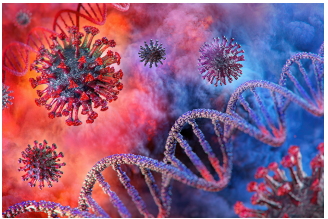
Data-Driven Safety Verification of Unknown Systems with Formal Guarantees

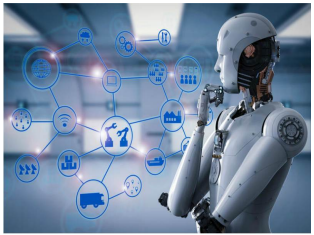
Abolfazl Lavaei
School of Computing, Newcastle University, UK

Workshop on Data-Driven Verification and Control of Cyber-Physical Systems
IFAC World Congress 2023

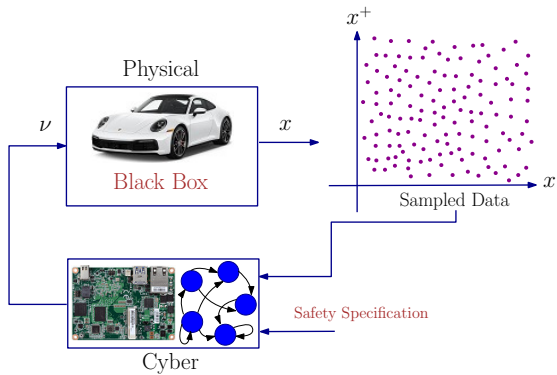
Data-Driven Control Approaches

- Data-driven systems are crucial everywhere from machines to environment and society



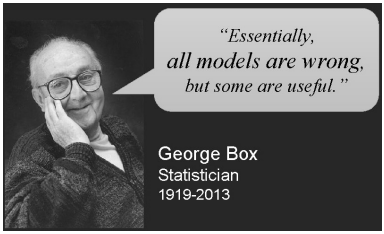


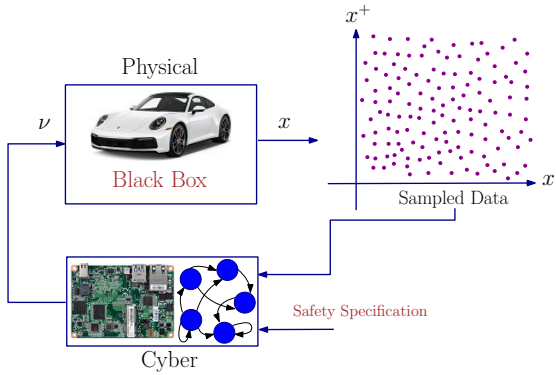
Data-Driven Analysis with Provable Guarantees



Data-Driven Analysis with Provable Guarantees

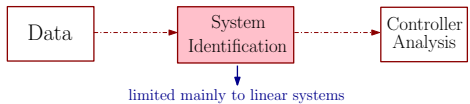
- Closed-form mathematical models: not available or too complex to be used
- Model-based techniques are not applicable





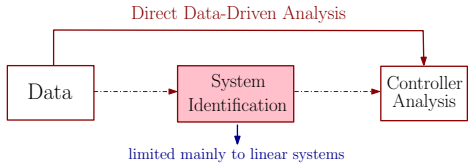
Data-Driven Analysis: Indirect and Direct Methods

- Indirect data-driven techniques: System identification followed by model-based methods
  - complicated and expensive
  - two-level computational complexity



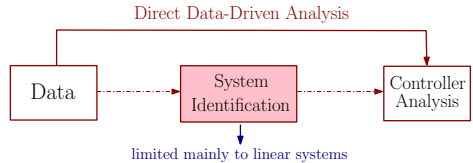
Data-Driven Analysis: Indirect and Direct Methods

- Indirect data-driven techniques: System identification followed by model-based methods
  - complicated and expensive
  - two-level computational complexity
- Direct data-driven techniques: Bypass system identification and directly employ system measurements



Data-Driven Analysis: Indirect and Direct Methods

- Indirect data-driven techniques: System identification followed by model-based methods
  - complicated and expensive
  - two-level computational complexity
- Direct data-driven techniques: Bypass system identification and directly employ system measurements

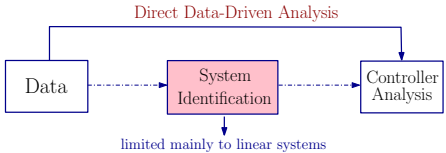


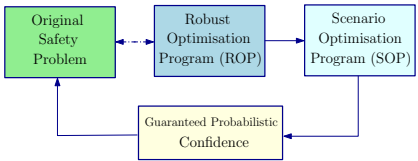
Question of interest

How to provide safety certificates using direct data-driven techniques for general class of nonlinear systems with unknown models?

Data-Driven Analysis: Our Proposed Framework

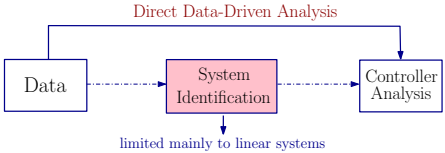
- Cast original safety problem as an ROP
- Provide SOP corresponding to ROP
- Establish a probabilistic relation between optimal values of SOP (η_S^*) and ROP (η_R^*) with a threshold ε
- Quantify an a-priori guaranteed confidence over safety of unknown systems





Data-Driven Analysis: Our Proposed Framework

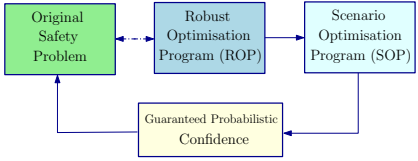
- Cast original safety problem as an ROP
- Provide SOP corresponding to ROP
- Establish a probabilistic relation between optimal values of SOP (η_S^*) and ROP (η_R^*) with a threshold ε
- Quantify an a-priori guaranteed confidence over safety of unknown systems



Theorem (guaranteed confidence)

If $\eta_S^* + \varepsilon \leq 0$, then

$$\mathbb{P}\Big\{\text{Black-box system} \vDash \text{safety}\Big\} \geq 1 - \beta, \quad \beta \in [0, 1]$$



SOP Solving

- Linear programing / mixed-integer linear programing via solver Mosek

Collaborators

[1] A. Nejati, A. Lavaei, P. Jagtap, S. Soudjani, M. Zamani, “Formal Verification of Unknown Discrete- and Continuous-Time Systems: A Data-Driven Approach", ***IEEE Transactions on Automatic Control - Special Issue on Learning for Control (Full paper)***, 2023.

