Data-Driven Safety Verification of Stochastic Systems via Barrier Certificates: A Wait-and-Judge Approach

Ali Salamati ALI.SALAMATI@LMU.DE
Computer Science Department, Ludwig-Maximilians-Universität München, Germany

Majid Zamani MAJID.ZAMANI@COLORADO.EDU
Computer Science Department, University of Colorado Boulder, USA
Computer Science Department, Ludwig-Maximilians-Universität München, Germany

Editors: R. Firoozi, N. Mehr, E. Yel, R. Antonova, J. Bohg, M. Schwager, M. Kochenderfer

Abstract

We provide a data-driven approach equipped with a formal guarantee for verifying the safety of stochastic systems with unknown dynamics. First, using a notion of barrier certificates, the safety verification for a stochastic system is cast as a robust convex program (RCP). Solving this optimization program is hard because the model of the stochastic system, which is unknown, appears in one of the constraints. Therefore, we construct a scenario convex program (SCP) by collecting a number of samples from trajectories of the system. Then, under some condition over the optimal value of the resulted SCP, we are able to relate its optimal decision variables to the safety of the original stochastic system and provide a formal out-of-sample performance guarantee. Particularly, we propose a so-called wait-and-judge approach which a posteriori checks some condition over the optimal value of the SCP for a fixed number of sampled data. If the condition is satisfied, then the safety specification is satisfied with some probability lower bound and a desired confidence. The effectiveness of our approach in requiring only a low number of samples compared to existing results in the literature is illustrated on a two-tank system by ensuring that the water levels in both tanks never reach a critical zone within a specific time horizon.

Keywords: Data-driven approach, Stochastic systems, Safety specification, Formal verification, Barrier certificate, Robust convex program, Scenario convex program.

1. Introduction

Safety-critical application are becoming more and more ubiquitous due to recent advances in computation and communication devices. Examples of such applications include self-driving cars, power grids, traffic networks, and integrated medical devices. In order to deploy these safety-critical systems, rigorous safety analysis is required to ensure the correctness of their functionalities.

In order to ensure safety of such applications, there have been many results in the past two decades on developing discretization-based or discretization-free techniques to either verify safety specifications or synthesize controllers ensuring them. In abstraction-based techniques, e.g., Tabuada (2009); Belta et al. (2017); Girard et al. (2010); Zamani et al. (2014), finite approximations are constructed by discretizing state and input sets. Those approximations are then utilized for verification and synthesis purposes. Unfortunately, those abstraction-based techniques suffer from the curse of dimensionality due to discretizing state and input sets and, hence, they are not amenable to large-scale systems. One of the abstraction-free techniques leveraged in the past decade is to utilize a notion

© 2022 A. Salamati & M. Zamani.

of barrier certificates (BC). The main advantage of using barrier certificates in comparison with the abstraction-based techniques is that we do not need to discretize state and input sets to verify safety specifications or synthesize controllers ensuring them (Prajna and Jadbabaie, 2004; Ames et al., 2017; Jagtap et al., 2020b). Unfortunately, all of the above-mentioned discretization-based or discretization-free results require a model of the system which may not be available or too complex to be of any use.

In the last few years, there have been some investigations on verifying the safety of dynamical systems by collecting data from their trajectories, see, e.g, Sadraddini and Belta (2018), Wijesuriya and Abate (2019); Lavaei et al. (2020); Wang and Jungers (2020). There are also some results that combine notions of barrier certificates and collected data from the systems in order to provide a formal guarantee on the safety verification, see, e.g, Han et al. (2015); Robey et al. (2020); Jagtap et al. (2020a); Lindemann et al. (2020); Salamati et al. (2021). However, those results either need a complete or partial knowledge of a model of the system, suffer from sample complexity to provide out-of-sample performance guarantees, may not provide any out-of-sample performance guarantees, require some stability assumptions, or treat only non-stochastic systems.

Inspired by the results in Campi and Garatti (2018), in this paper we propose a so-called wait-and-judge approach which provides a data-driven scheme for the safety verification of stochastic systems with unknown models while providing an out-of-sample performance guarantee and at the same time alleviating the sample complexity issue. In particular, we use a notion of barrier certificates and use it to cast the safety problem as a robust convex program (RCP). Since solving this optimization program is not tractable due to the unknown model of which appears in one of the constraints, instead we propose a scenario convex program (SCP) corresponding to the original RCP by using an arbitrary number of samples collected from the system's trajectories. Then, we derive a condition over the optimal value of the obtained SCP under which the original unknown stochastic system is safe with some probability lower bound and a guaranteed confidence. This condition is related to the number of support constraints. For a given amount of data, support constraints are the ones whose elimination affects the optimal value substantially. Since, we relate the desired confidence, probability of violation of constraints, and the number of samples a posteriori, the required amount of data reduces dramatically compared to other approaches which require this relation a priori, see the results in Salamati et al. (2021). We finally apply our approach to a two-tank system in order to verify that the water levels in both tanks never reach a critical zone within a specific time horizon. We refer the interested readers to this case study showing the effectiveness of our approach in comparison with the one in Salamati et al. (2021) in terms of sample complexity.

