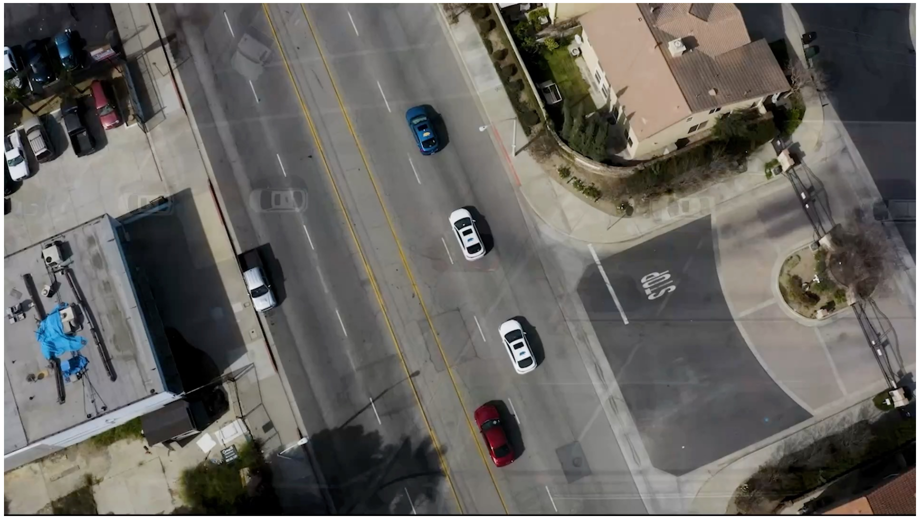
IFAC World Congress 2026

Scalable Safe Set Methods for Control and Verification with Learning

Murat Arcak
UC Berkeley

Overview

Reachable and invariant sets are critical for formal verification of safety and other requirements in autonomous systems.



Problem: Standard methods for estimating these sets do not scale to large system models.

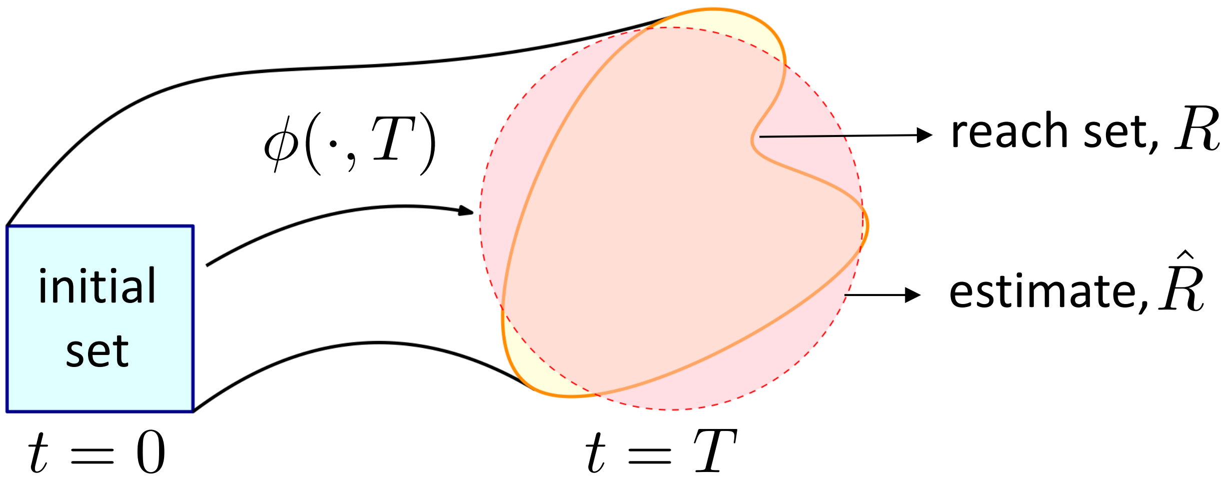
Approach in this talk: Use sample trajectories and *generalize* to unsampled ones using statistical learning.

