Guarantees for Learning-Enabled Control

Sarah Dean, UC Berkeley

joint work with Nikolai Matni, Ben Recht, and Vickie Ye

Interplay between Control, Optimization, and Machine Learning Workshop at 2019 ACC
Machine learning has enabled...
Machine learning has enabled...
Machine learning has enabled...

[Images of flying robots and driving robots]
Machine learning has enabled...

- flying robots
- driving robots
- walking robots
Machine learning has enabled…

- Flying robots
- Driving robots
- Walking robots
- Grasping robots
Machine learning has enabled...

- Flying robots
- Driving robots
- Walking robots
- Grasping robots

Online advertising
Machine learning has enabled...
control of systems with complex dynamics and complex sensing modalities

flying robots

walking robots

driving robots

grasping robots

datacenter cooling

online advertising
...control of systems with complex dynamics and complex sensing modalities

aerodynamics

flying robots

walking robots

grasping robots

datacenter cooling

online advertising
...control of systems with complex dynamics and complex sensing modalities

- aerodynamics
- flying robots
- walking robots
- driving robots
- grasping robots
- contact forces

- online advertising

- datacenter cooling
…control of systems with complex dynamics and complex sensing modalities

aerodynamics

flying robots

driving robots

grazing robots

contact forces

walking robots

human behavior

online advertising

datacenter cooling

online advertising
...control of systems with complex dynamics and complex sensing modalities

- flying robots
- driving robots
- walking robots
- grasping robots
- contact forces
- aerodynamics
- cameras
- human behavior
- online advertising
- datacenter cooling
…control of systems with complex dynamics and complex sensing modalities

- aerodynamics
- cameras
- flying robots
- driving robots
- walking robots
- grasping robots
- contact forces
- cameras
- human behavior
- online advertising
- datacenter cooling
...control of systems with complex dynamics and complex sensing modalities

- aerodynamics
- cameras
- flying robots
- driving robots
- walking robots
- grasping robots
- contact forces
- cameras
- human behavior
- click-streams
- online advertising
- datacenter cooling
…control of systems with complex dynamics and complex sensing modalities

- aerodynamics
- cameras
- flying robots
- driving robots
- walking robots
- grasping robots
- contact forces
- cameras
- datacenter cooling
- human behavior
- click-streams
- online advertising
Example: high dimensional sensors in robotics
Example: high dimensional sensors in robotics

Traditional Approach:

- Physics-based state estimation with EKF or UKF
- Careful control design and tuning

Loianno et al. 2016
Example: high dimensional sensors in robotics

Traditional Approach:
- Physics-based state estimation with EKF or UKF
- Careful control design and tuning

End-to-end Approach:
- Deep networks map images to actions

Loianno et al. 2016
Giusti et al. 2015
Optimal Control Problem

\[
\min_{\gamma} \text{cost}(x, u)
\]

s.t. \( x_{k+1} = f(x_k, u_k, w_k) \),
\( z_k = g(x_k, v_k) \),
\( u_k = \gamma_k(z_{0:k}) \)
Optimal Control Problem

\[
\min_{\gamma} \text{cost}(x, u)
\]

s.t. \( x_{k+1} = f(x_k, u_k, w_k), \)
\( z_k = g(x_k, \nu_k), \)
\( u_k = \gamma_k(z_{0:k}) \)

Traditional Approach:
Focus on state estimation,
since high dimensional
sensors are hard
**Optimal Control Problem**

\[
\min_{\gamma} \text{cost}(x, u)
\]

s.t. \( x_{k+1} = f(x_k, u_k, w_k) \),

\( z_k = g(x_k, v_k) \),

\( u_k = \gamma(\hat{x}_k) \)

**Traditional Approach:**
Focus on state estimation,
since high dimensional sensors are hard
Optimal Control Problem

\[
\min_{\gamma} \text{cost}(x, u)
\]

s.t. \( x_{k+1} = f(x_k, u_k, w_k) \),
\( z_k = g(x_k, \nu_k) \),
\( u_k = \gamma_k(z_{0:k}) \)

