REVISITING DESIGN CHOICES IN OFFLINE MODEL-BASED REINFORCEMENT LEARNING

Cong Lu*, Philip J. Ball*, Jack Parker-Holder, Michael A. Osborne, Stephen J. Roberts
Department of Engineering
University of Oxford

ABSTRACT

Offline reinforcement learning enables agents to leverage large pre-collected datasets of environment transitions to learn control policies, circumventing the need for potentially expensive or unsafe online data collection. Significant progress has been made recently in offline model-based reinforcement learning, approaches which leverage a learned dynamics model. This typically involves constructing a probabilistic model, and using the model uncertainty to penalize rewards where there is insufficient data, solving for a pessimistic MDP that lower bounds the true MDP. Existing methods, however, exhibit a breakdown between theory and practice, whereby pessimistic return ought to be bounded by the total variation distance of the model from the true dynamics, but is instead implemented through a penalty based on estimated model uncertainty. This has spawned a variety of uncertainty heuristics, with little to no comparison between differing approaches. In this paper, we compare these heuristics, and design novel protocols to investigate their interaction with other hyperparameters, such as the number of models, or imaginary rollout horizon. Using these insights, we show that selecting these key hyperparameters using Bayesian Optimization produces superior configurations that are vastly different to those currently used in existing hand-tuned state-of-the-art methods, and result in drastically stronger performance.

1 INTRODUCTION

In offline (or batch) reinforcement learning (RL) (Ernst et al., 2005; Levine et al., 2020), the goal is to leverage offline datasets of transitions in an environment to train a policy that transfers to an online task. This could have vast implications for using RL in real-world settings, as agents can make use of ever-increasing amounts of data without the need for an accurate simulator, while also avoiding expensive and potentially even unsafe exploration in the environment.

Model-based reinforcement learning (MBRL) has recently shown promise in this paradigm, obtaining state-of-the-art performance on offline RL benchmarks (Kidanibi et al., 2020; Yu et al., 2021), improving upon powerful model-free approaches (e.g. Kumar et al. (2020)). MBRL works by training a dynamics model from the offline data, then optimizing a policy using imaginary rollouts from the model. This allows the agent to learn from on-policy experience, as the model is agnostic to the policy used to generate data, making it possible to achieve high returns using data collected from even a random policy. Furthermore, recent work has demonstrated the utility of world models beyond maximizing return, such as generalizing to unseen variations in an environment (Ball et al., 2021), transferring to new tasks (Yu et al., 2020), and learning with safety constraints (Argenson & Dulac-Arnold, 2021). Therefore, the case for MBRL in offline RL is clear: not only does it represent state-of-the-art in terms of performance, but it also provides the opportunity to maximize the signal in the offline data to generalize onto tasks beyond those encoded by the behavior policy. This is crucial for offline RL to be useful for real-world tasks (Dulac-Arnold et al., 2021), where there will inevitably be differences between the data and desired task.

However, a common failure mode of MBRL is when policies exploit the model in parts of the state-action space where the model is inaccurate. Thus, naïve application of MBRL to offline data

*Joint first authors. Correspondence: cong.lu@stats.ox.ac.uk, ball@robots.ox.ac.uk
In this paper, we conduct a rigorous investigation into a series of these design choices. We begin by focusing on the choice of uncertainty metric, comparing both recent state-of-the-art offline approaches (Kidambi et al., 2020; Yu et al., 2020; Rafailov et al., 2020) with additional metrics used in the online setting (Ball et al., 2020; Pan et al., 2020; Cowen-Rivers et al., 2022). We also explore the interaction with a series of other hyperparameters, such as the number of models and imaginary rollout length. Interestingly, the relationship between these variables and model uncertainty varies significantly depending on the choice of uncertainty penalty. Furthermore, we compare these uncertainty heuristics under new evaluation protocols that, for the first time, capture the specific covariate shift induced by model-based RL. This allows us to assess calibration to model exploitation in MBRL, observing that some existing penalties are surprisingly successful at capturing the errors in predicted dynamics, as seen in Fig. 1a (see App. D for details). Then, using the insights gained from sections 4 and 5, we then achieve a 43% gain over a previously grid-searched method by using a single hyperparameter value across all environments. We then jointly fine-tune our identified key variables using a powerful Bayesian Optimization algorithm (Wan et al., 2021) and find the simpler uncertainty measures can provide state-of-the-art results in continuous control offline benchmarks, and that the chosen optimal hyperparameters continue to align with our analysis. Finally, we rigorously confirm the aggregate improvement of our results using the rliable framework (Agarwal et al., 2021) in Fig. 1b, and show that the improvements over existing methods are significant (see App. H for details). This work is intended to benefit both researchers and practitioners in offline RL. Our main findings include:

- **Longer horizon rollouts with larger penalties can improve existing methods.** Contrary to common wisdom, conducting significantly longer rollouts inside the model, coupled with larger uncertainty penalties, typically improves performance.

- **Penalties that use canonical forms of uncertainty estimation achieve better correlation with OOD measures.** The uncertainty estimation approach of Lakshminarayanan et al. (2017) often outperforms the penalty from state-of-the-art methods (Yu et al., 2020; Kidambi et al., 2020). We observe that the ensemble standard deviation is statistically strikingly similar to that used in Kidambi et al. (2020), but has improved correlation and scaling behavior.

- **Uncertainty is more correlated with dynamics error than distribution shift.** We find that successful penalties measure the discrepancy in dynamics, and can in fact assign high certainty to data far away from the offline data.

## 2 Related Work

Two recent works concurrently demonstrated the effectiveness of model-based reinforcement learning (MBRL) in the offline setting. MOPO (Yu et al., 2020) follows the successful online RL algorithm MBPO (Janner et al., 2019) but trains inside a conservative MDP, penalizing the reward based on the maximum aleatoric uncertainty over the ensemble members. MOReL (Kidambi et al., 2020) achieves...
even stronger performance, penalizing the rewards by a penalty based on the maximum pair-wise difference in ensemble member predictions. For pixel-based tasks, LOMPO (Rafailov et al., 2020) also proposed a novel penalty, using the variance of ensemble log-likelihoods. Outside the offline setting, probabilistic dynamics models leveraging uncertainty have underpinned a series of successes (Chua et al., 2018; Kurutach et al., 2018; Buckman et al., 2018; Pan et al., 2020; Pacchiano et al., 2021). Uncertainty can also be measured in MBRL without the use of neural networks (Deisenroth & Rasmussen, 2011), although these methods tend to be harder to scale and thus lack widespread use.

Effective hyperparameter selection in RL has been shown to be crucial to the success of popular algorithms (Engstrom et al., 2020; Andrychowicz et al., 2021). This becomes even more challenging in MBRL with additional hyperparameters/design-choices for the dynamics model. Recent work has shown that carefully optimizing these hyperparameters for online MBRL can significantly improve performance, with the tuned agent breaking the MuJoCo simulator (Zhang et al., 2021). In contrast, we focus on the offline setting, and investigate parameters specifically related to uncertainty estimation. Previous work studied the impact of hyperparameters in offline RL (Paine et al., 2020), finding offline RL algorithms to be brittle to hyperparameter choices. However, unlike our work they only consider model-free approaches, whereas we specifically investigate model-based offline algorithms. Abbas et al. (2020) investigates the impact of different uncertainty estimation methods in online MBRL; they too find penalizing with combined aleatoric and epistemic uncertainty improves performance.

Our work also relates to the rich literature on deep ensembles (Lakshminarayanan et al., 2017), which train multiple deep neural networks with different initializations and dataset orderings, and generally outperform variational Bayes methods (Mackay, 1992; Blundell et al., 2015). Achieving effective calibration with neural networks is notoriously difficult (Guo et al., 2017; Kuleshov et al., 2018; Maddox et al., 2019), and furthermore we require calibration under co-variate shift (Ovadia et al., 2019), as the policy learned in the model will likely deviate from the behavior policy that generated the offline data. Recent work has highlighted this issue in offline RL (Kumar et al., 2020; Yu et al., 2021) and has reported superior performance when eschewing model uncertainty entirely, and instead performing “conservative” Q-updates. However, it is unclear if this improvement is due to poor uncertainty calibration, implementation details, or a limitation in the pessimistic-MDP formulation.

