian et al., 2015; Cauchi et al., 2019; Lavaei et al., 2022), or via stochastic barrier functions (Jagtap et al., 2020; Mazouz et al., 2022; Santoyo et al., 2021; Lechner et al., 2022). However, all those works assume a known model and known disturbances, i.e., no *epistemic uncertainty*. To tackle this issue and account for epistemic uncertainty, data-driven formal approaches have been recently developed to estimate model dynamics from data (Martin et al., 2023; Jackson et al., 2021b; Schön et al., 2023). These works generally employ concentration inequalities to estimate the system dynamics from noisy measurements of the system and then rely on existing formal methods for verification and control of the estimated model. However, these approaches generally assume that the noise distribution of the system is known and only the vector field of the dynamics needs to be learnt. In addition, they often restrict themselves to linear disturbances. The complementary case where the noise distribution is unknown and needs to be estimated from data is considered in (Badings et al., 2023b; Mathiesen et al., 2023; Gracia et al., 2023), which however, are specific for linear systems or additive noise.

In this paper, we propose a formal data-driven approach for controller synthesis of nonlinear stochastic systems with unknown disturbances against linear temporal logic specifications over finite traces (LTL_f) (De Giacomo and Vardi, 2013). Our approach combines tools from optimal transport theory with abstractions methods. In particular, given a dataset, we first exploit results from (Fournier, 2022) to build an *ambiguity set* for the disturbance distribution, that is, a set of distributions that contains the unknown law of the disturbance with high confidence. Then, we abstract the resulting uncertain model into a robust Markov decision process (RMDP) (Nilim and El Ghaoui, 2005), which formally accounts for both aleatoric and epistemic uncertainty in the system. The resulting abstraction is employed to synthesize a controller that maximizes the probability that the system satisfies an LTL_f property and is robust against the uncertainties, thus guaranteeing correctness. The efficacy of our framework is illustrated on various benchmarks showing how our approach can successfully synthesize high-confidence formal controllers for uncertain nonlinear stochastic systems from data.

The key contributions of this paper are:

- a novel strategy synthesis framework for nonlinear switched stochastic systems with general (e.g., non-additive) disturbances of unknown distributions under LTL_f specifications,
- an efficient procedure to obtain a finite and sound abstraction of said class of systems,
- probabilistic satisfaction guarantees whose confidence is independent of the abstraction size,
- extensive case studies and empirical evaluations involving five different systems, several choices of hyperparameters, and comparisons with the state-of-the-art approaches.

Basic Notation The set of non-negative integers is defined as $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For a set X , $|X|$ denotes its cardinality. Given $X \subseteq \mathbb{R}^n$ we denote by $\mathbb{1}_X$ its indicator function, that is $\mathbb{1}_X(x) = 1$ if $x \in X$ and 0 otherwise. We let $\mathcal{B}(X)$ be the Borel σ -algebra of X and $\mathcal{P}(X)$ denote the set of probability distributions on $(X, \mathcal{B}(X))$. For $P \in \mathcal{P}(X)$ and $x \in X$, $P(x)$ denotes the probability of the (singleton) event $\{x\}$. Given a continuous cost $c : X \times X \rightarrow \mathbb{R}_{\geq 0}$, we denote by $\mathcal{P}_c(X)$ the set of distributions $P \in \mathcal{P}(X)$ with $\int_X c(x, x') P(dx) < \infty$ for some $x' \in X$. The optimal transport discrepancy between $P, P' \in \mathcal{P}_c(X)$ is defined as $\mathcal{T}^c(P, P') = \inf_{\pi \in \Pi(P, P')} \int_{X \times X} c(x, x') \pi(dx, dx')$, where $\Pi(P, P')$ is the set of distributions on $\mathcal{P}(X \times X)$ with marginals P and P' . For an l -norm $\|\cdot\|_l$, with $l \in [1, \infty]$, and $s \geq 1$, if $c(x, x') = \|x - x'\|_l^s$ for all $x, x' \in X$, we use the notation $\mathcal{T}_s^{(l)}(P, P')$. Furthermore, if $X \subseteq \mathbb{R}^d$, then $\mathcal{W}_s(P, P') := (\mathcal{T}_s^{(l)}(P, P'))^{1/s}$ is the s -Wasserstein distance between P and P' . We let $\delta_x \in \mathcal{P}(X)$ be the Dirac measure located at $x \in X$. We use bold symbols, e.g., $\mathbf{x}$, to denote random variables.

2. Problem Formulation

In this work, we focus on discrete-time switched stochastic processes described by

$$\mathbf{x}_{k+1} = f_{a_k}(\mathbf{x}_k, \mathbf{w}_k), \quad (1)$$

where $\mathbf{x}_k \in \mathbb{R}^n$ is the state and $a_k \in A := \{a_1, \dots, a_{|A|}\}$ is the control (mode or action) at time k . Noise term $\mathbf{w}_k \in W$ is an i.i.d. random variable taking values in a bounded set $W \subset \mathbb{R}^d$ with probability distribution P_w identical at each time step k . Distribution P_w , however, is assumed to be *unknown*. For each $a \in A$, $f_a : \mathbb{R}^n \times W \rightarrow \mathbb{R}^n$ is the vector field, which is assumed to be Lipschitz continuous in w with Lipschitz constant $L_w(x, a) \geq 0$, i.e., $\|f_a(x, w) - f_a(x, w')\| \leq L_w(x, a)\|w - w'\|$ for all $w, w' \in W$. Consequently, Process (1) describes a general model of nonlinear switched stochastic process, which encompasses many models commonly used in practice.

For $x_0, \dots, x_K \in \mathbb{R}^n$ and $K \in \mathbb{N}_0$, $\omega_x = x_0 \xrightarrow{a_0} x_1 \xrightarrow{a_1} \dots \xrightarrow{a_{K-1}} x_K$ represents a finite *trajectory* of Process (1), and Ω_x is the set of all finite trajectories (of any length). We denote by $\omega_x(k)$ the state of ω_x at time $k \in \{0, \dots, K\}$. A *switching strategy* $\sigma_x : \Omega_x \rightarrow A$ is a function that assigns an action $a \in A$ to each finite trajectory. For $x \in \mathbb{R}^n$, $a \in A$ and $B \in \mathcal{B}(\mathbb{R}^n)$, the *transition kernel* of Process (1) is $T^a(B | x) = \int_W \mathbb{1}_B(f_a(x, v))P_w(dv)$. Given a strategy σ_x and an initial condition $x_0 \in \mathbb{R}^n$, the transition kernel uniquely defines a probability measure $P_{x_0}^{\sigma_x}$ over the trajectories of Process (1) (Bertsekas and Shreve, 1996) such that $P_{x_0}^{\sigma_x}[\omega_x(k) \in X]$ represents the probability that, under strategy σ_x , $\mathbf{x}_k$ is in set $X \subseteq \mathbb{R}^n$ starting from x_0 .

