Robust Guarantees for Perception-Based Control

Sarah Dean   DEAN_SARAH@BERKELEY.EDU

Nikolai Matni   NMATNI@SEAS.UPENN.EDU

Benjamin Recht   BRECHT@BERKELEY.EDU

Vickie Ye   VYE@BERKELEY.EDU

Abstract

Motivated by vision-based control of autonomous vehicles, we consider the problem of controlling a known linear dynamical system for which partial state information, such as vehicle position, is extracted from complex and nonlinear data, such as a camera image. Our approach is to use a learned perception map that predicts some linear function of the state and to design a corresponding safe set and robust controller for the closed loop system with this sensing scheme. We show that under suitable smoothness assumptions on both the perception map and the generative model relating state to complex and nonlinear data, parameters of the safe set can be learned via appropriately dense sampling of the state space. We then prove that the resulting perception-control loop has favorable generalization properties. We illustrate the usefulness of our approach on a synthetic example and on the self-driving car simulation platform CARLA.

Keywords: Robust control, learning theory, generalization, perception, robotics.

1. Introduction

Incorporating insights from rich, perceptual sensing modalities such as cameras remains a major challenge in controlling complex autonomous systems. While such sensing systems clearly have the potential to convey more information than simple, single output sensor devices, interpreting and robustly acting upon the high-dimensional data streams remains difficult. Recent end-to-end approaches tackle the problem of image based control by learning an optimized map from pixel values directly to low level control inputs. Though there has been tremendous success in accomplishing sophisticated tasks, critical gaps in understanding robustness and safety still remain (Levine et al., 2016). On the other hand, methods rooted in classical state estimation and robust control explicitly characterize a model of the underlying system and its environment in order to design a feedback controller. These approaches have provided strong and rigorous guarantees of robustness and safety in domains such as aerospace and process control, but the level of specification of the underlying system required has thus far limited their impact for complex sensor inputs.

In this paper, we aim to leverage contemporary techniques from machine learning and robust control to understand the conditions under which safe and reliable behavior can be achieved in controlling a system with uncertain and high-dimensional sensors. Whereas much recent work has been devoted to proving safety and performance guarantees for learning-based controllers applied to systems with unknown dynamics (Wabersich and Zeilinger, 2018; Akametalu et al., 2014; Ostafew et al., 2014; Hewing and Zeilinger, 2017; Dean et al., 2017, 2018; Abbasi-Yadkori et al., 2019; Abbasi-Yadkori and Szepesvári, 2011; Cheng et al., 2019; Taylor et al., 2019; Williams et al., 2018; Agarwal et al., 2019; Berkenkamp et al., 2017), we focus on the practical scenario where the underlying dynamics of a system are well understood, and it is instead the integration of perceptual sensor data into the control loop that must be learned. Specifically, we consider controlling a known linear dynamical system for which partial state information can only be extracted from complex observations. Our approach is to design a *virtual sensor* by learning both a perception map (i.e., a map from observations to a linear function of the state) and a bound on its estimation errors. We show that under suitable

smoothness assumptions, we can guarantee bounded errors within a neighborhood of the training data. This model of uncertainty allows us to synthesize a robust controller that ensures that the system does not deviate too far from states visited during training. Finally, we show that the resulting perception and robust control loop is able to robustly generalize under adversarial noise models. To the best of our knowledge, this is the first such guarantee for a vision-based control system.

1.1. Related work

Vision based estimation, planning, and control There is a rich body of work, spanning several research communities, that integrate high-dimensional sensors, specifically cameras, into estimation, planning, and control loops. The robotics community has focused mainly on integrating camera measurements with inertial odometry via an Extended Kalman Filter (EKF) (Jones and Soatto, 2011; Kelly and Sukhatme, 2011; Hesch et al., 2014). Similar approaches have also been used as part of Simultaneous Localization and Mapping (SLAM) algorithms in both ground (Lynen et al., 2015) and aerial (Lynen et al., 2013) vehicles. We note that these works focus solely on the estimation component, and do not consider downstream use of state estimates in control loops. In contrast, the papers (Loianno et al., 2016; Tang et al., 2018; Lin et al., 2018) demonstrate techniques that use camera measurements to aid inertial position estimates to enable aggressive control maneuvers in unmanned aerial vehicles.

The machine learning community has taken a more data-driven approach. The earliest such example is likely (Pomerleau, 1989), in which a 3-layer neural-network is trained to infer road direction from images. Modern approaches to vision based planning, typically relying on deep neural networks, include learning maps from image to trail direction (Giusti et al., 2015), learning Q-functions for indoor navigation using 3D CAD images (Sadeghi and Levine, 2016), and using images to specify waypoints for indoor robotic navigation (Bansal et al., 2019). Moving from planning to low-level control, end-to-end learning for vision based control has been achieved through imitation learning from training data generated via human (Bojarski et al., 2016) and model predictive control (Pan et al., 2018). The resulting policies map raw image data directly to low-level control tasks. In Codevilla et al. (2018), higher level navigational commands, images, and other sensor measurements are mapped to control actions via imitation learning. Similarly, Williams et al. (2018) and related works, image and inertial data is mapped to a cost landscape, that is then optimized via a path integral based sampling algorithm. More closely related to our approach is Lambert et al. (2018), where a deep neural network is used to learn a map from image to system state – we note that this perception module is naturally incorporated into our proposed pipeline. To the best of our knowledge, none of the aforementioned results provide safety or performance guarantees.

Learning, robustness, and control Our theoretical contributions are similar in spirit to those of the online learning community, in that we provide generalization guarantees under adversarial noise models (Anava et al., 2013, 2015; Kuznetsov and Mohri, 2016; Hassibi and Kaliath, 2001; Yasini and Pelckmans, 2018). Similarly, Agarwal et al. (2019) shows that adaptive disturbance feedback control of a linear system under adversarial process noise achieves sublinear regret – we note that this approach assumes full state information. We also draw inspiration from recent work that seeks to bridge the gap between linear control and learning theory. These assume a linear time invariant system, and derive finite-time guarantees for system identification (Dean et al., 2017; Hardt et al., 2018; Simchowitz et al., 2018; Sarkar and Rakhlin, 2018; Oymak and Ozay, 2018; Sarkar et al., 2019; Tsiamis and Pappas, 2019; Fattahi and Sojoudi, 2018; Fattahi et al., 2019; Pereira et al., 2010), and/or integrate learned models into control schemes with finite-time performance guarantees (Dean et al., 2017; Abbasi-Yadkori and Szepesvári, 2011; Russo et al., 2018; Abeille and Lazaric, 2018;

Ouyang et al., 2017; Abbasi-Yadkori et al., 2019; Dean et al., 2018; Cohen et al., 2019; Mania et al., 2019; Rantzer, 2018).

1.2. Notation

We use letters such as x and A to denote vectors and matrices, and boldface letters such as $\boldsymbol{x}$ and $\boldsymbol{\Phi}$ to denote infinite horizon signals and linear convolution operators. Thus, for $\boldsymbol{y} = \boldsymbol{\Phi} \boldsymbol{x}$, we have by definition that $y_k = \sum_{t=0}^{k} \Phi_t x_{k-t}$. We write $x_{0:t} = \{x_0, x_1, \ldots, x_t\}$ for the history of signal $\boldsymbol{x}$ up to time t. For a function $x_k \mapsto f_k(x_k)$, we write $\boldsymbol{f}(\boldsymbol{x})$ to denote the signal $\{f_k(x_k)\}_{k=0}^{\infty}$.

We overload the norm $\|\cdot\|$ so that it applies equally to elements x_k, signals $\boldsymbol{x}$, and linear operators $\boldsymbol{\Phi}$. For any element norm, we define the signal norm as $\|\boldsymbol{x}\| = \sup_k \|x_k\|$ and the linear operator norm as $\|\boldsymbol{\Phi}\| = \sup_{\|\boldsymbol{w}\| \leq 1} \|\boldsymbol{\Phi} \boldsymbol{w}\|$. We primarily focus on the triple $(\|x_k\|_\infty, \|\boldsymbol{x}\|_\infty, \|\boldsymbol{\Phi}\|_{\mathcal{L}_1})$. Note that as $\|\boldsymbol{\Phi}\|$ is an induced norm, it satisfies the sub-multiplicative property $\|\boldsymbol{\Phi}\boldsymbol{\Psi}\| \leq \|\boldsymbol{\Phi}\|\|\boldsymbol{\Psi}\|$.

We define the ball $B_r(x_0) = \{x \; : \; \|x - x_0\| \leq r\}$. We say that a fuction f is locally S-slope bounded for a radius r around x_0 if for $x \in B_r(x_0)$, $\|f(x) - f(x_0)\| \leq S\|x - x_0\|$, or similarly locally L-Lipschitz if for $x, y \in B_r(x_0)$, $\|f(x) - f(y)\| \leq L\|x - y\|$.

2. Problem setting

Consider the LTI dynamical system

$$x_{k+1} = Ax_k + Bu_k + Hw_k, \tag{1}$$

$$z_k = q(x_k) \tag{2}$$

with system state $x \in \mathbb{R}^n$, control input $u \in \mathbb{R}^m$, disturbance $w \in \mathbb{R}^w$, and observation $z \in \mathbb{R}^M$. We take the dynamics matrices (A, B, H) to be known. The observation process is determined by the unknown *generative model* q, which is nonlinear and potentially quite high-dimensional. As an example, consider a camera affixed to the dashboard of a car tasked with driving along a road. Here, the observations $\{z_k\}$ are the captured images and the map q generates these images as a function of position and velocity.

