中国科学院软件研究所
Institute of Software Chinese Academy of Sciences

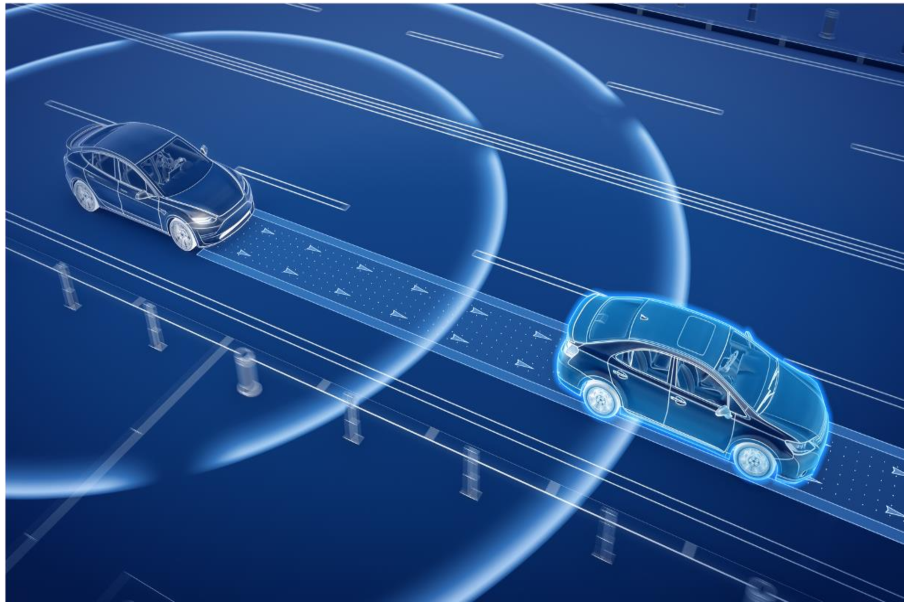
A Framework for Safe Probabilistic Invariance Verification of Stochastic Dynamical Systems

Bai Xue

Email: xuebai@ios.ac.cn
Homepage: http://lcs.ios.ac.cn/~xuebai/

April 23, 2025

Background

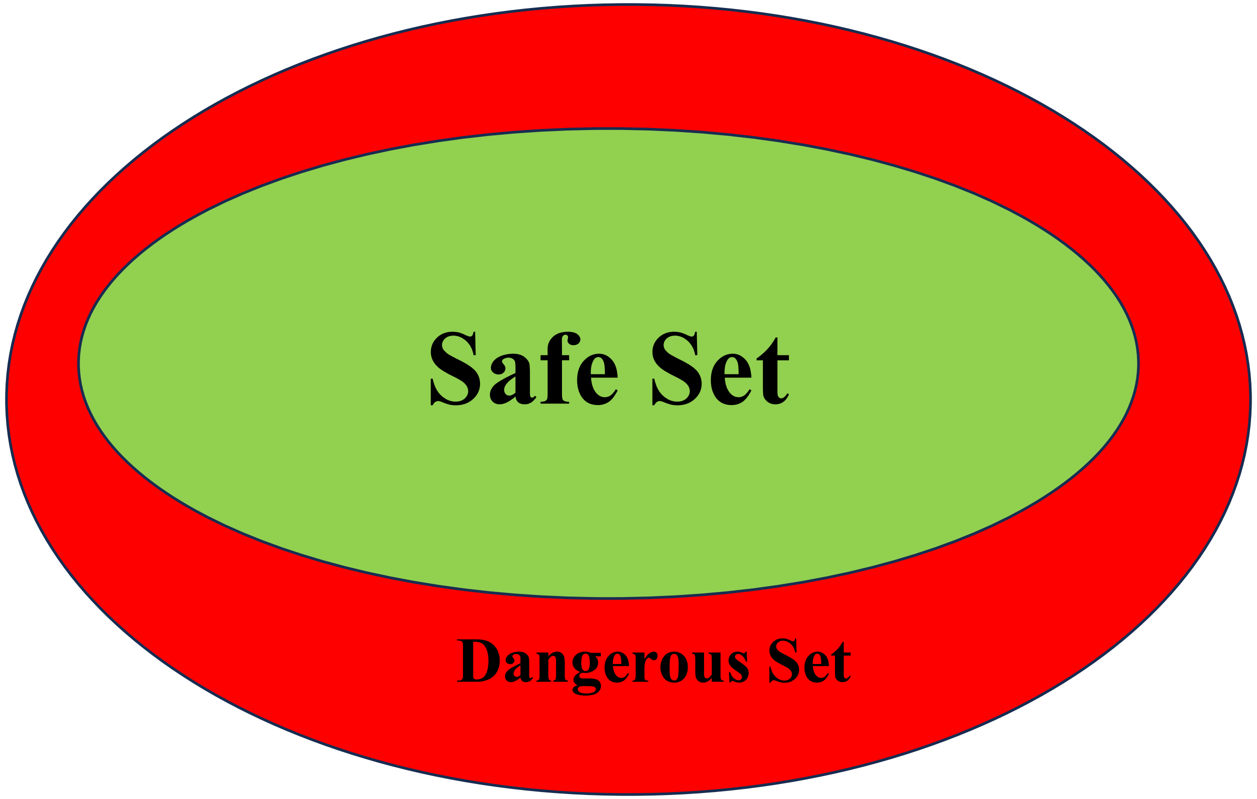


Safety Is Paramount!

A safety property asserts that some “bad thing” does not happen during execution [Leslie Lamport, 1977]

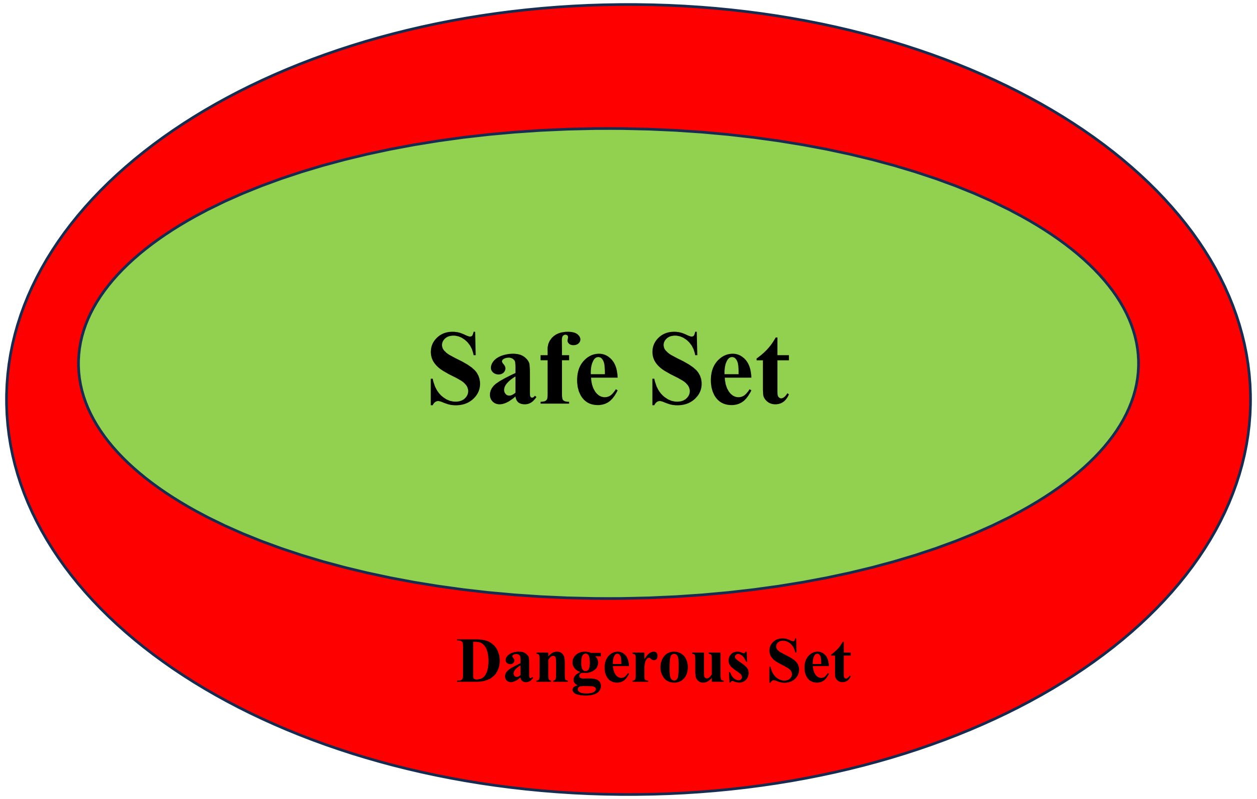
A safety property asserts that some “bad thing” does not happen during execution [Leslie Lamport, 1977]

It is closely related to set-invariance for dynamical systems [Aaron D. Ames, et.al., 2019]



A safety property asserts that some “bad thing” does not happen during execution [Leslie Lamport, 1977]

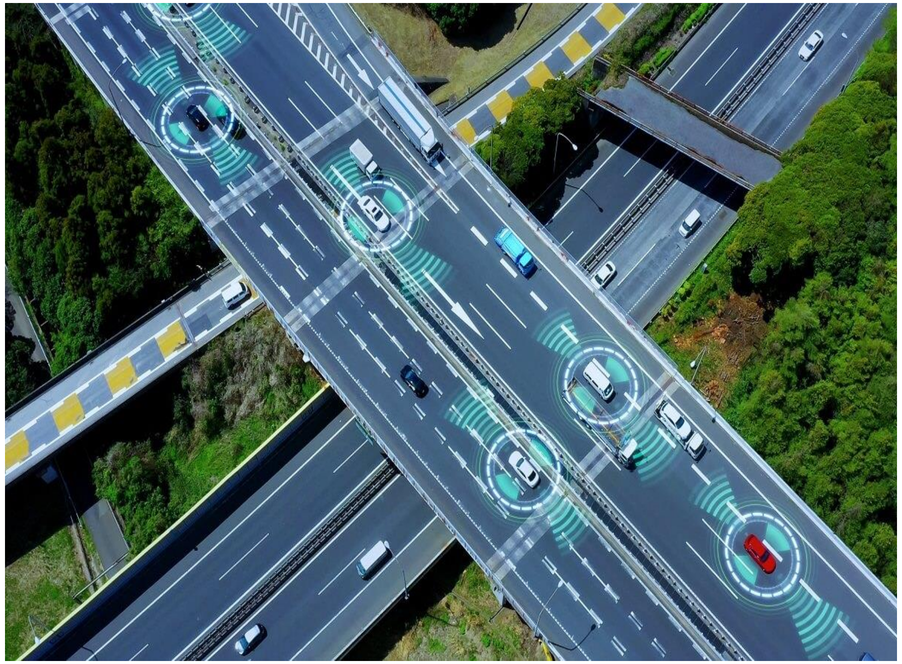
It is closely related to set-invariance for dynamical systems [Aaron D. Ames, et.al., 2019]



