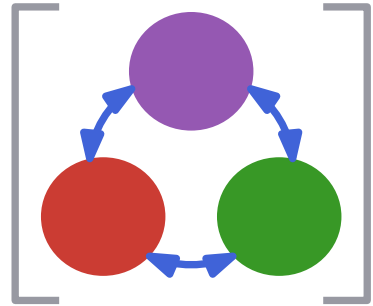
Formal Verification of Stochastic Systems: From Stochastic Barrier Functions to Abstraction-Based Methods

Hybrid Systems TC seminar

Frederik Baymler Mathiesen

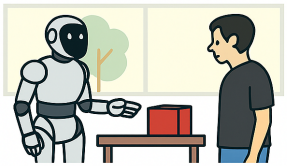
Delft Center for Systems and Control

28-10-2025

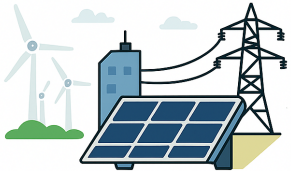


TU Delft

Safety-critical systems



Robotic Systems

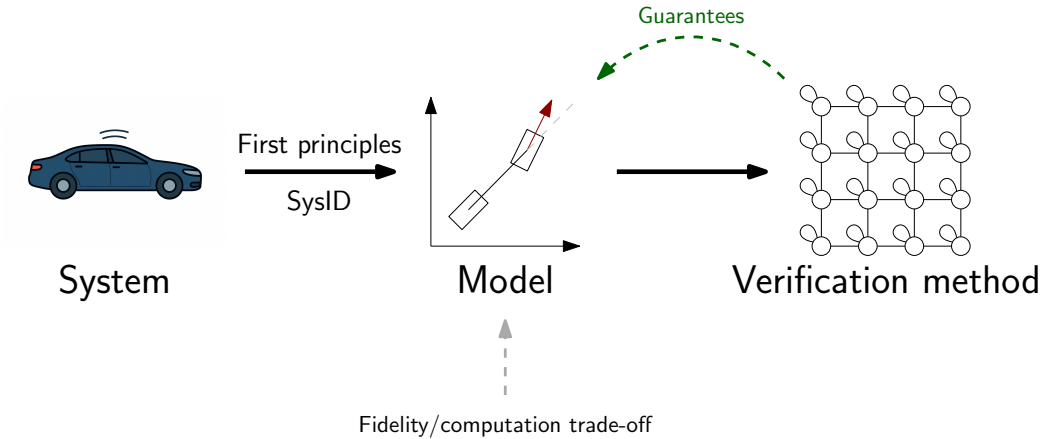


Energy Systems

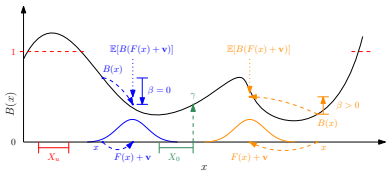
Medical Appliances

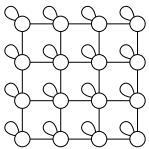
Financial Markets

Verification process



Verification of stochastic systems: SBFs and finite-state abstractions





Stochastic Barrier Functions

- Design value function measuring ”unsafety level”
- Evolve only a single time step of system

Finite-state abstractions

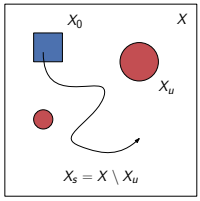
a. Construct a finite-state model
b. Perform model checking
c. Lift guarantees from abstract to concrete model

Formalizing and characterizing safety

Probabilistic Safety

Given autonomous dynamics $\mathbf{x}[k+1] = f(\mathbf{x}[k], \mathbf{v}[k])$ with a known i.i.d. noise distribution $p_{\mathbf{v}}$. Then the safety probability is

$$P_{safe}(X_0, X_s, K) = \inf_{x_0 \in X_0} \mathbb{P}^{x_0}\left[\mathbf{x}[k] \in X_s,\ \forall 0 \leq k \leq K\right].$$



[1] Abate, A., Prandini, M., Lygeros, J., & Sastry, S. (2008). Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica.

Formalizing and characterizing safety

Probabilistic Safety

Given autonomous dynamics $\mathbf{x}[k+1] = f(\mathbf{x}[k], \mathbf{v}[k])$ with a known i.i.d. noise distribution $p_{\mathbf{v}}$. Then the safety probability is

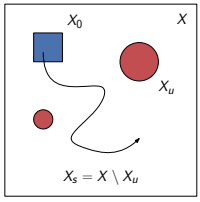
$$P_{safe}(X_0, X_s, K) = \inf_{x_0 \in X_0} \mathbb{P}^{x_0}\left[\mathbf{x}[k] \in X_s,\ \forall 0 \leq k \leq K\right].$$

Bellman equation for safety[1]

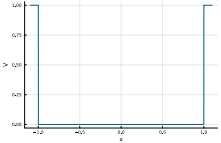
If $V_k, k \in \{0, \ldots, K\}$ is satisfying

$$V_0(x) = \mathbb{1}_{X_u}(x)$$
$$V_{k+1}(x) = \mathbb{1}_{X_u}(x) + \mathbb{1}_{X_s}(x)\mathbb{E}[V_k(f(x, v))]$$

then $P_{safe}(X_0, X_s, K) = 1 - \sup_{x \in X_0} V_K(x)$.