**Traditional Approach:**
Focus on state estimation, since high dimensional sensors are hard
Optimal Control Problem

$$\min_{\gamma} \text{cost}(x, u)$$

s.t.

$$x_{k+1} = f(x_k, u_k, w_k),$$

$$z_k = g(x_k, \nu_k),$$

$$u_k = \gamma_k(z_{0:k})$$

Traditional Approach:
Focus on state estimation, since high dimensional sensors are hard

End-to-end Approach:
Focus on control map, since dynamics of observations are hard
Optimal Control Problem

\[
\min_{\gamma} \text{cost}(\mathbf{x}, \mathbf{u})
\]

s.t. \[x_{k+1} = f(x_k, u_k, w_k),\]

\[z_k = g(x_k, \nu_k),\]

\[u_k = \gamma_k(z_{0:k})\]

**Traditional Approach:**
Focus on state estimation, since high dimensional sensors are hard

**End-to-end Approach:**
Focus on control map, since dynamics of observations are hard
Optimal Control Problem

$$\min_{\gamma} \cos(x, u)$$

s.t. $x_{k+1} = f(x_k, u_k, w_k)$,
$z_k = g(x_k, v_k)$,
$u_k = \gamma_k(z_{0:k})$.

Traditional Approach:
Focus on state estimation, since high dimensional sensors are hard.

End-to-end Approach:
Focus on control map, since dynamics of observations are hard.
Optimal Control Problem

\[ \min_{\gamma} \text{cost}(x, u) \]

\[ s.t. \ x_{k+1} = f(x_k, u_k, w_k), \]
\[ z_k = g(x_k, v_k), \ y_k = p(z_k) \approx C x_k \]
\[ u_k = \gamma_k(y_{0:k}) \]

This Work:
Learn a simplifying perception map to sidestep interactions between dynamics and high dimensional observation
Problem Setting

- Linear dynamics

\[ x_{k+1} = Ax_k + Bu_k + H\omega_k \]
Problem Setting

- Linear dynamics \[ x_{k+1} = Ax_k + Bu_k + Hw_k \]
- Observation model \[ z_k = q(x_k) + \Delta_{q,k}(x_k) + v_k \]
Problem Setting

- Linear dynamics
  \[ x_{k+1} = Ax_k + Bu_k + Hw_k \]

- Observation model
  \[ z_k = q(x_k) + \Delta_{q,k}(x_k) + v_k \]

- Perception map as virtual sensor
  \[ y_k = p(z_k) = Cx_k + e_k \]
Problem Setting

- Linear dynamics
  \[ x_{k+1} = Ax_k + Bu_k + Hw_k \]

- Observation model
  \[ z_k = q(x_k) + \Delta_{q,k}(x_k) + v_k \]

- Perception map as virtual sensor
  \[ y_k = p(z_k) = Cx_k + e_k \]
Problem Setting: Output Feedback Control

- Perception as virtual sensor leads to familiar control setting
Problem Setting: Output Feedback Control

- Perception as virtual sensor leads to familiar control setting

\[
\min_{K} \text{cost}(x, u)
\]

s.t. \[x_{k+1} = Ax_k + Bu_k + Hw_k,\]

\[y_k = Cx_k + e_k,\]

\[u_k = K(y_{0:k})\]
Problem Setting: Output Feedback Control

- Perception as virtual sensor leads to familiar control setting

\[
\begin{align*}
\min_{K} & \quad \text{cost}(x, u) \\
\text{s.t.} \quad & x_{k+1} = Ax_k + Bu_k + Hw_k, \\
& y_k = Cx_k + e_k, \quad u_k = K(y_{0:k})
\end{align*}
\]

Well-studied solutions for various combinations of cost and error/noise models
Linear Output Feedback Control

