Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Data-Driven Verification under Signal Temporal Logic Constraints ⋆

Ali Salamati [*] **Sadegh Soudjani** [**] **Majid Zamani** [*,***]

[*] *Computer Science Department, Ludwig Maximilian University of Munich, Germany (e-mail: ali.salamati@lmu.de)*
[**] *School of Computing, Newcastle University, Newcastle upon Tyne, United Kingdom (e-mail: sadegh.soudjani@newcastle.ac.uk)*
[***] *Computer Science Department, University of Colorado Boulder, USA (e-mail: majid.zamani@colorado.edu)*

Abstract: We consider systems under uncertainty whose dynamics are partially unknown. Our aim is to study satisfaction of temporal properties by trajectories of such systems. We express these properties as signal temporal logic formulas and check if the probability of satisfying the property is at least a given threshold. Since the dynamics are parameterized and partially unknown, we collect data from the system and employ Bayesian inference techniques to associate a confidence value to the satisfaction of the property. The main novelty of our approach is to combine both data-driven and model-based techniques in order to have a two-layer probabilistic reasoning over the behavior of the system: one layer is related to the stochastic noise inside the system and the next layer is related to the noisy data collected from the system. We provide approximate algorithms for computing the confidence for linear dynamical systems.

Keywords: Bayesian Inference, Data-Driven Methods, Verification, Signal Temporal Logic, Parametrized Models.

1. INTRODUCTION

Formal methods have been vastly used in computer science to provide correctness guarantees on the expected behavior of a program. Most of these formal techniques have been developed for finite-state models (Beyer et al., 2018; Beyer and Keremoglu, 2011). In order to fully utilize the advantages of formal techniques in real physical applications, one needs to first construct a sufficiently precise model of the system. Usually, it is hard to model a system accurately. Besides, the dynamics of a system may vary throughout the course of time. In such cases, statistical model checking can be beneficial if all the states of the system can be measured (Sen et al., 2004; Clarke and Zuliani, 2011; Sen et al., 2005). However, statistical model checking usually needs a large number of experiments, is not able to deal efficiently with uncertainties in the system, and is not able to handle synthesis problems directly (Sen et al., 2005).

A data-driven approach was developed by Sadraddini and Belta (2018) for control of piecewise affine systems with additive disturbances against signal temporal logic (**STL**) properties. Bartocci et al. (2014) exploit concepts from formal modeling and machine learning to develop methodologies that can identify temporal logic formulae that discriminate different stochastic processes based on observations. Chou and Sankaranarayanan (2019) propose an approach to approximate the posterior distribution of unknown parameters for a nonlinear and deterministic system. Lavaei et al. (2020) use model-free reinforcement learning for policy synthesis of dynamical systems with finite-horizon properties under continuity assumptions on the dynamics of the system. Kazemi and Soudjani (2020) have used reinforcement learning for satisfying all (infinite-horizon) linear temporal logic properties with convergence guarantees and without any continuity assumption on the dynamics of the system.

STL properties are introduced and used in the literature including the works by Raman et al. (2015) and Fainekos and Pappas (2006). Sadigh and Kapoor (2016) introduce a new definition for the probabilistic **STL** that assigns probabilities to the atomic propositions and then combines them through Boolean operators. Farahani et al. (2018b) utilize probabilistic **STL** properties to design a control strategy for Barcelona wastewater system. Satisfaction of properties expressed in linear temporal logic on finite traces for linear time-invariant (LTI) systems is investigated by Haesaert et al. (2015, 2016) using Bayesian inference. Polgreen et al. (2017) apply Bayesian inference to parametric Markov chain.

In this work, a Bayesian framework is introduced in order to give a probabilistic confidence measure over an **STL** property for a set of parameterized models of stochastic systems. In our approach, a prior knowledge of the system accompanied by the collected data from the system are leveraged together to improve the confidence of satisfaction for the properties of interest expressed as **STL** formulas. Our main objective is to combine both data-driven and model-based techniques for stochastic systems in order to verify the system against probabilistic **STL** properties.

⋆ This work was supported in part by the H2020 ERC Starting Grant AutoCPS (grant agreement No. 804639).

The results are demonstrated for partially unknown linearly parameterized models of stochastic systems.

Our approach considers a probability threshold as lower bound for the satisfaction of **STL** property by the stochastic trajectories of the system. We under-approximate the feasible parameter set of the probabilistic constraint by transforming them into algebraic inequalities. Then, a confidence value is computed using the obtained feasible set and the distribution of the parameter is updated based on collected data from the system. We did not include the proofs due to space limitations and will be included in an online arXiv version of the paper.

2. PRELIMINARIES AND PROBLEM FORMULATION

In this section, we make a clear overview of our problem and the proposed approach to tackle that. Assume that there are parametric models $M(\theta)$ of the original system in which θ comes from a parameter set Θ. This set of models is described as $\Omega = \{M(\theta) \mid \theta \in \Theta\}$.