Timestep 10



$\mathbf{x}[k+1] = 0.99\mathbf{x}[k] + \mathbf{v}[k]$,
$\mathbf{v}[k] \sim \mathcal{N}(0, 0.05)$

[1] Abate, A., Prandini, M., Lygeros, J., & Sastry, S. (2008). Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica.

Formalizing and characterizing safety

Probabilistic Safety

Given autonomous dynamics $\mathbf{x}[k+1] = f(\mathbf{x}[k], \mathbf{v}[k])$ with a known i.i.d. noise distribution $p_{\mathbf{v}}$. Then the safety probability is

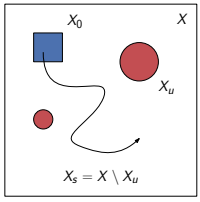
$$P_{safe}(X_0, X_s, K) = \inf_{x_0 \in X_0} \mathbb{P}^{x_0}\left[\mathbf{x}[k] \in X_s,\ \forall 0 \leq k \leq K\right].$$

Bellman equation for safety[1]

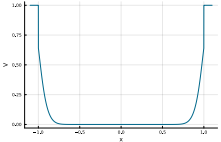
If $V_k, k \in \{0, \ldots, K\}$ is satisfying

$$V_0(x) = \mathbb{1}_{X_u}(x)$$
$$V_{k+1}(x) = \mathbb{1}_{X_u}(x) + \mathbb{1}_{X_s}(x)\mathbb{E}[V_k(f(x, v))]$$

then $P_{safe}(X_0, X_s, K) = 1 - \sup_{x \in X_0} V_K(x)$.



Timestep 5



$\mathbf{x}[k+1] = 0.99\mathbf{x}[k] + \mathbf{v}[k]$,
$\mathbf{v}[k] \sim \mathcal{N}(0, 0.05)$

[1] Abate, A., Prandini, M., Lygeros, J., & Sastry, S. (2008). Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica.

Formalizing and characterizing safety

Probabilistic Safety

Given autonomous dynamics $\mathbf{x}[k+1] = f(\mathbf{x}[k], \mathbf{v}[k])$ with a known i.i.d. noise distribution $p_{\mathbf{v}}$. Then the safety probability is

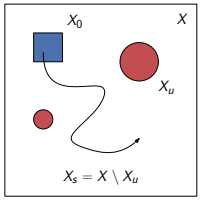
$$P_{safe}(X_0, X_s, K) = \inf_{x_0 \in X_0} \mathbb{P}^{x_0}\left[\mathbf{x}[k] \in X_s,\ \forall 0 \leq k \leq K\right].$$

Bellman equation for safety[1]

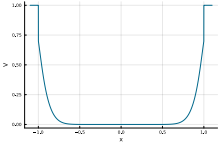
If $V_k, k \in \{0, \ldots, K\}$ is satisfying

$$V_0(x) = \mathbb{1}_{X_u}(x)$$
$$V_{k+1}(x) = \mathbb{1}_{X_u}(x) + \mathbb{1}_{X_s}(x)\mathbb{E}[V_k(f(x, v))]$$

then $P_{safe}(X_0, X_s, K) = 1 - \sup_{x \in X_0} V_K(x)$.



Timestep 0



$$\mathbf{x}[k+1] = 0.99\mathbf{x}[k] + \mathbf{v}[k],$$
$$\mathbf{v}[k] \sim \mathcal{N}(0, 0.05)$$

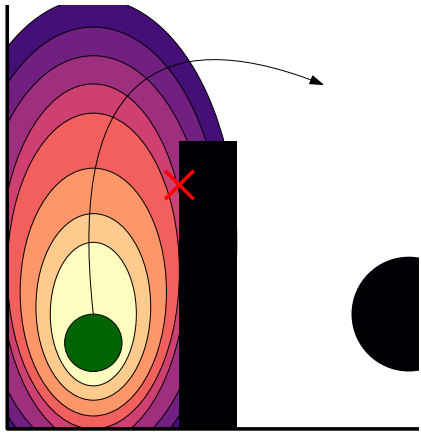
[1] Abate, A., Prandini, M., Lygeros, J., & Sastry, S. (2008). Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica.

01

Stochastic Barrier Functions

TU Delft

Idea: design a function with bounded increase under system evolution

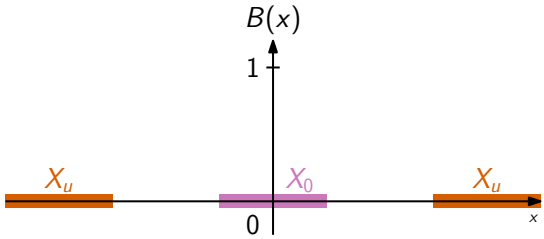


Stochastic Barrier Functions[1]

$$
\begin{aligned}
B(x) &\geq 0 && \forall x \in X \\
B(x) &\geq 1 && \forall x \in X_u \\
B(x) &\leq \gamma && \forall x \in X_0 \\
\mathbb{E}[B(f(x,v))] &\leq B(x) + \beta && \forall x \in X_s
\end{aligned}
$$

Safety certification

$$P_{safe}(X_0, X_s, K) \geq 1 - (\gamma + \beta K)$$



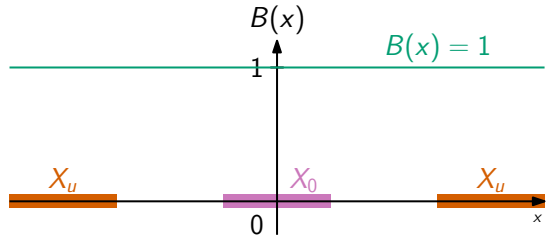
[1] Santoyo, C., Dutreix, M., & Coogan, S. (2021). A barrier function approach to finite-time stochastic system verification and control. Automatica.