Outline

1. Forward reachability with scenario optimization
2. Forward reachability with Christoffel functions
3. Probabilistic invariance for Gaussian Process (GP) state-space models

1. Forward Reachability with Scenario Optimization

Goal: Develop a data-driven reachability method that samples trajectories and provides a probabilistic containment guarantee.

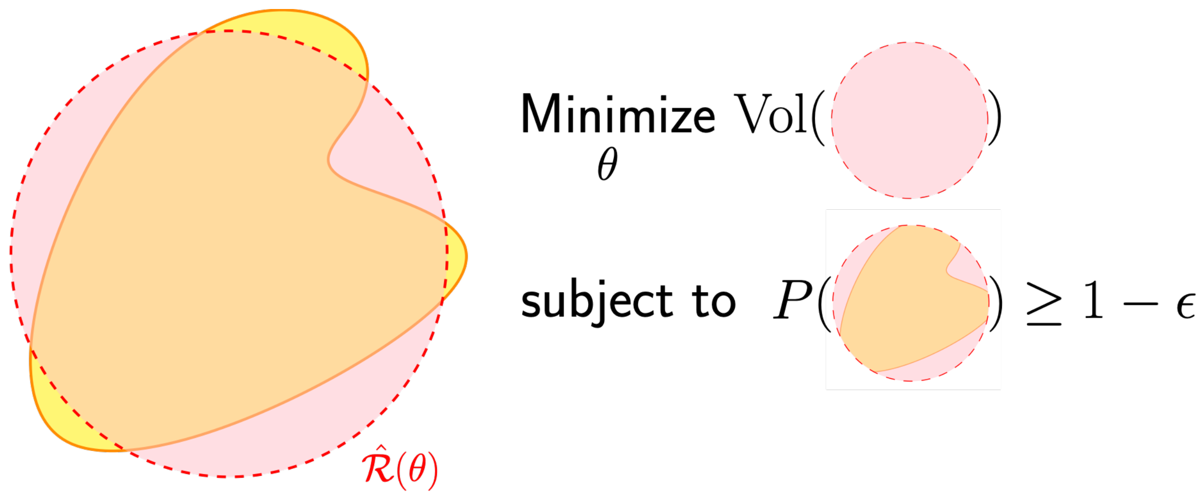


Given a probability distribution on the initial set, the solution map induces a probability measure for the exact reachable set.

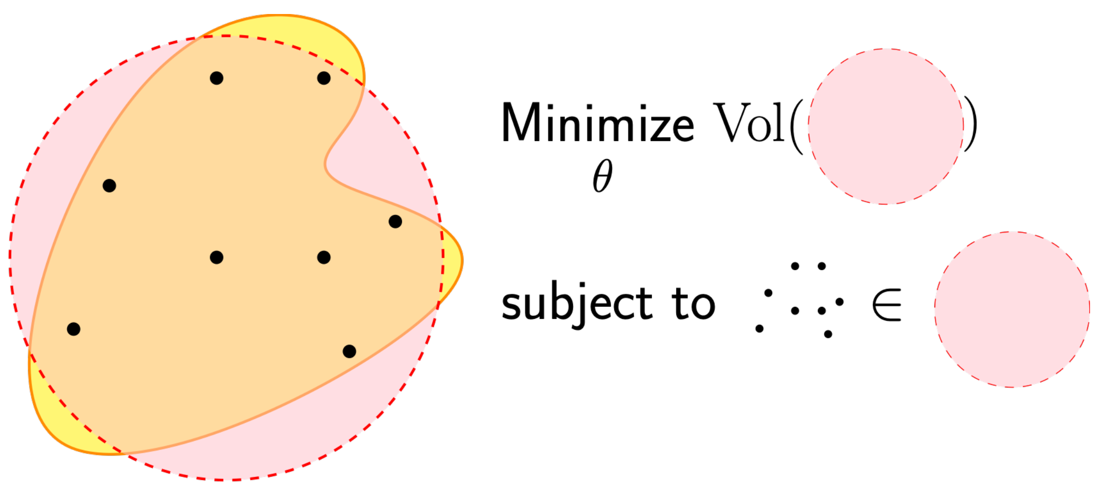
Find the smallest set from a parameterized family $\hat{R}(\theta)$ that contains $1 - \epsilon$ of the reachable set under this measure.