3 BACKGROUND

All of the methods we investigate in this paper model the environment as a Markov Decision Process (MDP), defined as a tuple $\mathcal{M} = (\mathcal{S}, \mathcal{A}, P, R, \rho_0, \gamma)$, where $\mathcal{S}$ and $\mathcal{A}$ denote the state and action spaces respectively, $P(s'|s, a)$ the transition dynamics, $R(s, a)$ the reward function, $\rho_0$ the initial state distribution, and $\gamma \in (0, 1)$ the discount factor. The goal is to optimize a policy $\pi(a|s)$ that maximizes the expected discounted return $\mathbb{E}_{\pi, P, \rho_0, \gamma} \left[ \sum_{t=0}^{\infty} \gamma^t R(s_t, a_t) \right]$.

In offline RL, the policy is not deployed in the environment until test time. Instead, the algorithm only has access to a static dataset $D_{\text{env}} = \{(s_j, a_j, r_j, s_{j+1})\}_{j=1}^J$, collected by one or more behavioral policies $\pi_b$. Following the notation in Yu et al. (2020) we refer to the distribution from which $D_{\text{env}}$ was sampled as the behavioral distribution. The canonical approach in offline MBRL is to train an ensemble of $N$ probabilistic dynamics models (Nix & Weigend, 1994). These usually learn to predict both the next state $s_{t+1}$ and reward $r_t$ from a state-action pair, and are trained on $D_{\text{env}}$ using supervised learning. Concretely, each of the $N$ models output a Gaussian $P^i_{\phi}(s_{t+1}, r_t|s_t, a_t) = \mathcal{N}(\mu^i_{\phi}(s_t, a_t), \Sigma^i_{\phi}(s_t, a_t))$ parameterized by $\phi$. The resulting learned dynamics model $P^i$ and reward model $R^i$ define a model MDP $\bar{\mathcal{M}} = (\mathcal{S}, \mathcal{A}, P^i, R^i, \rho_0, \gamma)$. To train the policy, we use $k$-step rollouts inside $\bar{\mathcal{M}}$ to generate trajectories (Sutton, 1991).

To prevent policy exploitation in a model, a pessimistic MDP (P-MDP) is constructed by lower bounding the true-expected return, $\eta_{\mathcal{M}}(\pi)$, using some error between the true and estimated models. For instance, in Yu et al. (2020), the authors show that a lower bound on the return can be established by penalizing the reward by a measure that corresponds to estimated model error:

$$\eta_{\mathcal{M}}(\pi) \geq \mathbb{E}_{(s, a) \sim \rho^P_{\pi}} \left[ R(s, a) - \gamma |G^\pi_{\bar{\mathcal{M}}}(s, a)| \right]$$

where $\rho^P_{\pi}$ represents transitioning under the dynamics model $P$ and policy $\pi$. Several potential choices for $|G^\pi_{\bar{\mathcal{M}}}(s, a)|$ are proposed, including an upper bound based on the total variation distance.
between the learned and true dynamics. However, for their practical algorithm, the authors elect to use a heuristic based on impressive empirical results. Concurrent to MOPO, MOREL (Kidambi et al., 2020) in theory constructs a P-MDP by augmenting a standard MDP with a negative valued absorbing state that is transitioned to when total variation distance between true and learned dynamics is exceeded. They show that a policy learned in this P-MDP exceeds simple behavior cloning. However, while dynamics-based total variation distance has desirable theoretical properties, the practical algorithm relies on another heuristic to approximate this quantity. This motivates the study of penalties used, as well as other under-used candidates, and their overall effectiveness.

4 Uncertainty Penalty

The key idea underpinning recent success in offline MBRL is the introduction of a P-MDP, penalized by some uncertainty penalty. The theory dictates this should be some distance measure between the true and predicted dynamics. Of course, this cannot be truly estimated without access to an oracle, so a proxy for this quantity is constructed instead based on uncertainty heuristics. In this paper, we compare the following uncertainty heuristics, from recent works in both offline and online MBRL:

Max Aleatoric (Yu et al., 2020): \[ \max_{i=1,...,N} ||\mu_i(s, a)||_F, \] which corresponds to the maximum aleatoric error, computed over the variance heads of the model ensemble.

Max Pairwise Diff (Kidambi et al., 2020): \[ \max_{i,j} ||\mu_i(s, a) - \mu_j(s, a)||_2, \] which corresponds to the pairwise maximum difference of the ensemble predictions.

LL Var (Log-Likelihood Variance) (Rafailov et al., 2020): \[ \text{Var} \left( \{ \log \hat{P}_{\phi_i}(s'|s, a), i = 1, \ldots, N \} \right), \] where \( s' \) is a next state sampled from a single ensemble member. We evaluate its log-likelihood under each ensemble member and take the variance.

LOO KL (Leave-One-Out KL Divergence (Pan et al., 2020): \[ D_{KL} [\hat{P}_{\phi_i}(\cdot|s, a)||\hat{P}_{\phi_{-i}}(\cdot|s, a)], \] which corresponds to the KL divergence between the Gaussian parameterized by a randomly selected ensemble member, and the aggregated Gaussian of the remaining ensemble members.

Ensemble Standard Deviation/Variance (Lakshminarayanan et al., 2017): The variance is given as: \[ \Sigma(s, a) = \frac{1}{N} \sum_{i=1}^{N} (1(N_i(s, a))^2 + (\mu_i(s, a))^2) - (\mu(s, a))^2 \] where \( \mu(s, a) \) is the mean of the means. \( \text{Var}(s, a) = \frac{1}{N} \sum_{i=1}^{N} \mu_i^2(s, a) \). This corresponds to a combination of epistemic and aleatoric model uncertainty.

These can all be computed using the output from an ensemble of probabilistic dynamics models (Lakshminarayanan et al., 2017), so we are able to compare them in a controlled manner.

4.1 How Well Do Ensemble Penalties Detect Out of Distribution Errors?

We begin by assessing how well uncertainty penalties correlate with next state MSE (we justify the MSE under deterministic dynamics in App. A.2). This is crucial in penalizing the policy from visiting parts of the state-action space where the model is inaccurate, and therefore exploitable. Using D4RL (Fu et al., 2021a), we train models on each dataset, then evaluate them on other datasets from the same environment, but collected under different policies. These form our “Transfer” experiments as they directly measure the ability of uncertainty penalties at detecting errors on unseen data. We compare the penalties against true MSE for a variety of settings in App. A.3, and summarize this in the “Transfer” column of Table 1. We measure Spearman rank (\( \rho \)) and Pearson bivariate (\( r \)) correlations, and justify their use in App. A.1. Full details of all experiments and hyperparameters are given in App. G. We will analyze these results in detail in the next section, after introducing a novel protocol for assessing our penalties under the out-of-distribution (OOD) data induced by model exploitation.

4.2 How Do These Perform During an Imaginary Rollout?

We additionally design an experiment aimed at capturing the OOD data generated by the actual offline MBRL process, which we call our “True Model-Based” experiments. First, we train a set of policies with 4 different starting seeds without a penalty inside the model for 500 iterations. We...
We are now in a position to analyze the results in Table 1. It is immediately obvious that the LOO KL is significantly lower than the other penalties, which trains seven probabilistic dynamics models of the same architecture (with different initializations), using only the top five models based on validation accuracy (referred to as “Elites” in the Evolutionary community, e.g. Mouret & Clune (2015)). The reason for this is not discussed, but it has seemingly been adopted in the wider MBRL setting (Shen et al., 2020; Omer et al., 2021; Pineda et al., 2021). However, offline RL is a totally different paradigm, where it is possible that access to compute is less of a bottleneck and it may be preferable to use more models to extract the most signal possible from the static dataset. Inevitably, many of the ensemble penalties are dependent on the number of models; for example, it is easy to see that the Max Aleatoric value could scale poorly with more models. Then measure the difference between the return predicted by the model over a rollout, and the true return in the real environment. We define a policy to be “exploitative” if the model significantly over-estimates the return compared to the true return. It is these exploitative policies that induce the types of extrapolation errors which cause MBRL methods to fail in the offline setting. It is therefore important that the penalty is able to accurately determine when the model is being exploited in this way. We use a subset of the 5 most exploitative policies to generate trajectories in the model, and record the uncertainty predicted by each penalty at every time step. To generate the true Model-Based data, we then “replay” these trajectories in the true environment, loading the state and action taken in the model into the environment, and record the “true” next state according to the MuJoCo simulator (Todorov et al., 2012). True Model-Based therefore calculates the MSE between the predicted and actual next states. Table 1 summarizes the results from both the Transfer and True Model-Based experiments. Additional details are provided in App. D along with full correlation plots in App. A.3.

