Data-Driven Safety Verification using Barrier Certificates and Matrix Zonotopes

Mohammed Adib Oumer, Amr Alanwar, and Majid Zamani

Abstract— **Ensuring safety in cyber-physical systems (CPSs) is a critical challenge, especially when system models are difficult to obtain or cannot be fully trusted due to uncertainty, modeling errors, or environmental disturbances. Traditional model-based approaches rely on precise system dynamics, which may not be available in real-world scenarios. To address this, we propose a data-driven safety verification framework that leverages matrix zonotopes and barrier certificates to verify system safety directly from noisy data. Instead of trusting a single unreliable model, we construct a set of models that capture all possible system dynamics that align with the observed data, ensuring that the true system model is always contained within this set. This model set is compactly represented using matrix zonotopes, enabling efficient computation and propagation of uncertainty. By integrating this representation into a barrier certificate framework, we establish rigorous safety guarantees without requiring an explicit system model. Numerical experiments demonstrate the effectiveness of our approach in verifying safety for dynamical systems with unknown models, showcasing its potential for real-world CPS applications.**

I. Introduction

Ensuring safety is a fundamental requirement in the design and operation of cyber-physical systems (CPSs), particularly in safety-critical applications such as autonomous vehicles, robotics, power grids, and industrial automation [1]. Barrier certificates have emerged as a powerful and widely adopted tool for formal safety verification in dynamical systems [2]. These certificates are Lyapunov-like functions that ensure that system trajectories remain within a predefined safe region and do not reach an unsafe region. A barrier certificate is a real-valued function that is nonpositive over the initial states, positive over the unsafe states, and nonincreasing with transitions. Thus, such a certificate guarantees safety as its zero-level set separates the reachable and unsafe states. Moreover, its zero-sublevel set over-approximates the set of reachable states. By formulating safety conditions as inequalities involving the system's dynamics, a barrier certificate provides a computationally tractable alternative to reachability analysis. However, traditional approaches [2]–[7] assume explicit knowledge of the system model, significantly limiting their applicability in scenarios where the true system dynamics are unknown or uncertain.

To overcome this limitation, recent research has shifted towards data-driven approaches that construct barrier certificates directly from observed system behavior. The authors in [8] introduced a method for synthesizing barrier certificates using the Fundamental Lemma, which allows for the derivation of system properties from input-output data. While this approach removes the need for an explicit system model, it inherently assumes noiseless data, as the Fundamental Lemma relies on exact trajectory observations to infer system behavior. Consequently, its applicability is limited in real-world scenarios, where measurement noise, disturbances, and modeling uncertainties are inevitable. The study in [9], [10] explores data-driven safety verification of unknown discrete-time stochastic systems, presenting a novel approach that formulates the computation of barrier certificates as a robust convex optimization problem. This formulation leverages trajectory-based sampling to construct constraints, ensuring that the derived barrier certificates accurately capture system behavior under uncertainty. The paper in [11] transforms probabilistic barrier certificate constraints into a data-driven optimization framework by defining an ambiguous set of possible transition kernels. To tackle the resulting problem, it leverages sum-of-squares (SOS) optimization [12].

Recent advancements in data-driven reachability analysis have provided a promising alternative to traditional barrier certificate methods. A variety of approaches have emerged to tackle the problem of the unknown model from different perspectives. One approach in [13] introduced two probabilistic methods: one reformulated reachability as a classification problem, while the other applied Monte Carlo sampling to estimate reachable sets. Similarly, [14] proposed a hybrid strategy combining measurement-driven and model-based formal verification techniques. Other works have focused on refining reachability estimates through active learning [15], [16]. A probabilistic framework for general nonlinear systems, based on Christoffel function level sets, was developed in [17]. More recently, neural network-based approaches have gained traction. In [18], feedforward neural networks [19] were employed to approximate reachable sets, with uncertainty quantified via conformal inference [20], [21]. Additionally, kernel density estimation, accelerated by the fast Fourier transform, has been applied to model uncertainties and compute probabilistic reachable sets [22]. A distinct data-driven framework for forward stochastic reachability analysis was introduced in [23]. This method estimates the evolution of the state's probability density function using trajectory data, which is then used to construct a Gaussian mixture model. Although these probabilistic approaches enhance estimation accuracy with larger datasets, they still lack robust safety guarantees. In particular, rare but safety-critical events remain challenging to capture, limiting the reliability of purely

M. A. Oumer and M. Zamani are with the Department of Computer Science at the University of Colorado, Boulder, CO, USA. Emails: {mohammed.oumer, majid.zamani}@colorado.edu.

A. Alanwar is with the TUM School of Computation, Information and Technology at the Technical University of Munich, Heilbronn, Germany. E-mail: alanwar@tum.de.

probabilistic reachability methods.

Conversely, researchers have also investigated robust over-approximations of reachability using noise-free data. In [24], interval Taylor-based techniques were applied to systems modeled by differential inclusions, with later extensions incorporating noisy data. Another notable approach, proposed in [25], integrated partial model knowledge with data-driven learning to capture state-dependent uncertainties, relying on the assumption that the unknown dynamics conformed to a known bounding set. Additionally, [26] explored the computation of robust backward reachable sets for unknown linear systems, leveraging noisy data to ensure safety guarantees despite uncertainty. The method proposed in [27], [28] formulates a set of possible system models encapsulated within a matrix zonotope, guaranteeing that every model consistent with the noisy data and prescribed noise bounds is included. However, this approach often results in conservative reachable sets for long horizons. This conservatism can be partially mitigated if there is additional side information available [29]. A key approach to providing infinite horizon safety guarantees is through the use of barrier certificates.

