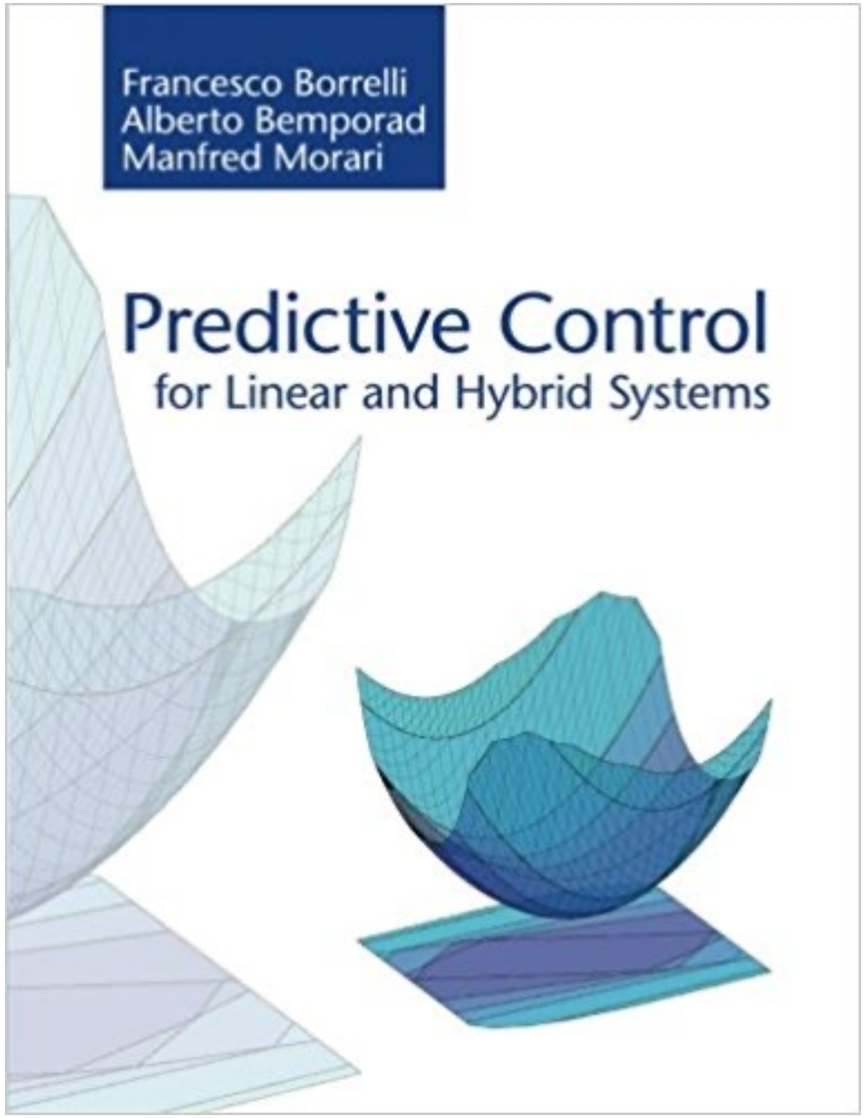
Safe CPS: Complexity, Guarantees and Conservatism

Francesco Borrelli

Email: fborrelli@berkeley.edu
University of California
Berkeley, USA

www.mpc.berkeley.edu

25 years of Predictive Control Research



Disciplined Control Design with Safety Guarantees

$$\begin{array}{ll} \min_{\pi_0,\pi_1,\ldots,\pi_T} & \text{cost over T} \\ \text{s.t.} & \text{uncertain model} \\ & \text{constraints} \end{array}$$

Principles

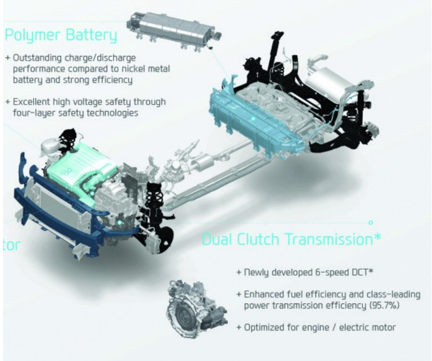
- Lift and project to enable abstractions at different level of architecture
- Bound uncertainty to design for robustness
- Use Control Invariants and CLF at end of horizon

Predictive Control Lab Success – Industrial , Widely Deployed

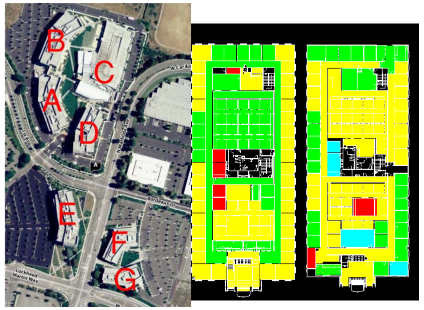
- Transportation
- Energy
- Advanced Robotics

Solar Power Plans

Autonomous Vehicles



Vehicle Powertrain



Building HVAC

Todays Complex Control Problems

- ***Complex** architectures*
  - *Hard to find people with system-level knowledge*

- *Abstraction at each level is **complex***
  - *Pushing the performance boundaries*
  - *Limited computation*
  - *Complex human interaction*

Toyota Research Institute
Mar 23 · 8 min read · Listen

Leveraging Envelope Control to Unlock Capabilities for Future Vehicle Safety Systems

TRI's Approach to Shared Control and Autonomy

By: Dr. Carrie Bobier-Tiu, Dr. Sarah Koehler

In comparison to peers, Toyota Research Institute (TRI) has a unique perspective on autonomous vehicles. One of the many reasons we were both drawn to working at TRI was the focus on applications of new technologies, particularly those being developed for autonomy, to continually improve driver safety. This focus on driver safety and autonomy has led to Toyota's Guardian and Chauffeur concepts.

"Academic Success" in this Context

Complex Problem

Systematic Solution

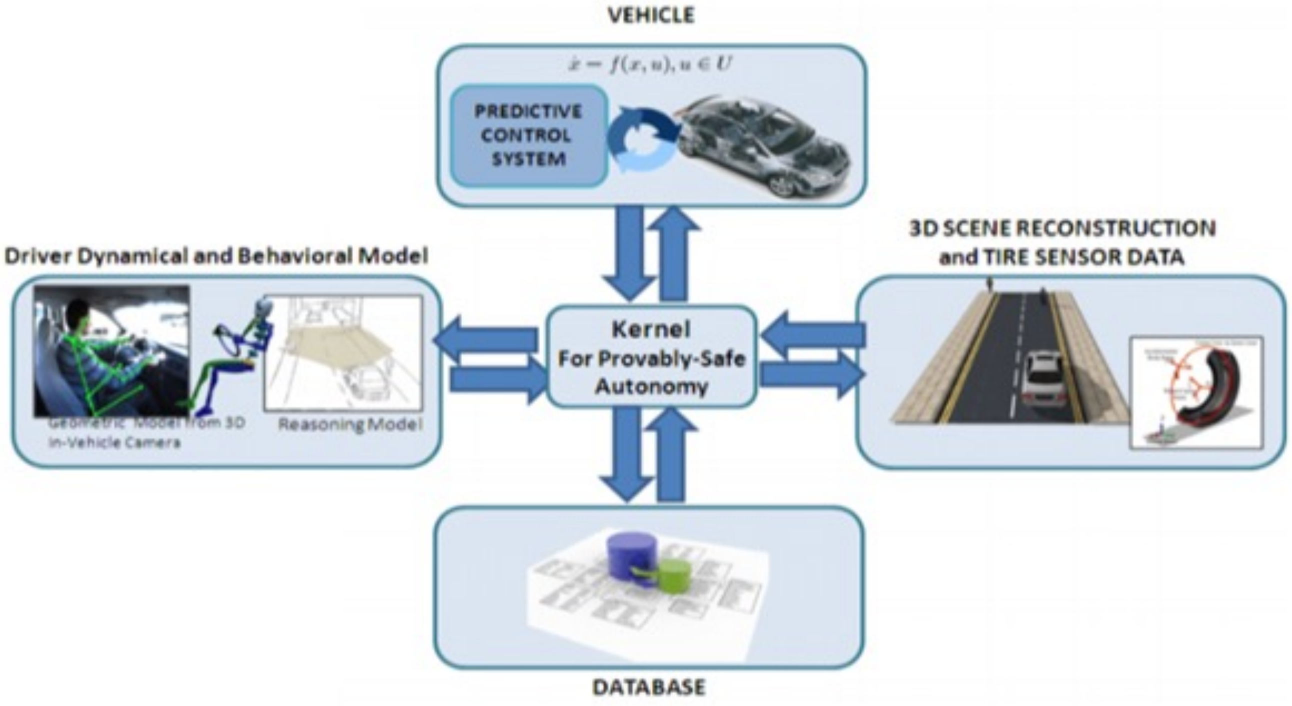
Provides Guarantees

Not Conservative

Generalize

Very Hard

2012 CPS: Provably Safe Automotive Cyber-Physical Systems with Humans-in-the-Loop

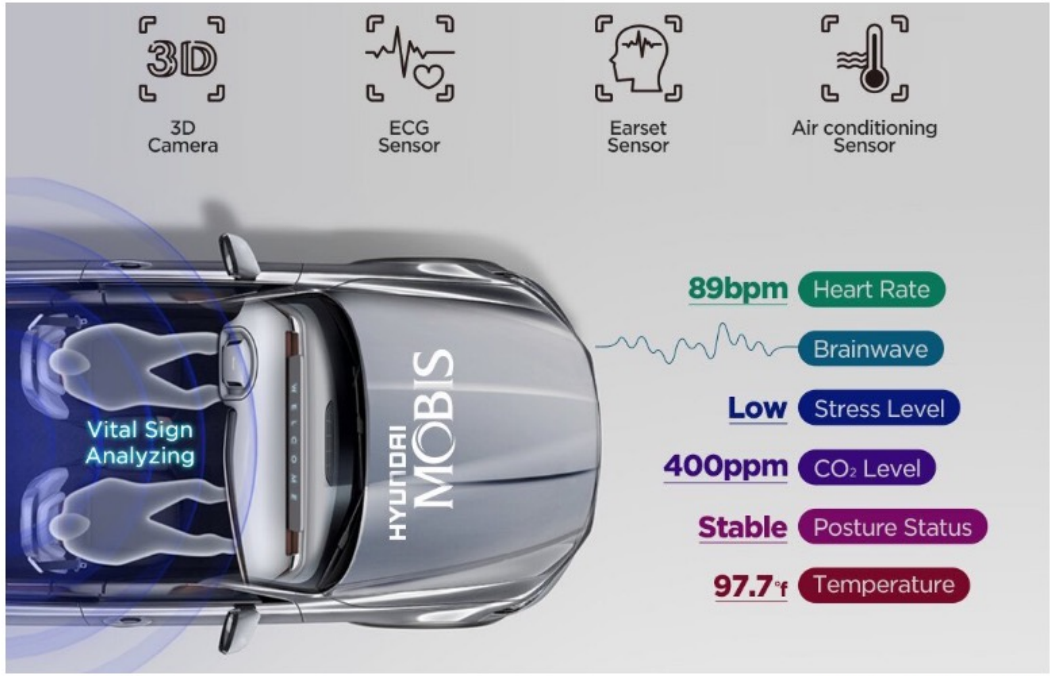


OVERVIEW

- When to intervene to obtain a provably safe closed-loop behavior
- How to enable real-time operations on embedded platforms
- How to quantify uncertainty in the environment using large data sets