Motivated by such vision based control systems, our goal is to solve the optimal control problem

$$\text{minimize}_{\{\gamma_k\}} \quad c(\boldsymbol{x}, \boldsymbol{u}) \text{ subject to dynamics (1) and measurement (2), } u_k = \gamma_k(z_{0:k}), \tag{3}$$

where $c(\boldsymbol{x}, \boldsymbol{u})$ is a suitably chosen cost function and γ_k is a measurable function of the image history $z_{0:k}$. This problem is made challenging by the nonlinear, high-dimensional, and unknown generative model.[1]

Suppose instead that there exists a *perception map* p that imperfectly predicts partial state information; that is $p(z_k) = Cx_k + e_k$ for $C \in \mathbb{R}^{\ell \times n}$ a known matrix, and error $e_k \in \mathbb{R}^{\ell}$. Using this map, we define a new measurement model in which the map p plays the role of a noisy sensor:

$$y_k = p(z_k) = Cx_k + e_k. \tag{4}$$

This allows us to reformulate problem (3) as a *linear* optimal control problem, where the measurements are defined by (4) and the control law $u_k = \boldsymbol{K}(y_{0:k})$ is a *linear* function of the outputs of past measurements $y_{0:k}$. As illustrated in Figure 1, guarantees of performance, safety, and robustness require designing a controller

---

1. We remark that a nondeterministic appearance map q may be of interest for modeling phenomena like noise and environmental uncertainty. While we focus our exposition on the deterministic case, we note that many of our results can be extended in a straightforward manner to any noise class for which the perception map has a bounded response. For example, many computer vision algorithms are robust to random Gaussian pixel noise, gamma corrections, or sparse scene occlusions.
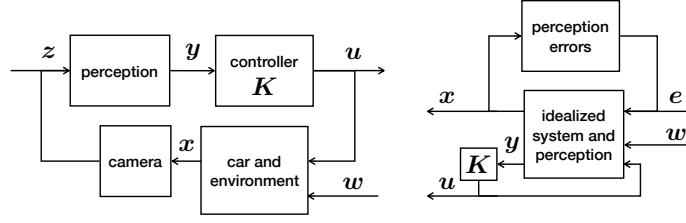
Figure 1: (Left) A diagram of the proposed perception-based control pipeline. (Right) The conceptual rearrangement of the closed-loop system permitted through our perception error characterization.

which suitably responds to system disturbance w and sensor noise e. For linear optimal control problems, a variety of cost functions and noise models have well-understood solutions; we expand on this observation further in Section 2.1.

In light of this discussion, we approach our problem with the following data-driven procedure: First, we use supervised learning to fit a perception map and explicitly characterize its errors in terms of the data it was trained on. Second, we compute a robust controller that mitigates the effects of the measurement error e. We will show that under suitable local smoothness assumptions on the generative model q and perception map p we can guarantee closed-loop robustness using a number of samples depending only on the state dimension.

2.1. Background on linear optimal control

We first recall some basic concepts from linear optimal control in the partially observed setting. In particular we consider the optimal control problem

$$
\begin{aligned}
\text{minimize}_{\boldsymbol{K}} \quad & c(\boldsymbol{x}, \boldsymbol{u}) \\
\text{subject to} \quad & x_{k+1} = Ax_k + Bu_k + Hw_k \\
& y_k = Cx_k + e_k \\
& u_k = \boldsymbol{K}(y_{0:k}),
\end{aligned}
\tag{5}
$$

for x_k the state, u_k the control input, w_k the process noise, e_k the sensor noise, $\boldsymbol{K}$ a linear-time-invariant operator, and $c(\boldsymbol{x}, \boldsymbol{u})$ a suitable cost function.

Control design depends on how the disturbance w and measurement error e are modeled, as well as performance objectives. By modeling the disturbance w and sensor noise e as being drawn from different signal spaces, and by choosing correspondingly suitable cost functions, we can incorporate practical performance, safety, and robustness considerations into the design process. For example, the well-studied LQG control problem minimizes the expected quadratic cost for user-specified positive definite matrices and normally distributed process and measurement noise. The resulting optimal estimation and control policy is to apply a static state feedback controller with the Kalman filter state estimate. The robust version of this problem considers instead the worst-case quadratic cost for ℓ_2 or power-norm bounded noise. This is the $\mathcal{H}_\infty$ optimal control problem, which has a rich history (Zhou et al., 1996).

As a final example, we recall the $\mathcal{L}_1$ optimal control problem, which seeks to minimize the $\ell_\infty \to \ell_\infty$ induced norm of a system. This formulation best accommodates real-time safety constraints and actuator saturation, which we motivate in the following example.

Example 1 (Waypoint Tracking) *Suppose that the control objective is to keep the system within a bounded distance of a sequence of waypoints at every timestep, and that the distance between sequential waypoints is*

4

bounded. Denoting the system state as $\boldsymbol{\xi}$ and the waypoint sequence as $\boldsymbol{r}$, the cost function is

$$c(\boldsymbol{\xi}, \boldsymbol{u}) = \sup_{\substack{\|r_{k+1}-r_k\|_\infty \leq 1, \\ \|e_k\|_\infty \leq 1, k \geq 0}} \left\| \begin{array}{c} Q^{1/2}(\xi_k - r_k) \\ R^{1/2}u_k \end{array} \right\|_\infty .$$

If we specify costs by $Q = \mathrm{diag}(1/q_i^2)$ and $R = \mathrm{diag}(1/r_i^2)$, then as long as the optimal cost is less than 1, we can guarantee that bounded trackking error $|\xi_{i,k} - r_{i,k}| \leq q_i$ and actuation $|u_{i,k}| \leq r_i$ for all possible realizations of the waypoint and sensor error processes. By defining an augmented state, e.g. $x_k = [\xi_k - r_k; r_k]$, and formulating waypoints as bounded disturbances, e.g. $w_k = r_{k+1} - r_k$, we can reformulate this cost into a standard $\mathcal{L}_1$ optimal control problem.

In Appendix A, we provide further details on these optimal control problem formulations and solutions. Returning to the goals of perception-based control, it is clear that the perception errors e_k will not follow a Guassian distribution. Because this invalidates the optimality of the LQG control strategy, we focus on bounded norm assumptions, particularly for the case of $\mathcal{L}_1$ control.

3. Data-dependent perception error

In this section, we introduce a procedure to estimate regions for which a learned perception map can be used safely during operation. We first suppose access to initial training data $\mathcal{S}_0 = \{(x_i, z_i)\}_{i=1}^{N_0}$, used to learn a perception map via any wide variety of traditional supervised methods. We then estimate safe regions around the training data, potentially using parameters learned from a second dataset. The result is a characterization of how quickly the learned perception map degrades as we move away from the initial training data.

We will describe the regions of the state space within which the sensing is reliable using a safe set which approximates sub-level sets of the error function $e(x) = p(q(x)) - Cx$. We make this precise in the following Lemma, defining a safe set which is valid under an assumption that the error function is locally slope bounded around training data.

Lemma 1 (Closeness implies generalization) *Suppose that $p \circ q - C$ is locally S-slope bounded with a radius of r around training datapoints. Define the safe set*

$$\mathcal{X}_\gamma = \bigcup_{(x_d, z_d) \in \mathcal{S}_0} \{x \in B_r(x_d) : \|p(z_d) - Cx_d\| + S\|x - x_d\| \leq \gamma\} . \tag{6}$$

Then for any (x, z) with $x \in \mathcal{X}_\gamma$, the perception error is bounded: $\|p(z) - Cx\| \leq \gamma$.

Proof The proof follows by a simple argument. For training data point (x_d, z_d) such that $x_d \in B_r(x)$,

$$\|p(z) - Cx\| = \|p(q(x)) - Cx - (p(q(x_d)) - Cx_d) + p(q(x_d)) - Cx_d\|$$
$$\leq S\|x - x_d\| + \|p(q(x_d)) - Cx_d\| .$$

The second line follows from the local slope bounded assumption. Then further choosing x_d to correspond to minimizing over training data in the definition of $\mathcal{X}_\gamma$, we have

$$\|p(z) - Cx\| \leq S\|x - x_d\| + \|p(q(x_d)) - Cx_d\| \leq \gamma .$$

■

The validity of the safe set $\mathcal{X}_\gamma$ depends on bounding the slope of the error function locally around the training data. We remark that this notion of slope boundedness has connections to sector bounded nonlinearities, a classic setting for nonlinear system stability analysis (Desoer and Vidyasagar, 1975).

Deriving the slope boundedness of the error function relies on the learned perception map as well as the underlying generative model, so we propose a second step learning step to estimate the bound S. We use an additional dataset made of samples around each training data point: $\mathcal{S}_N = \cup_{x_d \in \mathcal{S}_0} \mathcal{S}_{x_d}$, where each $\mathcal{S}_{x_d}$ contains N points densely sampled from $B_r(x_d)$. For each x_d in the training set, we then fix a radius r and estimate S with the maximum observed slope:

$$\widehat{S}_{x_d} = \max_{x_i \in \mathcal{S}_{x_d}} s(x_i, x_d), \quad \text{where} \;\; s(x, x') = \|e(x) - e(x')\| / \|x - x'\|. \tag{7}$$

By taking the maximum over training datapoints x_d, the slope bound S can be estimated with $|\mathcal{S}_0| N$ samples.