- Different system desiderata and noise characterizations $\nu = (w, e)$

<table>
<thead>
<tr>
<th>Name</th>
<th>Disturbance class</th>
<th>Cost function</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>LQR/$\mathcal{H}_2$</td>
<td>$\mathbb{E}<em>\nu = 0$, $\mathbb{E}</em>\nu^4 &lt; \infty$, $\nu_k$ i.i.d.</td>
<td>$\mathbb{E}<em>\nu \left[ \lim</em>{T \to \infty} \sum_{k=0}^{T} \frac{1}{T} x_k^\top Q x_k + u_k^\top R u_k \right]$</td>
<td>Sensor noise, aggregate behavior, natural processes</td>
</tr>
<tr>
<td>$\mathcal{H}_\infty$</td>
<td>$|\nu|_{pow} \leq 1$</td>
<td>$\sup_{|\nu|<em>{pow} \leq 1} \lim</em>{T \to \infty} \frac{1}{T} \sum_{k=0}^{T} x_k^\top Q x_k + u_k^\top R u_k$</td>
<td>Modeling error, energy/power constraints</td>
</tr>
<tr>
<td>$\mathcal{L}_1$</td>
<td>$|\nu|_{\infty} \leq 1$</td>
<td>$\sup_{|\nu|_{\infty} \leq 1, k \geq 0} \frac{Q^{1/2} x_k}{R^{1/2} u_k}$</td>
<td>Real-time safety constraints, actuator saturation/limits</td>
</tr>
</tbody>
</table>
# Linear Output Feedback Control

- Different system desiderata and noise characterizations $\nu = (w, e)$

<table>
<thead>
<tr>
<th>Name</th>
<th>Disturbance class</th>
<th>Cost function</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{LQR/} \mathcal{H}_2$</td>
<td>$\mathbb{E}\nu = 0$, $\mathbb{E}\nu^4 &lt; \infty$, $\nu_k$ i.i.d.</td>
<td>$\mathbb{E}<em>\nu \left[ \lim</em>{T \to \infty} \sum_{k=0}^{T} \frac{1}{T} x_k^T Q x_k + u_k^T R u_k \right]$</td>
<td>Sensor noise, aggregate behavior, natural processes</td>
</tr>
<tr>
<td>$\mathcal{H}_\infty$</td>
<td>$|\nu|_{pow} \leq 1$</td>
<td>$\sup_{|\nu|<em>{pow} \leq 1} \lim</em>{T \to \infty} \frac{1}{T} \sum_{k=0}^{T} x_k^T Q x_k + u_k^T R u_k$</td>
<td>Modeling error, energy/power constraints</td>
</tr>
<tr>
<td>$\mathcal{L}_1$</td>
<td>$|\nu|_{\infty} \leq 1$</td>
<td>$\sup_{|\nu|_{\infty} \leq 1, k \geq 0} \frac{Q^{1/2} x_k}{R^{1/2} u_k}$</td>
<td>Real-time safety constraints, actuator saturation/limits</td>
</tr>
</tbody>
</table>

- Strong distributional assumptions or potentially adversarial and norm bounded
Perception Errors as Sensing Matrix Uncertainty

\[ e_k = p(q(x_k) + \Delta_{q,k}(x_k) + v_k) - Cx_k \]
Perception Errors as Sensing Matrix Uncertainty

\[ e_k = p(q(x_k) + \Delta_{q,k}(x_k) + v_k) - Cx_k \]
\[ = \Delta_{C,k}x_k + \eta_k \]
Perception Errors as Sensing Matrix Uncertainty

\[ e_k = p(q(x_k) + \Delta_{q,k}(x_k) + v_k) - Cx_k \]
\[ = \Delta_{C,k}x_k + \eta_k \]

Nonlinear observation process

Time-varying and state-dependent error process
Perception Errors as Sensing
Matrix Uncertainty

$$e_k = p(q(x_k) + \Delta_{q,k}(x_k) + v_k) - Cx_k$$
$$= \Delta_{C,k}x_k + \eta_k$$

Nonlinear observation process

Time-varying and state-dependent error process

$$y_k = (C + \Delta_{C,k})x_k + \eta_k$$
Robust Control via System Level Synthesis