***Assumption** 1.* It is assumed that there is a true parameter θ_{true} such that $M(\theta_{true})$ describes the behavior of the original system **S**. This true parameter is unknown in general.

Consider a property ψ defined over trajectories of the system **S**. We assume this property belongs to the class of **STL** properties which will be defined in Subsection 4.1. We denote satisfaction of ψ by the trajectories of the system with $\mathbf{S} \models \psi$. We intend to give a confidence value for the satisfaction of a probabilistic **STL** property ψ for a system **S** by combining Bayesian inference and model-based techniques. We consider both process noise over the dynamics of the system, and measurement noises over outputs of the system.

Let us define the set of data collected from the system $\mathcal{D} = \{\tilde{u}_{exp}(t), \tilde{y}_{exp}(t)\}_{t=0}^{\mathbf{N_{exp}}-1}$, in which $\tilde{u}_{exp}(t)$ and $\tilde{y}_{exp}(t)$ are input-output pairs for $\mathbf{N_{exp}}$ measurements. In general, it is assumed that we can excite the system with any desirable input signal but within the acceptable range of inputs.

***Assumption** 2.* Both process and measurement noises are considered independent and identically distributed. Besides, they are not correlated to the input signals. Initial state vector $x(0)$ is considered to be known.

2.1 Stochastic Bayesian Confidence

Satisfaction of a property ψ for a deterministic system can be considered as a binary value over the parameter space Θ. If we have Ω as the set of parameterized deterministic models over the whole parameter space Θ, satisfaction function for the deterministic system can be defined as $g_\psi : \Theta \to \{0, 1\}$ in which $g_\psi(\theta) \equiv M(\theta) \models \psi$. This confidence value can be only zero or one. If the system is affected by the process noise, the satisfaction of the desired property can be explained by a probabilistic measure. Now, we can define a threshold on the probability of satisfaction of a property ψ as

$$\mathbf{Pr}(M(\theta) \models \psi) \geq 1 - \delta, \tag{1}$$

where $\delta \in (0, 1)$. Now we can assign a satisfaction function f_ψ^δ to the above chance constraint which is again a binary function on the parameter space Θ.

***Definition** 1.* Consider Ω as the set of stochastic models $\mathbf{M}(\theta)$ in which $\theta \in \Theta$, and let ψ be a temporal logic formula (e.g. **STL**). The stochastic satisfaction function $f_\psi^\delta : \Theta \to \{0, 1\}$ is defined as:

$$f_\psi^\delta(\theta) = \begin{cases} 1 & \text{if } \mathbf{Pr}(M(\theta) \models \psi) \geq 1 - \delta, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Let $\mathbf{Pr}(.)$ and $p(.)$ denote a probability value and a probability density function, respectively. Then, we can define a stochastic notion of confidence using Bayesian probability inference. It can be expressed as a distribution over the whole set of models Ω.

***Definition** 2.* Given a property ψ and a set of data $\mathcal{D}$, the notion of confidence for the stochastic system can be computed as:

$$\mathbf{Pr}(\mathbf{S} \models \psi \mid \mathcal{D}) = \int_\Theta f_\psi^\delta(\theta)\ p(\theta \mid \mathcal{D}) d\theta, \tag{3}$$

where $p(\theta \mid \mathcal{D})$ is a posteriori uncertainty distribution, given input-output pairs of data, and $f_\psi^\delta(\theta)$ is the stochastic satisfaction function defined in (2).

2.2 Parametric LTI Systems

Note that the integral in (3) is difficult to be tackled analytically in general. Therefore, we provide a computational approach suitable for *linear time-invariant (LTI) systems* defined next. The nominal model for the stochastic system **S** is defined as:

$$\mathbf{M}(\theta) \in \begin{cases} x(t+1) = Ax(t) + Bu(t) + Gw(t) \\ \hat{y}(t, \theta) = C(\theta)x(t), \end{cases} \tag{4}$$

where, $x(t) \in \mathbb{R}^n$, $y(t) \in \mathbb{R}^p$, and $u(t) \in \mathcal{U} \subset \mathbb{R}^m$, respectively. $\mathcal{U}$ is the set of valid inputs and is assumed to be bounded. We assume that matrices A and B are known. Signal $w(t)$ is the process noise with a zero-mean Gaussian distribution, which has a covariance matrix $\mathbf{\Sigma_w}$. The output of the stochastic system is also affected by the measurement noise as

$$y(t, \theta) = C(\theta)x(t) + e(t), \tag{5}$$

in which $e(t) \in \mathbb{R}^p$ is the measurement noise with a zero-mean Gaussian distribution, which has a covariance matrix $\mathbf{\Sigma_e}$. Both process and measurement noises are assumed to be uncorrelated from the input signals.

2.3 Problem Statement

There is a set of parameterized models $\mathbf{M}(\theta)$ for the stochastic system without the measurement noise. Also, we assume that there is a θ_{true} from the parameter space Θ such that $M(\theta_{true})$ describes the behaviors of the stochastic system.