[2] A. Salamati, A. Lavaei, S. Soudjani, M. Zamani, “Data-Driven Verification and Synthesis of Stochastic Systems via Barrier Certificates", ***Automatica (Full paper)***, 2023.

Ameneh Nejati: Incoming Assistant Professor at Newcastle University, UK

Sadegh Soudjani: Associate Professor at Newcastle University, UK

Pushpak Jagtap: Assistant Professor at IISc Bangalore, India

Majid Zamani: Associate Professor at CU Boulder, US

Ali Salamati: PhD Graduate from LMU Munich, Germany

Outline

Data-driven safety verification of unknown systems:

- Discrete-time systems

$$\Sigma_d \colon x(k+1) = f(x(k))$$

- Continuous-time systems

$$\Sigma_c \colon \dot{x}(t) = f(x(t))$$

- Discrete-time stochastic systems

$$\Sigma_d \colon x(k+1) = f(x(k), \varsigma(k))$$

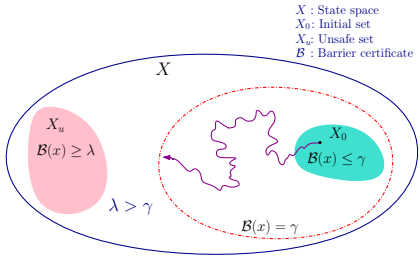
- Continuous-time stochastic systems

$$\Sigma_c \colon \mathrm{d}x(t) = f(x(t))\mathrm{d}t + \sigma(x(t))\mathrm{d}\mathbb{W}_t$$

Barrier Certificate (BC)

Safety property

Given $\Sigma_d : x(k+1) = f(x(k))$ and safety specification $\varphi = (X_0, X_u, \mathcal{T})$, where $X_0, X_u \subseteq X$, Σ_d is called safe within infinite time horizon $\mathcal{T}$, denoted by $\Sigma \models \varphi$, if all trajectories of Σ_d started from $X_0 \subseteq X$ never reach $X_u \subseteq X$.



Initial works:

- S. Prajna and A. Jadbabaei, “Safety Verification of Hybrid Systems using Barrier Certificates”, *ACM HSCC*, 2004. (HSCC Test-of-Time Award - CPS-IoT Week 2021)
- S. Prajna, A. Jadbabaei, G. J. Pappas, ”A Framework for Worst-case and Stochastic Safety Verification using Barrier Certificates”, *IEEE TAC*, 2007.

Barrier Certificate (BC)

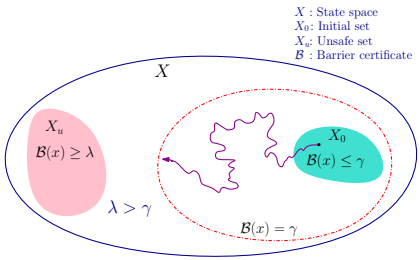
Safety property

Given $\Sigma_d : x(k+1) = f(x(k))$ and safety specification $\varphi = (X_0, X_u, \mathcal{T})$, where $X_0, X_u \subseteq X$, Σ_d is called safe within infinite time horizon $\mathcal{T}$, denoted by $\Sigma \models \varphi$, if all trajectories of Σ_d started from $X_0 \subseteq X$ never reach $X_u \subseteq X$.

Barrier Certificate: Verification Problem

If there exist a function $\mathcal{B} : X \to \mathbb{R}$ and constants $\gamma, \lambda \in \mathbb{R}$, with $\lambda > \gamma$, such that:

- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma$,
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda$,
- $\forall x \in X$: $\mathcal{B}(f(x)) \leq \mathcal{B}(x)$,



Initial works:

- S. Prajna and A. Jadbabaei, "Safety Verification of Hybrid Systems using Barrier Certificates", *ACM HSCC*, 2004. (HSCC Test-of-Time Award - CPS-IoT Week 2021)
- S. Prajna, A. Jadbabaei, G. J. Pappas, "A Framework for Worst-case and Stochastic Safety Verification using Barrier Certificates", *IEEE TAC*, 2007.

Barrier Certificate (BC)

Safety property

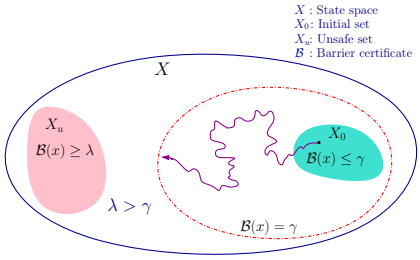
Given $\Sigma_d : x(k+1) = f(x(k))$ and safety specification $\varphi = (X_0, X_u, \mathcal{T})$, where $X_0, X_u \subseteq X$, Σ_d is called safe within infinite time horizon $\mathcal{T}$, denoted by $\Sigma \models \varphi$, if all trajectories of Σ_d started from $X_0 \subseteq X$ never reach $X_u \subseteq X$.

Barrier Certificate: Verification Problem

If there exist a function $\mathcal{B} : X \to \mathbb{R}$ and constants $\gamma, \lambda \in \mathbb{R}$, with $\lambda > \gamma$, such that:

- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma$,
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda$,
- $\forall x \in X$: $\mathcal{B}(f(x)) \leq \mathcal{B}(x)$,

Then $\Sigma_d \models \varphi$.



