Differentiable Robust LQR Layers

Ngo Anh Vien 1
Gerhard Neumann 2

1 Bosch Center for Artificial Intelligence, Germany
2 Karlsruhe Institute of Technology, Germany

Abstract
This paper proposes a differentiable robust LQR layer for reinforcement learning and imitation learning under model uncertainty and stochastic dynamics. The robust LQR layer can exploit the advantages of robust optimal control and model-free learning. It provides a new type of inductive bias for stochasticity and uncertainty modeling in control systems. In particular, we propose an efficient way to differentiate through a robust LQR optimization program by rewriting it as a convex program (i.e. semi-definite program) of the worst-case cost. Based on recent work on using convex optimization inside neural network layers, we develop a fully differentiable layer for optimizing this worst-case cost, i.e. we compute the derivative of a performance measure w.r.t the model’s unknown parameters, model uncertainty and stochasticity parameters. We demonstrate the proposed method on imitation learning and approximate dynamic programming on stochastic and uncertain domains. The experiment results show that the proposed method can optimize robust policies under uncertain situations, and are able to achieve a significantly better performance than existing methods that do not model uncertainty directly.

1 INTRODUCTION
Combining model-free and model-based reinforcement learning (RL) has recently received much attentions by researchers in the community. While model-free approaches can be easy for training, they suffer from poor sample efficiency and weak generalization and being too task-specific. Therefore they might have limited applicability to real-world physical systems, where long-time running would lead to being unsafe or to break the system. In contrast, model-based approaches are known to be sample-efficient, however when trained on a physical system they often suffer from a similar safety and robustness issues. These issues can possibly mislead the system to breaking states [Amodei et al., 2016]. Model learning and policy optimization are sometimes treated as two separate stages, which is a common approach in dual control, i.e. learning and control [Feldbaum, 1960]. However, they can not fully exploit the advantages of domain knowledge in an end-to-end fashion, i.e. inductive bias of optimal control. Injecting inductive bias of optimal control in end-to-end RL algorithms has recently shown many great successes in terms of sample-efficiency and robustness [Tamar et al., 2016, Silver et al., 2017, Karkus et al., 2017, Farquhar et al., 2018, Hafner et al., 2020]. We follow work using inductive bias of optimal control in end-to-end RL [Amos et al., 2018]. While existing work has not yet included model uncertainty and dynamics stochasticity, modeling uncertainty and perturbation is considered very important for robot learning [Mankowitz et al., 2019]. In this paper, we will propose a differentiable robust linear quadratic regulator (LQR) layer that introduces an inductive bias of robust optimal control. We combine the advantages of model-based robust optimal control and model-free policy learning. Based on recent work on using convex optimization inside neural network layers [Agrawal et al., 2019a], our algorithm differentiates through a robust optimization algorithm, and hence becomes end-to-end trainable without the necessity of unrolling the planning procedure. Specifically, similar to a standard neural network (NN) layer the developed robust optimization layer computes an optimal solution of a robust optimization program as output. This layer can be differentiated through, and integrated into a NN as a differentiable module to achieve an end-to-end task network. The parameters of this layer are parameters used in the parameterization of the dynamics model, uncertainty set, and the distribution of the dynamics stochasticity. Different from existing approaches, our robust LQR layer is able to model stochasticity (stochastic dynamics models), and uncertainty (uncertainty set over models). We will show that we can differentiate through this robust layer by resorting to the Linear Matrix Inequality (LMI) formulation [Boyd et al., 1994]. In particular, we rewrite robust constraints...
as the worst-case cost, and derive an approximation to the objective of the robust control program. The resulting convex semi-definite program can then be differentiated using the differentiable conic program algorithm as introduced recently by Agrawal et al. [Agrawal et al., 2019b].

We will show that on imitation learning under the presence of task uncertainty we can estimate both i) the model parameters, i.e. the cost and dynamics, and also ii) the model uncertainty, i.e. the stochasticity of the dynamics and the model parameter’s uncertainty. The uncertainty might come from environment disturbances or from the expert’s non-stationary model, i.e. where the environment dynamics or the expert’s mental state change.

2 RELATED WORK

Model-free and model-based methods are two common approaches in RL. Model-free approaches are learning direct mappings from raw inputs to actions [Mnih et al., 2013; Lillicrap et al., 2016; Schulman et al., 2015]. Although these approaches might be easy to implement and can make training fast and easy, they have weak generalization ability, are not sample-efficient, and tend to be task-specific [Sun, 2019]. On the other hand, model-based approaches learn an approximate model of the environment dynamics from real interactions, and optimize an optimal policy using fictitious data generated from the learnt dynamics model. There have been efforts to combine the advantages of model-based RL with control theory, where optimal control is used both as domain knowledge embedded in model learning and as a solver for policy optimization, i.e. model predictive control (MPC), linear quadratic regulator (LQR), or differential dynamic programming (DDP) [Levine and Koltun, 2013; Zhang et al., 2016; Nagabandi et al., 2018; Hafner et al., 2019].

Differentiable optimization layer: There has been recent effort in using convex optimization inside neural network layers. Most existing model-based methods propose to integrate unrolling out planning steps into policy networks, i.e. a connection between two layers is defined as coming from a planning step. [Tamar et al., 2016; Karkus et al., 2017; Silver et al., 2017; Oh et al., 2017; Farquhar et al., 2018]. However this rolling procedure makes forward and backward calculations become computationally expensive. There are recent approaches that can handle analytic differentiation of optimization, hence they have more efficient computation. In particular, Mensch et. al. [Mensch and Blondel, 2018] propose a differentiable dynamics programming layer. Otto et al. [2021] propose a differentiable trust region layer that can be integrated directly into TRPO and PPO [Schulman et al., 2015]. A concurrent work by Doni et al. [2020] also proposes to integrate robust control as a custom convex-optimization-based projection layer for generic nonlinear control policy networks. Other work [Amos and Kolter, 2017; Agrawal et al., 2019a] incorporate general convex programs inside deep networks. However it is non-trivial to extend those approaches to incorporate a robust optimal control program within deep policy networks.

