Safety Assessment Based on Physically-Viable Data-Driven Models

Mohamadreza Ahmadi, Arie Israel, Ufuk Topcu

***Abstract*— We consider the problem of safety assessment of a dynamical system for which no model and just limited data on the states is available. That is, given samples of the state $\{x(t_i)\}_{i=1}^N$ at time instances $t_1 \leq t_2 \leq \cdots \leq t_N$ and some other side information in terms of the regularity of the state evolutions, we are interested in checking whether $x(T) \notin \mathcal{X}_u$, where $T > t_N$ and $\mathcal{X}_u \subset \mathbb{R}^n$ (the unsafe set) are pre-specified. To this end, we use piecewise-polynomial approximations of the trajectories based on the data along with the regularity side information to formulate a data-driven differential inclusion model. For these classes of data-driven differential inclusions, we propose a safety assessment theorem based on barrier certificates. The barrier certificates are then found using polynomial optimization. The method is illustrated by two examples.**

I. INTRODUCTION

Emerging control applications, in particular concerned with safety-critical systems, require system analysis and controller synthesis methods that are resilient to abrupt system changes. For instance, consider an unmanned aerial vehicle flying on a specified trajectory. Due to external conditions, such as a wind gust, severe damage is incurred to one of the wings [1]. The dynamics of the aircraft after the incident does not follow the equations of motions based on which the system was initially designed. Hence, to preclude further damage or *safe* landing, we require data-driven methods for system analysis and control synthesis.

Recent studies have shown that certain physical laws, in the form of differential equations, can be extracted from data [2]. In particular, [3] studied the problem of finding system dynamics when the system follows Lagrangian mechanics. Also, see [4] for a method that can extract chaotic polynomial differential equations from noisy data and relies on an ergodicity property of the data such that the central limit theorem can be applied. However, these methods often require large amounts of training data, which may not be available, especially, after an abrupt change in a safety-critical system.

In the control literature, system analysis based on input-output data or input-state data is not new. System identification techniques [5] have looked into the problem of finding a model of the system based on data. Yet, the available methods are either "data-hungry" or computationally expensive (especially if they require a validation stage). Adaptive control techniques [6] also studied controller synthesis methods for systems in which the system model is known up to a parametrization. Such parametrization of the system dynamics is not often available in the case of an abrupt system change.

Once an abrupt change in system dynamics occurs, one of the fundamental issues to consider is to assess whether the system behaves *safely* or whether the system avoids certain *unsafe* behavior. If the system model is given, verifying safety is a familiar subject to the control community [7], [8], [9]. One of the methods for safety verification relies on the construction of a function of the states, called the *barrier certificate* that satisfies a Lyapunov-like inequality [9]. The barrier certificates have shown to be useful in several system analysis and control problems running the gamut of bounding moment functionals of stochastic systems [10] to control of a swarm of silk moths [11]. To the authors' knowledge, the only article that applied barrier certificates for system analysis based on data is [12]. However, the latter method requires large amounts of data, as well.

In this paper, we study safety assessment of systems for which limited data (by *limited*, we imply N is not large enough for determining the complete dynamics using a system identification or machine learning method) is available. To this end, motivated by the recent works on Whitney's extension problem [13], we propose a data-driven differential inclusion model of the system based on the piecewise-polynomial approximation of the state data and some regularity information on the evolution of system state. Equipped with this data-driven model, we formulate a safety assessment theorem based on barrier certificates for differential inclusions. The barrier certificates are then computed using semi-definite programming (SDP). We illustrate the proposed method using two numerical examples.

The paper is organized as follows. The next section presents the notation and the some preliminary mathematical definitions. In Section III, we present the data-driven differential inclusion model, propose a method based on barrier certificates for safety assessment of differential inclusions and describe a computational approach for finding barrier certificates based on polynomial optimization. In Section IV, we illustrate the proposed method by two examples. Finally, Section V concludes the paper and provides directions for future research.

II. PRELIMINARIES

Notation: The notations employed in this paper are relatively straightforward. $\mathbb{R}_{\geq 0}$ denotes the set $[0, \infty)$. $\| \cdot \|$ denotes the Euclidean vector norm on $\mathbb{R}^n$ and $\langle \cdot \rangle$ the inner product. $\mathcal{R}[x]$ accounts for the set of polynomial functions

M. Ahmadi and U. Topcu are with the Department of Aerospace Engineering and Engineering Mechanics, and the Institute for Computational Engineering and Sciences (ICES), University of Texas, Austin, 201 E 24th St, Austin, TX 78712. A. Israel is with the Department of Mathematics, University of Texas, Austin, 2515 Speedway, Austin, TX 78712. e-mail: ({mrahmadi, arie, utopcu}@utexas.edu).