Proposition 2 *Assume that the error function $p \circ q - C$ is locally L-Lipschitz for a radius r around a training point x_d. Further assume that the true maximum slope $S_{x_d} := \max_{x \in B_r(x_d)} s(x, x_d)$ is achieved by a point with distance from x_d greater than $0 < \tau \leq r$. Then for $\widehat{S}_{x_d}$ estimated with an ε-covering[2] of $B_r(x_d)$,*

$$S_{x_d} \leq \widehat{S}_{x_d}(1 + \varepsilon/\tau) + L\varepsilon/\tau .$$

Proof Let $e(x) = p(q(x)) - Cx$. For $x_* \in \mathrm{argmax}_{x \in B_r(x_d)} s(x, x_d)$, we have

$$S = \frac{\|e(x_*) - e(x_d)\|}{\|x_* - x_d\|} = \frac{\|e(x') - e(x_d) + e(x_*) - e(x')\|}{\|x_* - x_d\|} \leq \frac{s(x', x_d)\|x' - x_d\| + L\|x_* - x'\|}{\|x_* - x_d\|},$$

for x' in the ε cover of $B_r(x_d)$. Because S can be achieved at least τ away from x_d, and x_* is at most ε away from x', we can bound S as

$$S \leq \frac{s(x', x_d)(\|x' - x_*\| + \|x_* - x_d\|) - L\|x_* - x'\|}{\|x_* - x_d\|} \leq \widehat{S}(1 + \varepsilon/\tau) + L\varepsilon/\tau.$$

∎

This result shows that adding a margin to the observed slope bound $\widehat{S}$ effectively estimates an upper bound on S. This margin decreases with the number of samples N and depends on an assumption about the local smoothness of the system. This estimation problem is similar to Lipschitz estimation, which has been widely studied with an eye toward optimization (Sergeyev and Kvasov, 2010). We note that Lipschitz smoothness is a stronger condition than our bounded slope condition, and requires several additional smoothness assumptions to estimate (Wood and Zhang, 1996).

By combining Lemma 1 with Proposition 2, we estimate bounds on the perception errors within a neighborhood of the training data. In what follows, we use these local error bounds in robust control.

4. Analysis and synthesis of perception-based controllers

The local generalization result in Lemma 1 is useful only if the system remains close to states visited during training. In this section, we show that robust control can ensure that the system will remain close to training data so long as the perception map generalizes well. By then enforcing that the composition of the bounds is a contraction, a natural notion of controller robustness emerges that guarantees favorable behavior and

---

2. We can achieve an ε-cover by gridding with $N = \left(\frac{r}{\varepsilon}\right)^d$ points from $B_r(x_d)$.

generalization. In what follows, we adopt an adversarial noise model and exploit the fact that we can design system behavior to bound how far the system deviates from states visited during training.

Recall that for a state-observation pair (x, z), the perception error, defined as $e := p(z) - Cx$, acts as additive noise to the measurement model $y = p(z)$. While standard linear control techniques can handle uniformly bounded errors, more care is necessary to further ensure that the system remains with a safe region of the state space, as determined by the training data. Through a suitable convex reformulation of the safe region, this goal can be addressed through receding horizon strategies (e.g. Wan and Kothare (2002); Mayne et al. (2006)). While these methods are effective in practice, constructing terminal sets and ensuring a priori that feasible solutions exist is not an easy task. To make explicit connections between learning and control, we turn our analysis to a system level perspective on the closed-loop to characterize its sensitivity to noise.

4.1. System-level parametrization

The system level synthesis (SLS) framework, proposed by Wang et al. (2016), provides a parametrization of our problem that makes explicit the effects of errors e on system behavior. Namely, for any controller that is a linear function of the history of system outputs, we can write the state and input as a convolution of the system noise and the closed-loop system responses $\{\Phi_{xw}(k), \Phi_{xe}(k), \Phi_{uw}(k), \Phi_{ue}(k)\}$,

$$\begin{bmatrix} x_k \\ u_k \end{bmatrix} = \sum_{t=1}^{k} \begin{bmatrix} \Phi_{xw}(t) & \Phi_{xe}(t) \\ \Phi_{uw}(t) & \Phi_{ue}(t) \end{bmatrix} \begin{bmatrix} Hw_{k-t} \\ e_{k-t} \end{bmatrix}. \tag{8}$$

As the equation (8) is linear in the system response elements Φ, convex constraints on state and input translate to convex constraints on the system response elements. The *system level synthesis* (SLS) framework shows that for any elements $\{\Phi_{xw}(k), \Phi_{xe}(k), \Phi_{uw}(k), \Phi_{ue}(k)\}$ constrained to obey, for all $k \geq 1$,

$$\Phi_{xw}(1) = I, \quad \begin{bmatrix} \Phi_{xw}(k+1) & \Phi_{xe}(k+1) \end{bmatrix} = A \begin{bmatrix} \Phi_{xw}(k) & \Phi_{xe}(k) \end{bmatrix} + B \begin{bmatrix} \Phi_{uw}(k) & \Phi_{ue}(k) \end{bmatrix},$$
$$\begin{bmatrix} \Phi_{xw}(k+1) \\ \Phi_{uw}(k+1) \end{bmatrix} = \begin{bmatrix} \Phi_{xw}(k) \\ \Phi_{uw}(k) \end{bmatrix} A + \begin{bmatrix} \Phi_{xe}(k+1) \\ \Phi_{ue}(k+1) \end{bmatrix} C,$$

there exists a feedback controller that achieves the desired system responses (8). That this parameterization is equivalent is shown in Wang et al. (2016), and therefore any optimal control problem over linear systems can be cast as a corresponding optimization problem over system response elements.

To lessen the notational burden of working with these system response elements, we will work with their z transforms. This is particularly useful for keeping track of semi-infinite sequences, especially since convolutions in time can now be represented as multiplications, i.e.

$$\begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{u} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\Phi_{xw}} & \boldsymbol{\Phi_{xe}} \\ \boldsymbol{\Phi_{uw}} & \boldsymbol{\Phi_{ue}} \end{bmatrix} \begin{bmatrix} H\boldsymbol{w} \\ \boldsymbol{e} \end{bmatrix}.$$

The corresponding control law $\boldsymbol{u} = \boldsymbol{Ky}$ is given by $\boldsymbol{K} = \boldsymbol{\Phi_{ue}} - \boldsymbol{\Phi_{uw}}\boldsymbol{\Phi_{xw}}^{-1}\boldsymbol{\Phi_{xe}}$. This controller can be implemented via a state-space realization (Anderson and Matni, 2017) or as an interconnection of the system response elements (Wang et al., 2016). The affine *realizability constraints* can be rewritten as

$$\begin{bmatrix} zI - A & -B \end{bmatrix} \boldsymbol{\Phi} = \begin{bmatrix} I & 0 \end{bmatrix}, \quad \boldsymbol{\Phi} \begin{bmatrix} zI - A \\ -C \end{bmatrix} = \begin{bmatrix} I \\ 0 \end{bmatrix} \iff \boldsymbol{\Phi} \in \mathcal{A}, \tag{9}$$

where we denote the affine space defined by (A, B, C) as $\mathcal{A}$.

7

In this SLS framework, many robust control costs can be written as system norms,

$$
c(\boldsymbol{x}, \boldsymbol{u}) = \sup_{\substack{\|\boldsymbol{w}\| \le \varepsilon_w \\ \|\boldsymbol{e}\| \le \varepsilon_e}} \left\| \begin{bmatrix} Q^{1/2} & \\ & R^{1/2} \end{bmatrix} \begin{bmatrix} \boldsymbol{\Phi}_{\boldsymbol{xw}} & \boldsymbol{\Phi}_{\boldsymbol{xe}} \\ \boldsymbol{\Phi}_{\boldsymbol{uw}} & \boldsymbol{\Phi}_{\boldsymbol{ue}} \end{bmatrix} \begin{bmatrix} H\boldsymbol{w} \\ \boldsymbol{e} \end{bmatrix} \right\| = \left\| \begin{bmatrix} Q^{1/2} & \\ & R^{1/2} \end{bmatrix} \begin{bmatrix} \boldsymbol{\Phi}_{\boldsymbol{xw}} & \boldsymbol{\Phi}_{\boldsymbol{xe}} \\ \boldsymbol{\Phi}_{\boldsymbol{uw}} & \boldsymbol{\Phi}_{\boldsymbol{ue}} \end{bmatrix} \begin{bmatrix} \varepsilon_w H \\ \varepsilon_e I \end{bmatrix} \right\| .
$$

For LQG control, the objective is equivalent to a system $\mathcal{H}_2$ norm (Zhou et al., 1996).

A comment on finite-dimensional realizations Although the constraints and objective function in this framework are infinite dimensional, two finite-dimensional approximations have been successfully applied. The first consists of selecting an approximation horizon T, and enforcing that $\boldsymbol{\Phi}(T) = 0$ for some appropriately large T, which is always possible for systems that are controllable and observable. When this is not possible, one can instead enforce bounds on the norm of $\boldsymbol{\Phi}(T)$ and use robustness arguments to show that the sub-optimality gap incurred by this finite dimensional approximation decays exponentially in the approximation horizon T (Anderson et al., 2019; Boczar et al., 2018; Dean et al., 2017; Matni et al., 2017). Finally, in the interest of clarity, we always present the infinite horizon version of the optimization problems, with the understanding that a finite horizon approximations are necessary in practice.

4.2. Robust control for generalization

In what follows, we specialize controller design concerns to our perception-based setting, and develop further conditions on the closed-loop response $\boldsymbol{\Phi}$ to incorporate into the synthesis problem. Because system level parametrization makes explicit the effects of perception errors $\boldsymbol{e}$ on system behavior, we can transparently keep track of closed-loop behavior, as made precise in the following Lemma.

Lemma 3 (Generalization implies closeness) *For a perception map p with errors $\boldsymbol{e} = p(\boldsymbol{z}) - C\boldsymbol{x}$, let the system responses $\{\boldsymbol{\Phi}_{\boldsymbol{xw}}, \boldsymbol{\Phi}_{\boldsymbol{xe}}, \boldsymbol{\Phi}_{\boldsymbol{uw}}, \boldsymbol{\Phi}_{\boldsymbol{ue}}\}$ lie in the affine space defined by dynamics (A, B, C), and let $\boldsymbol{K}$ be the associated controller. Then the state trajectory $\boldsymbol{x}$ achieved by the control law $\boldsymbol{u} = \boldsymbol{K}p(\boldsymbol{z})$ and driven by noise process $\boldsymbol{w}$, satisfies, for any target trajectory $\boldsymbol{x}_d$,*

$$
\|\boldsymbol{x} - \boldsymbol{x}_d\| \le \|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| + \|\boldsymbol{\Phi}_{\boldsymbol{xe}}\| \|\boldsymbol{e}\|. \tag{10}
$$

where we define the nominal closeness *as the deviation from the target in the absence of measurement errors:* $\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| = \|\boldsymbol{\Phi}_{\boldsymbol{xw}}H\boldsymbol{w} - \boldsymbol{x}_d\|$.