Stochastic Barrier Functions[1]

$$
\begin{aligned}
&B(x) \geq 0 && \forall x \in X \\
&B(x) \geq 1 && \forall x \in X_u \\
&B(x) \leq \gamma && \forall x \in X_0 \\
&\mathbb{E}[B(f(x,v))] \leq B(x) + \beta && \forall x \in X_s
\end{aligned}
$$

Safety certification

$$P_{safe}(X_0, X_s, K) \geq 1 - (\gamma + \beta K)$$



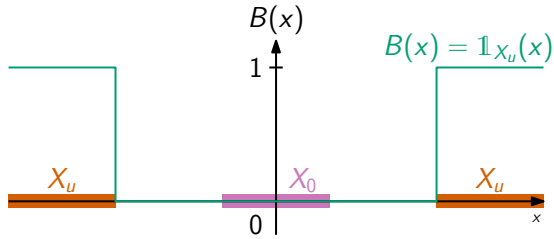
[1] Santoyo, C., Dutreix, M., & Coogan, S. (2021). A barrier function approach to finite-time stochastic system verification and control. Automatica.

Stochastic Barrier Functions[1]

$$B(x) \geq 0 \qquad \forall x \in X$$
$$B(x) \geq 1 \qquad \forall x \in X_u$$
$$B(x) \leq \gamma \qquad \forall x \in X_0$$
$$\mathbb{E}[B(f(x,v))] \leq B(x) + \beta \qquad \forall x \in X_s$$

Safety certification

$$P_{safe}(X_0, X_s, K) \geq 1 - (\gamma + \beta K)$$



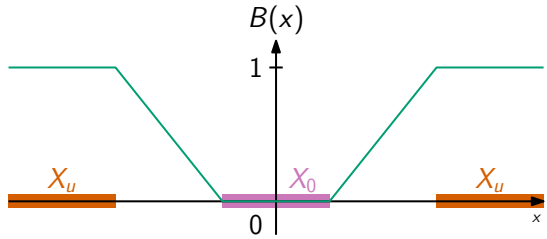
[1] Santoyo, C., Dutreix, M., & Coogan, S. (2021). A barrier function approach to finite-time stochastic system verification and control. Automatica.

Stochastic Barrier Functions[1]

$$B(x) \geq 0 \qquad \forall x \in X$$
$$B(x) \geq 1 \qquad \forall x \in X_u$$
$$B(x) \leq \gamma \qquad \forall x \in X_0$$
$$\mathbb{E}[B(f(x,v))] \leq B(x) + \beta \qquad \forall x \in X_s$$

Safety certification

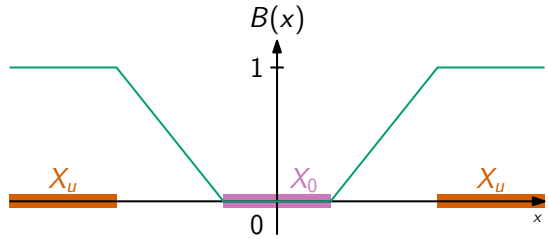
$$P_{safe}(X_0, X_s, K) \geq 1 - (\gamma + \beta K)$$



[1] Santoyo, C., Dutreix, M., & Coogan, S. (2021). A barrier function approach to finite-time stochastic system verification and control. Automatica.

Stochastic Barrier Functions[1]

$$B(x) \geq 0 \qquad \forall x \in X$$
$$B(x) \geq 1 \qquad \forall x \in X_u$$
$$B(x) \leq \gamma \qquad \forall x \in X_0$$
$$\mathbb{E}[B(f(x,v))] \leq B(x) + \beta \qquad \forall x \in X_s$$



Safety certification

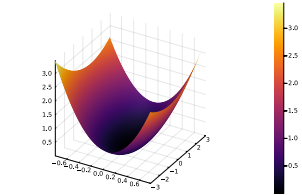
$$P_{safe}(X_0, X_s, K) \geq 1 - (\gamma + \beta K)$$

SBF Safety via Bellman equation

$$V_0(x) = \mathbb{1}_{X_u}(x) \leq B(x) \Rightarrow V_1(x) \leq B(x) + \beta \Rightarrow \cdots \Rightarrow V_K(x) \leq B(x) + \beta K$$

[1] Santoyo, C., Dutreix, M., & Coogan, S. (2021). A barrier function approach to finite-time stochastic system verification and control. Automatica.

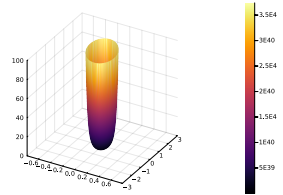
Convex Optimization-based SBF Synthesis



$$B(x) = x^T P x$$

Quadratic

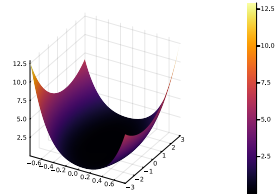
- Linear dynamics
- SDP/LMI
- Inflexible due to symmetry