Assume that we have a prior knowledge of parameterized models for this system. This prior knowledge can be used in order to improve the posterior distribution function over the parameter space after collecting data from the system.

***Problem** 1.* Given a parameterized LTI system in (4) together with the noisy output data in (5), data set $\mathcal{D}$, and

an **STL** property ψ, we aim at computing the confidence value in (3), with which the **STL** specification ψ is satisfied independently of the input value.

This approach is depicted in Fig. 1. In this figure, Θ is the whole parameter space. We denote by Θ_ψ the initial feasible set of parameters which their related parametric models satisfy the given probabilistic **STL** formula ψ. In addition, $p(\theta \mid \mathcal{D})$ denotes a posterior distribution function which is improved based on the collected data from the system, i.e., $\mathcal{D} = \{\tilde{u}_{exp}(t), \tilde{y}_{exp}(t)\}_{t=0}^{\mathbf{N_{exp}}-1}$. The updated posterior distribution function will be leveraged in order to compute the confidence value using (3). Moreover, the prior information regarding appropriate parameters θ, can be incorporated in order to achieve a more precise confidence.

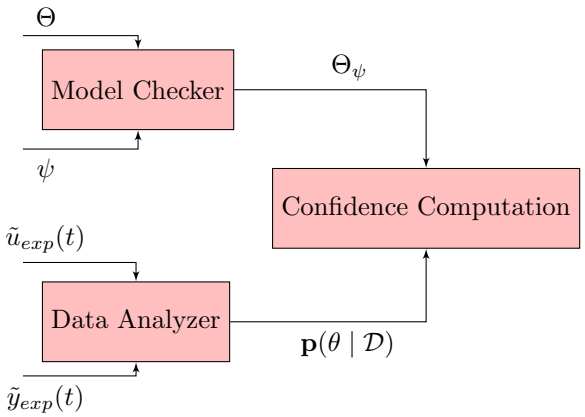

Fig. 1. An overview of our proposed approach

3. BAYESIAN INFERENCE

We use Bayesian inference in order to provide the confidence of property satisfaction for parametric LTI systems. In many practical situations, we have an initial insight over the behaviors of the system that can be leveraged in order to increase our perception about the system. Bayesian inference is a powerful framework in order to incorporate this prior knowledge. Furthermore, the Bayesian framework is an efficient data-driven method. As it was mentioned before, confidence can be computed using (3). In (3), given the set of input-output data pairs, a posterior uncertainty distribution $p(\theta \mid \mathcal{D})$ can be inferred for the parameter θ by

$$p(\theta \mid \mathcal{D}) = \frac{p(\mathcal{D} \mid \theta)\, p(\theta)}{\int_\Theta p(\mathcal{D} \mid \theta)\, p(\theta) d\theta}, \tag{6}$$

where $p(\theta)$ indicates a prior distribution over the whole parameter set Θ and comes from our initial knowledge of the system. Here, $p(\mathcal{D} \mid \theta)$ is the *likelihood distribution function* which is computed based on our observations within the noisy environment. Let us consider the set of data $\mathcal{D} = \{\tilde{u}_{exp}(t), \tilde{y}_{exp}(t)\}_{t=0}^{\mathbf{N_{exp}}-1}$ in which $\tilde{u}_{exp}(t)$ and $\tilde{y}(t)_{exp}$ are input-output pairs for $\mathbf{N_{exp}}$ measurements. The system gets excited with inputs $\tilde{u}_{exp}(t)$, and $\tilde{y}_{exp}(t)$ are the corresponding observed outputs of the system at time t which are noisy. If the system is only affected by the measurement noise, observations can be assumed to be independent and identically distributed. In this case, the likelihood distribution $p(\mathcal{D} \mid \theta)$ can be computed simply as $p(\mathcal{D} \mid \theta) = \prod_{t=0}^{\mathbf{N_{exp}}-1} p(\tilde{y}_{exp}(t) \mid \theta)$. By considering the process noise, one can clearly observe that measurements will not be independent anymore. In this scenario, we consider the likelihood distribution as a joint distribution function of all $\mathbf{N_{exp}}$ measurements in the form of:

$$p(\tilde{y}_{exp}(0), \tilde{y}_{exp}(1), \ldots, \tilde{y}_{exp}(\mathbf{N_{exp}} - 1) \mid \theta), \tag{7}$$

where distributions for both measurement and process noises are assumed to be Gaussian with zero means and their corresponding covariances. We can consider this joint probability distribution function as a multi-variate Gaussian distribution function. The next theorem provides covariance matrix for the noisy outputs of the system.