We are now in a position to analyze the results in Table 1. It is immediately obvious that the LOO KL and LL Var penalties have very weak correlation with MSE. We believe this is because LL Var relies on likelihood statistics, which are notoriously sensitive; it was designed for use with a KL-regularized probabilistic dynamics model of the same architecture, as such penalties appear sensitive to the quality of their estimated distributions. We observe that Max Aleatoric, Max Pairwise Diff and the Ensemble penalties perform broadly similarly despite their different analytical forms; Ensemble measures do however exhibit noticeably higher rank correlation. We also observe a significant performance loss between the Transfer and True Model-Based HalfCheetah settings, with the latter being relatively poor. This implies further work is needed to develop penalties that can successfullly detect the type of dynamics discrepancies that actually arise in offline MBRL. Finally, we observe that despite the similar rank correlations $\rho$, the bivariate correlations $r$ can vary considerably, and observe from the scatter plots that Max Aleatoric exhibits low kurtosis, having large penalty values “bunched” at its extreme; we provide 3rd and 4th order moment statistics to facilitate shape comparisons in App. C.

5 Key Hyperparameters in Offline MBRL

5.1 How Many Models Do We Need?

At present the number of models used has not been discussed since MBPO, which trains seven probabilistic dynamics models of the same architecture (with different initializations), using only the top five models based on validation accuracy (referred to as “Elites” in the Evolutionary community, e.g. Mouret & Clune (2015)). The reason for this is not discussed, but it has seemingly been adopted in the wider MBRL setting (Shen et al., 2020; Omer et al., 2021; Pineda et al., 2021). However, offline RL is a totally different paradigm, where it is possible that access to compute is less of a bottleneck and it may be preferable to use more models to extract the most signal possible from the static dataset. Inevitably, many of the ensemble penalties are dependent on the number of models; for example, it is easy to see that the Max Aleatoric value could scale poorly with more models.

How Does Penalty Distribution Change with Model Count? We now vary the number of models used in the calculation of the penalties and plot their respective distributions; an illustrative example is shown in Fig. 2 with full results in App. B. The scaling of penalties relying on max over sets is most affected with increasing the number of models due to admitting more extreme values, and we observe that the distribution shape of Max Aleatoric changes significantly as we admit more models, which

<table>
<thead>
<tr>
<th>Penalty</th>
<th>HalfCheetah</th>
<th>Hopper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Aleatoric</td>
<td>0.78±0.00</td>
<td>0.71±0.01</td>
</tr>
<tr>
<td>Max Pairwise Diff</td>
<td>0.79±0.01</td>
<td>0.62±0.00</td>
</tr>
<tr>
<td>Ens. Std.</td>
<td>0.82±0.01</td>
<td>0.67±0.00</td>
</tr>
<tr>
<td>Ens. Var.</td>
<td>0.82±0.01</td>
<td>0.67±0.00</td>
</tr>
<tr>
<td>LL Var.</td>
<td>0.13±0.05</td>
<td>0.14±0.02</td>
</tr>
<tr>
<td>LOO KL</td>
<td>0.03±0.02</td>
<td>0.11±0.02</td>
</tr>
</tbody>
</table>
we validate in App. C. This impacts the tuning of this hyperparameter, as we have to contend with a changing distribution along with calibration quality (which we explore in the next section). Finally, we observe that the Ensemble penalties change the least with differing model count, highlighting their ease of tuning; this is clearly a desirable property for designing such metrics going forward.

### How does Penalty Performance Scale with Model Count?

Empirically, there exists an optimal number of models to use in an ensemble for model-based RL (Kurutach et al., 2018; Matsushima et al., 2021). Up to now, heuristics have been used to select how many models we use for uncertainty estimation, despite it being possible to use a different number of models for dynamics prediction and uncertainty estimation. For instance, in MOPO, transitions are generated with five Elite models, but all seven models are used to calculate the penalty. In MOREl, four models are used for both transitions and penalty prediction. Therefore, we wish to understand if there is merit to using a larger number of models for uncertainty estimation compared with next state prediction. We provide a snapshot in Fig. 3, showing the aggregated results on the True Model-Based data in Hopper, with full results in App. B. We see there is no clear consensus, and that the optimal number of models is highly dependent on environment, the behavior data, and penalty type, with some settings showing improved calibration with model count and vice-versa. This clearly justifies treating the number of models as a hyperparameter that is important to tune, especially on transfer tasks. Interestingly, we observe that it is possible to simultaneously improve rank ($\rho$) correlation, but reduce bivariate ($r$) correlation, especially with the MOPO penalty. This again suggests that the number of models not only affects the quality of the estimation, but also its distributional shape.

#### 5.2 The Weight of Uncertainty $\lambda$

To weight penalty against reward, MOPO introduces a parameter $\lambda$ that trades off between the two terms. In their paper, the authors sweep over $\lambda \in \{1, 5\}$ for each environment. However, the optimal values may lie outside this region. Furthermore, we have shown this value will need to drastically change to account for using a different penalty or even number of models.

#### 5.3 The Rollout Horizon $h$

The horizon $h$ of the rollouts plays a crucial role in offline RL. Longer horizon rollouts increase the likelihood of errors in the transitions (we verify this intuition in App. D), but conversely can improve performance when errors are properly managed (Janner et al., 2019; Pan et al., 2020). Furthermore, as highlighted in Fig. 1a, the model can generalize, and dynamics error does not necessarily increase with drift away from the offline dataset. Instead, we observe spikes, and note it is possible to recover from these to valid states and transitions. It is therefore imperative that a penalty captures these spikes over the course of an entire model rollout with horizon $h$, and down-weights the reward accordingly.

Using this observation, we design a novel experiment that treats these spikes as “positive” labels, and normalize each penalty to $[0, 1]$. This converts the penalties into a probabilistic classifier, and we evaluate how well they classify these events that occur increasingly under longer $h$. This is precisely the intuition behind the LOO KL and LL Var approaches, whereby the penalty acts as an
### Table 2: Performance of different penalties as OOD event detectors averaged over all datasets in Hopper and HalfCheetah (i.e., Random through to Expert) showing ± 1 SD over 12 seeds. AUC is “Area Under Curve” and AP is “Average Precision”. The best (highest) in each column is highlighted in **bold**.

<table>
<thead>
<tr>
<th>Penalty</th>
<th>90th</th>
<th>95th</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AUC</td>
<td>AP</td>
</tr>
<tr>
<td>Max Absolute</td>
<td>0.89±0.01</td>
<td>0.50±0.02</td>
</tr>
<tr>
<td>Max Pairwise Diff</td>
<td>0.90±0.00</td>
<td>0.54±0.01</td>
</tr>
<tr>
<td>Ensemble Std</td>
<td>0.90±0.00</td>
<td>0.54±0.01</td>
</tr>
<tr>
<td>Ensemble Var</td>
<td>0.90±0.00</td>
<td>0.54±0.01</td>
</tr>
<tr>
<td>LL Var</td>
<td>0.66±0.03</td>
<td>0.34±0.00</td>
</tr>
<tr>
<td>LOO KL</td>
<td>0.59±0.03</td>
<td>0.21±0.01</td>
</tr>
</tbody>
</table>

Anomaly detection, removing detrimental transitions that lie above a threshold. This is the regime we focus on here, where binary detection is more important than correlation. Finally, we assess two “True Model-Based” errors: the dynamics error as before, and introduce the distance from the offline distribution trained on, which we calculate as the 2-norm between a state-action tuple and its nearest point in the offline data (Dadashi et al., 2021); these are called “Dynamics” and “Distribution” respectively. We provide precision-recall curves and more details on this experiment in App. D and E.