with real coefficients in $x \in \mathbb{R}^n$, $p : \mathbb{R}^n \to \mathbb{R}$ and $\Sigma \subset \mathcal{R}$ is the subset of polynomials with an SOS decomposition; i.e, $p \in \Sigma[x]$ if and only if there are $p_i \in \mathcal{R}[x],\ i \in \{1,\dots,k\}$ such that $p = p_i^2 + \cdots + p_k^2$. We denote by $\mathcal{C}^m(X)$, with $X \subseteq \mathbb{R}^n$, the space of m-times continuously differentiable functions and by $\partial^m = \frac{\partial^m}{\partial x^m}$ the derivatives up to order m. For $f \in \mathcal{C}^m(X)$, we denote by $\|f\|_{\mathcal{C}^m}$ the $\mathcal{C}^m$-norm given by

$$\|f\|_{\mathcal{C}^m} = \max_{\alpha \le m} \sup_{x \in X} |\partial^\alpha f(x)|.$$

For $f \in \mathcal{C}^m(X)$ and $x \in X$, we denote by $J_x(f)$ the mth degree Taylor polynomial of f at x

$$J_x(f)(x') = \sum_{\alpha \le m} \frac{\partial^\alpha f(x)(x'-x)^\alpha}{\alpha!}.$$

Note that $J_x(f) \in \mathcal{R}[x]$. Finally, for a finite set A, we denote by $co\{A\}$ the convex hull of the set A.

A. Whitney's Extension Problem

Whitney's extension problem is concerned with the question of whether, given data on a function f, i.e., $\{\partial^m f_i\}_{i=1}^N$ corresponding to $\{x_i\}_{i=1}^N$, one can find a $\mathcal{C}^m$ function that approximates f.

Whitney's classic problem can be described as follows. Suppose we are given an arbitrary subset $D \subset \mathbb{R}^n$ and a function $f : D \to \mathbb{R}$, how can we determine whether there exists a function $F \in \mathcal{C}^m(\mathbb{R}^n)$ such that $F = f$ on D.

Whitney indeed addressed this problem for the case $n = 1$.

Theorem 1 (Whitney's Extension Theorem [14]): : Let $E \subset \mathbb{R}^n$ be a closed set, and let $\{P_x\}_{x\in E}$ be a family of polynomials $P_x \in \mathcal{R}[x]$ indexed by the points of E. Then the following are equivalent

A. There exists $F \in \mathcal{C}^m(\mathbb{R}^n)$ such that $J_x(F) = P_x$ for each $x \in E$.
B. There exists a real number $M > 0$ such that

$$|\partial^\alpha P_x(x)| \le M \quad \text{for} \quad |\alpha| \le m,\ x \in E.$$

Recently Fefferman and collaborators [15], [16] considered a more general problem. That is, given $\{f_i = f(x_i)\}_{i=1}^N$ corresponding to $\{x_i\}_{i=1}^N$, the problem of computing a function $F \in \mathcal{C}^m(\mathbb{R}^n)$ and a real number $M \ge 0$ such that

$$\|F\|_{\mathcal{C}^m} \le M, \quad \text{and} \quad |F(x) - f(x)| \le M\sigma(x), \quad \forall x \in E.$$

The function $\sigma : \mathbb{R}^n \to \mathbb{R}_{\ge 0}$ is determined by the problem under study and from "observations".

Computing such a function F in the general form is a cumbersome task and amounts to computing sets containing F [17], [18]. In this paper, instead of considering general interpolants of data, we focus on piecewise-polynomial approximations for which construction algorithm are widely available [19].

B. Piecewise-Polynomial Approximation: B-Splines

B-spline functions [20] have properties that make them very suitable candidates for function approximation. They can be efficiently computed in closed form based on available algorithms [19]. They B-splines are widely employed in computer graphics, automated manufacturing (CAM), data fitting, computer graphics, and computer aided design (CAD) [21].

A pth degree B-spline curve, $f(t)$, defined by n control points and $m = n + p + 1$ knots $\hat{t}$, is given by

$$f(t) = \sum_{i=1}^{n} \beta_i Q_{i,p}(t) \tag{1}$$

Knot vectors are sets of non-decreasing real numbers. The spacing between knots defines the shape of the curve along with the control points.

Function $Q_{i,p}(t)$ is called ith B-spline basis function of order p and it can be described by the recursive equations

$$Q_{i,0}(t) = \begin{cases} 1 & t \in [\hat{t}_i, \hat{t}_{i+1}) \\ 0 & \text{else} \end{cases} \tag{2}$$

and

$$Q_{i,p}(t) = \frac{t - \hat{t}_i}{\hat{t}_{i+p} - \hat{t}_i} Q_{i,p-1}(t) + \frac{\hat{t}_{i+p+1} - t}{\hat{t}_{i+p+1} - \hat{t}_{i+1}} Q_{i+1,p-1}(t). \tag{3}$$

defined using the Cox-de Boor algorithm [19]. First order basis functions are evaluated using equation (2), followed by iterative evaluation of (3) until the desired order is reached. In contrast to Bézier curves, the number of control points of the curve, n, is independent of the order, p . This provides more robustness for the generated paths topology.

