MOPO: Model-based Offline Policy Optimization

Tianhe Yu *1 Garrett Thomas *1 Lantao Yu 1 Stefano Ermon 1 James Zou 1 Sergey Levine 2 Chelsea Finn †1 Tengyu Ma †1

Abstract

Offline reinforcement learning (RL) refers to the problem of learning policies entirely from a batch of previously collected data. Despite significant progress in model-free offline RL, the most successful prior methods constrain the policy to the support of the data, precluding generalization to new states and actions. In this paper, we propose a model-based approach that enables some degree of generalization beyond the behavioral distribution. To limit exploitation of errors in the model, we penalize the reward function by a measure of model uncertainty, in such a way that the expected return in the penalized MDP is a lower bound of the return in the true MDP. Based on our theoretical results, we develop a practical model-based offline RL algorithm that outperforms both standard model-based RL methods and state-of-the-art model-free offline RL approaches on existing offline RL benchmarks, as well as two challenging continuous control tasks that require generalizing from data collected for a different task.

1. Introduction

Recent advances in machine learning using deep neural networks have shown significant successes in scaling to large datasets, such as ImageNet (Deng et al., 2009) in computer vision, SQuAD (Rajpurkar et al., 2016) in NLP, and RoboNet (Dasari et al., 2019) in robot learning. Reinforcement learning (RL) methods, in contrast, struggle to scale to many real-world applications, e.g., autonomous driving (Yu et al., 2018) and healthcare (Gottesman et al., 2019), because they rely on costly online trial-and-error. Designing RL algorithms that can learn from diverse, static datasets would enable more practical RL training in the real world.

While off-policy RL algorithms (Lillicrap et al., 2015; Haarnoja et al., 2018; Fujimoto et al., 2018b) can in principle utilize previously collected datasets, they perform poorly without online data collection. These failures are generally caused by large extrapolation error when the Q-function is evaluated on out-of-distribution actions (Fujimoto et al., 2018a; Kumar et al., 2019), which can lead to unstable learning and divergence. Offline RL methods propose to mitigate bootstrapped error by constraining the learned policy to the behavior policy induced by the dataset (Fujimoto et al., 2018a; Kumar et al., 2019; Wu et al., 2019; Jaques et al., 2019; Nachum et al., 2019; Peng et al., 2019; Siegel et al., 2020). While these methods achieve reasonable performances in some settings, their learning is limited to behaviors within the data manifold. We argue that it is important for an offline RL algorithm to be equipped with the ability to leave the data support to learn a better policy for two reasons: (1) the provided batch dataset is usually sub-optimal in terms of both the states and actions covered by the dataset, and (2) the target task can be different from the tasks performed in the batch data for various reasons, e.g., because data is not available or hard to collect for the target task.

We hypothesize that model-based RL methods (Sutton, 1991; Deisenroth & Rasmussen, 2011; Levine & Koltun, 2013; Kumar et al., 2016; Janner et al., 2019; Luo et al., 2018) make a natural choice for enabling generalization, for a number of reasons. First, model-based RL algorithms effectively receive more supervision, since the model is trained on every transition, even in sparse-reward settings. Second, they are trained with supervised learning, which provides more stable and less noisy gradients than bootstrapping. Lastly, uncertainty estimation techniques, such as bootstrap ensembles, are well developed for supervised learning methods (Lakshminarayanan et al., 2017; Kuleshov et al., 2018; Snoek et al., 2019) and are known to perform poorly for value-based RL methods (Wu et al., 2019). All of these attributes have the potential to improve or control generalization.

However, because offline model-based algorithms cannot improve the dynamics model using additional experience, we expect that such algorithms require careful use of the model in regions outside of the data support. To do so, we modify the model MDP via a reward penalty based on an
estimate of the model error. Crucially, this estimate is model-dependent, and does not necessarily penalize all out-of-distribution states and actions equally, but rather prescribes penalties based on the estimated magnitude of model error. Further, this estimation is done both on states and actions, allowing generalization to both, in contrast to model-free approaches that only reason about uncertainty with respect to actions.