In this paper, we build on the results in [27], [28] to compute a set of models for a linear control system and leverage barrier certificates as a discretization-free approach to provide safety guarantees over an infinite horizon for this given set of models. We use sum-of-squares (SOS) optimization to search for these certificates. To tackle the presence of a set of models, we start by formulating a computationally heavy condition for safety directly from the computed model parameters. Normally, the transition function is a function of the state, input, and noise parameters in some compact set. In the condition we formulate, the transition function is additionally a function of the model parameters that are also in some compact set. This dramatically increases the total number of parameters we need to keep track of, particularly when the barrier certificate is applied over the transition function. The larger memory usage makes it harder to run the optimization problem successfully. Thus, we address this computational challenge of the given condition by stating an equivalent condition that exploits the matrix zonotope representation of the models of the system and scales relatively well with the dimension of the system. We substantiate the benefit of the latter condition by implementing both conditions and investigating their performance for systems with different dimensions. As the models of the system can be made to be less conservative using available side information, our approach can also be integrated with the enhanced model parameters. Moreover, as the computation of matrix zonotope over-approximation of system model parameters has been generalized for polynomial nonlinear control systems, our approach seems promising to be adopted for such systems with appropriate updates. The codes to recreate our findings are publicly available. [1]

The remainder of the paper is organized as follows. Section II introduces preliminaries, notation, and problem formulation used in the paper. Section III covers our approach of safety verification via barrier certificates for the data-driven system models while section IV highlights a computation method of finding the barrier certificates via SOS programming. Section V illustrates numerical simulations. Finally, Section VI offers conclusive remarks.

II. Preliminaries and Problem Formulation

We start with the notations used in the paper, followed by the preliminaries and problem formulations.

A. Notations

The set of natural numbers, nonnegative integers, positive reals, the real n-dimensional space, and the space of real $n \times m$ matrices are denoted by $\mathbb{N}$, $\mathbb{Z}_{\geq 0}$, $\mathbb{R}_{>0}$, $\mathbb{R}^n$, and $\mathbb{R}^{n \times m}$, respectively. For a matrix A, $(A)_j$ denotes its jth column, $A^\top$ represents its transpose, and $A^\dagger$ its Moore-Penrose pseudoinverse. The operator $\operatorname{diag}(\cdot)$ constructs a diagonal matrix from its arguments. The vectors $\mathbb{1}_n$ and $\mathbb{0}_n$ are the n-dimensional vectors with all entries equal to 1 and 0, respectively. We use $\mathbb{1}$ and $\mathbb{0}$ to represent matrices of appropriate dimensions with all entries equal to 1 and 0, respectively. If a system, denoted by $\mathcal{S}$, satisfies a property Ψ, it is written as $\mathcal{S} \models \Psi$. Given a variable x that can have values in the range from x_{min} to x_{max}, we use $[x_{min}, x_{max}]$ to represent the interval.

B. Set representation

In this work, we utilize zonotopes as a mathematical representation of sets defined as follows.

Definition 1 (Zonotope [30]): Given a center $c_{\mathcal{Z}} \in \mathbb{R}^n$ and a number $\gamma_{\mathcal{Z}} \in \mathbb{N}$ of generator vectors $g_{\mathcal{Z}_i} \in \mathbb{R}^n$, a zonotope is defined as

$$\mathcal{Z} = \Big\{ x \in \mathbb{R}^n \Big| x = c_{\mathcal{Z}} + \sum_{i=1}^{\gamma_{\mathcal{Z}}} \beta_i \, g_{\mathcal{Z}_i}, -1 \leq \beta_i \leq 1 \Big\}.$$

We use the short notation $\mathcal{Z} = \langle c_{\mathcal{Z}}, G_{\mathcal{Z}} \rangle$ to denote a zonotope, where $G_{\mathcal{Z}} = [g_{\mathcal{Z}_1} \dots g_{\mathcal{Z}_{\gamma_{\mathcal{Z}}}}] \in \mathbb{R}^{n \times \gamma_{\mathcal{Z}}}$.

Given $L \in \mathbb{R}^{m \times n}$, the linear transformation of a zonotope $\mathcal{Z}$ is a zonotope $L\mathcal{Z} = \langle L c_{\mathcal{Z}}, L G_{\mathcal{Z}} \rangle$. Given two zonotopes $\mathcal{Z}_1 = \langle c_{\mathcal{Z}_1}, G_{\mathcal{Z}_1} \rangle \subset \mathbb{R}^n$ and $\mathcal{Z}_2 = \langle c_{\mathcal{Z}_2}, G_{\mathcal{Z}_2} \rangle \subset \mathbb{R}^n$, the Minkowski sum and the Cartesian product are respectively computed as [31]:

$$\begin{aligned} \mathcal{Z}_1 \oplus \mathcal{Z}_2 &= \Big\langle c_{\mathcal{Z}_1} + c_{\mathcal{Z}_1}, [G_{\mathcal{Z}_1} \ G_{\mathcal{Z}_2}] \Big\rangle, \\ \mathcal{Z}_1 \times \mathcal{Z}_2 &= \left\langle \begin{bmatrix} c_{\mathcal{Z}_1} \\ c_{\mathcal{Z}_2} \end{bmatrix}, \begin{bmatrix} G_{\mathcal{Z}_1} & \mathbb{0} \\ \mathbb{0} & G_{\mathcal{Z}_2} \end{bmatrix} \right\rangle. \end{aligned}$$

A matrix zonotope is represented as $\mathcal{M} = \langle C_{\mathcal{M}}, G_{\mathcal{M}} \rangle$, and its definition is analogous to that of a zonotope. It is characterized by a center matrix $C_{\mathcal{M}} \in \mathbb{R}^{n \times m}$ and $\gamma_{\mathcal{M}} \in \mathbb{N}$ generator matrices $G_{\mathcal{M}} = \begin{bmatrix} G_{\mathcal{M}_1} & \cdots & G_{\mathcal{M}_{\gamma_{\mathcal{M}}}} \end{bmatrix} \in \mathbb{R}^{n \times (m \gamma_{\mathcal{M}})}$ [1, p. 52].