Safe reinforcement learning [Garcia and Fernández, 2015] is concerned with how safety should be addressed in learning to control systems. Safety can be defined through risk-averse reward functions [Coraluppi and Marcus, 1999] where high costs are at risk or at undesirable states. Similarly, safe exploration [Schreiter et al., 2015; Achiam et al., 2017] and robust policy search [Mankowitz et al., 2019] guide RL agents to explore the state space while adhering to certain safety constraints while the policy is being optimized. In addition, robust Markov decisions processes (MDPs) [Iyengar, 2005] and robust optimal control [Vandenberghhe et al., 2002; Bemporad and Morari, 1999] consider policy optimization under the presence of uncertainty over the dynamics models and state knowledge. These approaches require an explicit definition of safety, e.g. a risk-averse reward function, or auxiliary cost constraint functions. Alternatively, robust dual control is concerned with simultaneous learning and control subject to uncertainty and stochastic dynamics [Abbasi-Yadkori and Szepesvári, 2011; Weiss and Di Cairano, 2014; Cohen et al., 2018; Dean et al., 2018; 2019]. These algorithms are able to offer a differentiable objective for policy optimization and model estimation, however they cannot perform full end-to-end learning, i.e. the possibility of being integrated into a fully differentiable task network.

3 BACKGROUND

In this paper, we are concerned with the robust infinite-horizon linear-quadratic-Gaussian (LQG) control problem under ellipsoidal uncertainty,

\[
\pi^* = \arg \min_{\pi \in \mathcal{P}} \sum_{t=0}^{\infty} \left( x_t^T Q x_t + u_t^T R u_t \right),
\]

s.t. \( x_{t+1} = A x_t + B u_t + w_t \)

\( w_t \sim \mathcal{N}(0, \sigma^2 I_n), \quad x_0 \sim P_0 \)

\( [A, B] \in [A, B : (X^T - \mu)^T D (X^T - \mu) \leq 1] \),

where \( x_t \in \mathbb{R}^n, u_t \in \mathbb{R}^m, A \in \mathbb{R}^{n \times n}, B \in \mathbb{R}^{n \times m}, I_n, I_m \) are \( n \times n \) and \( (m+n) \times (m+n) \) identity matrices, respectively. We denote \( X = [A, B] \) a concatenated vector of \( A \) and \( B \); \( P_0 \) denotes an initial state distribution. The random variable \( w_t \) denotes the noise of the stochastic dynamics, which is assumed to follow a Gaussian distribution \( \mathcal{N}(0, \sigma^2 I_n) \), where \( \sigma \in \mathbb{R} \). \( Q \in \mathbb{R}^{n \times n}, R \in \mathbb{R}^{m \times m} \) are positive definite matrices which model the quadratic costs. In addition, we assume the model parameter uncertainty is described by an ellipsoidal uncertainty that is parameterized by a nominal model \( \mu = [\bar{A}, \bar{B}] \) and a symmetric positive definite matrix \( D \).
3.1 DIFFERENTIABLE LQR

Recently there has been significant effort in using differentiable programs as a neural network layer, e.g. optimization layers [Agrawal et al., 2019a], differentiable ODE solvers [Chen et al., 2018], MPC-based policy layers [Amos et al., 2018]. Amos et al. [Amos et al., 2018] propose an algorithm that can differentiate through a policy that is represented by a LQR and MPC. In particular, Amos et al. [Amos et al., 2018] use a discrete-time finite-horizon LQR (with a formulation similar to [1]) with a finite time horizon and without uncertainty and stochasticity, i.e. without the last two inequality constraints) as a learnable module with trainable parameters \( \theta = \{A, B, Q, R\} \). The differentiation is made through the fixed-point solution \( \tau^* = \{x^*_t, u^*_t\}_{t=1:T} \) of the LQR problem. The fixed-point solution can be found using the iterative method (involving a forward and a backward recursion). The main challenge is to compute the derivative \( \partial l / \partial \theta \) of a generic loss function \( l(\tau^*) \) w.r.t the parameters \( \theta \) of the LQR-based policy. This derivative can be written as \( \partial l / \partial \theta = \frac{\partial l}{\partial \tau^*} \frac{\partial \tau^*}{\partial \theta} \). Then the authors suggested to compute the derivatives and differentiation through the constrained convex quadratic LQR problem at the fixed point by applying the implicit function theorem [Dontchev and Rockafellar, 2009]. The implicit mapping between \( \tau^* \) and \( \theta \) is expressed as the zero of the partial derivative of the Lagrange function \( \nabla_{\tau, \lambda} \mathcal{L}(\tau^*, \lambda^*) = 0 \), where \( \mathcal{L} \) is the Lagrange function of the constrained optimization problem Eq. [1] and can be written as follows

\[
\mathcal{L}(\tau, \lambda) = \sum_{t=1}^{T} (x^*_t^\top Q x_t + u^*_t^\top R u_t) + \sum_{t=0}^{T-1} \lambda_t^\top (Ax_t + Bu_t - x_{t+1}),
\]

where \( T \) is the length of the time horizon, and \( \lambda = \{\lambda_t\}_{t=0}^{T-1} \) with \( \lambda_t \in \mathbb{R}^n \) being a Langrange multiplier at time \( t \).

This LQR control layer can also be extended to become a differentiable MPC-based control layer by differentiating the convex approximation at a fixed point of the iterative approximation procedure, i.e. an iterative linearization of the dynamics and second-order Taylor approximation of the cost. Finite-horizon LQR-based policies are open-loop, therefore stability is not guaranteed [Bitmead and Gevers, 1991]. This problem could be mitigated through the online open-loop MPC-based extension [Amos et al., 2018].

However, it is non-trivial to extend this approach to obtain a differentiable robust control layer that would require to model stochastic dynamics and/or model uncertainty. A differentiable robust control layer with a robust optimal control inductive bias is expected to better model the underlying problem, hence will improve the robustness of learnt policies. For example, demonstration data can be generated by a stochastic process with an uncertain model, as shown in Eq. [1]. In addition, both the forward and backward recursion used by Amos et al. [Amos et al., 2018] based on the constrained convex quadratic program formulation will suffer from a poor convergence and high computation when the horizon \( T \) increases.