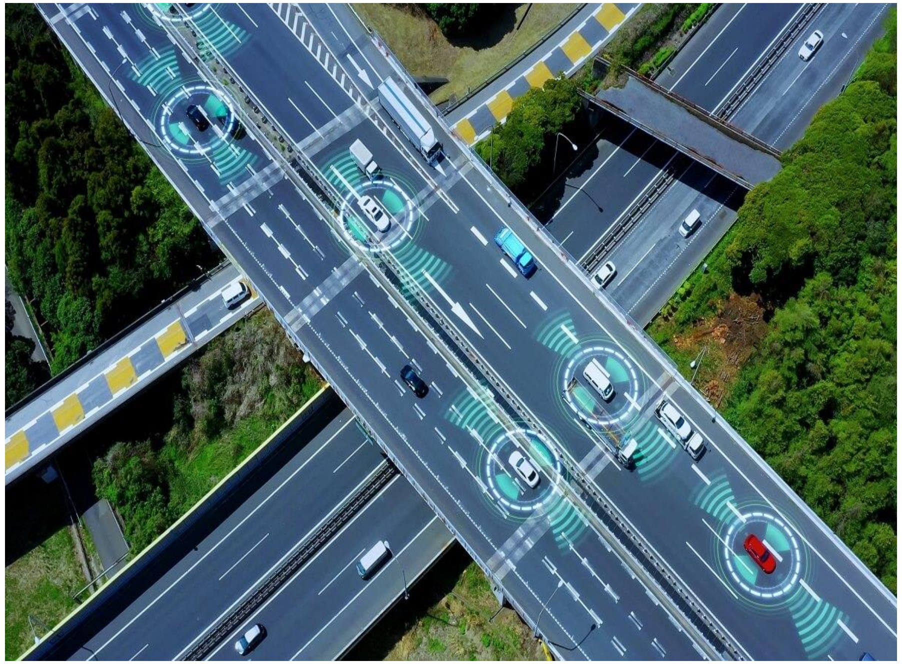
Dynamical systems:

- Discrete-time Systems: $x(k+1) = f\big(x(k)\big)$
- Continuous-time Systems: $\frac{dx}{dt} = f(x)$

The real system is highly complex: the complete information of such a system can indeed be challenging to acquire, especially in open environments.



The real system is highly complex: the complete information of such a system can indeed be challenging to acquire, especially in open environments.



How do we guarantee safety of these systems?

Safe Robust Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

- $d(k) \in \mathcal{D}$ is the perturbation input

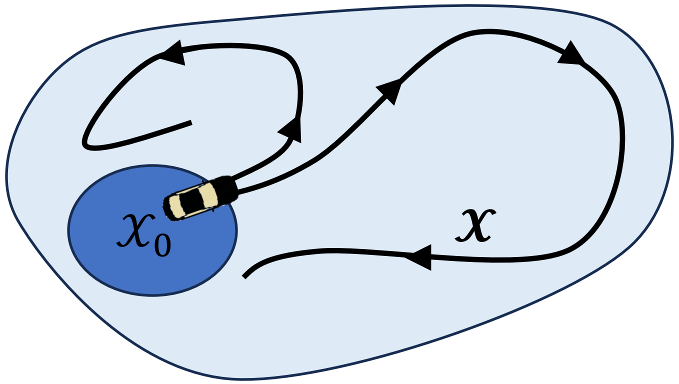
Safe Robust Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

- $d(k) \in \mathcal{D}$ is the perturbation input

Safe robust invariance verification：

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, to verify that the system starting from $\mathcal{X}_0$ will **remain inside the safe set $\mathcal{X}$ for all time, regardless of disturbances**



Safe Robust Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

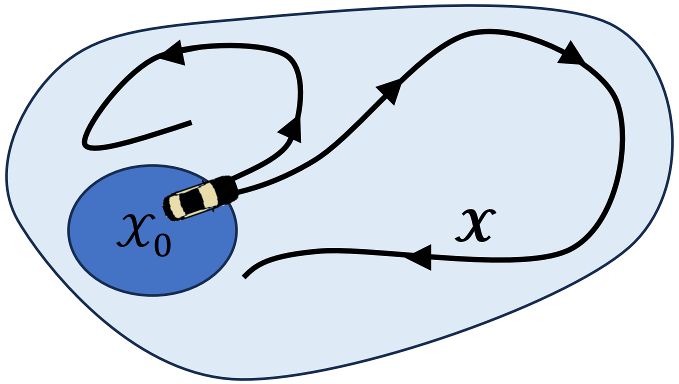
- $d(k) \in \mathcal{D}$ is the perturbation input

Safe robust invariance verification:

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, to verify that the system starting from $\mathcal{X}_0$ will **remain inside the safe set $\mathcal{X}$ for all time, regardless of disturbances**

Given $\lambda > 0$, **finding Barrier Functions $B(x)$:**

$$\begin{cases} B(x) \geq 0, & \forall x \in \mathcal{X}_0, \\ B\big(f(x,d)\big) \geq \lambda B(x), & \forall x \in \mathcal{X}, \forall d \in \mathcal{D}, \\ B(x) < 0, & \forall x \in \mathbb{R}^n \setminus \mathcal{X}. \end{cases}$$



Safe Robust Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

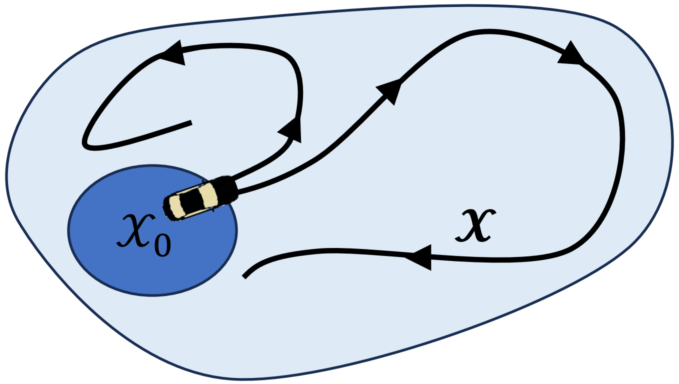
- $d(k) \in \mathcal{D}$ is the perturbation input

Safe robust invariance verification：

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, to verify that the system starting from $\mathcal{X}_0$ will **remain inside the safe set $\mathcal{X}$ for all time, regardless of disturbances**

Given $\lambda > 0$, **finding Barrier Functions $B(x)$:**

$$\begin{cases} B(x) \geq 0, & \forall x \in \mathcal{X}_0, \\ B\big(f(x,d)\big) \geq \lambda B(x), & \forall x \in \mathcal{X}, \forall d \in \mathcal{D}, \\ B(x) < 0, & \forall x \in \mathbb{R}^n \setminus \mathcal{X}. \end{cases}$$



Safe Robust Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

- $d(k) \in \mathcal{D}$ is the perturbation input

Safe robust invariance verification:

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, to verify that the system starting from $\mathcal{X}_0$ will **remain inside the safe set $\mathcal{X}$ for all time, regardless of disturbances**

Given $\lambda > 0$, **finding Barrier Functions $B(x)$:**

$$\begin{cases} B(x) \geq 0, & \forall x \in \mathcal{X}_0, \\ B\big(f(x,d)\big) \geq \lambda B(x), & \forall x \in \mathcal{X}, \forall d \in \mathcal{D}, \\ B(x) < 0, & \forall x \in \mathbb{R}^n \setminus \mathcal{X}. \end{cases}$$

Too Conservative!

Safe Probabilistic Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

- $d(k) \in \mathcal{D}$ is the stochastic perturbation input, **following certain known distribution**

Safe Probabilistic Invariance Verification

$$x(k+1) = f\big(x(k), d(k)\big)$$

- $d(k) \in \mathcal{D}$ is the stochastic perturbation input, **following certain known distribution**

Safe probabilistic invariance verification:

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, to verify that the system starting from $\mathcal{X}_0$ will remain inside the safe set $\mathcal{X}$ with a certain probability

Safe Probabilistic Invariance Verification

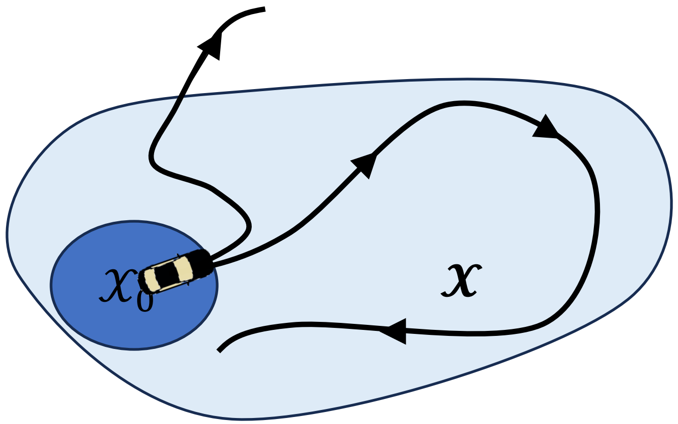
$$x(k+1) = f\big(x(k), d(k)\big)$$

- $d(k) \in \mathcal{D}$ is the stochastic perturbation input, following certain known distribution

Safe probabilistic invariance verification:

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, to verify that the system starting from $\mathcal{X}_0$ will remain inside the safe set $\mathcal{X}$ with a certain probability

This approach reduces conservatism by allowing probabilistic violations



Related Work

- Probabilistic Invariant Sets [e.g., E. Kofman, et.al., 2012 (Kofman); E. Kofman, et.al., 2016 (Kofman); L. Hewing, et.al., ECC 2018]: **Linear Systems**

- Finite-time Probabilistic Invariance Problem [e.g., A. Abate, et. al., 2008 (Automatica); A. Abate, et. Al., 2010 (European Journal of Control); C. Santoyo et.al, 2021 (Automatica)]

- Infinite-time Probabilistic Invariance Problem:
  - **Finite-time Probabilistic Invariance + Robust Invariant Sets** [e.g., I. Tkachev and A. Abate, et.al., CDC 2011; I. Tkachev and A. Abate, et.al., 2014 (Theoretical Computer Science)]
  - **Barrier Certificates Methods** [e.g., M. Anand, et. al., HSCC 2022; Peixin Wang, et.al., CAV 2024]

…

Problem Formulation

Stochastic Discrete-time Systems

$$x(k+1) = f\big(x(k), d(k)\big), \quad x(0) = x_0$$

- $d(k) \in \mathcal{D}$ is the stochastic perturbation input.
- $d(0), d(1), \dots,$ are independent and identically distributed (i.i.d) on a probability space $(\boldsymbol{\mathcal{D}}, \mathcal{F}, \mathbb{P})$, with support $\boldsymbol{\mathcal{D}}$: for any measurable set $B \subseteq \boldsymbol{\mathcal{D}}, \mathrm{Prob}(d(l) \in B) = \mathbb{P}(B), \forall l \in \mathbb{N}$. The expectation is denoted by $\mathbb{E}[\cdot]$.