2. Problem Statement and Preliminaries

2.1. Notation

The set of positive integers, non-negative integers, real numbers, non-negative real numbers, and positive real numbers are denoted by $\mathbb{N} := \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$, $\mathbb{R}$, $\mathbb{R}_0^+$, and $\mathbb{R}^+$, respectively. We denote the indicator function by $\mathbb{1}_{\mathscr{A}}(X) : X \to \{0, 1\}$, where $\mathbb{1}_{\mathscr{A}}(x)$ is 1 if and only if $x \in \mathscr{A}$, and 0 otherwise. Notation $\mathbf{1}_m$ is used to indicate a column vector of ones in $\mathbb{R}^m$. We denote by $\|x\|$ the Euclidean norm of any $x \in \mathbb{R}^n$. We also denote the induced norm of any matrix $A \in \mathbb{R}^{m\times n}$ by $\|A\| := \sup_{x\neq 0} \|Ax\|/\|x\|$. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}$, and $i \in \{1, \ldots, N\}$, we use $[x_1; \ldots; x_N]$ and $[x_1, \ldots, x_N]$ to denote the corresponding column and row vectors, respectively, with dimension $\sum_i n_i$. Considering a random variable z, Var(z) denotes its variance. The absolute value of a real number $x \in \mathbb{R}$ is denoted by $|x|$. We use the notation $S \models_H \Psi$ to denote that system S satisfies a property Ψ during a time horizon H. We also use $\models$ in this paper to show that a solution is feasible for an optimization problem.

The sample space of random variables is denoted by Ω. The Borel σ-algebra on a set X is denoted by $\mathfrak{B}(X)$. The measurable space on X is denoted by $(X, \mathfrak{B}(X))$. We have two probability spaces in this work. The first one is represented by $(X, \mathfrak{B}(X), \mathbb{P})$ which is the probability space defined over the state set X with $\mathbb{P}$ as a probability measure. The second one, $(V_w, \mathfrak{B}(V_w), \mathbb{P}_w)$, defines the probability space over V_w for the random variable w affecting the stochastic system as process noise with $\mathbb{P}_w$ as its probability measure. With a slight abuse of notation, we use the same notation for $\mathbb{P}$ and $\mathbb{P}_w$ when the product measures are needed in the formulations.

2.2. System Definition

In this work, we deal with discrete-time stochastic systems as formalized in the next definition.

Definition 1 *Consider a discrete-time stochastic system (dt-SS), denoted by $S = (X, V_w, w, f)$, described by:*

$$S\colon x(t+1) = f(x(t), w(t)), \quad t \in \mathbb{N}_0, \tag{1}$$

where X and V_w are Borel σ-algebras on the set $\mathbb{R}^n$ and uncertainty spaces, respectively. Here, x denotes the state sequence of the system as $x := \{x(t) : \Omega \to X, t \in \mathbb{N}_0\}$, and w denotes a sequence of i.i.d random variables over V_w as $w := \{w(t) : \Omega \to V_w, t \in \mathbb{N}_0\}$. Map $f : X \times V_w \to X$ is a measurable function characterizing the state evolution of the system. A finite trajectory of the system in (1) is denoted by $\xi(t) := x(0)x(1)\ldots x(t), t \in \mathbb{N}_0$.

2.3. Problem Statement

In order to define the main problem we are interested to solve in this paper, we introduce the following definition.

Definition 2 *Consider a safety specification denoted by Ψ and a dt-SS S. System S is called safe for a finite time horizon $H \in \mathbb{N}_0$, denoted by $S \models_H \Psi$, if all trajectories of S started from a given initial set $X_{in} \subset X$ never reach a given unsafe set $X_u \subset X$ within time horizon H.*

Now, we state the main problem we aim at solving in this paper.

Problem 3 *Consider a dt-SS S as in Definition 1, where f and $\mathbb{P}_w$ are* unknown. *With a confidence of at least $(1-\beta) \in [0,1]$, provide a lower bound $(1-\Delta) \in [0,1]$ on the probability with which S satisfies safety specification Ψ, i.e., $\mathbb{P}_w\big(S \models_H \Psi\big) \geq 1-\Delta$, using a finite number of samples collected from the system's trajectories.*

To tackle this problem, we first need to present a safety analysis of stochastic systems via barrier certificates as in the next subsection. Afterwards in Section 3, we show how the proposed safety problem can be cast as a robust convex program (RCP) and consequently as a scenario convex program (SCP) with the help of data collected from the system. Eventually, we provide a result in Section 4 which addresses Problem 3. Fig. 1 shows an overview of our approach for solving Problem 3 by connecting the related optimizations and results in the paper.