***Theorem** 1.* Consider the LTI model (4)-(5). The joint distribution $p(\mathcal{D} \mid \theta)$ is multi-variate Gaussian with mean

$$\bar{\mathbf{y}}(\theta) = [\bar{y}(0); \cdots; \bar{y}(\mathrm{N}_{exp})], \tag{8}$$

and covariance matrix $\Sigma_{\tilde{\mathbf{y}}}(\theta)$, where

$$\bar{y}(t) := C(\theta)A^t x(0) + \sum_{i=0}^{t-1} C(\theta)A^i B u(t-i-1)$$

$$\Sigma_{\tilde{\mathbf{y}}}(\theta) := \mathbf{M}(\theta)\ \Sigma_W\ \mathbf{M}(\theta)^T + \Sigma_E.$$

Matrices $\Sigma_W := diag(\Sigma_w, \Sigma_w, \ldots, \Sigma_w)$ and $\Sigma_E := diag(\Sigma_e, \ldots, \Sigma_e)$ are block diagonal.
$\mathbf{M}(\theta) \in \mathbb{R}^{(m\mathrm{N}_{exp}+m)\times(n\mathrm{N}_{exp})}$ is computable using matrices of the system as

$$\mathbf{M}(\theta) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ C(\theta)G & 0 & 0 & \cdots & 0 \\ C(\theta)AG & C(\theta)G & 0 & \cdots & 0 \\ C(\theta)A^2G & C(\theta)AG & C(\theta)G & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C(\theta)A^{\mathrm{N}_{exp}-1}G & C(\theta)A^{\mathrm{N}_{exp}-2}G & \cdots & \cdots & C(\theta)G \end{bmatrix}.$$

The previous theorem results in a symmetric parametric covariance matrix, $\boldsymbol{\Sigma_{\tilde{\mathbf{y}}}(\theta)}$, for $\mathbf{N_{exp}}$ measurements of the system. Now, the joint Gaussian distribution function for $\mathbf{N_{exp}}$ measurements is given by:

$$p(\tilde{y}_{exp}(0), \tilde{y}_{exp}(1), \ldots, \tilde{y}_{exp}(\mathbf{N_{exp}} - 1) \mid \theta) = \frac{1}{|\boldsymbol{\Sigma_{\tilde{\mathbf{y}}}(\theta)}|^{\frac{1}{2}}(2\pi)^{\frac{\mathbf{N_{exp}}}{2}}} \exp\left\{-\frac{1}{2}(\tilde{\mathbf{y}} - \hat{\mathbf{y}}(\theta))^{\mathbf{T}}\, \boldsymbol{\Sigma_{\tilde{\mathbf{y}}}(\theta)}^{-1}(\tilde{\mathbf{y}} - \hat{\mathbf{y}}(\theta))\right\}, \tag{9}$$

where, $\tilde{\mathbf{y}}$ and $\hat{\mathbf{y}}(\theta)$ are measured noisy output and parametric output vectors for $\mathbf{N_{exp}}$ experiments. $|\boldsymbol{\Sigma_{\tilde{\mathbf{y}}}(\theta)}|$ is determinant of the covariance matrix. Likelihood function obtained in (9) as the joint distribution of $\mathbf{N_{exp}}$ measurements, can be used in order to update a posterior probability using (6).

4. **STL** CONSTRAINTS

*4.1 Signal Temporal Logic (**STL**)*

One of the advantages of **STL** specifications is their capabilities in defining temporal specifications for trajectories of physical systems. We denote an infinite trajectory of the system in (4) by $\xi = x(0)x(1)x(2), \ldots$ where $x(t)$ is the state of the system at time $t \in \mathbb{N}_0 := \{0, 1, 2, \ldots\}$.
Syntax: Signal temporal logic (**STL**) formulae are defined recursively using the following syntax:

$$\psi ::= \mathsf{T} \mid \mu \mid \neg\psi \mid \psi \wedge \phi \mid \psi \, \mathsf{U}_{[a,b]} \, \phi,$$

where, T is the true predicate, and $\mu : \mathbb{R}^n \to \{\mathsf{T}, \mathsf{F}\}$ is a predicate which its truth value is determined by the sign of a function of the state x, i.e., $\mu(x) = \mathsf{T}$ if and only if $\alpha(x) \geq 0$ with $\alpha : \mathbb{R}^n \to \mathbb{R}$ being an affine function of the state and is associated with μ. Notations $\neg$ and $\wedge$ denote negation and conjunction of formulas. Notation $\mathsf{U}_{[a,b]}$ denote the until operator where $a, b \in \mathbb{R}_{\geq 0}$.
Semantics: The satisfaction of an **STL** formula ψ by a trajectory ξ at time t is defined recursively as follows:

$(\xi, t) \models \mu \Leftrightarrow \mu(\xi, t) = \mathsf{T}$
$(\xi, t) \models \neg\mu \Leftrightarrow \neg((\xi, t) \models \mu)$
$(\xi, t) \models \psi \wedge \phi \Leftrightarrow (\xi, t) \models \psi \wedge (\xi, t) \models \phi$
$(\xi, t) \models \psi \, \mathsf{U}_{[a,b]} \, \phi \Leftrightarrow \exists t' \in [t + a, t + b]$ s.t. $(\xi, t') \models \phi$
$\wedge \, \forall t'' \in [t, t'], \ (\xi, t'') \models \psi.$