Given a matrix zonotope $\mathcal{M}$, one can convert it to an interval matrix $\mathcal{M}_{int} = [M^{min}, M^{max}]$ where M^{min} and M^{max} are matrices and for $Z \in \mathcal{M}$, each component

[1] [Online]. Available: https://github.com/maoumer/Data-Driven-Safety-Verification-using-Barrier-Certificates-and-Matrix-Zonotopes

satisfies $M_{i,j}^{min} \leq Z_{i,j} \leq M_{i,j}^{max}$. This inequality can then be represented as a vector of polynomial inequalities over all elements of the matrix given by:

$$\begin{bmatrix} Z_{i,j} - M_{i,j}^{min} \\ M_{i,j}^{max} - Z_{i,j} \end{bmatrix} \geq 0. \tag{1}$$

Note the comma to distinguish these interval matrices from the concatenation of matrices. A similar argument applies to zonotopes.

C. System Dynamics

We consider an unknown discrete-time linear system $\mathcal{S}$ as follows:

$$x_{k+1} = A_{\text{tr}} x_k + B_{\text{tr}} u_k + w_k, \tag{2}$$

where $A_{\text{tr}} \in \mathbb{R}^{n_x \times n_x}$ and $B_{\text{tr}} \in \mathbb{R}^{n_x \times n_u}$ are unknown true system dynamics matrices, $x_k \in \mathcal{Z}_x = \langle c_{\mathcal{Z}_x}, G_{\mathcal{Z}_x} \rangle \subseteq \mathbb{R}^{n_x}$ and $u_k \in \mathcal{Z}_u = \langle c_{\mathcal{Z}_u}, G_{\mathcal{Z}_u} \rangle \subseteq \mathbb{R}^{n_u}$ are respectively the state and the input of the system at time $k \in \mathbb{Z}_{\geq 0}$, and w_k denotes the noise. Here, $\mathcal{Z}_x$ and $\mathcal{Z}_u$ represent the time-invariant domains of states and inputs, respectively, corresponding to inherent constraints of the problem and possibly driven by physical limitations.

D. Reachability Analysis

Reachability analysis computes the set of states x_k, which can be reached given a set of uncertain initial states $\mathcal{X}_0$ and a set of uncertain inputs $\mathcal{U}_k$. More formally, it can be defined as follows.

Definition 2 (Exact Reachable Set): The exact reachable set $\mathcal{R}_N$ after N time steps subject to inputs $u_k \in \mathcal{U}_k$, $\forall k \in \{0, \dots, N-1\}$, and noise $w(\cdot) \in \mathcal{Z}_w$, is the set of all states trajectories starting from initial set $\mathcal{X}_0$ after N steps:

$$\begin{aligned} \mathcal{R}_N = \big\{ x(N) \in \mathbb{R}^{n_x} \, \big| & x_{k+1} = A x_k + B u_k + w_k, \\ & x_0 \in \mathcal{X}_0, u_k \in \mathcal{U}_k, w_k \in \mathcal{Z}_w : \\ & \forall k \in \{0, ..., N{-}1\} \big\}. \end{aligned} \tag{3}$$

E. Barrier Certificate

A barrier certificate is a real-valued function defined over the system's state space, where its zero level set serves to separate the unsafe region $\mathcal{X}_u$ from all potential trajectories originating from a specified set of initial states $\mathcal{X}_0$.

Definition 3 (Barrier Certificate [2]): Consider a system as in (2). A function $\mathcal{B} : \mathcal{Z}_x \to \mathbb{R}$ is a barrier certificate for a system $\mathcal{S}$ if:

$$\mathcal{B}(x_k) \leq 0 \quad \forall x_k \in \mathcal{X}_0, \tag{4}$$

$$\mathcal{B}(x_k) > 0 \quad \forall x_k \in \mathcal{X}_u, \text{ and} \tag{5}$$

$$\begin{aligned} \mathcal{B}(A x_k + B u_k + w_k) \leq \mathcal{B}(x_k) \quad & \forall x_k \in \mathcal{Z}_x \backslash \mathcal{X}_u, \\ & \forall u_k \in \mathcal{Z}_u, \forall w_k \in \mathcal{Z}_w. \end{aligned} \tag{6}$$

Note that the above definition implies that the barrier certificate $\mathcal{B}(x_k)$ is a non-increasing function with respect to the state sequence of the system.

F. Problem formulation

Given a set of initial states $\mathcal{X}_0 \subset \mathcal{Z}_x$, a set of unsafe states $\mathcal{X}_u \subset \mathcal{Z}_x$, we aim to guarantee that all trajectories of $\mathcal{S}$ that start from $\mathcal{X}_0$ never reach $\mathcal{X}_u$ by employing only the input and noisy state data of the system $\mathcal{S}$ in (2) and without explicit knowledge of the system matrices. We denote this safety property by Ψ, and its satisfaction by $\mathcal{S}$ is written as $\mathcal{S} \models \Psi$.