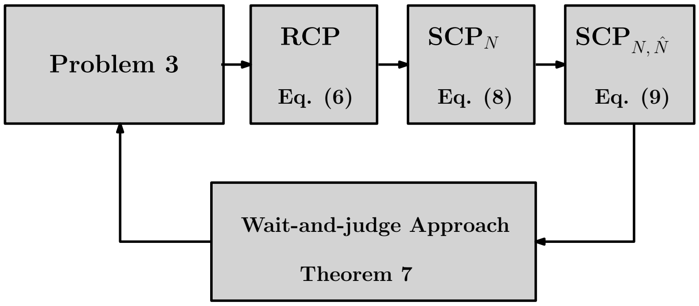

Figure 1: An overview of the proposed wait-and-judge approach in this work

2.4. Safety Verification for Stochastic Systems

Here, we introduce a concept of barrier certificates and its application in the safety verification of stochastic systems. Let us start with the formal definition of barrier certificates.

Definition 4 *Consider a safety specification Ψ and a dt-SS S as in Definition 1. A non-negative function* $\mathrm{B} : X \to \mathbb{R}_0^+$ *is called a barrier certificate (BC) for S if there exist constants $\lambda > 1$, and $c \in \mathbb{R}_0^+$ such that*

$$\mathrm{B}(x) \leq 1, \qquad \forall x \in X_{in}, \tag{2}$$

$$\mathrm{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{3}$$

$$\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \mathrm{B}(x) + c, \qquad \forall x \in X, \tag{4}$$

where $X_{in} \subset X$ and $X_u \subset X$ are initial and unsafe sets, respectively, corresponding to Ψ.

Next theorem, borrowed from Jagtap et al. (2020b), provides a lower bound on the probability of safety satisfaction for a dt-SS.

Theorem 5 *Consider a dt-SS S as in Definition 1, and a safety specification Ψ. Suppose that there exists a barrier certificate* B *satisfying conditions (2)-(4). Then one obtains*

$$\mathbb{P}_w\big(S \models_H \Psi\big) \geq 1 - \frac{1 + c\,H}{\lambda}, \tag{5}$$

where $H \in \mathbb{N}_0$ is the finite time horizon associated with Ψ.

In this work, we fix the structure of barrier certificates as $B(b,x) = \sum_{j=1}^{r} b_j p_j(x)$ with some user-defined (possibly nonlinear) basis functions $p_j(x)$ and unknown coefficients $b = [b_1; \cdots; b_r] \in \mathbb{R}^r$. For the sake of simplicity of the presentation, we consider polynomial-type barrier certificates with degree $k \in \mathbb{N}_0$, where basis functions $p_j(x)$ are monomials over x.

3. Data-driven Safety Verification for Stochastic Systems

According to Salamati et al. (2021), a barrier-based safety verification as in Theorem 5 together with Definition (4) can be reformulated as a robust convex program as follows:

$$\text{RCP}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x,d)\big) \leq 0, z \in \{1,\ldots,4\}, \forall x \in X, \\ \qquad d = [K;\lambda;c;b], \\ \qquad K \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{6}$$

where,

$$\begin{aligned} g_1(x,d) &= -\mathrm{B}(b,x) - K, \\ g_2(x,d) &= \mathrm{B}(b,x)\mathbb{1}_{X_{in}}(x) - 1 - K, \\ g_3(x,d) &= -\mathrm{B}(b,x)\mathbb{1}_{X_u}(x) + \lambda - K, \\ g_4(x,d) &= \mathbb{E}\Big[\mathrm{B}(b,f(x,w)) \mid x\Big] - \mathrm{B}(b,x) - c - K. \end{aligned} \tag{7}$$

An extra constraint can be added to the above optimization problem in order to enforce a desired probability lower bound of $1-\Delta$ using the relation in (5) according to Salamati et al. (2021). In general, finding an optimal solution for the RCP in (6) is hard because the map f and the probability measure $\mathbb{P}_w$ are both unknown. Furthermore, there are infinitely many constraints in the RCP since $x \in X$, where X is a continuous set. To tackle this issue, we collect N i.i.d samples $\mathcal{D}_N := \{x_i, f(x_i,w)\} \subset X^2$, for $i \in \{1,\ldots,N\}$, using an assigned probability distribution over the state set. Substituting these samples in the RCP in (6) results in the following scenario convex program denoted by SCP_N:

$$\text{SCP}_N: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x_i,d)\big) \leq 0, z \in \{1,\ldots,4\}, \forall i \in \{1,\ldots,N\}, \\ \qquad d = [K;\lambda;c;b], \\ \qquad K \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{8}$$