Proof Notice that over the course of a trajectory, we have system outputs $\boldsymbol{y} = p(\boldsymbol{z}) = C\boldsymbol{x} + \boldsymbol{e}$. Then recalling that the system responses are defined such that $\boldsymbol{x} = \boldsymbol{\Phi}_{\boldsymbol{xw}}H\boldsymbol{w} + \boldsymbol{\Phi}_{\boldsymbol{xe}}\boldsymbol{e}$, we have that

$$
\|\boldsymbol{x} - \boldsymbol{x}_d\| = \|\boldsymbol{\Phi}_{\boldsymbol{xw}}H\boldsymbol{w} + \boldsymbol{\Phi}_{\boldsymbol{xe}}\boldsymbol{e} - \boldsymbol{x}_d\| \le \|\boldsymbol{\Phi}_{\boldsymbol{xw}}H\boldsymbol{w} - \boldsymbol{x}_d\| + \|\boldsymbol{\Phi}_{\boldsymbol{xe}}\| \|\boldsymbol{e}\| .
$$

∎

The terms in bound (10) capture different generalization properties. The first is small if we plan to visit states during operation that are similar to those seen during training. The second term is a measure of the robustness of our system to the error $\boldsymbol{e}$.

We are now in a position to state the main result of the paper, which shows that under an additional robustness condition, Lemmas 1 and 3 combine to define a control invariant set around the training data within which we can bound the perception errors and consequently the performance.

Theorem 4 *Let the assumptions of Lemmas 1 and 3 hold and suppose that the training error is bounded, i.e.* $\|p(z_d) - Cx_d\| \leq R_0$ *for all* $(x_d, z_d) \in \mathcal{S}_0$. *Then as long as*

$$\|\boldsymbol{\Phi_{xe}}\| \leq \frac{1 - \frac{1}{r}\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\|}{S + \frac{R_0}{r}} \, , \tag{11}$$

the perception errors remain bounded

$$\|p(\boldsymbol{z}) - C\boldsymbol{x}\| \leq \frac{\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| + R_0}{1 - S\|\boldsymbol{\Phi_{xe}}\|} := \gamma, \tag{12}$$

and the closed-loop trajectory lies within $\mathcal{X}_\gamma$.

Proof Recall that as in the proof of Lemma 1, as long as $x_k \in B_r(x_{d,k})$ for all k and some arbitrary $x_{d,k} \in \mathcal{S}_0$,

$$\|e_k\| \leq S\|x_k - x_{d,k}\| + \|e_{d_k}\| \implies \|\boldsymbol{e}\| = \max_k \|e_k\| \leq S\|\boldsymbol{x} - \boldsymbol{x}_d\| + \|\boldsymbol{e}_d\| \, . \tag{13}$$

By assumption, $\|\boldsymbol{e}_d\| \leq R_0$. Substituting this expression into the result of Lemma 3, we see that as long as $\|x_k - x_{d,k}\| \leq r$ for all k,

$$\|\boldsymbol{x} - \boldsymbol{x}_d\| \leq \|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| + \|\boldsymbol{\Phi_{xe}}\|(S\|\boldsymbol{x} - \boldsymbol{x}_d\| + \|\boldsymbol{e}_d\|) \iff \|\boldsymbol{x} - \boldsymbol{x}_d\| \leq \frac{\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| + \varepsilon_\eta\|\boldsymbol{\Phi_{xe}}\|}{1 - S\|\boldsymbol{\Phi_{xe}}\|} \, ,$$

Next, to ensure that the the radius is bounded, first note that by norm definition, $\max_k \|x_k - x_{d,k}\|_\infty \leq r$ if and only if $\|\boldsymbol{x} - \boldsymbol{x}_d\| \leq r$. A sufficient condition for this is given by

$$\frac{\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| + R_0\|\boldsymbol{\Phi_{xe}}\|}{1 - S\|\boldsymbol{\Phi_{xe}}\|} \leq r \iff \|\boldsymbol{\Phi_{xe}}\| \leq \frac{1 - \frac{1}{r}\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\|}{S + \frac{R_0}{r}} \, ,$$

and thus we arrive at the robustness condition. Since the bound on $\|\boldsymbol{x} - \boldsymbol{x}_d\|$ is valid, we now use it to bound $\|\boldsymbol{e}\|$, starting with (13) and rearranging,

$$\|\boldsymbol{e}\| \leq \frac{\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| + R_0}{1 - S\|\boldsymbol{\Phi_{xe}}\|} \, .$$

∎

Theorem 4 shows that the bound (11) should be used during controller synthesis to ensure generalization. Feasibility of the synthesis problem depends on the controllability and observability of the system (A, B, C), which impose limits on how small $\|\boldsymbol{\Phi_{xe}}\|$ can be made to be, and on the planned deviation from training data as captured by the quantity $\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\|$.

4.3. Robust synthesis for waypoint tracking

We now specialize to the task of waypoint tracking to simplify the term $\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\|$ and propose a robust control synthesis problem. Recall that waypoint tracking can be encoded by defining the state $x_k = [\xi_k - r_k; r_k]$ as the concatenation of tracking error and waypoint and the disturbance as the change in reference, $w_k = r_{k+1} - r_k$.

Proposition 5 *For a reference tracking problem with $\|r_{k+1} - r_k\| \le \Delta_{\text{ref}}$ and a reference trajectory within a ball of radius r_{ref} from the training data,*

$$\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| \le \Delta_{\text{ref}} \| \begin{bmatrix} I & 0 \end{bmatrix} \boldsymbol{\Phi_{xw}} H \| + r_{\text{ref}} \ .$$

Proof For the training data, we can assume zero tracking errors, so that $\boldsymbol{\xi}_d = \boldsymbol{r}_d$. Then $x_{d,k} = [0; \xi_{d,k}]$. Thus, we can rewrite $\|\widehat{\boldsymbol{x}} - \boldsymbol{x}_d\| \le \|\boldsymbol{\xi} - \boldsymbol{r}\| + \|\boldsymbol{r} - \boldsymbol{\xi}_d\| = \| \begin{bmatrix} I & 0 \end{bmatrix} \boldsymbol{\Phi_{xw}} \boldsymbol{w} \| + \|\boldsymbol{r} - \boldsymbol{\xi}_d\|.$ ∎

Using this setting, we add the robustness condition in (11) to a control synthesis problem as

$$\begin{aligned} \text{minimize}_{\boldsymbol{\Phi}} \quad & c(\boldsymbol{\Phi}) \\ \text{subject to} \quad & \boldsymbol{\Phi} \in \mathcal{A}, \ \ (S + \tfrac{R_0}{r})\|\boldsymbol{\Phi_{xe}}\| + \tfrac{\Delta_{\text{ref}}}{r} \| \begin{bmatrix} I & 0 \end{bmatrix} \boldsymbol{\Phi_{xw}} H \| + \tfrac{r_{\text{ref}}}{r} \le 1 \ . \end{aligned}$$

Notice the trade-off between the size of different parts of the system response. Because the responses must lie in an affine space, they cannot both become arbitrarily small. Therefore, the synthesis problem must trade off between sensitivity to measurement errors and tracking fidelity. These trade-offs are mediated by the quality of the perception map, through its slope-boundedness and training error, and the ambition of the control task, through its deviation from training data and distances between waypoints.

While the robustness constraint in (11) is enough to guarantee a finite cost, it does not guarantee a small cost. To achieve this, we incorporate the error bound to arrive at the following robust synthesis procedure:

$$\begin{aligned} \text{minimize}_{\boldsymbol{\Phi},\gamma} \quad & \left\| \begin{bmatrix} Q^{1/2} & \\ & R^{1/2} \end{bmatrix} \begin{bmatrix} \boldsymbol{\Phi_{xw}} & \boldsymbol{\Phi_{xe}} \\ \boldsymbol{\Phi_{uw}} & \boldsymbol{\Phi_{ue}} \end{bmatrix} \begin{bmatrix} \Delta_{\text{ref}} H \\ \gamma I \end{bmatrix} \right\| \\ \text{subject to} \quad & \boldsymbol{\Phi} \in \mathcal{A}, \ \ (S + \tfrac{R_0}{r})\|\boldsymbol{\Phi_{xe}}\| + \tfrac{\Delta_{\text{ref}}}{r} \| \begin{bmatrix} I & 0 \end{bmatrix} \boldsymbol{\Phi_{xw}} H \| + \tfrac{r_{\text{ref}}}{r} \le 1 \\ & \Delta_{\text{ref}} \| \begin{bmatrix} I & 0 \end{bmatrix} \boldsymbol{\Phi_{xw}} H \| + r_{\text{ref}} + R_0 \le \gamma(1 - S\|\boldsymbol{\Phi_{xe}}\|) \ . \end{aligned}$$

This is a convex program for fixed γ, so the full problem can then be approximately solved via one-dimensional search.

4.4. Necessity of robustness

Robust control is notoriously conservative, and our main result is distinctly small-gain theorem in nature. Can the conservatism inherent in this approach be generally reduced? In this section, we answer in the negative by describing a class of examples for which the robustness condition in Theorem 4 is necessary. For simplicity, we specialize to the goal of regulating a system to the origin, and assume that $(0, z_0)$ is in the training set, with $p(z_0) = 0$.