- Correspondence between feedback controller and system response

Wang et al. 2016
Robust Control via System Level Synthesis

- Correspondence between feedback controller and system response

\[ \Phi \in \text{affine}(A, B, C) \]

\[ K = \Phi_{ue} - \Phi_{uw} \Phi_{xw}^{-1} \Phi_x \]

achieves response \( \Phi \) in closed-loop

Wang et al. 2016
Robust Control via System Level Synthesis

- Correspondence between feedback controller and system response

\[
\Phi \in \text{affine}(A, B, C)
\]

\[
K = \Phi_{ue} - \Phi_{uw} \Phi_{xw}^{-1} \Phi_{xe}
\]

achieves response \( \Phi \) in closed-loop

Wang et al. 2016
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior

\[ \hat{\Phi} \in \text{affine}(A, B, C) \]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior

\[ \hat{\Phi} \in \text{affine}(A, B, C) \]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior

\[ \Phi \in \text{affine}(A, B, C) \]

\[ K = \Phi_{ue} - \Phi_{uw} \Phi_{xw}^{-1} \Phi_{xe} \]

in closed-loop with \((A, B, C + \Delta C)\)

achieves response

\[ \Phi = (I - \Delta)\hat{\Phi} \]

as long as \( \|\Phi_{xe}\| \leq \frac{1}{\varepsilon C} \)

Boczar et al. 2018
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior

\[ \hat{\Phi} \in \text{affine}(A, B, C) \]

\[ K = \hat{\Phi}_{ue} - \hat{\Phi}_{uw} \hat{\Phi}_{xw}^{-1} \hat{\Phi}_{xe} \]

in closed-loop with \((A, B, C + \Delta C)\) achieves response

\[ \Phi = (I - \Delta)\hat{\Phi} \]

as long as \( \|\hat{\Phi}_{xe}\| \leq \frac{1}{\varepsilon C} \)

Boczar et al. 2018
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior

\[ \Phi = (I - \Delta)\hat{\Phi} \]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior \[ \Phi = (I - \Delta) \hat{\Phi} \]

- Trajectories depend on process noise, designed system response, and perception errors
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior
  \[ \Phi = (I - \Delta)\hat{\Phi} \]

- Trajectories depend on process noise, designed system response, and perception errors

\[
\begin{bmatrix}
    x \\
    u
\end{bmatrix} = (I - \Delta)\hat{\Phi}
\begin{bmatrix}
    w \\
    \eta
\end{bmatrix}
\]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior
  \[ \Phi = (I - \Delta) \hat{\Phi} \]

- Trajectories depend on process noise, designed system response, and perception errors
  \[
  \begin{bmatrix}
  x \\ u
  \end{bmatrix} = (I - \Delta) \hat{\Phi} 
  \begin{bmatrix}
  w \\ \eta
  \end{bmatrix}
  \]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior

\[ \Phi = (I - \Delta)\hat{\Phi} \]

- Trajectories depend on process noise, designed system response, and perception errors

\[
\begin{bmatrix}
    x \\
    u
\end{bmatrix} = (I - \Delta)\hat{\Phi} 
\begin{bmatrix}
    w \\
    \eta
\end{bmatrix}
\]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior
  \[ \Phi = (I - \Delta)\hat{\Phi} \]

- Trajectories depend on process noise, designed system response, and perception errors

\[
\begin{bmatrix}
  x \\
  u
end{bmatrix} = (I - \Delta)\Phi
\begin{bmatrix}
  w \\
  \eta
end{bmatrix}
\]
Robust SLS

- Transparent map between sensing uncertainties and closed-loop behavior
  \[ \Phi = (I - \Delta)\hat{\Phi} \]

- Trajectories depend on process noise, designed system response, and perception errors

\[
\begin{bmatrix}
    x \\
    u
\end{bmatrix} = (I - \Delta)\Phi
\begin{bmatrix}
    w \\
    \eta
\end{bmatrix}
\]

\[ y_k = (C + \Delta C,k) x_k + \eta_k \]
Learning Perception Map and Errors

- Error characterization via *error profile*
Learning Perception Map and Errors

- Error characterization via error profile

\[ e = p(z) - Cx = \Delta_C x + \eta \]

\[ \|\Delta_C\| \leq \varepsilon_C, \quad \|\eta\| \leq \varepsilon_\eta \]
Learning Perception Map and Errors