We have access to past n_T input-state trajectories of different lengths, denoted by $T_i + 1$, for $i = 1, \dots, n_T$. These trajectories are denoted as $\{u_k\}_{k=0}^{T_i}$ and $\{x_k\}_{k=0}^{T_i}$. For notational simplicity, in the theoretical formulation, we consider a single trajectory ($n_T = 1$) of adequate length T and collect all the input and noisy state data into the following matrices:

$$\begin{aligned} X_+ &= \begin{bmatrix} x_1 & x_2 & \cdots & x_T \end{bmatrix}, \\ X_- &= \begin{bmatrix} x_0 & x_1 & \cdots & x_{T-1} \end{bmatrix}, \\ U_- &= \begin{bmatrix} u_0 & u_1 & \cdots & u_{T-1} \end{bmatrix}. \end{aligned}$$

We define $D_- = \begin{bmatrix} X_-^\top & U_-^\top \end{bmatrix}^\top$ and denote all available past data by $D = \begin{bmatrix} X_+^\top & X_-^\top & U_-^\top \end{bmatrix}^\top$. We consider the following standing assumption necessary for our data-driven approach.

Assumption 1: The noise w_k is bounded by a known zonotope, i.e., $w_k \in \mathcal{Z}_w = \langle c_{\mathcal{Z}_w}, G_{\mathcal{Z}_w} \rangle \; \forall \, k \in \mathbb{Z}_{\geq 0}$, which includes the origin.

Assumption 2: We assume that the data matrix D_- has full row rank, i.e., $\text{rank}(D_-) = n_x + n_u$.

We represent the sequence of unknown noise corresponding to the available input-state trajectories as $\{w_k\}_{k=0}^{T}$. From Assumption 1, it follows that

$$W_- = \begin{bmatrix} w_0 & \cdots & w_{T-1} \end{bmatrix} \in \mathcal{M}_w = \langle C_{\mathcal{M}_w}, G_{\mathcal{M}_w} \rangle,$$

where $C_{\mathcal{M}_w} \in \mathbb{R}^{n_x \times n_T}$ and $G_{\mathcal{M}_w} \in \mathbb{R}^{n_x \times \gamma_{\mathcal{Z}} n_T}$. Here, $\mathcal{M}_w$ denotes the matrix zonotope resulting from the concatenation of multiple noise zonotopes $\mathcal{Z}_w$ [28].

III. Data-Driven Safety Verification

This section describes a data-driven safety verification process for an unknown linear system in (2) subject to noise. Barrier certificates [2] use a model of the system to verify safety per condition (6). Due to the presence of noise in the data, no single model can be trusted or made to fit the data precisely to use for the search of a barrier certificate. Instead, we compute a set of models that are consistent with the observed data. Importantly, this set of models is guaranteed to include the true system model, as shown in [28], and it is represented using a matrix zonotope. The following lemma provides a systematic approach to compute this set of models. As we will show later, one can search for barrier certificates for this set of models methodically.

Lemma 1 ([28, Lemma 1]): Given the input-state trajectories D of the unknown system (2), the matrix zonotope

$$\mathcal{M}_\Sigma = (X_+ \oplus -\mathcal{M}_w) D_-^\dagger, \tag{7}$$

with $D_- = \begin{bmatrix} X_-^\top & U_-^\top \end{bmatrix}^\top$, contains all system dynamics matrices $\begin{bmatrix} A & B \end{bmatrix}$ that are consistent with the data D and the noise bound $\mathcal{M}_w$.

We compute the reachable regions by propagating the initial set $\mathcal{X}_0$ using the set of models $\mathcal{M}_\Sigma$ as presented in the following theorem.

Theorem 1 ([28, Theorem 1]): Given input-state trajectories D of the system in (2), then the reachable set

$$\hat{\mathcal{R}}_{k+1} = \mathcal{M}_\Sigma(\hat{\mathcal{R}}_k \times \mathcal{U}_k) + \mathcal{Z}_w$$

over-approximates the exact reachable set, i.e., $\hat{\mathcal{R}}_k \supseteq \mathcal{R}_k$ starting from $\hat{\mathcal{R}}_0 = \mathcal{X}_0$.

By converting $\mathcal{M}_\Sigma$ into an interval matrix, we can extract the minimum and maximum possible values of A and B, denoted by $A^{min}, A^{max}, B^{min}$ and B^{max}, respectively (that is, $[A^{min}\ B^{min}] = M_\Sigma^{min}$ and $[A^{max}\ B^{max}] = M_\Sigma^{max}$). Note that the unknown true model parameters can be bounded as $A^{min} \le A_{\text{tr}} \le A^{max}$ and $B^{min} \le B_{\text{tr}} \le B^{max}$, where the inequalities are element-wise. Following the above, as A_{tr} and B_{tr} are unknown, condition (6) can be restated using the interval matrix conversion of $\mathcal{M}_\Sigma$ as:

$$\begin{aligned} \mathcal{B}(Ax_k + Bu_k + w_k) \le \mathcal{B}(x_k) \quad \forall x_k \in \mathcal{Z}_x \backslash \mathcal{X}_u, \forall u_k \in \mathcal{Z}_u, \\ \forall w_k \in \mathcal{Z}_w, \forall A \in [A^{min}, A^{max}], \forall B \in [B^{min}, B^{max}]. \end{aligned} \tag{8}$$