$$B(x) = e^{x^T P x} - 1$$

Exponential

- Linear dynamics
- Relaxed to SDP
- Inflexible due to symmetry

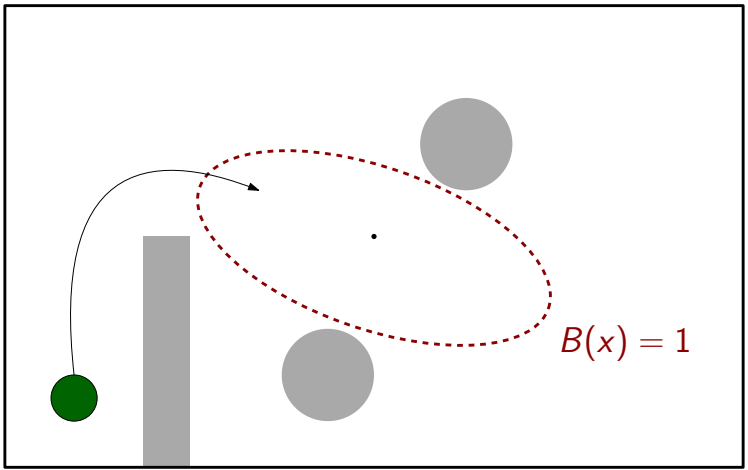


$$B(x) = m(x)^T P m(x)$$

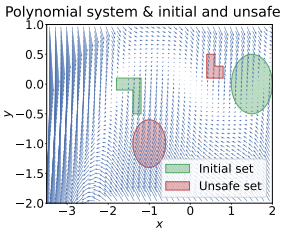
Sum-of-Squares

- Polynomial dynamics
- SDP with squared multinomial scaling
- Partial symmetry

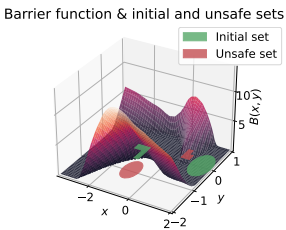
Reference frames, symmetries, and set geometries in SBFs



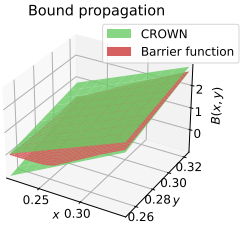
Neural Stochastic Barrier Functions[2]



(a)



(b)



(c)

[2] Mathiesen, F. B., Calvert, S. C., & Laurenti, L. (2022). Safety certification for stochastic systems via neural barrier functions. IEEE Control Systems Letters.

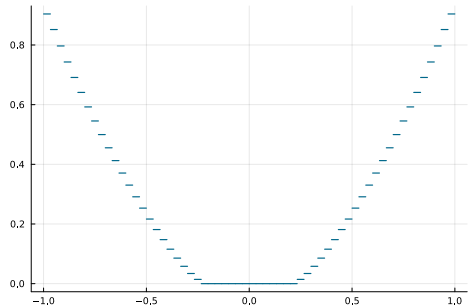
Piece-wise Constant Stochastic Barrier Functions[3]

Piece-wise constant barrier template

$$B(x) = \max(B_1(x), B_2(x), \ldots, B_\ell(x))$$

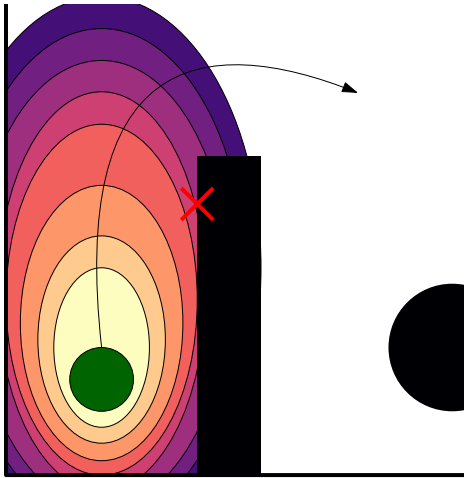
where $B_i(x) = b_i$ if $x \in P_i$ and 0 otherwise.

- Optimal wrt. measurable SBFs as $\ell \to \infty$
- Synthesis methods:
  - Dual linear programming
  - LP-based CEGIS
  - Projected (sub)-gradient descent



[3] Mazouz, R., Mathiesen, F. B., Laurenti, L., & Lahijanian, M., Piecewise Stochastic Barrier Functions, Under review.

The downfall of SBFs

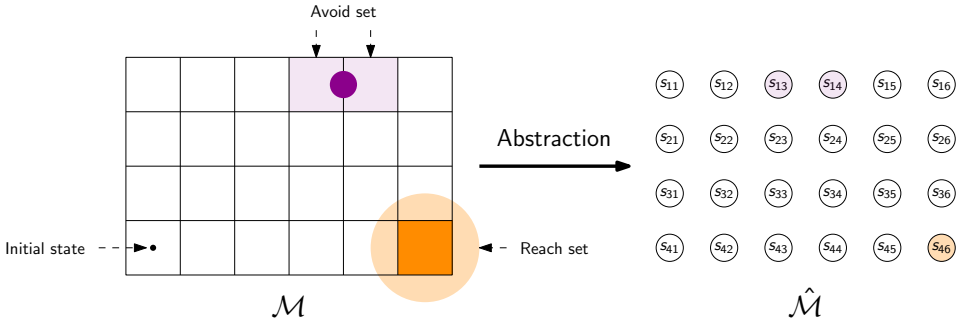


02

Finite-state Abstractions

TU Delft

Idea: construct a finite-state model that "contains" the concrete system



$$\mathcal{B}(\mathcal{M}) \subseteq \mathcal{B}(\hat{\mathcal{M}})$$

Finite-state models

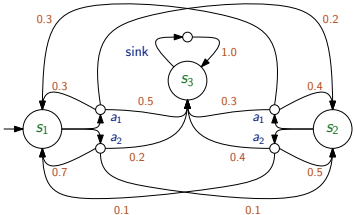


Figure: MDP[1]