where $g_z(x,d)$, $z \in \{1,\ldots,4\}$, are as in (7). To address the issue of not knowing $\mathbb{P}_w$ and the expectation term in g_4 (7), we replace the expectation term with its empirical mean approximation by sampling $\hat{N}$ i.i.d. values w_j from $\mathbb{P}_w$ for each x_i: $\mathcal{D}_{\hat{N}} := \{x_i, w_j, f(x_i,w_j)\} \subset X \times V_w \times X$, $\forall j \in \{1,\ldots,\hat{N}\}$, which results in the following SCP denoted by $\text{SCP}_{N,\hat{N}}$:

$$\text{SCP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x_i,d), \bar{g}_4(x_i,d)\big) \leq 0,\ z \in \{1,2,3\}, \\ \qquad \forall x_i \in X, \forall i \in \{1,\cdots,N\}, \\ \qquad d = [K;\lambda;c;b], \\ \qquad K \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{9}$$

where

$$\bar{g}_4(x_i,d) = \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x_i,w_j)) - \ \mathrm{B}(b,x_i) - c - K + \delta. \tag{10}$$

We denote by $K^*_{N,\hat{N}}$ and $\hat{\mathrm{B}}(b,x|\mathcal{D}_N,\mathcal{D}_{\hat{N}})$, respectively, the optimal value of $\mathrm{SCP}_{N,\hat{N}}$ and the barrier function constructed based on solution of $\mathrm{SCP}_{N,\hat{N}}$. Note that the expectation term in g_4 (8) is approximated by the empirical mean in (10). This approximation introduces an error which is denoted by δ in (10).

Remark 6 *In this paper, N is selected arbitrarily. According to Salamati et al. (2021), $\hat{N}$ can be computed as $\hat{N} \geq \frac{\hat{M}}{\delta^2 \beta_s}$ for a desired confidence value $\beta_s \in (0,1)$. This is the confidence that a solution of $SCP_{N,\hat{N}}$ is a feasible solution for SCP_N, i.e., $\mathbb{P}_w\big(\hat{\mathrm{B}}(b,x|\mathcal{D}_N,\mathcal{D}_{\hat{N}}) \models SCP_N\big) \geq 1-\beta_s$. In this inequality, $\hat{M}$ is a positive constant defined as $Var\big(\mathrm{B}(b,f(x,w))\big) \leq \hat{M},\ \forall x \in X$, and δ is the approximation error in (10).*

In the next section, we show how the solution of a $\mathrm{SCP}_{N,\hat{N}}$ for an N and $\hat{N}$ is related to the safety of a stochastic system with an unknown model.

4. Safety Verification of Stochastic Systems via Wait-and-judge Approach

In this section, we aim to establish a probabilistic bridge between the solution of the SCP in (9) and the safety of a dt-SS as in Definition (1). To do so, we need to assume that all constraints in (7) are Lipschitz continuous with respect to x. Next theorem connects the safety of a stochastic system to the optimal solution of the SCP resulted from substituting N number of samples by the number of so-called support constraints. Given N number of constraints, support constraints are those whose elimination affects the optimal value *considerably*.

Theorem 7 *Consider a stochastic system* S *as in* (1)*, where f and $\mathbb{P}_w$ are* unknown*, a safety specification Ψ, and a finite time horizon H. Assume that all constraints in* (7) *are Lipschitz continuous with respect to x with a Lipschitz constant* L_{x}*. Select an arbitrary number of samples N and confidence $\beta \in (0,1)$. Choose $\hat{N}$ as in Remark 6 to achieve a given confidence $1-\beta_s,\ \beta_s \in (0,1)$. Let us denote by $K^*_{N,\hat{N}}$ and $d^*_{N,\hat{N}} = [\lambda^*; c^*; b^*]$, the optimal value and the optimal solution of $SCP_{N,\hat{N}}$ in* (9)*, respectively. If*

$$K^*_{N,\hat{N}} + \mathrm{L}_{\mathrm{x}}\ (1-T_{N^*})^{\frac{1}{n}} \leq 0, \tag{11}$$

where T_{N^*} is the unique solution of

$$\frac{\beta}{N+1}\sum_{m=N^*}^{N}\binom{m}{N^*}T_{N^*}^{m-N^*} - \binom{N}{N^*}T_{N^*}^{N-N^*} = 0, \tag{12}$$

with N^* as the number of support constraints, then the following statement holds true with a confidence of at least $1-\beta-\beta_s$:

$$\mathbb{P}_w(\mathrm{S} \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}, \tag{13}$$

Remark 8 *There is an upper-bound on the number of support constraints, i.e, $N^* \leq |d|+1$, where $|d|$ is the number of decision variables in $SCP_{N,\hat{N}}$* (9)*. Note that the value of $1-T_{N^*}$ is increasing* *with respect to N^*. As a result, one can use this upper-bound instead of the actual number of support constraints N^* in Theorem 7.*

The proof of the theorem in provided in the Appendix. The steps required for applying Theorem 7 are presented in Algorithm 1. The inputs are the desired confidence, and the Lipschitz constant of constraints in (7). The output is a lower bound on the safety of the stochastic system in (1) based on the solution of the SCP in (9) with an a priori guaranteed confidence. The coefficients of the barrier certificate satisfying conditions (2)-(4) are obtained in step 5 of Algorithm 1.

