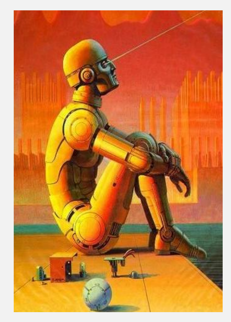
Data-Driven Cyberphysical Systems

Provably correct control in data rich/labels scarce scenarios

Northeastern



Robust Systems Lab

Begüm Taşkazan

Tianyu Dai

Mario Sznaier

Collaborators from other institutions

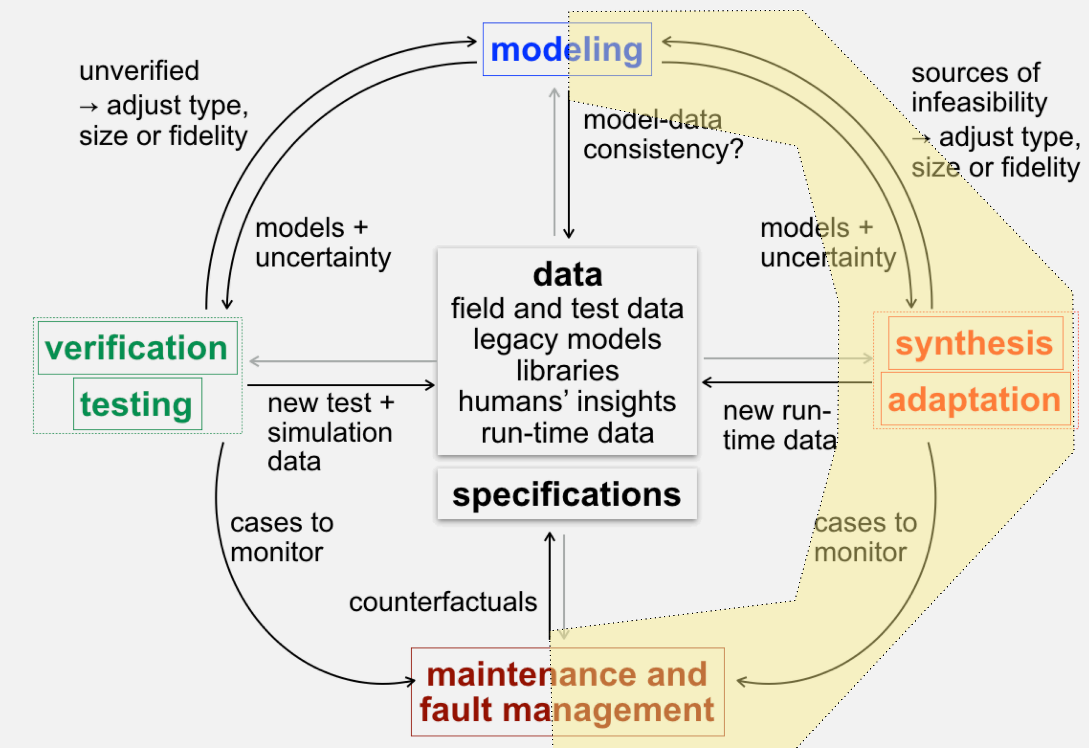
Baihong Jin
Xiangyu Yue
Uduak Inyang-Udoh
Yuxin Chen
Alexander Nettekoven
Sandipan Mishra
A. Sangiovani-Vincentelli
Ufuk Topcu
Yisong Yue

Motivation

How can we synthesize control strategies for CPS in scenarios with rich run-time data, but where labeling is expensive and off-line training may not capture rare but potentially catastrophic events?