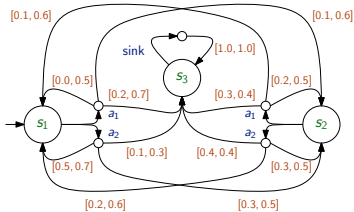


Figure: IMDP[2]

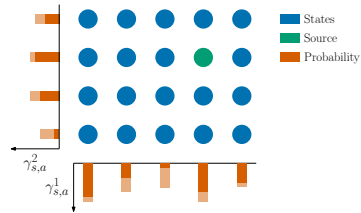


Figure: fIMDP[3]

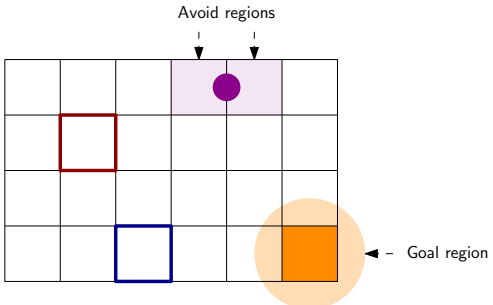
[1]Van Huijgevoort, B., Schön, O., Soudjani, S., & Haesaert, S. (2023). SySCoRe: Synthesis via stochastic coupling relations. Hybrid Systems: Computation and Control.

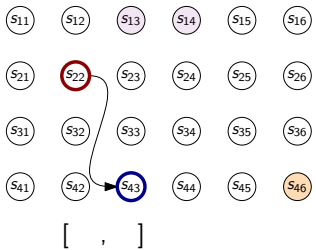
[2]Lahijanian, M., Andersson, S. B., & Belta, C. (2015). Formal verification and synthesis for discrete-time stochastic systems. IEEE TAC.

[3]Mathiesen, F. B., Haesaert, S., & Laurenti, L. (2025). Scalable control synthesis for stochastic systems via structural IMDP abstractions. Hybrid Systems: Computation and Control.

Constructing abstractions

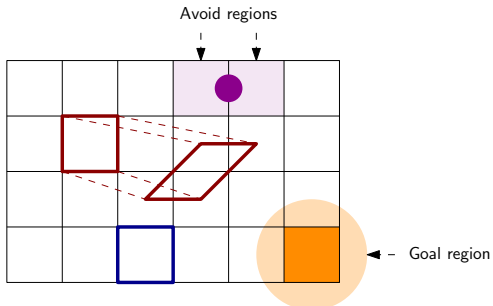
$$\mathbf{x}[k+1] = F(a)\mathbf{x}[k] + G(a)\omega, \quad a \in A, \omega \sim \mathcal{N}(0, \Sigma_\omega)$$

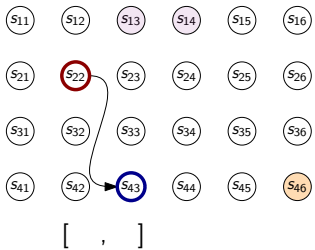




Constructing abstractions

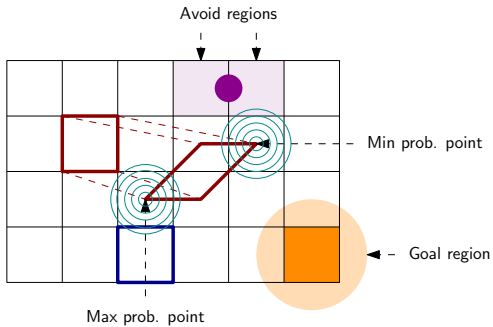
$$\mathbf{x}[k+1] = F(a)\mathbf{x}[k] + G(a)\omega, \quad a \in A, \omega \sim \mathcal{N}(0, \Sigma_\omega)$$

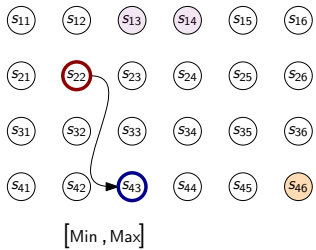




Constructing abstractions

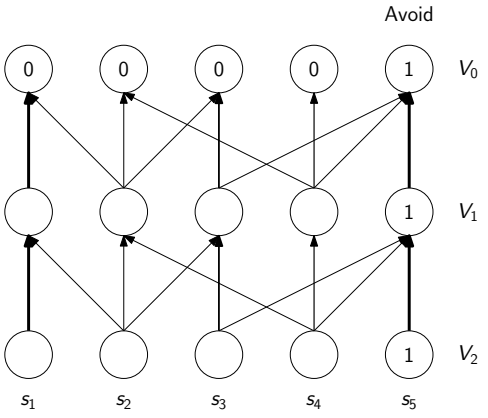
$$\mathbf{x}[k+1] = F(a)\mathbf{x}[k] + G(a)\omega, \quad a \in A, \omega \sim \mathcal{N}(0, \Sigma_\omega)$$