The primary contribution of this work is an offline model-based RL algorithm that optimizes a policy in an uncertainty-penalized MDP, where the reward function is penalized by an estimate of the model’s error, yielding a lower bound of the return in the true MDP. We present a practical algorithm that estimates model error using the predicted variance of a Lipschitz-regularized model. We empirically compare this model-based off-policy optimization (MOPO) to existing state-of-the-art model-free offline RL algorithms. Our results suggest that MOPO substantially outperforms these prior methods on the offline RL benchmark D4RL (Fu et al., 2020) as well as on offline RL problems where the agent must generalize to out-of-distribution states in order to succeed.

2. Preliminaries

We consider a standard Markov decision process (MDP) $M = (S, A, T, r, \mu_0, \gamma)$, where $S$ and $A$ denote the state space and action space respectively, $T(s' | s, a)$ the transition dynamics, $r(s, a)$ the reward function, $\mu_0$ the initial state distribution, and $\gamma \in (0, 1)$ the discount factor. The goal in RL is to optimize a policy $\pi(a | s)$ that maximizes the expected discounted return $\pi_M(\pi) := \mathbb{E}_\pi,\mu_0 \sum_{t=0}^{\infty} \gamma^t r(s_t, a_t)$. The value function $V^\pi_M(s) := \mathbb{E}_{\pi, T, s_0 \sim \mu_0}[\sum_{t=0}^{\infty} \gamma^t r(s_t, a_t) | s_0 = s]$ gives the expected discounted return under $\pi$ if starting from state $s$.

In the model-based approach we will have a dynamics model $\tilde{T}$ estimated from the transitions in the static dataset $D_{env} = \{(s, a, r, s')\}$. This estimated dynamics defines a model MDP $\tilde{M} = (S, A, \tilde{T}, r, \mu_0, \gamma)$. Let $\mathbb{P}_{\tilde{T}, t}^\pi(s)$ denote the probability of being in state $s$ at time step $t$ if actions are sampled according to $\pi$ and transitions according to $\tilde{T}$. Let $\rho_{\tilde{T}}^\pi(s)$ be the discounted state distribution of policy $\pi$ under dynamics $\tilde{T}$: $\rho_{\tilde{T}}^\pi(s) := \sum_{t=0}^{\infty} \gamma^t \mathbb{P}_{\tilde{T}, t}^\pi(s)$. We also define (abusing notation) the discounted state-action distribution $\rho_{\tilde{T}}^\pi(s, a) := \mathbb{P}_{\tilde{T}}^\pi(s)\pi(a | s)$. Note that $\rho_{\tilde{T}}^\pi$, as defined here, is not a properly normalized probability distribution, as it integrates to $1/(1-\gamma)$. We will denote (improper) expectations with respect to $\rho_{\tilde{T}}^\pi$ with $\mathbb{E}$, as in $\mathbb{E}_{\tilde{T}}[r(s, a)]$.

We summarize model-based policy optimization (MBPO) (Janner et al., 2019), which we build on in this work, in Appendix D.

3. MOPO: Model-Based Offline Policy Optimization

We now present our approach to model-based offline RL. We first bound the true return from below by the return of a constructed model MDP penalized by the uncertainty of the dynamics (Section 3.1). Then we maximize the conservative estimation of the return by an off-the-shelf reinforcement learning algorithm, which gives MOPO, a generic model-based off-policy algorithm (Section 3.2). We discuss important practical implementation details in Section 3.3.

3.1. Quantifying the uncertainty: from the dynamics to the total return

Our key idea is to build a lower bound for the return of a policy $\pi$ under the true dynamics and then maximize the lower bound over $\pi$. A natural estimator for the true return $\pi_M(\pi)$ is $\eta_{\tilde{M}}(\pi)$, the return under the estimated dynamics. The error of this estimator depends on, potentially in a complex fashion, the error of $\tilde{T}$, which may compound over time. In this subsection, we characterize how the error of $\tilde{T}$ influences the uncertainty of the total return. We will state a lemma that bounds the difference between the performance of a policy under dynamics $T$ and dynamics $\tilde{T}$. All proofs are given in Appendix B. We first require some assumptions.