Challenges

- Obtaining space-spanning data, specially for situations involving unsafe operations
- Real-time labeling with certifiable performance, even for data previously unseen
- Synthesizing non-conservative, provably stabilizing control laws



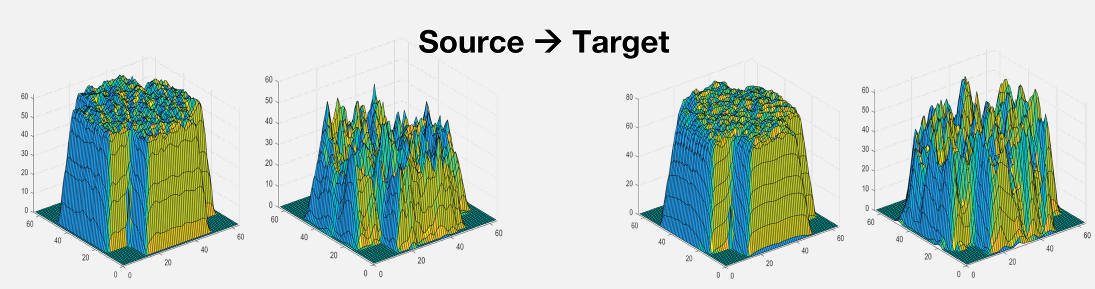
Leveraging Simulations to Handle Scarce Labels

Goal: Leverage simulations to obtain spanning data

- Obtaining enough trajectory space spanning data for CPS can be costly or unfeasible
- Physics based simulators can generate data cheaply, but require costly tuning to match the actual CPS

Proposed approach: Domain adaptation

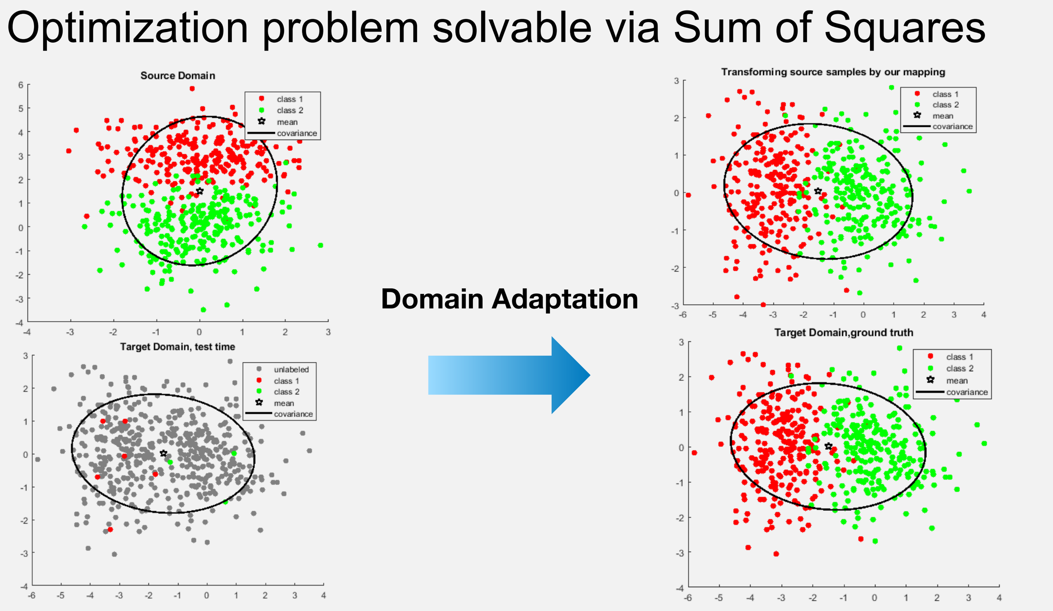
- Generate a large simulation dataset (source) and collect a smaller set of (labeled) real data (target)
- Find a transformation from source to target that optimizes classification accuracy
- Use simulator adapted data for classification and controller design



Training Data (Left: Regular Simulation, Right: Clogged Nozzle)   *Testing Data (Left: Regular Scenario, Right: Clogged Nozzle)*

Technical details:

- Align covariances and use the extra degrees of freedom to optimize classification accuracy
- Optimization problem solvable via Sum of Squares



Training Input (Top: Source, Bottom: Target)   *Training Output /Testing (Top: Transformed Source, Bottom: Ground Truth Target)*

Results:

	PCA300	PCA200	PCA100	PCA20
Accuracy on Target after adaptation	85.91% (↑11.26%)	86.45% (↑12.94%)	86% (↑11%)	81.67% (↑2.64%)