We consider the following optimal control problem

$$\min_{\boldsymbol{\Phi}} c(\boldsymbol{\Phi}) \text{ subject to } \boldsymbol{\Phi} \in \mathcal{A}, \ \ \|\boldsymbol{\Phi_{xe}}\| \le \alpha$$

and define $\bar{\boldsymbol{\Phi}}$ as a minimizing argument for the problem without the inequality constraint. For simplicity, we consider only systems in which the closed-loop is strictly proper and has a state-space realization.

Proposition 6 *Suppose that*

$$\|\bar{\boldsymbol{\Phi}}_{\boldsymbol{xn}}\|_{\mathcal{L}_1} = \|\bar{\boldsymbol{\Phi}}_{\boldsymbol{xn}}(1)\|_{\infty \to \infty} \ .$$

Then there exists a differentiable error function with slope bound S such that the $x = 0$ is an asymptotically stable equilibrium if and only if $\alpha < \frac{1}{S}$.

Proof The sufficiency follows from our main analysis, or alternately a simple application of small gain theorem. The necessity follows by construction, with a combination of classic nonlinear instability arguments and by considering real stability radii.

Recall that $y_k = Cx_k + (p(q(x_k)) - Cx_k)$. Define ζ_k to represent the internal state of the controller. Then we can write the system's closed-loop behavior as (ignoring for now the effect of process noise, which does not affect the stability analysis)

$$\begin{bmatrix} x_{k+1} \\ \zeta_{k+1} \end{bmatrix} = A_{\text{CL}} \begin{bmatrix} x_k \\ \zeta_k \end{bmatrix} + B_{\text{CL}} e(x_k) \,.$$

Suppose that the error function $e(x)$ is differentiable at $x = 0$ with derivative J. Then the stability of the origin depends on the linearized closed loop system $A_{\text{CL}}(J) := A_{\text{CL}} + B_{\text{CL}} J C_{\text{CL}}$ where $C_{\text{CL}} = [I \; 0]$ picks out the relevant component of the closed-loop state. If any eigenvalues of $A_{\text{CL}}(J)$ lie outside of the unit disk, then $x = 0$ is not an asymptotically stable equilibrium.

Switching gears, recall that $\mathbf{\Phi}_{\boldsymbol{xe}}(z) = C_{\text{CL}}(zI - A_{\text{CL}})^{-1} B_{\text{CL}}$. We define $S = 1/\|\bar{\mathbf{\Phi}}_{\boldsymbol{xe}}\|$ and notice that if $\alpha \geq \frac{1}{S}$, then $\bar{\mathbf{\Phi}}$ is also the solution to the constrained problem. By assumption, $\|\bar{\mathbf{\Phi}}_{\boldsymbol{xn}}\|_{\mathcal{L}_1} = \|\bar{\mathbf{\Phi}}_{\boldsymbol{xn}}(1)\|_{\infty \to \infty}$. Thus, there exist real w, v such that $v^\top \bar{\mathbf{\Phi}}_{\boldsymbol{xn}}(1) w = \|\bar{\mathbf{\Phi}}_{\boldsymbol{xn}}\|$. If we set $J = Swv^\top$, then $A_{\text{CL}}(J)$ has an eigenvalue on the unit disk and $x = 0$ is not an asymptotically stable equilibrium. To see why this is true, recall the classic result for stability radii (e.g. Corollary 4.5 in Hinrichsen and Pritchard (1990)) and notice

$$\bar{\mathbf{\Phi}}_{\boldsymbol{xn}}(1) = \sum_{k \geq 0} \Phi_{xn}(k) = \sum_{k \geq 0} C_{\text{CL}} A_{\text{CL}}^k B_{\text{CL}} = C_{\text{CL}}(I - A_{\text{CL}})^{-1} B_{\text{CL}} \,.$$

Thus, for any error function with derivative $J = Swv^\top$ at zero, the robustness condition is necessary as well as sufficient. One such error function is simply $e(x) = Jx$, though many more complex forms exist. ∎

We now present a simple example in which this condition is satisfied, and construct the corresponding error function which results in an unstable system.

Example Consider the double integrator

$$x_{k+1} = \begin{bmatrix} 1 & dt \\ 0 & 1 \end{bmatrix} x_k + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_k, \quad y_k = p(z_k) = x_k + e(x_k) \,, \tag{14}$$

and the control law resulting from the $\mathcal{H}_2$ optimal control problem with identity weighting matrices along with the robustness constraint $\|\mathbf{\Phi}_{\boldsymbol{xe}}\| \leq \alpha$. Notice that the solution to the unconstrained problem would be the familiar LQG combination of Kalman filtering and static feedback on the estimated state. We denote the optimal unconstrained system response by $\bar{\mathbf{\Phi}}$.

Consider an error function with slope bounded by $S = 1/\|\bar{\mathbf{\Phi}}_{\boldsymbol{xe}}\|$ and derivative at $x = 0$ equal to

$$J = \begin{bmatrix} -1/\|\bar{\mathbf{\Phi}}_{\boldsymbol{xe}}\| & 0 \\ -1/\|\bar{\mathbf{\Phi}}_{\boldsymbol{xe}}\| & 0 \end{bmatrix} \,,$$

Calculations confirm that the $\mathcal{L}_1$ norm satisfies the relevant property and that the origin is not a stable fixed point if the synthesis constraint $\alpha \geq \frac{1}{S}$.

Figure 2: In (a), visual inputs $\{z_t\}$ for the synthetic (left) and CARLA (right) examples. In (b), (left) the ℓ_∞ bounded ball the synthetic circle must remain inside in the face of bounded adversarial noise, (center) the nominal trajectory the synthetic circle is driven to follow, and (right) and the nominal trajectory the simulated vehicle is driven to follow.

5. Experiments

We demonstrate our theoretical results with examples of control from pixels, using both simple synthetic images and complex graphics simulation. The synthetic example uses generated 64×64 pixel images of a moving blurry white circle on a black background; the complex example uses 800×600 pixel dashboard camera images of a vehicle in the CARLA simulator platform (Dosovitskiy et al., 2017). Figure 5(a) shows representative images seen by the controllers.

For both visual settings, we demonstrate our results in controlling a 2D double integrator to track a periodic reference. The 2D double integrator state is given by $x_k^\top = [(x_k^{(1)})^\top \, (x_k^{(2)})^\top]$, and each component evolves independently according to the dynamics in (14) with $dt = 0.1$. For all examples, the sensing matrix C extracts the position of the system, i.e., $Cx_k = [x_{1,k}^{(1)}, x_{1,k}^{(2)}]$. Training and validation trajectories are generated by driving the system with an optimal state feedback controller (i.e. where measurement $\boldsymbol{y} = \boldsymbol{x}$) to track a desired reference trajectory $\boldsymbol{w} = \boldsymbol{r} + \boldsymbol{v}$, where $\boldsymbol{r}$ is a nominal reference, and $\boldsymbol{v}$ is a random norm bounded random perturbation satisfying $\|v_k\|_\infty \le 0.1$.

We consider three different perception maps: a linear map for the synthetic example and both visual odometry and a convolutional neural net for the CARLA example. To train the CNN, we collect a dense set of training examples around the reference, and train a CNN with a fully connected layer to output position and heading of the camera pose. We require ≈ 30000 training points. During operation, pixel-data z is passed through the CNN to obtain position estimates y, which are then used by the robust controller.

To perform visual odometry, we first collect images from known poses around the desired reference trajectory. We then use ORB SLAM (Mur-Artal and Tardós, 2016) to build a global map of visual features and a database of reference images with known poses. This is the "training" phase. We use one trajectory of 200 points; the reference database is approximately this size. During operation, an image z is matched with an image z_d in the database. The reprojection error between the matched features in z_d with known pose x_d and their corresponding features in z is then minimized to generate pose estimate y. For more details on standard visual odometry methods, see Scaramuzza and Fraundorfer (2011). We highlight that modern visual SLAM algorithms incorporate sophisticated filtering and optimization techniques for localization in previously unseen environments with complex dynamics; we use a simplified algorithm under this training and testing paradigm in order to better isolate the data dependence.

We then estimate safe regions for all three maps, as described in Section 3. In the top panels of Figure 3 we show the error profiles as a function of distance to the nearest training point for the linear (right), SLAM (middle), and CNN (right) maps. We see that these data-dependent localization schemes exhibit the local slope bounded property posited in the previous section.
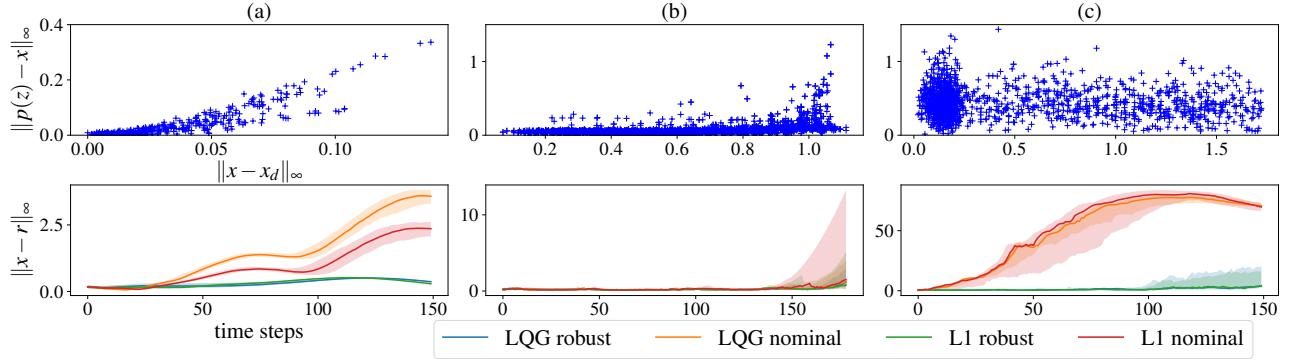
Figure 3: (top) Test perception error $\|p(z) - Cx\|_\infty$ vs. distance to the nearest training point $\|x - x_d\|_\infty$; and (bottom) median ℓ_∞ tracking error for 200 rollouts using the (a) linear map on synthetic images, (b) SLAM and (c) CNN on CARLA dashboard images. Error bars show upper and lower quartiles.