3.2 LQR AND LINEAR MATRIX INEQUALITIES

In the case of deterministic dynamics and without uncertainty, the problem in Eq. [1] becomes an infinite-horizon LQR control problem with a standard formulation as follows

\[
\pi^* = \arg \min_{\pi} \sum_{t=0}^{\infty} (x_t^\top Q x_t + u_t^\top R u_t)
\]

\[
\text{s.t. } x_{t+1} = Ax_t + Bu_t, \quad x_0 = x_{\text{init}},
\]

Its optimal controller is state-feedback, \( u_t = K x_t \), with \( K = -(B^\top P B + R)^{-1} B^\top PA \), where \( P \) is a positive definite matrix and can be computed by solving the Algebraic Riccati Equation (ARE) [Camacho and Alba, 2013].

\[
P = A^\top PA + Q - A^\top P B (B^\top P B + R)^{-1} B^\top PA.
\]

A solution for \( P \) can be found using iterative methods [Hewer, 1971] (backward recursion) or by a convex SDP formulation through the use of Linear Matrix Inequalities (LMI) [Boyd et al., 1994, Balakrishnan and Vandenberghe, 2003]. The SDP formulation can be done via by assuming the ARE to be a Lyapunov-inequality. The objective is to minimize the trace of \( P \),

\[
\max_{P} \text{trace}(P)
\]

\[
\text{s.t. } \begin{bmatrix} R + B^\top P B & B^\top PA & 0 \\ A^\top P B & A^\top PA + Q - P & 0 \\ 0 & 0 & P \end{bmatrix} \succeq 0,
\]

where \( P \) is symmetric positive definite: \( P \succeq 0, P = P^\top \).

Stability of infinite-horizon LQR has been extensively studied in optimal control [Kalman et al., 1960]. It has been shown via the Lyapunov analysis that LQR is robust to uncertainty in the model parameters (e.g. the \( A \) and \( B \) matrices) and to perturbations (e.g. the noise \( w \)) under certain conditions, i.e. the bounds on the uncertainty. In other words, as long as the uncertainty and perturbations are small enough the solution to the LMI constraint problem could exist and could stabilize the controller. We will show that such a limited guarantee is not sufficient if the uncertainty level increases. A higher uncertainty would increase the divergence possibility and result in a higher task cost.

4 DIFFERENTIABLE ROBUST LQG

We now propose a family of robust LQR-based policies that is based on the robust discrete time-invariant LQG problem in Eq. [1]. We consider a differentiable robust LQR program in the infinite-horizon setting. One of the main technical challenges is how to differentiate through such a program
with an unbounded dimensionality and uncertain constraints. To tackle this challenge, we will exploit the LMI techniques which are used commonly in optimal control. In particular, rewriting the objective and constraints using LMI techniques would take advantages of robust optimal control and convex optimization. The robust LQR problem’s solution can be found by solving a (convex) SDP. This SDP can be solved and differentiated through using the technique developed by Agrawal et al. [Agrawal et al., 2019a], called differentiable convex optimization layers. We will discuss how to make this SDP disciplined parameterized optimization (DPP) compliant so that it can be differentiated through.

4.1 DIFFERENTIABLE INFINITE-HORIZON LQR

This section starts with the LMI formulation in Eq. 1 for the robust LQR-based policy whose output is the solution to the LQR problem as written in Eq. 2. We term this approach as our first contribution, LMI-LQR layer, which is considered as an alternative solution for the dynamic Riccati recursion solver used in the differentiable LQR approach described in [3.1]. The LMI-based LQR layer provides the solution of the SDP program in Eq. 1 as output. This LQR-based policy module is parameterized by parameters \( \theta = \{A, B, Q, R\} \). In order for learning with this policy to be end-to-end differentiable, we need an efficient method to compute the derivatives, \( \partial \pi^*/\partial \theta \), of the output policy \( \pi^* \) w.r.t the parameters \( \theta \). The SDP program in Eq. 1 can be solved using standard convex optimization tools, however it can only be differentiated through efficiently if its constraints and objectives are affine mappings of the problem data (e.g. \( \theta \)) [Agrawal et al., 2019b], i.e. to be DPP-compliant for general differentiable convex optimization layers [Agrawal et al., 2019a]. In this paper, we resort to the differentiable convex optimization layers as a differentiation technique, with the introduction of two auxiliary variables \( S1, S2 \), subject to the additional constraints \( S1 = PB, S2 = PA \) in order to make the SDP program in Eq. 1 to be DPP-compliant.

The above LMI-based LQR layer cannot directly model uncertainty. Thus this approach will only work well if the uncertainty is small enough. In next section, we will propose a new approach that directly models uncertainty by means of the parameters \( \{D, \sigma\} \).

4.2 DIFFERENTIABLE ROBUST INFINITE-HORIZON LQR

We now want to explicitly represent the uncertainty and perturbations and learn these terms. As a first step we focus on the dynamics alone by assuming that there is uncertainty about \( X = [A, B] \). We denote the uncertainty set as \( \Theta = \{X : (X^\top - \mu)^\top D(X^\top - \mu) \leq I\} \), where \( \mu = [\bar{A}, \bar{B}] \) are the nominal parameters. Thus, the robust LQR-based policy module has parameters \( \theta = \{\bar{A}, \bar{B}, Q, R, D, \sigma\} \). We now discuss how to rewrite our robust problem so that its derivatives w.r.t \( \theta \) can be computed efficiently. We follow similar derivations like the system level synthesis framework for \( \mathcal{H}_\infty \) optimal control studied by Anderson et al. [Anderson et al., 2019], which is recently used in the robust RL framework by Umenberger et al. [Umenberger et al., 2019]. The robust LQR objective can be rewritten as a worst-case problem,

\[
J(\theta, K) = \min_{K} E \left[ \sup_{\theta \in \Theta} \lim_{T \to \infty} \sum_{t=0}^{T} c(x_t, u_t) \right],
\]

s.t. the linear time-invariant dynamics

\[
x_{t+1} = Ax_t + Bu_t + w_t, w_t \sim \mathcal{N}(0, \sigma^2 I), x_0 = x\text{init}.
\]

Assuming the policy parameterization \( u_t = Kx_t \). We can rewrite the infinite horizon cost as

\[
J(\theta, K) = \lim_{T \to \infty} \frac{1}{T} E \left[ \sum_{t=0}^{T} (x_t^\top Qx_t + u_t^\top Ru_t) \right]
\]

\[
= \text{trace} \left( \left[ \begin{array}{cc} Q & 0 \\ 0 & R \end{array} \right] \frac{1}{T} \sum_{t=1}^{T} E \left[ \begin{array}{c} x_t \\ u_t \end{array} \right] \right)
\]

\[
= \text{trace} \left( \left[ \begin{array}{cc} Q & 0 \\ 0 & R \end{array} \right] \frac{1}{T} \sum_{t=1}^{T} E \left[ \begin{array}{c} x_t Kx_t \\ x_t \end{array} \right] \right)
\]

where we denote \( W = E [x_t x_t^\top] \), the stationary state covariance. Given certain \( A \) and \( B \), \( W \) can be found by solving the following optimization problem,

\[
\arg \min_{W} \text{trace}(W), \quad \text{s.t. } W \succeq (A + BK)W(A + BK)^\top + \sigma^2 I.
\]

If we assume that the policy has only parameters \( K \), we receive a semidefinite program (SDP), which is convex. However, in the case of uncertain \( \{A, B\} \), solving the above program is very challenging [El Ghaoui et al., 1998].