Assumption 3.1. Assume a scalar $c \geq 0$ and a function class $\mathcal{F}$ such that $V^\pi_{\tilde{M}} \in c\mathcal{F}$ for all $\pi$.

In our analysis, the integral probability metric (IPM) (Müller, 1997) associated with $\mathcal{F}$, defined as $d_{\mathcal{F}}(P, Q) := \sup_{f \in \mathcal{F}}|\mathbb{E}_{X \sim P}[f(X)] - \mathbb{E}_{Y \sim Q}[f(Y)]|$, relates the error of the model with the error of the return. Although Assumption 3.1 is somewhat abstract, it typically holds in practice: if we assume that the reward function is bounded by $r_{\text{max}}$, then $V^\pi_{\tilde{M}}$ is bounded by $r_{\text{max}}/(1-\gamma)$ for any $\pi$, so Assumption 3.1 holds with $c = r_{\text{max}}/(1-\gamma)$ and $\mathcal{F} = \{f : \|f\|_{\infty} \leq 1\}$. In this case $d_{\mathcal{F}}$ is the total variation distance. We note that with stronger assumptions on the MDP, one can also obtain bounds in terms of 1-Wasserstein distance or maximum mean discrepancy.

Assumption 3.2. We assume a function $u : S \times A \to \mathbb{R}$ which is an admissible error estimator for $\tilde{T}$, meaning that $d_{\mathcal{F}}(\tilde{T}(s, a), T(s, a)) \leq u(s, a)$ for all $s, a$.

Lemma 3.3. Let $M$ and $\tilde{M}$ be two MDPs with reward function $r$ but different dynamics $T$ and $\tilde{T}$ respectively. Then, under Assumptions 3.1 and 3.2, letting $\lambda := c\gamma$ we have

$$|\eta_{\tilde{M}}(\pi) - \eta_M(\pi)| \leq \lambda \mathbb{E}_{(s,a) \sim \rho_{\tilde{T}}^\pi}[u(s, a)]$$

(1)

Thus,

$$\eta_M(\pi) \geq \mathbb{E}_{(s,a) \sim \rho_{\tilde{T}}^\pi}[r(s, a) - \lambda u(s, a)]$$

(2)
Algorithm 1 Framework for Model-based Offline Policy Optimization (MOPO) with Reward Penalty

Require: Dynamics model $\hat{T}$ with admissible error estimator $u(s,a)$; constant $\lambda$
1: Define $\hat{r}(s,a) = r(s,a) - \lambda u(s,a)$. Let $\tilde{M}$ be the MDP with dynamics $\hat{T}$ and reward $\hat{r}$.
2: Run any RL algorithm on $\tilde{M}$ until convergence to obtain
\[
\hat{\pi} = \arg\max_\pi \eta_{\tilde{M}}(\pi) \tag{4}
\]

Equation (2) suggests that a policy that obtains high reward in the estimated MDP while also minimizing model error will obtain high reward in the real MDP. Motivated by Lemma 3.1, we define the uncertainty-penalized reward $\bar{r}(s,a) := r(s,a) - \lambda u(s,a)$, and the uncertainty-penalized MDP $\bar{M} := (S, A, \hat{T}, \bar{r}, \mu_0, \gamma)$. We observe that $\bar{M}$ is conservative in that the return under it bounds from below the true return:
\[
\eta_M(\pi) \geq \mathbb{E}_{(s,a) \sim \rho_\pi}[\bar{r}(s,a)] = \eta_{\bar{M}}(\pi) \tag{3}
\]

3.2. Policy optimization on the penalized MDP

Motivated by (3), we optimize the policy on the uncertainty-penalized MDP $\bar{M}$ in Algorithm 1. We establish a lower bound on the performance of the policy returned by the algorithm.