We observe in Table 2 that the penalties are powerful at identifying dynamics discrepancy, but not as accurate at identifying when the world-model data is out-of-distribution with respect to the offline data. This is a well-known phenomenon in deep neural networks and has been recently investigated in terms of feature collapse (Van Amersfoort et al., 2020), where latent representations of points far away in the input space get mapped close together. On the other hand, this shows an important distinction between the regularization induced by MBRL uncertainty and explicit state-action regularization in model-free approaches, such as Kumar et al. (2020); Wu et al. (2021). In the latter approaches, policies are penalized for taking out of distribution actions w.r.t. the offline dataset, but this is not always the case with policies trained under MBRL and uncertainty penalties. The success of MBRL methods in RL may therefore lie in the generation of state-action samples that are OOD but represent accurate dynamics, thus facilitating dynamics generalization in policies; recent work has shown that augmenting dynamics improves offline RL policy generalization (Ball et al., 2021). We believe future work understanding the implications of this property is vitally important.

### 6 Testing the Limits of Current Approaches

Given our previous analysis, in this section we seek to answer the following question: how well can existing methods perform with a more optimal selection of the discussed hyperparameters? To answer this, we consider, first, a naive selection of one hyperparameter set across all environments (based on our previous analysis), and then more definitively, tuning the configuration for each individual D4RL MuJoCo environment using a state-of-the-art Bayesian Optimization (BO) algorithm (Wan et al., 2021). Our first set of results show that following our analysis can provide significant gains over existing baselines, whilst the second beats the current SoTA. Note, previous analysis focused on HalfCheetah and Hopper environments, so we extend our evaluation to Walker2d as a held-out test.

**General applicability of our insights.** Two of our main takeaways in Sections 4 and 5 are that we should favor the canonical Ensemble penalties and longer rollout horizons. To test these claims, we design an experiment where we fix $h = 20$ for the horizon (c.f. $h = 5$ in MOPO at most), and only use Ensemble Std. as our penalty (see App. G for details). Since tuning the penalty weight $\lambda$ per environment is unrealistic, we employ an automatic penalty tuning scheme, analogous to the automatic entropy tuning used in Haarnoja et al. (2018). We tune the penalty weight on-the-fly to a constraint value of $\Lambda = 1$, meaning we use only a single hyperparameter across all environments. Full details on the penalty weight tuning are provided in App. I. With this approach, we get an average reward of **49.0** in the D4RL locomotion test suite (Fu et al., 2021a), an increase of **43%** over MOPO, which was grid-searched per environment.

This clearly shows that applying the findings from our analysis provides large performance gains generally. This result is the best we know for a single hyperparameter setup, and is particularly significant as other offline MBRL algorithms tune many hyperparameters per environment. This ‘zero-shot’ hyperparameter restriction is also the most realistic application of offline RL to real world problems. If we were to allow ourselves to take the maximum over just 2 hyperparameter setups (the second setup being $h = 10$, $\Lambda = 0.5$), we achieve an average reward of **57.8**, an increase of **69%** over MOPO. We show the full results in Table 8 in App. I with improvement probabilities.
Table 3: Best hyperparameters discovered by our BO algorithm, followed by a comparative evaluation on the D4RL benchmark suite against other model-based RL algorithms. We use D4RL v0 datasets. The raw score for Optimized\(^1\) and MOPO\(^1\) was taken to be the average over the last 10 iterations of policy training, averaged over 4 seeds and showing ±1 SD. Results of MOPO and COMBO were taken from the COMBO paper. Results for MOREL were taken from its paper. \(*\) indicates $p < 0.05$ for Welch’s t-test for gain over MOPO. \(^\dagger\) Run on our codebase. \(^\ddagger\) Authors used D4RL v2, which has more performant offline data.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Discovered Hyperparameters</th>
<th>Optimized(^1)</th>
<th>MOPO(^1)</th>
<th>MOPO(^2)</th>
<th>MOREL(^\ddagger)</th>
<th>COMBO</th>
</tr>
</thead>
<tbody>
<tr>
<td>HalfCheetah</td>
<td>N: 10, h: 6.64, (\lambda): 12</td>
<td>Tmax Aleatoric</td>
<td>31.7 ± 1.5</td>
<td>32.7 ± 1.7</td>
<td>35.4</td>
<td>25.6</td>
</tr>
<tr>
<td></td>
<td>N: 11, h: 0.96, (\lambda): 37</td>
<td>Ensemble Var</td>
<td>58.0 ± 2.3</td>
<td>52.8 ± 1.1</td>
<td>53.1</td>
<td>40.2</td>
</tr>
<tr>
<td></td>
<td>N: medium, h: 5.92, (\lambda): 6</td>
<td>Ensemble Var</td>
<td>45.7 ± 2.6</td>
<td>46.5 ± 0.7</td>
<td>42.3</td>
<td>42.1</td>
</tr>
<tr>
<td></td>
<td>N: med.-exp., h: 4.56, (\lambda): 5</td>
<td>Max Aleatoric</td>
<td>104.2 ± 5.7</td>
<td>67.6 ± 23.6</td>
<td>63.3</td>
<td>53.3</td>
</tr>
<tr>
<td>Hopper</td>
<td>N: random, h: 4.46, (\lambda): 47</td>
<td>Ensemble Std</td>
<td>12.1 ± 0.2</td>
<td>4.2 ± 1.5</td>
<td>11.7</td>
<td>53.6</td>
</tr>
<tr>
<td></td>
<td>N: mixed, h: 5.90, (\lambda): 5</td>
<td>Max Aleatoric</td>
<td>90.8 ± 11.1</td>
<td>66.7 ± 27.8</td>
<td>67.5</td>
<td>93.6</td>
</tr>
<tr>
<td></td>
<td>N: medium, h: 37.28, (\lambda): 42</td>
<td>Ensemble Std</td>
<td>69.3 ± 15.2</td>
<td>17.3 ± 6.3</td>
<td>28.0</td>
<td>95.4</td>
</tr>
<tr>
<td></td>
<td>N: med.-exp., h: 39.08, (\lambda): 43</td>
<td>Max Aleatoric</td>
<td>105.8 ± 1.2</td>
<td>24.9 ± 5.5</td>
<td>23.7</td>
<td>108.7</td>
</tr>
<tr>
<td>Walker2d</td>
<td>N: random, h: 0.21, (\lambda): 12</td>
<td>Ensemble Var</td>
<td>21.7 ± 0.1</td>
<td>13.6 ± 1.4</td>
<td>13.6</td>
<td>37.3</td>
</tr>
<tr>
<td></td>
<td>N: mixed, h: 2.48, (\lambda): 47</td>
<td>Ensemble Std</td>
<td>65.8 ± 17.4</td>
<td>37.6 ± 20.6</td>
<td>39.0</td>
<td>49.8</td>
</tr>
<tr>
<td></td>
<td>N: medium, h: 5.28, (\lambda): 14</td>
<td>Ensemble Std</td>
<td>79.7 ± 2.3</td>
<td>-0.1 ± 0.0</td>
<td>17.8</td>
<td>77.8</td>
</tr>
<tr>
<td></td>
<td>N: med.-exp., h: 12.99, (\lambda): 37</td>
<td>Ensemble Std</td>
<td>97.1 ± 4.9</td>
<td>46.2 ± 27.0</td>
<td>44.6</td>
<td>95.6</td>
</tr>
<tr>
<td></td>
<td>N: - , h: -</td>
<td>Ensemble Var</td>
<td>65.2 ± 5.4</td>
<td>34.2 ± 9.8</td>
<td>36.7</td>
<td>64.4</td>
</tr>
</tbody>
</table>

Testing the limits of current approaches. Next, we wish to further validate that our earlier theoretical analysis can correspond to strong empirical performance gains by performing BO over the key hyperparameters. Details on the BO algorithm are listed in App. G. We define our search space over hyperparameters most related to uncertainty quantification:

- **Penalty type (categorical):** taking values over \{Max Aleatoric, Max Pairwise Diff, LOO KL, LL Var, Ensemble Std, Ensemble Variance\}.
- **Penalty scale \(\lambda\) (continuous):** taking values over \([1, 100]\).
- **h (integer):** taking values over \([1, 2, \ldots, 50]\).
- **Models N (integer):** taking values over \([1, 2, \ldots, 15]\).