Any Impact? -Yes

By **Adam Ang** | June 24, 2022 | 12:17 am



Credit: Hyundai Mobis

Toyota Research Institute
Mar 23 · 8 min read · Listen

Leveraging Envelope Control to Unlock Capabilities for Future Vehicle Safety Systems

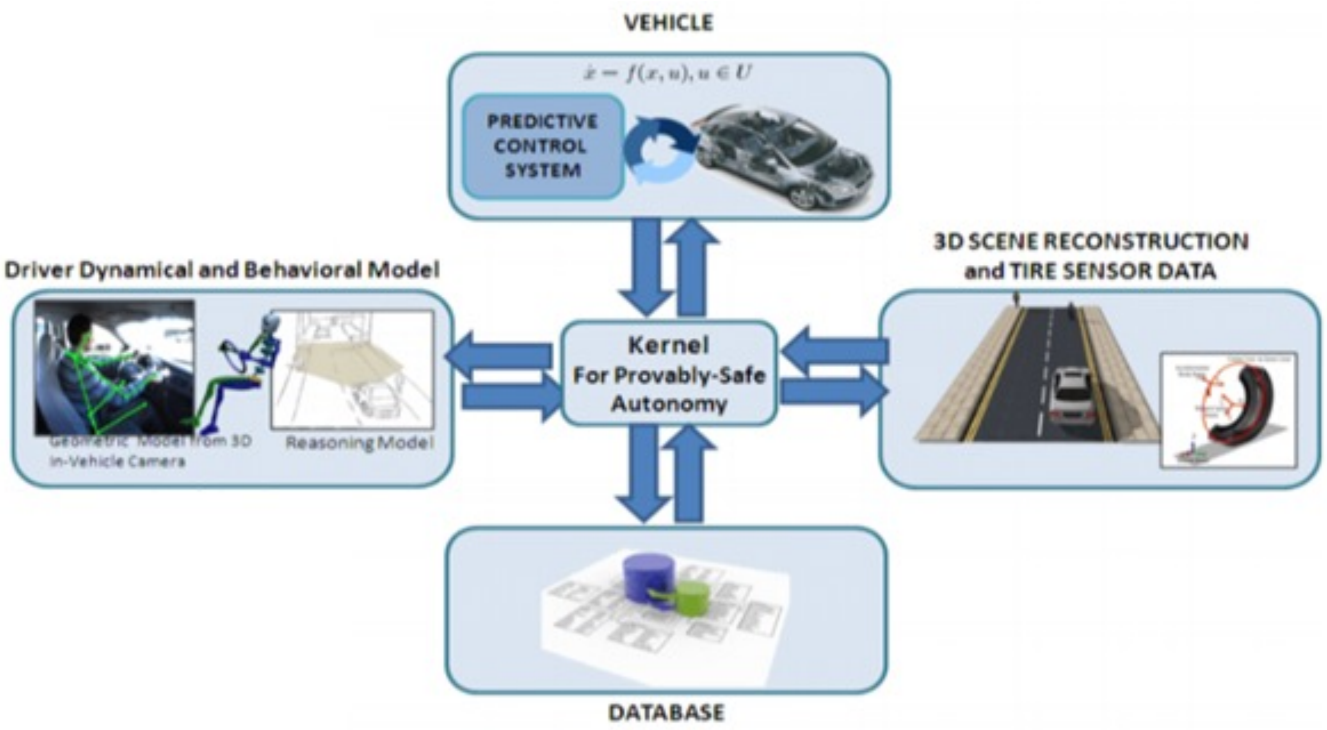
TRI's Approach to Shared Control and Autonomy

By: Dr. Carrie Bobier-Tiu, Dr. Sarah Koehler

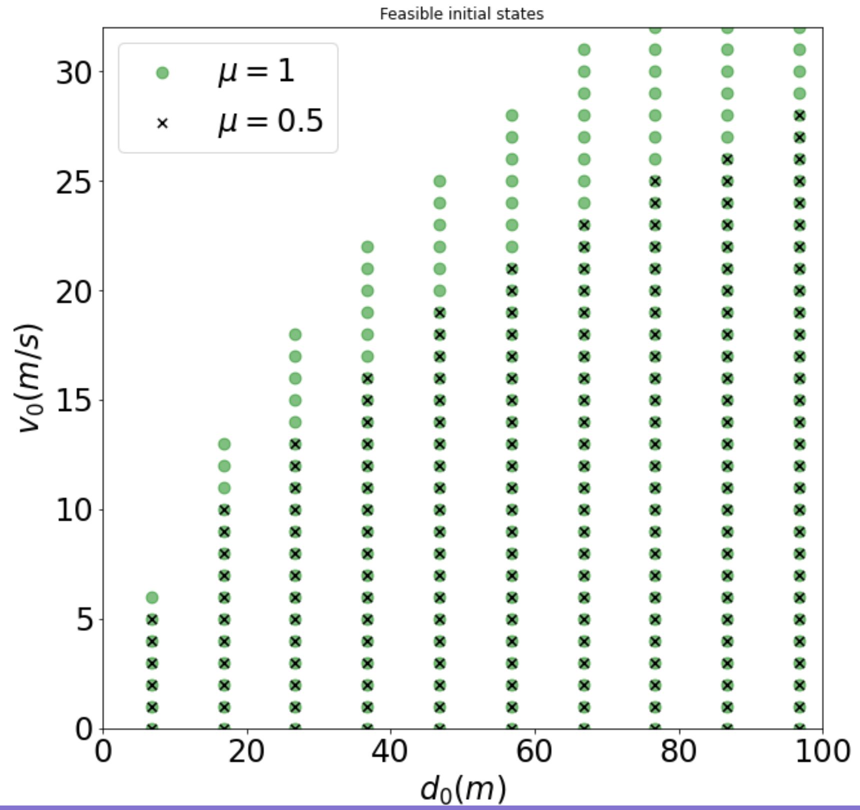
In comparison to peers, Toyota Research Institute (TRI) has a unique perspective on autonomous vehicles. One of the many reasons we were both drawn to working at TRI was the focus on applications of new technologies, particularly those being developed for autonomy, to continually improve driver safety. This focus on driver safety and autonomy has led to Toyota's Guardian and Chauffeur concepts.

Any Impact? - No

- *Revolutionize how controllers were designed*
- *Provide System Guarantees*
- *Safety Centric architecture*



Example Safe ACC Design



Model

$$\dot{x}(t) = v(t)$$
$$\dot{v}(t) = a(t)$$

Front Car Model

Constraints

$$x \leq d_{safe}$$
$$v \geq 0, \;\; v \leq v_{max}$$
$$-\mu g \leq u \leq \mu g$$

Sampled

Control invariant Set

https://colab.research.google.com/drive/1uao3-OKkTirBqQ68W9_xqit46dROU18S?usp=sharing

Discussion

- **Beautiful disciplined approach**
- **Beautiful theory with safety guarantees**
- **Oversimplified abstraction**