We will now reformulate it by resorting to a worst-case scenario. Using similar notations used as by Umenberger et al. [Umenberger et al., 2019]. We denote \( Z = WK^\top \), \( Y = KWK^\top \), and

\[
\Xi = \left[ \begin{array}{cc} W & Z \\ Z^\top & Y \end{array} \right].
\]

The non-convex semidefinite constraint in Eq. 5 can be rewritten as a convex one as

\[
W \succeq \Xi \Xi^\top + \sigma^2 I.
\]
where according to the the Schur complement, it can be further rewritten as
\[
\begin{bmatrix}
I & \sigma I \\
\sigma I & W - XE X^T
\end{bmatrix} \succeq 0.
\]

The second challenge of the uncertain parameters can be handled through the use of the worst-case formulation as
\[
\min_W \left( \begin{bmatrix} Q & 0 \\ 0 & R \end{bmatrix} \Xi \right)
\text{s.t.} \ \begin{bmatrix}
I & \sigma I \\
\sigma I & W - XE X^T
\end{bmatrix} \succeq 0,
(8)
\]

where \(\Xi\) is defined in Eq. \ref{eq:xi}. In order to further rewrite the uncertain constraints in Eq. \ref{eq:xi}, we follow similar derivations from [Umenberger et al., 2019; Luo et al., 2004]. We use the following Theorem from [Luo et al., 2004] (Theorem 3.7).

**Theorem 1** The data matrices \((A, B, C, D, \bar{F}, \bar{G}, H)\) satisfy the robust fractional quadratic matrix inequalities
\[
\begin{bmatrix}
\bar{H} & \bar{F} \\
\bar{F}^\top & C + X^\top B + B^\top X + X^\top A X
\end{bmatrix} \succeq 0,
\forall X
\]
\[
\text{such that } I - X^\top H X \succeq 0,
\]

if and only if there is \(\lambda \geq 0\) such that
\[
\begin{bmatrix}
\bar{H} & \bar{F} \\
\bar{F}^\top & C - \lambda I + B^\top A X
\end{bmatrix} \succeq 0.
\]

We use substitutions similar to the one in [Umenberger et al., 2019]: \(A = -\Xi, \bar{B} = \Xi [\bar{A}, \bar{B}]^\top, C = W - [\bar{A}, \bar{B}] \Xi [\bar{A}, \bar{B}]^\top, \bar{D} = D, \bar{F} = \sigma I, \bar{G} = 0, H = I\). In addition, we substitute \(X = X - \mu\) with the definition of \(X = [\bar{A}, \bar{B}] - X\).

As a final result of the substitutions, we receive the program in Eq. \ref{eq:xi} as a SDP,
\[
\min_{\lambda} \left( \begin{bmatrix} Q & 0 \\ 0 & R \end{bmatrix} \Xi \right)
\text{s.t.} \ \begin{bmatrix}
I & \sigma I \\
\sigma I & W - [\bar{A}, \bar{B}] \Xi [\bar{A}, \bar{B}]^\top \\
0 & \Xi [\bar{A}, \bar{B}]^\top \\
0 & \lambda D - \Xi
\end{bmatrix} \succeq 0, \lambda \geq 0,
(9)
\]

Solving the above cone program, we receive the optimal \(W\), that helps to reconstruct the policy as \(K = Z^TW^{-1}\). We are interested in computing the derivative:
\[
\frac{\partial l}{\partial \theta} = \frac{\partial l}{\partial K} \frac{\partial K}{\partial W} \frac{\partial W}{\partial \theta}
(10)
\]
where \(\theta = [\bar{A}, \bar{B}, Q, R, D, \sigma]\) are the robust LQR’s parameters. The scalar function \(l\) is the task objective depending on the policy (parameterized by \(K\), i.e. imitation learning cost. The middle part in R.H.S can be computed easily, according to the definition of the resulting policy where \(W\) is the optimal solution of the SDP problem. The last derivative can be computed by differentiating through a cone program, for which we can utilize the general approach proposed in a recent work by Agrawal et. al. [Agrawal et al., 2019], differentiating through a cone program. Our practical implementation needs the introduction of an auxiliary variable \(S\), with an additional constraint \(S = \Xi [\bar{A}, \bar{B}]\). An extension to modeling also the uncertainty \(Q\) and \(R\) is simple, which has little intuition so we do not consider in this work.

5 EXPERIMENTS

In this section, we evaluate the differentiable robust LQR layers, i.e. the LMI-based LQR (LMI-LQR) and LMI-based robust LQR (LMI-Robust-LQR) layers proposed in [4.1 and 4.2] in terms of their performance and uncertainty handling capabilities in comparisons to other baseline methods. Our main contender is the differentiable LQR framework (mpc.pytorch) [Amos et al., 2018]. Both LMI-LQR and mpc.pytorch can be considered as a solver for the nominal system. Our implementation is based on PyTorch and uses cvxpylayers [Agrawal et al., 2019a] as the main differentiable solver for both LMI-LQR and LMI-Robust-LQR layers (where a SCS cone programming solver (O’Donoghue et al., 2016) is chosen by default).