Table 3 shows the optimal hyperparameters under BO. We note that Ensemble penalties are mainly selected, corroborating the findings in our analysis that these are most correlated with model error. We observe that Max Pairwise Diff is not chosen, likely because ensemble penalties are better correlated with true dynamics error, and are more stable under tuning since their scaling changes less with model number; we know that Max Pairwise Diff has very similar shape statistics to Ensemble Std. (App. C). Finally, we also observe these solutions have lower performance variance than MOPO.

The selection of Max Aleatoric is also explainable; we observe it displays significantly lower skew and kurtosis than all other metrics (App. C), while still maintaining strong rank correlation. We also found that in all Hopper experiments, Ensemble Var. never achieved high performance, despite the only difference with Ensemble Std. being its distributional shape. Interestingly, in HalfCheetah, the opposite is true, with Ensemble Var. delivering significant performance gains. This implies that distributional shape may play as important a role as calibration, and advocates the learning of *meta-parameters* that control for this. Finally, in Walker2d, the well-grounded ensemble penalties win in all cases. We note that values of the rollout horizon \(h\) and penalty weight \(\lambda\) differ greatly from those chosen in the original MOPO paper, which chooses both from \([1, 5]\). Notably, the Hopper and Walker2d environments can prefer a much longer rollout length and higher penalty weight, even accounting for penalty magnitudes. Again this is backed up by our analysis; along a single rollout, dynamics errors do not necessarily accumulate, they simply become more likely to occur. Therefore, as long as we penalize errors appropriately, we can handle longer rollouts and, as a result, generate more on-policy data. The number of models used to compute the uncertainty estimates can also differ greatly from the standard 7. This again aligns with our findings that using more models for uncertainty estimation can be beneficial, but is dependent on environment, data, and penalty.

Table 3 also demonstrates how these unconventional hyperparameter choices fare against state-of-the-art offline MBRL algorithms. We spent considerable effort ensuring that our implementation of MOPO matched the authors’ results using the same hyperparameters. We note the two are very similar\(^2\), thereby allowing us to make a faithful comparison when modifying hyperparameters. Our approach, labeled “Optimized\(^1\)”, achieves *statistically significant* improvements over MOPO on 9

\(^1\)There was a disparity in Walker2d-medium, but this was also noted in Ball et al. (2021)
out of 12 environments, validating our prior analysis over the key design choices. As an additional bonus, and it is not the stated aim of this work, our approach achieves state-of-the-art performance on five HalfCheetah and Walker2d environments by a considerable margin. Further notable results include the Hopper mixed and Hopper medium-expert environments, in which we show we are able to tune the MOPO-like method up to the performance of COMBO (Yu et al., 2021) and MOREL. The importance of good uncertainty estimation and hyperparameter selection is shown visually in Fig. 4 where we improve MOPO performance by over 5× whilst obtaining a stable solution.

As aforementioned, we found our policies are more stable than previous works and consequently do not need to cherry-pick high performing checkpoints. Instead, we report the average performance over our final 10 policy-improvement iterations. It should be noted that stability during training (Chan et al., 2020) is paramount for successful policy deployment in offline RL, and we should therefore prioritize hyperparameters that ensure this. We further confirm the reliability of our evaluation using the reliable framework (Agarwal et al., 2021) in Fig. 1b, showing that the improvement over MOPO (with 95% bootstrap CIs shaded) is clear in both MuJoCo and Adroit.

Results on Adroit dexterous hand manipulation tasks. We present results in Table 4 on the Adroit Pen and Hammer environments which, as far as we are aware, have not previously been used in offline MBRL, and present very different challenges to the locomotion tasks. These tasks feature sparse rewards, real human demonstrations and narrow data distributions. We compare against the current state-of-the-art model-free algorithm (CQL, Kumar et al. (2020)) and find that offline MBRL can learn useful policies in the Adroit domains, providing the best performance seen so far on the hammer-cloned setting. Best found penalties and hyperparameters are listed in App. J, and mirror the findings in the locomotion experiments. We believe issues with the world model not accurately capturing sparse rewards may account for any major performance difference. Our work is therefore an important step towards bridging the gap between model-based and model-free methods for sparse reward tasks, especially in the offline setting where exploration is not possible. We define MOPO to be the best performance with the Max Aleatoric penalty, searching \( \lambda, h \) in \{1, 5\}².

7 Conclusion

In this paper, we rigorously evaluated the impact of various key design choices on offline MBRL, comparing for the first time a number of different uncertainty penalties used in the literature. By proposing novel evaluation protocols, we have also gained key insights into the nature of uncertainty in offline MBRL that we believe benefits the RL community. We demonstrated the impact of this analysis by significantly improving upon existing offline MBRL by using vastly different key hyperparameters, obtaining statistically significant performance improvements in almost all benchmarks.

Going forward, we are excited by developments in offline evaluation (Chen et al., 2021; Fu et al., 2021b) to accurately assess agent performance without querying the environment. This would open the door for population-based training methods (Jaderberg et al., 2017; Parker-Holder et al., 2020), which have shown great success in online MBRL (Zhang et al., 2021). Furthermore, throughout the paper we have highlighted potential areas of interest, from better understanding the generalization provided by world models, through to the development of meta-parameters controlling penalty distribution shape. We also highlight key issues in implementation in App. F as we strongly believe this is a vital frontier for disentangling the effect of algorithmic innovations from code-level details. Finally, Offline MBRL so far has only focused on deterministic environments; the ensemble penalties we investigate support the modeling of stochastic dynamics, and the novel tools for analysis we develop here can be readily applied to such settings.

### Table 4: Comparative evaluation on the D4RL Adroit v0 dataset against Model Free CQL

<table>
<thead>
<tr>
<th>Environment</th>
<th>MOPO†</th>
<th>Optimized†</th>
<th>CQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>pen</td>
<td>cloned</td>
<td>5.4 ±10.8</td>
<td>23.0 ±4.2</td>
</tr>
<tr>
<td>human</td>
<td>human</td>
<td>6.2 ±7.8</td>
<td>19.0 ±7.9</td>
</tr>
<tr>
<td>expert</td>
<td>expert</td>
<td>15.1 ±9.7</td>
<td>50.6 ±10.5</td>
</tr>
<tr>
<td>hammer</td>
<td>cloned</td>
<td>0.2 ±0.1</td>
<td>5.2 ±1.5</td>
</tr>
<tr>
<td>human</td>
<td>human</td>
<td>0.2 ±0.0</td>
<td>0.5 ±0.8</td>
</tr>
<tr>
<td>expert</td>
<td>expert</td>
<td>6.2 ±8.4</td>
<td>23.3 ±4.1</td>
</tr>
</tbody>
</table>

*It is unclear what procedure is used in some prior work (indeed issues have been raised about this).*
ACKNOWLEDGMENTS

The authors would like to acknowledge Rishabh Agarwal for helpful feedback during the project. We would also like to thank the anonymous reviewers for their constructive feedback, which helped to improve the paper. Cong Lu is funded by the Engineering and Physical Sciences Research Council (EPSRC). Philip J. Ball is funded through the Willowgrove Studentship.

REFERENCES


Jean-Baptiste Mouret and Jeff Clune. Illuminating search spaces by mapping elites, 2015.