A disturbance signal $\boldsymbol{\pi}$ is an ordered sequence $\{d(k), k \in \mathbb{N}\}$: a sample path of a stochastic process defined on the canonical sample space $\boldsymbol{\Omega}^{\infty} = \boldsymbol{\mathcal{D}} \times \boldsymbol{\mathcal{D}} \times \cdots$ with the probability measure $\mathbb{P}^{\infty} = \mathbb{P} \times \mathbb{P} \times \cdots$.

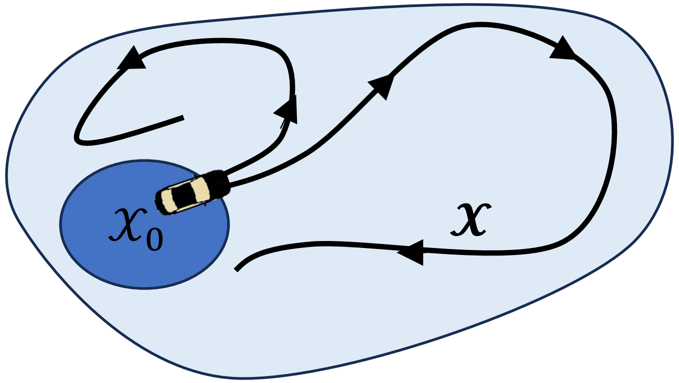
Trajectory $\boldsymbol{\phi_{\pi}^{x_0}}(\cdot): \mathbb{N} \to \mathbb{R}^n$: $\quad \boldsymbol{\phi_{\pi}^{x_0}(k+1) = f\left(\phi_{\pi}^{x_0}(k), \pi(k)\right), \phi_{\pi}^{x_0}(0) = x_0}$

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$,

the safe probabilistic invariance verification is to compute lower and upper bounds, denoted by $\epsilon_1 \in [0,1]$ and $\epsilon_2 \in [0,1]$ respectively, for the safety probability that the system, starting from any state in $\mathcal{X}_0$, will remain inside the safe set $\mathcal{X}$ for all time, i.e.,

to compute ϵ_1 and ϵ_2 such that

$$\epsilon_1 \leq \mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x_0}}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2.$$



Doob's Supermartingale Inequality Based Method

Doob's Supermartingale Inequality [J. Ville, 1939]

Let $(\Omega_1, \mathcal{F}, \mathbb{P}_1)$ be the probability space and $\{B_i\}_{i\in\mathbb{N}}$ be a non-negative supermartingale, then for $b > 0$,

$$\mathbb{P}_1\left(\sup_{i\in\mathbb{N}} B_i \geq b \mid B_0\right) \leq \frac{B_0}{b}.$$

Doob's Supermartingale Inequality Based Method

Doob's Supermartingale Inequality [J. Ville, 1939]

Let $(\Omega_1, \mathcal{F}, \mathbb{P}_1)$ be the probability space and $\{B_i\}_{i\in\mathbb{N}}$ be a non-negative supermartingale, then for $b > 0$,

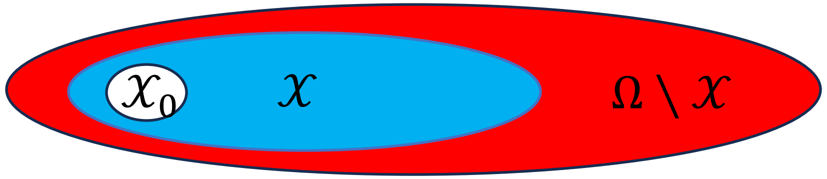
$$\mathbb{P}_1\left(\sup_{i\in\mathbb{N}} B_i \geq b \mid B_0\right) \leq \frac{B_0}{b}.$$

In [M. Anand, et. al., HSCC 2022],
Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{d}): \boldsymbol{\Omega} \times \boldsymbol{\mathcal{D}} \to \boldsymbol{\Omega}$, and $\mathcal{X}_0 \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \Omega, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \Omega, \\ v(x) \geq 1, & \forall x \in \boldsymbol{\Omega} \setminus \boldsymbol{\mathcal{X}}, \end{cases}$$

where $\boldsymbol{\Omega} \setminus \boldsymbol{\mathcal{X}}$ is a set of unsafe states, then

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x_0}}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$



中国科学院软件研究所
Institute of Software Chinese Academy of Sciences

Doob's Supermartingale Inequality Based Method

Doob's Supermartingale Inequality [J. Ville, 1939]

Let $(\Omega_1, \mathcal{F}, \mathbb{P}_1)$ be the probability space and $\{B_i\}_{i\in\mathbb{N}}$ be a non-negative supermartingale, then for $b > 0$,

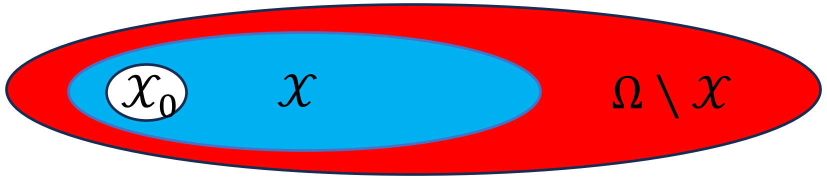
$$\mathbb{P}_1\left(\sup_{i\in\mathbb{N}} B_i \geq b \mid B_0\right) \leq \frac{B_0}{b}.$$

In [M. Anand, et. al., HSCC 2022],
Under the assumption that $\boldsymbol{\Omega} \subset \mathbb{R}^n$ is a robust invariant set, i.e., $\boldsymbol{f(x,d)}: \boldsymbol{\Omega} \times \boldsymbol{\mathcal{D}} \to \boldsymbol{\Omega}$, and $\mathcal{X}_0 \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \Omega, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \Omega, \\ v(x) \geq 1, & \forall x \in \boldsymbol{\Omega} \setminus \boldsymbol{\mathcal{X}}, \end{cases}$$

where $\boldsymbol{\Omega} \setminus \boldsymbol{\mathcal{X}}$ is a set of unsafe states, then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi_{\pi}^{x_0}(k)} \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$



Doob's Supermartingale Inequality Based Method

Doob's Supermartingale Inequality [J. Ville, 1939]

Let $(\Omega_1, \mathcal{F}, \mathbb{P}_1)$ be the probability space and $\{B_i\}_{i\in\mathbb{N}}$ be a non-negative supermartingale, then for $b > 0$,

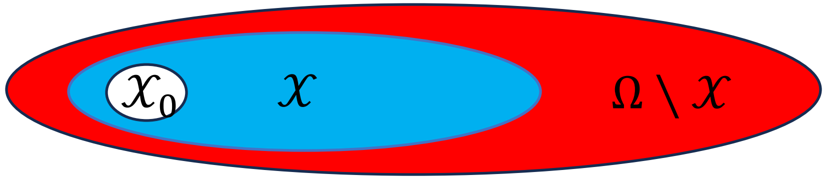
$$\mathbb{P}_1\left(\sup_{i\in\mathbb{N}} B_i \geq b \mid B_0\right) \leq \frac{B_0}{b}.$$

In [M. Anand, et. al., HSCC 2022],
Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $f(x,d): \Omega \times \mathcal{D} \to \Omega$, and $\mathcal{X}_0 \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \Omega, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \Omega, \\ v(x) \geq 1, & \forall x \in \Omega \setminus \mathcal{X}, \end{cases}$$

where $\Omega \setminus \mathcal{X}$ is a set of unsafe states, then

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$



- **$\Omega \neq \mathbb{R}^n$: challening to compute (if it exists)**
- **$\Omega = \mathbb{R}^n$: producing conservative lower bounds**

Running Example

A computer-based model, which is modified from the reversed-time Van der Pol oscillator based on Euler's method with the time step 0.01:

$$\begin{cases} x(l+1) = x(l) - 0.02y(l), \\ y(l+1) = y(l) + 0.01\Big(\big(0.8 + d(l)\big)x(l) + 10(x^2(l) - 0.21)y(l)\Big). \end{cases}$$

- $d(\cdot): \mathbb{N} \to \mathcal{D} = [-0.1, 0.1]$
- $\mathcal{X} = \{(x, y) \mid x^2 + y^2 - 1 \leq 0\}$
- $\mathcal{X}_0 = \{(x, y) \mid x^2 + y^2 - 0.01 < 0\}$

❖ Monto-carlo method: $\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\pi}^{x_0}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big) \approx \mathbf{1}$

❖ Method in [M. Anand, et. al., HSCC 2022]($\boldsymbol{\Omega} = \mathbb{R}^{\mathbf{2}}$)+ semi-definite programming tool:

$$\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\pi}^{x_0}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big) \geq \mathbf{2.1368}\boldsymbol{e} - \mathbf{07}$$