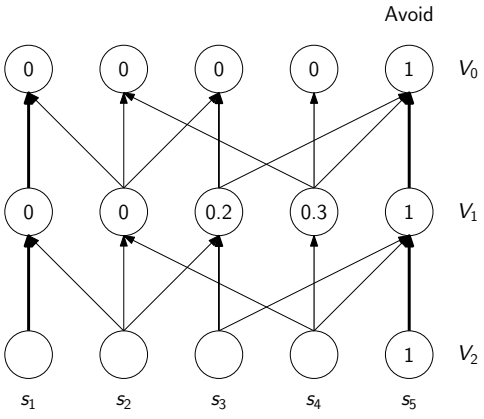
Model checking: value iteration

$$V_0(s) = \mathbb{1}_{S_u}(s), \qquad V_k(s) = \mathbb{1}_{S_u}(s) + \mathbb{1}_{S \setminus S_u}(s) \min_{\gamma_s \in \Gamma_s} \mathbb{E}_{s' \sim \gamma_s}[V_{k-1}]$$



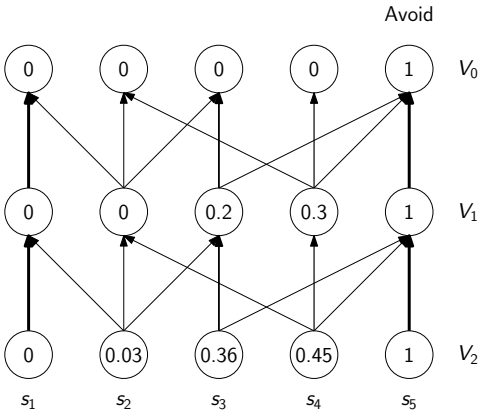
Model checking: value iteration

$$V_0(s) = \mathbb{1}_{S_u}(s), \qquad V_k(s) = \mathbb{1}_{S_u}(s) + \mathbb{1}_{S \setminus S_u}(s) \min_{\gamma_s \in \Gamma_s} \mathbb{E}_{s' \sim \gamma_s}[V_{k-1}]$$



Model checking: value iteration

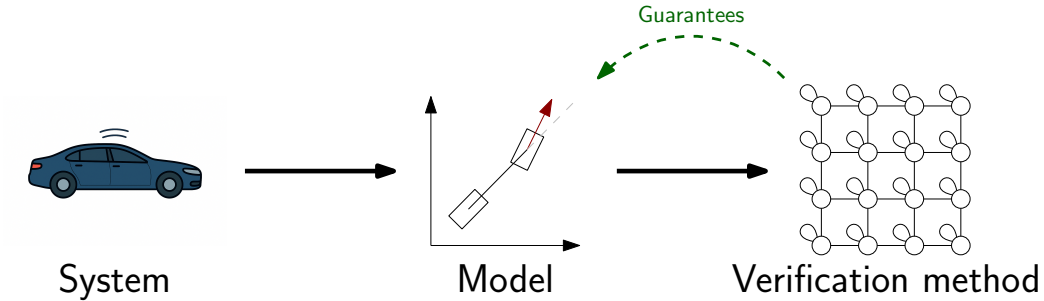
$$V_0(s) = \mathbb{1}_{S_u}(s), \qquad V_k(s) = \mathbb{1}_{S_u}(s) + \mathbb{1}_{S \setminus S_u}(s) \min_{\gamma_s \in \Gamma_s} \mathbb{E}_{s' \sim \gamma_s}[V_{k-1}]$$



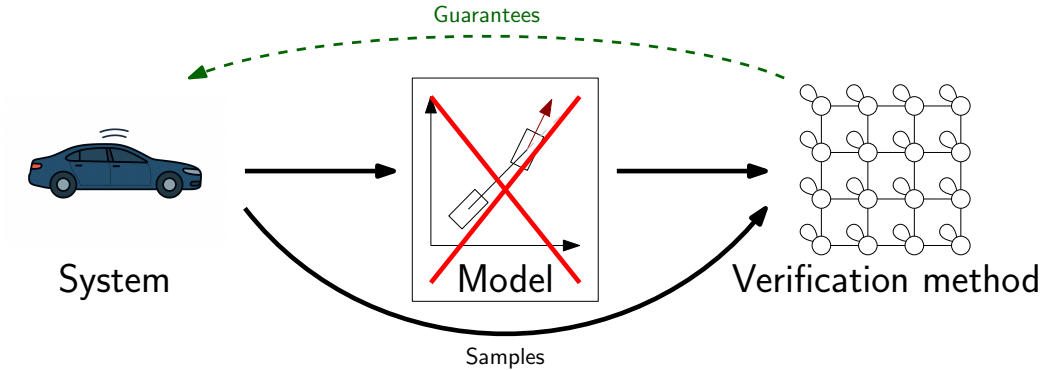
03

Data-driven methods

Why data-driven methods?



Why data-driven methods?



Data-driven Stochastic Barrier Functions

- Samples from additive noise, known nominal model
  - Standard scenario approach[4]
- Samples of source-destination pairs + known Lipschitz bounds
  - Scenario approach for robust programming[5]
- Samples of source-destination pairs
  - Conditional mean embeddings[6]

[4] Mathiesen, F. B., Romao, L., Calvert, S. C., Abate, A., & Laurenti, L. (2023). Inner Approximations of Stochastic Programs for Data-driven Stochastic Barrier Function Design. Conference on Decision and Control.

[5] Salamati, A., Lavaei, A., Soudjani, S., & Zamani, M. (2024). Data-driven verification and synthesis of stochastic systems via barrier certificates. Automatica.

[6] Schön, O., Zhong, Z., & Soudjani, S. (2024). Data-driven distributionally robust safety verification using barrier certificates and conditional mean embeddings. American Control Conference.

