Distributionally Robust Model-based Reinforcement Learning with Large State Spaces

Shyam Sundhar Ramesh
University College London

Pier Giuseppe Sessa
ETH Zurich

Yifan Hu
EPFL

Andreas Krause
ETH Zurich

Ilija Bogunovic
Univeristy College London

Abstract

Three major challenges in reinforcement learning are the complex dynamical systems with large state spaces, the costly data acquisition processes, and the deviation of real-world dynamics from the training environment deployment. To overcome these issues, we study distributionally robust Markov decision processes with continuous state spaces under the widely used Kullback–Leibler, chi-square, and total variation uncertainty sets. We propose a model-based approach that utilizes Gaussian Processes and the maximum variance reduction algorithm to efficiently learn multi-output nominal transition dynamics, leveraging access to a generative model (i.e., simulator). We further demonstrate the statistical sample complexity of the proposed method for different uncertainty sets. These complexity bounds are independent of the number of states and extend beyond linear dynamics, ensuring the effectiveness of our approach in identifying near-optimal distributionally-robust policies. The proposed method can be further combined with other model-free distributionally robust reinforcement learning methods to obtain a near-optimal robust policy. Experimental results demonstrate the robustness of our algorithm to distributional shifts and its superior performance in terms of the number of samples needed.

Proceedings of the 27[th] International Conference on Artificial Intelligence and Statistics (AISTATS) 2024, Valencia, Spain. PMLR: Volume 238.

1 INTRODUCTION

The use of reinforcement learning (RL) algorithms is gaining momentum in various complex domains, including robotics, nuclear fusion, and molecular discovery. Data acquisition in such environments can be a challenging and resource-intensive process. Safety considerations may also limit the amount of data that can be collected through interactions with the environment. To address this issue, a commonly adopted approach is to train RL policies using a simulator (generative model) enabling RL agents to learn from a simulated environment.

Dealing with complex applications that involve large state spaces requires data-efficient learning, even when a simulator is available. However, achieving optimal policies using existing approaches often requires a significant amount of training data, making data-efficient learning an ongoing challenge. Additionally, when deploying a policy to a real-world system, it is crucial to ensure its performance remains reliable despite mismatches between the simulator and the real-world system. Such mismatches can arise from approximation errors, time-varying system parameters, or even due to adversarial influence. For example, in self-driving, it is infeasible to precisely model all possible variables, such as road conditions, brightness, and tire pressure, which can all vary over time. The resulting mismatch, known as the 'sim-to-real gap', can diminish the performance or impact the reliability of RL algorithms trained on a simulator model.

In this work, we examine the use of a generative model in *distributionally-robust model-based reinforcement learning*. Our aim is to find a distributionally-robust policy that is near-optimal by actively querying the simulator with a state-action pair selected by the learning algorithm. To achieve this, we introduce the kernelized Maximum Variance Reduction (MVR) algorithm, which identifies a state-action pair with the highest un-

certainty according to the model to learn the nominal model dynamics. The algorithm produces a nominal dynamics estimate that is utilized within the robust Markov Decision Process (MDP) framework, where an uncertainty set that includes all models close (according to, e.g., Kullback Leibler divergence) to the learned one is considered. The overall protocol is summarized in Figure 1. We provide a thorough characterization of statistical sample complexity rates by utilizing the learned model to generate a near-optimal robust policy.

Related Work: Reinforcement learning with a generative model, introduced in Kearns et al. (2002), assumes access to a simulator that outputs the next state given any state-action pair. It appears frequently in the RL literature and is of signi cant practical relevance. Kakade (2003) elucidate various uses for this generative setting and analyze it in further detail. For the nite MDP case, such a generative setting has been subsequently studied in various works such as Kakade (2003); Gheshlaghi Azar et al. (2013); Li et al. (2020) and, recently, by Agarwal et al. (2020) who provide minimax optimality guarantees for the naive plug-in estimator based algorithm. For large state spaces, generative RL is typically combined with function approximation as studied, e.g., by Abbasi-Yadkori et al. (2019); Shari and Szepesvári (2020); Lattimore et al. (2020); Li et al. (2023). Recently, Mehta et al. (2021) consider generative RL in continuous state-action spaces from an experimental perspective and showcase the relevance of this setting to the nuclear fusion dynamics research. Degrave et al. (2022) study the tokamak magnetic control problem also using a generative simulator. In addition, Li et al. (2023) present an active exploration strategy that utilizes the least-squares value iteration. Their approach aims to identify a near-optimal policy across the entire state space, providing polynomial sample complexity guarantees that remain una ected by the number of states. In contrast to these works, we use generative RL to discoverdistributionally robust policies through the modeling of unknown transition dynamics, aiming to address the sim-to-real gap considering the uncertainty in transition dynamics.

The local accesssimulator setting, introduced in Yin et al. (2022), operates under a similar generative model framework. However, the input state to the simulator is restricted to the states already visited. In particular, Tkachuk et al. (2023) study such a setting and employ a model-free approach, focusing on learning the Q-function using an uncertainty-based algorithm. In contrast, our method utilizes the kernel estimator to construct a model of the transition dynamics, offering approximation guarantees. These guarantees are subsequently extended to ensure the robustness of the policy. The novelty of our approach lies in the proposed combination of employing the maximum variance reduction algorithm to learn transition dynamics and constructing a robust policy based on the learned transition dynamics resulting in sample e ciency.

In model-based reinforcement learning, the model learned from a simulator encounters two issues well discussed in the literature, namely, the model-bias (Deisenroth and Rasmussen, 2019; Clavera et al., 2018) and the simulation to reality (sim2real) gap (Andrychowicz et al., 2020; Peng et al., 2018; Mankowitz et al., 2019; Christiano et al., 2016; Rastogi et al., 2018; Wulfmeier et al., 2017). To address this from the perspective of distributional robustness, previous works (Zhou et al., 2021; Panaganti and Kalathil, 2022; Yang et al., 2022) have considered distributional robustness aspects in the context of nite Markov decision processes (MDPs) using the robust MDP framework from Iyengar (2005); Nilim and El Ghaoui (2005). Various other works utilize this robust MDP framework such as Xu and Mannor (2010); Wiesemann et al. (2013); Yu and Xu (2015); Mannor et al. (2016); Badrinath and Kalathil (2021); Petrik and Russel (2019) for the planning problem, and provide asymptotic guarantees for tabular and linear function approximators Lim et al. (2013); Tamar et al. (2014); Roy et al. (2017); Wang and Zou (2021). Our work is closely related to the recent works on distributionally robust RL (Zhou et al., 2021; Panaganti and Kalathil, 2022; Yang et al., 2022; Shi and Chi, 2022; Xu et al., 2023; Clavier et al., 2023; Shi et al., 2024). However, unlike ours, the sample complexity bounds established in these works rely on the number of states and actions, making them impractical for large or in nite state spaces.

A recent work (Blanchet et al., 2024) also consider an in nite state space setup with kernelized function approximation. They consider an o ine setting, where the data is already available with the partial coverage assumption satis ed, while we propose to actively collect data from the environment in the generative robust MDPs. Note that the partial coverage assumption introduces an additional variable (coverage coe cient) in their guarantees. Moreover, they propose to utilize the MLE method to estimate their model via o ine data. In comparison, we use the maximum variance reduction method to actively generate sample and estimate the model, and demonstrate the sample complexity. Further, their kernel-based transition model is di erent since they model the transition probability as an inner product between a feature map and a kernel function while we assume that there is a ground truth unknown function. Finally, unlike their work, we consider the ^{2} divergence as well, which invokes a di erent type of reformulations and analysis. A similar work Ma et al. (2022) deal with linear transition dynamics setup, i.e.,

Figure 1: An illustration of distributionally robust RL with a generative model (simulator). Our proposed algorithm MVR (Algorithm 1) queries the simulator and estimates the nominal model $\hat{f}_n$. Then, using the estimated model $\hat{f}_n$ together with a specified uncertainty set, a robust policy is obtained by using model-free RL (e.g., Panaganti et al. (2022)). Finally, the robust policy is deployed in the real-world system.

its Assumption 4.1 is akin to the kernel-based transition dynamics assumption in Blanchet et al. (2024). Still, it also does not involve active sampling.

In the model-free setting with finite state-action space, Liu et al. (2022) propose a distibutionally robust Q-learning algorithm based on access to a generative simulator. Wang et al. (2023a,c) extend the distributionally robust Q-learning framework by improving the design and analysis of the estimation and provide finite sample complexity bounds for this framework. Liang et al. (2023) consider the same problem in the online setting with single trajectory data wherein one is not allowed to sample repeatedly from a state but is allowed to choose actions within that single trajectory. In the model-free setting with large state space (though, still assumed to be finite), Panaganti et al. (2022) study the problem of distributionally robust RL in a function approximation setup. They assume access to offline data from the nominal transition dynamics and provide computational sample complexity bounds in terms of the size of the hypothesis space that is used to represent the set of state-action value functions (Q-function). Other works such as Pinto et al. (2017); Derman et al. (2020); Mankowitz et al. (2019); Zhang et al. (2020) consider robustness aspects in deep reinforcement learning, but these approaches lack theoretical guarantees. To the best of our knowledge, our work is the first one to address the distributionally robust RL problem in the generative model setting with a model-based approach and large state spaces. Moreover, we are the first to consider general non-linear transition dynamics and derive provable sample complexity guarantees for such a setting.