We compare robust synthesis to the behavior of *nominal controllers* that do not take into account the nonlinearity in the measurement model. In particular, we compare the performance of naively synthesized LQG and $\mathcal{L}_1$ optimal controllers with controllers designed with the robustness condition (11). LQG is a standard control scheme that explicitly separates state estimation (Kalman Filtering) from control (LQR control), and is emblematic of much of standard control practice. $\mathcal{L}_1$ optimal control minimizes worst case state deviation and control effort by modeling process and sensor errors as ℓ_∞ bounded adversarial processes. For further discussion and details, refer to Section 2.1 and Appendix B. The bottom panels of Figure 3 show that the robustly synthesized controllers remain within a bounded neighborhood around the training data. On the other hand, the nominal controllers drive the system away from the training data, leading to a failure of the perception and control loop. We note that although visual odometry may not satisfy smoothness assumptions when the feature detection and matching fails, we nevertheless observe safe system behavior, suggesting that using our robust controller, no such failures occur.

6. Conclusion

Though standard practice is to treat the output of a perception module as an ordinary signal, we have demonstrated both in theory and experimentally that accounting for the inherent uncertainty of perception based sensors can dramatically improve the performance of the resulting control loop. Moreover, we have shown how to quantify and account for such uncertainties with tractable data-driven safety guarantees. We hope to extend this study to the control of more complex systems, and to apply this framework to standard model-predictive control pipelines which form the basis of much of contemporary control practice.

We further hope to highlight the challenges involved in adapting learning-theoretic notions of generalization to the setting of controller synthesis. First note that if we collect data using one controller, and then use this data to build a new controller, there will be a distribution shift in the observations seen between the two controllers. Any statistical generalization bounds on performance must necessarily account for this shift. Second, from a more practical standpoint, most generalization bounds require knowing instance specific quantities governing properties of the class of functions we use to fit a predictor. Hence, they will include constants that are not measurable in practice. This issue can perhaps be mitigated using some sort of bootstrap technique for post-hoc validation. However, we note that the sort of bounds we aim to bootstrap are worst case, not average case. Indeed, the bootstrap typically does not even provide a consistent estimate of the maximum of independent random variables, see for instance Bickel et al. (1981), and Ch 9.3 in Chernick (2011). Other measures such as conditional value at risk require billions of samples to guarantee five 9s of

reliability (Rockafellar et al., 2000). We highlight these issues only to point out that adapting statistical generalization to robust control is an active area with many open challenges to be considered in future work.

Acknowledgments

References

Yasin Abbasi-Yadkori and Csaba Szepesvári. Regret bounds for the adaptive control of linear quadratic systems. In *Proceedings of the 24th Annual Conference on Learning Theory*, pages 1–26, 2011.

Yasin Abbasi-Yadkori, Nevena Lazic, and Csaba Szepesvári. Model-free linear quadratic control via reduction to expert prediction. In *The 22nd International Conference on Artificial Intelligence and Statistics*, pages 3108–3117, 2019.

Marc Abeille and Alessandro Lazaric. Improved regret bounds for thompson sampling in linear quadratic control problems. In *International Conference on Machine Learning*, pages 1–9, 2018.

Naman Agarwal, Brian Bullins, Elad Hazan, Sham M Kakade, and Karan Singh. Online control with adversarial disturbances. *arXiv preprint arXiv:1902.08721*, 2019.

Anayo K Akametalu, Jaime F Fisac, Jeremy H Gillula, Shahab Kaynama, Melanie N Zeilinger, and Claire J Tomlin. Reachability-based safe learning with gaussian processes. In *53rd IEEE Conference on Decision and Control*, pages 1424–1431. IEEE, 2014.

Oren Anava, Elad Hazan, Shie Mannor, and Ohad Shamir. Online learning for time series prediction. In *Conference on learning theory*, pages 172–184, 2013.

Oren Anava, Elad Hazan, and Shie Mannor. Online learning for adversaries with memory: price of past mistakes. In *Advances in Neural Information Processing Systems*, pages 784–792, 2015.

James Anderson and Nikolai Matni. Structured state space realizations for sls distributed controllers. In *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 982–987. IEEE, 2017.

James Anderson, John C Doyle, Steven Low, and Nikolai Matni. System level synthesis. *arXiv preprint arXiv:1904.01634*, 2019.

MOSEK ApS. *MOSEK Optimizer API for Python Release 9.0.88*, 2019. URL https://docs.mosek.com/9.0/pythonapi.pdf.

Somil Bansal, Varun Tolani, Saurabh Gupta, Jitendra Malik, and Claire Tomlin. Combining optimal control and learning for visual navigation in novel environments. *arXiv preprint arXiv:1903.02531*, 2019.

Felix Berkenkamp, Matteo Turchetta, Angela Schoellig, and Andreas Krause. Safe model-based reinforcement learning with stability guarantees. In *Advances in neural information processing systems*, pages 908–918, 2017.

Peter J Bickel, David A Freedman, et al. Some asymptotic theory for the bootstrap. *The annals of statistics*, 9 (6):1196–1217, 1981.

Ross Boczar, Nikolai Matni, and Benjamin Recht. Finite-data performance guarantees for the output-feedback control of an unknown system. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 2994–2999. IEEE, 2018.

Mariusz Bojarski, Davide Del Testa, Daniel Dworakowski, Bernhard Firner, Beat Flepp, Prasoon Goyal, Lawrence D Jackel, Mathew Monfort, Urs Muller, Jiakai Zhang, et al. End to end learning for self-driving cars. *arXiv preprint arXiv:1604.07316*, 2016.

Richard Cheng, Gábor Orosz, Richard M Murray, and Joel W Burdick. End-to-end safe reinforcement learning through barrier functions for safety-critical continuous control tasks. *arXiv preprint arXiv:1903.08792*, 2019.

Michael R Chernick. *Bootstrap methods: A guide for practitioners and researchers*, volume 619. John Wiley & Sons, 2011.

Felipe Codevilla, Matthias Miiller, Antonio López, Vladlen Koltun, and Alexey Dosovitskiy. End-to-end driving via conditional imitation learning. In *2018 IEEE International Conference on Robotics and Automation (ICRA)*, pages 1–9. IEEE, 2018.

Alon Cohen, Tomer Koren, and Yishay Mansour. Learning linear-quadratic regulators efficiently with only $\sqrt{T}$ regret. *arXiv preprint arXiv:1902.06223*, 2019.

M. Dahleh and J. Pearson. ℓ^1-optimal feedback controllers for MIMO discrete-time systems. *IEEE Transactions on Automatic Control*, 32(4):314–322, April 1987. ISSN 0018-9286. doi: 10.1109/TAC.1987. 1104603.

Sarah Dean, Horia Mania, Nikolai Matni, Benjamin Recht, and Stephen Tu. On the sample complexity of the linear quadratic regulator. *arXiv preprint arXiv:1710.01688*, 2017.

Sarah Dean, Horia Mania, Nikolai Matni, Benjamin Recht, and Stephen Tu. Regret bounds for robust adaptive control of the linear quadratic regulator. In *Advances in Neural Information Processing Systems*, pages 4192–4201, 2018.

Charles A Desoer and Mathukumalli Vidyasagar. *Feedback systems: input-output properties*, volume 55. Siam, 1975.

Alexey Dosovitskiy, German Ros, Felipe Codevilla, Antonio Lopez, and Vladlen Koltun. Carla: An open urban driving simulator. *arXiv preprint arXiv:1711.03938*, 2017.

Salar Fattahi and Somayeh Sojoudi. Data-driven sparse system identification. In *2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 462–469. IEEE, 2018.

Salar Fattahi, Nikolai Matni, and Somayeh Sojoudi. Learning sparse dynamical systems from a single sample trajectory. *arXiv preprint arXiv:1904.09396*, 2019.

Alessandro Giusti, Jérôme Guzzi, Dan C Cireşan, Fang-Lin He, Juan P Rodríguez, Flavio Fontana, Matthias Faessler, Christian Forster, Jürgen Schmidhuber, Gianni Di Caro, et al. A machine learning approach to visual perception of forest trails for mobile robots. *IEEE Robotics and Automation Letters*, 1(2):661–667, 2015.

Moritz Hardt, Tengyu Ma, and Benjamin Recht. Gradient descent learns linear dynamical systems. *The Journal of Machine Learning Research*, 19(1):1025–1068, 2018.

Babak Hassibi and Thomas Kaliath. H-∞ bounds for least-squares estimators. *IEEE Transactions on Automatic Control*, 46(2):309–314, 2001.

Joel A Hesch, Dimitrios G Kottas, Sean L Bowman, and Stergios I Roumeliotis. Camera-imu-based localization: Observability analysis and consistency improvement. *The International Journal of Robotics Research*, 33(1):182–201, 2014.

Lukas Hewing and Melanie N Zeilinger. Cautious model predictive control using gaussian process regression. *arXiv preprint arXiv:1705.10702*, 2017.

Diederich Hinrichsen and Anthony J Pritchard. Real and complex stability radii: a survey. In *Control of uncertain systems*, pages 119–162. Springer, 1990.

Eagle S Jones and Stefano Soatto. Visual-inertial navigation, mapping and localization: A scalable real-time causal approach. *The International Journal of Robotics Research*, 30(4):407–430, 2011.

