Verification with data-driven differential inclusions

Arie Israel (UT Austin)

February 19, 2019
Overview

- How to generate guarantees for safety properties for nonlinear ODE models with nonparametric uncertainty.
Consider the trajectories of a nonlinear system,

\[
\frac{dx}{dt} = f(x), \quad x \in \mathbb{R}^n, \quad x(t_0) = x_0.
\]

\(f\) is a \(C^m\) vector field: partial derivatives \(\partial^\alpha f(x)\) are uniformly bounded for \(|\alpha| \leq m\).
Assumptions

- Consider the trajectories of a nonlinear system,

\[ \frac{dx}{dt} = f(x), \quad x \in \mathbb{R}^n, \quad x(t_0) = x_0. \]

- \( f \) is a \( C^m \) vector field: partial derivatives \( \partial^\alpha f(x) \) are uniformly bounded for \( |\alpha| \leq m \).

- We observe snapshots of the state and state velocity

\[ (x_k, y_k) = \left( x, \frac{dx}{dt} \right) \bigg|_{t=t_k}, \quad k = 0, \cdots, N. \]

where \( t_0 < t_1 < \cdots < t_N = 0 \).

- Snapshots give rise to interpolation constraints on the unknown vector field:

\[ f(x_k) = y_k. \]
Assumptions

- Starting at time $t = 0$, we want to verify that the trajectory will satisfy the following safety property: $x(t)$ remains in the complement of an unsafe set $\mathcal{X}_u \subset \mathbb{R}^n$ for all times $t \in [0, T]$. 
Best-case (viability): We win if there exists at least one data-consistent vector field $f$ so that the associated trajectory $x(t)$ remains safe.
Three perspectives on verification

- **Best-case (viability):** We win if there exists at least one data-consistent vector field $f$ so that the associated trajectory $x(t)$ remains safe.
- **Worst-case (invariance):** We win if for all data-consistent vector fields $f$ the associated trajectory $x(t)$ remains safe.
Best-case (viability): We win if there exists at least one data-consistent vector field $f$ so that the associated trajectory $x(t)$ remains safe.

Worst-case (invariance): We win if for all data-consistent vector fields $f$ the associated trajectory $x(t)$ remains safe.

Probabilistic: Suppose the space of all functions $f$ is endowed with a probability measure $dProb$. We win if at least $\alpha$ percent of the associated trajectories $x(t)$ remain safe.
Viability certificates

- A vector field $f : \mathbb{R}^n \to \mathbb{R}^n$ is a "viability certificate" if the following conditions hold:

$$
\begin{cases}
|\partial^\alpha f(x)| \leq 1, & x \in \mathbb{R}^n, |\alpha| \leq m \\
f(x(t_k)) = \frac{dx}{dt}(t_k), & k = 0, \ldots, N \\
f(x) \cdot \vec{n}(x) \geq 0, & x \in \partial X_u,
\end{cases}
$$

where $\vec{n}$ is the outward-directed unit normal on the boundary of $X_u$. 

This certificate encodes the viability of the safety property on an infinite time-horizon ($T = \infty$). Bernat and Charlie's algorithm can be used to detect the existence of such a certificate.

We would like to produce less restrictive certificates for safety on a finite time-horizon $T < \infty$. 

Arie Israel (UT Austin)
Verification with data-driven differential inclusions
February 19, 2019 6 / 12
A vector field $f : \mathbb{R}^n \to \mathbb{R}^n$ is a “viability certificate” if the following conditions hold:

\[
\begin{cases}
|\partial^\alpha f(x)| \leq 1, & x \in \mathbb{R}^n, |\alpha| \leq m \\
f(x(t_k)) = \frac{dx}{dt}(t_k), & k = 0, \ldots, N \\
f(x) \cdot \vec{n}(x) \geq 0, & x \in \partial \mathcal{X}_u,
\end{cases}
\]

where $\vec{n}$ is the outward-directed unit normal on the boundary of $\mathcal{X}_u$.

This certificate encodes the viability of the safety property on an infinite time-horizon ($T = \infty$).

Bernat and Charlie’s algorithm can be used to detect the existence of such a certificate.