Theorem 3.4. Suppose Assumption 3.1 and 3.2 hold, and define $\epsilon_u(\pi) := \mathbb{E}_{(s,a) \sim \rho_\pi}[u(s,a)]$. Then the learned policy $\hat{\pi}$ in MOPO (Algorithm 1) satisfies
\[
\eta_M(\hat{\pi}) \geq \sup_{\pi} \{\eta_M(\pi) - 2\lambda \epsilon_u(\pi)\} \tag{5}
\]

The quantity $\epsilon_u(\pi)$ characterizes how erroneous the model is along trajectories induced by $\pi$. Crucially, it depends on the quality of the model and the uncertainty quantification, rather than an explicit divergence between $\pi$ and the behavioral distribution. We provide commentary on the theorem in Appendix C.

3.3. Practical implementation

The method is summarized in Algorithm 2 in Appendix E, and largely follows MBPO with a few key exceptions. We model the dynamics using a neural network that outputs a Gaussian distribution over the next state and reward: $\hat{T}_{\theta,\phi}(s_{t+1}, r|s_t, a_t) = \mathcal{N}(\mu_0(s_t, a_t), \Sigma_0(s_t, a_t))$. We learn an ensemble of $N$ dynamics models $\{\hat{T}_{\theta,\phi}^i = \mathcal{N}(\mu_0^i, \Sigma_0^i)\}_{i=1}^N$. Unlike standard MBPO, the model means $\mu_0^i$ are Lipschitz-regularized. This is shown to be helpful in various settings in Appendix G. We implement this regularization using spectral normalization (Miyato et al., 2018); for details, see Appendix F.

In this work we take $u(s,a) = \max_{i=1,...,N} ||\Sigma_0^i(s,a)||_F$. The learned variance of a Gaussian probabilistic model can theoretically recover the true aleatoric uncertainty when the model is well-specified, and taking the maximum over the ensemble causes $u$ to be more conservative. While this estimator lacks theoretical guarantees, we find that it is sufficiently accurate to achieve good performance in practice. Hence the practical uncertainty-penalized reward of MOPO is computed as $\hat{r}(s,a) = \hat{r}(s,a) - \lambda \max_{i=1,...,N} ||\Sigma_0^i(s,a)||_F$, where $\hat{r}$ is the mean of the predicted reward output by $\hat{T}$.

We treat the penalty coefficient $\lambda$ as a user-chosen hyperparameter. Since we do not have a true admissible error estimator, the value of $\lambda$ prescribed by the theory may not be an optimal choice in practice; it should be larger if our heuristic $u(s,a)$ underestimates the true error and smaller if $u$ substantially overestimates the true error.

4. Experiments

In our experiments, we aim to study the follow questions:
(1) How does MOPO perform on standard offline RL benchmarks in comparison to prior state-of-the-art approaches?
(2) Can MOPO solve tasks that require generalization to out-of-distribution behaviors? (3) How does each component in MOPO affect performance?

To study (2), we construct two additional continuous control tasks that demand out-of-distribution generalization, as described in Section 4.2. To answer question (3), we conduct a complete ablation study to analyze the effect of each module in MOPO in Appendix G. For more details on the experimental setup and hyperparameters, see Appendix H.

We compare against several baselines, including MBPO and the current state-of-the-art model-free offline RL algorithms. BEAR aims to constrain the policy’s actions to lie in the support of the behavioral distribution (Kumar et al., 2019). BRAC is a family of algorithms that penalize the value function by some measure of discrepancy between the actor and the behavioral policy (Wu et al., 2019). BRAC-v uses this penalty both when updating the critic and when updating the actor, while BRAC-p uses this penalty only when updating the actor and does not explicitly penalize the critic.