- Error characterization via error profile

\[ e = p(z) - Cx = \Delta_C x + \eta \]

\[ \|\Delta_C\| \leq \varepsilon_C, \quad \|\eta\| \leq \varepsilon_\eta \]

\[ \|p(z) - Cx\| \leq \varepsilon_C \|x\| + \varepsilon_\eta \]
Learning Perception Map and Errors

- Error characterization via error profile

\[
e = p(z) - Cx = \Delta_C x + \eta \leq \varepsilon_C \|x\| + \varepsilon_\eta
\]

- Slope and intercept in (state norm, error norm) space
Robust Optimization for Learning Perception

- Robust optimization problem
Robust Optimization for Learning Perception

- Robust optimization problem

\[
\min_{\varepsilon_C, \varepsilon_\eta} M\varepsilon_C + \varepsilon_\eta \\
\text{s.t. } \|p(z_k) - Cx_k\| \leq \varepsilon_C \|x_k\| + \varepsilon_\eta
\]
Robust Optimization for Learning Perception

- Robust optimization problem

\[
\min_{\varepsilon_C, \varepsilon_\eta} M\varepsilon_C + \varepsilon_\eta \\
\text{s.t. } \|p(z_k) - Cx_k\| \leq \varepsilon_C\|x_k\| + \varepsilon_\eta
\]

\[
M = \frac{1}{T} \sum_{k=1}^{T} \|x_k\|
\]
Robust Optimization for Learning Perception

- Robust optimization problem

$$\begin{align*}
\min_{p, \varepsilon_C, \varepsilon_\eta} & \quad M \varepsilon_C + \varepsilon_\eta + \lambda R(p) \\
\text{s.t.} & \quad \| p(z_k) - C x_k \| \leq \varepsilon_C \| x_k \| + \varepsilon_\eta \\
M & = \frac{1}{T} \sum_{k=1}^{T} \| x_k \| 
\end{align*}$$
Robust Optimization for Learning Perception

- Robust optimization problem

\[
\min_{p, \epsilon_C, \epsilon}\ M \epsilon_C + \epsilon + \lambda R(p)
\]

\[
\text{s.t. } \|p(z_k) - Cx_k\| \leq \epsilon_C \|x_k\| + \epsilon
\]

\[
M = \frac{1}{T} \sum_{k=1}^{T} \|x_k\|
\]

- Train vs. test

```
\begin{tabular}{c|c|c}
\hline
\lambda & train & test \\
\hline
0.022 & \includegraphics[width=0.4\textwidth]{train_test_0.022.png} & \includegraphics[width=0.4\textwidth]{train_test_0.022.png} \\
0.072 & \includegraphics[width=0.4\textwidth]{train_test_0.072.png} & \includegraphics[width=0.4\textwidth]{train_test_0.072.png} \\
\hline
\end{tabular}
```
Generalization

- Classic generalization results rely on statistical arguments about closeness of training and testing data
- Usually assume same distribution
Generalization

- Classic generalization results rely on statistical arguments about closeness of training and testing data
- Usually assume same distribution
Generalization

- Classic generalization results rely on statistical arguments about closeness of training and testing data
  - Usually assume same distribution

- The closed-loop distribution of states depends on the perception errors
Generalization

- Classic generalization results rely on statistical arguments about closeness of training and testing data
  - Usually assume same distribution

- The closed-loop distribution of states depends on the perception errors
Generalization

- Classic generalization results rely on statistical arguments about closeness of training and testing data
  - Usually assume same distribution
- The closed-loop distribution of states depends on the perception errors
Generalization

- Classic generalization results rely on statistical arguments about closeness of training and testing data
  - Usually assume same distribution

- The closed-loop distribution of states depends on the perception errors

- Idea: leverage control authority to ensure closeness
Closeness Implies Generalization