Furthermore, the derivative of a B-spline of degree p, $Q_{i,p}$, is simply a function of B-splines of degree $p - 1$. That is,

$$\frac{\mathrm{d}Q_{i,p}(t)}{\mathrm{d}t} = (p-1)\left(\frac{-Q_{i+1,p-1}}{t_{i+p} - t_{i+1}} + \frac{Q_{i,p-1}}{t_{i+p-1} - t_i}\right) \tag{4}$$

At this stage, we are ready to present the main results of this paper.

III. Main Results

A. Data-Driven Differential Inclusions

We are given $\{x(t_i)\}_{i=1}^N$, samples of the state at time instances $t_1 \le t_2 \le \cdots \le t_N$. That is, only samples of the states are available. This often the case in practical engineering applications. Denote by $X(t)$ the approximation of $x(t)$ based on the observations $\{x(t_i)\}_{i=1}^N$.

In this study, we consider state evolutions that belong to $\mathcal{C}^2(\mathbb{R}_{\ge 0})$. Hence, $\dot{x}(t) \in \mathcal{C}^1(\mathbb{R}_{\ge 0})$.

We assume in addition to state samples, some prior regularity knowledge (side information) on the state evolutions of the system are available in the form of

$$\|x\|_{\mathcal{C}^2} \le M,$$

for a constant $M > 0$. In order to account for the uncertainty in approximating $\dot{x}$ with the function $\dot{X}$, we introduce a function $\sigma : \mathbb{R}_{\ge 0} \to \mathbb{R}_{\ge 0}$ such that

$$|\dot{X}(t) - \dot{x}(t)| \le M\sigma(t).$$

In the case of piecewise-polynomial approximation of the data, we have $X(t) = \sum_i \beta_i Q_{i,p}(t)$ and $\dot{X}(t) = \sum_i \beta_i \dot{Q}_{i,p}(t)$ which can be determined using (4).

Let $\dot{X}_- = \dot{X}(t) - M\sigma(t)$ and $\dot{X}_+ = \dot{X}(t) + M\sigma(t)$. The dynamics of the system for $t > t_N$ can be described by the following data-driven differential inclusion

$$\begin{aligned} \dot{x}(t) &\in co\{\dot{X}_-(t), \dot{X}_+(t)\}, \\ x(t_N) &= x_N. \end{aligned} \tag{5}$$

Remark 1: Differential inclusion (5) in fact over-approximates the dynamics after $t > t_N$. Note that the information on the system state is only available for $0 < t < t_N$ and the regularity information (M and σ) provides the means using (5) to predict the behavior of system state.

We are interested in solving the following problem:

Problem 1: Consider the data-driven differential inclusion (5). Given $\mathcal{X}_u \subset \mathbb{R}^n$ and $T > t_N$, check whether $x(T) \notin \mathcal{X}_u$.

Next, we discuss differential inclusions in the form of (5) and we propose a safety assessment method based on barrier certificates.

B. Barrier Certificates for Differential Inclusions

Let $\{f_i(x,t)\}_{i=1}^m$, $f : \mathcal{X} \times \mathcal{T} \to \mathbb{R}^n$ with $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{T} \subseteq \mathbb{R}_{\geq 0}$ and f_i's be (piecewise) smooth functions. Define

$$\mathcal{F}(x,t) = co\{f_1(x,t), \ldots, f_m(x,t)\}.$$

Consider the following differential inclusion

$$\begin{aligned} \dot{x} &\in \mathcal{F}(x,t), \quad t \geq t_0 \\ x(t_0) &= x_0 \end{aligned} \tag{6}$$

Well-posedness conditions of differential inclusions [22, Theorem 1, p. 106] require $\mathcal{F}$ to be closed and convex. Since $\mathcal{F}$ is defined as the convex hull of a finite set, then it is closed and convex. Furthermore, $\mathcal{F}$ is upper hemi-continuous, because $\mathcal{F} = \sum_{i=1}^m \alpha_i f_i(x,t)$ with $0 \leq \alpha_i \leq 1$, $i = 1, 2, \ldots, m$ and $\sum_{i=1}^m \alpha_i = 1$ and f_i's being smooth functions. Furthermore, the mapping $\mathcal{F}(x,t)$ is one-sided Lipschitz, i.e., it satisfies

$$(x_1 - x_2)^T \left(\mathcal{F}(x_1,t) - \mathcal{F}(x_2,t)\right) \leq C\|x_1 - x_2\|^2, \quad \forall t > 0,$$

for some $C > 0$ and all x_1 and x_2, which follows from the fact that $\mathcal{F}$ is a convex hull of smooth and thus Lipschitz functions.

We are interested in the problem of verifying whether we can ensure that the trajectories of (6) avoid a specified unsafe set $\mathcal{X}_u \subset \mathbb{R}^n$ at some point in time $T > t_0$. In this respect, we first need to extend the concept of barrier certificates to differential inclusions.