Computation of BC

- Sum-of-squares (SOS) optimization: SOSTOOLS, SDP solver SeDuMi
- Counter-example guided inductive synthesis (CEGIS): SMT solvers such as Z3, dReal

Initial works:

- S. Prajna and A. Jadbabaei, "Safety Verification of Hybrid Systems using Barrier Certificates", *ACM HSCC*, 2004. (HSCC Test-of-Time Award - CPS-IoT Week 2021)
- S. Prajna, A. Jadbabaei, G. J. Pappas, "A Framework for Worst-case and Stochastic Safety Verification using Barrier Certificates", *IEEE TAC*, 2007.

Data-Driven Construction of BC

Robust Optimization Program (ROP)

$$\Sigma_d : x(k+1) = f(x) \qquad \mathcal{B}(q, x) = \sum_{j=1}^{z} q_j p_j(x)$$

Data-Driven Construction of BC

Robust Optimization Program (ROP)

$$\Sigma_d : x(k+1) = f(x) \qquad \mathcal{B}(q,x) = \sum_{j=1}^{z} q_j p_j(x)$$

$$\text{ROP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, & \forall x \in X_u, \\ & \mathcal{B}(q,f(x)) - \mathcal{B}(q,x) \leq \eta, & \forall x \in X, \\ & d = [\gamma; \lambda; q_1; \ldots; q_z], & \eta, \gamma, \lambda \in \mathbb{R} \end{cases}$$

Data-Driven Construction of BC

Robust Optimization Program (ROP)

$$\Sigma_d : x(k+1) = f(x) \qquad \mathcal{B}(q,x) = \sum_{j=1}^{z} q_j p_j(x)$$

$$\text{ROP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \le \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \le \eta, & \forall x \in X_u, \\ & \mathcal{B}(q,f(x)) - \mathcal{B}(q,x) \le \eta, & \forall x \in X, \\ & d = [\gamma;\lambda;q_1;\ldots;q_z], & \eta,\gamma,\lambda \in \mathbb{R} \end{cases}$$

Scenario Optimization Program (SOP)

Let $(\hat{x}_i)_{i=1}^{M}$ denote M i.i.d. data sampled within X

$$\text{SOP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \le \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \le \eta, & \forall x \in X_u, \\ & \mathcal{B}(q,f(\hat{x}_i)) - \mathcal{B}(q,\hat{x}_i) \le \eta, & \forall \hat{x}_i \in X, \forall i \in \{1,\ldots,M\}, \\ & d = [\gamma;\lambda;q_1;\ldots;q_z], & \eta,\gamma,\lambda \in \mathbb{R} \end{cases}$$

Relation between SOP and Original ROP

Theorem (out-of-sample performance guarantees)

Consider an unknown system Σ_d and the corresponding SOP with its associated optimal value η_S^* and solution d^*, with

$$M(\varepsilon,\beta) := \min\left\{M \in \mathbb{N} \,|\, \sum_{i=0}^{c-1} \binom{M}{i} \varepsilon^i (1-\varepsilon)^{M-i} \leq \beta\right\}.$$

If

$$\eta_S^* + \varepsilon \leq 0,$$

then the solution d^* is a feasible solution for original ROP, *i.e.,* $d^* \models$ ROP, with a confidence of at least $1-\beta$.

Relation between SOP and Original ROP

Theorem (out-of-sample performance guarantees)

Consider an unknown system Σ_d and the corresponding SOP with its associated optimal value η_S^* and solution d^*, with

$$M(\varepsilon,\beta) := \min\Big\{M \in \mathbb{N} \,|\, \sum_{i=0}^{c-1} \binom{M}{i} \varepsilon^i (1-\varepsilon)^{M-i} \leq \beta\Big\}.$$

If

$$\eta_S^* + \varepsilon \leq 0,$$

then the solution d^* is a feasible solution for original ROP, *i.e.,* $d^* \models$ ROP, with a confidence of at least $1-\beta$.

Require: $\varepsilon, \beta \in [0,1]$ and degree of barrier certificate

1: Compute the M based on ε, β

2: Solve the SOP with acquired M and obtain η_S^*

Ensure: if $\eta_S^* + \varepsilon \leq 0$, then $d^* \models$ ROP, and accordingly $\Sigma_d \models \varphi$, with a confidence of at least $1-\beta$

Case Study: DC Motor

- Σ_d: $\begin{cases} x_1(k+1) = x_1(k) + \tau(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)) \\ x_2(k+1) = x_2(k) + \tau(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)) \end{cases}$

Case Study: DC Motor

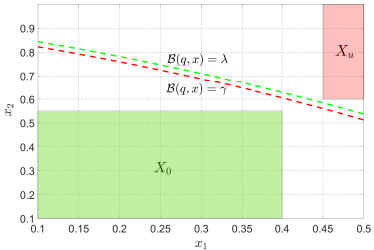
- Σ_d: $\begin{cases} x_1(k+1) = x_1(k) + \tau(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)) \\ x_2(k+1) = x_2(k) + \tau(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)) \end{cases}$
- Regions of interest: $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, $X_u = [0.45, 0.5] \times [0.6, 1]$

Case Study: DC Motor

- Σ_d: $\begin{cases} x_1(k+1) = x_1(k) + \tau(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)) \\ x_2(k+1) = x_2(k) + \tau(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)) \end{cases}$
- Regions of interest: $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, $X_u = [0.45, 0.5] \times [0.6, 1]$
- $\mathcal{B}(q, x) = 0.5x_1^2 + 0.5x_1x_2 + 0.5x_2^2 + 0.5$
- $\eta_S^* = -0.0155$, $\eta_S^* + \varepsilon = -5 \times 10^{-4} \leq 0$
- Unknown DC motor is safe with confidence of 99%