A trajectory ξ satisfies a specification ψ, denoted by $\xi \models \psi$, if $(\xi, 0) \models \psi$. Furthermore, other standard operators can be defined using the above defined operators. For *disjunction*, we can write $\psi \vee \phi := \neg(\neg\psi \wedge \neg\phi)$ and the *eventually* operator can be defined as $\Diamond_{[a,b]}\psi := \mathsf{T} \, \mathsf{U}_{[a,b]} \, \psi$. Finally, the *always* operator is defined as $\Box_{[a,b]}\psi := \neg\Diamond_{[a,b]}\neg\psi$. The *horizon* of an **STL** formula denoted by $len(\psi)$ is the maximum over all upper bounds of intervals on the temporal operators. Intuitively, $len(\psi)$ is the horizon in which satisfaction of $(\xi, t) \models \psi$ should be studied. Let us now denote a finite trajectory by $\xi(t : N) := x(t)x(t+1)...x(t+N)$. For checking $(\xi, t) \models \psi$, it is sufficient to consider a finite trajectory $\xi(t : N)$ with $N = len(\psi)$.

*4.2 Under-approximation of **STL** Constraints*

The stochastic satisfaction function defined in (2) requires the exact feasible set of the chance constraint in (1). This feasible set does not have a closed form in general. Previous works tried to find under-approximations of the feasible set. We leverage the proposed procedure in Farahani et al. (2018a) to get an under-approximation of the feasible set. This procedure transforms the chance constraints on the **STL** property into similar constraints on the predicates of the property using the structure of the **STL** formula. We discuss this procedure in this subsection.

Suppose an **STL** formula ψ has a finite horizon $len(\psi)$. The robustness of ψ indicates that the trajectory ξ of the system satisfies ψ at time t with probability greater than or equal to $1-\delta$, if $\xi(t : N) = x(t)x(t+1)x(t+2)\cdots x(t+N)$ with $N = len(\psi)$ satisfies $\mathbf{Pr}(\rho^{\psi}(\xi(t : N)) > 0) \geq 1 - \delta$.

The next lemma, borrowed from Farahani et al. (2018a), shows how one can transform the chance constraints on the satisfaction of **STL** formulae into similar constraints on the predicates of formulae.

***Lemma** 1.* For any **STL** formula ψ and a value $\delta \in (0, 1)$, probability constraints of the forms $\mathbf{Pr}(\xi(t : N) \models \psi) \geq 1 - \delta$ and $\mathbf{Pr}(\xi(t : N) \models \psi) \leq 1 - \delta$ can be transformed into similar constraints on the predicates of ψ based on the structure of ψ.

Lemma 1 enables us to write down probabilistic inequalities on the satisfaction of atomic predicates and use them as an under-approximation of the original probabilistic **STL** constraint. These probabilistic inequalities can be equivalently written as algebraic inequalities given that we know the statistical properties of the state trajectories. In the case of LTI systems with Gaussian disturbances, $x(t)$ is also Gaussian with known mean and covariance matrix. For the predicate $\mu(x) = \{\alpha(x) \geq 0\}$ with $\alpha(x) := \tilde{\theta}_0 + \tilde{\theta}^T x$, for some $\tilde{\theta} \in \mathbb{R}^n$ and $\tilde{\theta}_0 \in \mathbb{R}$, we have $\mathbb{E}[\alpha(x)] = \tilde{\theta}_0 + \tilde{\theta}^T \mathbb{E}[x]$ and $\mathrm{Var}[\alpha(x)] = \tilde{\theta}^T \mathrm{Cov}(x)\tilde{\theta}$. Therefore,

$$\begin{aligned} &\mathbf{Pr}(\alpha(x) \geq 0) \geq 1 - \delta \ \Leftrightarrow \ \mathbf{Pr}(\alpha(x) < 0) \leq \delta \\ &\Leftrightarrow \mathbb{E}(\alpha(x)) + \mathrm{Var}(\alpha(x))\mathbf{q}^{-1}(\delta) \geq 0, \end{aligned} \tag{10}$$

where $\mathbf{q}^{-1}$ is the error inverse function with $\mathbf{q} = \frac{1}{\pi}\int_{-x}^{x} e^{-t^2}$. In the following theorem, we show that the algebraic inequalities of the form (10) are linear with respect to the input.

***Theorem** 2.* Chance constraint $\mathbf{Pr}(\alpha(x(t)) \geq 0) \geq 1 - \delta$, where $\alpha(x) = \tilde{\theta}_0 + \tilde{\theta}^T x$ and $x(t)$ is the trajectory of the stochastic system (4) at time t, can be written as the following affine constraint in terms of the input trajectory:

$$\tilde{\theta}_0 + \sum_{i=1}^{t} \tilde{\theta}^T A^{i-1} B \, u(t - i + 1) + \Gamma(\tilde{\theta}, \delta) \geq 0, \tag{11}$$

where

$$\Gamma(\tilde{\theta}, \delta) := \Big(\sum_{i=1}^{t} \tilde{\theta}^T A^{i-1} G \, \boldsymbol{\Sigma_w} \, G^T (A^T)^{i-1} \tilde{\theta} \Big) \mathbf{q}^{-1}(\delta),$$

and $\boldsymbol{\Sigma_w}$ is the covariance matrix of the process noise.