Given a bounded set $X \subset \mathbb{R}^n$, we are interested in the temporal properties of Process (1) w.r.t. a set of regions of interest $R := \{r_1, \dots, r_{|R|-1}, r_u\}$ with $r_i \subseteq X$ for all $i \leq |R|-1$, and $r_u = \mathbb{R}^n \setminus X$. To each region $r_i \in R$, we associate an atomic proposition $\mathbf{p}_i$, and say that $\mathbf{p}_i \equiv \top$ (i.e., $\mathbf{p}_i$ is *true*) at $x \in \mathbb{R}^n$ iff $x \in r_i$. Denote by $AP := \{\mathbf{p}_1, \dots, \mathbf{p}_{|R|-1}, \mathbf{p}_u\}$ the set of all atomic propositions and define the labeling function $L : \mathbb{R}^n \rightarrow 2^{AP}$ as the function that maps each state $x \in \mathbb{R}^n$ to the set of atomic propositions that are true at that state, i.e., $\mathbf{p}_i \in L(x)$ iff $x \in r_i$. Then, to each trajectory $\omega_x = x_0 \xrightarrow{a_0} x_1 \xrightarrow{a_1} \dots \xrightarrow{a_{K-1}} x_K$, we can associate the (observation) *trace* $\rho = \rho_0\rho_1 \dots \rho_K$, where $\rho_k := L(x_k)$ for all $k \in \{0, \dots, K\}$.

To specify temporal properties of Process (1), we use LTL_f (De Giacomo and Vardi, 2013), which is a formal language commonly employed to express finite behaviors. An LTL_f formula φ is defined from a set of atomic propositions AP and is closed under the Boolean connectives “negation” ($\neg$) and “conjunction” ($\wedge$), and the temporal operators “until” ($\mathcal{U}$) and “next” ($\mathcal{X}$):

$$\varphi := \top \mid \mathbf{p} \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathcal{X}\varphi \mid \varphi_1 \mathcal{U} \varphi_2$$

where $\mathbf{p} \in AP$ and φ_1, φ_2 are LTL_f formulas themselves. The temporal operators “eventually”, $\mathcal{F}$, and “globally”, $\mathcal{G}$, are defined as $\mathcal{F}\varphi := \top \mathcal{U} \varphi$ and $\mathcal{G}\varphi := \neg \mathcal{F}(\neg \varphi)$. The semantics (interpretation) of LTL_f are defined over finite traces (De Giacomo and Vardi, 2013). We say a trajectory ω_x satisfies a formula φ , denoted by $\omega_x \models \varphi$, if a prefix of its trace ρ satisfies the formula.

We are interested in synthesizing a strategy that maximizes the probability that Process (1) satisfies a given LTL_f formula, while accounting for the uncertainty coming from the fact that P_w is unknown and can only be estimated from data. A formal statement of the problem is as follows.

Problem 1 Consider the switched stochastic Process (1), a set $\{\mathbf{w}^{(i)}\}_{i=1}^N$ of N i.i.d. samples of P_w , a bounded set $X \subset \mathbb{R}^n$, and an LTL_f formula φ defined over the regions of interest R . Then,

given a confidence level $1 - \beta \in (0, 1)$, synthesize a switching strategy σ_x such that, for every initial state $x_0 \in X$, with confidence at least $1 - \beta$, σ_x maximizes the probability that the paths $\omega_x \in \Omega_x$ satisfy φ while remaining in X , i.e., $\sigma_x \in \arg \max_{\sigma_x} P_{x_0}^{\sigma_x}[\omega_x \models \varphi \wedge \mathcal{G}\neg \mathbf{p}_u]$.

Note that in Problem 1 the noise distribution P_w is unknown. Consequently, P_w must be estimated from data. This inevitably leads to a confidence probability on the resulting strategy, which irrespective of the method of quantification, depends on the data. Problem 1 requires this confidence to be at least $1 - \beta$. We should also remark that we assume that a set of N samples from the noise is given. This may seem like a strong assumption as, in general, only observations $\{\mathbf{y}^{(i)}\}_{i=1}^{N+1}$ of the state can be collected. However, in several cases, e.g., when successive full-state observations $\mathbf{y}^{(i)} = \mathbf{x}^{(i)}$ are available, one can use the system's dynamics $\mathbf{y}^{(i+1)} = f_{a^{(i)}}(\mathbf{y}^{(i)}, \mathbf{w}^{(i)})$ and knowledge of its actions $a^{(i)}$ to obtain i.i.d. samples $\{\mathbf{w}^{(i)}\}_{i=1}^N$ of the noise distribution P_w . For instance, this is possible when f is linear in w or, more generally, if the data are collected where $f_{a^{(i)}}(\mathbf{y}^{(i)}, \cdot) : W \rightarrow \mathbb{R}^n$ is injective. Such regions can be easily identified in many non-linear systems commonly employed in practice, as shown in the examples in Section 6.

Overview of the approach Since P_w is unknown and the state space of the process is uncountable, obtaining the exact solution to Problem 1 is generally infeasible. Hence, we follow an abstraction-based approach instead and synthesize an optimal strategy that is robust against the uncertainty in estimating P_w from data. First, in Section 4.1, we use the noise samples to learn an ambiguity set of probability distributions that contains P_w with confidence $1 - \beta$. Next, in Section 4.3.1, we obtain an interval MDP (IMDP) abstraction of Process (1) by considering that $\mathbf{w}$ is distributed according to a fixed distribution supported on the samples. In Section 4.3.2, to account for all the distributions in the ambiguity set, we expand the set of transition probabilities of the IMDP, obtaining a robust MDP. Then, in Section 5, we synthesize a (robust) optimal strategy for the robust MDP via robust dynamic programming. Finally, we refine this strategy to the original system, obtaining a guaranteed lower bound on the satisfaction of the LTL_f specification for Process (1).

3. Preliminaries on Robust Markov Decision Processes

A robust MDP (RMDP) is a generalization of a Markov decision process in which the transition probability distributions are uncertain and belong to an ambiguity set (Nilim and El Ghaoui, 2005; Wiesemann et al., 2013).