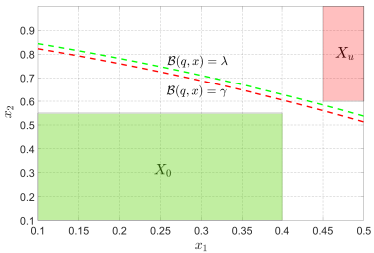
Case Study: DC Motor

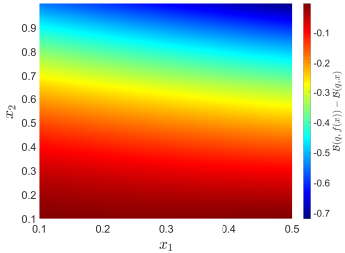
- Σ_d: $\begin{cases} x_1(k+1) = x_1(k) + \tau(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)) \\ x_2(k+1) = x_2(k) + \tau(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)) \end{cases}$
- Regions of interest: $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, $X_u = [0.45, 0.5] \times [0.6, 1]$
- $\mathcal{B}(q, x) = 0.5x_1^2 + 0.5x_1x_2 + 0.5x_2^2 + 0.5$
- $\eta_S^* = -0.0155$, $\eta_S^* + \varepsilon = -5 \times 10^{-4} \leq 0$
- Unknown DC motor is safe with confidence of 99%



Case Study: DC Motor

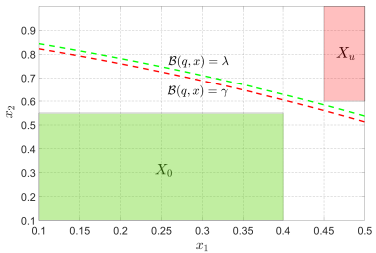
- Σ_d: $\begin{cases} x_1(k+1) = x_1(k) + \tau(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)) \\ x_2(k+1) = x_2(k) + \tau(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)) \end{cases}$
- Regions of interest: $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, $X_u = [0.45, 0.5] \times [0.6, 1]$
- $\mathcal{B}(q, x) = 0.5x_1^2 + 0.5x_1x_2 + 0.5x_2^2 + 0.5$
- $\eta_S^* = -0.0155$, $\eta_S^* + \varepsilon = -5 \times 10^{-4} \leq 0$
- Unknown DC motor is safe with confidence of 99%

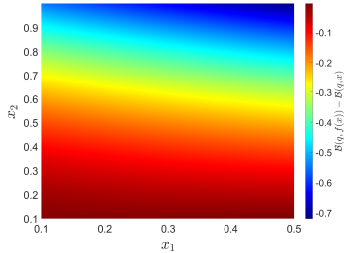


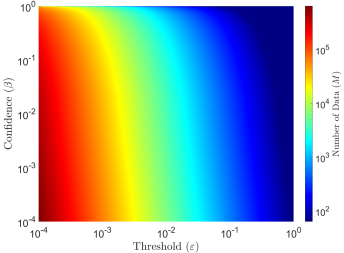


Case Study: DC Motor

- Σ_d: $\begin{cases} x_1(k+1) = x_1(k) + \tau(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)) \\ x_2(k+1) = x_2(k) + \tau(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)) \end{cases}$
- Regions of interest: $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, $X_u = [0.45, 0.5] \times [0.6, 1]$
- $\mathcal{B}(q, x) = 0.5x_1^2 + 0.5x_1x_2 + 0.5x_2^2 + 0.5$
- $\eta_S^* = -0.0155$, $\eta_S^* + \varepsilon = -5 \times 10^{-4} \leq 0$
- Unknown DC motor is safe with confidence of 99%







Data-Driven Construction of BC: Continuous-Time Systems

- $\Sigma_c : \dot{x}(t) = f(x(t))$
- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma$,
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda$,
- $\forall x \in X$: $\mathsf{L}_f \mathcal{B}(x) = \partial_x \mathcal{B}(x) f(x) \leq 0$,

Data-Driven Construction of BC: Continuous-Time Systems

- $\Sigma_c : \dot{x}(t) = f(x(t))$
- $\forall x \in X_0$: $\quad \mathcal{B}(x) \leq \gamma,$
- $\forall x \in X_u$: $\quad \mathcal{B}(x) \geq \lambda,$
- $\forall x \in X$: $\quad \mathsf{L}_f \mathcal{B}(x) = \partial_x \mathcal{B}(x) f(x) \leq 0,$

Robust Optimization Program (ROP)

$$\text{ROP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, \qquad \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, \qquad \forall x \in X_u, \\ & \mathsf{L}_f \mathcal{B}(q,x) \leq \eta, \qquad \forall x \in X, \\ & d = [\gamma; \lambda; q_1; \ldots; q_z], \quad \eta, \gamma, \lambda \in \mathbb{R} \end{cases}$$

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Lie Derivative

$$\widehat{\mathsf{L}}_f \mathcal{B}(q,x) := \frac{\mathcal{B}(q,x_\tau) - \mathcal{B}(q,x)}{\tau}, \quad \forall x \in X$$

- x_τ is the solution process at time $\tau \in \mathbb{R}_{\geq 0}$ starting from x

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Lie Derivative

$$\widehat{\mathsf{L}}_f \mathcal{B}(q,x) := \frac{\mathcal{B}(q,x_\tau) - \mathcal{B}(q,x)}{\tau}, \quad \forall x \in X$$

- x_τ is the solution process at time $\tau \in \mathbb{R}_{\geq 0}$ starting from x

$$|\widehat{\mathsf{L}}_f \mathcal{B}(q,x) - \mathsf{L}_f \mathcal{B}(q,x)| \leq \delta, \qquad \forall x \in X$$

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Lie Derivative

$$\widehat{\mathsf{L}}_f\mathcal{B}(q,x) := \frac{\mathcal{B}(q,x_\tau)-\mathcal{B}(q,x)}{\tau}, \quad \forall x \in X$$