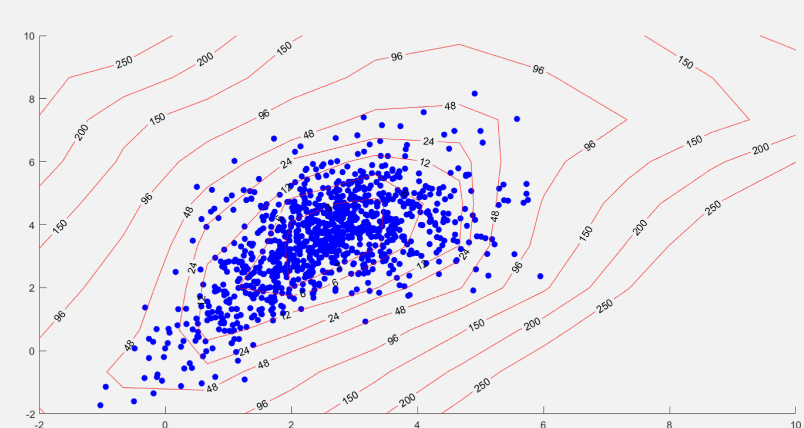
Efficient Data Labeling

Goal: On the fly data labeling

- On the fly data labeling is challenging in the presence of rare events
- Traditional learning relying on large amounts of training data may not be feasible in some CPS applications

Proposed approach: SoS based classifiers

- Use empirical statistical information to build SoS polynomials that approximate the support of the data
- Given an unknown sample, assign it to the most likely distribution or label it as "unseen before" (with certified probability of miss-classification)



N=1000, d=2, n=2

Technical details:

- Lift the data:

$$\mathbf{x} \doteq [x_1 \dots x_d] \rightarrow \mathbf{v}_n(\mathbf{x}) \doteq [1 \quad x_1 \quad x_2 \quad \dots (x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_d^{\alpha_d}) \dots x_d^n]^T$$

- Create the moment matrix:

$$\mathbf{M} \doteq \frac{1}{N} \sum_{i=1}^{N} \mathbf{v}_n(\mathbf{x}_i)\mathbf{v}_n^T(\mathbf{x}_i)$$

- Classify unknown samples y according to:

$$Q(\mathbf{y}) \doteq \mathbf{v}_n^T(\mathbf{y})\mathbf{M}^{-1}\mathbf{v}_n(\mathbf{y})$$

- Certificate:

$$\textbf{prob}\,\{Q(\mathbf{y}) > t\} < \frac{t}{s} \textbf{ where } s = \binom{d+n}{n}$$

Results:

	PCA300	PCA200	PCA100	PCA20
Accuracy (SVM)	96.20%	95.91%	95.76%	89.91%
Accuracy (SoS)			99.56%	95.03%

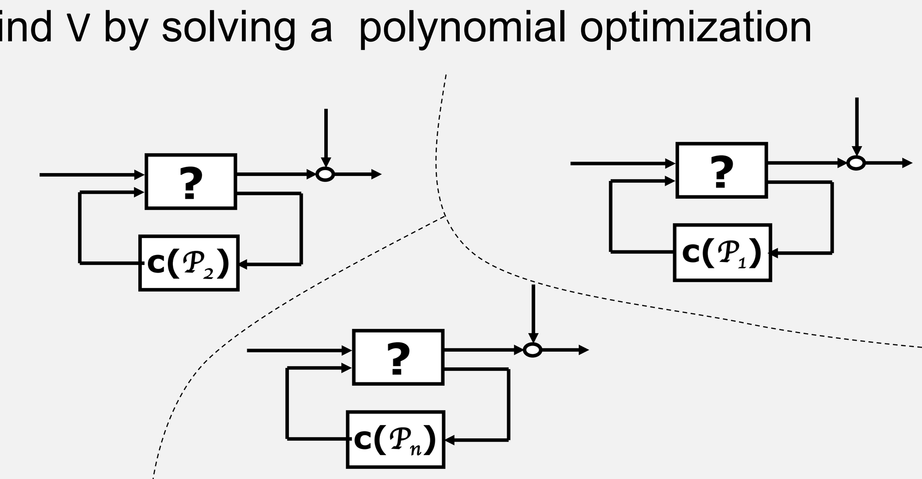
Non-conservative Control Synthesis

Goal: Synthesizing certified controllers

- Traditional approach based on SysId + Robust Control is computationally expensive and potentially conservative
- Existing model free data-driven approaches cannot certify stability or performance