A Calibration

A.1 Choice of calibration metrics

We consider both the Spearman rank ($\rho$) correlation and Pearson bivariate ($r$) correlation. We believe that the former better represents the actual statistical power of the metric compared to the true distributional shift value, as it is robust to outliers and isn’t impacted by distributional shape (i.e., skewness, kurtosis). After all, we do not know if some ‘true’ $|G^\pi_M(s, a)|$ is even linearly correlated with the MSE values that we report, so naively comparing based on bivariate correlation may result in incorrect assessment of penalty efficacy. However, we do also include the Pearson bivariate correlation to gain insight into how the penalty distribution shape changes with design choices. For instance, consider two metrics that have identical Spearman coefficients, but vastly different Pearson coefficients—this implies they have significantly different distributional shapes whilst having the same statistical ranking power. The two correlation coefficients have the further advantage that they are unaffected by the scale of the uncertainty penalty, which can vary widely. Furthermore, algorithms such as MOPO and MOReL will often scale the penalty by some coefficient $\lambda$ and thus the raw unscaled value is hard to interpret.

A.2 The use of MSE as the ground truth for deterministic dynamics

Following Yu et al. (2020), it is possible upper bound the expected performance $\eta_M$ of a policy $\pi$ in the true MDP $M$ under training in a world model MDP $\hat{M}$ as follows:

$$\eta_M(\pi) \geq \mathbb{E}_{(s,a) \sim \rho^\pi_P}[R(s,a) - \gamma|G^\pi_M(s, a)|]$$  \hspace{1cm} (2)$$

where $R(\cdot, \cdot)$ is the reward function, $\rho^\pi_P$ represents transitioning under the world model dynamics $\hat{P}$ and policy $\pi$. The quantity $|G^\pi_M(s, a)|$ can be upper-bounded by an integral probability metric (IPM):

$$|G^\pi_M(s, a)| \leq \sup_{f \in \mathcal{F}} \left| \mathbb{E}_{s' \sim P(s,a)}[f(s')] - \mathbb{E}_{s' \sim \hat{P}(s,a)}[f(s')] \right| =: d_{\mathcal{F}}(\hat{P}(s,a), P(s,a))$$  \hspace{1cm} (3)$$

where $\mathcal{F}$ is some set of functions mapping $S$ to $R$, and $P$ is the dynamics under the true MDP $M$. As noted in Yu et al. (2020), making assumptions over the functional form of $\mathcal{F}$ induces different distance measures. Restricting $\mathcal{F}$ to the set of 1-Lipschitz functions results in an IPM with the following form:

$$|G^\pi_M(s, a)| \leq cW_1(\hat{P}(s,a), P(s,a))$$  \hspace{1cm} (4)$$

which is the 1-Wasserstein distance, where the constant $c$ is the Lipschitz constant of the value function $V_M$ with respect to a norm $\|\cdot\|$. Recalling that the environments we evaluate have deterministic dynamics (Todorov et al., 2012), this means the dynamics distributions $P$ and $\hat{P}$ in Eq. 4 are Dirac delta functions. In this case, the 1-Wasserstein distance simply reduces to the 2-norm between some ‘true dynamics’ $T(s, a)$ and the ‘estimated dynamics’ $\hat{T}(s, a)$. This justifies the use of MSE between the oracle dynamics (as detailed in Sec. 4.1 and App. D.1) and the world model dynamics as the ground truth measure under which we assess calibration.
A.3 Offline Dataset Transfer Calibration

We present the full calibration scatter plots described in Sec. 4.2. Concretely, we plot penalty values on the y-axis, and ground-truth MSE on the x-axis. First, we present the transfer performance of training sets onto offline datasets. Then, we present the results for all training datasets under the True Model-Based experiment under the adversarial policies.

A.3.1 HalfCheetah

Figure 5: Scatter Plots showing HalfCheetah D4RL transfer tasks.
A.3.2 HOPPER

Figure 6: Scatter Plots showing Hopper D4RL transfer tasks.
A.4 True Model-Based Error Calibration

A.4.1 HalfCheetah

Figure 7: Scatter Plots showing HalfCheetah D4RL true model-based error calibration.
A.4.2 HOPPER

![Figure 8: Scatter Plots showing Hopper D4RL true model-based error calibration.](image)

A.5 ADDITIONAL LOG PROBABILITY CORRELATION ANALYSIS

Table 5 shows correlation between reward penalties and the negative log-likelihood of the true data under the model in the Transfer experiments.

<table>
<thead>
<tr>
<th>Transfer</th>
<th>HalfCheetah</th>
<th>Hopper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalty</td>
<td>ρ</td>
<td>r</td>
</tr>
<tr>
<td>Max Aleatoric</td>
<td>0.87±0.00</td>
<td>0.82±0.01</td>
</tr>
<tr>
<td>Max Pairwise Diff.</td>
<td>0.79±0.01</td>
<td>0.62±0.00</td>
</tr>
<tr>
<td>Ens. Std.</td>
<td>0.93±0.00</td>
<td>0.86±0.01</td>
</tr>
<tr>
<td>Ens. Var.</td>
<td>0.90±0.01</td>
<td>0.74±0.01</td>
</tr>
<tr>
<td>LL Var.</td>
<td>0.04±0.07</td>
<td>0.07±0.03</td>
</tr>
<tr>
<td>LOO KL</td>
<td>-0.04±0.06</td>
<td>-0.02±0.04</td>
</tr>
</tbody>
</table>
B Full Results Increasing Models

B.1 Penalty Distribution

In this section we provide the full set of results showing the impact of increasing model count on the distribution quantile statistics as introduced in Sec. 5.1. We show inter-quartile range and the median (the latter being denoted by a black vertical line) of each penalty as a function of increasing model number across all training domains and test settings. First, we present the transfer performance of all training sets onto all offline datasets. Then, we present the results for all training datasets under the True Model-Based experiment under the adversarial policies.

B.1.1 Offline Dataset Transfer Distribution

Figure 9: Box Plots showing HalfCheetah D4RL transfer tasks.
Figure 10: Box Plots showing Hopper D4RL transfer tasks.
B.1.2 True Model-Based Error Distribution

Figure 11: Boxplots showing HalfCheetah D4RL true model-based error penalty distributions.
Figure 12: Boxplots showing Hopper D4RL true model-based error penalty distributions.
B.2 PENALTY PERFORMANCE

In this section, we provide the full set of results showing the impact of increasing model count on the correlation statistics of each penalty, as described in Sec. 5.1. We show the Spearman and Pearson correlation between penalty and ground truth MSE for all training datasets. First, we present the transfer performance of all training sets onto all offline datasets. Then, we present the results for all training datasets under the True Model-Based experiment under the adversarial policies.

B.2.1 HALF CHEETAH D4RL: TRANSFER

Figure 13: HalfCheetah Spearman Statistics
Figure 14: HalfCheetah Pearson Statistics
B.2.2 **HOPPER D4RL: TRANSFER**

![Figure 15: Hopper Spearman Statistics](image-url)
Figure 16: Hopper Pearson Statistics
B.2.3 HalfCheetah D4RL: True Model-Based Error

Figure 17: HalfCheetah Spearman Statistics

Figure 18: HalfCheetah Pearson Statistics

B.2.4 Hopper D4RL: True Model-Based Error

Figure 19: Hopper Spearman Statistics

Figure 20: Hopper Pearson Statistics
### B.2.5 All Aggregated

![Figure 21: Aggregated True Model-Based correlation statistics over all datasets (i.e., Random through to Expert); Left: HalfCheetah; Right: Hopper](image)

#### C Skewness and Kurtosis Comparisons

##### C.1 Skewness and Kurtosis Overall

Here we present the 3rd and 4th order statistics (skew and kurtosis respectively) of each penalty, illustrating that even with identical model counts, the shape statistics between penalties are vastly different.

<table>
<thead>
<tr>
<th>Penalty</th>
<th>HalfCheetah</th>
<th>Hopper</th>
<th>HalfCheetah</th>
<th>Hopper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Aleatoric</td>
<td>-0.010</td>
<td>0.580</td>
<td>0.689</td>
<td>1.377</td>
</tr>
<tr>
<td>Max Pairwise Diff.</td>
<td>0.919</td>
<td>0.957</td>
<td>1.967</td>
<td>4.578</td>
</tr>
<tr>
<td>Ensemble Std.</td>
<td>0.794</td>
<td>0.806</td>
<td>2.136</td>
<td>6.560</td>
</tr>
<tr>
<td>Ensemble Var.</td>
<td>1.823</td>
<td>4.830</td>
<td>3.436</td>
<td>15.983</td>
</tr>
<tr>
<td>LL Var.</td>
<td>6.893</td>
<td>114.843</td>
<td>10.920</td>
<td>180.716</td>
</tr>
<tr>
<td>LOO KL</td>
<td>1.778</td>
<td>5.729</td>
<td>3.729</td>
<td>29.606</td>
</tr>
</tbody>
</table>

#### C.2 Skew and Kurtosis Scaling with Model Count

We omit LL Var. and LOO KL due to the fact that their changes were so significant as to obfuscate the changes of the more performant penalties.