Complex Problem

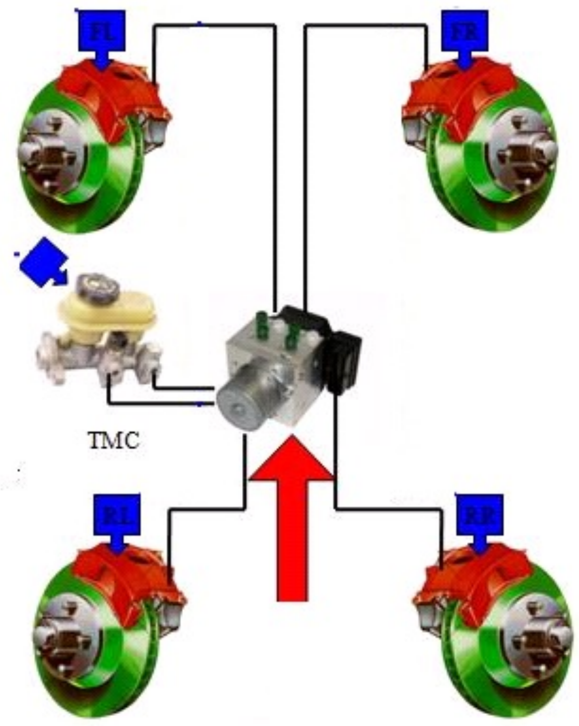
Systematic Solution

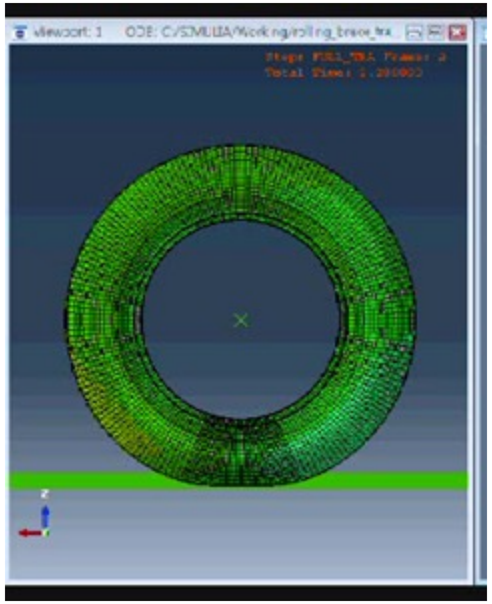
Provides Guarantees

~~Not Conservative~~

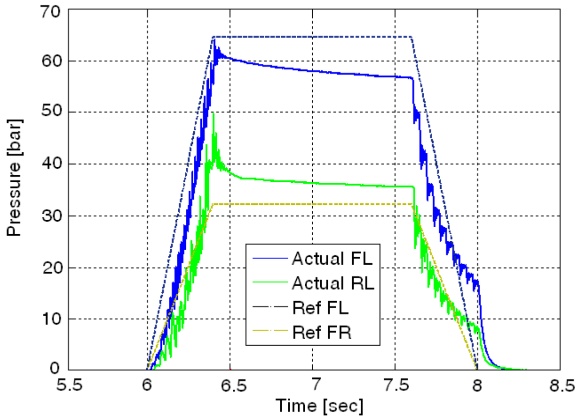
~~Generalize~~

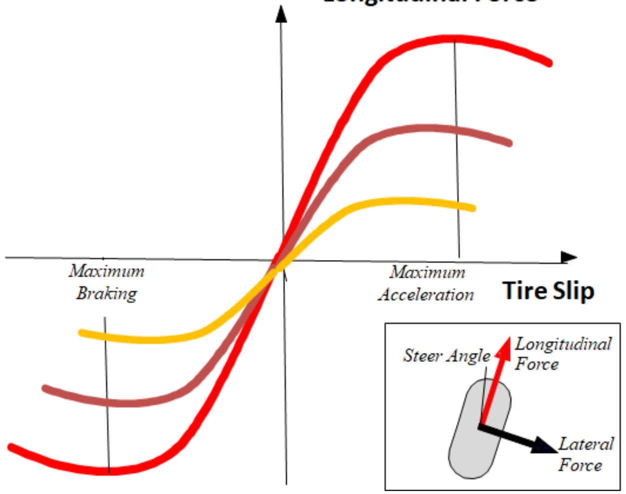
The brake system





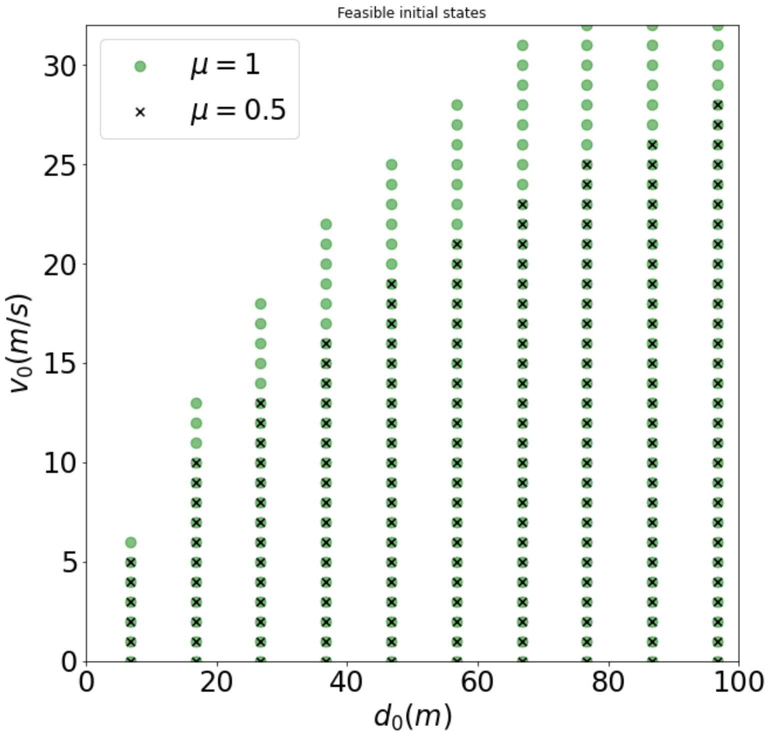
Tests carried by
Velardocchia's Lab University of Torino





Discussion

- **Beautifully, disciplined approach**
- **Beautiful theory with safety guarantees**
- **Questionable Abstraction**
- **Conservative (to the point of being useless)**



Complex Problem

Systematic Solution

Provides Guarantees

~~Not Conservative~~

~~Generalize~~

Today’s question

Can we use data and communication to bound the risk of failure in a non-conservative way?

The Theory of “Disciplined Learning” in Predictive Control.

Learning in Model Predictive Control
Safety and Robustness

Ugo Rosolia, Monimoy Bujarbaruah, Francesco Borrelli

November 3, 2022

Outline

- A success on a simple example
- A success on a more complex example
- A complex problem without a systematic solution

Outline

- **A success on a simple example**
- A success on a more complex example
- A complex problem without a systematic solution

Data-driven Constrained LQR

Infinite Time Constrained LQR

$$\min_{\pi_0(\cdot),\pi_1(\cdot),\ldots} \quad E\left(\sum_{k=0}^{\infty} x_k' Q x_k + u_k' R u_k\right)$$

$$\begin{aligned} \text{s.t} \quad & x_{k+1} = A x_k + B u_k + w_k \\ & u_k = \pi_k(x_k) \in \mathcal{U} \\ & x_k \in \mathcal{X} \ \forall w_k \in \mathcal{W} \end{aligned}$$

Complex Problem $\leftrightarrow$ Curse of dimensionality

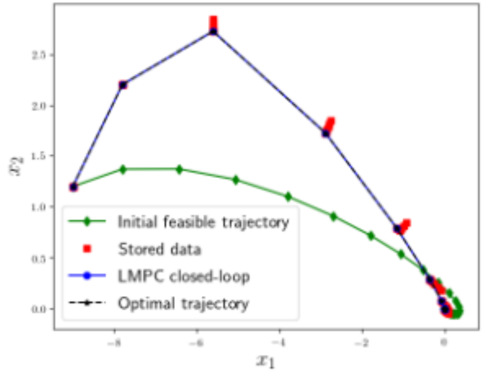
Github and Google Colab Solutions

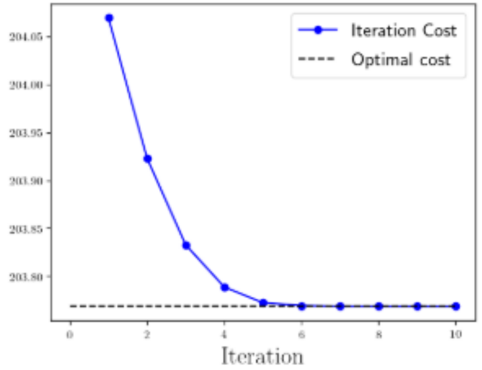
Linear LMPC

This code runs the LMPC from [1] and [2] to solve the following Contratined LQR problem

$$
\begin{aligned}
J^*_{0\rightarrow\infty}(x_S) = \min_{u_0,u_1,\ldots} \quad & \sum_{k=0}^{\infty} \left[||x_k||_2^2 + ||u_k||_2^2 \right] \\
\text{s.t.} \quad & x_{k+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} x_k + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_k, \ \forall k \geq 0 \\
& x_0 = x_S, \\
& \begin{bmatrix} -10 \\ -10 \end{bmatrix} \leq x_k \leq \begin{bmatrix} 10 \\ 10 \end{bmatrix} \quad \forall k \geq 0 \\
& -1 \leq u_k \leq 1 \quad \forall k \geq 0.
\end{aligned}
$$

The LMPC will improve the closed-loop performance, unitl the closed-loop trajectory converges to a steady state behavior. This state state closed-loop trajectory is the unique gloabl optimal solution to above control problem, if some the technical conditions hold. For more details we refer to [1].



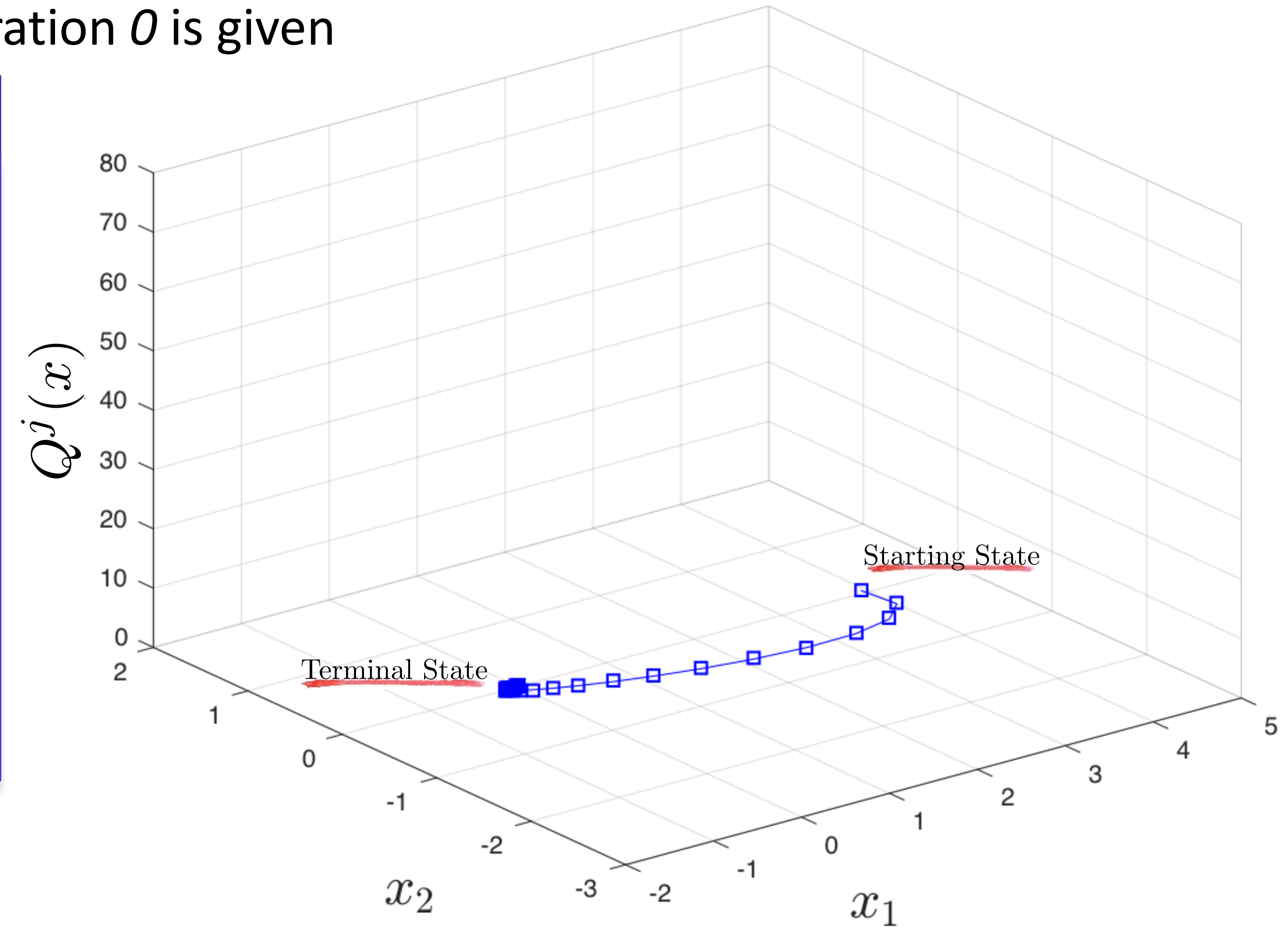


https://colab.research.google.com/drive/19x7K2jZXDOHKWFs4A7LW_uA0OIrpT9IJ?usp=sharing

Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC



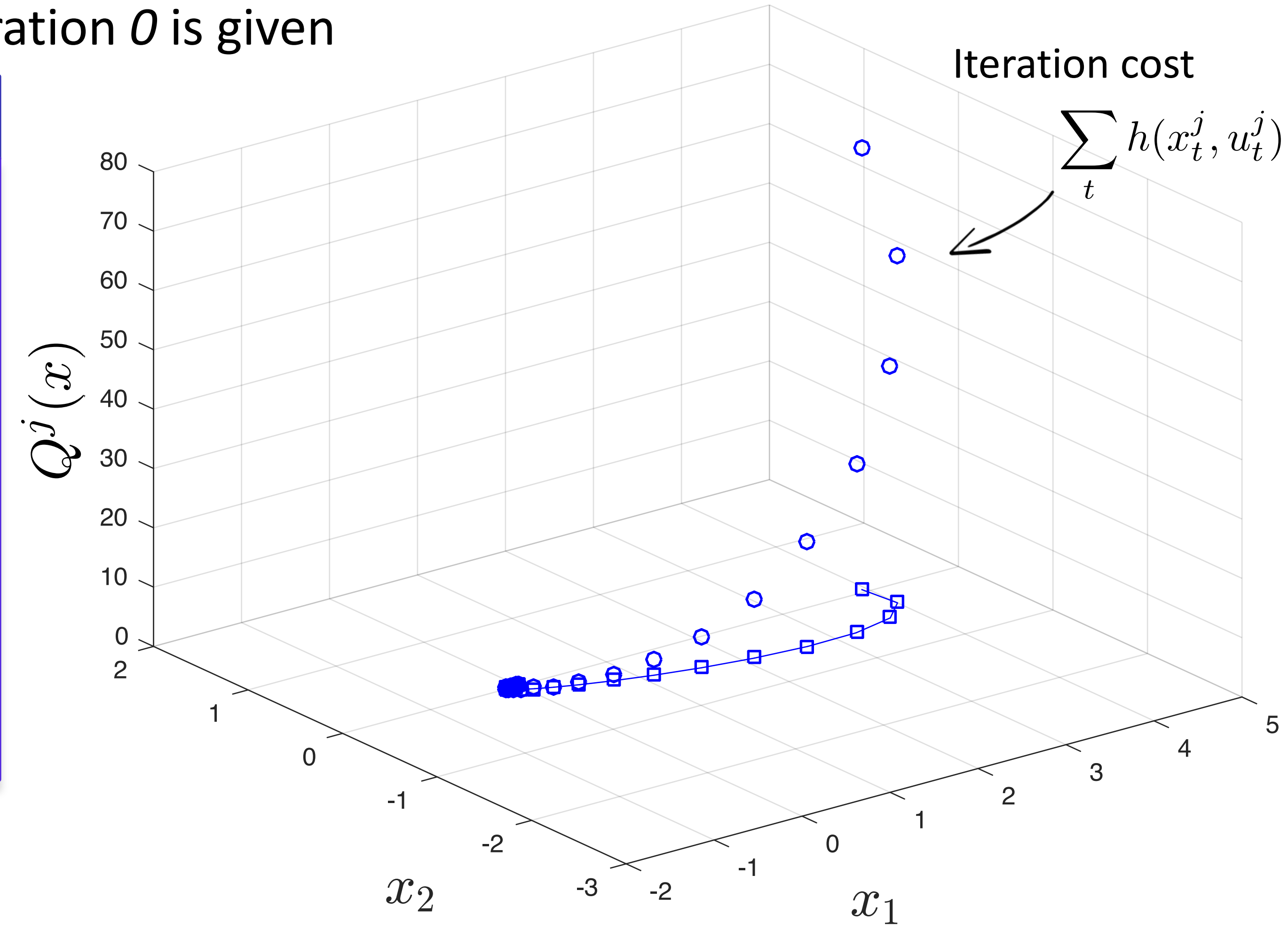
Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC

Step 0: Set iteration counter *j=0*

Step 1: Compute the roll-out cost for the recorded data up to iteration *j*



Example I: Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC

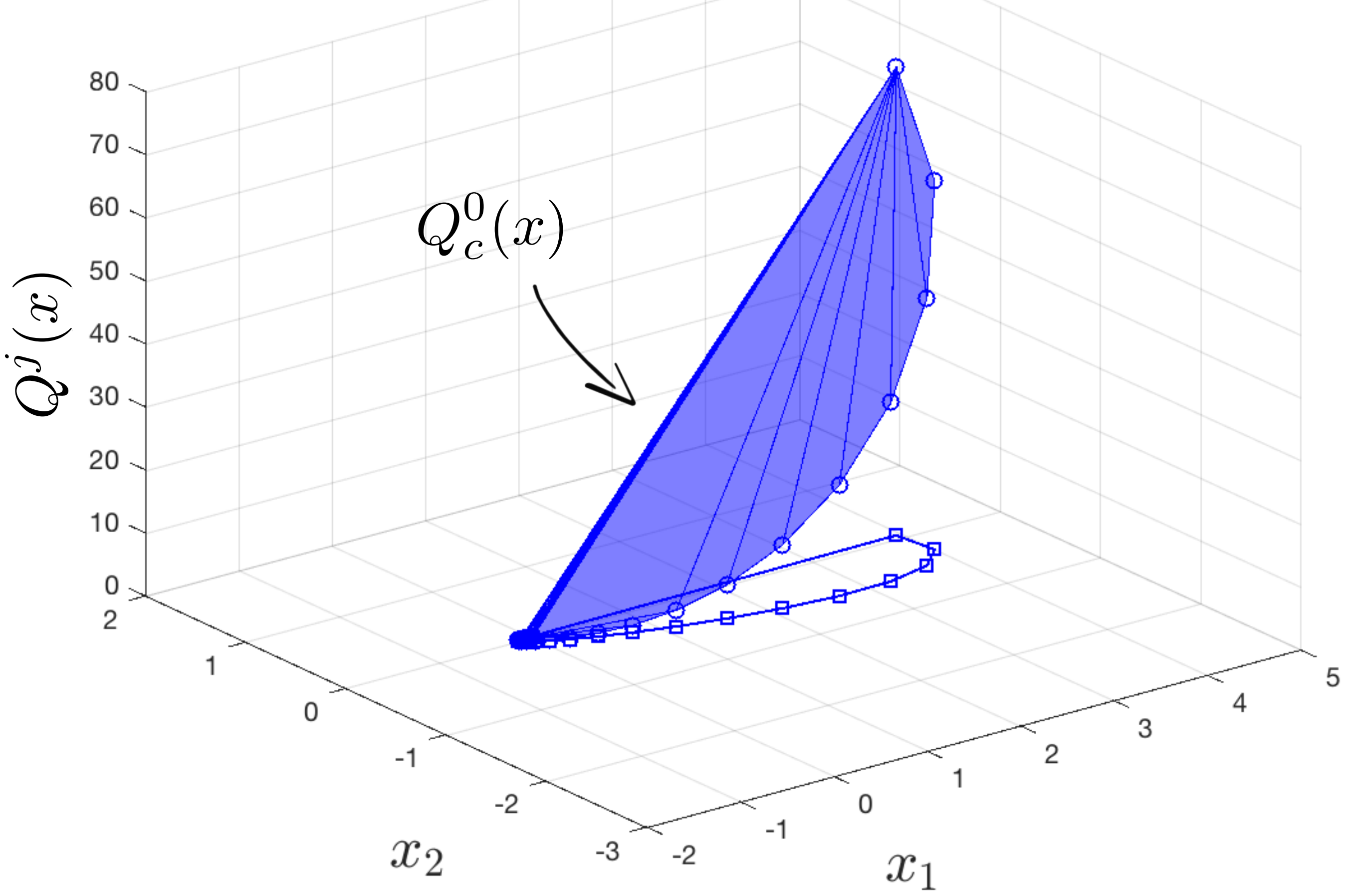
Step 0: Set iteration counter *j=0*

Step 1: Compute the roll-out cost for the recorded data up to iteration *j*

→ Step 2: Define Q^j which interpolates linearly the roll-out cost

Step 3: Run MPC in closed-loop at iteration *j+1*

Step 5: Set iteration counter *j = j+1.* Go to Step 1



Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC

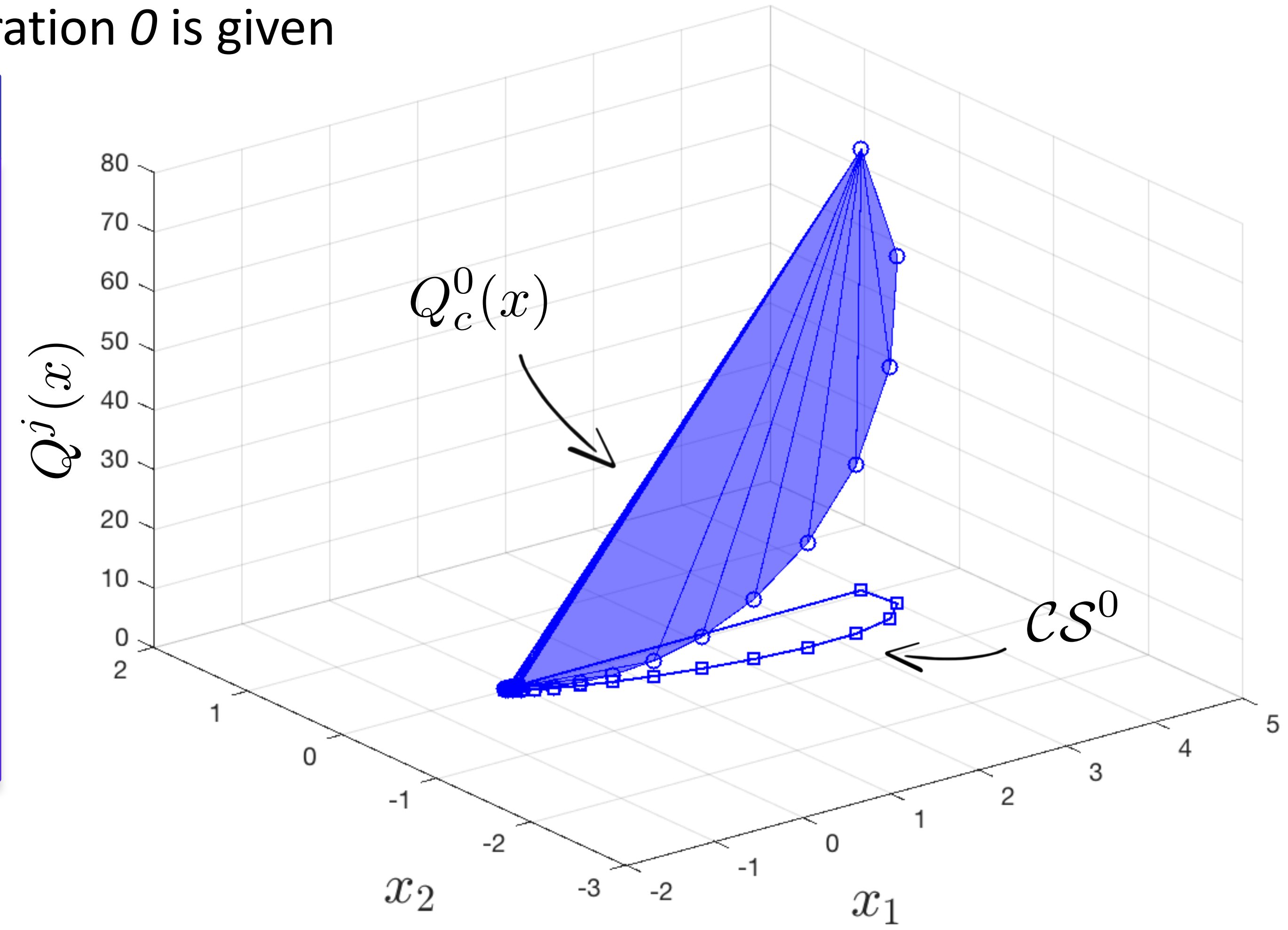
Step 0: Set iteration counter *j=0*

Step 1: Compute the roll-out cost for the recorded data up to iteration *j*

→ Step 2: Define Q^j which interpolates linearly the roll-out cost

Step 3: Run MPC in closed-loop at iteration *j+1*

Step 5: Set iteration counter *j = j+1.* Go to Step 1



Example I: Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC

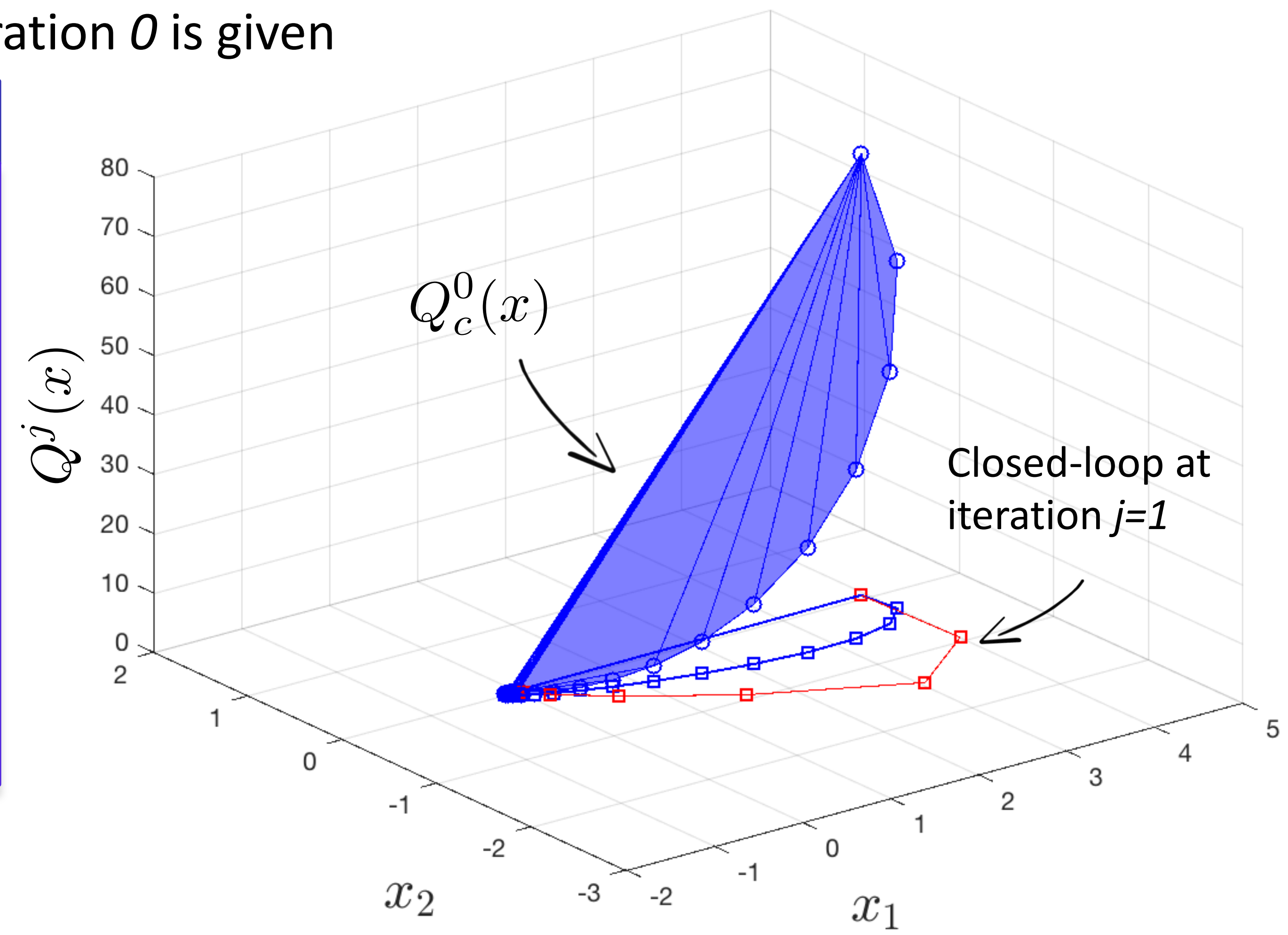
Step 0: Set iteration counter *j=0*

Step 1: Compute the roll-out cost for the recorded data up to iteration *j*

Step 2: Define Q^j which interpolates linearly the roll-out cost

→ Step 3: Run MPC in closed-loop at iteration *j+1*

Step 5: Set iteration counter *j = j+1.* Go to Step 1



Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC

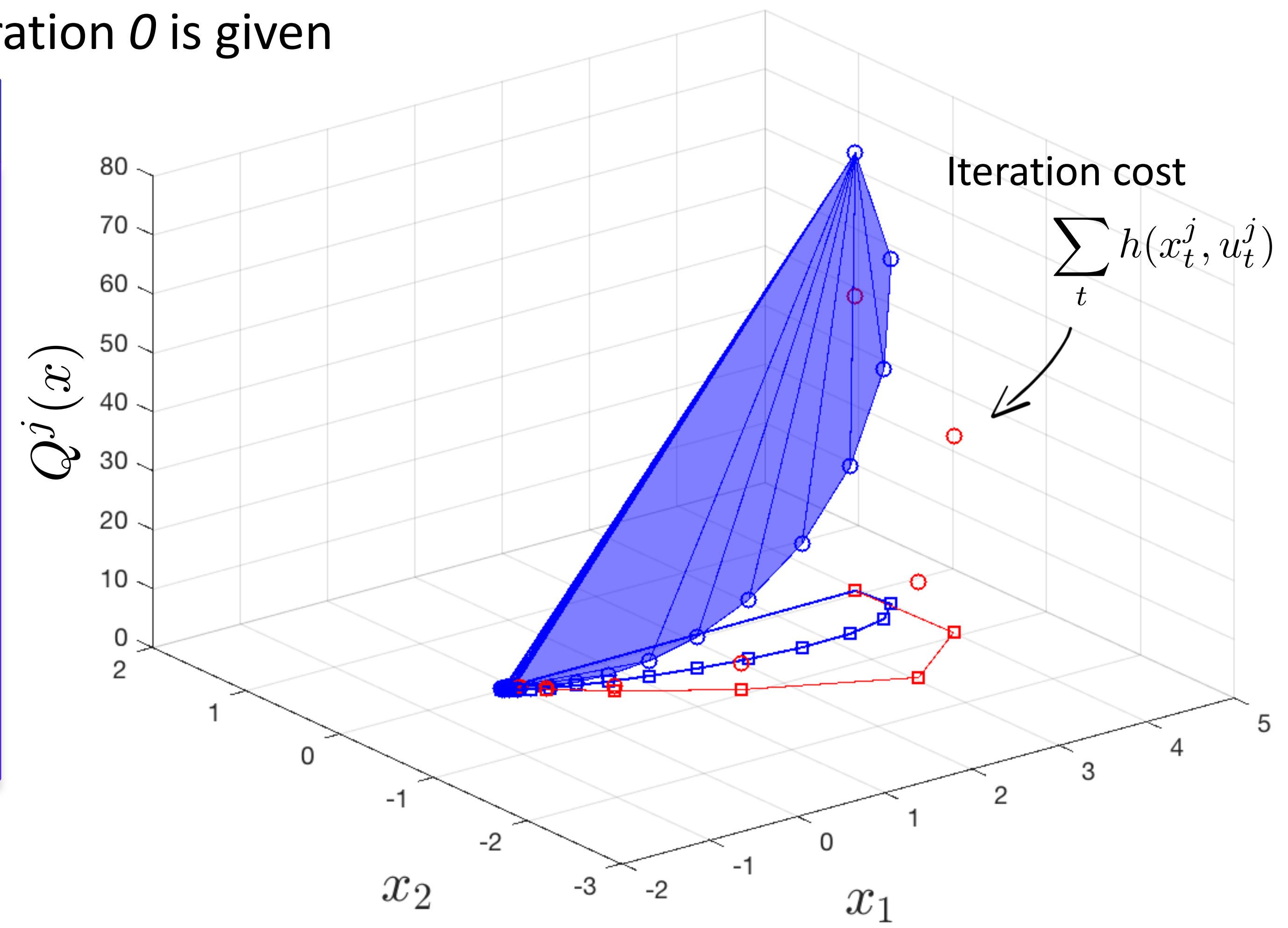
Step 0: Set iteration counter *j=0*

Step 1: Compute the roll-out cost for the recorded data up to iteration *j*

Step 2: Define Q^j which interpolates linearly the roll-out cost

Step 3: Run MPC in closed-loop at iteration *j+1*

Step 5: Set iteration counter *j = j+1.* Go to Step 1



Constrained LQR

Assumption: A first feasible trajectory at iteration *0* is given

Iterative LMPC

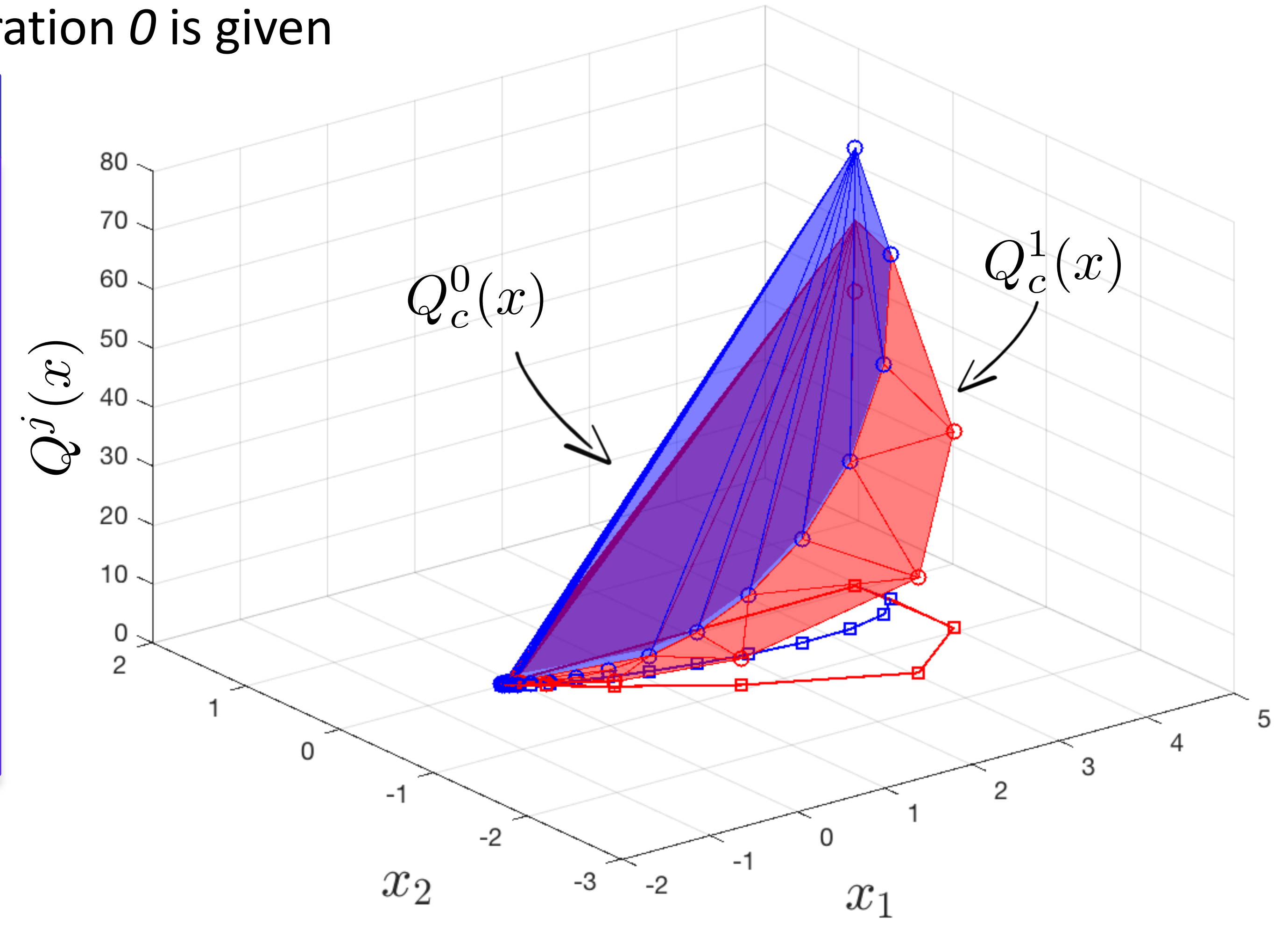
Step 0: Set iteration counter *j=0*

Step 1: Compute the roll-out cost for the recorded data up to iteration *j*

Step 2: Define Q^j which interpolates linearly the roll-out cost

Step 3: Run MPC in closed-loop at iteration *j+1*

Step 5: Set iteration counter *j = j+1.* Go to Step 1



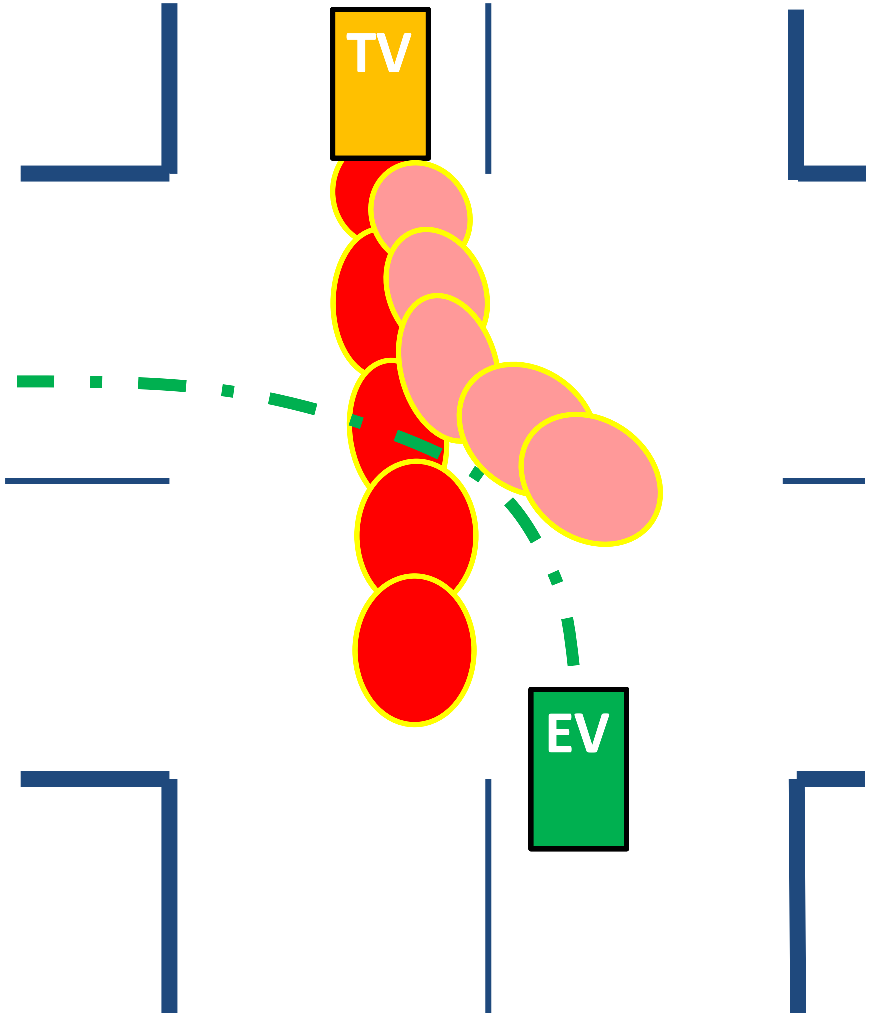
Outline

- A success on a simple example
- **A success on a more complex example**
- A complex problem without a systematic solution

Problem Formulation: Multi-modal Collision Avoidance using MPC

min Deviation of **EV** trajectory from Reference

s.t. Given **EV's** dynamical model and TV's
multi-modal predictions,
Satisfy speed, lane and actuation constraints,
Avoid collision with TV

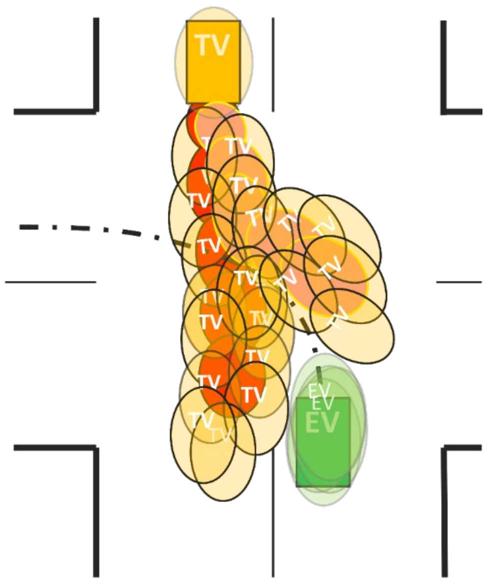


MPC = First optimal input