5.1 IMITATION LEARNING ON ROBUST LQR

In this section we design a robust LQR task with dynamics as defined in Eq. \ref{eq:dim}. The expert is parameterized with a robust LQR controller. This assumption also reflects the reality since under many uncertain scenarios in nature human behavior following to some worst-case strategies [Lipsitz and Strauss, 1997]. Three learners are mpc.pytorch, LMI-LQR, and LMI-Robust-LQR with different parameterization. We assume that the quadratic costs \(Q = R = I\), state and control dimensions \(n = 3, m = 3\) and the variance of the noise \(\sigma = 0.1\) are known to the learners. The learners are supposed to learn the the parameters \(\bar{A} and \bar{B}\) of the linear system dynamics and the model uncertainty \(D\). Note that mpc.pytorch and LMI-LQR can not learn \(D\). The experts are generated from random \(\bar{A}, \bar{B}, D\) (where we additionally control their stability), depending on a random seed. All algorithms use the same initialization for \(\bar{A}, \bar{B}\). All algorithms are implemented using PyTorch with the following settings: RMSprop optimizer (momentum = 0.5, learning rate = 0.01), a minibatch of 16 trajectories. Given demonstration data \(D = \{\tau^j\}_{j=1}^N\), all algorithms use a similar imitation objective for training, \(L = \frac{1}{N} \sum_{\tau^j} \|\tau^j - \tau\|^2\).

For validation, we generate separate \(N = 32\) trajectories \(\tau^j\) using the expert’s robust LQR policy. Each generated
trajectory $\tau_i$ is conditioned on only an initial state $x_i^0$ that initiated the expert trajectory $\tau_i$. The model loss is defined as a $L_2$ norm of the difference between the estimate vs. the ground-truth: e.g. $\hat{A}, \hat{B}$ vs. $\hat{A}^*, \hat{B}^*$ (scenario 1), or $D$ vs. $D^*$ (scenario 2). This loss is used only for reporting, which measures how the model-based module works based purely on a model-free loss (the imitation loss). The validation cost is obtained by running optimized controllers on the true stochastic dynamics and a known uncertainty set.

All results are averaged over ten random seeds. Experiments are run on an Intel i7 CPU (2.6Ghz, 12 core).

Scenario 1: Known $\hat{A}, \hat{B}$, unknown model uncertainty $D$
In this scenario only $D$ has to be learned. Since the differentiable LQR framework [Amos et al., 2018] and LMI-based LQR layer do not have uncertainty modeling, they do not require training. On the other hand, we train LMI-based robust LQR for 200 iterations to optimize the imitation loss w.r.t parameter $D$, where we assume both the true $D^*$ and $D$ are diagonal. We first evaluate the solving time of different algorithms. Table 1 shows the total computation time (forward passes) of three algorithms on different horizon lengths. The results show that our differentiable infinite-horizon (robust) LQR layer is more computationally efficient by a factor of the horizon length.

Table 2 (1st row: S1) shows the performance comparison of optimal controllers found by the three algorithms in terms of the validation cost. Only the LMI-based robust LQR layer algorithm requires training, so the performance of the final controller at convergence is reported. This result shows that mpc.pytorch performs poorly because it is not optimizing a controller that can be robust under uncertainty. On contrary, the differentiable LMI-based LQR layer method which incorporates robust control constraints via a LMI formulation performs much better. This shows the benefit of using a robust control constraint to stabilize the optimized controller as output. As this simple approach does not model uncertainty directly, therefore it can only stabilize the output controller within small bounded perturbations. In this experiment, the environment uncertainty is set to a high value, therefore we can see in Table 2 (1st row: S1) the performance of LMI-LQR is not optimal. This drawback is addressed by the LMI-based robust LQR layer method where its validation cost is significantly better than mpc.pytorch and LMI-LQR. This performance level is equal to the optimal cost received by running an optimal worse-case policy found on the true model. The plots of the model and imitation losses are reported in Figure 1. Similar to findings in mpc.pytorch [Amos et al., 2018], the imitation loss might converge to a local optima, while there are possible divergences of the model loss. This shows the challenges of optimizing a highly non-linear layer in which its weights are from parameters of an optimal control program.

| Time horizon | 10   | 50   | 100  |
|--------------|------|------|------|
| mpc.pytorch  | 1.67 | 0.99 | 0.99 |
| LMI-LQR      | 1.67 | 1.67 | 1.67 |
| LMI-Robust-LQR | 1.67 | 1.67 | 1.67 |

Figure 1: Model and imitation losses for 10 different runs (each plot corresponds to one run).

Scenario 2: Known uncertainty $D$, unknown model $\hat{A}, \hat{B}$
In this scenario, we evaluate the performance of the different algorithms on imitation learning, where $D$ is known and $\hat{A}, \hat{B}$ are supposed to be learnt. All algorithms are initialized randomly with the same stable $A, B$, with a horizon length of 20. Figure 2 shows the imitation and model losses of mpc.pytorch (right), LMI-LQR (middle), LMI-Robust-LQR (left). While the model losses may not be suitable to assess the performance of three differentiable layers (a similar observation was made in [Amos et al., 2018]), the imitation losses can reflect the actual quality of the controls, which are generated by these layers. The results show that mpc.pytorch converges only to a local optima that still has a large imitation loss. While LMI-LQR can achieve an optimal imitation loss, its optimized controller is not robust enough as reflected by its validation cost in Table 1 (2nd row: S1). LMI-Robust-LQR leads to controller that is more robust because it has an ability to learn model uncertainties.

5.2 Convex Approximate Dynamic Programming

In this section, we evaluate our methods with full functionalities, i.e. we differentiate and learn all parameters:

Table 2: Validation cost evaluated on the true dynamics, with a horizon set to 50. Both the mean cost and its standard deviation over 10 different runs are reported.

|                | mpc.pytorch | LMI-LQR | LMI-Robust-LQR |
|----------------|-------------|---------|----------------|
| S1             | 44.1 ± 1.6  | 41.2 ± 1.4 | 10.9 ± 0.5     |
| S2             | 124.5 ± 10.2 | 67.4 ± 18.7 | 11.8 ± 2.3     |
\{A, B, Q, R\} in LMI-LQR layer and \{Ã, B̅, Q̅, R̅, D, σ\} in LMI-Robust-LQR. For this purpose, we evaluate the proposed algorithms on an uncertain stochastic optimal control (SOC) problem,

\[
\min_{\theta} \lim_{T \to \infty} \mathbb{E}\left[\frac{1}{T} \sum_{t=0}^{T-1} \|x_t\|_2^2 + \|u_t\|_2^2\right]
\]

s.t. \[x_{t+1} = Ax_t + Bu_t + w_t\]
\[w_t \sim \mathcal{N}(0, \sigma^2 I), \quad x_0 \sim P_0,\]
\[\{A, B\} \in \{A, B : (X^T - \mu)^T D (X^T - \mu) \leq 1\}\]

where \(X\) denotes \([A, B]\), and \(\mu = [A, B]\). This problem introduces an uncertainty set \(D\) over model parameters \(A, B\), which is different from a similar problem for a nominal dynamic system considered by Agrawal et al. \[\text{Agrawal et al., 2019a}\]. We evaluate three different policy parameterization that are all based on the Lyapunov stability theory \[\text{Boyd et al., 1994}\], and three simple baselines that do not have optimal control base.