Jonathan Kelly and Gaurav S Sukhatme. Visual-inertial sensor fusion: Localization, mapping and sensor-to-sensor self-calibration. *The International Journal of Robotics Research*, 30(1):56–79, 2011.

Vitaly Kuznetsov and Mehryar Mohri. Time series prediction and online learning. In *Conference on Learning Theory*, pages 1190–1213, 2016.

Alexander Lambert, Amirreza Shaban, Amit Raj, Zhen Liu, and Byron Boots. Deep forward and inverse perceptual models for tracking and prediction. In *2018 IEEE International Conference on Robotics and Automation (ICRA)*, pages 675–682. IEEE, 2018.

Sergey Levine, Chelsea Finn, Trevor Darrell, and Pieter Abbeel. End-to-end training of deep visuomotor policies. *The Journal of Machine Learning Research*, 17(1):1334–1373, 2016.

Yi Lin, Fei Gao, Tong Qin, Wenliang Gao, Tianbo Liu, William Wu, Zhenfei Yang, and Shaojie Shen. Autonomous aerial navigation using monocular visual-inertial fusion. *Journal of Field Robotics*, 35(1): 23–51, 2018.

Giuseppe Loianno, Chris Brunner, Gary McGrath, and Vijay Kumar. Estimation, control, and planning for aggressive flight with a small quadrotor with a single camera and imu. *IEEE Robotics and Automation Letters*, 2(2):404–411, 2016.

Simon Lynen, Markus W Achtelik, Stephan Weiss, Margarita Chli, and Roland Siegwart. A robust and modular multi-sensor fusion approach applied to mav navigation. In *2013 IEEE/RSJ international conference on intelligent robots and systems*, pages 3923–3929. IEEE, 2013.

Simon Lynen, Torsten Sattler, Michael Bosse, Joel A Hesch, Marc Pollefeys, and Roland Siegwart. Get out of my lab: Large-scale, real-time visual-inertial localization. In *Robotics: Science and Systems*, 2015.

Horia Mania, Stephen Tu, and Benjamin Recht. Certainty equivalent control of lqr is efficient. *arXiv preprint arXiv:1902.07826*, 2019.

Nikolai Matni, Yuh-Shyang Wang, and James Anderson. Scalable system level synthesis for virtually localizable systems. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 3473–3480. IEEE, 2017.

David Q Mayne, SV Raković, Rolf Findeisen, and Frank Allgöwer. Robust output feedback model predictive control of constrained linear systems. *Automatica*, 42(7):1217–1222, 2006.

Raul Mur-Artal and Juan D. Tardós. ORB-SLAM2: an open-source SLAM system for monocular, stereo and RGB-D cameras. *CoRR*, abs/1610.06475, 2016. URL http://arxiv.org/abs/1610.06475.

C. J. Ostafew, A. P. Schoellig, and T. D. Barfoot. Learning-based nonlinear model predictive control to improve vision-based mobile robot path-tracking in challenging outdoor environments. In *2014 IEEE International Conference on Robotics and Automation (ICRA)*, pages 4029–4036, May 2014. doi: 10.1109/ICRA.2014.6907444.

Y. Ouyang, M. Gagrani, and R. Jain. Control of unknown linear systems with thompson sampling. In *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1198–1205, Oct 2017. doi: 10.1109/ALLERTON.2017.8262873.

Samet Oymak and Necmiye Ozay. Non-asymptotic identification of lti systems from a single trajectory. *arXiv preprint arXiv:1806.05722*, 2018.

Yunpeng Pan, Ching-An Cheng, Kamil Saigol, Keuntaek Lee, Xinyan Yan, Evangelos Theodorou, and Byron Boots. Agile autonomous driving using end-to-end deep imitation learning. *Proceedings of Robotics: Science and Systems. Pittsburgh, Pennsylvania*, 2018.

José Pereira, Morteza Ibrahimi, and Andrea Montanari. Learning networks of stochastic differential equations. In *Advances in Neural Information Processing Systems*, pages 172–180, 2010.

Dean A Pomerleau. Alvinn: An autonomous land vehicle in a neural network. In *Advances in neural information processing systems*, pages 305–313, 1989.

Anders Rantzer. Concentration bounds for single parameter adaptive control. In *2018 Annual American Control Conference (ACC)*, pages 1862–1866. IEEE, 2018.

R Tyrrell Rockafellar, Stanislav Uryasev, et al. Optimization of conditional value-at-risk. *Journal of risk*, 2: 21–42, 2000.

Daniel J. Russo, Benjamin Van Roy, Abbas Kazerouni, Ian Osband, and Zheng Wen. A tutorial on thompson sampling. *Foundations and Trends on Machine Learning*, 11(1):1–96, July 2018. doi: 10.1561/2200000070.

Fereshteh Sadeghi and Sergey Levine. Cad2rl: Real single-image flight without a single real image. *arXiv preprint arXiv:1611.04201*, 2016.

Tuhin Sarkar and Alexander Rakhlin. How fast can linear dynamical systems be learned? *arXiv preprint arXiv:1812.01251*, 2018.

Tuhin Sarkar, Alexander Rakhlin, and Munther A Dahleh. Finite-time system identification for partially observed lti systems of unknown order. *arXiv preprint arXiv:1902.01848*, 2019.

Davide Scaramuzza and Friedrich Fraundorfer. Visual odometry [tutorial]. *IEEE robotics & automation magazine*, 18(4):80–92, 2011.

Yaroslav D Sergeyev and Dmitri E Kvasov. L ipschitz global optimization. *Wiley Encyclopedia of Operations Research and Management Science*, 2010.

Max Simchowitz, Horia Mania, Stephen Tu, Michael I Jordan, and Benjamin Recht. Learning without mixing: Towards a sharp analysis of linear system identification. In *Conference On Learning Theory*, pages 439–473, 2018.

Sarah Tang, Valentin Wüest, and Vijay Kumar. Aggressive flight with suspended payloads using vision-based control. *IEEE Robotics and Automation Letters*, 3(2):1152–1159, 2018.

Andrew J Taylor, Victor D Dorobantu, Hoang M Le, Yisong Yue, and Aaron D Ames. Episodic learning with control lyapunov functions for uncertain robotic systems. *arXiv preprint arXiv:1903.01577*, 2019.

Anastasios Tsiamis and George J Pappas. Finite sample analysis of stochastic system identification. *arXiv preprint arXiv:1903.09122*, 2019.

Kim P Wabersich and Melanie N Zeilinger. Linear model predictive safety certification for learning-based control. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 7130–7135. IEEE, 2018.

Zhaoyang Wan and Mayuresh V Kothare. Robust output feedback model predictive control using off-line linear matrix inequalities. *Journal of Process Control*, 12(7):763–774, 2002.

Yuh-Shyang Wang, Nikolai Matni, and John C Doyle. A system level approach to controller synthesis. *arXiv preprint arXiv:1610.04815*, 2016.

Grady Williams, Paul Drews, Brian Goldfain, James M Rehg, and Evangelos A Theodorou. Information-theoretic model predictive control: Theory and applications to autonomous driving. *IEEE Transactions on Robotics*, 34(6):1603–1622, 2018.

GR Wood and BP Zhang. Estimation of the lipschitz constant of a function. *Journal of Global Optimization*, 8(1):91–103, 1996.

Sholeh Yasini and Kristiaan Pelckmans. Worst-case prediction performance analysis of the kalman filter. *IEEE Transactions on Automatic Control*, 63(6):1768–1775, 2018.

Seungil You and Ather Gattami. H infinity analysis revisited. *arXiv preprint arXiv:1412.6160*, 2014.

Kemin Zhou, John Comstock Doyle, Keith Glover, et al. *Robust and optimal control*, volume 40. Prentice Hall, 1996.

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

Table 1: Different noise model classes induce different cost functions, and can be used to model different phenomenon, or combinations thereof (Zhou et al., 1996; Dahleh and Pearson, 1987).

Appendix A. Linear optimal control

Table 1 shows several common cost functions that arise from different system desiderata and different classes of disturbances and measurement errors $\nu := (w, e)$. We recall the power norm,[3] defined as

$$\|\boldsymbol{x}\|_{pow} := \sqrt{\lim_{T\to\infty}\frac{1}{T}\sum_{k=0}^{T}\|x_k\|_2^2}\,.$$

We now recall some examples from linear optimal control in the partially observed setting.

Example 2 (Linear Quadratic Regulator) *Suppose that the cost function is given by*

$$c(\boldsymbol{x}, \boldsymbol{u}) = \mathbb{E}_\nu\left[\lim_{T\to\infty}\frac{1}{T}\sum_{k=0}^{T}x_k^\top Q x_k + u_k^\top R u_k\right],$$

for some user-specified positive definite matrices Q and R, $w_k \overset{i.i.d.}{\sim} \mathcal{N}(0, I)$, $H = I$, and that the controller is given full information about the system, i.e., that $C = I$ and $e_k = 0$ such that the measurement model collapses to $y_k = x_k$. Then the optimal control problem reduces to the familiar Linear Quadratic Regulator (LQR) problem

$$
\begin{aligned}
minimize_{\{\pi\}} \quad & \mathbb{E}_w\left[\lim_{T\to\infty}\frac{1}{T}\sum_{k=0}^{T}x_k^\top Q x_k + u_k^\top R u_k\right] \\
\text{subject to} \quad & x_{k+1} = Ax_k + Bu_k + w_k \\
& u_k = \pi(x_{0:k}),
\end{aligned}
\tag{15}
$$

For stabilizable (A, B), and detectable (A, Q), this problem has a closed-form stabilizing controller based on the solution of the discrete algebraic Riccati equation (DARE) (Zhou et al., 1996). This optimal control policy is linear, and given by

$$u_k^{\text{LQR}} = -(B^\top PB + R)^{-1}B^\top PAx_k =: K_{\text{LQR}}x_k,\tag{16}$$

where P is the positive-definite solution to the DARE defined by (A, B, Q, R).