1. Forward Reachability with Scenario Optimization

Chance-constrained optimization problem



Approximate solution by scenario optimization



1. Forward Reachability with Scenario Optimization

Given a parameterized class of approximating sets:

$$\hat{R}(\theta) = \{x : g(x, \theta) \leq 0\}, \ \theta \in \mathbb{R}^{n_\theta}$$

and a volume proxy $\mathrm{Vol}(\theta)$.

Scenario Optimization:

$$\begin{aligned} &\min_{\theta} \mathrm{Vol}(\theta) \\ &\text{s.t.} \quad g(d_i, \theta) \leq 0, \ i = 1, \ldots, N \end{aligned}$$

where $d_i = \phi(x_i, T)$ are successors of N iid samples $\{x_i\}_{i=1}^{N}$ from the given probability distribution on the initial set.

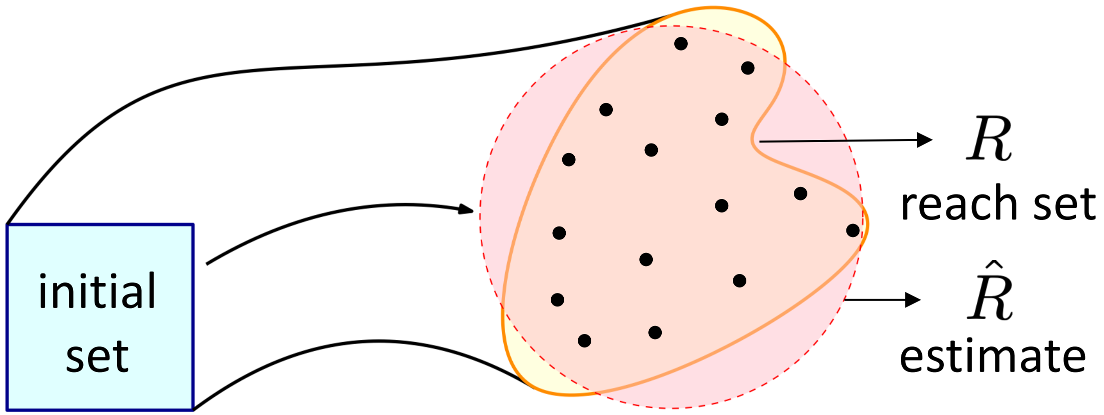
Note: convex problem if $\mathrm{Vol}(\cdot)$ and $g(x, \cdot)$ are convex

Example: $g(A, b, x) = \|Ax - b\| - 1, \ \theta = (A, b), A \succ 0$

(norm ball) $\mathrm{Vol}(\theta) = -\log\det A$

1. Forward Reachability with Scenario Optimization

How many samples do we need for $\hat{R}$ to cover $1-\epsilon$ of R ?



Thm: Assume $g(x,\cdot)$ convex. Given $\delta \in (0,1)$ we can state with $1-\delta$ *confidence* that $\hat{R}$ contains measure $1-\epsilon$ of reach set R if:

$$N \geq \frac{1}{\epsilon}\frac{e}{1-e}\left(\log\frac{1}{\delta} + n_\theta\right)$$

More precisely, the sample bound above guarantees:

$$P_R^N(\{d_1,\dots,d_N\} : P_R(\hat{R}(d_1,\dots,d_N)) \geq 1-\epsilon) \geq 1-\delta$$

1. Forward Reachability with Scenario Optimization

Next task: eliminate the convexity requirement so we can generate complex shapes with few parameters, e.g. using RBFs:

$$g(x, \underbrace{\mu, \sigma, \gamma}_{\theta}) = \sum_{n=1}^{N} e^{-\frac{1}{2}(x-\mu_n)^2/\sigma_n^2} - \gamma$$

$$\mathrm{Vol}(\theta) = \sum_{n=1}^{N} \sigma_n^2$$

Drawback: Number of samples can't be determined a priori. Samples collected in batches until accuracy passes threshold.