Doob’s Supermartingale Inequality Based Method

An auxiliary system

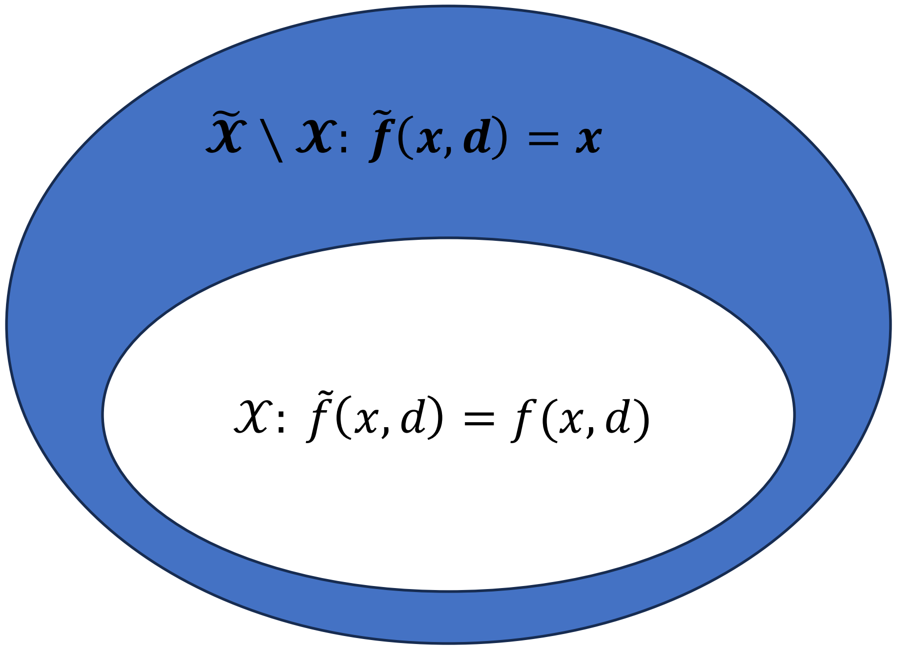
$$x(k+1) = \tilde{f}\big(x(k), d(k)\big)$$

with

$$\tilde{f}(x,d) = f(x,d)\cdot 1_{\mathcal{X}}(x) + x\cdot 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x)$$

$\widetilde{\mathcal{X}}$ is a set containing the union of the set $\mathcal{X}$ and all reachable states starting from $\mathcal{X}$ within one step:

$$\{x \mid x = f(x_0, d), x_0\in\mathcal{X}, d\in\mathcal{D}\}\cup\mathcal{X}\subseteq\widetilde{\mathcal{X}}$$



Doob's Supermartingale Inequality Based Method

An auxiliary system

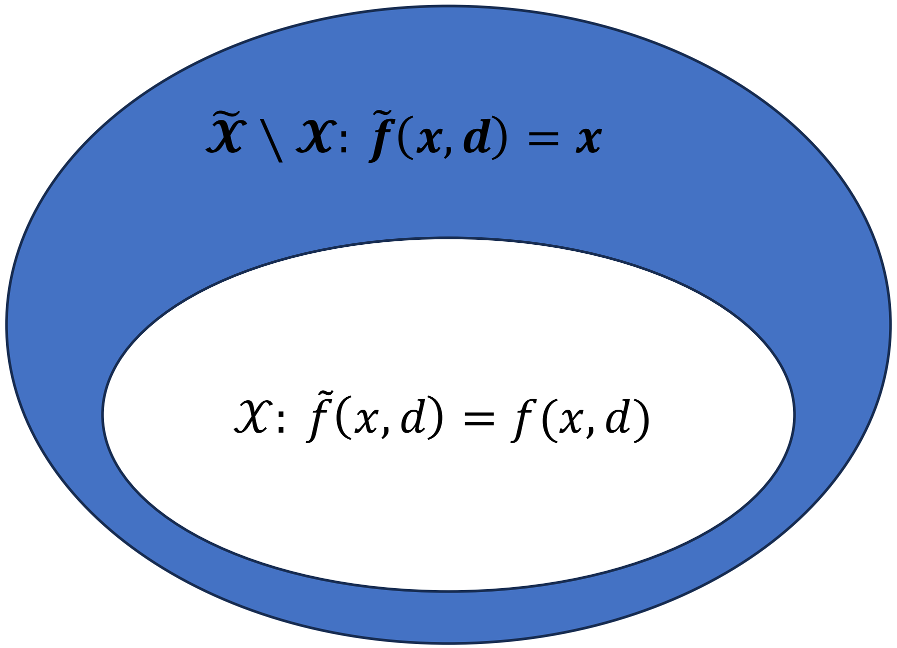
$$x(k+1) = \tilde{f}\big(x(k), d(k)\big)$$

with

$$\tilde{f}(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(x)$$

$\widetilde{\mathcal{X}}$ is a set containing the union of the set $\mathcal{X}$ and all reachable states starting from $\mathcal{X}$ within one step:

$$\{x \mid x = f(x_0, d), x_0 \in \mathcal{X}, d \in \mathcal{D}\} \cup \mathcal{X} \subseteq \widetilde{\mathcal{X}}$$



$\widetilde{\mathcal{X}}$ is a robust invariant set for the auxiliary system

Doob's Supermartingale Inequality Based Method

An auxiliary system

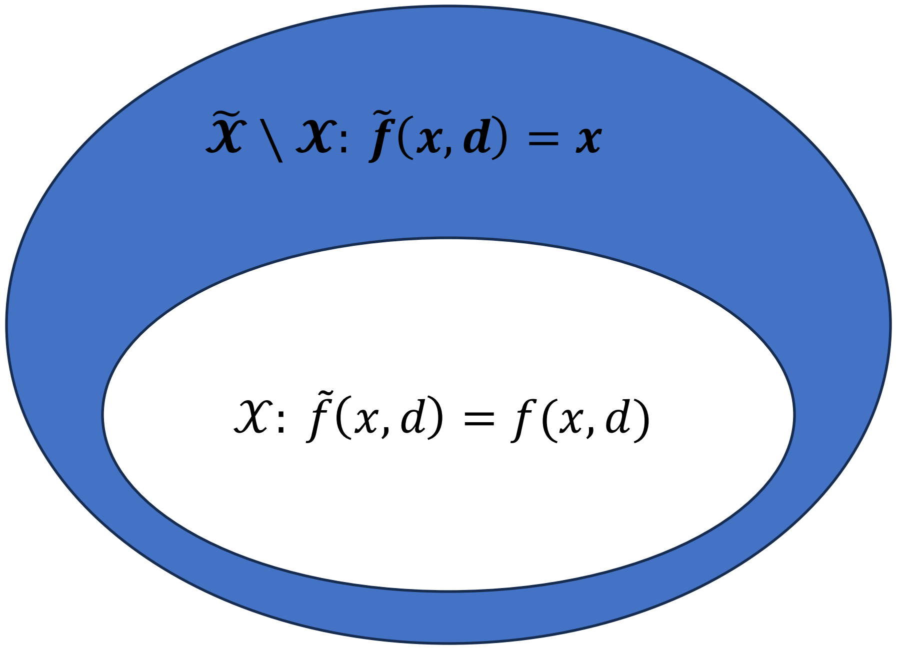
$$x(k+1) = \tilde{f}\big(x(k), d(k)\big)$$

with

$$\tilde{f}(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\tilde{\mathcal{X}} \setminus \mathcal{X}}(x)$$

$\tilde{\mathcal{X}}$ is a set containing the union of the set $\mathcal{X}$ and all reachable states starting from $\mathcal{X}$ within one step:

$$\{x \mid x = f(x_0, d), x_0 \in \mathcal{X}, d \in \mathcal{D}\} \cup \mathcal{X} \subseteq \tilde{\mathcal{X}}$$



$\tilde{\mathcal{X}}$ is a robust invariant set for the auxiliary system

Proposition 1 $\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big) = \mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \tilde{\phi}_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big)$

Doob's Supermartingale Inequality Based Method

Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $f(x,d): \Omega \times \mathcal{D} \to \Omega$, and $\mathcal{X} \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(x) \le 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \ge 0, & \forall x \in \Omega, \\ \mathbb{E}[v(f(x,d))] \le v(x), & \forall x \in \Omega, \\ v(x) \ge 1, & \forall x \in \Omega \setminus \mathcal{X}, \end{cases}$$

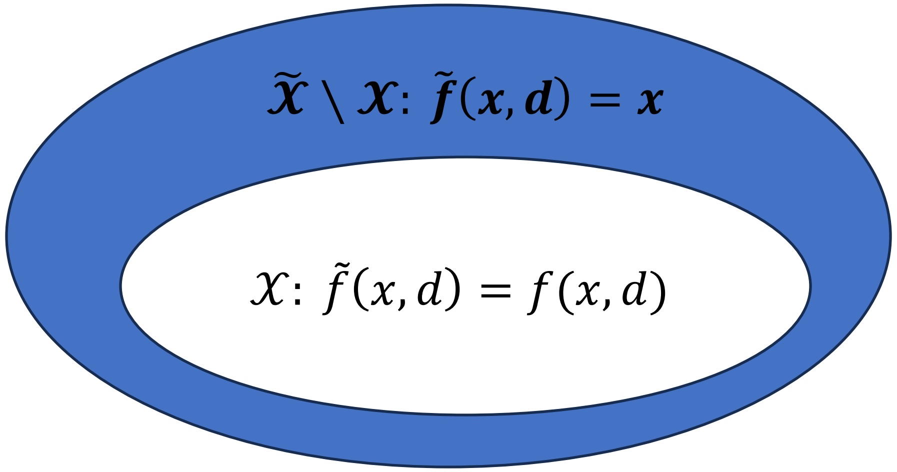
then $\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \ge \epsilon_1$.

⇒

If there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \le 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \ge 0, & \forall x \in \widetilde{\mathcal{X}}, \\ \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right] \le v(x), & \forall x \in \widetilde{\mathcal{X}}, \\ v(x) \ge 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then $\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \ge \epsilon_1$.



Doob's Supermartingale Inequality Based Method

Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $f(x,d): \Omega \times \mathcal{D} \to \Omega$, and $\mathcal{X} \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \Omega, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \Omega, \\ v(x) \geq 1, & \forall x \in \Omega \setminus \mathcal{X}, \end{cases}$$

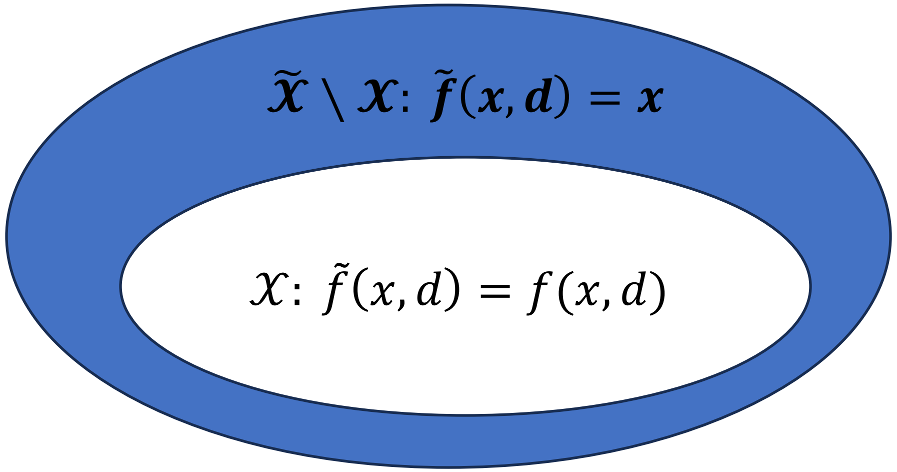
then $\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \geq \epsilon_1$.