Algorithm 1 Data-driven safety verification of a stochastic system via wait-and-judge approach

```
Require: Parameters $\beta \in (0,1)$, $\beta_s \in (0,1)$, $\mathrm{L_x} \in \mathbb{R}^+$, and the degree of the barrier certificate
1: Compute the number of noise realization $\hat{N}$ according to Remark 6
2: Choose an arbitrary number of samples $N$
3: Select a probability measure $\mathbb{P}$ over the state set $X$
4: Collect $N\hat{N}$ pairs $\big(x_i, f(x_i, w_{ij})\big)_{i,j} \in X^2$ from the system
5: Solve the SCP$_{N,\hat{N}}$ in (9) with the data-set in Step 4 and obtain $K^*_{N,\hat{N}}$
6: Compute the actual number of support constraints $N^*$ or the upper bound on it (see Remark 8)
7: Compute the parameter $T_{N^*}$ according to (12)
Ensure: If $K^*_{N,\hat{N}} + \mathrm{L_x}\ (1 - T_{N^*})^{\frac{1}{n}} \leq 0$, then $\mathbb{P}_w(S \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}$ with a confidence of at least
    $1 - \beta - \beta_s$.
```

5. Case Study

Consider a two-tank system characterized by the following discrete-time stochastic system:

$$\begin{aligned}
\mathrm{h}_1(t+1) &= (1 - \tau_s \frac{\alpha_1}{A_1})\ \mathrm{h}_1(t) + \tau_s \frac{q_i(t)}{A_1} + w_1(t) \\
\mathrm{h}_2(t+1) &= \tau_s \frac{\alpha_1}{A_2}\ \mathrm{h}_1(t) + (1 - \tau_s \frac{\alpha_2}{A_2})\ \mathrm{h}_2(t) + \tau_s \frac{q_o(t)}{A_2} + w_2(t),
\end{aligned} \tag{14}$$

where $\mathrm{h}_1(t)$ and $\mathrm{h}_2(t)$ are heights of two tanks, respectively. Terms $w_1(t)$ and $w_2(t)$ are additive zero-mean Gaussian noises with standard deviations of 0.01, which model the environmental uncertainties. Parameters α_i and A_i, $i \in \{1, 2\}$, are valve coefficients and the area of tank i. Variables $q_i(t)$ and $q_0(t)$ are inflow rate entering the first tank and outflow rate exiting the second one at time t, respectively. The model for this two-tank system is adapted from Ramos and Dos Santos (2007) discretized by $\tau_s = 0.1$ seconds. We consider $[\mathrm{h}_1(t+1); \mathrm{h}_2(t+1)] = A_\tau[\mathrm{h}_1(t); \mathrm{h}_2(t)] + b_\tau + [w_1(t); w_2(t)]$, where $A_\tau = [1 - \tau_s, 0; \tau_s, 1 - \tau_s]$ and $b_\tau = [4.5\tau_s; -3\tau_s]$ in the situation in which input and output valves are fully open, and two constant-rate feeding and retaining pumps ensure constant flows of $q_i(t)$ and $q_o(t)$ with values of $4.5m^3/s$ and $3m^3/s$, respectively. Let us consider $X_{in} = [1.75m, 2.25m]^2$, $X_u = [9m, 10m]^2$, and $X = [1m, 10m]^2$ as the initial, unsafe and the overall state sets, respectively. We assume the model of the system and the distribution of the noise are unknown. The main goal is to verify that the heights of tanks stay away from the unsafe region within the time horizon $H = 5$ with an a priori confidence 99%. Let us consider a barrier certificate with degree $k = 2$ in the polynomial form as $[\mathrm{h}_1;\mathrm{h}_2;1]^T\mathrm{P}[\mathrm{h}_1;\mathrm{h}_2;1] = b_0\mathrm{h}_1^2 + b_1\mathrm{h}_2^2 + b_2\mathrm{h}_1\mathrm{h}_2 + b_3\mathrm{h}_1 + b_4\mathrm{h}_2 + b_5$, where

$$\mathrm{P} = \begin{bmatrix} b_0 & \frac{b_3}{2} & \frac{b_2}{2} \\ \frac{b_3}{2} & b_1 & \frac{b_4}{2} \\ \frac{b_2}{2} & \frac{b_4}{2} & b_5 \end{bmatrix}. \tag{15}$$

By having $\|x\| \leq \sqrt{2} \times 10$ and enforcing $\|P\| \leq 0.2$, the Lipschitz constant can be computed as $\mathrm{L}_x = 11.03$ using (Salamati et al., 2021, Lemma 1). The value of empirical approximation error in (10) is selected as $\delta = 0.05$. By enforcing $\hat{M} = 0.001$, the required number of samples for the approximation of the expected value in (9) is computed as $\hat{N} = 400$ according to Remark 6 in order to provide a confidence of $1 - \beta_s$, where $\beta_s = 0.001$.