Similar to previous works, we utilize the kernelized MDP framework from Chowdhury and Gopalan (2019) to model transition dynamics with continuous states and actions by assuming that the transition function belongs to an associated Reproducing Kernel Hilbert Space (RKHS). Such continuous MDP formulations also appear in Curi et al. (2020, 2021), however, these works consider finite horizon MDPs while in our work we consider infinite horizon discounted MDPs. In particular, Curi et al. (2021) propose an adversarially robust upper-confidence algorithm to optimize performance in the worst case. However, their algorithm provides robustness guarantees against adversarial perturbations to the transition dynamics. Our work differs from this perspective as we consider robustness w.r.t. distributional shifts of the transition dynamics. Finally, in the related kernelized bandit setting, model-based distributionally robust algorithms are proposed in Kirschner et al. (2020); Bogunovic et al. (2018); Nguyen et al. (2020).

We further summarize some recent advancements in distributionally robust reinforcement learning (RL) that have emerged subsequent to our submission. Wang et al. (2023b) focus on developing a comprehensive theoretical framework for robust MDPs by expanding upon existing formulations. Specifically, they explore various types of decision-makers and adversaries' dynamics within the robust MDP framework, including Markovian and history-dependent behaviors, and examine conditions for the existence of the dynamic programming principle. Yang et al. (2023) consider the equivalent Lagrangian version of the robust MDP problem and propose a model-free sample-efficient algorithm to solve the same. Yu et al. (2024) propose a computationally efficient solution for solving robust MDPs with Wasserstein uncertainty set. Li and Shapiro (2023) focus on delineating the connections between static and game formulations of robust MDPs. Unlike our work, the aforementioned works consider the finite state-action space setting. Liu and Xu (2024) study ϕ-dynamics RL through the framework of robust MDPs under total variation uncertainty set and propose a model-free algorithm to learn the robust policy. Panaganti et al. (2023) incorporate techniques from the distributionally robust learning framework to solve the robust MDP problem in the offline RL setting. Both works adopt the linear transition dynamics, differing from our non-linear transition dynamics in the generative model setting with a model-based approach.

Main Contributions: We formalize a distributionally robust reinforcement learning setting with continuous state spaces and non-linear transition dynamics in Section 2. In the generative model setting, we propose (in Section 3) a model-based approach that utilizes Gaussian Process models and the Maximum Variance Reduction (MVR) principle to e ciently learn transition dynamics. We provide novel statistical sample complexity guarantees in Section 4 for the proposed method and widely used uncertainty sets. Our sample complexity bounds are independent of the number of states, ensuring the e ectiveness of our approach in identifying near-optimal distributionally robust policies for large state spaces. In Section 5, our experimental findings showcase the sample e ciency and robustness of our algorithm in the face of distributional shifts within popular RL-testing environments.

2 PROBLEM SETTING

A discounted Markov Decision Process (MDP) is a tuple (S, A, P, r, γ), with S denoting the state space, the action space A, and the probabilistic transition dynamics $P : S \times A \to \Delta(S)$. Here, $\Delta(S)$ denotes the set of all probability distributions over S. The reward function $r : S \times A \to [0, 1]$ characterizes the reward $r(s, a)$ the learner receives upon playing $a \in A$ in $s \in S$, and $\gamma \in [0, 1)$ denotes the discount factor. The learner uses a policy $\pi : S \to \Delta(A)$ to select $a \in A$ upon observing the state $s \in S$. We define the cumulative discounted reward as $\sum_{t=0}^{\infty} \gamma^t r(s_t, a_t)$ for known initial state s_0 and $s_t \sim P(s_{t-1}, a_{t-1})$ for $t \geq 0$ and $a_t = \pi(s_t)$. The value function V^π and the state-action value function Q^π are given as follows:

$$V^\pi(s) = E_{P,\pi}\left[\sum_{t=0}^{\infty} \gamma^t r(s_t, a_t) \mid s_0 = s\right],$$

$$Q^\pi(s, a) = r(s, a) + E_{P,\pi}\left[\sum_{t=1}^{\infty} \gamma^t r(s_t, a_t)\right],$$

where $a_t = \pi(s_t)$ and $s_{t+1} \sim P(s_t, a_t)$. Finally, we define the optimal policy π^* corresponding to dynamics P which yields the optimal value function, i.e., $V^{\pi^*}(s) = \max_\pi V^\pi(s)$ for all $s \in S$.

We assume the standard generative (or random) access model, in which the learner can query transition data arbitrarily from a simulator, i.e., each query to the simulator (s_t, a_t) outputs a sample $s_{t+1} \sim P(s_t, a_t)$, where $s_{t+1} \sim P(s_t, a_t)$. In particular, we consider the following frequently used transition dynamics model:

$$s_{t+1} = f(s_t, a_t) + \omega_t, \tag{1}$$

where $\omega_t \sim N(0, \sigma^2 I)$ represents independent additive transition noise and follows a Gaussian distribution with zero mean and covariance $\sigma^2 I$.

Regularity assumptions: We assume that f is unknown and continuous for tractability reasons which is a common assumption when dealing with continuous state spaces (e.g., Chowdhury and Gopalan (2019); Curi et al. (2020); Kakade et al. (2020)). Further on, we assume that f resides in the Reproducing Kernel Hilbert Space (RKHS). Considering the multi-output definition of f and in line with the previous work (e.g., Chowdhury and Gopalan (2019); Curi et al. (2020)), we define the modified state-action space $\bar{X}$ (over which the RKHS is defined) as $\bar{X} = S \times A \times \{1, 2, \ldots, d\}$, where the last dimension $i \in \{1, 2, \ldots, d\}$ incorporates the index of the output state vector, i.e., $f(x) = [\tilde{f}(x, 1), \ldots, \tilde{f}(x, d)]$ where $\tilde{f} : \bar{X} \to \mathbb{R}$. In particular, we assume that $\tilde{f}$ belongs to a space of well-behaved functions, denoted by $\mathcal{H}$, induced by some continuous, positive definite kernel function $k : \bar{X} \times \bar{X} \to \mathbb{R}$ and equipped with an inner product $\langle \cdot, \cdot \rangle_k$. All functions belonging to an RKHS $\mathcal{H}$ satisfy the reproducing property defined w.r.t. the inner product $\langle \tilde{f}, k(x, \cdot) \rangle_k = \tilde{f}(x)$ for $\tilde{f} \in \mathcal{H}$. We also make the following common assumptions: (i) the kernel function k is bounded $k(x, x') \leq 1$ for all $x, x' \in \bar{X}$ and $\bar{X}$ is a compact set ($\bar{X} \subset \mathbb{R}^p$), and (ii) every function $\tilde{f} \in \mathcal{H}$ has a bounded RKHS norm (induced by the inner product) $\|\tilde{f}\|_k \leq B$.

We refer to the simulator environment determined by f as the nominal model P_f, while the true environment encountered by the agent in the real world might not be the same (e.g., due to a sim-to-real gap). Consequently, we utilize the robust MDP framework to tackle this by considering an uncertainty set comprising of all models close to the nominal one.

Robust Markov Decision Process (RMDP) : We consider the robust MDP setting that addresses the uncertainty in transition dynamics and considers a set of transition models called the uncertainty set. We use $\mathcal{P}^f$ to denote the uncertainty set that satisfies the (s, a) rectangularity condition Iyengar (2005) (as defined in Equation (2)), an assumption that is commonly used in the related literature (e.g., Panaganti and Kalathil (2022); Panaganti et al. (2022); Zhou et al. (2021)). Similar to MDPs, we specify RMDP by a tuple $(S, A, \mathcal{P}^f, r, \gamma)$ where the uncertainty set $\mathcal{P}^f$ consists of all models close to a nominal model P_f in terms of a distance measure D:

$$\mathcal{P}^f = \bigotimes_{(s,a) \in S \times A} \mathcal{P}^f_{s,a}, \quad \mathcal{P}^f_{s,a} = \{P \in \Delta(S) : D(P \| P_f(s, a)) \leq \rho\}. \tag{2}$$

Here, D denotes some distance measure between probability distributions, and $\rho \geq 0$ defines the radius of the uncertainty set. In this work, we consider three probability distance measures, including Kullback Leibler (KL) divergence such that $KL(P \| Q) = \int \log(\frac{dP}{dQ}) dP$, Chi-Square ($\chi^2$) distance

such that $^2(P||Q) = \int \left(\frac{dP}{dQ} - 1\right)^2 dP$ for P being absolutely continuous with respect to Q, and Total Variation (TV) distance such that $TV(P||Q) = \frac{1}{2}\|P - Q\|_1$.