Stochastic MPC Formulations

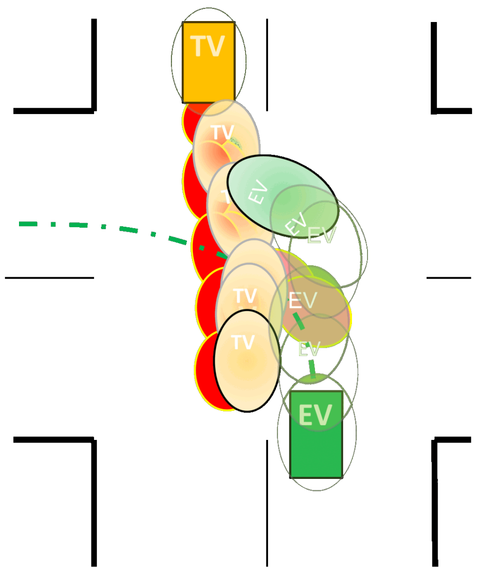
- Optimization over closed-loop sequences
- Smooth over-approximation of geometry

$$
\begin{aligned}
\min_{\boxed{u_{t|t},..,u_{t+N|t}}} \quad & \mathbb{E}\left[\sum_{k=t}^{t+N-1} l(x_{k|t}, u_{k|t}) + V(x_{t+N|t})\right] \\
\text{s.t.} \quad & x_{k+1|t} = f_k^{EV}(x_{k|t}, u_{k|t}), \\
& o_{k+1|t}|o_{k|t} \sim f_k^{TV}(o_{k|t}), \\
& \boxed{\mathbb{P}(g_k^{approx}(o_{k+1|t}, x_{k+1|t}) \leq 0) \leq \epsilon} \\
& (x_{k+1|t}, u_{k|t}) \in \mathcal{X} \times \mathcal{U} \\
& x_{t|t} = x_t, o_{t|t} = o_t, \\
& \forall k = t, .., t+N-1
\end{aligned}
$$



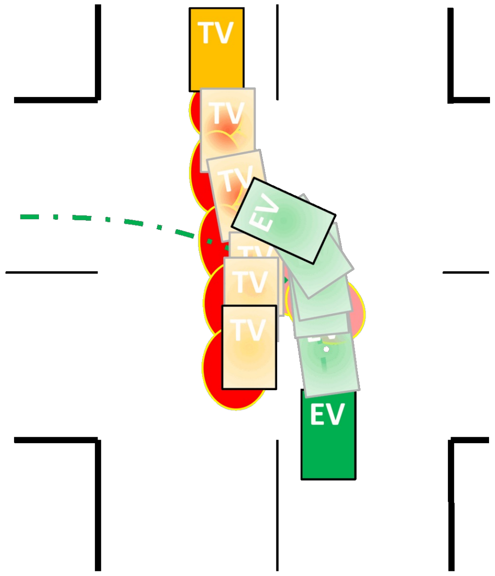
+ Optimization over closed-loop sequences
- Smooth over-approximation of geometry

$$
\begin{aligned}
\min_{\boxed{\pi_{\theta_{t|t}}(\cdot),..,\pi_{\theta_{t+N-1|t}}(\cdot)}} \quad & \mathbb{E}\left[\sum_{k=t}^{t+N-1} l(x_{k|t}, u_{k|t}) + V(x_{t+N|t})\right] \\
\text{s.t.} \quad & x_{k+1|t} = f_k^{EV}(x_{k|t}, u_{k|t}), \\
& o_{k+1|t}|o_{k|t} \sim f_k^{TV}(o_{k|t}), \\
& \boxed{\mathbb{P}(g_k^{approx}(o_{k+1|t}, x_{k+1|t}) \leq 0) \leq \epsilon} \\
& u_{k|t} = \pi_{\theta_{k|t}}(x_{k|t}, o_{k|t}), \\
& (x_{k+1|t}, u_{k|t}) \in \mathcal{X} \times \mathcal{U} \\
& x_{t|t} = x_t, o_{t|t} = o_t, \\
& \forall k = t, .., t+N-1
\end{aligned}
$$



+ Optimization over closed-loop sequences
+ Exact, Smooth Reformulation using Lagrange Duality

$$
\begin{aligned}
\min_{\boxed{\pi_{\theta_{t|t}}(\cdot),..,\pi_{\theta_{t+N-1|t}}(\cdot)}} \quad & \mathbb{E}\left[\sum_{k=t}^{t+N-1} l(x_{k|t}, u_{k|t}) + V(x_{t+N|t})\right] \\
\text{s.t.} \quad & x_{k+1|t} = f_k^{EV}(x_{k|t}, u_{k|t}), \\
& o_{k+1|t}|o_{k|t} \sim f_k^{TV}(o_{k|t}), \\
& \boxed{\mathbb{P}(g_k^{exact}(o_{k+1|t}, x_{k+1|t}) \leq 0) \leq \epsilon} \\
& u_{k|t} = \pi_{\theta_{k|t}}(x_{k|t}, o_{k|t}), \\
& (x_{k+1|t}, u_{k|t}) \in \mathcal{X} \times \mathcal{U} \\
& x_{t|t} = x_t, o_{t|t} = o_t, \\
& \forall k = t, .., t+N-1
\end{aligned}
$$



Stochastic MPC Formulations: Unprotected Left Demo in CARLA

− Optimization over open-loop sequences

− Smooth over-approximation of geometry

$$
\begin{aligned}
\min_{\boxed{u_{t|t},..,u_{t+N|t}}} \quad & \mathbb{E}\left[\sum_{k=t}^{t+N-1} l(x_{k|t},u_{k|t}) + V(x_{t+N|t})\right] \\
\text{s.t.} \quad & x_{k+1|t} = f_k^{EV}(x_{k|t},u_{k|t}), \\
& o_{k+1|t}|o_{k|t} \sim f_k^{TV}(o_{k|t}), \\
& \boxed{\mathbb{P}(g_k^{approx}(o_{k+1|t},x_{k+1|t}) \leq 0) \leq \epsilon} \\
& (x_{k+1|t},u_{k|t}) \in \mathcal{X}\times\mathcal{U} \\
& x_{t|t} = x_t, o_{t|t} = o_t, \\
& \forall k = t,..,t+N-1
\end{aligned}
$$