To show the effectiveness of our approach in allowing us to have a much lower number of samples, we first solve the safety verification problem for the two-tank system via the approach proposed in the literature and then we apply our proposed wait-and-judge approach here. We show that our approach provides the same formal guarantee with a significantly lower number of samples.

Data-driven safety verification using the method proposed in Salamati et al. (2021)

We choose $\epsilon = 0.04$ and $\Delta = 0.1$ in (Salamati et al., 2021, Algorithm 1). We also select the confidence parameter β as 0.009. The minimum number of samples needed for solving $\mathrm{SCP}_{N,\hat{N}}$ in (9) is computed as $N = 1337297$ using (Salamati et al., 2021, equation (17)). $\hat{N}$ is computed as 400 for a confidence value of $\beta_s = 0.001$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with acquired values of N and $\hat{N}$ which gives us the optimal value $K^*_{N,\hat{N}} = -0.1025$. Since $K^*_{N,\hat{N}} + \epsilon = -0.0625 \leq 0$, according to (Salamati et al., 2021, Theorem 4), one can conclude: $\mathbb{P}_w(S \models_5 \Psi) \geq 1 - \Delta = 0.90$ with a confidence of at least $1 - \beta - \beta_s = 99\%$.

Data-driven safety verification via the proposed wait-and-judge approach

We select the desired confidence parameter $\beta = 0.009$. There is no need to fix ϵ a priori in our proposed approach here. We initially select an arbitrary number of samples $N = 500$. Number of support constraints is computed as $N^* = 7$. Parameter $1 - T_{N^*}$ is computed using (12) as 0.0087. The optimal value $K^*_{N,\hat{N}}$ is computed for $N = 500$ and $\hat{N} = 400$ as -0.1871. Then, the condition in (11) is not satisfied, i.e., $K^*_{N,\hat{N}} + \mathrm{L}_x(1 - T_{N^*})^{\frac{1}{2}} = 0.8417 \nleq 0$. Therefore, we cannot say anything about the safety of the two-tank system based on Theorem 7. By computing T_{N^*} for several numbers of samples according to (12), the appropriate number of samples to satisfy (11) is computed as $N = 70000$. Since the value of $1 - T_{N^*}$ is increasing with respect to the number of support constraints N^*, and there is an upper-bound on it, we use this upper-bound in our experiment. One has $N^* \leq |d| + 1$, where $|d|$ is the number of decision variables in (9). Here, we select the upper-bound on N^* as 10, given that the number of decision variables is 9. The optimal value $K^*_{N,\hat{N}}$ is computed for $N = 70000$ and $\hat{N} = 400$ as -0.1065. In this case, $1 - T_{N^*}$ is computed as 0.6653×10^{-4}. Now the condition in (11) is satisfied, i.e., $K^*_{N,\hat{N}} + \mathrm{L}_x(1 - T_{N^*})^{\frac{1}{2}} = -0.0165 \leq 0$, hence one can obtain $\mathbb{P}_w(\mathrm{S} \models_5 \Psi) \geq 0.90$ with a confidence of at least $1 - \beta - \beta_s = 99\%$. The barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is as follows:

$$\hat{\mathrm{B}}\big(b, \mathrm{p}_1, \mathrm{p}_2 \,|\, \mathcal{D}_N, \mathcal{D}_{\hat{N}}\big) = 0.0648\mathrm{p}_1^2 + 0.1784\mathrm{p}_2^2 + 0.0145\mathrm{p}_1\mathrm{p}_2 - 0.1687\mathrm{p}_1 - 0.0321\mathrm{p}_2 + 0.0486.$$

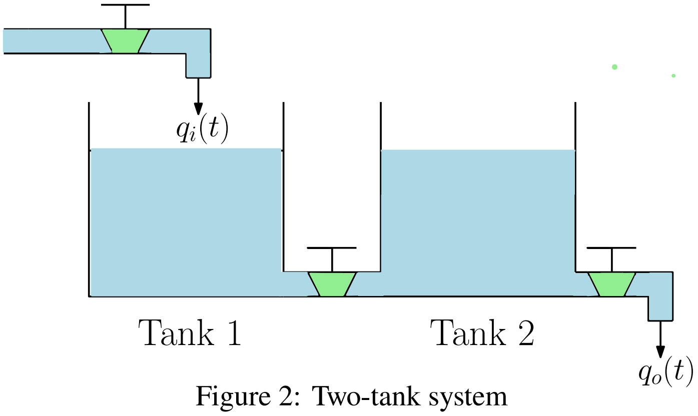

Figure 2: Two-tank system

The computed optimal values for c and λ are 0.1804 and 19.1280, respectively. It should be noted that the same desired confidence is achieved here as in the approach proposed in Salamati et al. (2021) using a significantly lower number of samples, i.e., 70000 compared to 1337297, which is the main benefit of our approach. In terms of computation time, our approach is much more faster than the one in Salamati et al. (2021). Computing the optimal value and checking the condition over the optimal value for the approach in Salamati et al. (2021) takes about 2 hours on a MacBook 2.8 GHz Quad-Core Intel Core i7, while it only takes less than 30 seconds using our proposed approach.