If there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}, \\ \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right] \leq v(x), & \forall x \in \widetilde{\mathcal{X}}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then $\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \geq \epsilon_1$.

$$\tilde{f}(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(x)$$



Theorem 1 If there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then $\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \geq \epsilon_1$.

Running Example

A computer-based model, which is modified from the reversed-time Van der Pol oscillator based on Euler's method with the time step 0.01:

$$\begin{cases} x(l+1) = x(l) - 0.02y(l), \\ y(l+1) = y(l) + 0.01\Big(\big(0.8 + d(l)\big)x(l) + 10\big(x^2(l) - 0.21\big)y(l)\Big). \end{cases}$$

- $d(\cdot): \mathbb{N} \to \mathcal{D} = [-0.1, 0.1]$
- $\mathcal{X} = \{(x, y) \mid x^2 + y^2 - 1 \le 0\}$
- $\mathcal{X}_0 = \{(x, y) \mid x^2 + y^2 - 0.01 < 0\}$

❖ Monto-carlo method: $\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big) \approx 1$

❖ Method in [M. Anand, et. al., HSCC 2022]($\boldsymbol{\Omega} = \mathbb{R}^{\mathbf{2}}$)+ semi-definite programming tool:

$$\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big) \ge 2.1368e-07$$

❖ **Our method** ($\widetilde{\mathcal{X}} = \{(x, y) \mid \boldsymbol{x^2 + y^2 - 2 \le 0}\}$) +semi-definite programming tool:

$$\mathbb{P}^{\infty}\big(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(\boldsymbol{k}) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\big) \ge 0.9465$$

Doob's Supermartingale Inequality Based Method

In [M. Anand, et. al., HSCC 2022],
Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $f(x,d): \Omega \times \mathcal{D} \to \Omega$, and $\mathcal{X} \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(\boldsymbol{x}) \leq \epsilon_2, & \forall \boldsymbol{x} \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall \boldsymbol{x} \in \boldsymbol{\Omega}, \\ \mathbb{E}[v(\boldsymbol{f}(\boldsymbol{x},\boldsymbol{d}))] - v(\boldsymbol{x}) \leq -\delta, & \forall \boldsymbol{x} \in \overline{\boldsymbol{\Omega} \setminus (\boldsymbol{\Omega} \setminus \mathcal{X})}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \partial\boldsymbol{\Omega} \setminus \partial(\boldsymbol{\Omega} \setminus \mathcal{X}), \end{cases}$$

then $\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2.$

Theorem 2 Let $\mathcal{X}$ be a closed set. If there exists $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(\boldsymbol{x}) \leq \epsilon_2, & \forall \boldsymbol{x} \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(\boldsymbol{f}(\boldsymbol{x},\boldsymbol{d}))] - v(\boldsymbol{x}) \leq -\boldsymbol{\delta}, & \forall \boldsymbol{x} \in \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \partial\widetilde{\mathcal{X}} \setminus \partial(\widetilde{\mathcal{X}} \setminus \mathcal{X}), \end{cases}$$

then
$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2.$

Doob's Supermartingale Inequality Based Method

In [M. Anand, et. al., HSCC 2022],
Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $f(x, d): \Omega \times \mathcal{D} \to \Omega$, and $\mathcal{X} \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(\boldsymbol{x}) \leq \epsilon_2, & \forall \boldsymbol{x} \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall \boldsymbol{x} \in \boldsymbol{\Omega}, \\ \mathbb{E}[v(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{d}))] - v(\boldsymbol{x}) \leq -\delta, & \forall \boldsymbol{x} \in \overline{\boldsymbol{\Omega} \setminus (\boldsymbol{\Omega} \setminus \mathcal{X})}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \partial\boldsymbol{\Omega} \setminus \partial(\boldsymbol{\Omega} \setminus \mathcal{X}), \end{cases}$$

then $\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2$.

Theorem 2 Let $\mathcal{X}$ be a closed set. If there exists $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(\boldsymbol{x}) \leq \epsilon_2, & \forall \boldsymbol{x} \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{d}))] - v(\boldsymbol{x}) \leq -\boldsymbol{\delta}, & \forall \boldsymbol{x} \in \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \partial\widetilde{\boldsymbol{\mathcal{X}}} \setminus \partial(\widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}), \end{cases}$$

then
$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2$.

If $v(x)$ is bounded over $\widetilde{\mathcal{X}}$, it provides strong guarantees of leaving the safe set $\mathcal{X}$ almost surely, i.e., $\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) = 0$.

Doob's Supermartingale Inequality Based Method

In [M. Anand, et. al., HSCC 2022],
Under the assumption that $\Omega \subset \mathbb{R}^n$ is a robust invariant set, i.e., $f(x,d): \Omega \times \mathcal{D} \to \Omega$, and $\mathcal{X} \subseteq \Omega$, if there exists $v(x): \Omega \to \mathbb{R}$ such that

$$\begin{cases} v(\boldsymbol{x}) \leq \epsilon_2, & \forall \boldsymbol{x} \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall \boldsymbol{x} \in \boldsymbol{\Omega}, \\ \mathbb{E}[v(f(x,d))] - v(x) \leq -\delta, & \forall x \in \overline{\Omega \setminus (\Omega \setminus \mathcal{X})}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \partial\boldsymbol{\Omega} \setminus \partial(\boldsymbol{\Omega} \setminus \mathcal{X}), \end{cases}$$

then $\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2$.

Theorem 2 Let $\mathcal{X}$ be a closed set. If there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(\boldsymbol{x}) \leq \epsilon_2, & \forall \boldsymbol{x} \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall \boldsymbol{x} \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(f(x,d))] - v(x) \leq -\delta, & \forall x \in \mathcal{X}, \\ v(\boldsymbol{x}) \geq 1, & \forall \boldsymbol{x} \in \partial\widetilde{\mathcal{X}} \setminus \partial(\widetilde{\mathcal{X}} \setminus \mathcal{X}), \end{cases}$$

then
$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2$.

If $v(x)$ is bounded over $\widetilde{\mathcal{X}}$, it provides strong guarantees of leaving the safe set $\mathcal{X}$almost surely,
i.e., $\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right)$=0.

Equation Relaxation Based Method

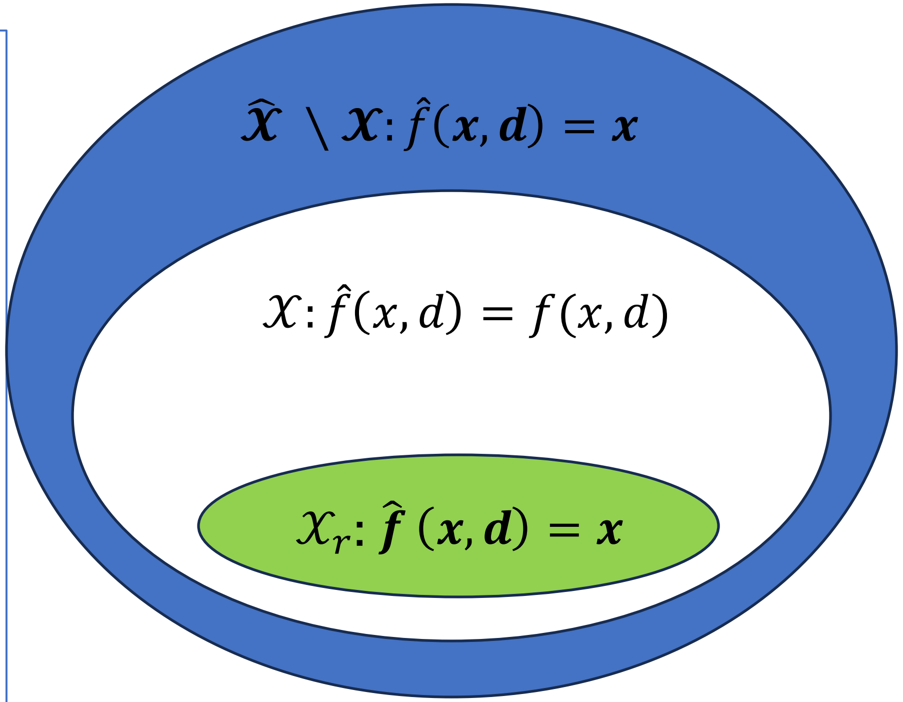
In [B. Xue, et. al., ACC 2021],
Given a safe set $\mathcal{X}$, a target set $\mathcal{X}_r$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_r, \mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x)$: $\widehat{\mathcal{X}} \to \mathbb{R}$ and $w(x)$: $\widehat{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) = \mathbb{E}\left[v\left(\hat{f}\,(x,d)\right)\right], \forall x \in \widehat{\mathcal{X}}, \\ v(x) = 1_{\mathcal{X}_r}(x) + \mathbb{E}\left[w\left(\hat{f}\,(x,d)\right)\right] - w(x), \forall x \in \widehat{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\exists k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X}_r \wedge \forall l \in [0,k].\ \phi_{\pi}^{x_0}(l) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) = v(x_0),$$

where $\hat{f}\,(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(x) + x \cdot 1_{\mathcal{X}_r}(x)$



B. Xue, R. Li, N. Zhan, and M. Fraenzle. Reach-avoid analysis for stochastic discrete-time systems. In 2021 American Control Conference (ACC), pages 4879–4885. IEEE, 2021

Equation Relaxation Based Method

In [B. Xue, et. al., ACC 2021],
Given a safe set $\mathcal{X}$, a target set $\mathcal{X}_r$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_r, \mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x)$: $\widehat{\mathcal{X}} \to \mathbb{R}$ and $w(x)$: $\widehat{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) = \mathbb{E}\left[v\left(\hat{f}\,(x,d)\right)\right], \forall x \in \widehat{\mathcal{X}}, \\ v(x) = 1_{\mathcal{X}_r}(x) + \mathbb{E}\left[w\left(\hat{f}\,(x,d)\right)\right] - w(x), \forall x \in \widehat{\mathcal{X}}. \end{cases}$$