+ Optimization over open-loop sequences

− Smooth over-approximation of geometry

$$
\begin{aligned}
\min_{\boxed{\pi_{\theta_{t|t}}(\cdot),..,\pi_{\theta_{t+N-1|t}}(\cdot)}} \quad & \mathbb{E}\left[\sum_{k=t}^{t+N-1} l(x_{k|t},u_{k|t}) + V(x_{t+N|t})\right] \\
\text{s.t.} \quad & x_{k+1|t} = f_k^{EV}(x_{k|t},u_{k|t}), \\
& o_{k+1|t}|o_{k|t} \sim f_k^{TV}(o_{k|t}), \\
& \boxed{\mathbb{P}(g_k^{approx}(o_{k+1|t},x_{k+1|t}) \leq 0) \leq \epsilon} \\
& u_{k|t} = \pi_{\theta_{k|t}}(x_{k|t},o_{k|t}), \\
& (x_{k+1|t},u_{k|t}) \in \mathcal{X}\times\mathcal{U} \\
& x_{t|t} = x_t, o_{t|t} = o_t, \\
& \forall k = t,..,t+N-1
\end{aligned}
$$

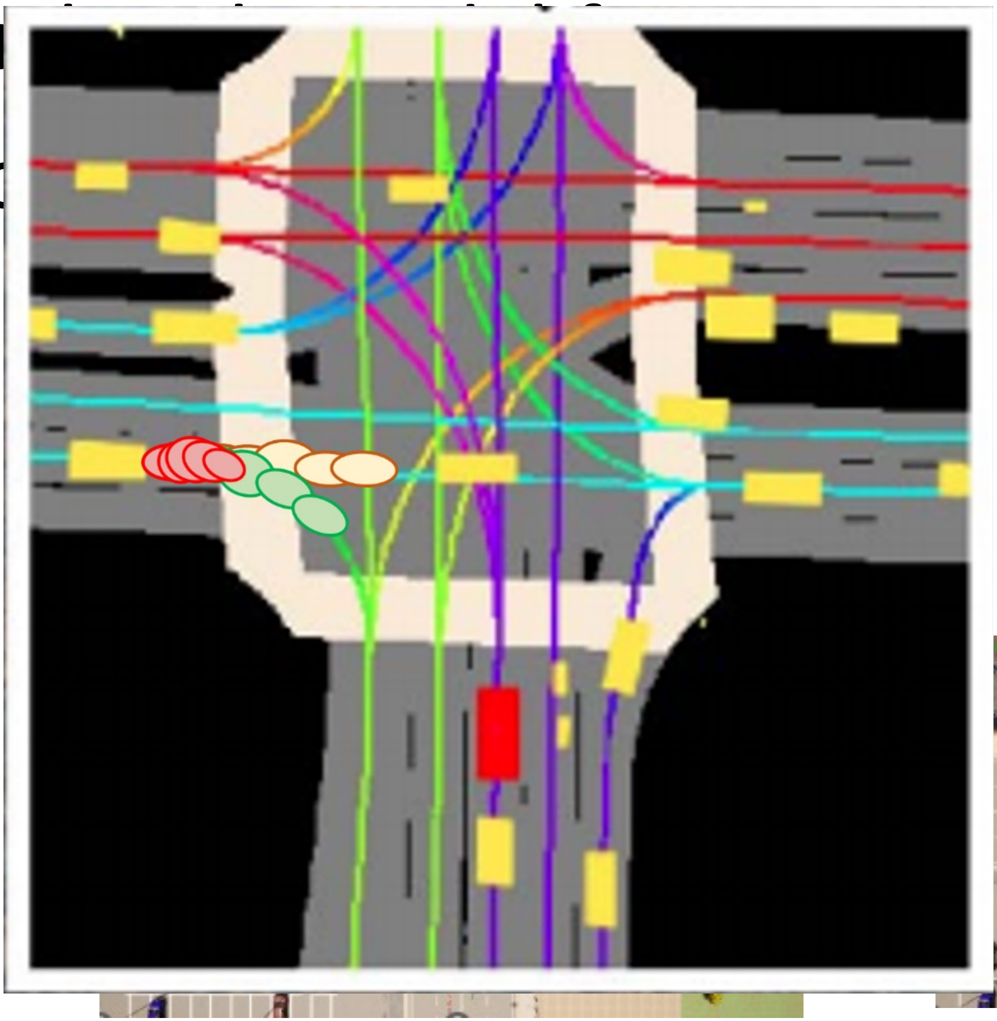
+ Optimization over open-loop sequences

+ Exact, Smooth Reformulation using Lagrange Duality

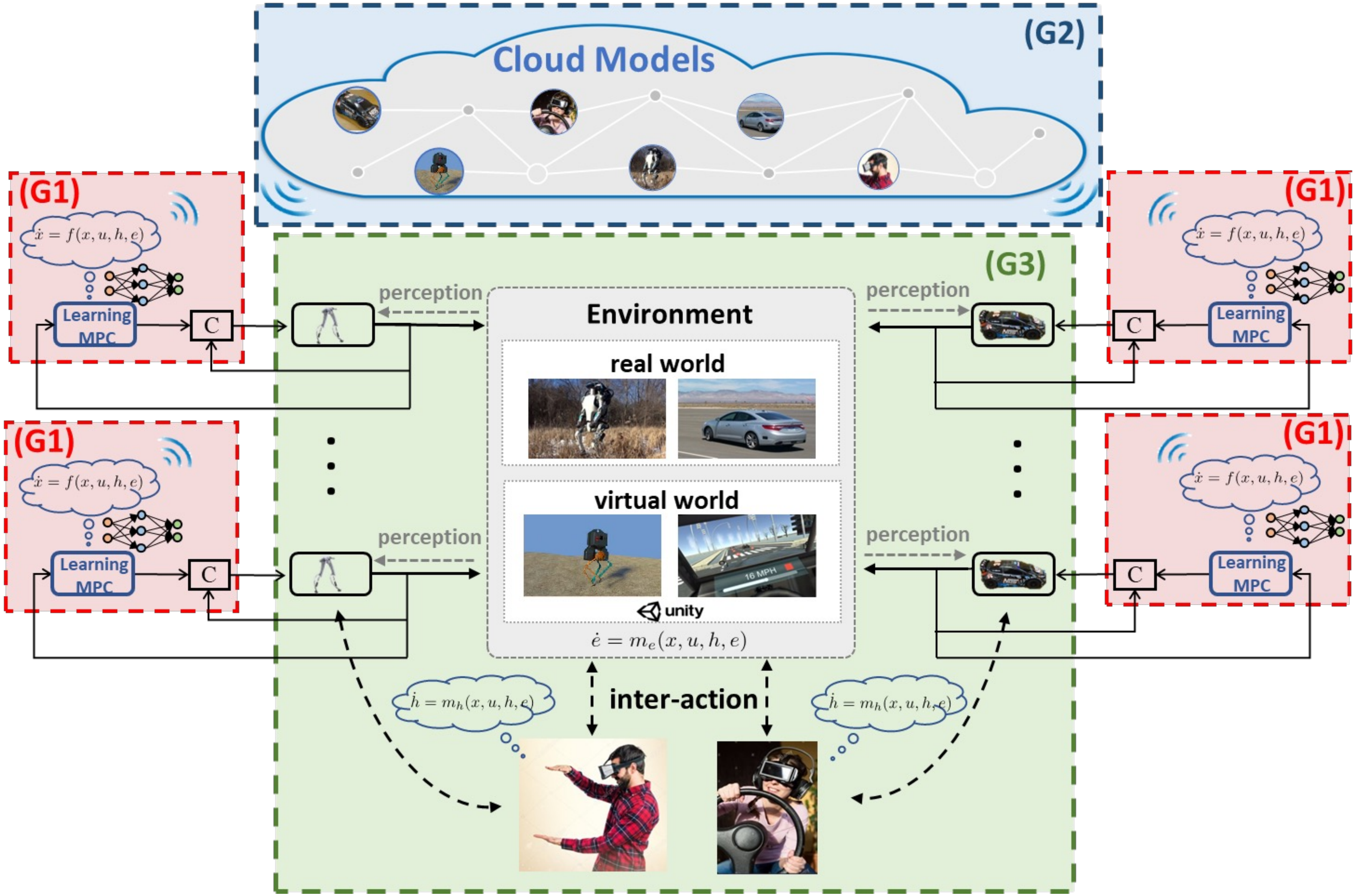
$$
\begin{aligned}
\min_{\boxed{\pi_{\theta_{t|t}}(\cdot),..,\pi_{\theta_{t+N-1|t}}(\cdot)}} \quad & \mathbb{E}\left[\sum_{k=t}^{t+N-1} l(x_{k|t},u_{k|t}) + V(x_{t+N|t})\right] \\
\text{s.t.} \quad & x_{k+1|t} = f_k^{EV}(x_{k|t},u_{k|t}), \\
& o_{k+1|t}|o_{k|t} \sim f_k^{TV}(o_{k|t}), \\
& \boxed{\mathbb{P}(g_k^{exact}(o_{k+1|t},x_{k+1|t}) \leq 0) \leq \epsilon} \\
& u_{k|t} = \pi_{\theta_{k|t}}(x_{k|t},o_{k|t}), \\
& (x_{k+1|t},u_{k|t}) \in \mathcal{X}\times\mathcal{U} \\
& x_{t|t} = x_t, o_{t|t} = o_t, \\
& \forall k = t,..,t+N-1
\end{aligned}
$$

The implementation cost of “disciplined” SMPC

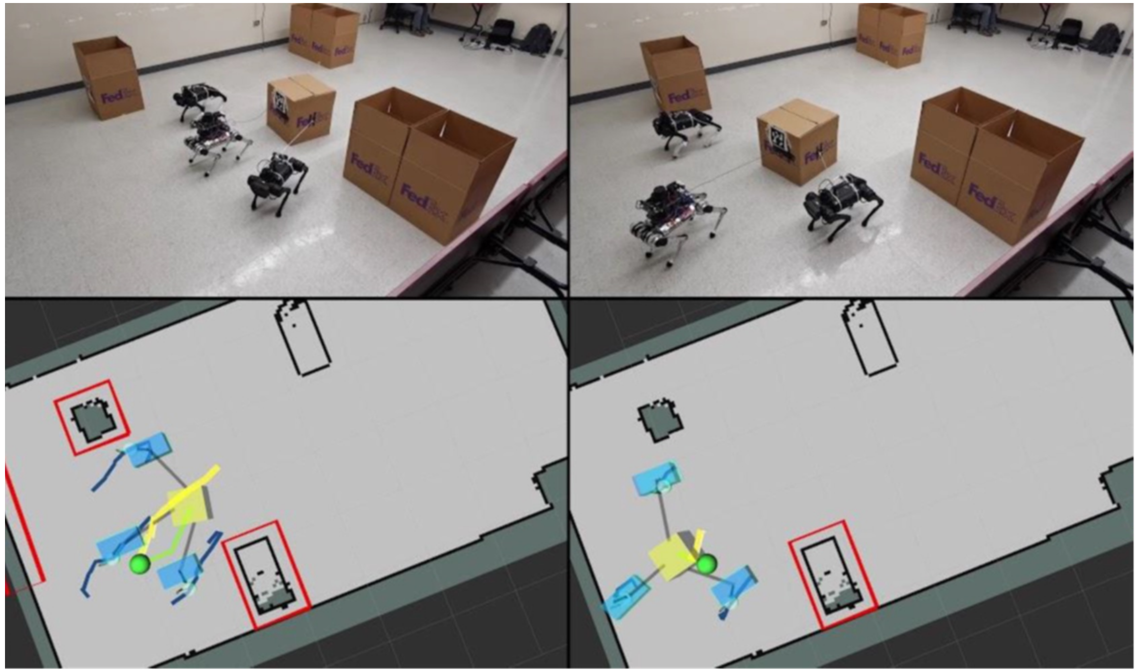
- Learning Contextu
- Learning interacti
- Optimization over
- Optimization over