Definition 1 (Robust MDP) A labelled robust Markov decision process (RMDP) $\mathcal{M}$ is a tuple $\mathcal{M} = (Q, A, \Gamma, q_0, AP, L)$, where

- Q and A are respectively a finite set of states and actions with q_0 being the initial state,
- $\Gamma = \{\Gamma_{q,a} : q \in Q, a \in A\}$, where $\Gamma_{q,a} \subseteq \mathcal{P}(Q)$ is the set of transition probability distributions for state-action pair $(q, a) \in Q \times A$,¹
- AP is a finite set of atomic propositions, and $L : Q \rightarrow 2^{AP}$ is the labeling function.

A finite path of RMDP $\mathcal{M}$ is a sequence of states $\omega = q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} \dots \xrightarrow{a_{K-1}} q_K$ such that $a_k \in A$ and there exists $\gamma \in \Gamma_{q_k, a_k}$ with $\gamma(q_{k+1}) > 0$ for all $k \in \{0, \dots, K-1\}$. We denote the

1. Notice that for two distinct state-action pairs, the respective sets of transition probability distributions of $\mathcal{M}$ are independent. This is the well-known *rectangular* property of robust MDPs (Nilim and El Ghaoui, 2005; Wiesemann et al., 2013).

set of all paths of finite length by Ω . Given a path $\omega \in \Omega$, we let $\omega(k) = q_k$ be the state of ω at time $k \in \{0, \dots, K\}$, and $\text{last}(\omega)$ be its last state. A labelled interval-valued MDP (IMDP) $\mathcal{I}$, also called bounded-parameter MDP (BMDP) (Givan et al., 2000), is an RMDP $\mathcal{I} = (Q, A, \Gamma, q_0, AP, L)$ where the transition probabilities lie within independent intervals. That is, $\Gamma_{q,a} = \{\gamma \in \mathcal{P}(Q) : \underline{P}(q, a, q') \leq \gamma(q') \leq \overline{P}(q, a, q') \text{ for all } q, q' \in Q, a \in A\}$.

Given a finite path of an RMDP or IMDP, a *strategy* σ chooses the next action. Formally, $\sigma : \Omega \rightarrow A$ is a function that assigns an action $a \in A$ to each finite path $\omega \in \Omega$ of $\mathcal{M}$. Any given strategy $\sigma \in \Sigma$ restricts the set of feasible transition probability distributions of the RMDP, thus yielding a set of Markov chains, or robust Markov chain. To further reduce this set to a single Markov chain, we define the adversary function (Givan et al., 2000) that chooses the distribution of the next state. Formally, an *adversary* is a function $\xi : \Omega \times A \rightarrow \mathcal{P}(Q)$ that maps each finite path $\omega \in \Omega$ and action $a \in A(\text{last}(\omega))$ to an admissible distribution $\gamma \in \Gamma_{q,a}$. The set of all adversaries is denoted by Ξ . Given an initial condition $q_0 \in Q$, a strategy $\sigma \in \Sigma$ and an adversary $\xi \in \Xi$, the RMDP collapses to a Markov chain with a unique probability distribution $Pr_{\xi}^{q_0, \sigma}$ on its paths.

4. Robust MDP Abstraction

Our approach is based on finite abstraction of Process (1) to an RMDP via ambiguity set learning. First, in Section 4.1 we show how we can build an ambiguity set that contains P_w with high confidence, and then, in the rest of the Section, we show how to build an RMDP abstraction $\mathcal{M} = (Q, A, \Gamma, AP, q_0, L)$ that formally accounts for this uncertainty.

4.1. Learning the Unknown Probability Distribution

In this section, we make use of the samples of $\mathbf{w}$ to obtain a formal representation of the unknown distribution P_w . Specifically, we learn an ambiguity set, i.e., a set of probability distributions that is guaranteed to contain P_w with high confidence. In particular, Lemma 2 below allows us to build an ambiguity set of distributions centered on the empirical distribution generated by the samples.

Lemma 2 (Ambiguity set) *Given $s \in \mathbb{N}$, $l \in [1, \infty]$, and N i.i.d. samples $\mathbf{w}^{(1)}, \dots, \mathbf{w}^{(N)}$ from P_w , define their empirical distribution as $\hat{P}_w := \frac{1}{N} \sum_{i=1}^N \delta_{\mathbf{w}^{(i)}}$. Further, let ϕ be the diameter of W in the ∞ -norm, $\beta \in (0, 1)$, and $g(N, \phi, d, s, l)$ be the upper bound on the expected transport cost $\mathbb{E}[\mathcal{T}_s^{(l)}(P_w, \hat{P}_w)]$ between P_w and $\hat{P}_w$ given in Fournier (2022). Then the Wasserstein ball*

$$\mathcal{D} := \{P \in \mathcal{P}(W) : \mathcal{W}_s(P, \hat{P}_w) \leq \varepsilon(N, \beta)\}, \quad (2)$$

where $\varepsilon(N, \beta) := g(N, \phi, d, s, l)^{\frac{1}{s}} + \phi\sqrt{d}(2 \log 1/\beta)^{\frac{1}{2s}} N^{-\frac{1}{2s}}$, contains P_w with confidence $1 - \beta$.

Proof In analogy to the proof of (Boskos et al., 2023, Proposition 24 of arXiv version), we leverage the fact that $\mathcal{W}_s(P_w, \hat{P}_w)$ concentrates around its mean (Boissard and Le Gouic, 2014): $\mathbb{P}(\mathcal{W}_s^{(l)}(P_w, \hat{P}_w) \geq \mathbb{E}[\mathcal{W}_s^{(l)}(P_w, \hat{P}_w)] + \tau) \leq e^{-N\tau^{2s}/(2\phi^{2s})}$, $\forall \tau \geq 0$. By the definition of the s -Wasserstein distance and Jensen's inequality, $\mathbb{E}[\mathcal{W}_s^{(l)}(P_w, \hat{P}_w)] := \mathbb{E}[(\mathcal{T}_s^{(l)}(P_w, \hat{P}_w))^{1/s}] \leq \mathbb{E}[\mathcal{T}_s^{(l)}(P_w, \hat{P}_w)]^{1/s}$, so $\forall \tau \geq 0$, $\mathbb{P}(\mathcal{W}_s^{(l)}(P_w, \hat{P}_w) \geq \mathbb{E}[\mathcal{T}_s^{(l)}(P_w, \hat{P}_w)]^{1/s} + \tau) \leq e^{-N\tau^{2s}/(2\phi^{2s})}$. Selecting τ such that $\beta = e^{-N\tau^{2s}/(2\phi^{2s})}$ and setting $\varepsilon := \mathbb{E}[\mathcal{T}_s^{(l)}(P_w, \hat{P}_w)]^{1/s} + \tau$, we arrive at the desired result. $\blacksquare$

It is important to stress that in all cases $g \rightarrow 0$ as N increases. Thus, the radius of the ambiguity set $\mathcal{D}$ shrinks with more data.