- x_τ is the solution process at time $\tau \in \mathbb{R}_{\geq 0}$ starting from x

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x) - \mathsf{L}_f\mathcal{B}(q,x)| \leq \delta, \qquad \forall x \in X$$

Scenario Optimization Program (SOP)

$$\mathsf{SOP}_\delta : \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, \qquad \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, \qquad \forall x \in X_u, \\ & \widehat{\mathsf{L}}_f\mathcal{B}(q,\hat{x}_i) + \delta \leq \eta, \qquad \forall \hat{x}_i \in X, \forall i \in \{1,\ldots,M\}, \\ & d = [\gamma;\lambda;q_1;\ldots;q_z], \quad \eta,\gamma,\lambda \in \mathbb{R} \end{cases}$$

Case Study: Jet Engine Compressor

- $\Sigma_c: \begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix}$

Case Study: Jet Engine Compressor

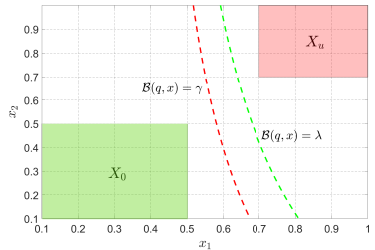
- Σ_c: $\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix}$
- Regions of interest: $X = [0.1, 1]^2, X_0 = [0.1, 0.5]^2$, and $X_u = [0.7, 1]^2$

Case Study: Jet Engine Compressor

- Σ_c: $\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix}$
- Regions of interest: $X = [0.1, 1]^2, X_0 = [0.1, 0.5]^2$, and $X_u = [0.7, 1]^2$
- $\mathcal{B}(q, x) = 0.4x_1 + 0.4x_1x_2 - 0.0728x_2 + 2.7288$
- $\eta_S^* = -0.0552$, $\eta_S^* + \varepsilon = -2 \times 10^{-4} \leq 0$
- Unknown jet engine is safe with confidence of 99%

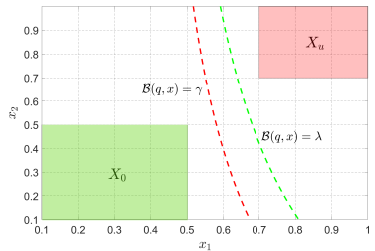
Case Study: Jet Engine Compressor

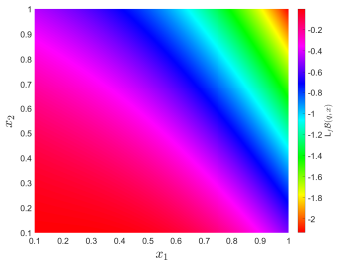
- Σ_c: $\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix}$
- Regions of interest: $X = [0.1, 1]^2, X_0 = [0.1, 0.5]^2$, and $X_u = [0.7, 1]^2$
- $\mathcal{B}(q, x) = 0.4x_1 + 0.4x_1x_2 - 0.0728x_2 + 2.7288$
- $\eta_S^* = -0.0552$, $\eta_S^* + \varepsilon = -2 \times 10^{-4} \leq 0$
- Unknown jet engine is safe with confidence of 99%



Case Study: Jet Engine Compressor

- Σ_c: $\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix}$
- Regions of interest: $X = [0.1, 1]^2, X_0 = [0.1, 0.5]^2$, and $X_u = [0.7, 1]^2$
- $\mathcal{B}(q, x) = 0.4x_1 + 0.4x_1x_2 - 0.0728x_2 + 2.7288$
- $\eta_S^* = -0.0552$, $\eta_S^* + \varepsilon = -2 \times 10^{-4} \leq 0$
- Unknown jet engine is safe with confidence of 99%



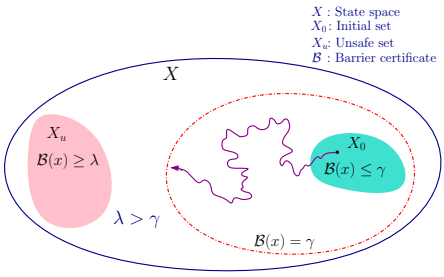


Barrier Certificate: Stochastic Setting

Barrier Certificate: Verification Problem

Consider $\Sigma_d : x(k+1) = f(x(k), \varsigma(k))$ and sets $X_0, X_u \subseteq X$. Suppose there exist a function $\mathcal{B} : X \to \mathbb{R}_0^+$ and constants $\gamma, \lambda \in \mathbb{R}_0^+$, with $\lambda > \gamma$, such that:

- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma$,
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda$,
- $\forall x \in X$: $\mathbb{E}[\mathcal{B}(f(x))] \leq \mathcal{B}(x)$.



Barrier Certificate: Stochastic Setting

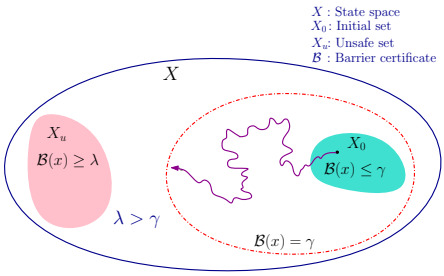
Barrier Certificate: Verification Problem

Consider $\Sigma_d : x(k+1) = f(x(k), \varsigma(k))$ and sets $X_0, X_u \subseteq X$. Suppose there exist a function $\mathcal{B} : X \to \mathbb{R}_0^+$ and constants $\gamma, \lambda \in \mathbb{R}_0^+$, with $\lambda > \gamma$, such that:

- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma$,
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda$,
- $\forall x \in X$: $\mathbb{E}[\mathcal{B}(f(x))] \leq \mathcal{B}(x)$.