Proposed approach: Lyapunov based DD control

- Define the consistency set S as the set of all plants compatible with existing priors and experimental data
- (non-conservatively) parameterize the set of all controllers the can stabilize S in terms of a polyhedral Lyapunov function V
- Find V by solving a polynomial optimization

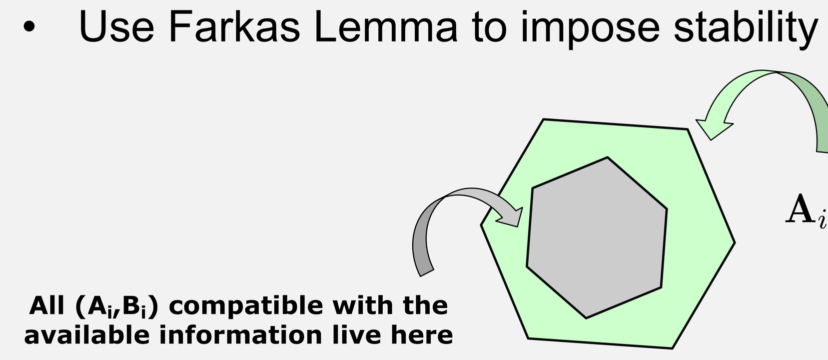


Technical details:

- The set of all (LTI) plants in S is a polytope P
- Use the fact that U_i stabilizes (A_i, B_i) iff there exist V, H_i

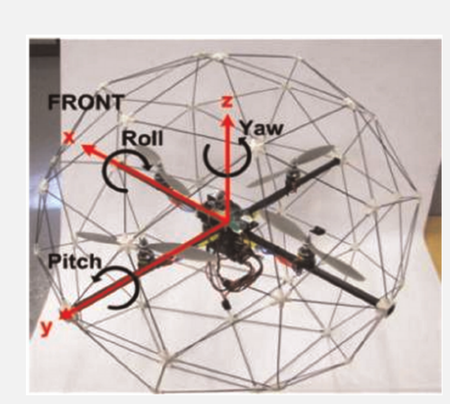
$$\begin{aligned} \mathbf{A}_i\mathbf{V} + \mathbf{B}_i\mathbf{U}_i &= \mathbf{V}\mathbf{H}_i, \\ \|\mathbf{H}\|_{\ell_1 \to \ell_1} &\leq d < 1 \end{aligned}$$

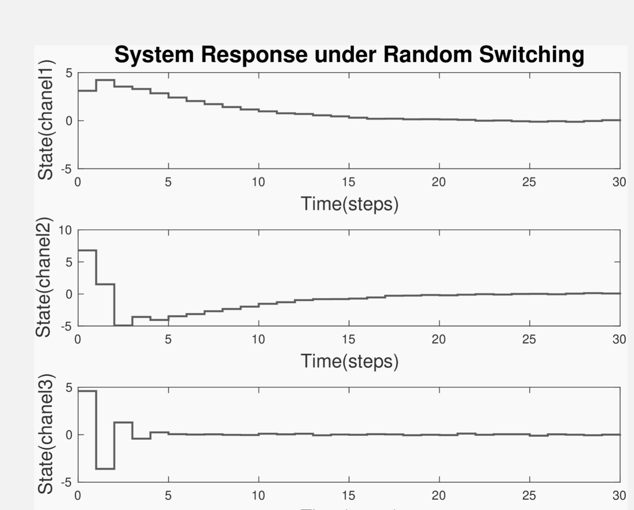
- Use Farkas Lemma to impose stability of P



$$\begin{aligned} \mathbf{A}_i\mathbf{V} + \mathbf{B}_i\mathbf{U}_i &= \mathbf{V}\mathbf{H}_i, \\ \|\mathbf{H}\|_{\ell_1 \to \ell_1} &\leq d < 1 \end{aligned}$$

Results:





http://DataDrivenCPS.org — {taskazan.b,dai.t}@husky.neu.edu, msznaier@coe.neu.edu

Grant CNS 1646121