4.2. States, Actions and Labeling Function of the Abstraction

The state-space of the abstraction is obtained as follows. First, we partition set X into the set of non-empty, non-overlapping regions $Q_{\text{safe}} := \{q_1, \dots, q_{|Q_{\text{safe}}|}\}$, i.e., $q \cap q' = \emptyset$ for all $q \neq q' \in Q_{\text{safe}}$ and $\cup_{q \in Q_{\text{safe}}} q = X$. Furthermore, this partition must respect the regions of interest, i.e., for every $r \in R$ and $q \in Q_{\text{safe}}$, $q \cap r \in \{\emptyset, q\}$. The state space is then defined by associating each state of the abstraction with a region in Q_{safe} and the additional “unsafe” region $q_u = \mathbb{R}^n \setminus X$, i.e., $Q := Q_{\text{safe}} \cup \{q_u\}$. With a small abuse of notation, we let $q \in Q$ denote at the same time a state of the abstraction and a region in $\mathbb{R}^n$. We also let the actions of the abstraction A be the same as those of Process (1), with $A(q) := A$ for all $q \in Q$. Furthermore, with an additional abuse of notation, we define the abstraction labeling function as $L : Q \rightarrow 2^{AP}$ such that $L(q) := L(x)$ if $x \in q$ for all $q \in Q$. Note that we do not fix the initial state, since our approach yields results for every $q_0 \in Q$.

4.3. Transition Probability Distributions of the Abstraction

4.3.1. ACCOUNTING FOR THE DISCRETIZATION ERROR

To embed the discretization error into the abstraction, we first abstract Process (1) to an IMDP $\mathcal{I} := (Q, A, \hat{\Gamma}, q_0, AP, L)$, namely the “empirical IMDP”, under the assumption that $\mathbf{w}_k$ is distributed according to the empirical distribution $\hat{P}_w$. Components Q , A , q_0 , AP , and L of $\mathcal{I}$ are as defined above. The following proposition defines the transition probability intervals $\hat{\Gamma}$ of $\mathcal{I}$.

Proposition 3 *Let $T_{\hat{P}_w}^u$ be the transition kernel of Process (1) when $\mathbf{w}_t \sim \hat{P}_w$, i.e., for $B \in \mathcal{B}(\mathbb{R}^n)$, $x \in X$, and $a \in A$, $T_{\hat{P}_w}^a(B | x) = \int_W \mathbb{1}_B(f_a(x, v)) \hat{P}_w(dv)$. Further, define $\text{Reach}(q, a, \mathbf{w}^{(i)}) := \{f_a(x, \mathbf{w}^{(i)}) \in \mathbb{R}^n : x \in q\}$. Then, for every $q \in Q_{\text{safe}}$, $q' \in Q$, and $a \in A$,*

$$\min_{x \in q} T_{\hat{P}_w}^a(q' | x) \geq \frac{1}{N} |\{i \in \{1, \dots, N\} : \text{Reach}(q, a, \mathbf{w}^{(i)}) \subseteq q'\}| \quad (3a)$$

$$\max_{x \in q} T_{\hat{P}_w}^a(q' | x) \leq \frac{1}{N} |\{i \in \{1, \dots, N\} : \text{Reach}(q, a, \mathbf{w}^{(i)}) \cap q' \neq \emptyset\}|. \quad (3b)$$

Proof Let $x \in X$, $a \in A$. Then, from the definition of the empirical distribution, we have $T_{\hat{P}_w}^a(q' | x) = \int_W \mathbb{1}_{q'}(f_a(x, v)) \hat{P}_w(dv) = \frac{1}{N} \sum_{i=1}^N \mathbb{1}_{q'}(f_a(x, \mathbf{w}^{(i)}))$ for all $q' \in Q$. For all $x \in q$, $q \in Q_{\text{safe}}$, the previous probability is upper bounded by $T_{\hat{P}_w}^a(q' | x) \leq \frac{1}{N} \sum_{i=1}^N \max_{x \in q} \mathbb{1}_{q'}(f_a(x, \mathbf{w}^{(i)})) = \frac{1}{N} |\{i \in \{1, \dots, N\} : \text{Reach}(q, a, \mathbf{w}^{(i)}) \cap q' \neq \emptyset\}|$, which yields (3b). Analogously, we obtain the lower bound (3a), which completes the proof. $\blacksquare$

We complete the abstraction $\mathcal{I}$ by defining the transition probability bounds $\underline{P}(q, a, q')$, $\overline{P}(q, a, q')$ of $\mathcal{I}$ as the bounds in (3) for all $q \in Q_{\text{safe}}$, $q' \in Q$, and $a \in A$. In this paper, following the approach in (Adams et al., 2022), we over-approximate the reachable sets by using affine relaxations of f , which yields sound and tight transition probabilities. To further ensure that the paths of $\mathcal{I}$ that exit Q_{safe} do not satisfy the specifications, we make q_u absorbing by setting $\underline{P}(q_u, a, q_u) = \overline{P}(q_u, a, q_u) = 1$ for all $a \in A$. These bounds define the set of transition probability distributions of $\mathcal{I}$: for all $q \in Q$, $a \in A$,

$$\hat{\Gamma}_{q,a} = \{\gamma \in \mathcal{P}(Q) : \underline{P}(q, a, q') \leq \gamma(q') \leq \overline{P}(q, a, q') \text{ for all } q' \in Q\}. \quad (4)$$

4.3.2. ACCOUNTING FOR THE DISTRIBUTIONAL AMBIGUITY

In section 4.3.1, we obtain an abstraction of Process (1) when the disturbance is distributed according to the center of the ambiguity set $\mathcal{D}$ in (2), i.e., $\hat{P}_w$. To obtain a sound abstraction of Process (1), we now need to account for all the distributions in said ambiguity set $\mathcal{D}$. To this end, we take $\mathcal{I}$ as a starting point and expand its set of transition probabilities according to $\mathcal{D}$, which yields the RMDP $\mathcal{M}$. However, since we consider nonlinear disturbances, we must first translate the distributional ambiguity in $\mathcal{P}(W)$ to distributional ambiguity on $\mathcal{P}(\mathbb{R}^n)$. Then, we leverage the results from optimal control of RMDPs (Gracia et al., 2023, 2022) to conclude correctness of the abstraction.