Then:

$$\mathbb{P}\Big\{x(k) \notin X_u \text{ for all } 0 \leq k < \infty\Big\} \geq 1 - \frac{\gamma}{\lambda}.$$



Barrier Certificate: Stochastic Setting

Barrier Certificate: Verification Problem

Consider $\Sigma_d : x(k+1) = f(x(k), \varsigma(k))$ and sets $X_0, X_u \subseteq X$. Suppose there exist a function $\mathcal{B} : X \to \mathbb{R}_0^+$ and constants $\gamma, \lambda \in \mathbb{R}_0^+$, with $\lambda > \gamma$, such that:

- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma$,
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda$,
- $\forall x \in X$: $\mathbb{E}[\mathcal{B}(f(x))] \leq \mathcal{B}(x)$.

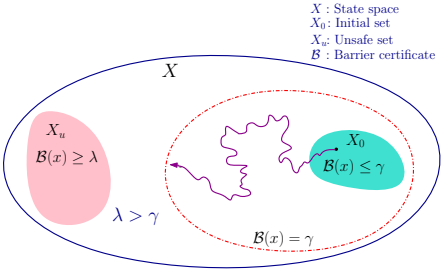
Then:

$$\mathbb{P}\Big\{x(k) \notin X_u \text{ for all } 0 \leq k < \infty\Big\} \geq 1 - \frac{\gamma}{\lambda}.$$

Corollary

If $\forall x \in X$: $\mathbb{E}[\mathcal{B}(f(x))] \leq \mathcal{B}(x) + c$, then:

$$\mathbb{P}\Big\{x(k) \notin X_u \text{ for all } 0 \leq k \leq \mathcal{T}\Big\} \geq 1 - \frac{\gamma + c\mathcal{T}}{\lambda}.$$



Data-Driven Construction of BC

Robust Optimization Program (ROP)

$$\text{ROP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, & \forall x \in X_u, \\ & \mathbb{E}[\mathcal{B}(q, f(x,\varsigma))] - \mathcal{B}(q,x) \leq \eta, & \forall x \in X, \\ & d = [\gamma; \lambda; q_1; \ldots; q_z], \quad \eta, \gamma, \lambda \in \mathbb{R} \end{cases}$$

Data-Driven Construction of BC

Robust Optimization Program (ROP)

$$\text{ROP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, & \forall x \in X_u, \\ & \mathbb{E}[\mathcal{B}(q, f(x,\varsigma))] - \mathcal{B}(q,x) \leq \eta, & \forall x \in X, \\ & d = [\gamma; \lambda; q_1; \ldots; q_z], \quad \eta, \gamma, \lambda \in \mathbb{R} \end{cases}$$

Scenario Optimization Program (SOP)

Let $(\hat{x}_i)_{i=1}^{M}$ denote M i.i.d. data sampled within X

$$\text{SOP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, & \forall x \in X_u, \\ & \mathbb{E}[\mathcal{B}(q, f(\hat{x}_i,\varsigma))] - \mathcal{B}(q,\hat{x}_i) \leq \eta, & \forall \hat{x}_i \in X, \forall i \in \{1,\ldots,M\}, \\ & d = [\gamma; \lambda; q_1; \ldots; q_z], \quad \eta, \gamma, \lambda \in \mathbb{R} \end{cases}$$

Data-Driven Construction of BC (cont.)

Empirical Approximation of Expected Value (Chebyshev's inequality)

$$\mathbb{P}\left\{\left|\mathbb{E}[\mathcal{B}(q, f(x, \varsigma))] - \frac{1}{N}\sum_{j=1}^{N}\mathcal{B}(q, f(x, \hat{\varsigma}_j))\right| \leq \mu\right\} \geq 1 - \beta_1$$

Data-Driven Construction of BC (cont.)

Empirical Approximation of Expected Value (Chebyshev's inequality)

$$\mathbb{P}\left\{\left|\mathbb{E}[\mathcal{B}(q, f(x,\varsigma))] - \frac{1}{N}\sum_{j=1}^{N}\mathcal{B}(q, f(x,\hat{\varsigma}_j))\right| \leq \mu\right\} \geq 1-\beta_1$$

Scenario Optimization Program (SOP)

$$\text{SOP}_\mu: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, & \forall x \in X_u, \\ & \frac{1}{N}\sum_{j=1}^{N}\mathcal{B}(q, f(\hat{x}_i,\hat{\varsigma}_j)) + \mu - \mathcal{B}(q,\hat{x}_i) \leq \eta, & \forall \hat{x}_i \in X, \forall i \in \{1,\ldots,M\}, \\ & d = [\gamma;\lambda;q_1;\ldots;q_z], \quad \eta,\gamma,\lambda \in \mathbb{R} \end{cases}$$

Relation between SOP$_\mu$ and Original ROP

Theorem (out-of-sample performance guarantees)

Consider an unknown stochastic system Σ_d and the corresponding SOP$_\mu$ with its associated optimal value $\eta^*_{S_\mu}$ and solution d^*, with

$$M(\varepsilon, \beta_2) := \min \left\{ M \in \mathbb{N} \,|\, \sum_{i=0}^{c-1} \binom{M}{i} \varepsilon^i (1-\varepsilon)^{M-i} \leq \beta_2 \right\}.$$

If

$$\eta^*_{S_\mu} + \varepsilon \leq 0,$$

then the solution d^* is a feasible solution for original ROP, *i.e.,* $d^* \models$ ROP, with a confidence of at least $1 - \beta_1 - \beta_2$.

Relation between SOP$_\mu$ and Original ROP

Theorem (out-of-sample performance guarantees)

Consider an unknown stochastic system Σ_d and the corresponding SOP$_\mu$ with its associated optimal value $\eta^*_{S_\mu}$ and solution d^*, with

$$M(\varepsilon, \beta_2) := \min \left\{ M \in \mathbb{N} \,|\, \sum_{i=0}^{c-1} \binom{M}{i} \varepsilon^i (1-\varepsilon)^{M-i} \leq \beta_2 \right\}.$$

If

$$\eta^*_{S_\mu} + \varepsilon \leq 0,$$

then the solution d^* is a feasible solution for original ROP, *i.e.,* $d^* \models$ ROP, with a confidence of at least $1 - \beta_1 - \beta_2$.