Approach 1: Wait-and-judge scenario optimization

\+ Major reduction in sample complexity

− Requires resolving the optimization for every scenario

Approach 2: Holdout method

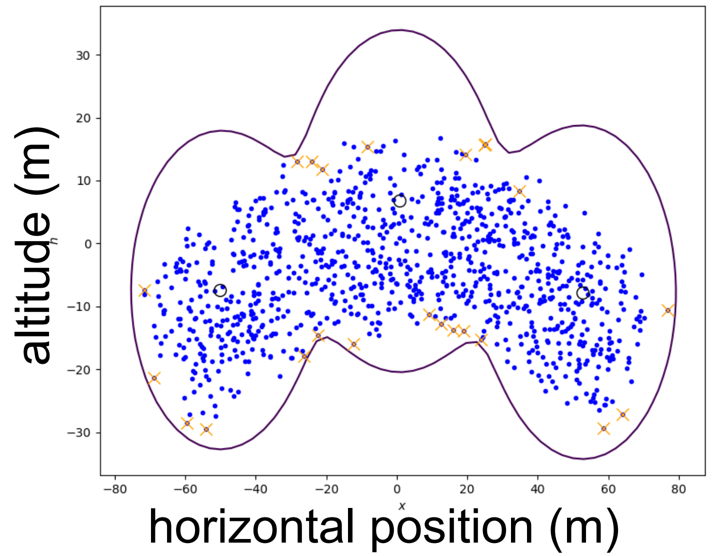
\+ Improves accuracy and reduces computation dramatically

− Requires test set, adding to sample complexity

1. Forward Reachability with Scenario Optimization

Example: Quadrotor

$$\ddot{x} = u_1 K \sin(\theta),$$
$$\ddot{h} = -g + u_1 K \cos(\theta),$$
$$\ddot{\theta} = -d_0\theta - d_1\dot{\theta} + n_0 u_2$$



Holdout Method:	Training (N)	Testing (M)	Vol($\hat{R}(\theta)$)	ε
	N = 10	M = 2990	11.50	0.765
	N = 50	M = 2950	22.97	0.280
	N = 100	M = 2900	24.29	0.120
	N = 1000	M = 2000	27.74	0.019
	N = 1500	M = 1500	27.19	0.026
	N = 2000	M = 1000	27.85	0.031
	N = 2900	M = 100	27.81	0.187
	N = 2950	M = 50	27.30	0.384
	N = 2990	M = 10	28.27	0.874
Wait and Judge:	N = 3000		27.80	0.051

Runtimes:

Holdout:
~40 sec

Wait and judge:
~ 5.5 hr

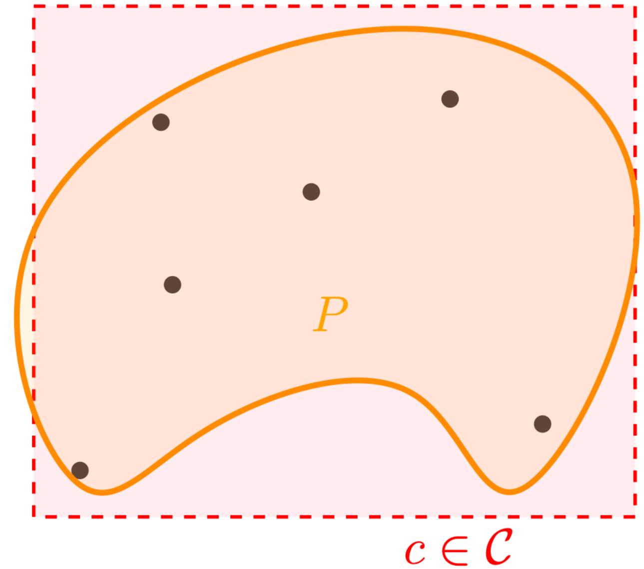
2. Forward Reachability with Christoffel Functions