Data-driven abstractions

- Approaches for MDPs
  - Bayesian statistics[7]
  - Compositional models[8]
- Approaches for IMDPs
  - Scenario approach[9]
  - Clopper-Pearson[10]
  - Gaussian Process[11]
- Wasserstein distance-based models
  - IMDP abstraction + Wasserstein-bounded disturbances[12]

[7] Schön, O., van Huijgevoort, B., Haesaert, S., & Soudjani, S. (2024). Bayesian formal synthesis of unknown systems via robust simulation relations. IEEE TAC.

[8] Lavaei, A., Soudjani, S., & Frazzoli, E. (2023). A compositional dissipativity approach for data-driven safety verification of large-scale dynamical systems. IEEE TAC.

[9] Badings, T., Romao, L., Abate, A., Parker, D., Poonawala, H. A., Stoelinga, M., & Jansen, N. (2023). Robust control for dynamical systems with non-gaussian noise via formal abstractions. Journal of A

[10] Nazeri, M., Badings, T., Schmuck, A. K., Soudjani, S., & Abate, A. (2025). Data-Driven Abstraction and Synthesis for Stochastic Systems with Unknown Dynamics. arXiv preprint.

[11] Skovbekk, J., Laurenti, L., Frew, E., & Lahijanian, M. (2023). Formal abstraction of general stochastic systems via noise partitioning. IEEE Control Systems Letters.

[12] Gracia, I., Boskos, D., Laurenti, L., & Lahijanian, M. (2024). Data-driven strategy synthesis for stochastic systems with unknown nonlinear disturbances. L4DC, PMLR.

04

Conclusion

Conclusion

Stochastic Barrier Functions

- ✓ Sound safety bound
- ✓ Complex specifications
- ✗ Limited scalability

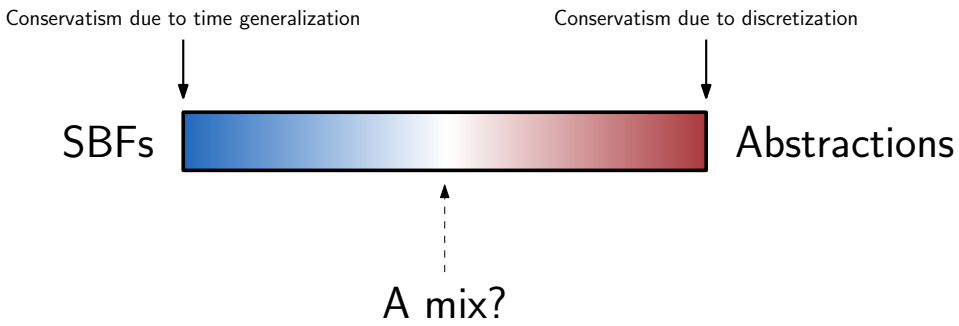
- ✗ Conservative for verification
- ✓ Useful for control design
- ✓ Standard optimization tools

Finite-state abstractions

- ✓ Sound safety bound
- ✓ Complex specifications
- ✗ Limited scalability

- ✗ Computationally expensive
- ✓ Converging to the true value
- ✓ Flexible models

What's next?


Conservatism due to time generalization
Conservatism due to discretization
SBFs
Abstractions
A mix?

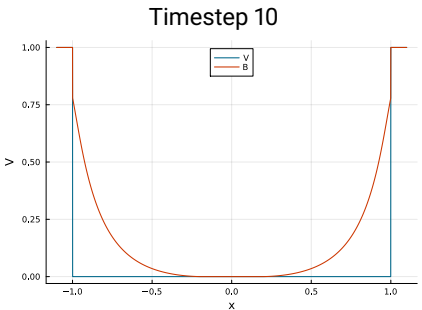
How can we guarantee safety using SBFs?

Safety via Bellman equation

$$V_0(x) = \mathbb{1}_{X_u}(x) \leq B(x)$$
$$V_k(x) \leq B(x) + \beta k \Rightarrow V_{k+1}(x) \leq B(x) + \beta(k+1)$$

So,

$$V_K(x) \leq B(x) + \beta K \quad \text{and}$$
$$P_{safe}(X_0, X_s, K) \geq 1 - \left(\sup_{x \in X_0} B(x) + \beta K \right)$$



$$\mathbf{x}[k+1] = 0.99\mathbf{x}[k] + \mathbf{v}[k],$$
$$\mathbf{v}[k] \sim \mathcal{N}(0, 0.05)$$

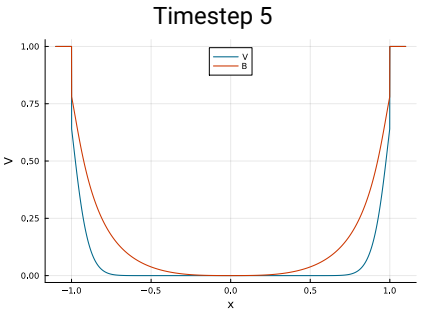
How can we guarantee safety using SBFs?