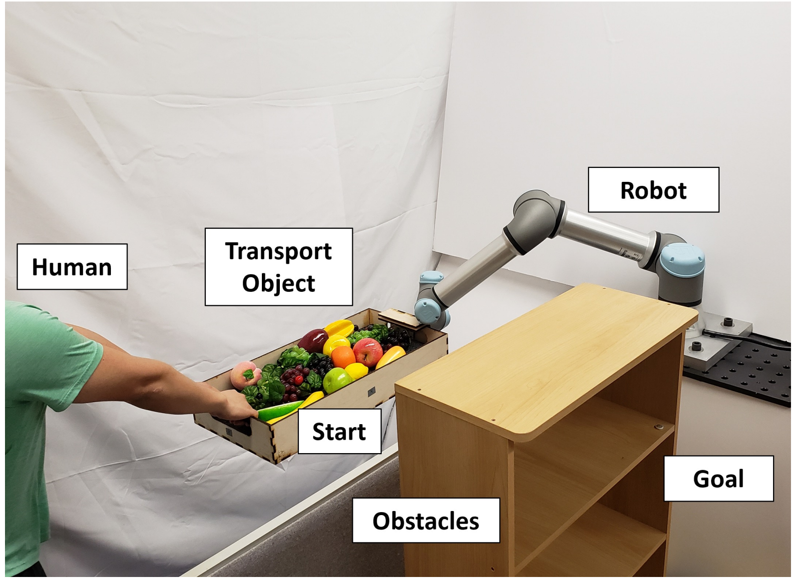


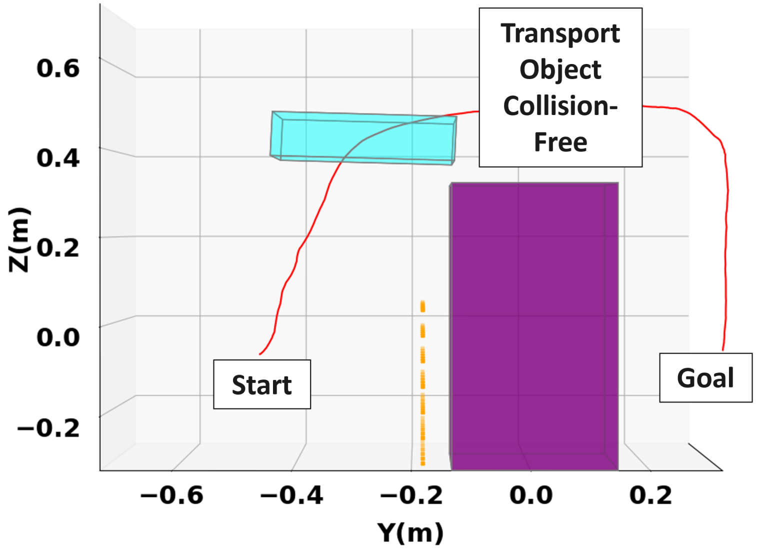
2019 CPS: Safe Learning for Co-Robots



Experimental Tests





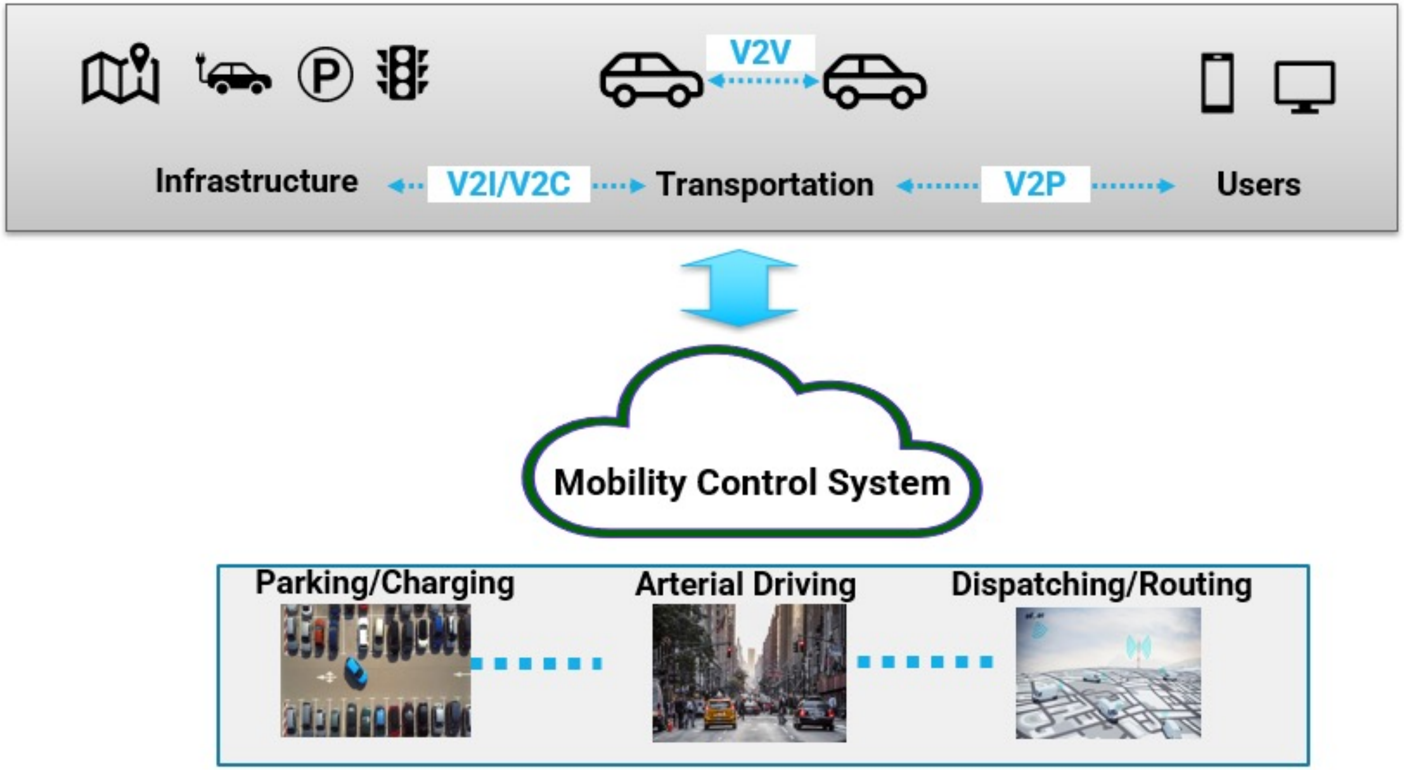


Still far from Safe co-Robots CPS!

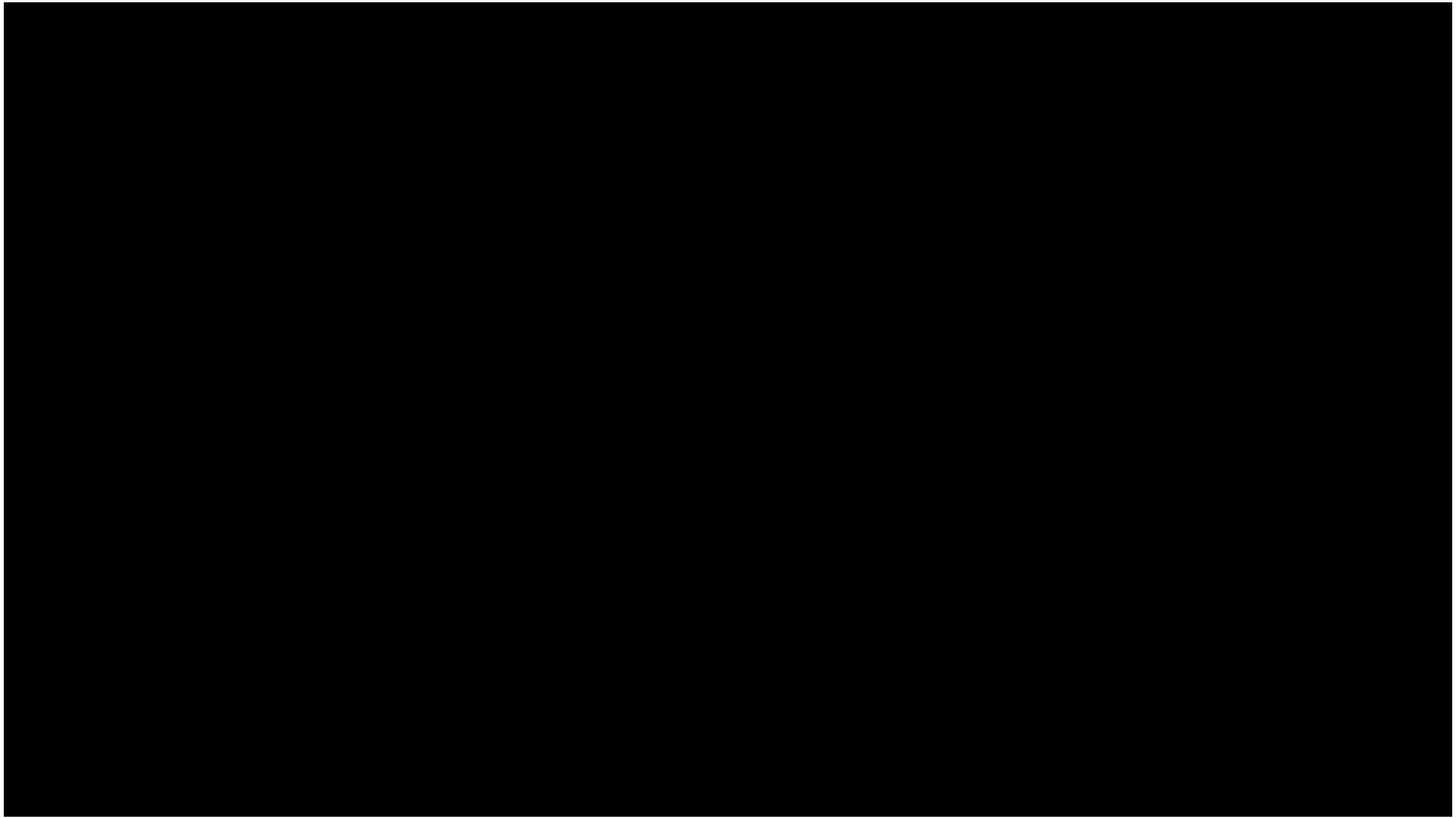
Connected and Automated Mobility

Population getting form A->B in safe, timely and energy efficient way

- Distributed learning control architecture
- Time varying and event triggered communication topology
- Cooperation with mixed of local and global objectives



Connected and Automated Mobility



Final Remarks

- Complex architectures
  - Make an effort to collaborate with people with system-level knowledge

- Impact time scale is longer than we expect/promise
  - Do not overpromise and do not give up

- While keeping system-level certification in mind
  - Focus on a subsystem and show tangible benefits with non conservative solution

- Young engineers often not knowledgeable on advanced tools for safe CPS
  - Bring relevant theory/ techniques faster to our graduate and undergraduate programs

Thanks!