We choose 7 models, as in Table 6, to act as our 'baseline' (following the default MOPO setting), and we measure the change in the skew and kurtosis relative to this, hence 7 models always has a 0% change in our graphs. For brevity, in the transfer experiments, we average over all ‘transferred to’ environments, e.g., Random, Medium, etc.; the graph title refers to the data that the model was trained on.

Again, we observe the environment and setting dependency of these metrics, sometimes having increasing skewness and kurtosis with model count, and other times decreasing. This further justifies using a ranking metric to compare penalties, as the overall penalty shape can vary hugely and unpredictably w.r.t. co-dependent hyperparameters. We do observe however in the True Model-Based experiments that ensemble standard deviation appears to be most robust to scaling with models. We also observe that the Max Aleatoric penalty can change shape significantly w.r.t. model count, and no penalties are fully immune to this. This further advocates the use of shape meta-parameters to control for changing distribution properties when adjusting the number of models as a hyperparameter, as well as selecting penalties that are relatively invariant to model count to make tuning easier.
Figure 22: HalfCheetah Transfer.

Figure 23: Hopper Transfer.
Figure 24: HalfCheetah True Model-Based.

Figure 25: Hopper True Model-Based.
D  **FURTHER DETAILS ON TRUE MODEL-BASED EXPERIMENTS**

D.1  **METHODOLOGICAL DETAILS**

We leverage the MuJoCo (Todorov et al., 2012) simulator to provide us with ground truth dynamics that we can use to compare against our model predictions and penalties. This is done by providing the state and action inputs given to the model to the simulator through the `set_state` method in the simulator API. It must be noted that this method also requires an addition ‘displacement’ value which is not modelled by the world models (nor is it provided in the D4RL data), however we found in practice this did not affect the dynamics predicted by the simulator, and simply setting this to 0 was sufficient to generate ground truth predictions.

This makes it possible to provide the simulator the hallucinated model states, and provide a true proxy to the *dynamics* discrepancy. We note that since the states are ‘hallucinated’ by the model, it might be the case that they may not be admissible under the true environment, but in reality the simulator was able to process almost any combination of state and action, barring settings that featured anomalously large magnitudes. To handle such cases, we found it necessary to clip the model states to the range $[-10, 10]$.

In order to assess the permissibility of states, as well as measure the accuracy of the penalties as OOD input detectors, we provide an alternative distance measure based on the distance away from the training set. We use this measure for our analysis in Section 5.3, and is calculated as the distance from the offline training dataset, which we define to be the 2-norm between a given state-action tuple and its nearest point in the offline data, a similar metric to those used in recent works on imitation learning (Dadashi et al., 2021). We describe this quantity henceforth as ‘Distribution Error’.

D.2  **ON THE NATURE OF OOD DATA ALONG HALLUCINATED TRAJECTORIES**

Here we discuss the nature of OOD data along a single hallucinated trajectory (in the model) in offline MBRL, analyzing the inductive bias that some ‘error’ increases with increasing rollout length in the model. We find that there is merit to this assumption, and show this in Fig. 26 for all HalfCheetah and Hopper environments in D4RL. Here, we plot the median error at each time-step across 30,000 aggregated trajectories in the model. Note that for all plots, we re-normalize all penalties by subtracting their mean and dividing by their standard deviation to facilitate comparison; this normalization was also applied in the analysis performed in Fig. 1a. Concretely, each time step corresponds to the normalized median value of 30,000 data-points.

![Figure 26: Median True Model-Based Errors as a function of rollout timestep](image)

We observe indeed that both median dynamics and distribution errors increase with increasing time step in the model. The only real exception is HalfCheetah Medium-Expert, which we believe to be due to our trained policy not being able to successfully exploit this environment.

The above analysis captures *overall trends* in the error over a large number of trajectories. However, the way errors manifest during an *individual rollout* is not so straightforward. To illustrate this,
observe Fig. 27, where we plot a random subset of 5 individual rollouts from the Hopper Medium-Expert data we generated.

Figure 27: Several Individual Ground Truth Rollouts in Hopper Medium-Expert

We observe that errors along any single trajectory tend to manifest as ‘spikes’, and that it is entirely possible to recover from these, returning to either admissible dynamics, or parts of the state-action space that have been seen in the data. This speaks to the nature of how we ought to penalize policies for accessing regions of inaccuracy/uncertainty, and may justify a hybrid MOPO/MOReL approach, whereby we penalize individual transitions along a trajectory, but do not stop rollouts early. Indeed, this is similar to the approach taken in M2AC (non-stop), albeit they choose to ‘mask’ uncertain transitions, not penalize them. We leave the design of such an algorithm to future work.

Finally, we address the issue of comparing OOD dynamics and inputs. As already observed in Fig. 27, these two errors are not necessarily always the same, and oftentimes it is possible that one quantity is large, whilst the other is small. We revisit Fig. 1a to explore this, now also plotting the Distribution Error in Fig. 28.

Figure 28: Comparing OOD dynamics and inputs on a Hopper Medium-Expert trajectory

We first speak to the inset annotated ‘1’. Here we observe that the transitions generated in fact closely resemble the data that our model was trained on, however the predicted dynamics are incorrect, and cause an aforementioned ‘spike’. This is the opposite of what is observed in the inset annotated ‘2’; where we actually predict accurate dynamics, however the resultant state-action tuples do not closely resemble the data that our model was trained on. We generally observe that regions of high Distribution Error tend to be preceded by ‘spikes’ pertaining to high Dynamics Error, and this present an exciting avenue for future work understanding how these quantities are related.

D.3 ON THE DIVERSITY OF EXPLOITATIVE POLICIES

It is possible that training policies purely to exploit the world models may result in generating state-action tuples that are low in diversity, as the policy could discover "pockets" in the model that provide consistently high return. To prevent this, we train multiple policies inside the model from different seeds, with the aim of inducing different modes of exploitation. To validate this induces diverse trajectories in the world models, we visualize the state-action manifold using a t-SNE projection (van der Maaten & Hinton, 2008) of: 1) the D4RL Hopper Mixed-Replay (which contains diverse samples); 2) the imagined rollouts inside the model from the exploitative policies in Fig. 29. The policies were trained to exploit a model that itself was trained on the Hopper Mixed-Replay data.
We observe that the induced policies inside the model displays some overlap with the D4RL data, but also resides in parts of the manifold where there is little coverage from the D4RL data, likely representing regions of exploitation. Importantly, the exploitative WM trajectories display strong state-action tuple diversity, comparable to that of the offline data it was trained on.

## E Using metrics as OOD event detectors

### E.1 Measuring Statistics

As noted previously, different penalties have varying scales and distribution profiles, so we need a way of standardizing the method of assessment. Using our observation that errors manifest as ‘spikes’ during a rollout, we propose treating each penalty as a classifier. Concretely, our test set consists of the ground truth data labeled by whether or not they exceed a certain percentile at a particular time step. Each penalty may be then be treated as a ‘classifier’ by normalizing its range to lie in $[0, 1]$. We can then use standard classification quality measures, such as AUC, to determine the effectiveness of these penalties at capturing these spikes, whilst sidestepping the issue of the different distributional profiles identified previously.

Fig. 30 shows how our proposed method may be used to compare the effectiveness of each metric at capturing OOD events. In the figure, we plot a single rollout in the model, and the resultant ground truth MSE between the predicted next state and the true next state in black. We then superimpose the 90th, 95th and 99th percentile MSEs across the entire imagined trajectories onto the figure in gray dashed lines. To construct our OOD labels, we label any point below the percentile line as being ‘False’, and any point above that line as being ‘True’. Finally, we normalize the uncertainty metrics as previously described into values in the range $[0, 1]$, allowing us to construct precision-recall graphs and calculate classifier statistics.
E.2 PRECISION RECALL CURVES

In this section we present the Precision-Recall curves described in App. E.1.