---

3. The power-norm is a semi-norm on ℓ_∞, as $\|\boldsymbol{x}\|_{pow} = 0$ for all $\boldsymbol{x} \in \ell_2$, and consequently is a norm on the quotient space ℓ_∞/ℓ_2. It can be used to define the $\mathcal{H}_\infty$ system norm (see You and Gattami (2014) and references therein).

Example 3 (Linear Quadratic Gaussian Control) *Suppose that we have the same setup as the previous example, but that now the measurement is instead given by* (4) *for some C such that the pair (A, C) is detectable, and that $e_k \overset{i.i.d.}{\sim} \mathcal{N}(0, I)$. Then the optimal control problem reduces to the Linear Quadratic Gaussian (LQG) control problem, the solution to which is:*

$$u_k^{\text{LQG}} = K_{\text{LQR}}\hat{x}_k, \tag{17}$$

where $\hat{x}_k$ is the Kalman filter estimate of the state at time k. The steady state update rule for the state estimate is given by

$$\hat{x}_{k+1} = A\hat{x}_k + Bu_k + L_{\text{LQG}}(y_{k+1} - C(A\hat{x}_k + Bu_k))$$

for filter gain $L_{\text{LQG}} = -PC^\top (CPC^\top + I)^{-1}$ where P is the solution to the DARE defined by $(A^\top, C^\top, I, I)$. This optimal output feedback controller satisfies the separation principle*, meaning that the optimal controller K_{LQR} is computed independently of the optimal estimator gain L_{LQG}.*

These first two examples are widely known due to the elegance of their closed-form solutions and the simplicity of implementing the optimal controllers. However, this optimality rests on stringent assumptions about the distribution of the disturbance and the measurement noise. We now turn to an example, first introduced in Example 1, for which disturbances are adversarial and the separation principle fails.

Consider a waypoint tracking problem where it is known that both the distances between waypoints and sensor errors are instantaneously ℓ_∞ bounded, and we want to ensure that the system remains within a bounded distance of the waypoints. In this setup, the $\mathcal{L}_1$ optimal control problem is most natural, and our cost function is then

$$c(\boldsymbol{x}, \boldsymbol{u}) = \sup_{\substack{\|r_{k+1} - r_k\|_\infty \leq 1, \\ \|e_k\|_\infty \leq 1, k \geq 0}} \left\| \begin{matrix} Q^{1/2}(x_k - r_k) \\ R^{1/2}u_k \end{matrix} \right\|_\infty,$$

for some user-specified positive definite matrices $Q = \text{diag}\frac{1}{q_i^2}$ and $R = \text{diag}\frac{1}{r_i^2}$. Then if the optimal cost is less than 1, we can guarantee that $|x_{i,k} - r_{i,k}| \leq q_i$ and $|u_{i,k}| \leq r_i$ for all possible realizations of the waypoint and sensor error processes. Considering the one-step lookahead case,[4] we can define the augmented state $\xi_k = [x_k - r_k; r_k]$ and pose the problem with bounded disturbances $w_k = r_{k+1} - r_k$. We can then formulate the following $\mathcal{L}_1$ optimal control problem,

$$
\begin{aligned}
\text{minimize}_{\{\pi\}} \quad & \sup_{\|\nu\|_\infty \leq 1, k \geq 0} \left\| \begin{matrix} \bar{Q}^{1/2}\xi_k \\ R^{1/2}u_k \end{matrix} \right\|_\infty \\
\text{subject to} \quad & \xi_{k+1} = \bar{A}\xi_k + \bar{B}u_k + \bar{H}w_k, \quad y_k = \bar{C}\xi_k + \eta_k \\
& u_k = \pi(y_{0:k}),
\end{aligned}
\tag{18}
$$

where

$$\bar{A} = \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} C & 0 \end{bmatrix}, \quad \bar{H} = \begin{bmatrix} 0 \\ I \end{bmatrix}$$

This optimal control problem is an instance of $\mathcal{L}_1$ robust control (Dahleh and Pearson, 1987). The optimal controller does not obey the separation principle, and as such, there is no clear notion of an estimated state.

---

4. A similar formulation exists for any T-step lookahead of the reference trajectory.

Appendix B. Experimental details

The robust SLS procedure we propose and analyze requires solving a finite dimensional approximation to an infinite dimensional optimization problem, as $\{\boldsymbol{\Phi}_{xw}, \boldsymbol{\Phi}_{xe}, \boldsymbol{\Phi}_{uw}, \boldsymbol{\Phi}_{ue}\}$ and the corresponding constraints (9) and objective function are infinite dimensional objects. As an approximation, we restrict the system responses $\{\boldsymbol{\Phi}_{xw}, \boldsymbol{\Phi}_{xe}, \boldsymbol{\Phi}_{uw}, \boldsymbol{\Phi}_{ue}\}$ to be finite impulse response (FIR) transfer matrices of length $T = 200$, i.e., we enforce that $\boldsymbol{\Phi}(T) = 0$. We then solve the resulting optimization problem with MOSEK under an academic license (ApS, 2019). More explicitly, we define $\mathrm{vec}(\boldsymbol{F}) := \begin{bmatrix} F_0^\top & \ldots & F_{T-1}^\top \end{bmatrix}^\top$ and $\overline{\mathrm{vec}}(\boldsymbol{F}) := \begin{bmatrix} F_0 & \ldots & F_{T-1} \end{bmatrix}$, where F_t are the FIR coefficients of the system responses. We further define

$$\boldsymbol{Z} := \begin{bmatrix} Q^{1/2} & \\ & R^{1/2} \end{bmatrix} \begin{bmatrix} \boldsymbol{\Phi}_{xw} & \boldsymbol{\Phi}_{xe} \\ \boldsymbol{\Phi}_{uw} & \boldsymbol{\Phi}_{ue} \end{bmatrix} \begin{bmatrix} H \\ \gamma I \end{bmatrix}. \tag{19}$$

The SLS constraints (9) and FIR condition are then enforced as

$$\begin{aligned}
&\begin{bmatrix} \overline{\mathrm{vec}}(\boldsymbol{\Phi}_{xw}) & 0 \end{bmatrix} - \begin{bmatrix} 0 & A\overline{\mathrm{vec}}(\boldsymbol{\Phi}_{xw}) \end{bmatrix} = \begin{bmatrix} 0 & B\overline{\mathrm{vec}}(\boldsymbol{\Phi}_{uw}) + \overline{\mathrm{vec}}(\boldsymbol{I}) \end{bmatrix} \\
&\begin{bmatrix} \overline{\mathrm{vec}}(\boldsymbol{\Phi}_{xe}) & 0 \end{bmatrix} - \begin{bmatrix} 0 & A\overline{\mathrm{vec}}(\boldsymbol{\Phi}_{xe}) \end{bmatrix} = \begin{bmatrix} 0 & B\overline{\mathrm{vec}}(\boldsymbol{\Phi}_{ue}) \end{bmatrix} \\
&\begin{bmatrix} \mathrm{vec}(\boldsymbol{\Phi}_{xw}) \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ \mathrm{vec}(\boldsymbol{\Phi}_{xw})A \end{bmatrix} = \begin{bmatrix} 0 \\ \mathrm{vec}(\boldsymbol{\Phi}_{xe})C + \mathrm{vec}(\boldsymbol{I}) \end{bmatrix} \\
&\begin{bmatrix} \mathrm{vec}(\boldsymbol{\Phi}_{uw}) \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ \mathrm{vec}(\boldsymbol{\Phi}_{uw})A \end{bmatrix} = \begin{bmatrix} 0 \\ \mathrm{vec}(\boldsymbol{\Phi}_{ue})C \end{bmatrix} \\
&\boldsymbol{\Phi}_{xw}(T) = 0, \ \boldsymbol{\Phi}_{uw}(T) = 0, \ \boldsymbol{\Phi}_{xe}(T) = 0, \ \boldsymbol{\Phi}_{ue}(T) = 0.
\end{aligned} \tag{20}$$

We then solve the following optimization problem

$$\begin{aligned}
\underset{\boldsymbol{\Phi}}{\mathrm{minimize}} \quad & \mathrm{cost}(\boldsymbol{Z}) \\
\text{subject to} \quad & (20), \ \mathrm{norm}(\boldsymbol{\Phi}_{xe}) \leq \alpha,
\end{aligned}$$

where the $\mathrm{cost}(\cdot)$ and $\mathrm{norm}(\cdot)$ operators are problem dependent.

For the $\mathcal{L}_1$ robust problem, both the cost function and robust norm constraint reduce to the $\ell_\infty \to \ell_\infty$ induced matrix norm for an FIR transfer response $\boldsymbol{F}$ with coefficients in $\mathbb{R}^{n \times m}$,

$$\mathrm{norm}_{\infty \to \infty}(\boldsymbol{F}) = \max_{i=1,\ldots,n} \|\overline{\mathrm{vec}}(\boldsymbol{F})_i\|_1,$$

where $\overline{\mathrm{vec}}(\boldsymbol{F})_i$ denotes the ith row of $\overline{\mathrm{vec}}(\boldsymbol{F})$.

For the robust LQG problem, the cost function reduces to the Frobenius norm for an FIR cost transfer matrix $\boldsymbol{Z}$, i.e.,

$$\mathrm{cost}(\boldsymbol{Z}) = \|\mathrm{vec}(\boldsymbol{Z})\|_F^2 = \sum_{t=0}^{T} \mathrm{Tr} Z_t^\top Z_t.$$

The robustness constraint is the same $\ell_\infty \to \ell_\infty$ induced matrix norm as in the $\mathcal{L}_1$ control problem.