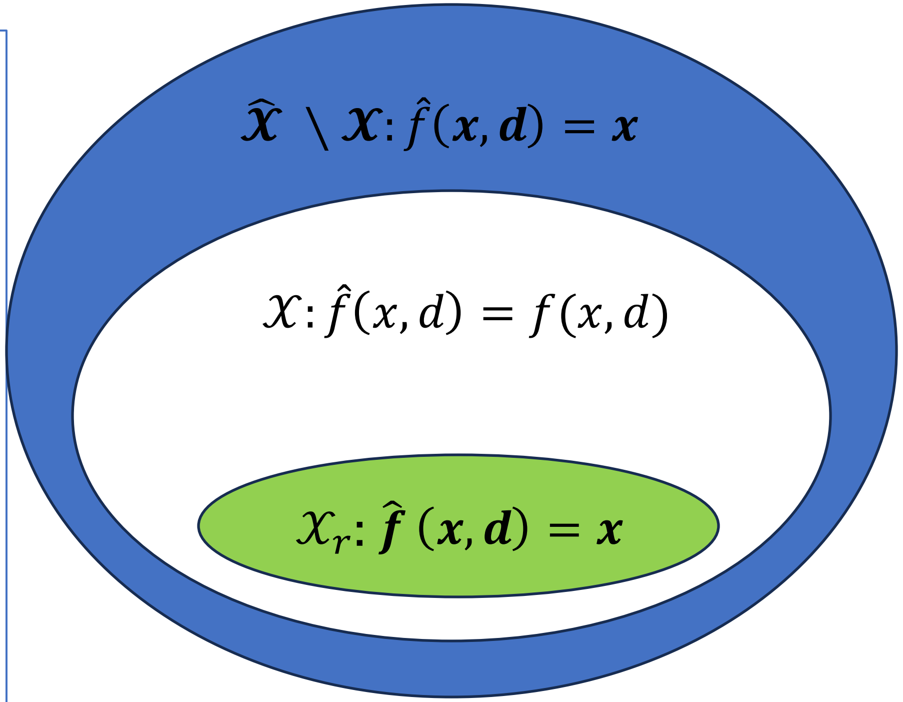
Then,

$$\mathbb{P}^{\infty}\left(\exists k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X}_r \wedge \forall l \in [0,k].\ \phi_{\pi}^{x_0}(l) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) = v(x_0),$$

where $\hat{f}\,(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\widehat{\mathcal{X}} \setminus \mathcal{X}}(x) + x \cdot 1_{\mathcal{X}_r}(x)$

$\widehat{\mathcal{X}}$ is a set containing the union of the set $\mathcal{X}$ and all reachable states starting from $\mathcal{X}$ within one step

$$\{x \mid x = f(x_0, d), x_0 \in \mathcal{X}, d \in \mathcal{D}\} \cup \mathcal{X} \subseteq \widehat{\mathcal{X}}$$



B. Xue, R. Li, N. Zhan, and M. Fraenzle. Reach-avoid analysis for stochastic discrete-time systems. In 2021 American Control Conference (ACC), pages 4879–4885. IEEE, 2021

Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x)\colon \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x)\colon \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

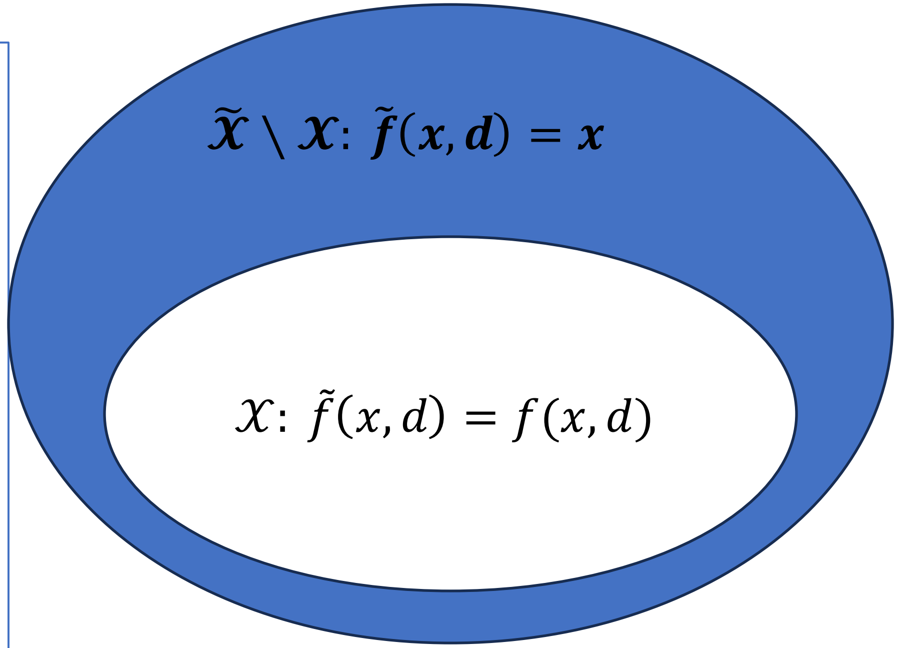
$$\begin{cases} v(x) = \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right], & \forall x \in \widetilde{\mathcal{X}}, \\ v(x) = 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x) + \mathbb{E}\left[w\left(\tilde{f}(x,d)\right)\right] - w(x), & \forall x \in \widetilde{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\exists k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \widetilde{\mathcal{X}} \setminus \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) = v(x_0).$$

Thus,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \phi_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) = 1 - v(x_0).$$



Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \le 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \ge \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right], & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}, \\ v(x) \ge 1_{\widetilde{\mathcal{X}} \setminus \mathcal{X}}(x) + \mathbb{E}\left[w\left(\tilde{f}(x,d)\right)\right] - w(x), & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \ge \epsilon_1.$$

Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right], & \forall x \in \widetilde{\mathcal{X}}, \\ v(x) \geq 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x) + \mathbb{E}\left[w\left(\tilde{f}(x,d)\right)\right] - w(x), & \forall x \in \widetilde{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

↓

$$\tilde{f}(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x)$$

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right], & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}, \\ v(x) \geq 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x) + \mathbb{E}\left[w\left(\tilde{f}(x,d)\right)\right] - w(x), & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \geq 1 - \epsilon_2, & \forall x \in \mathcal{X}_0, \\ v(x) \leq \mathbb{E}\left[v\left(\tilde{f}(x,d)\right)\right], & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}, \\ v(x) \leq 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x) + \mathbb{E}\left[w\left(\tilde{f}(x,d)\right)\right] - w(x), & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \leq \epsilon_2.$$

$$\tilde{f}(x,d) = f(x,d) \cdot 1_{\mathcal{X}}(x) + x \cdot 1_{\widetilde{\mathcal{X}}\setminus\mathcal{X}}(x)$$

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Theorem 4 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \geq 1 - \epsilon_2, & \forall x \in \mathcal{X}_0, \\ v(x) \leq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \leq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \leq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \leq \epsilon_2.$$

Comparison

Doob's Supermartingale Inequality Based Method

Theorem 1 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\pi}^{x_0}(k) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Equation Relaxation Based Method

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\pi}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Comparison

Doob's Supermartingale Inequality Based Method

Theorem 1 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exists $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x_0}}(k) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}_0 \right) \geq \epsilon_1.$$

⟺

Equation Relaxation Based Method

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x_0}}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \geq \epsilon_1.$$

Taoran Wu, Yiqing Yu, Bican Xia, Ji Wang and Bai Xue. A Framework for Safe Probabilistic Invariance Verification of Stochastic Dynamical Systems. Arxiv, 2024.

Comparison

Doob's Supermartingale Inequality Based Method

Theorem 1 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Equation Relaxation Based Method

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Sufficient and Necessary Barrier-like Conditions

Bai Xue. Sufficient and Necessary Barrier-like Conditions for Safety and Reach-avoid Verification of Stochastic Discrete-time Systems. Arxiv, 2024.

Comparison

Doob's Supermartingale Inequality Based Method

Theorem 1 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exists $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Theorem 2 Let $\mathcal{X}$ be a closed set. If there exists $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq \epsilon_2, & \forall x \in \mathcal{X}_0, \\ \mathbb{E}[v(f(x,d))] - v(x) \leq -\delta, & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \partial\widetilde{\boldsymbol{\mathcal{X}}} \setminus \partial(\widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}), \\ v(x) \geq 0, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \leq \epsilon_2.$$

Equation Relaxation Based Method

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Theorem 4 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ and $w(x): \widetilde{\boldsymbol{\mathcal{X}}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \geq 1-\epsilon_2, & \forall x \in \mathcal{X}_0, \\ v(x) \leq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \leq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \leq 1, & \forall x \in \widetilde{\boldsymbol{\mathcal{X}}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^{\infty}\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \leq \epsilon_2.$$

Bai Xue. Sufficient and Necessary Barrier-like Conditions for Safety and Reach-avoid Verification of Stochastic Discrete-time Systems . Arxiv, 2024.