In the RMDP setting, the goal is to discover a policy that maximizes the cumulative discounted reward for the worst-case transition model within the given uncertainty set. Concretely, the robust value function $V^R_{,f}$ corresponding to a policy $$ and the optimal robust value function are given as follows:

$$V^R_{,f}(s) = \inf_{P \in \mathcal{P}^f_{;}} E_{P;} \Big[\sum_{t=1}^{\infty} {}^t r(s_t; a_t) \,|\, s_0 = s \Big],$$
$$V^R_{,f}(s) = \max_{} V^R_{,f}(s) \quad @s \in S. \tag{3}$$

In fact, Iyengar (2005) shows that for any f, there exists a deterministic robust policy $$. Using the definition of the robust value function, we also define the robust Bellman operator (Iyengar, 2005) in terms of the robust state-action value function $Q^R_{,f}$ as follows:

$$Q^R_{,f}(s,a) = r(s,a) + \inf_{D(p||P_f(s,a)) \le} E_{s' \sim p} V^R_{,f}(s'). \tag{4}$$

The goal of the learner is to discover a near-optimal robust policy while minimizing the total number of samples N, i.e., queries to the nominal model (simulator). Concretely, for a fixed precision > 0, the goal is to output a policy $\hat{}_N$ after collecting N samples, such that $\|V^R_{\hat{}_N,f} - V^R_{,f}\|_\infty \le$.

3 SAMPLING ALGORITHM

In this section, we outline our methodology for addressing the problem described in Section 2. We begin by discussing the Gaussian process (GP) model often used in algorithms to learn RKHS functions (Rasmussen and Williams, 2006; Kanagawa et al., 2018).

Multi-output Gaussian process: Under the assumptions of Section 2, modeling uncertainty and learning the transition model f can be performed via the Gaussian process framework. A Gaussian process $GP(\mu(\cdot), k(\cdot,\cdot))$ over the input domain $\bar{X}$, is a collection of random variables $\{\tilde{f}(x)\}_{x \in \bar{X}}$ whose every finite subset $\{\tilde{f}(x_i)\}_{i=1}^n$, $n \in \mathbb{N}$, follows multivariate Gaussian distribution with mean $E[\tilde{f}(x_i)] = \mu(x_i)$ and covariance $E[(\tilde{f}(x_i) - \mu(x_i))(\tilde{f}(x_j) - \mu(x_j))] = k(x_i, x_j)$ for every $1 \le i, j \le n$. Standard algorithms implicitly use a zero-mean $GP(0, k(\cdot,\cdot))$ as the prior distribution over $\tilde{f}$, i.e, $\tilde{f} \sim GP(0, k(\cdot,\cdot))$ and assume that the noise variables are drawn independently across s from $N(0,)$ with > 0. Considering the multi-output definition of $f(\cdot) = (\tilde{f}(\cdot), \ldots, \tilde{f}(\cdot))$ we build d copies of the dataset such that $D_{1:n,l} = \{(s_i, a_i), s_{i+1,l}\}_{i=1}^n$ each with n transitions from a particular state-action pair (s,a) to component l of next state. For $x_i = (s_i, a_i)$ and $y_{i,l} = s_{i+1,l}$, the posterior mean, covariance and variance for $\tilde{f}(x), l)$ are given by:

$$\mu_{nd}(x, l) = k_{nd}(x, l)^\top (K_{nd} + I_{nd})^{-1} y_{nd}, \tag{5}$$
$$k_{nd}((x, l), (x', l')) = k((x, l), (x', l')) - k_{nd}(x, l)^\top (K_{nd} + I_{nd})^{-1} k_{nd}(x', l'),$$
$$\sigma^2_{nd}(x, l) = k_{nd}((x, l), (x, l)) \tag{6}$$

Here K_{nd} denotes the kernel matrix of dimensions $nd \times nd$ whose entries are $k((x_i, l), (x_j, l'))$ with $1 \le i, j \le n$ and $1 \le l, l' \le d$. $k_{nd}(x, l) = [k((x, l), (x_i, l'))]_{1 \le i \le n, 1 \le l' \le d}$ denotes the covariance vector and $y_{nd} = [y_{i,l}]_{1 \le i \le n, 1 \le l \le d}$ denotes the output vector.

Correspondingly, the posterior mean and variance for f would be

$$\mu_n(s,a) = [\mu_{nd}(s,a,1), \ldots, \mu_{nd}(s,a,d)], \tag{7}$$
$$\sigma_n(s,a) = [\sigma_{nd}(s,a,1), \ldots, \sigma_{nd}(s,a,d)] \tag{8}$$

Maximum variance reduction: With certain assumptions on the loss function (squared loss) and noise distribution, the function estimation in RKHS is analogous to the Bayesian Gaussian process framework (Rasmussen and Williams, 2006). When used with the same kernel function, this allows the construction of mean and variance estimates of $\tilde{f} \sim P(H)$ using Gaussian processes (eq. (5) and eq. (6)). Based on these, one can construct shrinking statistical confidence bounds (used in our analysis in Appendix A.2) that hold with probability at least $1 -$, i.e., the following holds $|\tilde{f}(x) - \mu_{n-1}(x)| \le \beta_n \sigma_{n-1}(x)$ for every $n \ge 1$ and $x \in \bar{X}$. Here $\{\beta_i\}_{i=1}^{n-1}$ stands for the sequence of parameters that are suitably set (see Lemma 5) to ensure the validity of the confidence bounds.

We use the maximum variance reduction (MVR) algorithm (Algorithm 1) to learn about the nominal model f. MVR works on the principle of reducing the maximum uncertainty measured by the posterior standard deviation of a GP model calculated by using previously collected data. At each iteration, MVR queries a state-action pair that has the highest uncertainty according to the model and uses the obtained observation to update the GP posterior. The algorithm outputs nominal dynamics estimate $\hat{f}_n$ corresponding to the final GP posterior mean μ_n.

To characterize the precision of the learned model, we use the max. information gain (Srinivas et al., 2009)

$$\gamma_n(\bar{X}) = \max_{x_1, \ldots, x_n \in \bar{X}} 0.5 \log\det(I_n + {}^{-1}K_n), \tag{9}$$

a kernel-dependent quantity that is frequently used in GP optimization. For many commonly used kernels, γ_n is sublinear in n, which implies that the predictive

Algorithm 1 Maximum Variance Reduction (MVR) for learning model dynamics

Require: Simulator f, kernel k, domain $S \times A$
Set $\sigma_0(s,a) = 0$, $\mu_0(s,a) = 1$ for all $(s,a) \in S \times A$
for $i = 1, \ldots, n$ do
  $(s_i, a_i) = \arg\max_{(s,a) \in S \times A} \{\sigma_{i-1}(s,a)\}^2$
  Observe $s_{i+1} = f(s_i, a_i) + \omega_i$ (i.e., sample s_{i+1} from nominal $P_f(s_i, a_i)$)
  Update to μ_i and σ_i by using (s_i, a_i, s_{i+1}) according to Eq. (5) and Eq. (6)
end for
return The dynamics estimate $\hat{f}_n = \mu_n$

uncertainties are shrinking sufficiently fast, and thus $\hat{f}_n$ is capable of generalizing well across the entire domain. This is formalized in the following lemma.

Lemma 1. For $\sigma_n(\cdot,\cdot)$ set as in Lemma 4 and I_d denoting $\{1, 2, \ldots, d\}$, the MVR algorithm (Algorithm 1) outputs the dynamics estimate $\hat{f}_n = \mu_n$ such that the following holds uniformly for all $(s,a) \in S \times A$ with probability at least $1 - \delta$,

$$\|\mu_n(s,a) - f(s,a)\|_2 \leq \mathcal{O}\left(\frac{\beta_n \sigma_n + \epsilon}{\bar{\eta}} \sqrt{\gamma_{nd}(S \times A \times I_d)}\right).$$

The preceding lemma asserts that we can effectively estimate the unknown dynamics by utilizing the pure exploration procedure and that the error in the model reduces as we increase the number of samples. In the subsequent section, we leverage this finding to establish the minimum number of samples needed to obtain a distributionally robust policy that is close to optimal.

4 SAMPLE COMPLEXITY

This section discusses the statistical sample complexity of the proposed MVR algorithm in distributionally robust MDPs. Specifically, given the optimal robust policies $\hat{\pi}_N$ and π corresponding to the learned nominal dynamics $\hat{f}_N$ by the MVR algorithm with N iterations and the true nominal dynamics f, respectively, we show the number of samples needed by the MVR algorithm to ensure that the following holds:

$$|V^R_{\hat{\pi}_N, \hat{f}_N}(s) - V^R_{\pi, f}(s)| \leq \epsilon, \ \forall s \in S. \tag{10}$$

Note that such an assumption on access to optimal policy is widely used in the generalization literature (Kleywegt et al., 2002; Hu et al., 2020; Zhang et al., 2024). Several model-free methods (Panaganti et al., 2022; Derman et al., 2018; Mankowitz et al., 2019) have studied how to learn an optimal robust policy under KL, TV, and χ^2 uncertainty set given trajectory samples generated from a transition dynamics. Thus, one can easily incorporate the MVR algorithm with these model-free algorithms to find an optimal $\hat{\pi}_N$ using samples generated by $\hat{f}_N$. One major benefit of our approach is that we do not need access to samples from the more costly simulator f when training the robust policy. Consequently, we focus on the statistical sample complexity of the MVR algorithm rather than designing algorithms to find $\hat{\pi}_N$.