**Simple baselines** We use three baseline methods that do not use differentiable optimal control layers, denoted as \(u = f_0(x)\): (1) a linear controller \(u = Kx\), where \(\theta = K\) is a parameterized feedback gain matrix; 2) \(f_0\) is a multilayer perceptron (MLP) with two hidden layers of shape (32,32) using ReLU activations; and 3) \(f_0\) is a long-short term memory network (LSTM) (a recurrent controller) with one 64-unit hidden layer. All three baselines use the Adam optimizer with a step-size \(\alpha = 1e^{-4}\).

**Optimal control-based policies** Besides our two proposals LMI-LQR, LMI-Robust-LQR, the next baseline is an approximate dynamic programming policy (ADP) from \[\text{Agrawal et al., 2019a}\]. They proposed to use a quadratic control-Lyapunov policy as output of a differentiable convex layer. This convex layer is designed to solve the following second-order cone program (SOCP) subject to a constraint of bounded controls,

\[
\min_{u} \ u^T P u + x_0^T Q u + q^T u \quad \text{s.t.} \quad \|u\| \leq 1
\]

This SOCP policy receives \(u\) as variable, and \(\{P, Q, q, x_0\}\) as parameters. Using a differentiable convex layer \[\text{Agrawal et al., 2019a}\], we can differentiate through the program in Eq. 11. As an alternative approach, our two proposed differentiable LQR layers are based on the Lyapunov inequality where we parameterize the policy directly, \(\pi\) is the optimal solution of the program defined in Eq. 11. Our differentiable layers receive \(K\) (as defined in Section 4.1) as variable (where \(T\) is the horizon length), and \(\{A, B, Q, R\}\) (for LMI-LQR layer) and \(\{\bar{A}, \bar{B}, Q, R, D, \sigma\}\) (for LMI-Robust-LQR) as parameters. Note that both the LMI-LQR layer and the SOCP policy cannot model the uncertainty set directly, hence they are just solvers for a nominal system (without uncertainty).

We use state and action dimensions \(n = m = 3\), a time horizon of \(T = 20\), a batch size of 64 randomly initial states, and run for 200 update iterations. We randomize different SOC problems in Eq. 11, the dynamics model \(\bar{A}, \bar{B}\) are initialized with Lyapunov-stable matrices, a random diagonal matrix \(D\) with diagonal entries, and a fixed noise variance \(\sigma = 0.1\). All algorithms use the same RMSprop optimizer with their optimized learning rate and decay rate, i.e. using grid-search. The parameters of the SOCP policy are initialized as in the original paper of Agrawal et al. \[\text{Agrawal et al., 2019a}\] where \(\{P, Q, q\}\) are initialized with the exact
The third baseline using LSTM is known to learn better variance for the stochastic dynamics.\footnote{The LSTM output is not reported in the plots. Its evaluated cost (the objective in Eq. 12) always returns nan or $\infty$. The second baseline using MLP may solve the task with a horizon of 20, but shows a very unstable behavior due to fluctuated cost evaluations, i.e. spikes as seen on the plots. As a result, it is not surprising that it becomes diverging when the horizon increases to 100 (we also design this long horizon task with a higher dynamics stochasticity $\sigma = 0.5$), hence not reported in the (right) plot. The third baseline using LSTM is known to learn better for tasks under uncertainty, e.g. POMDP. However on this challenging robust control task, it performs worse than our proposed methods in terms of sample-efficiency and the final task cost.\footnote{As the time horizon increases, the effect of uncertain model and stochastic dynamics can lead the system to instability. We rerun all three algorithms for 1000 training iterations. All trials using the SOCP policy return numerical errors within few iterations (so no plots are reported for the SOCP policy). The validation costs for LMI-LQR and LMI-Robust-LQR are reported in Fig. \ref{fig:results}(right). The results show that there is an extreme effect of uncertainty and stochasticity to training. While LMI-LQR seems to gradually attenuate the effect of perturbations, it might take the training very long to achieve a stable result. In contrary, LMI-Robust-LQR reduces the effect of uncertainty well. Its final controller is less fluctuating and starts becoming stable.}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig3.png}
\caption{Average cost for robust SOC with a horizon of 20 (left and center), and 100 (right). The plot of the SOCP policy is separated due to its large domain. The shading is the standard deviation of the mean estimator.}
\end{figure}

\textbf{Results} Figure \ref{fig:results} reports the average cost optimized by each algorithm. While the first simple baseline diverges on both tasks with a horizon of 20 and 100, hence they are not reported in the plots. Its evaluated cost (the objective in Eq. 12) always returns nan or $\infty$. The second baseline using MLP may solve the task with a horizon of 20, but shows a very unstable behavior due to fluctuated cost evaluations, i.e. spikes as seen on the plots. As a result, it is not surprising that it becomes diverging when the horizon increases to 100 (we also design this long horizon task with a higher dynamics stochasticity $\sigma = 0.5$), hence not reported in the (right) plot. The third baseline using LSTM is known to learn better for tasks under uncertainty, e.g. POMDP. However on this challenging robust control task, it performs worse than our proposed methods in terms of sample-efficiency and the final task cost. The main reason is that LSTM is a general neural network that can not exploit the inherent structure of the task, i.e. uncertainty constraints like in our method. This is further demonstrated on the right plot for the task with a horizon of 100 in which the LSTM controller is very unstable (in this task we set a longer horizon and a higher variance for the stochastic dynamics).