Define the cost $c : Q^2 \rightarrow \mathbb{R}_{\geq 0}$ s.t. $c(q, q') := \inf\{\|x - x'\|_l^s, x \in q, x' \in q'\}$ for all $q, q' \in Q$. The sets of transition probability distributions of the RMDP abstraction are defined as follows.

Definition 4 (Transition Probability Distributions of the RMDP Abstraction) *Consider the cost c and the set $\hat{\Gamma}$ of $\mathcal{I}$ as defined in (4). Let $L_w(q, a) = \max_{x \in q} L_w(x, a)$ for all $q \in Q_{\text{safe}}$, $a \in A$ and $\varepsilon(N, \beta)$ be as in Lemma 2 with $\beta \in (0, 1)$. We define the sets of transition probability distributions of $\mathcal{M}$ as $\Gamma_{q,a} := \{\gamma \in \mathcal{P}(Q) : \exists \hat{\gamma} \in \hat{\Gamma}_{q,a} \text{ s.t. } \mathcal{T}^c(\gamma, \hat{\gamma}) \leq (L_w(q, a)\varepsilon(\beta, N))^s\}$ for all $q \in Q_{\text{safe}}$, $a \in A$, and $\Gamma_{q_u,a} = \hat{\Gamma}_{q_u,a}$ for all $a \in A$, so the unsafe state remains absorbing.²*

The following proposition guarantees that the RMDP constructed per Def. 4 is a sound abstraction of Process (1), i.e., that every $P \in \mathcal{D}$, when propagated through f , has a discrete equivalent in Γ .

Proposition 5 (Soundness of the abstraction) *Consider the RMDP $\mathcal{M} = (Q, A, \Gamma, q_0, AP, L)$ as described in this section. Define, for all $x \in X$, $a \in A$, the distributions $\gamma_{x,a} \in \mathcal{P}(Q)$ such that $\gamma_{x,a}(q') := T^a(q' \mid x)$ for all $q' \in Q$. Then it holds that $\mathbb{P}(\gamma_{x,a} \in \Gamma_{q,a} \mid \forall x \in q, \forall q \in Q, \forall a \in A) \geq 1 - \beta$.*

Proof Let $x \in \mathbb{R}^n$, $a \in A$ denote by $f_a(x, \cdot)_{\#} P_w$ the push-forward measure of P_w through $f_a(x, \cdot)$. Start by assuming that P_w and $\hat{P}_w$ are ϵ -close in the sense of $\mathcal{W}_s$. Then it holds that (Villani, 2021) $\mathcal{W}_s(T^a(\cdot \mid x), T_{\hat{P}_w}^a(\cdot \mid x)) = \mathcal{W}_s(f_a(x, \cdot)_{\#} P_w, f_a(x, \cdot)_{\#} \hat{P}_w) \leq L_w(x, a)\epsilon$. Next, define the distribution $\hat{\gamma}_{x,a} \in \mathcal{P}(Q)$ with $\hat{\gamma}_{x,a}(q') := T_{\hat{P}_w}^a(q' \mid x)$ for all $q' \in Q$. By the construction of $\hat{\Gamma}_{q,a}$, $\hat{\gamma}_{x,a} \in \hat{\Gamma}_{q,a}$. Furthermore, from (Gracia et al., 2023, Lemma 2), $\mathcal{W}_s(T^a(\cdot \mid x), T_{\hat{P}_w}^a(\cdot \mid x)) \leq L_w(x, a)\epsilon \implies \mathcal{T}^c(\gamma_{x,a}, \hat{\gamma}_{x,a})^{1/s} \leq L_w(x, a)\epsilon$. By Lemma 2, when $\epsilon \equiv \varepsilon(N, \beta)$, this conclusion holds with probability $1 - \beta$ for all $x \in q$, $q \in Q$, $a \in A$. This in turn implies by Definition 4 that also $\gamma_{x,a} \in \Gamma_{q,a}$ for all $x \in q$, $q \in Q$, $a \in A$ with the same probability. ■

Remark 6 (Clustering Samples) *As shown in Sections 4.1 and 4.3.1, while the computational complexity of the abstraction is proportional to the number of samples, the ambiguity in the learned distribution and therefore the conservatism of the abstraction decrease with N . A straightforward way to deal with this trade-off is to reduce the number of samples used to construct the abstraction via clustering. By doing so, we obtain another discrete distribution $\tilde{P}_w$, supported on $N_{\text{cluster}} \ll N$ points, and which is very close (in the Wasserstein sense) to $\hat{P}_w$. By adding this small discrepancy to the original ambiguity radius and using the triangle inequality, we construct an ambiguity ball around $\tilde{P}_w$ that retains the exact same guarantees of containing P_w as our original ambiguity set.*

2. We can obtain a tighter representation of the uncertainty in $\Gamma_{q,a}$ by restricting ourselves to distributions in $\mathcal{P}(Q_{q,a})$, where $Q_{q,a} := \{q' \in Q : \exists x \in q, w \in W \text{ s.t. } q' \cap \text{Reach}(x, a, w) \neq \emptyset\}$, i.e., leveraging boundedness of W .

Remark 7 Notice that the confidence on $\mathcal{M}$ being a sound abstraction of Process (1) is the same as that of our ambiguity set containing P_w . This is an advantage of using an ambiguity set to represent learning uncertainty, instead of obtaining bounds on individual transition probabilities, as is commonly done in the literature, e.g., [Badings et al. \(2023a,b\)](#); [Ashok et al. \(2019\)](#). In fact, these approaches lead the resulting confidence bounds to decrease with the abstraction size and to the paradox that large abstractions can be more uncertain than coarser ones.

5. Strategy Synthesis

To obtain a strategy for Process (1), we compute a strategy σ^* for the abstraction $\mathcal{M}$ that maximizes the probability of satisfying φ and is robust against all uncertainties in the abstraction. Since $\mathcal{M}$ is a sound abstraction of (1), σ^* can be refined to a strategy on (1) with correctness guarantees. To synthesize such σ^* , we first construct a deterministic finite automaton (DFA) that represents formula φ ([De Giacomo and Vardi, 2013](#)).