While condition (8) is a robust condition for safety verification, using it to find a barrier certificate becomes intractable, particularly as the dimension of the system increases due to the large number of unknown parameters. To address this issue, we use $\mathcal{M}_\Sigma$ as follows. $\mathcal{M}_\Sigma = \langle C_{\mathcal{M}_\Sigma}, G_{\mathcal{M}_\Sigma} \rangle = \langle C_{\mathcal{M}_\Sigma}, \mathbb{0} \rangle \oplus \langle \mathbb{0}, G_{\mathcal{M}_\Sigma} \rangle$. We denote $[A_c\ B_c] = C_{\mathcal{M}_\Sigma}$ and $[A_G\ B_G] \in \langle \mathbb{0}, G_{\mathcal{M}_\Sigma} \rangle$. The unknown system dynamics $Ax_k + Bu_k + w_k$ can then be written as $A_c x_k + B_c u_k + (A_G x_k + B_G u_k + w_k)$ where $(A_G x_k + B_G u_k + w_k) \in \mathcal{Z}_d = (\langle \mathbb{0}, G_{\mathcal{M}_\Sigma} \rangle)(\mathcal{Z}_x \times \mathcal{Z}_u) + \mathcal{Z}_w$. Based on this setup, we provide the following definition for the safety verification of the system using the data-driven bounds provided above.

Definition 4: Consider a system as in (2). A function $\mathcal{B} : \mathcal{Z}_x \to \mathbb{R}$ is a barrier certificate for this system if:

$$\mathcal{B}(x_k) \le 0 \quad \forall x_k \in \mathcal{X}_0, \tag{9}$$

$$\mathcal{B}(x_k) > 0 \quad \forall x_k \in \mathcal{X}_u, \text{ and} \tag{10}$$

$$\begin{aligned} \mathcal{B}(A_c x_k + B_c u_k + d_k) \le \mathcal{B}(x_k) \quad \forall x_k \in \mathcal{Z}_x \backslash \mathcal{X}_u, \\ \forall u_k \in \mathcal{Z}_u, \forall d_k \in \mathcal{Z}_d. \end{aligned} \tag{11}$$

We now state the usefulness of Definition 4.

Theorem 2: Consider a system $\mathcal{S}$ as in (2). If there exists a function $\mathcal{B} : \mathcal{Z}_x \to \mathbb{R}$ for system $\mathcal{S}$ as in Definition 4, then the system is safe.

Proof: The proof follows from Definition 3. Conditions (4) and (5) are directly adopted. For condition (6), $A_c x_k + B_c u_k$ captures the nominal trajectory estimated by the matrix zonotope over-approximation, and d_k captures the "noise" from the over-approximation. The term $A_c x_k + B_c u_k + d_k$ thus captures all possible trajectories generated from the matrix zonotope $\mathcal{M}_\Sigma$ starting from state x_k under input u_k. Thus, condition (11) replaces condition (6) where the true trajectory $Ax_k + Bu_k + w_k$ is captured in $A_c x_k + B_c u_k + d_k$. ■

The next section covers a computational method to find barrier certificates that satisfy conditions (9)-(11) for the data-driven set of models.

IV. Computation of Safety Certificates

This section presents sum-of-squares (SOS) programming as a computational method of searching for barrier certificates for safety verification of our data-driven over-estimated system. To find barrier certificates, we first fix the template to be a linear combination of user-defined basis functions:

$$\mathcal{B}(x) = \mathbf{c}^T \mathbf{p}(x) = \sum_{i=1}^{n} c_i p_i(x),$$

where functions p_i are monomials over the state variable x, and $c_1, \dots, c_n$ are the real coefficients.

The system dynamics (2) is linear. We say a set $Q \subseteq \mathbb{R}^n$ is semi-algebraic if it can be defined with the help of a vector of polynomial inequalities $h(x)$ as $Q = \{x \mid h(x) \ge 0\}$, where the inequalities are element-wise. When the initial set $\mathcal{X}_0$ and unsafe set $\mathcal{X}_u$ are semi-algebraic [32], conditions (9)-(11) can be cast as a collection of SOS constraints in order to compute a polynomial barrier certificate of a predefined degree. We note that (matrix) zonotopes are semi-algebraic sets. As the conversion of (matrix) zonotopes to their half-space representation can be exponential in the number of generators [33], we instead convert them to interval matrices as they are scalable and computationally convenient due to their ease of representation as polynomial inequalities.

Assumption 3: The state set $\mathcal{Z}_x$ is a subset of $\mathbb{R}^n$, and the system dynamics (2) is a linear function of the state x and input u. Furthermore, sets $\mathcal{Z}_x$, $\mathcal{X}_0$, $\mathcal{X}_u$, $\mathcal{Z}_u$ and $\mathcal{Z}_d$ are zonotopes and their interval matrix representations can be described as vectors of polynomial inequalities: $\mathcal{Z}_{x,int} = \{x \in \mathbb{R}^n \mid g(x) \ge 0\}$, $\mathcal{X}_{0,int} = \{x \in \mathbb{R}^n \mid g_0(x) \ge 0\}$, $\mathcal{X}_{u,int} = \{x \in \mathbb{R}^n \mid g_u(x) \ge 0\}$, $\mathcal{Z}_{u,int} = \{u \in \mathbb{R}^n \mid g_{in}(u) \ge 0\}$, and $\mathcal{Z}_{d,int} = \{d \in \mathbb{R}^n \mid g_d(d) \ge 0\}$, where $g(\cdot), g_0(\cdot), g_u(\cdot), g_{in}(\cdot)$, and $g_d(\cdot)$ are each a vector of polynomials of the form in (1) and the inequalities are element-wise.

Under Assumption 3, conditions (9)-(11) can be formulated as a set of SOS constraints, as follows.