Figure 31: Precision Recall curves on ground truth data.
F IMPLEMENTATION DETAILS

This paper extensively discusses key hyperparameters specific to current offline MBRL algorithms. However, there are significant code-level implementation details which are often critical for strong performance and make it hard to disambiguate between algorithmic and implementation improvements. Worryingly, many of these details are not mentioned in their respective papers, or are different between the authors’ code and paper. We detail clear examples of this below. We believe further investigation of these code-level implementation details represents important future work, as has already been done for policy gradients (Engstrom et al., 2020; Andrychowicz et al., 2021). Indeed – it is unclear if the improvement of MOReL over MOPO is due to its different P-MDP formulation, or if it is successful in spite of this formulation, due to a superior policy optimization strategy or dynamics model design. We believe that this paper takes a significant first step in tackling this issue by directly comparing a number of key design choices, and understanding their individual impact. Now we summarize key differences between the paper and code for the MOPO and MOReL algorithms which we compare against that are crucial to achieve the same reported performance.

In MOPO,
- Each layer in the model neural network has a different level of weight-decay
- The authors’ code uses different objectives for training (log-likelihood) and validation (MSE).
- The authors use elites, but only for next state prediction (as discussed previously).

In MOReL,
- There is a difference in the authors’ code about how the penalty threshold is calculated and tuned, and isn’t provided as a hyperparameter in the appendix.
- The absorbing HALT state does not appear in the authors’ code.
- The negative halt penalty appears significantly different between code and paper.
- There is a minimum trajectory steps parameter (hard-coded to 4) not mentioned in the paper.
- The reward function appears to be hard-coded in the authors’ implementation, not learned as stated in the paper.
- The policy architecture is different in the authors’ code (64,64 hidden layers) and the paper (32,32 hidden layers)
- It is not clear when the optional behavior cloning initialization step is applied.

G HYPERPARAMETERS AND EXPERIMENT DETAILS

The D4RL (Fu et al., 2021a) codebase and datasets used for the empirical evaluation is available under the CC BY 4.0 Licence. As stated in the main text, we choose to use ‘v0’ experiments as these are more challenging for Hopper due to having low return trajectories (Kostrikov et al., 2021), and we clearly state when other benchmarks use the ‘v2’ experiments, which have offline trajectories with higher returns on Hopper.

The remaining hyperparameters for the MOPO algorithm that we do not vary by Bayesian Optimization were taken from the original MOPO paper (Yu et al., 2020), apart from we fix the number of policy epochs/iterations to 1,000 for all experiments. This means our implementation uses the same probabilistic dynamics models (with unchanged hyperparameters) and policy optimizer (SAC, Haarnoja et al. (2018)) as MOPO, differing from MOReL, which uses Natural Policy Gradient (Kakade, 2002).

The hyperparameters used for the BO algorithm, CASMOPOLITAN, are listed in Table 7. We use the batch-mode of CASMOPOLITAN, where multiple hyperparameters settings are proposed and evaluated concurrently.

Each BO iteration is run for 300 epochs on a single seed, and the full optimization over an offline dataset took ~200 hours on a NVIDIA GeForce GTX 1080 Ti GPU taken up predominantly by MOPO training.
Table 7: CASMOPOLITAN Hyperparameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of parallel trials</td>
<td>4</td>
</tr>
<tr>
<td>Number of random initializing points</td>
<td>20</td>
</tr>
<tr>
<td>ARD</td>
<td>False</td>
</tr>
<tr>
<td>Acquisition Function</td>
<td>Thompson Sampling</td>
</tr>
<tr>
<td>Global BO</td>
<td>True</td>
</tr>
<tr>
<td>Kernel</td>
<td>CoCaBo Kernel (Ru et al., 2020)</td>
</tr>
</tbody>
</table>

Unless specified otherwise, plots and reported statistics are completed with 7 models in the ensemble, as this is the number chosen in the original MOPO paper used with the Max Aleatoric penalty.

H R I L I A B L E FRAMEWORK FOR PERFORMANCE EVALUATION

Throughout this work, we choose to adopt the reliable framework introduced in Agarwal et al. (2021) to evaluate the performance of our approaches. reliable advocates for computing aggregate performance statistics and probability of improvement across many tasks in a benchmark suite; indeed we take this approach when reporting the values in the analysis performed in Sections 4 and 5. This is important when the number of tasks become large, and also prevents outliers from dominating mean statistics. Furthermore, this allows us to make clear statements about improvements given the relatively low number of seeds that are used in deep RL; indeed, Agarwal et al. (2021) show that even using high seed counts does not ameliorate the variance issues experienced when training such algorithms. For normalization, we use the standard D4RL return scaling.

I E V A L U A T I O N USING AUTOMATIC CONSTRAINT TUNING

We show the full tabulated results from Sec. 6 with statistical significance using the reliable framework in Table 8, using the ‘Probability of Improvement’ metric in Agarwal et al. (2021). To evaluate our claims in Sections 4 and 5 without needing to laboriously tune the penalty weight λ per environment, we employ an automatic penalty tuning scheme, analogous to the automatic entropy tuning used in Haarnoja et al. (2018). Concretely, given a constraint value Λ, at each epoch we minimize:

\[ J(\lambda) = \mathbb{E}_{s_t, a_t \sim D} \left[ \log \lambda (\Lambda - \lambda \cdot u(s_t, a_t)) \right] \]  

(5)

We start from an initial weight \( \lambda = 1 \). We observe that the penalty weight found by automatic tuning tends to converge within the first 50 epochs and then remains stable throughout training.

Table 8: Improvement over grid-searched MOPO through restricted hyperparameter choices (e.g., one single choice, or an arg max between two) on the D4RL MuJoCo benchmark. The single and two setup approaches both use the Ensemble Std. penalty and \( N = 10 \).

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Average Score</th>
<th>P[Improvement over MOPO]</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOPO (default hyperparameters)</td>
<td>34.2</td>
<td>-</td>
</tr>
<tr>
<td>Single setup: (h = 20, Λ = 1)</td>
<td>49.0 (+43%)</td>
<td>73.96%</td>
</tr>
<tr>
<td>Two setups: arg max{(h = 10, Λ = 0.5), (h = 20, Λ = 1)}</td>
<td>57.8 (+69%)</td>
<td>80.20%</td>
</tr>
<tr>
<td>Optimized MOPO (ours, Table 3)</td>
<td>65.2 (+91%)</td>
<td>89.06%</td>
</tr>
</tbody>
</table>
We present the best found hyperparameters under our BO procedure for the D4RL Adroit tasks in Table 4. We see similar trends as in our main evaluation in Table 3 favoring higher rollout lengths and the Ensemble penalties.

Table 9: Best discovered hyperparameters using BO for Adroit

<table>
<thead>
<tr>
<th>Environment</th>
<th>Discovered Hyperparameters</th>
<th>N</th>
<th>λ</th>
<th>h</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>pen cloned</td>
<td>10</td>
<td>6.64</td>
<td>12</td>
<td>Ensemble Std</td>
<td></td>
</tr>
<tr>
<td>pen human</td>
<td>11</td>
<td>0.96</td>
<td>37</td>
<td>Ensemble Var</td>
<td></td>
</tr>
<tr>
<td>pen expert</td>
<td>7</td>
<td>4.56</td>
<td>5</td>
<td>Max Aleatoric</td>
<td></td>
</tr>
<tr>
<td>hammer cloned</td>
<td>10</td>
<td>0.21</td>
<td>12</td>
<td>Ensemble Var</td>
<td></td>
</tr>
<tr>
<td>hammer human</td>
<td>13</td>
<td>2.48</td>
<td>47</td>
<td>Ensemble Std</td>
<td></td>
</tr>
<tr>
<td>hammer expert</td>
<td>12</td>
<td>0.99</td>
<td>37</td>
<td>Ensemble Std</td>
<td></td>
</tr>
</tbody>
</table>