Theorem 1. (Sample Complexity of MVR under KL uncertainty set) Consider a robust MDP with nominal transition dynamics f satisfying the regularity assumptions from Section 2 and with uncertainty set defined as in Equation (2) w.r.t. KL divergence. For ρ denoting the robust optimal policy w.r.t. nominal transition dynamics f and $\hat{\pi}_N$ denoting the robust optimal policy w.r.t. learned nominal transition dynamics $\hat{f}_N$ via MVR (Algorithm 1), and $P \in (0, 1)$, $P_0 \in (0, \frac{1}{1-\rho}]$, it holds that $\max_s |V^R_{\hat{\pi}_N, \hat{f}_N}(s) - V^R_{\pi, f}(s)| \leq \epsilon$ with probability at least $1 - \delta$ for any N such that

$$N \geq \mathcal{O}\left(e^{\frac{2}{(1-\rho)\sigma_{kl}}} \frac{\sigma_N^2 \beta_N^2 (1+\rho)\gamma_{Nd}^2}{(1-\rho)^4 \epsilon^2}\right). \tag{11}$$

Theorem 1 shows the number of samples required from the nominal transition dynamics f (simulator) to construct a robust optimal policy reliably with high probability. The complexity bound depends on the maximum information gain γ_{Nd} (Equation (9)), which is sublinear in N for many commonly used kernels (Srinivas et al., 2009), and on the confidence width $\beta_N^2(\delta)$ which also exhibits a logarithmic dependence on N according to the confidence bounds from Vakili et al. (2021). Specifically, for the squared exponential kernel used in the experiments, both γ_{Nd} and β_N depend only logarithmically on N, implying that a bound independent of N remains the same up to extra multiplicative log factors. An additional d factor that denotes the dimension of the state space S in the obtained bound comes from utilizing the multi-output (of dimension d) GP framework to model the transition dynamics, which also appears in the regret bounds of similar works (Chowdhury and Gopalan, 2019; Curi et al., 2020, 2021). Finally, the term $\sigma_{kl}(P_0, \frac{1}{2(1-\rho)})$ is a problem-dependent parameter that is independent of N, which similarly appears in the guarantees of Panaganti and Kalathil (2022).

We can compare our guarantees with the existing sample-complexity results in model-based distributionally robust RL which, however, only consider finite state-action spaces. In particular, when considering KL uncertainty sets with infinite horizon, Panaganti and Kalathil (2022) obtain sample complexity of order $\mathcal{O}\left(e^{\frac{\sigma_{kl}}{(1-\rho)^2}} \frac{|S|^2|A|}{(1-\rho)^4 \epsilon^2}\right)$ up to logarithmic factors. Notably, the latter complexity bound explicitly depends on the cardinality of the state and action spaces $|S|$ and $|A|$, thus scaling badly when S and A are large or continuous. Instead, the guarantee of Theorem 1 depends on the state-action space only through γ_{Nd} which remains bounded even when these are continuous. This

allows us to successfully extend the distributionally robust framework to continuous state spaces. Other terms in the bound of Theorem 1 such as γ (the discount factor), ρ (radius of the uncertainty set) have similar dependencies. Crucially, the dependence on the precision parameter ϵ remains the same when compared to the guarantees provided for finite state-action setting.

We relegate the proof of Theorem 1 to Appendix B but outline its main steps below:

Step (i): The first step is to bound the approximation error of policy $\hat{\pi}_n$ (i.e., the left-hand side of Equation (10)) by the sum of two error terms: $|V^R_{\hat{\pi}_N,f}(s) - V^R_{\hat{\pi}_N,\hat{f}_N}(s)|$ and $|V^R_{\hat{\pi}_N,\hat{f}_N}(s) - V^R_{\pi^*,f}|$. Utilizing the robust Bellman Equation (4), bounding such errors boils down to bounding differences of the form:

$$\max_s \Big| \inf_{KL(p\|P_f(s,\hat{\pi}_N(s)))\le\rho} \mathbb{E}_{s'\sim p}\big[V^R_{\hat{\pi}_N,f}(s')\big] - \inf_{KL(p\|P_{\hat{f}_n}(s,\hat{\pi}_N(s)))\le\rho} \mathbb{E}_{s'\sim p}\big[V^R_{\hat{\pi}_N,f}(s')\big]\Big|. \quad (12)$$

where $P_f(s,a)$ denotes the Gaussian transition distribution with mean $f(s,a)$ and covariance $\sigma^2 I$.

Step (ii): The major challenge of bounding Equation (12) lies in the inner infinite-dimensional minimization problems over distributions. To overcome this, we can reformulate such problems into single-dimensional ones using duality (Hu and Hong, 2013; Zhou et al., 2021; Panaganti and Kalathil, 2022) as follows:

Lemma 2. (Variant of Hu and Hong (2013)) For random variable X and function V satisfying that $V(X)$ has a finite Moment Generating function, it holds for all $\rho > 0$ and $P \in \{P : KL(P\|P_0) \le \rho\}$:

$$\inf_P \mathbb{E}_P[V(X)] = \sup_{\alpha\ge 0}\Big\{-\alpha \log\big(\mathbb{E}_{P_0}[e^{-\frac{V(X)}{\alpha}}]\big) - \alpha\rho\Big\}.$$

Let $H(V,P) := \sup_{\alpha\ge 0}\{-\alpha\log(\mathbb{E}_{X\sim P}[e^{-\frac{V(X)}{\alpha}}]) - \alpha\rho\}$. Thus, applying Lemma 2, we rewrite Equation (12) as the difference of two single-dimensional convex optimization problems with expectations over P_f and $P_{\hat{f}_N}$, respectively:

$$\begin{aligned}
&\max_s \big|H(V^R_{\hat{\pi}_N,f}, P_f(s,\hat{\pi}_N(s))) - H(V^R_{\hat{\pi}_N,f}, P_{\hat{f}_N}(s,\hat{\pi}_N(s)))\big| \\
&\le \max_{V(\cdot)\in\mathcal{V}} \max_{s,a} \big|H(V, P_f(s,a)) - H(V, P_{\hat{f}_N}(s,a))\big| \\
&\le \max_{V(\cdot)\in\mathcal{V}} \max_{s,a} \max_{\alpha\in[\underline{\alpha},\bar{\alpha}]} c\,\Big|\mathbb{E}_{s'\sim P_f(s,a)}\big[e^{-\frac{V(s')}{\alpha}}\big] \\
&\qquad\qquad - \mathbb{E}_{s'\sim P_{\hat{f}_N}(s,a)}\big[e^{-\frac{V(s')}{\alpha}}\big]\Big|,
\end{aligned} \quad (13)$$

where $c, \underline{\alpha}, \bar{\alpha} > 0$ are constants, $\mathcal{V}$ denotes the value functional space, and the last inequality holds due to certain structural properties of the single-dimensional optimization problem in the RHS of Equation (13).

Step (iii): Finally, we bound Equation (13) using the difference between the estimated model $\hat{f}_N$ and the true f, which is characterized by Lemma 1, in Appendix B. Moreover, to address the outer maximum over all value functions, states, and actions, we incorporate a covering number argument.

Other uncertainty sets: We further obtain the statistical sample complexities for χ^2 distance and TV distance uncertainty sets. We note that the analysis follows similar steps as the ones of Theorem 1. The major difference lies in incorporating and handling the dual forms of χ^2/TV uncertainty sets in our analysis which differ from the one of Lemma 2. For χ^2 uncertainty set, we utilize the dual formulation that appears in Duchi and Namkoong (2021), while for TV uncertainty sets we follow the approach of Yang et al. (2022). As before, we can upper bound Equation (12) via covering number arguments and the distance between the nominal transition dynamics f and the learned transition dynamics $\hat{f}_N$ by using Lemma 1. Below, we outline the statistical sample complexity in the case of χ^2 and TV uncertainty sets in Propositions 1 and 2, respectively.