**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

\[
\| p(z) - Cx \| \leq \varepsilon_C \| x \| + \varepsilon_\eta + (L_\Delta + \varepsilon_C) \| x - x_d \| + 2L_p \varepsilon_v.
\]
Closeness Implies Generalization

**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

\[ \| p(z) - Cx \| \leq \varepsilon_C \| x \| + \varepsilon_\eta + (L_\Delta + \varepsilon_C) \| x - x_d \| + 2L_p \varepsilon_v. \]
Closeness Implies Generalization

**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

\[ \| p(z) - Cx \| \leq \varepsilon_C \| x \| + \varepsilon_\eta + (L_\Delta + \varepsilon_C) \| x - x_d \| + 2L_p \varepsilon_v. \]

high dimensional sensor noise
Closeness Implies Generalization

**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

\[ \| p(z) - Cx \| \leq \varepsilon_C \| x \| + \varepsilon_\eta + (L_\Delta + \varepsilon_C) \| x - x_d \| + 2L_p\varepsilon_v. \]
Closeness Implies Generalization

**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

\[
\| p(z) - Cx \| \leq \varepsilon_C \| x \| + \varepsilon_\eta + (L_\Delta + \varepsilon_C) \| x - x_d \| + 2L_p \varepsilon_v.
\]
Closeness Implies Generalization

**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

$$\|p(z) - Cx\| \leq \varepsilon_C \|x\| + \varepsilon_\eta + \left( L_\Delta + \varepsilon_C \right) \|x - x_d\| + 2L_p \varepsilon_v. $$

Generalization error:

$$\|\delta\| = \|p(z) - Cx - \Delta_C x - \eta\| \leq \text{[value]}$$
**Lemma:** Under generative model and smoothness assumptions, perception errors are bounded everywhere by

\[ \| p(z) - Cx \| \leq \varepsilon_C \| x \| + \varepsilon_\eta + (L_\Delta + \varepsilon_C) \| x - x_d \| + 2L_p \varepsilon_v. \]

Generalization error:

\[ \| \delta \| = \| p(z) - Cx - \Delta_C x - \eta \| \leq \varepsilon_v \]

determines closed-loop:

\[
\begin{bmatrix}
x \\
u
\end{bmatrix} = (I - \Delta) \hat{\Phi} \begin{bmatrix}
w \\
\eta + \delta
\end{bmatrix}
\]
Generalization Implies Closeness

**Lemma:** For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}$ the closed-loop trajectory with $u = \hat{K}_p(z)$ satisfies
Generalization Implies Closeness

**Lemma:** For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}$ the closed-loop trajectory with $u = \hat{K}_p(z)$ satisfies

$$\|x - x_d\| \leq$$
Generalization Implies Closeness

**Lemma:** For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}$ the closed-loop trajectory with $u = \hat{K}_p(z)$ satisfies

$$\|x - x_d\| \leq \frac{\|\hat{x} - x_d\| + \varepsilon_C \|\hat{\Phi}_{xe}\| \|x_d\| + \|\hat{\Phi}_{xe}\| \|\delta\|}{1 - \varepsilon_C \|\hat{\Phi}_{xe}\|}$$
Generalization Implies Closeness

Lemma: For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = [\hat{\Phi}_{xw} \quad \hat{\Phi}_{xe}] [w \quad \eta]$ the closed-loop trajectory with $u = \hat{K}p(z)$ satisfies

$$\|x - x_d\| \leq \frac{\|\hat{x} - x_d\| + \varepsilon_C \|\hat{\Phi}_{xe}\| \|x_d\| + \|\hat{\Phi}_{xe}\| \|\delta\|}{1 - \varepsilon_C \|\hat{\Phi}_{xe}\|}$$

nominal closeness
Lemma: For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}$ the closed-loop trajectory with $u = \hat{K}_p(z)$ satisfies