We would like to produce less restrictive certificates for safety on a finite time-horizon $T < \infty$. 
To determine whether a safety property is satisfied for all possible realizations of the system, we need to consider the set of all possible vector fields $f$ consistent with the data.
A connection between ODEs and Differential Inclusions

- Suppose a function \( f : \mathbb{R}^n \rightarrow \mathbb{R}^n \) satisfies

  \[(\text{Bounded Derivatives}): \quad |\partial^{\alpha} f(x)| \leq 1 \quad \text{all} \ x \in \mathbb{R}^n, \ |\alpha| \leq m\]

  and

  \[(\text{Interpolation Constraints}): \quad f(x_k) = y_k \quad \text{all} \ k = 1, \cdots, N.\]

  For any \( x \in \mathbb{R}^n \), consider

  \[K(x) = \{ f(x) : f \text{ has (Bounded Derivatives),}
  \]
  
  \[\text{and satisfies (Interpolation Constraints)}\},\]

  a convex subset of \( \mathbb{R}^n \).
For any $x \in \mathbb{R}^n$, consider

$$K(x) = \{ f(x) : f \text{ has (Bounded Derivatives),}$$

and satisfies (Interpolation Constraints)\},

a convex subset of $\mathbb{R}^n$. 

![Diagram](image)
The Bo'az-Charlie interpolation algorithm produces an almost tight polytopal approximation \( \tilde{K}(x) \supseteq K(x) \).
The Bo'az-Charlie interpolation algorithm produces an almost tight polytopal approximation \( \tilde{K}(x) \supseteq K(x) \).

Therefore, any solution of \( \frac{dx}{dt} = f(x) \) will satisfy

\[
(3) \quad \frac{dx}{dt}(t) \in \tilde{K}(x(t)), \quad \text{all } t \geq 0.
\]
The Bo'az-Charlie interpolation algorithm produces an almost tight polytopal approximation \( \tilde{K}(x) \supseteq K(x) \).

Therefore, any solution of \( \frac{dx}{dt} = f(x) \) will satisfy

\[
(3) \quad \frac{dx}{dt}(t) \in \tilde{K}(x(t)), \quad \text{all } t \geq 0.
\]

In addition to (3), we know that the curve \( x(t) \) will be \((m + 1)\)-times differentiable, and

\[
(4) \quad \left| \frac{d^k x}{dt^k} \right| \leq \text{Const}, \quad \text{all } k = 1, \ldots, m.
\]
- The Bo'az-Charlie interpolation algorithm produces an almost tight polytopal approximation $\tilde{K}(x) \supset K(x)$.

- Therefore, any solution of $\frac{dx}{dt} = f(x)$ will satisfy

$$\text{(3)} \quad \frac{dx}{dt}(t) \in \tilde{K}(x(t)), \quad \text{all } t \geq 0.$$ 

- In addition to (3), we know that the curve $x(t)$ will be $(m + 1)$-times differentiable, and

$$\text{(4)} \quad \left| \frac{d^k x}{dt^k} \right| \leq \text{Const}, \quad \text{all } k = 1, \cdots, m.$$ 

- Conditions (3) and (4) yield a differential inclusion satisfied by the trajectories of the original dynamical system.

- Up to constant-factor enlargements, this is the tightest differential inclusion which is consistent with the data.
Given a differential inclusion

\[
(3) \quad \frac{dx}{dt}(t) \in \tilde{K}(x(t)), \quad \text{all } t \geq 0, \\
(4) \quad \left| \frac{d^k x}{dt^k} \right| \leq \text{Const}, \quad \text{all } k = 1, \cdots, m, \\
(5) \quad x(0) = x_0 \text{ (fixed)}. 
\]

How can we detect whether all the trajectories \( x(t) \) of (3)–(5) will remain in the complement of \( \mathcal{X}_u \) over a finite time-horizon?
Summary and future directions

- We defined viability certificates for safety verification over infinite-time horizons.
- We explained how to learn a Differential Inclusion from data.
- Barrier Certificates for Differential Inclusions?
- Online Interpolation?
  How to efficiently shrink the sets $\tilde{K}(x)$ with arrival of a single new data point?