Proposition 1. (Sample Complexity of MVR under χ^2 uncertainty set) Under the setup of Theorem 1 with uncertainty set defined w.r.t. χ^2 distance, it holds that $\max_s |V^R_{\hat{\pi}_N,f}(s) - V^R_{\pi^*,f}(s)| \le \epsilon$ with probability at least $1-\delta$ for any N such that

$$N \ge O\left(\left(\frac{\sqrt{1+2\rho}}{\sqrt{1+2\rho}-1}\right)^4 \frac{\beta^4_N(\delta)\, d^2\, \Gamma_{Nd}}{(1-\gamma)^8\epsilon^4}\right). \quad (14)$$

Proposition 2. (Sample Complexity of MVR under TV uncertainty set) Under the setup of Theorem 1 with uncertainty set defined w.r.t. TV distance, it holds that $\max_s |V^R_{\hat{\pi}_N,f}(s) - V^R_{\pi^*,f}(s)| \le \epsilon$ with probability at least $1-\delta$ for any N such that

$$N \ge O\left(\frac{(2+\rho)^2}{\rho^2}\frac{\beta^2_N(\delta)\, d^2\, \Gamma_{Nd}}{(1-\gamma)^4\epsilon^2}\right). \quad (15)$$

We relegate the proofs of Propositions 1 and 2 to Appendices C.1 and C.2. In comparison to the exponential dependence on $\frac{1}{1-\gamma}$ for KL uncertainty set in Theorem 1, we note that for both χ^2/TV uncertainty sets, we obtain polynomial dependence on $\frac{1}{1-\gamma}$. In the context of the TV uncertainty set, the dependency on ϵ in Proposition 2 remains consistent with the finite state case (Panaganti and Kalathil, 2022). However, in the χ^2 case, the bound presented in Proposition 1 exhibits a worse dependence on ϵ compared to the result derived in Panaganti and Kalathil (2022). This difference arises because we refrain from utilizing the same dual reformulation lemmas from Iyengar (2005), as they are applicable exclusively to finite state-action settings. Improving these rates is an interesting direction for future work.

5 EXPERIMENTS

The aim of our experiments is to show the e ectiveness of the proposed distributionally-robust model-based approach. In particular, our goal is to evaluate the robustness of our policies against di erent perturbations of the environment's parameters, and compare them with existing non-robust methods. Moreover, our experiments focus on demonstrating the e ectiveness of MVR to smartly collect data from the environment rather than using a sub-optimal/random policy to interact with the environment and collect data. This signi cantly reduces the number of samples required from the environment to perform robustly. In addition, we compare our approach with model-free methods (robust and non-robust) which typically require a signi cantly larger number of interactions with the nominal environment.

Environments: We consider the OpenAI's gym (Brockman et al., 2016) environments of swing-up Pendulum, Cartpole and Reacher, respectively. Pendulum has a 2-dimensional state space and scalar actions (Mehta et al., 2021). For Cartpole, we consider a scalar continuous action space as done in Mehta et al. (2021), while states are 4-dimensional. Reacher, instead, consists of a 2DOF robot arm with 8-dimensional states. For each environment we test our approach against various perturbations as outlined below.

Module 1: Learning the model. To learn the nominal environment, we utilize a setup similar to that of Mehta et al. (2021), but instead of considering the "EIG " which minimizes entropy of the optimal trajectory using model-predictive control, we use the proposed MVR method (Algorithm 1). Similar to Mehta et al. (2021), we use a GP prior with the squared exponential kernel to model the transition dynamics $f(s,a)$ (alternate models such as Neural Ensembles or Bayesian neural networks can be used to model the transition dynamics as done in, e.g., Curi et al. (2020, 2021)). As in continuous control problems the subsequent states are fairly close, we use our multi-output GP to model the di erence $f(s_t,a_t) \quad s_{t\ 1}$.

Module 2: Computing a robust policy. Given a learned model $\hat{f}_n$, we compute the associated robust policy $\hat{}_n$ using the Robust Fitted Q-Iteration (RFQI) algorithm recently introduced in Panaganti et al. (2022) (this e ectively approximates our robust optimization oracle). RFQI computes a robust policy from o ine data by alternated maximization of a dual-variable function and a Q-function. We generate such o ine data by using a -greedy non-robust policy (using Soft Actor-Critic (Haarnoja et al., 2018) or Model Predictive Control (Camacho and Alba, 2013; Chua et al., 2018)) which we train on the learned model $\hat{f}_n$ from Module 1 and let interact with it for 10^6 steps. Note that this is crucially di erent from the vanilla RFQI (Panaganti et al., 2022) where the true nominal environment was used both for training such policy and for generating o ine data. Indeed, this would require a signi cantly larger number of environment interactions.

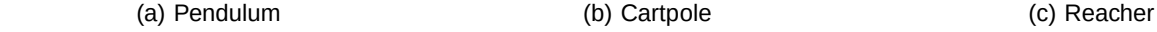
Alg \ Env	Pendulum	Cartpole	Reacher
MVR+RFQI (ours)	60	150	2000
MVR+FQI	60	150	2000
SAC	10^4	-	10^6
MPC	-	2250/step	-
RFQI	10^6 10^4	10^5 2250	10^6 10^6
FQI	10^6 10^4	10^5 2250	10^6 10^6

Table 1: Number of interactions with the nominal environment to obtain the results of Figure 2. For MPC , a total of 2250 interactions are required at each step for planning multiple rollouts and selecting the best action. Both RFQI and FQI utilize 10^6 o ine data points generated by SAC or MPC .

Baselines: We compare our approach, which we denote as MVR+RFQI , with the following baselines:

- MVR+FQI : A natural non-robust baseline that consists of computing a non-robust policy via the Fitted Q-Iteration (FQI) algorithm (Ernst et al., 2005) on the same o ine data used by MVR+RFQI ,
- Soft Actor-Critic (SAC) (Haarnoja et al., 2018), or Model Predictive Control (MPC) (Camacho and Alba, 2013; Chua et al., 2018), as model-free methods which compute non-robust policies interacting with the nominal environment (in case of MPC , the latter is used for planning),
- RFQI (Panaganti et al., 2022), which also requires the nominal environment and uses 10^6 o ine data collected by SAC or MPC to train a robust policy,
- FQI (Ernst et al., 2005), which trains a non-robust policy from the same data.

Training: Model-free methods are trained directly on the nominal environments. In particular, for Pendulum and Reacher we train SAC until convergence for 10^4 and 10^6 steps, respectively. On the continuous actions Cartpole, instead, we run MPC following the implementation of Pinneri et al. (2020); Mehta et al. (2021) which requires a total of 2250 planning interactions to select the optimal action at each step. Depending on the environment, we utilize SAC or MPC mixed with an -greedy rule to collect 10^6 o ine data points. These are used to train the o ine methods RFQI and FQI as done in Panaganti et al. (2022). For the model-based approaches, instead, we rst run MVR for a su ciently informative number of samples (60 for Pendulum, 150 for Cartpole and 2000 for Reacher) to obtain an estimated model $\hat{f}_n$. Then, we use SAC (trained against model $\hat{f}_n$) or MPC to collect 10^6 o ine data on such estimated environment.



(a) Pendulum (b) Cartpole (c) Reacher

Figure 2: Average performance (over 20 episodes) on the considered environments, as a function of di erent perturbations: length perturbation for Pendulum, force magnitude perturbation for Cartpole, and perturbed joint sti ness for Reacher. Unlike our MVR+RFQI and non-robust MVR+FQI , the other baselines are model-free and require access to the true nominal environment for training. The proposed approach MVR+RFQI achieves comparable performance to the model-free RFQI albeit requiring signi cantly fewer environment interactions (see Table 1). Moreover, as the perturbation magnitude increases, MVR+RFQI outperforms the other non-robust baselines.

These data are then used to train MVR+RFQI and MVR+FQI . We provide further implementation details and hyperparameters in Appendix D.

Evaluation: For each environment, we evaluate the computed policy against di erent perturbation types and magnitudes. For Cartpole, we perturb the magnitude of the actuation force. Its nominal value is 10 and we perturb up to 300% Also, we consider perturbations to gravity in the range of (-100%,100%) with the nominal value being 9:82. For the Pendulum, we consider perturbations to the length of the pendulum and action perturbations (where a random action is chosen with probability). Finally, in the case of Reacher we consider perturbations to the joint's sti ness (from 0 to 100) coupled with perturbations of the joint's equilibrium position. Further details on the chosen perturbations and hyperparameters used are provided in Appendix D. We provide the code to reproduce the results[1].

In Figure 2 we plot the average performance (over 20 episodes) of the baselines subject to di erent perturbation types and magnitudes for each environment. Results for other perturbations are relegated to Appendix D. In Table 1, we report the total number of interactions with the nominal environment required to compute the evaluated policies. We remark that MVR+RFQI and MVR+FQI interact with the environment only to learn a GP model via the MVR approach. Instead, the other model-free methods use the nominal environment throughout the whole training and, in case of RFQI and FQI , even to generate o ine data. Notably, the policy computed by MVR+RFQI displays comparable performance to its model-free counterpart RFQI which, as shown in Table 1, requires a signi cantly larger number of samples. This shows the sample-e ciency of MVR in acquiring informative data. Moreover, as the perturbation magnitude increases, MVR+RFQI achieves higher performance compared to MVR+FQI and the other non-robust methods, demonstrating the robustness of the computed policies. Additionally, as similarly noted e.g. by Kumar et al. (2021), we observe the o ine methods MVR+FQI and FQI to be generally more robust (although not explicitly computing robust policies) than SAC and MPC .