Lemma 2: Consider a system given by equation (2). Suppose Assumption 3 holds for this system and there exist constants $\epsilon \in \mathbb{R}_{>0}$, polynomial $\mathcal{B}(x)$ and SOS polynomials $\lambda_0(x)$, $\lambda_u(x)$, $\lambda(x)$ of appropriate dimensions such that:

$$-\mathcal{B}(x) - \lambda_0^T(x) g_0(x), \tag{12}$$

$$\mathcal{B}(x) - \epsilon - \lambda_u^T(x) g_u(x), \tag{13}$$

$$\mathcal{B}(x) - \mathcal{B}(A_c x + B_c u + d) - \lambda^T(x,u,d) g(x,u,d), \tag{14}$$

are SOS polynomials where x is the state variable over $\mathcal{Z}_{x,int}$, u is the input variable over $\mathcal{Z}_{u,int}$, d is the "noise" variable over $\mathcal{Z}_{d,int}$ and A_c, B_c are the data-driven nominal model parameters of the system. Here, $g(x,u,d)$ is the

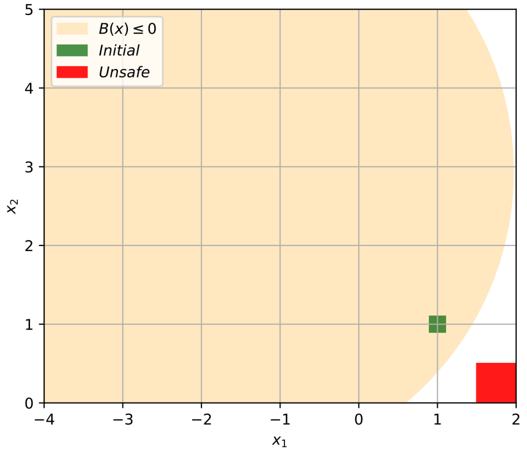

Fig. 1: Barrier Certificate for a 2D System.

concatenation of $g(x), g_{in}(u)$, and $g_d(d)$. Then the function $\mathcal{B}(x)$ is a barrier certificate following Definition 4. Note that ϵ is introduced in condition (13) to convert the strict inequality in condition (10) to an inclusive inequality.

In the next section, we demonstrate the application of our proposed approach over a case study.

V. Numerical simulations

In this section, we demonstrate the application of our approach in a case study. The simulations were conducted on a Windows 11 device equipped with an AMD Ryzen 9 4900HS Mobile Processor and 16 GB of RAM. We used CORA v2020 [34] in MATLAB for the matrix zonotope related computations and transferred the resulting model data to Julia where we used TSSOS [35] to implement the SOS optimization problem. We first obtain $\mathcal{M}_\Sigma$ and attempt to search for a barrier certificate using conditions (9), (10), and (8). For state $x \in \mathbb{R}^{n_x}, u \in \mathbb{R}^{n_u}$, the total number of parameters according to these conditions is $n_x \times n_x + n_x + n_x \times n_u + n_u + n_x = n_x^2 + n_x n_u + 2n_x + n_u$. This does not scale favorably with respect to the state dimension n_x and input dimension n_u. With each additional degree of the polynomial template for the barrier certificate, the memory needed scales exponentially over these parameters. Thus, it was not computationally tractable for our case study beyond a two dimensional system. Note that condition (14) in Lemma 2 is replaced with

$$\mathcal{B}(x) - \mathcal{B}(Ax + Bu + w) \\ - \lambda^T(x, u, w, B, A) g(x, u, w, B, A),$$

to incorporate the semi-algebraic set expressions for w, A and B for the optimization process based on condition (8). Figure 1 shows the resulting sublevel set of the barrier certificate for a two dimensional system along with the designated initial and unsafe states. Table I displays the true dynamics used for simulation (data collection) as well as the relevant vectors and matrices used for the SOS optimization.

We now present our results for a five dimensional system following Definition 4 and using Lemma 2. We were able to find a degree five polynomial barrier certificate. Two examples of the projection of the certificate over two states of the system are shown in Figure 2. Table II displays the true dynamics used for simulation as well as the relevant vectors and matrices used for the SOS optimization.

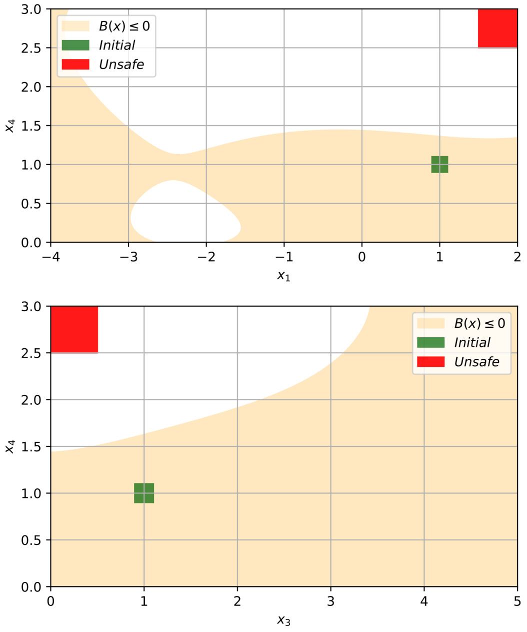

Fig. 2: Barrier Certificate Projections for a 5D System.