Empirical Risk Minimization setup:

- i.i.d. samples $d_1, \dots, d_N \sim P$
- a class of sets $C \subseteq 2^{\mathcal{X}}$
- loss function $\ell : \mathcal{X} \times C \to \{0, 1\}$
- risk $r(c) = \mathbb{E}_P[\ell(d, c)],\ c \in C$

  and empirical risk:

$$\hat{r}(c) = \frac{1}{N} \sum_{i=1}^{d} \ell(d_i, c)$$



$$\ell(\bullet, \boxed{}) = \mathbb{1}\{\bullet \notin \boxed{}\}$$

$$r(\boxed{}) = 1 - P(\boxed{})$$

- For reachability, C: class of reach set estimates,

  $\ell(d, c)$: indicator function that returns 1 when $d \notin c$

  $r(c)$: probability that a new sample not enclosed in c

  Choose c to enclose all d_i so $\hat{r}(c) = 0$

2. Forward Reachability with Christoffel Functions

If the class C has finite Vapnik-Chervonenkis (VC) dimension, we can derive a bound for $r(c)$ that decreases with N.

Theorem (adapted from Alamo et al. 2009):

If VC dimension $\leq m$ and

$$N \geq \frac{5}{\epsilon}\left(\log\frac{4}{\delta} + m\log\frac{40}{\epsilon}\right)$$

then, with confidence $1-\delta$, we can say that the estimate c contains measure $1-\epsilon$ of the actual reach set.

Lemma: For an m-dimensional vector space $\mathbb{V}$ of functions $g:\mathbb{R}^n \to \mathbb{R}$, the class of sublevel sets of g has VC dimension m.

2. Forward Reachability with Christoffel Functions

The empirical inverse Christoffel function of order k is the degree $2k$ polynomial

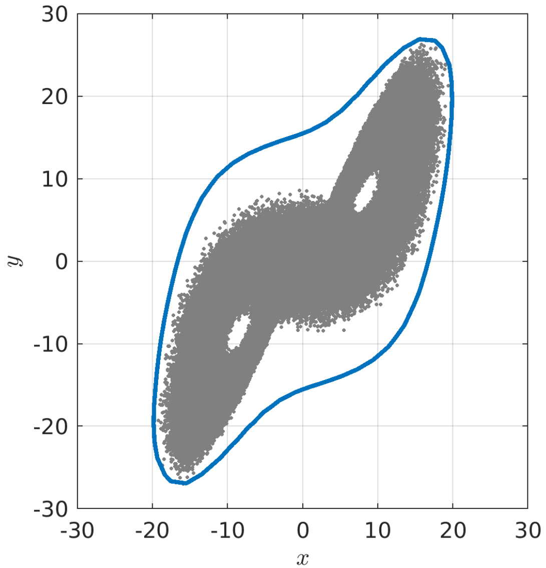
$$C_k(x) = \underbrace{z_k(x)^\top}_{\text{vector of monomials}} \underbrace{\left(\frac{1}{N}\sum_{i=1}^{N} z_k(d_i) z_k(d_i)^\top\right)^{-1}}_{\text{empirical moment matrix}} z_k(x).$$

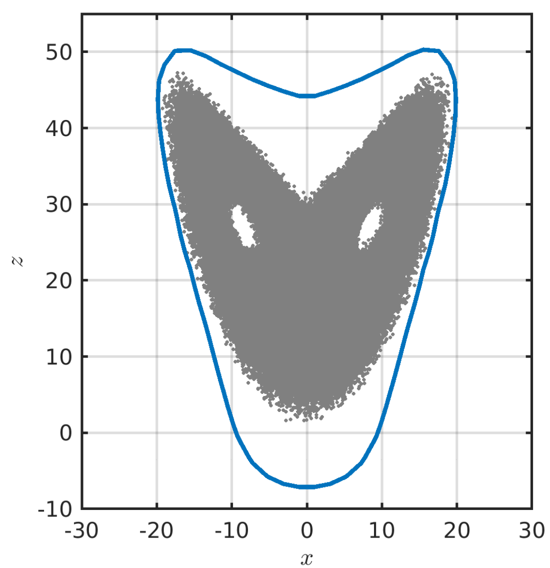
Use sublevel set, with level $= \max_i C_k(d_i)$ as reach set estimate.
VC dimension $m \leq \binom{n_x+2k}{n_x}$ so theorem above is applicable.