[1] https://github.com/rsshyam/MVR-RFQI

6 CONCLUSIONS

We investigated distributionally robust RL with continuous state spaces and non-linear transitions. Speci cally, we proposed a model-based approach in the generative model setting, utilizing max. variance reduction to learn nominal transitions. Our results include novel sample complexity guarantees for commonly used uncertainty sets, required for identifying near-optimal robust policies in large state spaces. Through experiments conducted in popular RL-environments, we demonstrated the sample e ciency and robustness of our algorithm in the presence of distributional shifts. An important avenue is the extension of our algorithm to the online and o ine RL settings.

Acknowledgements

PGS was gratefully supported by ELSA (European Lighthouse on Secure and Safe AI) funded by the European Union under grant agreement No. 101070617. YH was supported by NCCR Automation from Switzerland. IB was supported by the EPSRC New Investigator Award EP/X03917X/1 and Google Research Scholar award. The authors would like to thank Viraj Mehta, Zaiyan Xu, Zhengqing Zhou, Zhengyuan Zhou, Wenhao Yang, Laixi Shi, and Liangyu Zhang for the useful discussion.

References

Abbasi-Yadkori, Y., Bartlett, P., Bhatia, K., Lazic, N., Szepesvari, C., and Weisz, G. (2019). Politex: Regret bounds for policy iteration using expert prediction. International Conference on Machine Learning (ICML) .

Agarwal, A., Kakade, S., and Yang, L. F. (2020). Model-based reinforcement learning with a generative model is minimax optimal. Conference on Learning Theory (COLT) .

Ali, S. M. and Silvey, S. D. (1966). A general class of coe cients of divergence of one distribution from another. Journal of the Royal Statistical Society: Series B (Methodological)

Andrychowicz, O. M., Baker, B., Chociej, M., Jozefowicz, R., McGrew, B., Pachocki, J., Petron, A., Plappert, M., Powell, G., Ray, A., et al. (2020). Learning dexterous in-hand manipulation. The International Journal of Robotics Research

Badrinath, K. P. and Kalathil, D. (2021). Robust reinforcement learning using least squares policy iteration with provable performance guarantees. International Conference on Machine Learning (ICML).

Ben-Tal, A., Den Hertog, D., De Waegenaere, A., Melenberg, B., and Rennen, G. (2013). Robust solutions of optimization problems a ected by uncertain probabilities. Management Science (INFORMS)

Blanchet, J., Lu, M., Zhang, T., and Zhong, H. (2024). Double pessimism is provably e cient for distributionally robust o ine reinforcement learning: Generic algorithm and robust partial coverage. Conference on Neural Information Processing Systems (NeurIPS) .

Bogunovic, I., Scarlett, J., Jegelka, S., and Cevher, V. (2018). Adversarially robust optimization with Gaussian processes. Conference on Neural Information Processing Systems (NeurIPS)

Brockman, G., Cheung, V., Pettersson, L., Schneider, J., Schulman, J., Tang, J., and Zaremba, W. (2016). Openai gym.

Camacho, E. F. and Alba, C. B. (2013). Model predictive control. Springer Science & Business media.

Chen, J. and Jiang, N. (2019). Information-theoretic considerations in batch reinforcement learning. International Conference on Machine Learning (ICML).

Chowdhury, S. R. and Gopalan, A. (2019). Online learning in kernelized Markov decision processes. International Conference on Arti cial Intelligence and Statistics (AISTATS) .

Christiano, P., Shah, Z., Mordatch, I., Schneider, J., Blackwell, T., Tobin, J., Abbeel, P., and Zaremba, W. (2016). Transfer from simulation to real world through learning deep inverse dynamics model. arXiv preprint arXiv:1610.03518.

Chua, K., Calandra, R., McAllister, R., and Levine, S. (2018). Deep reinforcement learning in a handful of trials using probabilistic dynamics models. Conference on Neural Information Processing Systems (NeurIPS) .

Clavera, I., Rothfuss, J., Schulman, J., Fujita, Y., Asfour, T., and Abbeel, P. (2018). Model-based reinforcement learning via meta-policy optimization. Conference on Robot Learning

Clavier, P., Pennec, E. L., and Geist, M. (2023). Towards minimax optimality of model-based robust reinforcement learning. arXiv preprint arXiv:2302.05372

Cressie, N. and Read, T. R. (1984). Multinomial goodness-of- t tests. Journal of the Royal Statistical Society: Series B (Methodological)

Csiszár, I. (1967). Information-type measures of di erence of probability distributions and indirect observation. studia scientiarum Mathematicarum Hungarica, 2:229 318.

Curi, S., Berkenkamp, F., and Krause, A. (2020). Efficient model-based reinforcement learning through optimistic policy search and planning. Conference on Neural Information Processing Systems (NeurIPS)

Curi, S., Bogunovic, I., and Krause, A. (2021). Combining pessimism with optimism for robust and e cient model-based deep reinforcement learning. International Conference on Machine Learning (ICML).

Degrave, J., Felici, F., Buchli, J., Neunert, M., Tracey, B., Carpanese, F., Ewalds, T., Hafner, R., Abdolmaleki, A., de Las Casas, D., et al. (2022). Magnetic control of tokamak plasmas through deep reinforcement learning. Nature.

Deisenroth, M. P. and Rasmussen, C. E. (2019). Pilco: A model-based and data-e cient approach to policy search. International Conference on Machine Learning (ICML) .

Derman, E., Mankowitz, D., Mann, T., and Mannor, S. (2020). A Bayesian approach to robust reinforcement learning. Uncertainty in Arti cial Intelligence (UAI) .

Derman, E., Mankowitz, D. J., Mann, T. A., and Mannor, S. (2018). Soft-robust actor-critic policy-gradient. arXiv preprint arXiv:1803.04848 .

Duchi, J. C. and Namkoong, H. (2021). Learning models with uniform performance via distributionally robust optimization. The Annals of Statistics, Institute of Mathematical Statistics.

Ernst, D., Geurts, P., and Wehenkel, L. (2005). Tree-based batch mode reinforcement learning. Journal of Machine Learning Research (JMLR).

Gheshlaghi Azar, M., Munos, R., and Kappen, H. J. (2013). Minimax pac bounds on the sample complexity of reinforcement learning with a generative model. Springer Machine Learning.

Haarnoja, T., Zhou, A., Abbeel, P., and Levine, S. (2018). Soft actor-critic: O -policy maximum entropy deep reinforcement learning with a stochastic actor. International Conference on Machine Learning (ICML) .

Hu, Y., Chen, X., and He, N. (2020). Sample complexity of sample average approximation for conditional stochastic optimization. SIAM Journal on Optimization.

Hu, Z. and Hong, L. J. (2013). Kullback-Leibler divergence constrained distributionally robust optimization. Optimization Online.

Iyengar, G. N. (2005). Robust dynamic programming. Mathematics of Operations Research (INFORMS)

Kakade, S., Krishnamurthy, A., Lowrey, K., Ohnishi, M., and Sun, W. (2020). Information theoretic regret bounds for online nonlinear control. Conference on Neural Information Processing Systems (NeurIPS)

Kakade, S. M. (2003). On the sample complexity of reinforcement learning. University of London, University College London (United Kingdom).

Kanagawa, M., Hennig, P., Sejdinovic, D., and Sriperumbudur, B. K. (2018). Gaussian processes and kernel methods: A review on connections and equivalences. arXiv preprint arXiv:1807.02582.

Kearns, M., Mansour, Y., and Ng, A. Y. (2002). A sparse sampling algorithm for near-optimal planning in large Markov decision processes. Springer Machine learning.

Kirschner, J., Bogunovic, I., Jegelka, S., and Krause, A. (2020). Distributionally robust Bayesian optimization. International Conference on Arti cial Intelligence and Statistics (AISTATS).

Kleywegt, A. J., Shapiro, A., and Homem-de Mello, T. (2002). The sample average approximation method for stochastic discrete optimization. SIAM Journal on optimization.

Kumar, A., Hong, J., Singh, A., and Levine, S. (2021). Should i run o ine reinforcement learning or behavioral cloning? International Conference on Learning Representations (ICLR).

Lattimore, T., Szepesvari, C., and Weisz, G. (2020). Learning with good feature representations in bandits and in rl with a generative model. International Conference on Machine Learning (ICML).

Li, G., Wei, Y., Chi, Y., Gu, Y., and Chen, Y. (2020). Breaking the sample size barrier in model-based reinforcement learning with a generative model. Conference on Neural Information Processing Systems (NeurIPS).

Li, X., Mehta, V., Kirschner, J., Char, I., Neiswanger, W., Schneider, J., Krause, A., and Bogunovic, I. (2023). Near-optimal policy identi cation in active reinforcement learning. International Conference on Learning Representations (ICLR).

Li, Y. and Shapiro, A. (2023). Rectangularity and duality of distributionally robust Markov decision processes. arXiv preprint arXiv:2308.11139.

Liang, Z., Ma, X., Blanchet, J., Zhang, J., and Zhou, Z. (2023). Single-trajectory distributionally robust reinforcement learning. arXiv preprint arXiv:2301.11721.

Lim, S. H., Xu, H., and Mannor, S. (2013). Reinforcement learning in robust Markov decision processes. Conference on Neural Information Processing Systems (NeurIPS).