Before stating the theorem, we require a definition of the derivative for set-valued maps. Denote by

$$D_+V(x)(u) = \liminf_{h \to 0^+,\ v \to u} \frac{V(x+hv) - V(x)}{h},$$

the upper contingent derivative of V at x in the direction u. In particular, when V is Gateux differentiable and $\mathcal{F} = \{v\}$ is a singleton, $D_+V(x)$ coincides with the gradient

$$D_+V(x)(v) = \langle \nabla V(x), v \rangle.$$

Theorem 2: Consider differential inclusion (6) and let $T > t_0$. If there exist a $B \in \mathcal{C}^1(\mathbb{R}^n; \mathbb{R}) \cap \mathcal{C}^1(\mathbb{R}_{\geq 0}; \mathbb{R})$ and a positive definite function $W : L^1(\mathbb{R}^n \times \mathbb{R}_{\geq 0}; \mathbb{R}_{\geq 0})$ such that

$$B\left(x(T), T\right) - B\left(x(t_0), t_0\right) > 0, \quad x(T) \in \mathcal{X}_u, \tag{7}$$

$$D_+B(x,t)(v,1) \leq -W(x,t), \quad t \in [t_0, T], \quad v \in \mathcal{F}(x,t), \tag{8}$$

then the solutions of (6) satisfy $x(T) \notin \mathcal{X}_u$.

Proof: The proof is carried out by contradiction. Assume it holds that $x(T) \in \mathcal{X}_u$. Then, (7) implies that

$$B\left(x(T), T\right) > B\left(x(t_0), t_0\right).$$

Furthermore, using [23, Proposition 8, p. 289] and inequality (8), we can infer that

$$B(x(s), s) - B(x(t_0), t_0) \leq -\int_{t_0}^{s} W(x, \tau)\ d\tau \leq 0.$$

That is,

$$B(x(s), s) \leq B(x(t_N), t_N).$$

Since s was chosen arbitrary, this is a contradiction. Thus, the solutions of (6) satisfy $x(T) \notin \mathcal{X}_u$. ∎

C. Safety Assessment for Data-Driven Differential Inclusions

In the following, we propose conditions for safety analysis of the data-driven differential inclusion (5). In other words, given the limited data over states up to some time t_N and the regularity information, we verify whether the system behaves safely at a given time $T > t_N$.

Corollary 1: Consider differential inclusion (5) and let $T > t_N$. If there exist a $B \in \mathcal{C}^1\left(\mathbb{R}^n; \mathbb{R}\right) \cap \mathcal{C}^1([t_N, \infty); \mathbb{R})$ and a positive definite function $W : L^1\left(\mathbb{R}^n \times [t_N, \infty); [t_N, \infty)\right)$ such that

$$B\left(x(T), T\right) - B\left(x(t_N), t_N\right) > 0, \quad x(T) \in \mathcal{X}_u, \tag{9}$$

$$D_+B(x,t)\left(\dot{X}_-, 1\right) \leq -W_-(x,t), \quad t \in [t_N, T], \tag{10}$$

$$D_+B(x,t)\left(\dot{X}_+, 1\right) \leq -W_+(x,t), \quad t \in [t_N, T], \tag{11}$$

then the solutions of (5) satisfy $x(T) \notin \mathcal{X}_u$.

Proof: Inequality (9) ensures that (7) holds. Multiplying both sides of inequality (10) a constant $0 \leq \alpha_- \leq 1$ and inequality (11) a constant $0 \leq \alpha_+ \leq 1$ such that $\alpha_- + \alpha_+ = 1$ and adding them, we obtain

$$\begin{aligned} \alpha_- D_+B(x,t)(\dot{X}_-, 1) &+ \alpha_+ D_+B(x,t)(\dot{X}_+, 1) \\ &\leq -\alpha_- W_-(x,t) - \alpha_+ W_+(x,t). \end{aligned}$$

Since D_+ is a linear operator, we have

$$\begin{aligned} D_+B(x,t)(\alpha_- \dot{X}_- &+ \alpha_+ \dot{X}_+, 1) \\ &\leq -\alpha_- W_-(x,t) - \alpha_+ W_+(x,t). \end{aligned}$$

Let $W(x,t) = \min\{W_-(x,t), W_+(x,t)\}$. We obtain

$$D_+B(x,t)(\alpha_-\dot{X}_- + \alpha_+\dot{X}_+, 1) \\ \leq -\alpha_- W_-(x,t) - \alpha_+ W_+(x,t) \\ \leq -(\alpha_- + \alpha_+)W(x,t) = -W(x,t).$$

That is,

$$D_+B(x,t)(v,1) \leq -W(x,t), \quad v \in co\{\dot{X}_-, \dot{X}_+\}.$$

Thus inequality (8) is also satisfied. This completes the proof. ■

D. Computational Method

In this section, we propose a computational method based on polynomial optimization. For dynamical systems approximated by piecewise-polynomials, we propose conditions based on sum-of-squares (SOS) programs.

Assuming $\sigma \in \Sigma[t]$, (5) becomes a differential inclusion with polynomial vector fields.