Note that $\Gamma(\tilde{\theta}, \delta)$ is a quadratic function of $\tilde{\theta}$ and depends on δ nonlinearly.

5. VERIFICATION OF **STL** CONSTRAINTS

5.1 Feasible Set Computation

After transforming the probabilistic **STL** constraints into the algebraic inequalities, as described in Section 4, these inequalities are in the form of (11) which are linear with respect to the input trajectory and must hold for the whole input range. We use *robust linear programming* to solve those inequalities. Here, the primary robust linear programming problem is converted to another dual linear programming one without a universal quantifier over the target value based on Farkas' lemma (Georghiou et al., 2019). In the next theorem, we show that the feasible set of the probabilistic predicates at each time step can be characterized by a set of constraints at that time step.

***Theorem** 3.* Assume that inputs at each time step t are restricted as $\underline{l} \leq u(t) \leq \bar{l}, \ u(t), \underline{l}, \bar{l} \in \mathbb{R}^m$. The feasible set of each approximated algebraic inequality in (11) for the whole range of inputs can be characterized by the set of constraints

$$P^T d \leq b, \quad D^T P = \mathbf{f}_{\tilde{\theta}}, \quad P \geq 0, \tag{12}$$

where

$$P^T = [P_1, \ldots, P_{2mt}] \in \mathbb{R}^{1 \times 2mt}, \ P_k \in \mathbb{R}_{\geq 0}, \ \forall k \in \{1, \ldots, 2mt\},$$
$$d = [\bar{l}, \underline{l}, \ldots, \bar{l}, \underline{l}]^T \in \mathbb{R}^{2mt \times 1},$$
$$b = \tilde{\theta}_0 + \Gamma(\tilde{\theta}, \delta), \ \tilde{\theta}_0 \in \mathbb{R},$$
$$\mathbf{f}_{\tilde{\theta}} = \tilde{\theta}^T [A^{t-1}B; A^{t-2}B; \ldots; B] \in \mathbb{R}^{t \times 1},$$

and D is a matrix with all diagonal elements equal to 1 and the ones right below diagonal is -1. Solving these constraints simultaneously for all predicates of **STL** specification in horizon N, leads to the feasible set of parameters for the stochastic system $\mathbf{S}$ in (4). The complexity of computation of confidence value in (3) can be tackled using integrating the updated posteriori distribution over this feasible set by virtue of numerical techniques. Two different numerical approaches are described in the next subsection.

5.2 Confidence Computation Techniques

Mont Carlo Method. Considering the nonlinearity in the constraints, computation of integral in (3) can be done efficiently using *Monte Carlo techniques*. The idea is to choose $\mathbf{N}$ points uniformly from the bounded region of the parameters and using them in the computation of confidence integral in (3) as long as they satisfy all the required constraints in (12) for the whole horizon of **STL** properties. Now, the confidence integral is a random variable and can be represented as $Q_{\mathbf{N}} = \frac{V}{\mathbf{N}} \sum_{i=1}^{\mathbf{N}} K(\tilde{\theta}_i)$, where $K(\tilde{\theta}_i) = f_{\psi}^{\delta}(\tilde{\theta}_i)\, p(\tilde{\theta}_i \mid \mathcal{D})$ and $V = \int_{\tilde{\theta}} d\tilde{\theta}$. According to Chebyshev's inequality, one has

$$\mathbf{Pr}(|Q_{\mathbf{N}} - \mathbb{E}[Q_{\mathbf{N}}]| \leq \varepsilon) \geq 1 - \frac{\mathrm{Var}[Q_{\mathbf{N}}]}{\varepsilon^2}, \qquad (13)$$

for a given ε, in which $\mathrm{Var}[Q_{\mathbf{N}}] = \frac{V^2}{\mathbf{N}^2} \sum_{i=1}^{\mathbf{N}} \mathrm{Var}[K(\tilde{\theta}_i)] = \frac{V^2 \delta_{\mathbf{K}}^2}{\mathbf{N}}$ with $\delta_{\mathbf{K}}^2 = \mathrm{Var}[K(\tilde{\theta}_i)]$. Finally, we get $\mathbf{Pr}(Q_{\mathbf{N}} - \mathbb{E}[Q_{\mathbf{N}}] \leq \varepsilon) \geq 1 - \frac{V^2 \delta_{\mathbf{K}}^2}{\varepsilon^2 \mathbf{N}}$. By choosing an appropriate $\mathbf{N}$ and ε, one can expect an efficient approximation of the confidence integral.