Comparison

Doob's Supermartingale Inequality Based Method

Theorem 1 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}, \\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{\boldsymbol{x}_0}(k) \in \mathcal{X} \mid \boldsymbol{x}_0 \in \mathcal{X}_0 \right) \geq \epsilon_1.$$

Theorem 2 Let $\mathcal{X}$ be a closed set. If there exists $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq \epsilon_2, & \forall x \in \mathcal{X}_0, \\ \mathbb{E}[v(f(x,d))] - v(x) \leq -\delta, & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \partial\widetilde{\mathcal{X}} \setminus \partial(\widetilde{\mathcal{X}} \setminus \mathcal{X}), \\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}, \end{cases}$$

then

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2.$$

Equation Relaxation Based Method

Theorem 3 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \geq \epsilon_1.$$

Theorem 4 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist bounded functions $v(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ and $w(x): \widetilde{\mathcal{X}} \to \mathbb{R}$ such that

$$\begin{cases} v(x) \geq 1-\epsilon_2, & \forall x \in \mathcal{X}_0, \\ v(x) \leq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X}, \\ v(x) \leq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X}, \\ v(x) \leq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}, \end{cases}$$

then
$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \boldsymbol{\phi}_{\boldsymbol{\pi}}^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) \leq \epsilon_2.$$

$$1 - v(x) \text{ with } w(x) = M\big(1 - v(x)\big), \text{ where } M\delta \geq \sup_{x \in \widetilde{\mathcal{X}}} 1 - v(x)$$

Optimization

Doob's Supermartingale Inequality Based Method

Op1 $\quad \mathrm{Max}_v\ \epsilon_1$

$$\text{s.t.}\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0,\\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}},\\ \mathbb{E}[v(f(x,d))] \leq v(x), & \forall x \in \mathcal{X},\\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}.\end{cases}$$

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Op2 $\quad \mathrm{Min}_v\ \epsilon_2$

$$\text{s.t.}\begin{cases} v(x) \leq \epsilon_2, & \forall x \in \mathcal{X}_0,\\ \mathbb{E}[v(f(x,d))] - v(x) \leq -\delta, & \forall x \in \mathcal{X},\\ v(x) \geq 1, & \forall x \in \partial\widetilde{\mathcal{X}} \setminus \partial(\widetilde{\mathcal{X}} \setminus \mathcal{X}),\\ v(x) \geq 0, & \forall x \in \widetilde{\mathcal{X}}.\end{cases}$$

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \leq \epsilon_2.$$

Equation Relaxation Based Method

Op3 $\quad \mathrm{Max}_{v,w}\ \epsilon_1$

$$\text{s.t.}\begin{cases} v(x) \leq 1-\epsilon_1, & \forall x \in \mathcal{X}_0,\\ v(x) \geq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X},\\ v(x) \geq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X},\\ v(x) \geq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}.\end{cases}$$

$$\mathbb{P}^\infty\left(\forall k \in \mathbb{N}.\ \phi_\pi^{x_0}(k) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\right) \geq \epsilon_1.$$

Op4 $\quad \mathrm{Min}_{v,w}\ \epsilon_2$

$$\text{s.t.}\begin{cases} v(x) \geq 1-\epsilon_2, & \forall x \in \mathcal{X}_0,\\ v(x) \leq \mathbb{E}[v(f(x,d))], & \forall x \in \mathcal{X},\\ v(x) \leq \mathbb{E}[w(f(x,d))] - w(x), & \forall x \in \mathcal{X},\\ v(x) \leq 1, & \forall x \in \widetilde{\mathcal{X}} \setminus \mathcal{X}.\end{cases}$$

$$\mathbb{P}^\infty\left(\forall \mathrm{k} \in \mathbb{N}.\ \phi_\pi^{\mathrm{x}_0}(\mathrm{k}) \in \mathcal{X} \mid \mathrm{x}_0 \in \mathcal{X}_0\right) \leq \epsilon_2.$$

They were relaxed into semi-definite programming problems

Example

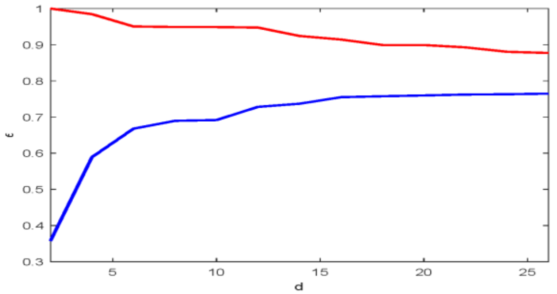
Consider

$$x(l+1) = \big(-0.5 + d(l)\big)x(l)$$

- $d(\cdot): \mathbb{N} \to \mathcal{D} = [-1,1]$ （**uniform distribution**）
- $\mathcal{X} = \{x \mid x^2 - 1 \leq 0\}$
- $\mathcal{X}_0 = \{x \mid (x+0.8)^2 = 0\}$ (i.e., $x_0 = -0.8$)
- $\widehat{\mathcal{X}} = \{x \mid x^2 - 2 \leq 0\}$

The lower and upper bounds of the safety probability obtained by Monte Carlo are $\epsilon_1 = \epsilon_2 = 0.8312$

Op3 and Op4													
d	2	4	6	8	10	12	14	16	18	20	22	24	26
ϵ_1	0.3574	0.5890	0.6678	0.6895	0.6917	0.7281	0.7368	0.7549	0.7575	0.7597	0.7622	0.7630	0.7647
ϵ_2	1.0000	0.9844	0.9505	0.9489	0.9488	0.9474	0.9242	0.9143	0.8991	0.8991	0.8927	0.8804	0.8771
Op1													
ϵ_1	0.3574	0.5890	0.6678	0.6895	0.6917	0.7281	0.7368	0.7549	0.7575	0.7597	0.7622	0.7630	0.7647



Safe Probabilistic Invariance Verification of Stochastic Continuous-time Systems

Stochastic continuous-time systems modeled by time-homogeneous SDEs:

$$d\boldsymbol{X}(t,\boldsymbol{w}) = \boldsymbol{b}\big(\boldsymbol{X}(t,\boldsymbol{w})\big)dt + \boldsymbol{\sigma}\big(\boldsymbol{X}(t,\boldsymbol{w})\big)d\boldsymbol{W}(t,\boldsymbol{w}), t \geq 0$$

Its trajectory

$$X^{x_0}(\cdot,w)\colon \big[0, T^{x_0}(w)\big) \times \Omega \to R^n$$

satisfies

$$X^{x_0}(t,w) = x_0 + \int_0^t b(X^{x_0}(s,w)ds + \int_0^t \sigma(X^{x_0}(s,w)dW(s,w)$$

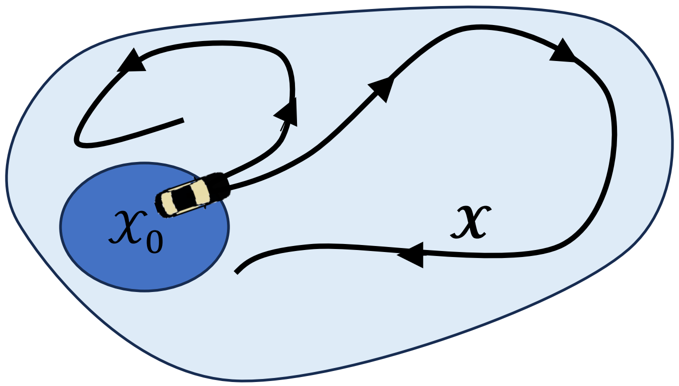
Bai Xue, Naijun Zhan and Martin Fränzle. Reach-Avoid Analysis for Polynomial Stochastic Differential Equations. IEEE Transactions on Automatic Control(IEEE TAC), 69(3): 1882--1889, 2024.

Given a safe set $\mathcal{X}$ (bounded and open) and an initial set $\mathcal{X}_0 \subseteq \mathcal{X}$,

the safe probabilistic invariance verification is to compute lower and upper bounds, denoted by $\epsilon_1 \in [0,1]$ and $\epsilon_2 \in [0,1]$ respectively, for the safety probability that the system, starting from any state in $\mathcal{X}_0$, will remain inside the safe set $\mathcal{X}$ for all time, i.e.,

to compute ϵ_1 and ϵ_2 such that

$$\epsilon_1 \leq \mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}. X^{x_0}(t,w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \leq \epsilon_2.$$



Doob's Supermartingale Inequality Based Method

Doob's Supermartingale Inequality [J. Ville, 1939]

Let $(\Omega_1, \mathcal{F}, \mathbb{P}_1)$ be the probability space and $\{B_i\}_{i\in\mathbb{N}}$ be a non-negative supermartingale, then for $b > 0$,

$$\mathbb{P}_1\left(\sup_{i\in\mathbb{N}} B_i \geq b \mid B_0\right) \leq \frac{B_0}{b}$$

In [S. Prajna, et. al., 2007(IEEE TAC)],
Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \leq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \geq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \geq 0, & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \geq \epsilon_1.$$

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, 52(8):1415–1428, 2007.

Doob’s Supermartingale Inequality Based Method

Doob’s Supermartingale Inequality [J. Ville, 1939]

Let $(\Omega_1, \mathcal{F}, \mathbb{P}_1)$ be the probability space and $\{B_i\}_{i\in\mathbb{N}}$ be a non-negative supermartingale, then for $b > 0$,

$$\mathbb{P}_1\left(\sup_{i\in\mathbb{N}} B_i \geq b \mid B_0\right) \leq \frac{B_0}{b}$$

In [S. Prajna, et. al., 2007(IEEE TAC)],
Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \leq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \geq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \geq 0, & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \geq \epsilon_1.$$

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, 52(8):1415–1428, 2007.

There are **no barrier-like conditions** based on the Doob’s nonnegative supermartingale inequality that have been developed in previous studies to **examine upper bounds of the reachability probability**

Equation Relaxation Based Method

In [B. Xue, et. al., 2024(IEEE TAC)],
Given a safe set $\mathcal{X}$, a target set $\mathcal{X}_r$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_r, \mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

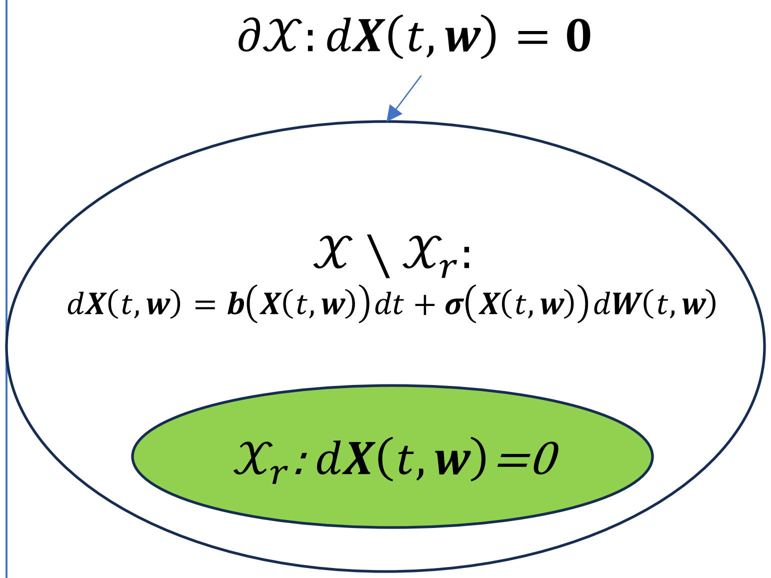
$$\begin{cases} \tilde{\mathcal{A}}v(x) = 0, \forall x \in \overline{\mathcal{X}}, \\ v(x) = 1_{\mathcal{X}_r}(x) + \tilde{\mathcal{A}}u(x), \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\exists \tau \in \mathbb{R}_{\geq 0}. X^{x_0}(\tau, w) \in \mathcal{X}_r \wedge \forall t \in [0,\tau].\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) = v(x_0),$$

where

$$\tilde{\mathcal{A}}v(x) = \begin{cases} \mathcal{A}v(x)\left(= \frac{\partial v(x)}{\partial x} b(x) + \frac{1}{2} tr(\sigma^{\top}(x) \frac{\partial^2 v(x)}{\partial x^2} \sigma(x))\right), & if\ x \in \mathcal{X} \setminus \mathcal{X}_r, \\ 0, & if\ x \in \partial\mathcal{X} \cup \mathcal{X}_r. \end{cases}$$



B. Xue, N. Zhan, and M. Fraenzle. Reach-avoid analysis for polynomial stochastic differential equations. IEEE Transactions on Automatic Control, 69(3):1882–1889, 2024.

Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

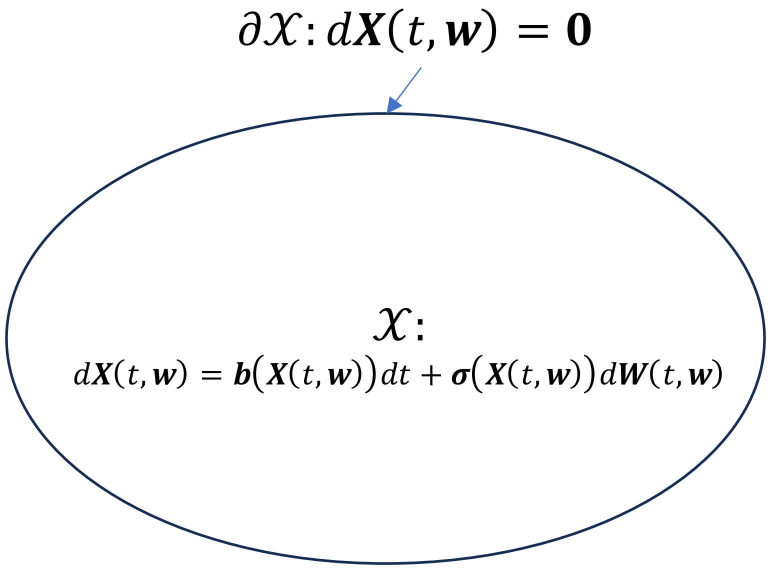
$$\begin{cases} \tilde{\mathcal{A}} v(x) = 0, \forall x \in \overline{\mathcal{X}}, \\ v(x) = 1_{\partial \mathcal{X}}(x) + \tilde{\mathcal{A}} u(x), \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}\left(\exists \tau \in \mathbb{R}_{\geq 0}. X^{x_0}(\tau, w) \in \partial \mathcal{X} \wedge \forall t \in [0, \tau).\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) = v(x_0).$$

Thus,

$$\mathbb{P}\left(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0 \right) = 1 - v(x_0).$$



Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \tilde{\mathcal{A}}v(x) \leq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \geq 1_{\partial \mathcal{X}}(x) + \tilde{\mathcal{A}}u(x), & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\, \forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\,) \geq \epsilon_1.$$

Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \tilde{\mathcal{A}}v(x) \leq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \geq 1_{\partial\mathcal{X}}(x) + \tilde{\mathcal{A}}u(x), & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\ \forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\ ) \geq \epsilon_1.$$

$$\tilde{\mathcal{A}}u(x) = \tilde{\mathcal{A}}v(x) = 0 \qquad \forall x \in \partial\mathcal{X}$$

Theorem 6 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \leq 0, & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \geq \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}(\ \forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\ ) \geq \epsilon_1.$$

Equation Relaxation Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \tilde{\mathcal{A}}v(x) \leq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \geq 1_{\partial\mathcal{X}}(x) + \tilde{\mathcal{A}}u(x), & \forall x \in \overline{\mathcal{X}}, \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \geq \epsilon_1.$$

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \geq 1 - \epsilon_2, & \forall x \in \mathcal{X}_0, \\ \tilde{\mathcal{A}}v(x) \geq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \leq 1_{\partial\mathcal{X}}(x) + \tilde{\mathcal{A}}u(x), & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \leq \epsilon_2.$$

$$\tilde{\mathcal{A}}u(x) = \tilde{\mathcal{A}}v(x) = 0 \qquad \forall x \in \partial\mathcal{X}$$

Theorem 6 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \leq 0, & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \geq \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \geq \epsilon_1.$$

Theorem 7 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \geq 1 - \epsilon_2, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \geq 0, & \forall x \in \mathcal{X}, \\ v(x) \leq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \leq \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \leq \epsilon_2.$$

Comparison

Doob's Supermartingale Inequality Based Method

Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \leq 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \geq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \geq 0, & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \geq \epsilon_1.$$

Equation Relaxation Based Method

Theorem 6 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \leq 1 - \epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \leq 0, & \forall x \in \mathcal{X}, \\ v(x) \geq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \geq \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \geq \epsilon_1.$$

Theorem 7 Given a safe set $\mathcal{X}$ and an initial set $\mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$, if there exist $v(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ and $u(x) \in \mathcal{C}^2(\overline{\mathcal{X}})$ such that

$$\begin{cases} v(x) \geq 1 - \epsilon_2, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \geq 0, & \forall x \in \mathcal{X}, \\ v(x) \leq 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \leq \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

Then,

$$\mathbb{P}(\forall t \in \mathbb{R}_{\geq 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0) \leq \epsilon_2.$$

Optimization

Doob's Supermartingale Inequality Based Method

Op5 $\quad \mathrm{Max}_{v}\ \epsilon_1$

$$\text{s.t.} \begin{cases} v(x) \le 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \le 0, & \forall x \in \overline{\mathcal{X}}, \\ v(x) \ge 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \ge 0, & \forall x \in \overline{\mathcal{X}}. \end{cases}$$

$$\mathbb{P}(\ \forall t \in \mathbb{R}_{\ge 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\ ) \ge \epsilon_1$$

Equation Relaxation Based Method

Op6 $\quad \mathrm{Max}_{v,u}\ \epsilon_1$

$$\text{s.t.} \begin{cases} v(x) \le 1-\epsilon_1, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \le 0, & \forall x \in \mathcal{X}, \\ v(x) \ge 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \ge \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

$$\mathbb{P}(\ \forall t \in \mathbb{R}_{\ge 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\ ) \ge \epsilon_1$$

Op7 $\quad \mathrm{Min}_{v,u}\ \epsilon_2$

$$\text{s.t.} \begin{cases} v(x) \ge 1-\epsilon_2, & \forall x \in \mathcal{X}_0, \\ \mathcal{A}v(x) \ge 0, & \forall x \in \mathcal{X}, \\ v(x) \le 1, & \forall x \in \partial\mathcal{X}, \\ v(x) \le \mathcal{A}u(x), & \forall x \in \mathcal{X}. \end{cases}$$

$$\mathbb{P}(\ \forall t \in \mathbb{R}_{\ge 0}.\ X^{x_0}(\tau, w) \in \mathcal{X} \mid x_0 \in \mathcal{X}_0\ ) \le \epsilon_2$$

They were relaxed into semi-definite programming problems

Example

Consider the stochastic differential equation:

$$\begin{cases} dX_1(t,w) = X_2(t,w)dt, \\ dX_2(t,w) = -\left(X_1(t,w) + X_2(t,w) + 0.5X_1^3(t,w)\right)dt + \left(X_1(t,w) + X_2(t,w)\right)dW(t,w). \end{cases}$$

- the safe set is $\mathcal{X} = \{(x_1, x_2) \mid x_1^2 + x_2^2 - 1 < 0\}$
- the initial set is $\mathcal{X}_0 = \{(x_1, x_2) \mid 100(x_1 + 0.4)^2 + 100(x_2 + 0.5)^2 - 1 < 0\}$

The lower and upper bounds of the safety probability obtained by Monte Carlo are

$\epsilon_1 = 0.5338$

$\epsilon_2 = 0.7101$

Op6 and Op7							
d	4	6	8	10	12	14	16
ϵ_1	0.3957	0.4217	0.4590	0.4660	0.4675	0.4682	0.4686
ϵ_2	0.7313	0.7279	0.7233	0.7224	0.7216	0.7213	0.7208
Op5							
ϵ_1	0.3957	0.4217	0.4590	0.4660	0.4675	0.4682	0.4686

Conclusion

Two sets of optimizations for computing lower and upper bounds of the safety probability are proposed.

1. The first one is based on Doob's supermartingale inequality.
2. The second one is based on relaxing an equation that characterizes the exact reachability probability.

Papers

- Yiqing Yu, Taoran Wu, Bican Xia, Ji Wang, Bai Xue. Safe Probabilistic Invariance Verification for Stochastic Discrete-time Dynamical Systems. CDC 2023, pp. 5804--5811, 2023.
- Taoran Wu, Yiqing Yu, Bican Xia, Ji Wang and Bai Xue. A Framework for Safe Probabilistic Invariance Verification of Stochastic Dynamical Systems. Arxiv, 2024.
- Bai Xue, Renjue Li, Naijun Zhan and Martin Fraenzle. Reach-avoid Analysis for Stochastic Discrete-time Systems. In Proceedings of the 2021 American Control Conference (ACC 2021), pp. 4879-4885, 2021.
- Bai Xue. Sufficient and Necessary Barrier-like Conditions for Safety and Reach-avoid Verification of Stochastic Discrete-time Systems . Arxiv, 2024.
- Bai Xue, Naijun Zhan and Martin Fraenzle. Reach-Avoid Analysis for Polynomial Stochastic Differential Equations. IEEE Transactions on Automatic Control(IEEE TAC), 69(3): 1882--1889, 2024.

Extensions

- Bai Xue. Finite-time Safety and Reach-avoid Verification of Stochastic Discrete-time Systems. Arxiv, 2024.
- Bai Xue. A New Framework for Bounding Reachability Probabilities of Continuous-time Stochastic Systems. Arxiv, 2023.
- Bai Xue. Safe Exit Controllers Synthesis for Continuous-time Stochastic Systems. CDC 2024, 2024.
- Bai Xue. Reach-avoid Controllers Synthesis for Safety Critical Systems. IEEE Transactions on Automatic Control(IEEE TAC), 2024.

Thanks for Your Attention!