$$
\|x - x_d\| \leq \frac{||\hat{x} - x_d||}{1 - \varepsilon_C \|\hat{\Phi}_{xe}\|} + \varepsilon_C \|\hat{\Phi}_{xe}\| \|x_d\| + \|\hat{\Phi}_{xe}\| \|\delta\|.
$$

nominal closeness
Lemma: For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \left[ \hat{\Phi}_x \omega \quad \hat{\Phi}_x e \right] \left[ \begin{array}{c} w \\ \eta \end{array} \right]$ the closed-loop trajectory with $u = \hat{K}_p(z)$ satisfies

$$\|x - x_d\| \leq \left\| \hat{x} - x_d \right\| + \varepsilon C \left\| \hat{\Phi}_x e \right\| \|x_d\| + \left\| \hat{\Phi}_x e \right\| \|\delta\| \frac{1 - \varepsilon C \left\| \hat{\Phi}_x e \right\|}{1 - \varepsilon C \left\| \hat{\Phi}_x e \right\|}$$

nominal closeness
Generalization Implies Closeness

**Lemma:** For designed system response \( \hat{\Phi} \) and nominal trajectory, \( \hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix} \) the closed-loop trajectory with \( u = \hat{K}_p(z) \) satisfies

\[
\|x - x_d\| \leq \|\hat{x} - x_d\| + \varepsilon_C \|\hat{\Phi}_{xe}\| \|x_d\| + \|\hat{\Phi}_{xe}\| \|\delta\| \frac{1 - \varepsilon_C \|\hat{\Phi}_{xe}\|}{1}
\]

- **nominal closeness**
- **perception errors**
Generalization Implies Closeness

**Lemma:** For designed system response \( \hat{\Phi} \) and nominal trajectory, \( \hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix} \) the closed-loop trajectory with \( u = \hat{K}_p(z) \) satisfies

\[
\| x - x_d \| \leq \left( \| \hat{x} - x_d \| + \varepsilon_C \| \hat{\Phi}_{xe} \| \| x_d \| \right) \frac{1 - \varepsilon_C \| \hat{\Phi}_{xe} \|}{1 - \varepsilon_C \| \hat{\Phi}_{xe} \|} + \| \hat{\Phi}_{xe} \| \| \delta \|
\]

- \( \| x - x_d \| \) nominal closeness
- \( \| \hat{x} - x_d \| \) perception errors
- \( \varepsilon_C \| \hat{\Phi}_{xe} \| \| x_d \| \) generalization error
Generalization Implies Closeness

**Lemma:** For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}$ the closed-loop trajectory with $u = \hat{K}p(z)$ satisfies

$$\|x - x_d\| \leq \left\|\hat{x} - x_d\right\| + \varepsilon_C \left\|\hat{\Phi}_{xe}\right\| \left\|x_d\right\| \frac{1}{1 - \varepsilon_C \left\|\hat{\Phi}_{xe}\right\|} + \left\|\hat{\Phi}_{xe}\right\| \left\|\delta\right\|$$

- **nominal closeness**
- **perception errors**
- **generalization error**
**Lemma:** For designed system response $\hat{\Phi}$ and nominal trajectory, $\hat{x} = \begin{bmatrix} \hat{\Phi}_{xw} & \hat{\Phi}_{xe} \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}$ the closed-loop trajectory with $u = \hat{K}p(z)$ satisfies

$$\|x - x_d\| \leq \|\hat{x} - x_d\| + \varepsilon_C \|\hat{\Phi}_{xe}\| \|x_d\| + \frac{\|\hat{\Phi}_{xe}\| \|\delta\|}{1 - \varepsilon_C \|\hat{\Phi}_{xe}\|}$$

- **nominal closeness**
- **perception errors**
- **generalization error**
Robust Generalization
Robust Generalization

**Theorem:** As long as previous assumptions hold and

\[ \|\hat{\Phi}_{xe}\| \leq \frac{1}{L_{\Delta} + 2\varepsilon_{C}} \]

we have that

- Trajectories remain close to training states

- Generalization errors are bounded and depend on smoothness \((L_{\Delta}, L_{p}\varepsilon_{v})\), errors \((\varepsilon_{C})\), designed sensitivity \((\|\hat{\Phi}_{xe}\|)\), and \(\|\hat{x} - x_{d}\|\)
Training Strategies

The training data affects the performance through \( \| \hat{x} - x_d \| \)

We bound this quantity in two settings:
Training Strategies

The training data affects the performance through $\|\hat{x} - x_d\|$

We bound this quantity in two settings:

**Dense Sampling**
Training Strategies

The training data affects the performance through \( ||\hat{x} - x_d|| \).