VI. Conclusion

This work presents a data-driven framework for safety verification of cyber-physical systems, addressing challenges posed by model uncertainty, noise, and environmental disturbances. By leveraging matrix zonotopes to construct a set of possible system models, our approach ensures that all dynamics consistent with the observed data are accounted for, providing a robust alternative to traditional model-based methods. The integration of this representation with barrier certificates enables rigorous safety guarantees without requiring explicit knowledge of the system model. Numerical experiments validate the effectiveness of our method in verifying safety for dynamical systems with unknown models. We plan to adopt our method for enhanced model parameters and generalize it for polynomial nonlinear control systems. Furthermore, we intend to investigate safe controller

TABLE I: Relevant Information for the 2D System

$\mathcal{Z}_{x,int}$	$[-4, 0]^T \leq x \leq [2, 5]^T$
$\mathcal{Z}_{u,int}$	$9.75 \leq u \leq 10.25$
$\mathcal{Z}_{w,int}$	$-0.005\mathbb{1}_2 \leq w \leq 0.005\mathbb{1}_2$
$\mathcal{X}_0$	$0.9\mathbb{1}_2 \leq x \leq 1.1\mathbb{1}_2$
$\mathcal{X}_u$	$[1.5, 0]^T \leq x \leq [2, 2.5]^T$
$[A^{min}\ B^{min}]$	$\begin{matrix} 0.928 & -0.194 & 0.0418 \\ 0.185 & 0.927 & 0.0514 \end{matrix}$
$[A^{max}\ B^{max}]$	$\begin{matrix} 0.935 & -0.184 & 0.0452 \\ 0.192 & 0.937 & 0.0549 \end{matrix}$
$[A_{\text{tr}}\ B_{\text{tr}}]$	$\begin{matrix} 0.932 & -0.189 & 0.0436 \\ 0.189 & 0.932 & 0.0533 \end{matrix}$

TABLE II: Relevant Information for the 5D System

$\mathcal{Z}_x^{min}$	$[-4, 0, 0, 0, 0]^T$
$\mathcal{Z}_x^{max}$	$[2, 5, 5, 3, 6]^T$
$\mathcal{Z}_{u,int}$	$9.75 \leq u \leq 10.25$
$\mathcal{Z}_{d,int}$	$-2.173\mathbb{1}_5 \leq u \leq 2.173\mathbb{1}_5$
$\mathcal{X}_0$	$0.9\mathbb{1}_5 \leq x \leq 1.1\mathbb{1}_5$
$\mathcal{X}_u^{min}$	$[1.5, 0, 0, 2.5, 0]^T$
$\mathcal{X}_u^{max}$	$[2, 0.5, 0.5, 3, 0.5]^T$
A^{min}	$\begin{matrix} 0.921 & -0.20 & -0.193 & -0.168 & -0.0877 \\ 0.178 & 0.922 & -0.193 & -0.168 & -0.0877 \\ -0.011 & -0.0106 & 0.667 & -0.125 & -0.0877 \\ -0.011 & -0.0106 & -0.236 & 0.692 & -0.0877 \\ -0.011 & -0.0106 & -0.193 & -0.168 & 0.817 \end{matrix}$
B^{min}	$[0.0357, 0.0454, 0.0397, 0.0374, 0.0397]^T$
A^{max}	$\begin{matrix} 0.941 & -0.177 & 0.171 & 0.18 & 0.0989 \\ 0.198 & 0.944 & 0.171 & 0.18 & 0.0989 \\ 0.0086 & 0.0118 & 1.031 & 0.223 & 0.0989 \\ 0.0086 & 0.0118 & 0.128 & 1.04 & 0.0989 \\ 0.0086 & 0.0118 & 0.171 & 0.18 & 1.004 \end{matrix}$
B^{max}	$[0.0516, 0.0612, 0.0555, 0.0532, 0.0555]^T$
A_c	$\begin{matrix} 0.931 & -0.188 & -0.0109 & 0.00579 & 0.00557 \\ 0.188 & 0.933 & -0.0109 & 0.0058 & 0.0056 \\ -0.0012 & 0.00061 & 0.849 & 0.0488 & 0.00557 \\ -0.0012 & 0.00061 & -0.0539 & 0.865 & 0.00557 \\ -0.0012 & 0.00061 & -0.0109 & 0.00579 & 0.91 \end{matrix}$
B_c	$[0.0437, 0.0533, 0.0476, 0.0453, 0.0476]^T$
A_{tr}	$\begin{matrix} 0.1890 & 0.9323 & 0 & 0 & 0 \\ 0 & 0 & 0.8596 & 0.0430 & 0 \\ 0 & 0 & -0.0430 & 0.8596 & 0 \\ 0 & 0 & 0 & 0 & 0.9048 \end{matrix}$
B_{tr}	$[0.0436, 0.0533, 0.0475, 0.0453, 0.0476]^T$

synthesis for a given set of models using barrier certificates by building upon this work.

REFERENCES

[1] M. Althoff, "Reachability Analysis and its Application to the Safety Assessment of Autonomous Cars," Ph.D. dissertation, Technische Universität München, 2010.

[2] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *International Workshop on Hybrid Systems: Computation and Control*, 2004, pp. 477–492.

[3] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *18th European Control Conference*, 2019, pp. 3420–3431.

[4] P. Jagtap, S. Soudjani, and M. Zamani, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Transactions on Automatic Control*, vol. 66, no. 7, pp. 3097–3110, 2020.

[5] L. Wang, D. Han, and M. Egerstedt, "Permissive barrier certificates for safe stabilization using sum-of-squares," in *Annual American control conference*. IEEE, 2018, pp. 585–590.

[6] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[7] ——, "Stochastic safety verification using barrier certificates," in *IEEE conference on decision and control*, vol. 1, 2004, pp. 929–934.

[8] M. Bajelani and K. van Heusden, "Data-driven input-output control barrier functions," *arXiv preprint arXiv:2502.17688*, 2025.