Definition 8 (DFA) Given an LTL_f formula φ defined over a set of atomic propositions AP , a deterministic finite automaton (DFA) constructed from φ is a tuple $\mathcal{A} = (Z, 2^{AP}, \delta, z_0, Z_F)$ where Z is a finite set of states, 2^{AP} is a finite set of input symbols, $\delta : Z \times 2^{AP} \rightarrow Z$ is the transition function, $z_0 \in Z$ is the initial state, and $Z_F \subseteq Z$ is the set of accepting states.

Trace $\rho = \rho_0 \rho_1 \dots \rho_K \in (2^{AP})^*$ induces run $z = z_0 z_1 \dots z_{K+1}$ on $\mathcal{A}$, where $z_{k+1} = \delta(z_k, \rho_k)$ for all $k \in \{0, \dots, K\}$. Per construction of $\mathcal{A}$ introduced by [De Giacomo and Vardi \(2013\)](#), trace ρ satisfies φ iff $z_{K+1} \in Z_F$, in which case run z is called *accepting* for $\mathcal{A}$. Next, we generate the product of RMDP abstraction $\mathcal{M}$ and $\mathcal{A}$ to capture the paths of $\mathcal{M}$ that induce accepting runs in $\mathcal{A}$.

Definition 9 (Product RMDP) Given RMDP $\mathcal{M}$ and DFA $\mathcal{A}$, the product $\mathcal{M}^\varphi = \mathcal{M} \otimes \mathcal{A}$ is another RMDP $\mathcal{M}^\varphi = (Q^\varphi, A^\varphi, \Gamma^\varphi, q_0^\varphi, Q_F^\varphi)$, where $Q^\varphi = Q \times Z$ is the set of states, $A^\varphi = A$ is the set of actions, $q_0^\varphi = \delta(z_0, L(q_0))$ is the initial state, $Q_F^\varphi = Q \times Z_F$ is the set of accepting states, and $\Gamma^\varphi = \{\Gamma_{(q,z),a}^\varphi : (q,z) \in Q^\varphi, a \in A^\varphi((q,z)) \text{ with } \Gamma_{(q,z),a}^\varphi := \{\gamma^\varphi \in \mathcal{D}(Q^\varphi) : \exists \gamma \in \Gamma_{q,a} \text{ s.t. } \forall q' \in Q, \gamma^\varphi((q', z')) = \gamma(q') \text{ iff } z' = \delta(z, L(q'))\}\}$.

By construction, a path of $\mathcal{M}^\varphi$ is accepting if and only if its projection onto $\mathcal{M}$ is a path ω whose trace ρ satisfies φ , i.e., ρ is accepting by $\mathcal{A}$. Therefore, obtaining a strategy σ^* that robustly maximizes the probability of $\mathcal{M}$ satisfying φ boils down to solving a *robust maximal reachability probability problem* in $\mathcal{M}^\varphi$. To this end, since Γ and, consequently, Γ^φ , are built extending the independent intervals of probabilities in the empirical IMDP with ambiguity sets of distributions in the sense of $\mathcal{T}^c$, we can rely on the efficient *robust dynamic programming* algorithm in ([Gracia et al., 2022](#)), which involves linear programming, and enjoys polynomial and exponential time complexity in the size of $\mathcal{M}$ and φ , respectively. The resulting strategy σ_φ^* of $\mathcal{M}^\varphi$ can be mapped to a memory-dependent strategy σ^* of $\mathcal{M}$, where the memory corresponds to the current state in $\mathcal{A}$. Besides σ^* , the synthesis process also yields bounds on the probability of $\mathcal{M}$ satisfying φ under strategy σ^* from each $q \in Q$, i.e., $\underline{p}(q) := \min_{\xi \in \Gamma} Pr_{\xi}^{q, \sigma^*}[\omega \models \varphi]$ and $\bar{p}(q) := \max_{\xi \in \Gamma} Pr_{\xi}^{q, \sigma^*}[\omega \models \varphi]$.

5.1. Correctness

In this section, we refine the strategy σ^* to a strategy σ_x of Process (1), ensuring its correctness. First, let $J : \mathbb{R}^n \rightarrow Q$ be the function that maps each continuous state to the corresponding region,

i.e., for all $q \in Q$, $J(x) := q$ iff $x \in q$. Given $\omega_x = x_0 \xrightarrow{a_0} \dots \xrightarrow{a_{K-1}} x_K$, we let $J(\omega_x) := J(x_0) \xrightarrow{a_0} \dots \xrightarrow{a_{K-1}} J(x_K)$ denote the corresponding path of $\mathcal{M}$. A switching strategy of (1) is obtained as $\sigma_x(\omega_x) := \sigma^*(J(\omega_x)) \quad \forall \omega_x \in \Omega_x$. The following theorem ensures correctness of σ_x .

Theorem 10 (Correctness) *Let $\mathcal{M}$ be a sound RMDP abstraction of Process (1) with confidence $1 - \beta$ and φ be an LTL_f formula. Let σ^* be an optimal robust strategy of $\mathcal{M}$ w.r.t. φ and σ_x the corresponding switching strategy of (1). Then it holds that, with confidence $1 - \beta$, $P_{x_0}^{\sigma_x}[\omega_x \models \varphi \wedge \mathcal{G}\neg p_u] \in [p(q), \bar{p}(q)]$ for all $x_0 \in q$, $q \in Q$, where $\underline{p}(q)$ and $\bar{p}(q)$ are the bounds on the probability of $\mathcal{M}$ satisfying φ .*

Proof If $\mathcal{M}$ is a sound abstraction of (1), then the theorem follows by making use of Theorem 2 in Jackson et al. (2021a) and letting the path length grow unbounded. Since the soundness argument holds with confidence $1 - \beta$, σ_x is a correct strategy for (1) with the same confidence. $\blacksquare$

6. Case Studies

We consider various stochastic systems from the literature and use our framework to synthesize optimal strategies against various LTL_f specifications. All experiments were run on an Intel Core i7 3.6GHz CPU with 32GB RAM. We consider $\beta = 10^{-9}$, $l = \infty$, and $s = 1$ in all experiments. In Table 1 we report our results on 3 nonlinear and 2 linear systems. These models include a nonlinear pendulum in the presence of random wind and where the aerodynamic torque is proportional to $-(\dot{\theta}_t - \mathbf{w}_t \cos \theta_t)|\dot{\theta}_t - \mathbf{w}_t \cos \theta_t|$, and a 3D car model (Rajamani, 2011) where (nonlinear) Coulomb friction is modeled by adding a random perturbation to the linear velocity. We also reproduce the results in (Skovbekk et al., 2023) for a system with multiplicative noise, and the results in (Gracia et al., 2023) for a 2D unicycle with additive noise. The specification considered for these systems is a reach-avoid one, i.e., $\varphi_1 = \mathcal{G}(\text{safe}) \wedge \mathcal{F}(\text{goal})$. To show that our approach can also tackle more complex formulas, we consider a 2D unicycle under specification $\varphi_2 := \mathcal{G}(\text{safe}) \wedge \mathcal{G}(\text{water} \rightarrow (\neg \text{charge} \mathcal{U} \text{carpet})) \wedge \mathcal{F}(\text{charge})$ (Vazquez-Chanlatte et al., 2018), which represents the task of simultaneously reaching a charge station while remaining safe and, if the system goes through a region with water, then it should first dry in a carpet before charging.