Why Christoffel functions?

- sublevel sets known for support-approximating quality in ML
- can morph into complex shapes (e.g., holes or disconnected)

2. Forward Reachability with Christoffel Functions

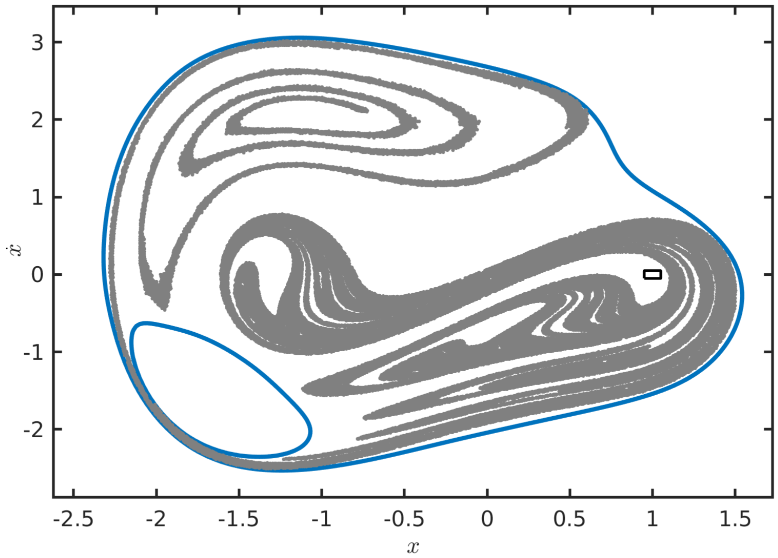




Lorenz oscillator

$n_x = 3, k = 5$

$N = 193,391$



Duffing oscillator

$n_x = 2, k = 10$

$N = 156,626$

$(\epsilon = 0.05, \delta = 10^{-9})$

3. Probabilistic Invariance for GP State-Space Models

Gaussian Process (GP): Collection of random variables $\mathbf{f}(x)$ indexed by x, where any finite subset is jointly Gaussian.

Mean: $m(x) = \mathbb{E}[\mathbf{f}(x)]$

Covariance: $k(x, x') = \mathbb{E}[(\mathbf{f}(x) - m(x))(\mathbf{f}(x') - m(x'))]$

Covariance called stationary if it depends only on $|x - x'|$

e.g., $k(x, x') = \exp\left(-|x - x'|^2/2\right)$

For any collection $\{x_1, \ldots, x_n\}$:

$$\begin{bmatrix} \mathbf{f}(x_1) \\ \vdots \\ \mathbf{f}(x_n) \end{bmatrix} \sim \mathcal{N}\left(\begin{bmatrix} m(x_1) \\ \vdots \\ m(x_n) \end{bmatrix}, \begin{bmatrix} k(x_1, x_1) & \cdots & k(x_1, x_n) \\ \vdots & \ddots & \vdots \\ k(x_n, x_1) & \cdots & k(x_n, x_n) \end{bmatrix} \right)$$

3. Probabilistic Invariance for GP State-Space Models

GP State-Space Model:

$$x_{k+1} = Ax_k + Bu_k + g(x_k, u_k) + w_k, \quad x_k \in \mathbb{R}^n$$

$$g_i \sim \mathrm{GP}(0, k_i) \text{ with } \textit{stationary } k_i$$

$$w_k \sim \mathcal{N}(0, Q)$$

Conditioning on data $\mathcal{D} = \{(\bar{x}_j, \bar{u}_j), \bar{x}_j^+\}_{j=1}^N$ yields posterior:

$$g(x_k, u_k) | \{x_k, u_k, \mathcal{D}\} \sim \mathcal{N}(\mu(x_k, u_k), \Sigma(x_k, u_k))$$

where μ, Σ depend on $\mathcal{D}, \{k_i\}_{i=1}^n$.