The next Lemma, which is based on the application of Putinar's Positivestellensatz, presents conditions in terms of polynomial positivity that can be efficiently checked via SDPs [24] (see Appendix A for more details). Parsers such as SOSTOOLs [25] can be used to cast the polynomial inequalities into semidefinite programs and then solvers such as Sedumi [26] can be used to solve the resultant SDPs.

Lemma 1: Consider the differential inclusion (5) and the following semi-algebraic unsafe set

$$\mathcal{X}_u = \{x \mid l_i(x) \leq 0,\ i = 1,2,...,n_c\}, \tag{12}$$

where $l_i \in \mathcal{R}[x]$. If there exist functions $B \in \mathcal{R}[x,t]$, $W_- \in \Sigma[x,t]$, $W_+ \in \Sigma[x,t]$, $m_i \in \Sigma[x,t]$, $i = 1,2$, $s_i \in \Sigma[x,t]$, $i = 1,\ldots,n_c$ and a positive constant $c > 0$, such that

$$B(x(T),T) - B(x(t_N),t_N) \\ + \sum_{i=1}^{n_c} s_i(x(T))\, l_i(x(T)) - c \in \Sigma[x(T)] \tag{13}$$

and

$$-\frac{\partial B}{\partial t} - \left\langle \frac{\partial B}{\partial x}, \dot{X}_- \right\rangle - W_-(x,t) \\ - m_1(x,t)(t-t_N)(t-T) \in \Sigma[x,t], \tag{14}$$

$$-\frac{\partial B}{\partial t} - \left\langle \frac{\partial B}{\partial x}, \dot{X}_+ \right\rangle - W_+(x,t) \\ - m_2(x,t)(t-t_N)(t-T) \in \Sigma[x,t], \tag{15}$$

then the solutions to (5) satisfy $x(T) \notin \mathcal{X}_u$.

Proof: Applying Putinar's Positivstellensatz, condition (13) implies that

$$B(x(T),T) - B(x(t_N),t_N) > 0,$$

for all $x(T) \in \mathcal{X}_u$ as in (12). Thus, inequality (9) holds. Moreover, given the smoothness property of B, we have

$$D_+B(x,t)\left(\dot{X}_-, 1\right) = \frac{\partial B}{\partial t} + \left\langle \frac{\partial B}{\partial x}, \dot{X}_- \right\rangle.$$

Hence, from condition (14), we have

$$D_+B(x,t)\left(\dot{X}_-, 1\right) \leq -W_-(x,t), \quad t \in [t_N, T].$$

Therefore, inequality (10) is satisfied. In a similar manner, we can show that (11) holds as well. Then, from Corollary 1, the solutions to (5) satisfy $x(T) \notin \mathcal{X}_u$. ■

IV. Numerical Results

In this section, we illustrate the proposed method using two examples. The first example is a single state system for which limited data is available and safety in a future time is of interest. The second example is the 2-state Van der Pol equation that exhibits a limit cycle.

A. Example I

We consider 20 samples of the solution to the following differential equation

$$\dot{x} = 0.5x^2 - 0.05x^3, \\ x(0) = 1, \tag{16}$$

in the interval $0 < t < 1.7$ (see Figure 1). The regularity information is given as $\|x\|_{\mathcal{C}^2} \leq 5$ and

$$|\dot{X}(t) - \dot{x}(t)| \leq 5,$$

which implies that $M = 5$ and $\sigma(t) = 1$. We use a cubic piecewise-polynomial approximation of $x(t)$. This can be carried out readily by the `spline` function in MATLAB.

The unsafe set in this example is given by

$$\mathcal{X}_u = \{x \in \mathbb{R} \mid x - 9 \geq 0\}.$$

The boundary of the unsafe set $x = 9$, the data points $\{x_i\}_{t=1}^{20}$ and the piecewise-polynomial approximation of the state $X(t) = \sum_i \beta_i Q_{i,p}(t)$ are shown in Figure 1. As it can be observed from the figure, since there exists an stable equilibrium at $x = 10$, the solution of the actual system converges to the equilibrium at $t \approx 3$. However, since the piecewise-polynomial approximation of the state is based on the information up to $t = 1.7$, $X(t)$ differs from $x(t)$ as time passes. Nonetheless, the data-driven differential inclusion (5) provides an approximation of the state evolutions for $t > 1.7$.

In this example, we are interested in finding the maximum T for which the solutions become unsafe, i.e., $x(T) \geq 9$. To this end, based on Corollary 1, we increase the value of T and look for a barrier certificate. We continue until no barrier certificate can be found.