[9] A. Salamati and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach," in *Learning for Dynamics and Control Conference*, 2022, pp. 441–452.

[10] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven verification and synthesis of stochastic systems via barrier certificates," *Automatica*, vol. 159, p. 111323, 2024.

[11] O. Schön, Z. Zhong, and S. Soudjani, "Data-driven distributionally robust safety verification using barrier certificates and conditional mean embeddings," in *American Control Conference*. IEEE, 2024, pp. 3417–3423.

[12] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical programming*, vol. 96, pp. 293–320, 2003.

[13] A. Devonport and M. Arcak, "Data-driven reachable set computation using adaptive gaussian process classification and monte carlo methods," in *American Control Conference*. IEEE, 2020, pp. 2629–2634.

[14] S. Haesaert, A. Abate, and P. M. Van den Hof, "Data-driven and model-based verification: A bayesian identification approach," in *4th Conference on Decision and Control*. IEEE, 2015, pp. 6830–6835.

[15] A. Chakrabarty, A. Raghunathan, S. Di Cairano, and C. Danielson, "Data-driven estimation of backward reachable and invariant sets for unmodeled systems via active learning," in *Conference on Decision and Control*. IEEE, 2018, pp. 372–377.

[16] A. Chakrabarty, C. Danielson, S. Di Cairano, and A. Raghunathan, "Active Learning for Estimating Reachable Sets for Systems With Unknown Dynamics," *IEEE Transactions on Cybernetics*, pp. 1–12, 2020.

[17] A. Devonport, F. Yang, L. El Ghaoui, and M. Arcak, "Data-driven reachability analysis with christoffel functions," in *60th Conference on Decision and Control*. IEEE, 2021, pp. 5067–5072.

[18] N. Hashemi, X. Qin, L. Lindemann, and J. V. Deshmukh, "Data-driven reachability analysis of stochastic dynamical systems with conformal inference," in *62nd Conference on Decision and Control*. IEEE, 2023, pp. 3102–3109.

[19] M. H. Sazlı, "A brief review of feed-forward neural networks," *Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering*, vol. 50, no. 01, 2006.

[20] V. Vovk, A. Gammerman, and G. Shafer, *Algorithmic learning in a random world*. Springer, 2005, vol. 29.

[21] J. Lei and L. Wasserman, "Distribution-free prediction bands for non-parametric regression," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 76, no. 1, pp. 71–96, 2014.

[22] P. Wu, S. Martinez, and J. Chen, "Fine-tuned convex approximations of probabilistic reachable sets under data-driven uncertainties," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 1319–1338, 2025.

[23] J. Choi, H. Park, and I. Hwang, "Bootstrapped gaussian mixture model-based data-driven forward stochastic reachability analysis," *IEEE Control Systems Letters*, vol. 8, pp. 1–6, 2024.

[24] F. Djeumou, A. P. Vinod, E. Goubault, S. Putot, and U. Topcu, "On-the-fly control of unknown systems: From side information to performance guarantees through reachability," *IEEE Transactions on Automatic Control*, vol. 68, no. 8, pp. 4857–4872, 2022.

[25] J. F. Fisac, A. K. Akametalu, M. N. Zeilinger, S. Kaynama, J. Gillula, and C. J. Tomlin, "A general safety framework for learning-based control in uncertain robotic systems," *IEEE Transactions on Automatic Control*, vol. 64, no. 7, pp. 2737–2752, 2019.

[26] M. Attar and W. Lucia, "Data-driven robust backward reachable sets for set-theoretic model predictive control," *IEEE Control Systems Letters*, vol. 7, pp. 2305–2310, 2023.

[27] A. Alanwar, A. Koch, F. Allgöwer, and K. H. Johansson, "Data-driven reachability analysis using matrix zonotopes," in *Learning for Dynamics and Control*, 2021, pp. 163–175.

[28] A. Alanwar, A. Koch, F. Allgower, and K. H. Johansson, "Data-driven reachability analysis from noisy data," *IEEE Transactions on Automatic Control*, vol. 68, no. 5, pp. 3054–3069, 2023.

[29] A. Alanwar, F. J. Jiang, M. Sharifi, D. V. Dimarogonas, and K. H. Johansson, "Enhancing data-driven reachability analysis using temporal logic side information," in *International Conference on Robotics and Automation*. IEEE, 2022, pp. 6793–6799.

[30] W. Kühn, "Rigorously computed orbits of dynamical systems without the wrapping effect," *Computing*, vol. 61, no. 1, pp. 47–67, 3 1998.

[31] M. Farjadnia, A. Fontan, A. Alanwar, M. Molinari, and K. H. Johansson, "Robust data-driven tube-based zonotopic predictive control with closed-loop guarantees," *arXiv preprint arXiv:2409.14366*, 2024.

[32] J. Bochnak, M. Coste, and M.-F. Roy, *Real algebraic geometry*. Springer Science & Business Media, 2013, vol. 36.

[33] M. Althoff, O. Stursberg, and M. Buss, "Computing reachable sets of hybrid systems using a combination of zonotopes and polytopes," *Nonlinear analysis: hybrid systems*, vol. 4, no. 2, pp. 233–249, 2010.

[34] M. Althoff, "An introduction to CORA 2015," in *Proc. of the 1st and 2nd Workshop on Applied Verification for Continuous and Hybrid Systems*, December 2015, pp. 120–151.

[35] J. Wang, V. Magron, and J.-B. Lasserre, "TSSOS: A moment-sos hierarchy that exploits term sparsity," *SIAM Journal on optimization*, vol. 31, no. 1, pp. 30–58, 2021.