The results illustrate how our framework is able to provide non-trivial certificates of correctness and synthesize controllers for each of the examples. As expected from the theoretical results in Section 4.1, it is possible to observe how the precision of our approach increases with the number

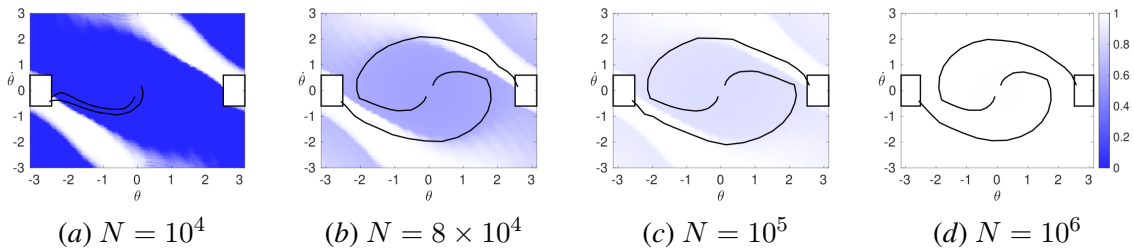


Figure 1: Lower bound on the probability of satisfying φ_1 for the pendulum system as a function of N , together with sampled trajectories. Boxes represent the goal regions.

Table 1: Results of the case studies. We denote by e_{avg} the average difference between the lower and upper bounds in the satisfaction probabilities. Abstraction and synthesis times are given in minutes, for which respective timeouts of 8 and 2 hours are fixed. We denote by ε and $\varepsilon_{cluster}$ the radius of the ambiguity set before and after clustering, respectively.

System (Spec.)	$ Q $	$ A $	N	ε	$N_{cluster}$	$\varepsilon_{cluster}$	e_{avg}	Abstr. Time	Synth. Time
Pendulum (φ_1)	4×10^4	5	10^4	0.177	43	0.186	0.744	5.484	7.474
				0.177	—	—	—	timeout	—
			8×10^4	0.063	48	0.071	0.219	5.438	120.000
			10^5	0.056	47	0.065	0.076	5.406	120.000
			10^6	0.018	49	0.027	0	5.273	61.167
3D Unicycle (φ_1)	6.4×10^4	10	10^7	0.0014	393	0.00245	0.517	22.632	51.942
				0.0014	—	—	—	timeout	—
			10^8	0.0047	453	0.0161	0.498	25.438	43.183
			5×10^8	0.0022	4505	0.006	0.453	235.950	46.117
				0.0022	8869	0.0048	0.447	457.431	43.342
Multiplicative noise (φ_1) (Skovbekk et al., 2023)	10^4	1	4.74×10^3	0.034	119	0.041	0.452	1.598	4.659
				0.034	—	—	0.440	59.947	4.691
			4.67×10^4	0.012	262	0.017	0.387	3.241	4.036
				0.012	—	—	—	timeout	—
			4.66×10^5	0.004	1066	0.0065	0.323	13.149	3.863
2D Unicycle (φ_1) (Gracia et al., 2023)	1.6×10^3	8	4×10^5	0.009	385	0.01	0.334	0.224	3.598
				0.009	—	—	0.284	341.463	3.978
			2×10^6	0.013	162	0.015	0.180	0.438	3.582
				0.015	—	—	—	timeout	—
			5×10^7	0.004	741	0.005	0.051	0.735	3.208
2D Unicycle (φ_2)	3.6×10^3	8	10^4	0.283	16	0.292	0.494	0.049	5.538
				0.283	—	—	0.484	19.567	5.260
			10^5	0.100	17	0.109	0.210	0.044	5.423
				0.100	—	—	0.195	180.454	4.072
			10^6	0.035	44	0.039	0.079	0.1021	3.470
				0.035	—	—	—	timeout	—
			10^7	0.012	46	0.016	0.03	0.106	3.043

of samples, i.e., e_{avg} , the difference between upper and lower bound in the probability of satisfying the LTL_f property, decreases with N . This can also be observed in Figure 1, where we show the lower bound on the satisfaction probability for the pendulum system, for different values of N , while keeping all the other parameters constant. Similarly, e_{avg} decreases by increasing $|Q|$, the size of the abstraction. As a trade-off, the computation times increases with both $|Q|$ and N . This highlights the importance of clustering the samples, which we can observe in Table 1 to only have a relatively small effect in conservatism, while leading to substantial improvements in the time to build the abstraction. Finally, we empirically validated the theoretical bounds in the satisfaction probabilities via thousands of Monte Carlo simulations for random initial conditions.

7. Conclusion and Future Work

We present a framework to perform formal control of switched stochastic systems with general nonlinear dynamics and unknown disturbances under LTL_f specifications. The experimental results show the generality and effectiveness of our approach. Future research directions include increasing the tightness of our results and analyzing convergence of our solution to the optimal one.

Acknowledgments

This work is supported in part by National Science Foundation (NSF) under grant number 2039062 and Air Force Research Lab (AFRL) under agreement number FA9453-22-2-0050.