Liu, Z., Bai, Q., Blanchet, J., Dong, P., Xu, W., Zhou, Z., and Zhou, Z. (2022). Distributionally robust q-learning. International Conference on Machine Learning (ICML) .

Liu, Z. and Xu, P. (2024). Distributionally robust o -dynamics reinforcement learning: Provable e ciency with linear function approximation. arXiv preprint arXiv:2402.15399.

Ma, X., Liang, Z., Blanchet, J., Liu, M., Xia, L., Zhang, J., Zhao, Q., and Zhou, Z. (2022). Distributionally robust o ine reinforcement learning with linear function approximation. arXiv preprint arXiv:2209.06620.

Mankowitz, D. J., Levine, N., Jeong, R., Abdolmaleki, A., Springenberg, J. T., Shi, Y., Kay, J., Hester, T., Mann, T., and Riedmiller, M. (2019). Robust reinforcement learning for continuous control with model misspeci cation. International Conference on Learning Representations (ICLR).

Mannor, S., Mebel, O., and Xu, H. (2016). Robust mdps with k-rectangular uncertainty. Mathematics of Operations Research (INFORMS).

Mehta, V., Paria, B., Schneider, J., Ermon, S., and Neiswanger, W. (2021). An experimental design perspective on model-based reinforcement learning. International Conference on Learning Representations (ICLR) .

Nguyen, T., Gupta, S., Ha, H., Rana, S., and Venkatesh, S. (2020). Distributionally robust Bayesian quadrature optimization. International Conference on Arti cial Intelligence and Statistics (AISTATS) .

Nilim, A. and El Ghaoui, L. (2005). Robust control of Markov decision processes with uncertain transition matrices. Operations Research (INFORMS).

Panaganti, K. and Kalathil, D. (2022). Sample complexity of robust reinforcement learning with a generative model. International Conference on Arti cial Intelligence and Statistics (AISTATS) .

Panaganti, K., Xu, Z., Kalathil, D., and Ghavamzadeh, M. (2022). Robust reinforcement learning using ofine data. Conference on Neural Information Processing Systems (NeurIPS) 35:32211 32224.

Panaganti, K., Xu, Z., Kalathil, D., and Ghavamzadeh, M. (2023). Bridging distributionally robust learning and o ine rl: An approach to mitigate distribution shift and partial data coverage. arXiv preprint arXiv:2310.18434.

Peng, X. B., Andrychowicz, M., Zaremba, W., and Abbeel, P. (2018). Sim-to-real transfer of robotic control with dynamics randomization. IEEE International Conference on Robotics and Automation (ICRA) .

Petrik, M. and Russel, R. H. (2019). Beyond con dence regions: Tight Bayesian ambiguity sets for robust MDPs. Conference on Neural Information Processing Systems (NeurIPS).

Pinneri, C., Sawant, S., Blaes, S., Achterhold, J., Stueckler, J., Rolinek, M., and Martius, G. (2020). Sample-e cient cross-entropy method for real-time planning. arXiv preprint arXiv:2008.06389 .

Pinto, L., Davidson, J., Sukthankar, R., and Gupta, A. (2017). Robust adversarial reinforcement learning. International Conference on Machine Learning (ICML) .

Rasmussen, C. E. and Williams, C. (2006). Gaussian processes for machine learning, vol. 1.

Rastogi, D., Koryakovskiy, I., and Kober, J. (2018). Sample-e cient reinforcement learning via di erence models. Machine Learning in Planning and Control of Robot Motion Workshop at ICRA.

Roy, A., Xu, H., and Pokutta, S. (2017). Reinforcement learning under model mismatch. Conference on Neural Information Processing Systems (NeurIPS)

Shapiro, A. (2017). Distributionally robust stochastic programming. SIAM Journal on Optimization .

Shari , R. and Szepesvári, C. (2020). E cient planning in large MDPs with weak linear function approximation. Conference on Neural Information Processing Systems (NeurIPS).

Shi, L. and Chi, Y. (2022). Distributionally robust model-based o ine reinforcement learning with near-optimal sample complexity. arXiv preprint arXiv:2208.05767.

Shi, L., Li, G., Wei, Y., Chen, Y., Geist, M., and Chi, Y. (2024). The curious price of distributional robustness in reinforcement learning with a generative model. Conference on Neural Information Processing Systems (NeurIPS).

Srinivas, N., Krause, A., Kakade, S. M., and Seeger, M. (2009). Gaussian process optimization in the bandit setting: No regret and experimental design. arXiv preprint arXiv:0912.3995.

Tamar, A., Mannor, S., and Xu, H. (2014). Scaling up robust mdps using function approximation. International Conference on Machine Learning (ICML) .

Tkachuk, V., Bakhtiari, S. A., Kirschner, J., Jusup, M., Bogunovic, I., and Szepesvári, C. (2023). E cient planning in combinatorial action spaces with applications to cooperative multi-agent reinforcement learning. International Conference on Arti cial Intelligence and Statistics (AISTATS) .

Vakili, S., Bouziani, N., Jalali, S., Bernacchia, A., and Shiu, D.-s. (2021). Optimal order simple regret for Gaussian process bandits. Conference on Neural Information Processing Systems (NeurIPS)

Wang, S., Si, N., Blanchet, J., and Zhou, Z. (2023a). A nite sample complexity bound for distributionally robust q-learning. International Conference on Arti cial Intelligence and Statistics (AISTATS) .

Wang, S., Si, N., Blanchet, J., and Zhou, Z. (2023b). On the foundation of distributionally robust reinforcement learning. arXiv preprint arXiv:2311.09018 .

Wang, S., Si, N., Blanchet, J., and Zhou, Z. (2023c). Sample complexity of variance-reduced distributionally robust q-learning. arXiv preprint arXiv:2305.18420.

Wang, Y. and Zou, S. (2021). Online robust reinforcement learning with model uncertainty. Conference on Neural Information Processing Systems (NeurIPS)

Wiesemann, W., Kuhn, D., and Rustem, B. (2013). Robust Markov decision processes Mathematics of Operations Research (INFORMS).

Wulfmeier, M., Posner, I., and Abbeel, P. (2017). Mutual alignment transfer learning. Conference on Robot Learning.

Xu, H. and Mannor, S. (2010). Distributionally robust Markov decision processes. Conference on Neural Information Processing Systems (NeurIPS)

Xu, Z., Panaganti, K., and Kalathil, D. (2023). Improved sample complexity bounds for distributionally robust reinforcement learning. International Conference on Arti cial Intelligence and Statistics (AISTATS) .

Yang, W., Wang, H., Kozuno, T., Jordan, S. M., and Zhang, Z. (2023). Avoiding model estimation in

robust Markov decision processes with a generative model. arXiv preprint arXiv:2302.01248.

Yang, W., Zhang, L., and Zhang, Z. (2022). Toward theoretical understandings of robust Markov decision processes: Sample complexity and asymptotics. The Annals of Statistics, Institute of Mathematical Statistics.

Yin, D., Hao, B., Abbasi-Yadkori, Y., Lazi¢, N., and Szepesvári, C. (2022). E cient local planning with linear function approximation. International Conference on Algorithmic Learning Theory.

Yu, P. and Xu, H. (2015). Distributionally robust counterpart in Markov decision processes. IEEE Transactions on Automatic Control.

Yu, Z., Dai, L., Xu, S., Gao, S., and Ho, C. P. (2024). Fast bellman updates for Wasserstein distributionally robust mdps. Conference on Neural Information Processing Systems (NeurIPS).

Zhang, H., Chen, H., Xiao, C., Li, B., Liu, M., Boning, D., and Hsieh, C.-J. (2020). Robust deep reinforcement learning against adversarial perturbations on state observations. Conference on Neural Information Processing Systems (NeurIPS).

Zhang, S., Hu, Y., Zhang, L., and He, N. (2024). Generalization bounds of nonconvex-(strongly)-concave stochastic minimax optimization. International Conference on Arti cial Intelligence and Statistics (AISTATS).

Zhou, Z., Zhou, Z., Bai, Q., Qiu, L., Blanchet, J., and Glynn, P. (2021). Finite-sample regret bound for distributionally robust o ine tabular reinforcement learning. International Conference on Arti cial Intelligence and Statistics (AISTATS).