In order to implement the Monte Carlo technique more effectively, one can restrict the search region by solving an optimization problem over the constraints (12) in order to find the extreme points for the parameters, therefore, fewer samples are needed to be chosen in this (potentially) smaller region.

Confidence Computation Using Piecewise Affine Approximation Of The Nonlinear Constraint. Another approach for computing the confidence value in (3) is approximating the nonlinear term $\Gamma(\tilde{\theta}, \delta)$ in (12) using *piecewise affine* (PWA) functions. Then, linear programming can be used in order to approximate the feasible set.

***Lemma** 2.* The feasible set of (12) for all predicates and time steps within the horizon of **STL** property (if existing) can be recovered in the limit for large numbers of piecewise regions in order to approximate the nonlinear part of (12).

6. EXPERIMENTAL RESULTS

Consider a parameterized class of models $\mathrm{M}(\theta)$ with the state-space representation

$$\mathrm{M}(\theta) \in \begin{cases} x(t+1) = \begin{bmatrix} a & 0 \\ 1-a^2 & a \end{bmatrix} x(t) + \begin{bmatrix} \sqrt{1-a^2} \\ -a\sqrt{1-a^2} \end{bmatrix} u(t) + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} w(t) \\ \hat{y}(t,\theta) = \theta^T x(t). \end{cases}$$

Each model in $\mathrm{M}(\theta)$ has a single input and a single output. The coefficient a is 0.4 and the parameter set is selected as $\theta \in \Theta = [-10, 10] \times [-10, 10]$. The system $\mathbf{S} \in \mathrm{M}(\theta)$ has the true parameter $\theta_{true} = [-0.5, 1]^T$. System $\mathbf{S}$ is a member of models demonstrated by the Laguerre-basis functions as transfer functions (Haesaert et al., 2015). This is a special case of the orthonormal basis functions and can be translated to the aforementioned parameterized state space format. The system is affected by a process noise which is a Gaussian process with covariance matrix $0.5\mathbb{I}_2$. There is also an additive measurement noise with zero-mean and variance 0.5. The input range is considered to be $[-0.2, 0.2]$.

We want to verify with high probability if the output of the system $\mathbf{S}$ remains in $\mathfrak{l}_1 = [-0.5, 0.5]$ until it reaches $\mathfrak{l}_2 = [-0.1, 0.1]$ at some time in the interval $[2, 4]$. We denote the atomic propositions $\mu_1 = \{y \geq -0.5\}$, $\mu_2 = \{-y \geq -0.5\}$, $\mu_3 = \{y \geq -0.1\}$, $\mu_4 = \{-y \geq -0.1\}$. Our desired property can be written as $\mathbf{Pr}(\mathbf{S} \models (\mu_1 \wedge \mu_2)\, \mathsf{U}_{[2,4]}\, (\mu_3 \wedge \mu_4)) \geq 1 - \delta$. We select $\delta = 0.01$. We use the procedure in Section 4 to decompose this **STL** property to algebraic constraints on the atomic propositions. The feasible set is approximated either using the Monte Carlo method or the piecewise affine approximation described in Section 5. The initial set can be restricted by finding the extreme values of θ over all constraints as described in Subsection 5.2 which is considered $[-3.5, 3.5]$ for this case study. Computed feasible set using the Monte Carlo technique is demonstrated in Fig. 2 with red-face squares. The feasible set which is recovered with the piecewise affine technique is illustrated in Fig. 2 with blue-edge diamonds. We found the feasible set of parameters for (12) for all time steps in θ and P space. Then, this feasible set is projected into θ space using MPT3 toolbox (Herceg et al., 2013).

As we do not have any prior knowledge about the parameters, we choose a uniform distribution $p(\theta)$ on the possible models. Based on the uniform prior, the confidence is computed using (3) as 0.0279 and 0.0258 with Monte Carlo and PWA approximations, respectively. Afterward, we designed an experiment on the system with the true parameter and an input sequence as Gaussian noise with a uniform distribution over $[-2, 2]$ and measured output for 50 consecutive time instances. Using updated $p(\theta \mid \mathcal{D})$ coming from the measurement data, confidence improved significantly into 0.9099 and 0.8962 for Monte Carlo and PWA, respectively. We repeated the same experiment 100 times for several other true parameters θ_{true}. For all of these instances, updated posteriori probability in (9), after 50 measurements, is used in order to compute the confidence value according to (3). Contours of the posterior distribution are illustrated in Fig. 2 . Results of computing