References

- Steven Adams, Morteza Lahijanian, and Luca Laurenti. Formal control synthesis for stochastic neural network dynamic models. *IEEE Control Systems Letters*, 6:2858–2863, 2022.
- David F Anderson and Thomas G Kurtz. Continuous time markov chain models for chemical reaction networks. In *Design and analysis of biomolecular circuits: engineering approaches to systems and synthetic biology*, pages 3–42. Springer, 2011.
- Pranav Ashok, Jan Křetínský, and Maximilian Weininger. PAC statistical model checking for Markov decision processes and stochastic games. In *Computer Aided Verification: 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part I 31*, pages 497–519. Springer, 2019.
- Thom Badings, Licio Romao, Alessandro Abate, and Nils Jansen. Probabilities are not enough: Formal controller synthesis for stochastic dynamical models with epistemic uncertainty. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 37, pages 14701–14710, 2023a.
- Thom Badings, Licio Romao, Alessandro Abate, David Parker, Hasan A Poonawala, Marielle Stoelinga, and Nils Jansen. Robust control for dynamical systems with non-gaussian noise via formal abstractions. *Journal of Artificial Intelligence Research*, 76:341–391, 2023b.
- Dimitri Bertsekas and Steven E Shreve. *Stochastic optimal control: the discrete-time case*, volume 5. Athena Scientific, 1996.
- Emmanuel Boissard and Thibaut Le Gouic. On the mean speed of convergence of empirical and occupation measures in Wasserstein distance. In *Annales de l’IHP Probabilités et statistiques*, volume 50, pages 539–563, 2014.
- Dimitris Boskos, Jorge Cortés, and Sonia Martínez. High-confidence data-driven ambiguity sets for time-varying linear systems. *IEEE Transactions on Automatic Control*, 2023. <https://arxiv.org/abs/2102.01142>.
- Nathalie Cauchi, Luca Laurenti, Morteza Lahijanian, Alessandro Abate, Marta Kwiatkowska, and Luca Cardelli. Efficiency through uncertainty: Scalable formal synthesis for stochastic hybrid systems. In *Proceedings of the 2019 22nd ACM International Conference on Hybrid Systems: Computation and Control*, Montreal, QC, Canada, Apr. 2019. ACM. doi: 10.1145/3302504.3311805.
- Giuseppe De Giacomo and Moshe Y Vardi. Linear temporal logic and linear dynamic logic on finite traces. In *IJCAI’13 Proceedings of the Twenty-Third international joint conference on Artificial Intelligence*, pages 854–860. Association for Computing Machinery, 2013.
- Nicolas Fournier. Convergence of the empirical measure in expected Wasserstein distance: non asymptotic explicit bounds in $\mathbb{R}^d$. *arXiv preprint arXiv:2209.00923*, 2022.

- Robert Givan, Sonia Leach, and Thomas Dean. Bounded-parameter Markov decision processes. *Artificial Intelligence*, 122(1-2):71–109, 2000.
- Ibon Gracia, Dimitris Boskos, Morteza Lahijanian, Luca Laurenti, and Manuel Mazo Jr. Efficient strategy synthesis for switched stochastic systems with distributional uncertainty, 2022. <https://arxiv.org/abs/2212.14260>.
- Ibon Gracia, Dimitris Boskos, Luca Laurenti, and Manuel Mazo Jr. Distributionally robust strategy synthesis for switched stochastic systems. In *Proceedings of the 26th ACM International Conference on Hybrid Systems: Computation and Control*, pages 1–10, 2023.
- John Jackson, Luca Laurenti, Eric Frew, and Morteza Lahijanian. Formal verification of unknown dynamical systems via Gaussian process regression. *arXiv preprint arXiv:2201.00655*, 2021a.
- John Jackson, Luca Laurenti, Eric Frew, and Morteza Lahijanian. Strategy synthesis for partially-known switched stochastic systems. In *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, pages 1–11, 2021b.
- Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, 66(7):3097–3110, 2020.
- Panqanamala Ramana Kumar and Pravin Varaiya. *Stochastic systems: Estimation, identification, and adaptive control*. SIAM, 2015.
- Morteza Lahijanian, Sean B Andersson, and Calin Belta. Formal verification and synthesis for discrete-time stochastic systems. *IEEE Transactions on Automatic Control*, 60(8):2031–2045, 2015.
- Abolfazl Lavaei, Sadegh Soudjani, Alessandro Abate, and Majid Zamani. Automated verification and synthesis of stochastic hybrid systems: A survey. *Automatica*, 146:110617, 2022.
- Mathias Lechner, Đorđe Žikelić, Krishnendu Chatterjee, and Thomas A Henzinger. Stability verification in stochastic control systems via neural network supermartingales. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 36, pages 7326–7336, 2022.
- Andrea Martin, Luca Furieri, Florian Dörfler, John Lygeros, and Giancarlo Ferrari-Trecate. Regret optimal control for uncertain stochastic systems. *arXiv preprint arXiv:2304.14835*, 2023.
- Frederik Baymler Mathiesen, Licio Romao, Simeon C Calvert, Alessandro Abate, and Luca Laurenti. Inner approximations of stochastic programs for data-driven stochastic barrier function design. *arXiv preprint arXiv:2304.04505*, 2023.
- Rayan Mazouz, Karan Muvvala, Akash Ratheesh Babu, Luca Laurenti, and Morteza Lahijanian. Safety guarantees for neural network dynamic systems via stochastic barrier functions. *Advances in Neural Information Processing Systems*, 35:9672–9686, 2022.
- Arnab Nilim and Laurent El Ghaoui. Robust control of Markov decision processes with uncertain transition matrices. *Operations Research*, 53(5):780–798, 2005.
- Hamed Rahimian and Sanjay Mehrotra. Distributionally robust optimization: A review. *arXiv preprint arXiv:1908.05659*, 2019.

- Rajesh Rajamani. *Vehicle dynamics and control*. Springer Science & Business Media, 2011.
- Cesar Santoyo, Maxence Dutreix, and Samuel Coogan. A barrier function approach to finite-time stochastic system verification and control. *Automatica*, 125:109439, 2021.
- Oliver Schön, Birgit van Huijgevoort, Sofie Haesaert, and Sadegh Soudjani. Bayesian approach to temporal logic control of uncertain systems. *arXiv preprint arXiv:2304.07428*, 2023.
- John Skovbekk, Luca Laurenti, Eric Frew, and Morteza Lahijanian. Formal abstraction of general stochastic systems via noise partitioning. *arXiv preprint arXiv:2309.10702*, 2023.
- Marcell Vazquez-Chanlatte, Susmit Jha, Ashish Tiwari, Mark K Ho, and Sanjit Seshia. Learning task specifications from demonstrations. *Advances in neural information processing systems*, 31, 2018.
- Cédric Villani. *Topics in optimal transportation*, volume 58. American Mathematical Soc., 2021.
- Wolfram Wiesemann, Daniel Kuhn, and Berç Rustem. Robust Markov decision processes. *Mathematics of Operations Research*, 38(1):153–183, 2013.