We bound this quantity in two settings:

- **Dense Sampling**
- **Imitation Learning**
Training Strategies

The training data affects the performance through $||\hat{x} - x_d||$

We bound this quantity in two settings:

- Dense Sampling
- Imitation Learning

Training data should resemble desired closed-loop behavior!
Simulation Experiments

CARLA vehicle simulation platform
Simulation Experiments

CARLA vehicle simulation platform
Simulation Experiments

CARLA vehicle simulation platform

Waypoint tracking objective with 2D double integrator dynamics
Simulation Experiments

CARLA vehicle simulation platform

Waypoint tracking objective with 2D double integrator dynamics

ORB-SLAM2 for position estimation
Simulation Experiments: Controller Synthesis

We formulate the waypoint tracking problem as an output-feedback control problem, and synthesize:

1. **Nominal control** disregarding measurement matrix errors

2. **Robust control** by constraining the norm $\|\hat{\Phi}_{xe}\|$
Video: Experimental Results
Video: Experimental Results
Experimental Results

Without robustness condition, close-loop system diverges
Experimental Results

Without robustness condition, close-loop system diverges
Experimental Results

Without robustness condition, close-loop system diverges

Due to increasing errors in perception
Experimental Results

Without robustness condition, close-loop system diverges

Due to increasing errors in perception
Synthetic Experimental Results

Similar results in simple synthetic example
Synthetic Experimental Results

Similar results in simple synthetic example
Key Points
Key Points

1. Perception map as virtual sensor
2. Affine error profile via robust optimization
3. Generalization via robust control
Discussion

- We leverage control to sidestep distribution shift
Discussion

- We leverage control to sidestep distribution shift

\[ x_d = \Phi_x^{(d)} \begin{bmatrix} w_d \\ e_d \end{bmatrix} \quad x = \Phi_x \begin{bmatrix} w \\ p(g(x)) - Cx \end{bmatrix} \]
Discussion

- We leverage control to sidestep distribution shift

\[
x_d = \Phi_x^{(d)} \begin{bmatrix} w_d \\ e_d \end{bmatrix}
\]

\[
x = \Phi_x \begin{bmatrix} w \\ p(g(x)) - Cx \end{bmatrix}
\]
Discussion

- We leverage control to sidestep distribution shift

\[
\begin{align*}
x_d &= \Phi^{(d)}_x \begin{bmatrix} w_d \\ e_d \end{bmatrix} \\
x &= \Phi_x \begin{bmatrix} w \\ p(g(x)) - Cx \end{bmatrix}
\end{align*}
\]
Discussion

- We leverage control to sidestep distribution shift

\[ x_d = \Phi_x^{(d)} \begin{bmatrix} w_d \\ e_d \end{bmatrix} \]

\[ x = \Phi_x \begin{bmatrix} w \\ p(g(x)) - Cx \end{bmatrix} \]

controllers

process noise

measurement noise
Discussion

- We leverage control to sidestep distribution shift

\[ x_d = \Phi_x^{(d)} \begin{bmatrix} w_d \\ e_d \end{bmatrix} \]

- Distribution shift is a problem in many practical applications of machine learning, especially due to feedback

\[ x = \Phi_x \begin{bmatrix} w \\ p(g(x)) - Cx \end{bmatrix} \]
Thank you!

S. Dean, N. Matni, B. Recht, and V. Ye, Robust Guarantees for Perception-Based Control. arXiv:1907.03680

Based on work supported by NSF Graduate Research Fellowship under Grant No. DGE 1752814