Require: $\varepsilon, \beta_1, \beta_2 \in [0, 1]$ and degree of barrier certificate

1: Compute M based on ε, β_2
2: Compute N based on μ, β_1
3: Solve the SOP with acquired M, N and obtain $\eta^*_{S_\mu}$

Ensure: if $\eta^*_{S_\mu} + \varepsilon \leq 0$, then $d^* \models$ ROP, and accordingly $\Sigma_d \models \varphi$, with a confidence of at least $1 - \beta_1 - \beta_2$

Case Study: Lane keeping System - BMW320i

- Σ_d: $\begin{cases} x(k+1) = x(k) + \tau\nu\cos(\psi(k)+b) + \varsigma_1(k) \\ y(k+1) = y(k) + \tau\nu\sin(\psi(k)+b) + \varsigma_2(k) \\ \psi(k+1) = \psi(k) + \frac{\tau\nu}{l_r}\sin(b) + \varsigma_3(k) \end{cases}$

Case Study: Lane keeping System - BMW320i

- Σ_d: $\begin{cases} x(k+1) = x(k) + \tau\nu\cos(\psi(k)+b) + \varsigma_1(k) \\ y(k+1) = y(k) + \tau\nu\sin(\psi(k)+b) + \varsigma_2(k) \\ \psi(k+1) = \psi(k) + \frac{\tau\nu}{l_r}\sin(b) + \varsigma_3(k) \end{cases}$
- Regions of interest: $X = [1,10]\times[-7,7]\times[-0.05,0.05]$, $X_0 = [1,2]\times[-0.5,0.5]\times[-0.005,0.005]$, $X_{u_1} = [1,10]\times[-7,-6]\times[-0.05,0.05]$, $X_{u_2} = [1,10]\times[6,7]\times[-0.05,0.05]$
- $\mathcal{B}(q,x,y,\psi) = 0.39y^2 + 0.15\psi^2 + 0.009x\psi - 0.007y - 0.015\psi + 0.452$
- $\eta^*_{S_\mu} = -0.0552$, $\eta^*_{S_\mu} + \varepsilon = -0.01 \leq 0$
- Unknown BMW320i is safe with confidence of 90%

Data-Driven Construction of BC: Continuous-Time Systems

- $\Sigma_c : \mathrm{d}x(t) = f(x(t))\mathrm{d}t + \sigma(x(t))\mathrm{d}\mathbb{W}_t$
- $\forall x \in X_0$: $\mathcal{B}(x) \leq \gamma,$
- $\forall x \in X_u$: $\mathcal{B}(x) \geq \lambda,$
- $\forall x \in X$: $\mathcal{L}\mathcal{B}(x) = \partial_x \mathcal{B}(x) f(x) + \frac{1}{2}\mathsf{Tr}(\sigma(x)\sigma^T(x)\partial_{x,x}\mathcal{B}(x)) \leq 0,$

Data-Driven Construction of BC: Continuous-Time Systems

- Σ_c: $\mathrm{d}x(t) = f(x(t))\mathrm{d}t + \sigma(x(t))\mathrm{d}\mathbb{W}_t$
- $\forall x \in X_0$: $\quad \mathcal{B}(x) \leq \gamma,$
- $\forall x \in X_u$: $\quad \mathcal{B}(x) \geq \lambda,$
- $\forall x \in X$: $\quad \mathcal{LB}(x) = \partial_x \mathcal{B}(x) f(x) + \frac{1}{2}\mathsf{Tr}(\sigma(x)\sigma^T(x)\partial_{x,x}\mathcal{B}(x)) \leq 0,$

Robust Optimization Program (ROP)

$$\mathsf{ROP}: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, & \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, & \forall x \in X_u, \\ & \mathcal{LB}(q,x) \leq \eta, & \forall x \in X, \\ & d = [\gamma; \lambda; q_1; \ldots; q_z], & \eta, \gamma, \lambda \in \mathbb{R} \end{cases}$$

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Infinitesimal Generator

$$\widehat{\mathcal{L}}_1\mathcal{B}(x) := \frac{\mathbb{E}_x\Big[\mathcal{B}(x_\tau)\Big] - \mathcal{B}(x)}{\tau}, \qquad |\widehat{\mathcal{L}}_1\mathcal{B}(x) - \mathcal{L}\mathcal{B}(x)| \leq \delta_1, \qquad \forall x \in X,$$

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Infinitesimal Generator

$$\widehat{\mathcal{L}}_1\mathcal{B}(x) := \frac{\mathbb{E}_x\Big[\mathcal{B}(x_\tau)\Big] - \mathcal{B}(x)}{\tau}, \qquad |\widehat{\mathcal{L}}_1\mathcal{B}(x) - \mathcal{L}\mathcal{B}(x)| \leq \delta_1, \qquad \forall x \in X,$$

$$\widehat{\mathcal{L}}_2\mathcal{B}(x) := \frac{\frac{1}{N}\sum_{i=1}^{N}\mathcal{B}(x_\tau^i) - \mathcal{B}(x)}{\tau}, \quad \mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{B}(x) - \widehat{\mathcal{L}}_1\mathcal{B}(x)| \leq \delta_2\Big\} \geq 1-\beta_1, \qquad \forall x \in X,$$

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Infinitesimal Generator

$$\widehat{\mathcal{L}}_1\mathcal{B}(x) := \frac{\mathbb{E}_x\Big[\mathcal{B}(x_\tau)\Big] - \mathcal{B}(x)}{\tau}, \qquad |\widehat{\mathcal{L}}_1\mathcal{B}(x) - \mathcal{L}\mathcal{B}(x)| \leq \delta_1, \qquad \forall x \in X,$$

$$\widehat{\mathcal{L}}_2\mathcal{B}(x) := \frac{\frac{1}{N}\sum_{i=1}^{N}\mathcal{B}(x_\tau^i) - \mathcal{B}(x)}{\tau}, \quad \mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{B}(x) - \widehat{\mathcal{L}}_1\mathcal{B}(x)| \leq \delta_2\Big\} \geq 1-\beta_1, \qquad \forall x \in X,$$