4.1. Evaluation on the D4RL benchmark

To answer question (1), we evaluate our method on a large subset of datasets in the D4RL benchmark\(^4\) (Fu et al., 2020), including three environments (halfcheetah, hopper, and

\(^4\)https://sites.google.com/view/d4rl
To answer question (2), we construct two environments

<table>
<thead>
<tr>
<th>Dataset type</th>
<th>Environment</th>
<th>Batch Mean</th>
<th>Batch Max</th>
<th>MOPO (ours)</th>
<th>MBPO</th>
<th>SAC</th>
<th>BEAR</th>
<th>BRAC-p</th>
<th>BRAC-v</th>
</tr>
</thead>
<tbody>
<tr>
<td>random</td>
<td>halfcheetah</td>
<td>-303.2</td>
<td>-0.1</td>
<td>3679.8 ± 70.7</td>
<td>3533.0 ± 201.8</td>
<td>350.2</td>
<td>2885.6</td>
<td>3207.3</td>
<td></td>
</tr>
<tr>
<td>random</td>
<td>hopper</td>
<td>299.26</td>
<td>365.9</td>
<td>412.8 ± 30.7</td>
<td>126.6 ± 173.9</td>
<td>347.7</td>
<td>289.5</td>
<td>370.5</td>
<td></td>
</tr>
<tr>
<td>random</td>
<td>walker2d</td>
<td>0.9</td>
<td>57.3</td>
<td>596.3 ± 121.8</td>
<td>395.9 ± 371.7</td>
<td>192.0</td>
<td>307.6</td>
<td>23.9</td>
<td></td>
</tr>
<tr>
<td>medium</td>
<td>halfcheetah</td>
<td>3953.0</td>
<td>4410.7</td>
<td>4706.9 ± 61.1</td>
<td>3230.0 ± 2543.6</td>
<td>-808.6</td>
<td>4508.7</td>
<td>4563.5</td>
<td></td>
</tr>
<tr>
<td>medium</td>
<td>hopper</td>
<td>1021.7</td>
<td>3254.3</td>
<td>840.9 ± 99.3</td>
<td>137.8 ± 87.5</td>
<td>5.7</td>
<td>1527.9</td>
<td>1030.0</td>
<td></td>
</tr>
<tr>
<td>mixed</td>
<td>halfcheetah</td>
<td>2016</td>
<td>3752.7</td>
<td>645.3 ± 464.6</td>
<td>582.6 ± 348.8</td>
<td>44.2</td>
<td>1526.7</td>
<td>3734.3</td>
<td></td>
</tr>
<tr>
<td>mixed</td>
<td>hopper</td>
<td>2300</td>
<td>4834.2</td>
<td>6418.3 ± 47.4</td>
<td>5598.4 ± 1285.1</td>
<td>-581.3</td>
<td>4211.3</td>
<td>5413.8</td>
<td></td>
</tr>
<tr>
<td>mixed</td>
<td>walker2d</td>
<td>358.4</td>
<td>1956.5</td>
<td>1963.5 ± 383.8</td>
<td>1021.8 ± 585.8</td>
<td>87.8</td>
<td>495.3</td>
<td>44.5</td>
<td></td>
</tr>
<tr>
<td>med-expert</td>
<td>halfcheetah</td>
<td>8074.9</td>
<td>12940.2</td>
<td>6913.5 ± 2793.0</td>
<td>929.6 ± 903.2</td>
<td>-55.7</td>
<td>6132.5</td>
<td>5342.4</td>
<td></td>
</tr>
<tr>
<td>med-expert</td>
<td>hopper</td>
<td>1850.5</td>
<td>3760.5</td>
<td>1663.5 ± 1375.6</td>
<td>1803.6 ± 1102.4</td>
<td>32.9</td>
<td>109.8</td>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td>med-expert</td>
<td>walker2d</td>
<td>1062.3</td>
<td>5408.6</td>
<td>2527.1 ± 879.8</td>
<td>351.7 ± 170.6</td>
<td>-5.1</td>
<td>1193.6</td>
<td>3058.0</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Results for D4RL datasets. Each number is the average undiscounted return of the policy at the last iteration of training, averaged over 3 random seeds, ± standard deviation. Numbers for model-free methods taken from (Fu et al., 2020), which does not report standard deviations. We omit BRAC-p in this table for space because BRAC-v outperforms it on these tasks.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Batch Mean</th>
<th>Batch Max</th>
<th>MOPO (ours)</th>
<th>MBPO</th>
<th>SAC</th>
<th>BEAR</th>
<th>BRAC-p</th>
<th>BRAC-v</th>
</tr>
</thead>
<tbody>
<tr>
<td>halfcheetah-jump</td>
<td>1022.6</td>
<td>1808.6</td>
<td>4140.6 ± 88.6</td>
<td>2971.4 ± 1262.1</td>
<td>-3588.2 ± 1436.3</td>
<td>16.8 ± 59.5</td>
<td>1069.9 ± 232.0</td>
<td>871 ± 41.4</td>
</tr>
<tr>
<td>ant-angle</td>
<td>866.7</td>
<td>2311.9</td>
<td>2502.2 ± 15.0</td>
<td>13.6 ± 0.5</td>
<td>-966.4 ± 777.5</td>
<td>1658.2 ± 16.0</td>
<td>1806.7 ± 265.0</td>
<td>2333 ± 138.9</td>
</tr>
</tbody>
</table>