Table I provides the numerical results. Notice that the actual system become unsafe at $T = 2.66$. However, due to system uncertainty and limited data, the lower bound on the unsafe set has been found to be $T = 2.49$ corresponding to certificates of degree 6. The barrier certificate of degree 3 is given bellow

$$B(x,t) = -0.496t^3 + 0.119t^2x + 0.0449t^2 - 0.0383tx^2 \\ -0.5855tx - 0.8398t + 0.1063x^2 + 1.389x.$$

TABLE I: Numerical results for 20 samples and $t_N = 2$.

deg	1	2	3	4	5	6
T	2.26	2.34	2.41	2.45	2.46	2.49

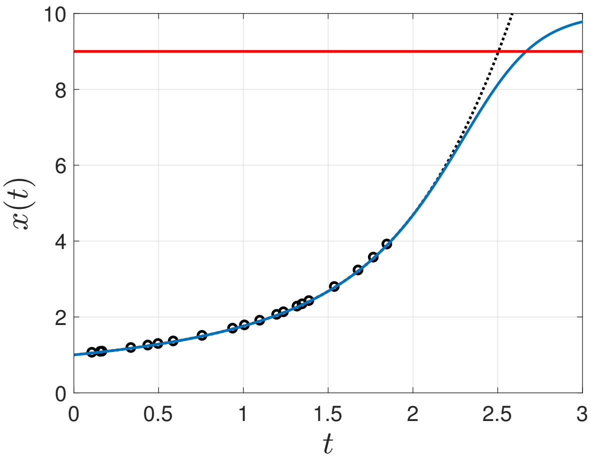

Fig. 1: The boundary of the unsafe set $x = 9$ (red line), the data points $\{x_i\}_{t=1}^{20}$ (black circles), the piecewise-polynomial approximation of the state $X(t)$ (black dots) and the actual solution of the system (solid blue).

B. Example II: Van der Pol Oscillator

We consider 40 samples of the states to the Van der Pol differential equation

$$\begin{aligned} \dot{x} &= y, \\ \dot{y} &= 2(1 - x^2)y - x, \\ (x(0), y(0))' &= (1, -2)', \end{aligned} \tag{17}$$

in the interval $0 < t < 3.5$ (see Figure 2). Notice that the system exhibits a limit cycle. Near the origin, the system is unstable, and far from the origin, the system is damped. We consider the following regularity side information

$$\|x\|_{\mathcal{C}^2} \le 8, \quad |\dot{X}(t) - \dot{x}(t)| \le 8(t - 3.5)^2,$$

which implies that $M = 8$ and $\sigma(t) = (t - 3.5)^2$. The unsafe set is given by

$$\mathcal{X}_u = \left\{(x, y) \in \mathbb{R}^2 \mid x \ge 0,\ y \ge 2\right\}$$

We are interested in checking whether the system is safe with respect to $\mathcal{X}_u$ at time T=4. Applying Corollary 1, with certificates of degree 2, we were able to find a barrier certificate. Hence, the system is safe at $T = 4$. This can also be corroborated by the simulation results as depicted in Figure 3. The constructed barrier certificate is given below

$$\begin{aligned} B(x, y, t) = &- 7.1441t^2 + 1.7154tx - 20.228ty \\ &- 7.5293t - 3.0302x^2 + 84.477xy \\ &+ 5.306x + 4.439y^2 - 11.394y. \end{aligned}$$

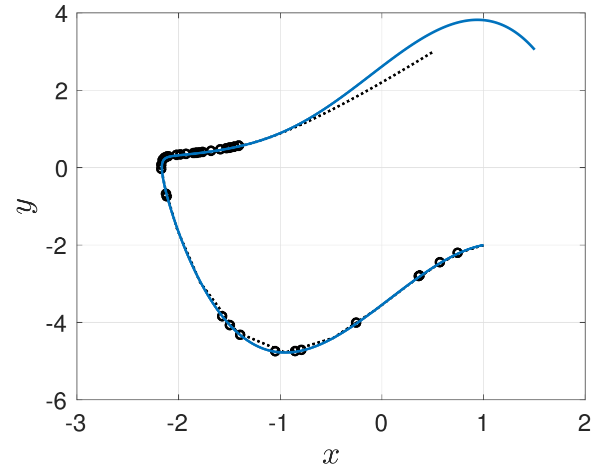

Fig. 2: The data points $\{x_i\}_{t=1}^{40}$ (black circles), the piecewise-polynomial approximation of the state $X(t)$ (black dots) and the trajectories of the system (solid blue).

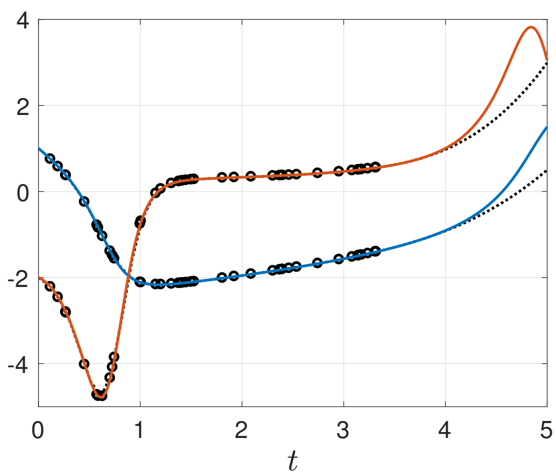

Fig. 3: The data points $\{x_i\}_{t=1}^{40}$ (black circles), the piecewise-polynomial approximation of the state $X(t)$ (black dots) and the actual solution of the system (x solid blue and y solid red).