The results also show that directly incorporating robust constraints in LMI-LQR and LMI-Robust-LQR in the layer, i.e. via the Lyapunov inequality, helps achieve much lower cost. The SOCP policy can only converge to an inferior local policy that incurs a very high cost. A direct principled uncertainty modeling like in LMI-Robust-LQR achieves the best overall performance. In addition, we observe that the total training time of one trial for each algorithm on a personal workstation with a modern CPU is 1-2 hours for SCOP policy, 20-30 minutes for LMI-LQR, and 30-45 minutes for LMI-Robust-LQR. This running time increases approximately linearly with respect to the time horizon.

As the time horizon increases, the effect of uncertain model and stochastic dynamics can lead the system to instability. We rerun all three algorithms for 1000 training iterations. All trials using the SOCP policy return numerical errors within few iterations (so no plots are reported for the SOCP policy). The validation costs for LMI-LQR and LMI-Robust-LQR are reported in Fig. \ref{fig:results}(right). The results show that there is an extreme effect of uncertainty and stochasticity to training. While LMI-LQR seems to gradually attenuate the effect of perturbations, it might take the training very long to achieve a stable result. In contrary, LMI-Robust-LQR reduces the effect of uncertainty well. Its final controller is less fluctuating and starts becoming stable.

\section{Conclusion}

This paper proposes a new differentiable optimal control-based layer. Our approach is motivated by recent work on using convex optimization inside neural network layers. We directly use a robust optimal control optimization program as a differentiable layer that can be incorporated in standard end-to-end neural networks. Our main contribution, which differentiates our work from the current state-of-the-art, is to model uncertainty and stochasticity directly inside a differentiable optimal control layer. As a result, our proposed optimal control layers can optimize a controller as output that is stable and robust to perturbations and noises residing in demonstration data. Our layer can be integrated as a differentiable controller in reinforcement learning and learning from demonstration on tasks where uncertainty and perturbations are present.

Using an infinite-horizon LQR setting has helped accelerate the computation time of both forward and backward passes significantly. This important achievement would open a variety of more applications for the differentiable LQR/MPC layers, for example on practical robotics tasks or hybrid model-based and model-free policy optimization. One main drawback of this setting is that the output is a linear controller that will have limitations on highly non-linear control tasks. One potential research direction can look at extend-
ing to robust time-dependent and finite-horizon settings for either LQR or MPC control theory.

Acknowledgements

Briefly acknowledge people and organizations here. All acknowledgements go in this section.

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.

Joshua Achiam, David Held, Aviv Tamar, and Pieter Abbeel. Constrained policy optimization. arXiv preprint arXiv:1705.10528, 2017.

Akshay Agrawal, Brandon Amos, Shane Barratt, Stephen Boyd, Steven Diamond, and J Zico Kolter. Differentiable convex optimization layers. In Advances in Neural Information Processing Systems, pages 9558–9570, 2019a.

Akshay Agrawal, Shane Barratt, Stephen Boyd, Enzo Busseti, and Walaa M Moursi. Differentiating through a conic program. arXiv preprint arXiv:1904.09043, 2019b.

Dario Amodei, Chris Olah, Jacob Steinhardt, Paul Christiano, John Schulman, and Dan Mané. Concrete problems in ai safety. arXiv preprint arXiv:1606.06565, 2016.

Brandon Amos and J Zico Kolter. Optnet: Differentiable optimization as a layer in neural networks. In Proceedings of the 34th International Conference on Machine Learning-Volume 70, pages 136–145. JMLR. org, 2017.

Brandon Amos, Ivan Dario Jimenez Rodriguez, Jacob Sacks, Byron Boots, and J. Zico Kolter. Differentiable MPC for end-to-end planning and control. In Advances in Neural Information Processing Systems 31, pages 8299–8310, 2018.

James Anderson, John C Doyle, Steven H Low, and Nikolai Matni. System level synthesis. Annual Reviews in Control, 47:364–393, 2019.

Venkataramanan Balakrishnan and Lieven Vandenberghe. Semidefinite programming duality and linear time-invariant systems. IEEE Transactions on Automatic Control, 48(1):30–41, 2003.

Alberto Bemporad and Manfred Morari. Robust model predictive control: A survey. In Robustness in identification and control, pages 207–226. Springer, 1999.

Robert R Bitmead and Michel Gevers. Riccati difference and differential equations: Convergence, monotonicity and stability. In The Riccati Equation, pages 263–291. Springer, 1991.

Stephen Boyd, Laurent El Ghaoui, Eric Feron, and Venkataramanan Balakrishnan. Linear matrix inequalities in system and control theory. SIAM, 1994.

Eduardo F Camacho and Carlos Bordons Alba. Model predictive control. Springer Science & Business Media, 2013.

Ricky TQ Chen, Yulia Rubanova, Jesse Bettencourt, and David K Duvenaud. Neural ordinary differential equations. In Advances in neural information processing systems, pages 6571–6583, 2018.

Alon Cohen, Avinatan Hassidim, Tomer Koren, Nevena Lazic, Yishay Mansour, and Kunal Talwar. Online linear quadratic control. arXiv preprint arXiv:1806.07104, 2018.

Stefano P Coraluppi and Steven I Marcus. Risk-sensitive and minimax control of discrete-time, finite-state markov decision processes. Automatica, 35(2):301–309, 1999.

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 31, pages 4192–4201, 2018.

Sarah Dean, Stephen Tu, Nikolai Matni, and Benjamin Recht. Safely learning to control the constrained linear quadratic regulator. In 2019 American Control Conference (ACC), pages 5582–5588. IEEE, 2019.

Asen L Dontchev and R Tyrrell Rockafellar. Implicit functions and solution mappings, volume 543. Springer, 2009.

Priya L. Donti, Melrose Roderick, Mahyar Fazlyab, and J. Zico Kolter. Enforcing robust control guarantees within neural network policies. CoRR, abs/2011.08105, 2020. URL https://arxiv.org/abs/2011.08105.

Laurent El Ghaoui, Francois Oustry, and Hervé Lebret. Robust solutions to uncertain semidefinite programs. SIAM Journal on Optimization, 9(1):33–52, 1998.

Gregory Farquhar, Tim Rocktäschel, Maximilian Igl, and Shimon Whiteson. Treenq and atreec: Differentiable tree-structured models for deep reinforcement learning. In 6th International Conference on Learning Representations, ICLR. OpenReview.net, 2018.