Acknowledgments

This work was supported in part by the NSF under grant CNS-2039062 and the H2020 ERC Starting Grant AutoCPS (grant agreement No 804639).

Appendix

Proof of Theorem 7:
From the robust convex program in (6), one can construct a chance constraint program (CCP) as follows:

$$\mathrm{CCP}_{\epsilon}:\begin{cases}\min\limits_{d} \quad K\\ \text{s.t.} \quad \mathbb{P}\Big(\max\big(g_z(x,d)\big)\leq 0\Big)\geq 1-\epsilon,\ z\in\{1,\ldots,4\},\\ \qquad d=[K;\lambda;c;b],\\ \qquad K\in\mathbb{R},\ \lambda>1,\ c\geq 0,\end{cases} \tag{16}$$

for some $\epsilon > 0$, where $g_z(x,d)$, $z \in \{1,\ldots,4\}$, are defined in (7). According to (Campi and Garatti, 2018, Theorem2), for any $\beta \in (0,1)$ and an arbitrary number of samples N, one has:

$$\mathbb{P}\big(d_N^* \models \mathrm{CCP}_{\epsilon(k)}\big)\geq 1-\beta, \tag{17}$$

where d_N^* is the optimal solution of the SCP_N in (8) and $\epsilon(k) := 1 - t(k)$, with $t(k)$ as the unique solution of

$$\frac{\beta}{N+1}\sum_{m=k}^{N}\binom{m}{k}\,t^{\,m-k}-\binom{N}{k}\,t^{\,N-k}=0, \tag{18}$$

for $k = \{0, \dots, |d|\}$, where $|d|$ is the number of decision variables d. Let us construct a relaxed version of RCP in (6) in amount of $h(\epsilon)$ as the following:

$$\mathrm{RCP}_{h(\epsilon(k))} : \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x,d)\big) \leq h(\epsilon(k)), z \in \{1,\dots,4\}, \forall x \in X, \\ \qquad d = [K; \lambda; c; b], \\ \qquad K \in \mathbb{R}, \ \lambda > 1, \ c \geq 0, \end{cases} \tag{19}$$

where $h(\epsilon)$ is a uniform level-set bound as defied in (Esfahani et al., 2014, Definition 3.1). According to (Esfahani et al., 2014, Lemma 3.2), one can deduce from (17) that $\mathbb{P}\big(d^*_N \models \mathrm{RCP}_{h(\epsilon(k))}\big) \geq 1-\beta$ which leads to:

$$\mathbb{P}(K^*_{\mathrm{RCP}_{h(\epsilon(k))}} \leq K^*_N) \geq 1-\beta, \tag{20}$$

where K^*_N is the optimal value of SCP_N in (8). Using Lemma 3.4 in Esfahani et al. (2014), we have:

$$K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_{\mathrm{RCP}_{h(\epsilon(k))}} + \mathcal{L}_{sp} h(\epsilon(k)), \tag{21}$$

where $\mathcal{L}_{sp}$ is the slater constant which is defined in (Esfahani et al., 2014, Assumption 3.3). Combination of (20) and (21) results in:

$$\mathbb{P}\Big(K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_N + \mathcal{L}_{sp} h(\epsilon(k))\Big) \geq 1-\beta. \tag{22}$$

Since the optimization problem in (6) is a min-max problem, $\mathcal{L}_{sp}$ can be chosen as 1 according to Remark 3.5 in Esfahani et al. (2014). Uniform level-set bound $h(\epsilon(k))$ can be computed as $\mathrm{L_x} \sqrt[n]{\epsilon(k)}$ as stated in (Esfahani et al., 2014, Remark 3.8), where $\mathrm{L_x}$ is the Lipschitz constant of constraints in (7). From now on, we use ϵ instead of $\epsilon(k)$ for $k = N^*$, where N^* is the number of support constraints. Therefore, (22) can be written as:

$$\mathbb{P}\Big(K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_N + \mathrm{L_x}\ \epsilon^{\frac{1}{n}}\Big) \geq 1-\beta. \tag{23}$$

By writing $1 - T_{N^*}$ instead of $\epsilon = 1 - t(k)$ for $k = N^*$, the above inequality can be re-written as:

$$\mathbb{P}\Big(K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_N + \mathrm{L_x}\ (1-T_{N^*})^{\frac{1}{n}}\Big) \geq 1-\beta. \tag{24}$$