Safety via Bellman equation

$$V_0(x) = \mathbb{1}_{X_u}(x) \leq B(x)$$
$$V_k(x) \leq B(x) + \beta k \Rightarrow V_{k+1}(x) \leq B(x) + \beta(k+1)$$

So,

$$V_K(x) \leq B(x) + \beta K \quad \text{and}$$
$$P_{safe}(X_0, X_s, K) \geq 1 - \left(\sup_{x \in X_0} B(x) + \beta K \right)$$



$$\mathbf{x}[k+1] = 0.99\mathbf{x}[k] + \mathbf{v}[k],$$
$$\mathbf{v}[k] \sim \mathcal{N}(0, 0.05)$$

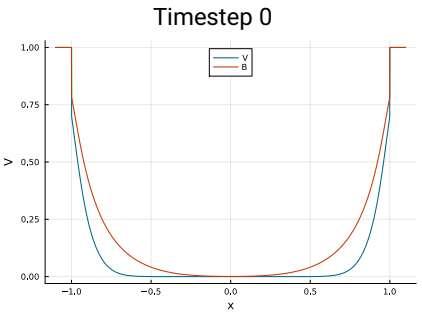
How can we guarantee safety using SBFs?

Safety via Bellman equation

$$V_0(x) = \mathbb{1}_{X_u}(x) \leq B(x)$$
$$V_k(x) \leq B(x) + \beta k \Rightarrow V_{k+1}(x) \leq B(x) + \beta(k+1)$$

So,

$$V_K(x) \leq B(x) + \beta K \quad \text{and}$$
$$P_{safe}(X_0, X_s, K) \geq 1 - \left(\sup_{x \in X_0} B(x) + \beta K \right)$$



$$\mathbf{x}[k+1] = 0.99\mathbf{x}[k] + \mathbf{v}[k],$$
$$\mathbf{v}[k] \sim \mathcal{N}(0, 0.05)$$

Piece-wise Constant Stochastic Barrier Functions

Linear Programming

The following LP synthesizes a PWC SBF guaranteeing

$$P_{safe}(X_0, X_s, K) \geq 1 - (\gamma + \beta K).$$

$$
\begin{array}{lll}
\min & \gamma + \beta K & \\
\text{s.t.} & 0 \leq B_j \leq 1 & \forall j \\
& B_j = 1 & \forall j : X_j \cap X_u \neq \emptyset \\
& B_j \leq \gamma & \forall j : X_j \cap X_0 \neq \emptyset \\
& h_j^\top \lambda_j \leq B_j + \beta & \forall j : X_j \cap X_s \neq \emptyset \\
& H_j^\top \lambda_j = \begin{bmatrix} B_1 & \cdots & B_N \end{bmatrix}^\top & \forall j : X_j \cap X_s \neq \emptyset
\end{array}
$$

$$
H_j p_j = \begin{bmatrix} -1 & & & \\ 1 & & & \\ & \ddots & & \\ & & -1 & \\ & & 1 & \\ -1 & \cdots & -1 & \\ 1 & \cdots & 1 & \end{bmatrix} p_j \leq \begin{bmatrix} -\underline{p}_{1j} \\ \bar{p}_{1j} \\ \vdots \\ -\underline{p}_{Nj} \\ \bar{p}_{Nj} \\ -1 \\ 1 \end{bmatrix} = h_j
$$

Piece-wise Constant Stochastic Barrier Functions

Projected Subgradient Descent

- Loss function

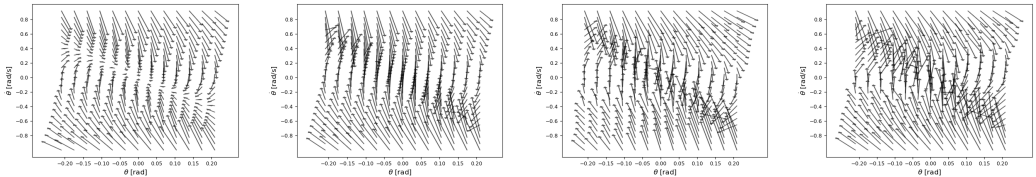
$$\mathcal{L}(B) = \gamma + \beta K$$

$$\text{where} \quad \gamma = \max_{\forall j \,:\, X_j \cap X_0 \neq \emptyset} B_j$$

$$\beta = \max_{\forall j \,:\, X_j \cap X_s \neq \emptyset} \sup_{p_j \in P_j} \max(B^\top p_j - B_j, 0)$$

- Project onto $[0, 1]^N$ where all regions $j \,:\, X_j \cap X_u \neq \emptyset$ is forced 1.

Stochastic Barrier Functions for Neural Network Dynamics Systems[13]



(a) 1 layer (b) 2 layers (c) 3 layers (d) 5 layers

Figure: Vector fields of the NNDMs for representing an inverted pendulum.

[13] Mazouz, R., Muvvala, K., Ratheesh Babu, A., Laurenti, L., & Lahijanian, M. (2022). Safety Guarantees for Neural Network Dynamic Systems via Stochastic Barrier Functions. Advances in Neural Information Processing Systems.

Computational ”hacks”

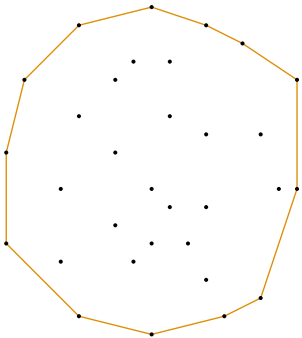


Figure: Convex hull over noise

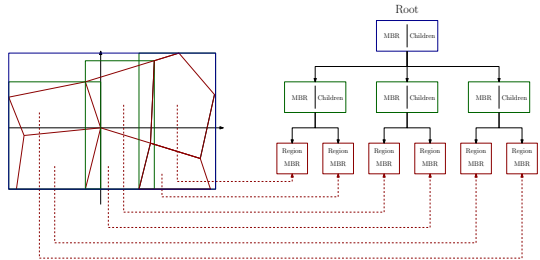


Figure: R-tree spatial indexing