AA Feldbaum. Dual control theory. I. Avtomatika i Telemekhanika, 21(9):1240–1249, 1960.
Javier García and Fernando Fernández. A comprehensive survey on safe reinforcement learning. *Journal of Machine Learning Research*, 16(1):1437–1480, 2015.

Danijar Hafner, Timothy Lillicrap, Ian Fischer, Ruben Villegas, David Ha, Honglak Lee, and James Davidson. Learning latent dynamics for planning from pixels. In *International Conference on Machine Learning*, pages 2555–2565, 2019.

Danijar Hafner, Timothy P. Lillicrap, Jimmy Ba, and Mohammad Norouzi. Dream to control: Learning behaviors by latent imagination. In *8th International Conference on Learning Representations, ICLR*. OpenReview.net, 2020.

G Hewer. An iterative technique for the computation of the steady state gains for the discrete optimal regulator. *IEEE Transactions on Automatic Control*, 16(4):382–384, 1971.

Garud N Iyengar. Robust dynamic programming. *Mathematics of Operations Research*, 30(2):257–280, 2005.

Rudolf Emil Kalman et al. Contributions to the theory of optimal control. *Bol. soc. mat. mexicana*, 5(2):102–119, 1960.

Peter Karkus, David Hsu, and Wee Sun Lee. Qmdp-net: Deep learning for planning under partial observability. In *Advances in Neural Information Processing Systems*, pages 4694–4704, 2017.

Sergey Levine and Vladlen Koltun. Guided policy search. In *Proceedings of the 30th International Conference on Machine Learning, ICML 2013*, Atlanta, GA, USA, 16–21 June 2013, volume 28 of *JMLR Workshop and Conference Proceedings*, pages 1–9. JMLR.org, 2013.

Timothy P. Lillicrap, Jonathan J. Hunt, Alexander Pritzel, Nicolas Heess, Tom Erez, Yuval Tassa, David Silver, and Daan Wierstra. Continuous control with deep reinforcement learning. In *4th International Conference on Learning Representations, ICLR*, 2016.

Raanan Lipshitz and Orna Strauss. Coping with uncertainty: A naturalistic decision-making analysis. *Organizational behavior and human decision processes*, 69(2):149–163, 1997.

Zhi-Quan Luo, Jos F Sturm, and Shuzhong Zhang. Multivariate nonnegative quadratic mappings. *SIAM Journal on Optimization*, 14(4):1140–1162, 2004.

Daniel J Mankowitz, Nir Levine, Rae Jeong, Abbas Abdolmaleki, Jost Tobias Springenberg, Timothy Mann, Todd Hester, and Martin Riedmiller. Robust reinforcement learning for continuous control with model misspecification. *arXiv preprint arXiv:1906.07516*, 2019.

Arthur Mensch and Mathieu Blondel. Differentiable dynamic programming for structured prediction and attention. *arXiv preprint arXiv:1802.03676*, 2018.

Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Alex Graves, Ioannis Antonoglou, Daan Wierstra, and Martin Riedmiller. Playing atari with deep reinforcement learning. In *NIPS Deep Learning Workshop*. 2013.

Anusha Nagabandi, Gregory Kahn, Ronald S Fearing, and Sergey Levine. Neural network dynamics for model-based deep reinforcement learning with model-free fine-tuning. In *2018 IEEE International Conference on Robotics and Automation (ICRA)*, pages 7559–7566. IEEE, 2018.

B. O’Donoghue, E. Chu, N. Parikh, and S. Boyd. Conic optimization via operator splitting and homogeneous self-dual embedding. *Journal of Optimization Theory and Applications*, 169(3):1042–1068, June 2016. URL [http://stanford.edu/~boyd/papers/scs.html](http://stanford.edu/~boyd/papers/scs.html)

Junhyuk Oh, Satinder Singh, and Honglak Lee. Value prediction network. In *Advances in Neural Information Processing Systems*, pages 6118–6128, 2017.

Fabian Otto, Philipp Becker, Ngo Anh Vien, Hanna Carolin Ziesche, and Gerhard Neumann. Differentiable trust region layers for deep reinforcement learning. *CoRR*, abs/2101.09207, 2021. URL [https://arxiv.org/abs/2101.09207](https://arxiv.org/abs/2101.09207)

Jens Schreiter, Duy Nguyen-Tuong, Mona Eberts, Bastian Bischoff, Heiner Markert, and Marc Toussaint. Safe exploration for active learning with gaussian processes. In *Machine Learning and Knowledge Discovery in Databases - European Conference, ECML PKDD*, volume 9286 of *Lecture Notes in Computer Science*, pages 133–149. Springer, 2015.

John Schulman, Sergey Levine, Pieter Abbeel, Michael Jordan, and Philipp Moritz. Trust region policy optimization. In *International conference on machine learning*, pages 1889–1897, 2015.

David Silver, Hado Hasselt, Matteo Hessel, Tom Schaul, Arthur Guez, Tim Harley, Gabriel Dulac-Arnold, David Reichert, Neil Rabinowitz, Andre Barreto, et al. The predictron: End-to-end learning and planning. In *International Conference on Machine Learning*, pages 3191–3199. PMLR, 2017.

Wen Sun. *Towards Generalization and Efficiency in Reinforcement Learning*. PhD thesis, Carnegie Mellon University, 2019.

Avi Tamar, Yi Wu, Garrett Thomas, Sergey Levine, and Pieter Abbeel. Value iteration networks. In *Advances in Neural Information Processing Systems*, pages 2154–2162, 2016.
Jack Umenberger, Mina Ferizbegovic, Thomas B Schön, and Håkan Hjalmarsson. Robust exploration in linear quadratic reinforcement learning. In Advances in Neural Information Processing Systems, pages 15310–15320, 2019.

Lieven Vandenberghe, Stephen Boyd, and Mehrdad Nouralishahi. Robust linear programming and optimal control. IFAC Proceedings Volumes, 35(1):271–276, 2002.

Avishai Weiss and Stefano Di Cairano. Robust dual control mpc with guaranteed constraint satisfaction. In 53rd IEEE Conference on Decision and Control, pages 6713–6718. IEEE, 2014.

Tianhao Zhang, Gregory Kahn, Sergey Levine, and Pieter Abbeel. Learning deep control policies for autonomous aerial vehicles with mpc-guided policy search. In 2016 IEEE international conference on robotics and automation (ICRA), pages 528–535. IEEE, 2016.