By denoting the optimal solution of the $\mathrm{SCP}_{N,\hat{N}}$ in (9) by $d^*_{N,\hat{N}}$, one obtains $\mathbb{P}\big(d^*_{N,\hat{N}} \models \mathrm{SCP}_N\big) \geq 1-\beta_s$ according to (Salamati et al., 2021, Theorem 3.3) which implies:

$$\mathbb{P}\big(K^*_N \leq K^*_{N,\hat{N}}\big) \geq 1-\beta_s. \tag{25}$$

By defining two events $A := \{K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_N + \mathrm{L_x}\ (1-T_{N^*})^{\frac{1}{n}}\}$ and $B := \{K^*_N \leq K^*_{N,\hat{N}}\}$ with $\mathbb{P}(A) \geq 1-\beta$ and $\mathbb{P}(B) \geq 1-\beta_s$, it is easy to see that $(A \cap B) \subseteq (K^*_{\mathrm{RCP}} \leq K^*_{N,\hat{N}} + \mathrm{L_x}(1-T_{N^*})^{\frac{1}{n}})$. By assumption, we have $K^*_{N,\hat{N}} + \mathrm{L_x}(1-T_{N^*})^{\frac{1}{n}} \leq 0$ and, hence, one can deduce:

$$\mathbb{P}(K^*_{\mathrm{RCP}} \leq K^*_{N,\hat{N}} + \mathrm{L_x}(1-T_{N^*})^{\frac{1}{n}} \leq 0) \geq \mathbb{P}(A \cap B) \geq 1 - \mathbb{P}(A^c) - \mathbb{P}(B^c) \geq 1-\beta-\beta_s. \tag{26}$$

This concludes the proof because the non-positiveness of K^*_{RCP} guarantees that the feasible solution of RCP in (6) satisfies with a confidence of at least $1-\beta-\beta_s$ the barrier conditions in Theorem 5. ■

References

Aaron D. Ames, Xiangru Xu, Jessy W. Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 62(8): 3861–3876, 2017.

Calin Belta, Boyan Yordanov, and Ebru Aydin Gol. *Formal methods for discrete-time dynamical systems*, volume 15. Springer, 2017.

Marco C Campi and Simone Garatti. Wait-and-judge scenario optimization. *Mathematical Programming*, 167(1):155–189, 2018.

Peyman Mohajerin Esfahani, Tobias Sutter, and John Lygeros. Performance bounds for the scenario approach and an extension to a class of non-convex programs. *IEEE Transactions on Automatic Control*, 60(1):46–58, 2014.

Antoine Girard, Giordano Pola, and Paulo Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1):116–126, 2010.

Shuo Han, Ufuk Topcu, and George J Pappas. A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems. In *54th IEEE conference on decision and control (CDC)*, pages 2049–2054, 2015.

Pushpak Jagtap, George J. Pappas, and Majid Zamani. Control barrier functions for unknown nonlinear systems using gaussian processes. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3699–3704, 2020a.

Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, 2020b.

Abolfazl Lavaei, Fabio Somenzi, Sadegh Soudjani, Ashutosh Trivedi, and Majid Zamani. Formal controller synthesis for continuous-space mdps via model-free reinforcement learning. In *ACM/IEEE 11th International Conference on Cyber-Physical Systems*, pages 98–107. IEEE, 2020.

Lars Lindemann, Haimin Hu, Alexander Robey, Hanwen Zhang, Dimos V Dimarogonas, Stephen Tu, and Nikolai Matni. Learning hybrid control barrier functions from data. *arXiv:2011.04112*, 2020.

Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

José A Ramos and P Lopes Dos Santos. Mathematical modeling, system identification, and controller design of a two tank system. In *46th IEEE Conference on Decision and Control*, pages 2838–2843. IEEE, 2007.

Alexander Robey, Haimin Hu, Lars Lindemann, Hanwen Zhang, Dimos V Dimarogonas, Stephen Tu, and Nikolai Matni. Learning control barrier functions from expert demonstrations. *arXiv:2004.03315*, 2020.

Sadra Sadraddini and Calin Belta. Formal guarantees in data-driven model identification and control synthesis. In *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week)*, pages 147–156, 2018.

Ali Salamati, Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Data-driven safety verification of stochastic systems. *7th IFAC Conference on Analysis and Design of Hybrid Systems*, 2021.

Paulo. Tabuada. *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, 2009.

Zheming Wang and Raphaël M Jungers. Scenario-based set invariance verification for black-box nonlinear systems. *IEEE Control Systems Letters*, 5(1):193–198, 2020.

Viraj Brian Wijesuriya and Alessandro Abate. Bayes-adaptive planning for data-efficient verification of uncertain Markov decision processes. In *International Conference on Quantitative Evaluation of Systems*, pages 91–108. Springer, 2019.

Majid Zamani, Peyman Mohajerin Esfahani, Rupak Majumdar, Alessandro Abate, and John Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12):3135–3150, 2014.