V. Conclusions and Future Work

A. Conclusions

We considered the problem of safety assessment based on limited data and some regularity information on system states. We reformulated the problem into safety assessment of differential inclusions and we proposed a safety assessment theorem for differential inclusions based on barrier certificates. In the case of piecewise-polynomial approximations of data, we showed that the barrier certificates can be found by polynomial optimization. Two examples were used to illustrate the proposed approach.

B. Future Work

The regularity side information used in this paper to obtain the data-driven differential inclusions may be too restrictive in the case of systems with less smoothness properties. A formulation based on side information in the sense of Lipschitz continuity can relax this constraint. Preliminary works in this area are currently under development.

In this study, we assumed the measurements of the states are not noisy. In many practical situations, this is not the case and sensor measurements are subject to measurement noise, say due to heat. In this setting, safety assessment requires side information in the probabilistic sense. In this respect, one can use notions such as spline smoothing [27].

Future research can study the controller synthesis framework based on data-driven models. This would require an extension of the notion of control barrier functions [28] to the proposed data-driven differential inclusions.

The application of the proposed safety assessment results in this paper are not only limited to data-driven differential inclusions but also the discussions in Section III-C can be used to tackle safety assessment of discontinuous and hybrid systems, such as mechanical system with impact and Columb friction [29].

References

[1] D. Leone, "How an israeli F-15 eagle managed to land with one wing," 2014. [Online]. Available: https://theaviationist.com/2014/09/15/f-15-lands-with-one-wing/

[2] M. Schmidt and H. Lipson, "Distilling free-form natural laws from experimental data," *Science*, no. 5923, pp. 81–85, 2009.

[3] D. Hills, A. Grutter, and J. Hudson, "An algorithm for discovering Lagrangians automatically from data," *Peer J. Computer Science*, no. 1:e31, 2015.

[4] G. Tran and R. Ward, "Exact recovery of chaotic systems from highly corrupted data," *arXiv preprint arXiv:1607.01067*, 2016.

[5] L. Ljung, "Perspectives on system identification," *Annual Reviews in Control*, vol. 34, no. 1, pp. 1 – 12, 2010.

[6] G. Tao, "Multivariable adaptive control: A survey," *Automatica*, vol. 50, no. 11, pp. 2737 – 2764, 2014.

[7] H. Guéguen, M. Lefebvre, J. Zaytoon, and O. Nasri, "Safety verification and reachability analysis for hybrid systems," *Annual Reviews in Control*, vol. 33, no. 1, pp. 25 – 36, 2009.

[8] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 986–1001, July 2003.

[9] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117 – 126, 2006.

[10] M. Ahmadi, A. W. K. Harris, and A. Papachristodoulou, "An optimization-based method for bounding state functionals of nonlinear stochastic systems," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 5342–5347.

[11] M. A. Haque, M. Egerstedt, and C. F. Martin, "First-order, networked control models of swarming silkworm moths," in *2008 American Control Conference*, June 2008, pp. 3798–3803.

[12] S. Han, U. Topcu, and G. J. Pappas, "A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems," in *2015 54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 2049–2054.

[13] C. Fefferman, *Smooth Interpolation of Data by Efficient Algorithms*. Boston: Birkhäuser Boston, 2013, pp. 71–84.

[14] H. Whitney, "Analytic extensions of differentiable functions defined in closed sets," *Transactions of the American Mathematical Society*, vol. 36, no. 1, pp. 63–89, 1934.

[15] C. L. Fefferman, "A sharp form of Whitney's extension theorem," *Annals of Mathematics*, vol. 161, no. 1, pp. 509–577, 2005.

[16] C. Fefferman and B. Klartag, "Fitting a C^m-smooth function to data i," *Rev. Mat. Iberoamericana*, vol. 25, no. 1, pp. 49–273, 2009.

[17] C. Fefferman and A. Israel, "The jet of an interpolant on a finite set," *Rev. Mat. Iberoamericana*, vol. 27, no. 1, pp. 355–360, 2011.

[18] C. Fefferman, "Fitting a C^m -smooth function to data, III," *Annals of Mathematics*, vol. 170, no. 1, pp. 427–441, 2009.

[19] C. de Boor, *A Practical Guide to Splines*, ser. Applied Mathematical Sciences. Springer New York, 2001.

[20] P. Lancaster and K. Šalkauskas, *Curve and Surface Fitting: An Introduction*, ser. Computational mathematics and applications. Academic Press, 1986.

[21] G. Farin, "Cubic spline interpolation," in *Curves and Surfaces for Computer-Aided Geometric Design (Third Edition)*, third edition ed., G. Farin, Ed. Boston: Academic Press, 1993, pp. 133 – 155.