Using stationarity we can find bounds:

$$\|\mu(x, u)\| \leq \overline{\mu} \quad \forall x, u$$

$$\Sigma(x, u) \preceq \overline{\Sigma} \quad \forall x, u$$

3. Probabilistic Invariance for GP State-Space Models

With feedback $u = Lx$ the closed-loop system becomes:

$$x_{k+1} = (A + BL)x_k + d_k + v_k(x_k)$$

$$\mathbb{E}[v_k(x_k)|x_k] = 0,\ \mathrm{Cov}[v_k(x_k)|x_k] \preceq \overline{\Sigma} + Q$$

$$\|d_k\| \leq \overline{\mu}$$

Given $W \succeq 0$ define ellipsoid $\mathcal{E}(W) = \{W^{1/2}x : \|x\| \leq 1\}$

Theorem (Probabilistic Invariance): If we can find a set $X \subset \mathbb{R}^n$ s.t.

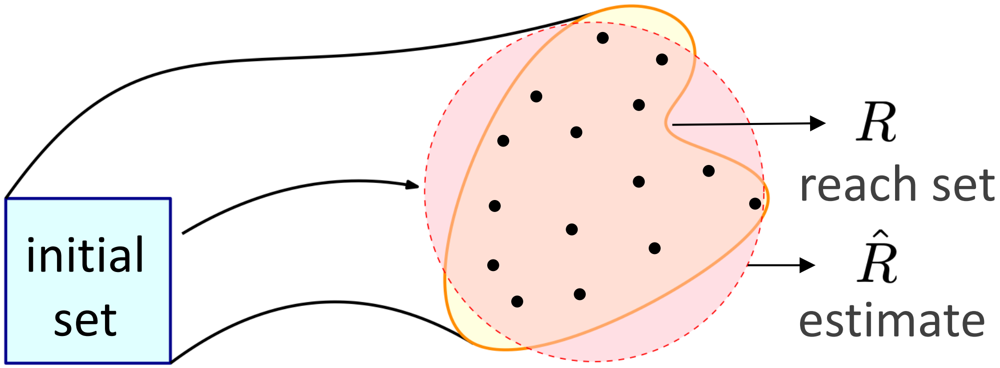
$$(A + BL)\,X \oplus \mathcal{E}(\overline{\mu}^2 I) \oplus \mathcal{E}\left(\frac{n}{1-p}(\overline{\Sigma} + Q)\right) \subseteq X \qquad (\dagger)$$

Then: $x_o \in X \implies \Pr(x_k \in X) \geq p \ \ \forall k \geq 1$

We formulate a semidefinite program to search for L and an ellipsoidal X satisfying (†). We then maximize p via bisection.

Conclusions

- Proposed a sampling approach for scalable estimation of reachable and invariant sets.



- To generalize from samples to unsampled trajectories, we used probabilistic structure and regularity of sets.
- Past work emphasized forward reachability. Now exploring backward reachable and controlled invariant sets. Essential for characterizing safe envelopes for autonomous systems.
- Gaussian Processes are promising for blending models and data. Demonstrated their use for probabilistic set invariance.

References

- Devonport and Arcak. *Estimating reachable sets with scenario optimization.* L4DC 2020
- Dietrich, Devonport and Arcak. *Nonconvex scenario optimization for data-driven reachability*. L4DC 2024
- Dietrich, Devonport, Tu, Arcak. *Data-driven reachability with scenario optimization and the holdout method.* CDC 2025
- Devonport, Yang, El Ghaoui, Arcak. *Data-driven reachability analysis and support set estimation with Christoffel functions.* IEEE TAC 2023
- Griffioen, Zhong, Arcak, Zamani, Caccamo. *Controlled invariant sets for Gaussian Process state space models.* Under review.