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{B}(x) - \mathcal{L}\mathcal{B}(x)| \leq \delta = \delta_1 + \delta_2\Big\} \geq 1-\beta_1, \qquad \forall x \in X.$$

Data-Driven Construction of BC: Continuous-Time Systems

Empirical Approximation of Infinitesimal Generator

$$\widehat{\mathcal{L}}_1\mathcal{B}(x) := \frac{\mathbb{E}_x\Big[\mathcal{B}(x_\tau)\Big] - \mathcal{B}(x)}{\tau}, \qquad |\widehat{\mathcal{L}}_1\mathcal{B}(x) - \mathcal{L}\mathcal{B}(x)| \leq \delta_1, \qquad \forall x \in X,$$

$$\widehat{\mathcal{L}}_2\mathcal{B}(x) := \frac{\frac{1}{N}\sum_{i=1}^{N}\mathcal{B}(x_\tau^i) - \mathcal{B}(x)}{\tau}, \quad \mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{B}(x) - \widehat{\mathcal{L}}_1\mathcal{B}(x)| \leq \delta_2\Big\} \geq 1-\beta_1, \qquad \forall x \in X,$$

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{B}(x) - \mathcal{L}\mathcal{B}(x)| \leq \delta = \delta_1 + \delta_2\Big\} \geq 1-\beta_1, \qquad \forall x \in X.$$

Scenario Optimization Program (SOP)

$$\text{SOP}_\delta: \begin{cases} \min\limits_{[d;\eta]} & \eta, \\ \text{s.t.} & \mathcal{B}(q,x) - \gamma \leq \eta, \qquad \forall x \in X_0, \\ & -\mathcal{B}(q,x) + \lambda \leq \eta, \qquad \forall x \in X_u, \\ & \widehat{\mathcal{L}}_2\mathcal{B}(q,x) + \delta \leq \eta, \qquad \forall \hat{x}_i \in X, \forall i \in \{1,\ldots,M\}, \\ & d = [\gamma;\lambda;q_1;\ldots;q_z], \quad \eta,\gamma,\lambda \in \mathbb{R} \end{cases}$$

Relation between SOP$_\delta$ and Original ROP

Theorem (out-of-sample performance guarantees)

Consider an unknown stochastic system Σ_c and the corresponding SOP with its associated optimal value $\eta^*_{S_\delta}$ and solution d^*, with

$$M(\varepsilon, \beta_2) := \min \Big\{ M \in \mathbb{N} \,|\, \sum_{i=0}^{c-1} \binom{M}{i} \varepsilon^i (1-\varepsilon)^{M-i} \leq \beta_2 \Big\}.$$

If

$$\eta^*_{S_\delta} + \varepsilon \leq 0,$$

then the solution d^* is a feasible solution for original ROP, *i.e.,* $d^* \models$ ROP, with a confidence of at least $1 - \beta_1 - \beta_2$.

Relation between SOP$_\delta$ and Original ROP

Theorem (out-of-sample performance guarantees)

Consider an unknown stochastic system Σ_c and the corresponding SOP with its associated optimal value $\eta^*_{S_\delta}$ and solution d^*, with

$$M(\varepsilon, \beta_2) := \min \Big\{ M \in \mathbb{N} \,|\, \sum_{i=0}^{c-1} \binom{M}{i} \varepsilon^i (1-\varepsilon)^{M-i} \leq \beta_2 \Big\}.$$

If

$$\eta^*_{S_\delta} + \varepsilon \leq 0,$$

then the solution d^* is a feasible solution for original ROP, *i.e.,* $d^* \models$ ROP, with a confidence of at least $1 - \beta_1 - \beta_2$.

Require: $\varepsilon, \beta_1, \beta_2 \in [0, 1]$ and degree of barrier certificate

1: Compute M based on ε, β_2
2: Compute δ based on N, β_1
3: Solve the SOP with acquired δ, M and obtain $\eta^*_{S_\delta}$

Ensure: if $\eta^*_{S_\delta} + \varepsilon \leq 0$, then $d^* \models$ ROP, and accordingly $\Sigma_c \models \varphi$, with a confidence of at least $1 - \beta_1 - \beta_2$

Summary

- Data-driven safety verification of unknown systems:
  - Discrete-time systems
  - Continuous-time systems
  - Discrete-time stochastic systems
  - Continuous-time stochastic systems

Summary

- Data-driven safety verification of unknown systems:
  - Discrete-time systems
  - Continuous-time systems
  - Discrete-time stochastic systems
  - Continuous-time stochastic systems
- Cast original safety problem as an ROP
- Provide SOP corresponding to ROP
- Establish a probabilistic relation between optimal values of SOP (η_S^*) and ROP (η_R^*) with a threshold ε
- Quantify an a-priori guaranteed confidence over safety of unknown systems

Summary

- Data-driven safety verification of unknown systems:
  - Discrete-time systems
  - Continuous-time systems
  - Discrete-time stochastic systems
  - Continuous-time stochastic systems
- Cast original safety problem as an ROP
- Provide SOP corresponding to ROP
- Establish a probabilistic relation between optimal values of SOP (η_S^*) and ROP (η_R^*) with a threshold ε
- Quantify an a-priori guaranteed confidence over safety of unknown systems

- Data-driven results for safety controller synthesis via control barrier certificates
- Data-driven results for unknown jump-diffusion systems

Acknowledgment

European Research Council

Engineering and Physical Sciences Research Council

Thank you for your attention!