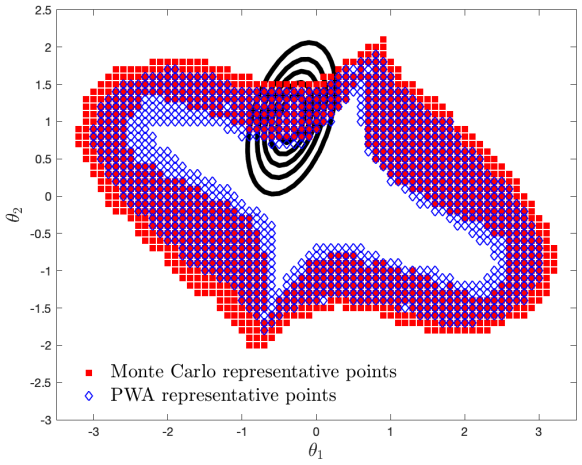

Fig. 2. Contours of $p(\theta \mid \mathcal{D})$ for $\theta_{true} = [-0.5, 1]^T$ after 50 measurements over the feasible set computed by the Monte Carlo and PWA techniques.

the confidence with Monte Carlo and PWA approximation are shown in Table 6. As it can be seen, for parameters that lie deep inside the feasible set, the confidence value is high with a low variance for both techniques. Meanwhile, for the points near the edges, the variance is higher and confidence value is lower. For points far enough from the feasible set, confidence tends to be zero.

Table1. Means and variances of computed confidence values for 5 different true parameters.

	Monte Carlo		PWA	
θ_{true}	Mean	Variance	Mean	Variance
$[-0.5, 1]^T$	0.9587	0.0023	0.9514	0.0042
$[3, -1]^T$	0.4902	0.0061	0.5032	0.0062
$[1, 0.5]^T$	0.7932	0.0025	0.7584	0.0053
$[-2, 1.5]^T$	0.9018	0.0009	0.9156	0.0005
$[2, -1]^T$	0.0278	0.0005	0.0480	0.0006

REFERENCES

Bartocci, E., Bortolussi, L., and Sanguinetti, G. (2014). Data-driven statistical learning of temporal logic properties. In *FORMATS*, 23–37. Springer.

Beyer, D., Dangl, M., and Wendler, P. (2018). A unifying view on SMT-based software verification. *Journal of Automated Reasoning*, 60(3), 299–335.

Beyer, D. and Keremoglu, M.E. (2011). CPAchecker: A tool for configurable software verification. In *CAV*, 184–190.

Chou, Y. and Sankaranarayanan, S. (2019). Bayesian parameter estimation for nonlinear dynamics using sensitivity analysis. In *AAAI*, 5708–5714.

Clarke, E.M. and Zuliani, P. (2011). Statistical model checking for cyber-physical systems. In *ATVA*, 1–12.

Fainekos, G.E. and Pappas, G.J. (2006). Robustness of temporal logic specifications. In *Formal Approaches to Software Testing*, 178–192. Springer.

Farahani, S.S., Majumdar, R., Prabhu, V.S., and Soudjani, S. (2018a). Shrinking horizon model predictive control with signal temporal logic constraints under stochastic disturbances. *IEEE Transactions on Automatic Control*.

Farahani, S.S., Soudjani, S., Majumdar, R., and Ocampo-Martinez, C. (2018b). Formal controller synthesis for wastewater systems with signal temporal logic constraints: The Barcelona case study. *Journal of Process Control*, 69, 179–191.

Georghiou, A., Tsoukalas, A., and Wiesemann, W. (2019). Robust dual dynamic programming. *Operations Research*.

Haesaert, S., Van den Hof, P.M., and Abate, A. (2015). Data-driven property verification of grey-box systems by Bayesian experiment design. In *ACC*, 1800–1805.

Haesaert, S., Van den Hof, P.M., and Abate, A. (2016). Data-driven and model-based verification via Bayesian identification and reachability analysis. *Science and Technology*, 26, 35.

Herceg, M., Kvasnica, M., Jones, C.N., and Morari, M. (2013). Multi-Parametric Toolbox 3.0. In *ECC*, 502–510.

Kazemi, M. and Soudjani, S. (2020). Formal policy synthesis for continuous-space systems via reinforcement learning. *arXiv:2005.01319*.

Lavaei, A., Somenzi, F., Soudjani, S., Trivedi, A., and Zamani, M. (2020). Formal controller synthesis for continuous-space MDPs via model-free reinforcement learning. *arXiv:2003.00712*.

Polgreen, E., Wijesuriya, V.B., Haesaert, S., and Abate, A. (2017). Automated experiment design for data-efficient verification of parametric Markov decision processes. In *QEST*, 259–274. Springer.

Raman, V., Donzé, A., Sadigh, D., Murray, R.M., and Seshia, S.A. (2015). Reactive synthesis from signal temporal logic specifications. In *HSCC*, 239–248. ACM.

Sadigh, D. and Kapoor, A. (2016). Safe control under uncertainty with probabilistic signal temporal logic.

Sadraddini, S. and Belta, C. (2018). Formal guarantees in data-driven model identification and control synthesis. In *HSCC*, 147–156.

Sen, K., Viswanathan, M., and Agha, G. (2004). Statistical model checking of black-box probabilistic systems. In *CAV*, 202–215. Springer.

Sen, K., Viswanathan, M., and Agha, G. (2005). On statistical model checking of stochastic systems. In *CAV*, 266–280. Springer.