[22] A. F. Filippov, *Differential Equations with Discontinuous Right-Hand Sides*, ser. Mathematics and Its Applications. Kluwer, 1988.

[23] J. P. Aubin and A. Celina, *Differential Inclusions*. Springer-Verlag, Berlin, 1984.

[24] P. Parrilo, "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization," Ph.D. dissertation, California Institute of Technology, 2000.

[25] S. Prajna, A. Papachristodoulou, P. Seiler, and P. Parrilo, "SOSTOOLS: Sum of squares optimization toolbox for MATLAB V3.00," 2013.

[26] J. F. Sturm, "Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones," 1998.

[27] R. L. Smith, L. M. Howser, and J. M. Price, *A smoothing algorithm using cubic spline functions*. Washington: National Aeronautics and Space Administration, Technical Report, 1974.

[28] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, 2016.

[29] M. Posa, M. Tobenkin, and R. Tedrake, "Stability analysis and control of rigid-body systems with impacts and friction," *IEEE Transactions on Automatic Control*, vol. 61, no. 6, pp. 1423–1437, 2016.

[30] M. Choi, T. Y. Lam, and B. Reznick, "Sums of squares of real polynomials," in *Proceedings of Symposia in Pure mathematics*, vol. 58. American Mathematical Society, 1995, pp. 103–126.

[31] G. Chesi, A. Tesi, A. Vicino, and R. Genesio, "On convexification of some minimum distance problems," in *5th European Control Conference*, Karlsruhe, Germany, 1999.

[32] M. Nie, J.and Schweighofer, "On the complexity of Putinar's positivstellensatz," *Journal of Complexity*, vol. 23, no. 1, pp. 135–150, 2007.

[33] J. B. Lasserre, *Moments, Positive Polynomials and Their Applications*. Imperial College Press, London, 2009.

[34] G. Chesi, "LMI techniques for optimization over polynomials in control: a survey," *IEEE Transactions on Automatic Control*, vol. 55, no. 11, pp. 2500–2510, 2010.

Appendix

A. Sum-of-Squares Polynomials

A polynomial $p(x)$ is a sum-of-squares polynomial if $\exists p_i(x) \in \mathcal{R}[x]$, $i \in \{1, \dots, n_d\}$ such that $p(x) = \sum_i p_i^2(x)$. Hence $p(x)$ is clearly non-negative. A set of polynomials p_i is called *SOS decomposition* of $p(x)$. The converse does not hold in general, that is, there exist non-negative polynomials which do not have an SOS decomposition [24]. The computation of SOS decompositions, can be cast as an SDP (see [30], [24], [31]). The Theorem below proves that, in sets satisfying a property stronger than compactness, any positive polynomial can be expressed as a combination of sum-of-squares polynomials and polynomials describing the set.

For a set of polynomials $\bar{g} = \{g_1(x), \dots, g_m(x)\}$, $m \in \mathbb{N}$, the *quadratic module* generated by m is

$$M(\bar{g}) := \left\{ \sigma_0 + \sum_{i=1}^{m} \sigma_i g_i | \sigma_i \in \Sigma[x] \right\}. \tag{18}$$

A quadratic module $M \in \mathcal{R}[x]$ is said *archimedean* if $\exists N \in \mathbb{N}$ such that

$$N - |x|^2 \in M.$$

An archimedian set is always compact [32]. It is then possible to state [33, Theorem 2.14]

Theorem 3 (Putinar Positivstellensatz): Suppose the quadratic module $M(\bar{g})$ is archimedian. Then for every $f \in \mathcal{R}[x]$,

$$f > 0 \;\forall\; x \in \{x | g_1(x) \geq 0, \ldots, g_m(x) \geq 0\} \Rightarrow f \in (\bar{g}).$$

The subsequent proposition formalizes the problem of constrained positivity of polynomials which is a direct result of applying Positivstellensatz.

Proposition 1 ([34]): Let $\{a_i\}_{i=1}^k$ and $\{b_i\}_{i=1}^l$ belong to $\mathcal{P}$, then

$$\begin{aligned} p(x) \geq 0 \qquad & \forall x \in \mathbb{R}^n : a_i(x) = 0, \, \forall i = 1, 2, ..., k \\ & \text{and} \quad b_j(x) \geq 0, \, \forall j = 1, 2, ..., l \end{aligned} \tag{19}$$

is satisfied, if the following holds

$$\begin{aligned} \exists r_1, r_2, \ldots, r_k \in \mathcal{R}[x] \quad \text{and} \quad \exists s_0, s_1, \ldots, s_l \in \Sigma[x] \\ p = \textstyle\sum_{i=1}^k r_i a_i + \sum_{i=1}^l s_i b_i + s_0 \end{aligned} \tag{20}$$

Proposition 2: The multivariable polynomial $p(x)$ is strictly positive ($p(x) > 0 \quad \forall x \in \mathbb{R}^n$), if there exists a $\lambda > 0$ such that

$$\big(p(x) - \lambda\big) \in \Sigma[x] \tag{21}$$