Table 2. Average returns halfcheetah-jump and ant-angle that require out-of-distribution policy. The results are averaged over 3 random seeds. Our method outperforms all the baselines by a large margin, indicating that our approach is effective in generalizing to out-of-distribution states where model-free offline RL methods struggle.

walker2d) and four dataset types (random, medium, mixed, medium-expert), yielding a total of 12 problem settings. 

The results are given in Table 1. Our method is the strongest by a significant margin on all the mixed datasets and most of the medium-expert datasets, while also achieving the best performance on all of the random datasets. Our model-based approach performs less well on the medium datasets. We hypothesize that the lack of action diversity in the medium datasets makes it more difficult to learn a model that generalizes well. Fortunately, this setting is one in which model-free methods can perform well, suggesting that model-based and model-free approaches are able to perform well in complementary settings.

4.2. Evaluation on tasks requiring out-of-distribution generalization

To answer question (2), we construct two environments halfcheetah-jump and ant-angle where the agent must solve a task that is different from the purpose of the behavioral policy. The trajectories of the batch data in these datasets are from policies trained for the original dynamics and reward functions HalfCheetah and Ant in OpenAI Gym (Brockman et al., 2016) which incentivize the cheetah and ant to move forward as fast as possible. Note that for HalfCheetah, we set the maximum velocity to be 3. Concretely, we train SAC for 1M steps and use the entire training replay buffer as the trajectories for the batch data. Then, we assign these trajectories with new rewards that incentivize the cheetah to jump and the ant to run towards the top right corner with a 30 degree angle. Thus, to achieve good performance for the new reward functions, the policy needs to leave the observational distribution. We include the exact forms of the new reward functions in Appendix H. In these environments, learning the correct behaviors requires leaving the support of the data distribution; optimizing solely within the data manifold will lead to sub-optimal policies.

In Table 2, we show that MOPO significantly outperforms the state-of-the-art model-free approaches. In particular, model-free offline RL cannot outperform the best trajectory in the batch dataset, whereas MOPO exceeds the batch max by a significant margin. This validates that MOPO is able to generalize to out-of-distribution behaviors while existing model-free methods are unable to solve those challenges.

5. Conclusion

We develop an algorithm, model-based offline policy optimization (MOPO), based on a modified MDP that penalizes states and actions according to model uncertainty. MOPO is theoretically motivated and trades off the risk of making mistakes and the benefit of diverse exploration from escaping the behavioral distribution. In our experiments, MOPO outperforms state-of-the-art offline RL methods in both standard benchmarks (Fu et al., 2020) and out-of-distribution generalization environments.
Model-based Offline Policy Optimization

References


Snoek, J., Ovadia, Y., Fertig, E., Lakshminarayanan, B., Nowozin, S., Sculley, D., Dillon, J., Ren, J., and Nado,