Checklist

1. For all models and algorithms presented, check if you include:
   (a) A clear description of the mathematical setting, assumptions, algorithm, and/or model. [Yes]
   (b) An analysis of the properties and complexity (time, space, sample size) of any algorithm. [Yes]
   (c) (Optional) Anonymized source code, with speci cation of all dependencies, including external libraries. [Yes] Included in the supplementary material

2. For any theoretical claim, check if you include:
   (a) Statements of the full set of assumptions of all theoretical results. [Yes]
   (b) Complete proofs of all theoretical results. [Yes]
   (c) Clear explanations of any assumptions. [Yes]

3. For all gures and tables that present empirical results, check if you include:
   (a) The code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL). [Yes] Included in the supplementary material
   (b) All the training details (e.g., data splits, hyperparameters, how they were chosen). [Yes]
   (c) A clear de nition of the speci c measure or statistics and error bars (e.g., with respect to the random seed after running experiments multiple times). [Yes]
   (d) A description of the computing infrastructure used. (e.g., type of GPUs, internal cluster, or cloud provider). [Yes]

4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets, check if you include:
   (a) Citations of the creator If your work uses existing assets. [Yes]
   (b) The license information of the assets, if applicable. [Yes]
   (c) New assets either in the supplemental material or as a URL, if applicable. [Yes] Included in the supplementary material
   (d) Information about consent from data providers/curators. [Not Applicable]
   (e) Discussion of sensible content if applicable, e.g., personally identi able information or offensive content. [Not Applicable]

5. If you used crowdsourcing or conducted research with human subjects, check if you include:
   (a) The full text of instructions given to participants and screenshots. [Not Applicable]
   (b) Descriptions of potential participant risks, with links to Institutional Review Board (IRB) approvals if applicable. [Not Applicable]
   (c) The estimated hourly wage paid to participants and the total amount spent on participant compensation. [Not Applicable]

A Theoretical Guarantees of Maximum Variance Reduction (MVR)

We formally introduce the Gaussian process model in Appendix A.1. In Appendix A.2, we describe the con dence bound results from Vakili et al. (2021) and adapt them to the case of multi-output GP models. Finally, in Appendix A.3, we provide sample complexity guarantees for the MVR algorithm.

We recall the introduced notation $X = S \times A$ and remark that we use both (s_i, a_i) and x_i interchangeably in this section.

A.1 Gaussian Process Model

Gaussian process (GP) is a non-parametric model that is often used to express uncertainty over functions on any set (e.g., RKHS). They allow to tractably construct posterior distribution over functions in the set to estimate the unknown non-linear function $\tilde{f}: X \to R$ given data containing samples from function $\tilde{f}$. It follows the Bayesian methodology of calculating posterior given the prior and assumes that the function values at any nite subset of the domain X follow the multivariate Gaussian distribution. One speci es a GP by a prior mean function and a covariance function usually de ned using a kernel $k(x, x')$ where $x, x' \in X$.

Assuming that the samples of $\tilde{f}: X \to R$ are noisy measurements of the underlying true function $\tilde{f}$ with i.i.d. Gaussian noise $N(0, \sigma)$, the posterior mean and covariance function of the posterior distribution can be explicitly calculated. In essence, for $\{x_1, \ldots, x_N\} \subset X$ and $y_n = \tilde{f}(x_n) + \omega_n$, the posterior mean, covariance and variance are given by:

$$\mu_n(x) = k_n(x)^T (K_n + \sigma I_n)^{-1} y_n, \tag{16}$$

$$k_n(x, x') = k(x, x') - k_n(x)^T (K_n + \sigma I_n)^{-1} k_n(x'),$$

$$\sigma_n^2(x) = k_n(x, x). \tag{17}$$

Here K_n denotes the covariance matrix whose entries are $(K_n)_{i,j} = k(x_i, x_j)$ with $x_i, x_j \in \{x_1, \ldots, x_N\}$ and $k_n(x) = [k(x, x_1), \ldots, k(x, x_N)]^T$ denotes the covariance vector whose entries are the covariance between x and x_j for all $x_j \in \{x_1, \ldots, x_N\}$. The $n \times n$ identity matrix is denoted as I_n.

We consider multi-output GPs to model the unknown function f that outputs states in R^d. (see Section 3). Similar to Equation (16) and Equation (17), we get analogous expressions for the multi-output case in Equation (5) and Equation (6).

A.2 Non-adaptive Multi-output Con dence Bounds

Our Algorithm 1 uses the maximum variance reduction rule to learn about the transition dynamics. As seen in our analysis (see Theorem 2), we are interested in constructing con dence intervals for $\tilde{f}$ only at the end of n iterations (i.e., after taking n samples), and hence, we do not require anytime con dence bounds (e.g., as in Srinivas et al. (2009)). Moreover, in our algorithm, the current decision (s_i, a_i) does not depend on the previous noise realizations. By focusing on the single-output case rst, the following con dence lemma from Vakili et al. (2021), can be used to construct con dence intervals with (β) independent of n which holds w.h.p. for a xed $x \in X$:

Lemma 3. Given n noisy observations of $\tilde{f}: X \to R$ with $\|\tilde{f}\|_k \leq B$ where noise $\{\omega_1, \ldots, \omega_n\}$ is independent of inputs $\{x_1, \ldots, x_n\}$, for $\beta = B + \sigma\sqrt{2\log(2/\delta)}$, and μ_n, σ_n as de ned in Equation (16) and Equation (17), the following holds for a xed $x \in X$ with probability at least $1 - \delta$,

$$|\tilde{f}(x) - \mu_n(x)| \leq \beta\, \sigma_n(x).$$

To extend this result over the entire input set $x \in X$, the authors in Vakili et al. (2021) use a discretization assumption which ensures that there exists a discretization D_n such that $\tilde{f}(x) - \tilde{f}(r(x)) \leq \frac{1}{n^2}$, where $r(x) = \arg\min_{x' \in D_n} \|x - x'\|_2$ and $|D_n| \leq CB^d n^{d/2}$ for C being independent of n and B (RKHS norm bound). Consequently, they obtain the following lemma providing uniform con dence bounds:

Lemma 4. ((Vakili et al., 2021, Theorem-3)) Given n noisy observations of $\tilde{f}: X \to R$, $X \subset R^d$ satisfying $\|\tilde{f}\|_k \leq B$ where noise $\{\omega_1, \ldots, \omega_n\}$ is independent of inputs $\{x_1, \ldots, x_n\} \subset X$ and when there exists discretization

D_n of X with $|D_n| \le CB^d n^{d/2}$, for $\alpha(\delta) = B + \frac{\sigma}{\lambda}\sqrt{2\log(2/\delta)}$ and $\beta_n(\delta) = 2B + \alpha\left(\frac{\delta}{3C(B+\sqrt{n}\,\alpha(2\delta/(3n)))^d n^{d/2}}\right)$, σ_n, μ_n as defined in Equation (16) and Equation (17), the following holds for all $x \in D_n$ with probability at least $1-\delta$,

$$|\tilde{f}(x) - \mu_n(x)| \le \beta_n(\delta)\sigma_n(x).$$

To extend this result to multiple dimensions as required in our work, we take the same discretization assumption as in Vakili et al. (2021). But considering the multi-output definition of f, we define the modified state-action space $\tilde{X}$. This is in line with Chowdhury and Gopalan (2019), which also has a similar multi-output setting. We define the modified state-action space as $\tilde{X} := S \times A \times \{1, 2, \dots, d\}$ where the last dimension $i \in \{1, 2, \dots, d\}$ incorporates the index of the output vector, in the sense that $f(\cdot,\cdot) = (\tilde{f}(\cdot,\cdot,1), \dots, \tilde{f}(\cdot,\cdot,d))$ where $\tilde{f} : \tilde{X} \to \mathbb{R}$. We then detail the discretization assumption as in Vakili et al. (2021) w.r.t. $\tilde{f}$ (see also Section 2 for more details).

Assumption 1. For every $n \in \mathbb{N}$ and $\tilde{f} \in H_k(S \times A \times I)$ there exists a discretization $D_n(S \times A)$ of $S \times A$ such that $\tilde{f}(s,a,i) - \tilde{f}([s,a]_n, i) \le \frac{1}{\sqrt{n}}$, where $[s,a]_n = \arg\min_{(s',a') \in D_n(S\times A)} \|(s,a) - (s',a')\|_2$, $i \in I$, and $|D_n(S \times A)| \le CB^p n^{p/2}$ ($|D_n(S \times A \times I)| \le CB^p n^{p/2} d$) for C being independent of n and B, and $S \times A \subset \mathbb{R}^p$.

Assumption 1 allows us to provide bounds for $\|f(s,a) - \mu_n(s,a)\|_2$ for all $(s,a) \in S$ using Lemma 4. Note that Assumption 1 does not discretize the modified state-action space ($\tilde{X} = S \times A \times \{1, 2, \dots, d\}$) but instead discretizes $S \times A$ for each $i \in I$. Hence, $|D_n(S \times A \times I)| \le CB^p n^{p/2} d$, and $\beta_n(\delta)$ will change accordingly. We describe the following lemma detailing the same.

Lemma 5. Under Assumption 1 with $\beta_n(\delta)$ as in Lemma 4 and training a Gaussian process model on observations up to iteration n ($\{s_1, \dots, s_n\}$) and their corresponding inputs ($\{(s_0, a_0), \dots, (s_{n-1}, a_{n-1})\}$), it holds with probability at least $1-\delta$,

$$\|f(s,a) - \mu_n(s,a)\|_2 \le \beta_n(\delta)\sqrt{d}\,\|\sigma_n([s,a]_n)\|_2 + \frac{2\sqrt{d}}{\sqrt{n}};$$

uniformly for all $(s,a) \in S \times A$ and $[s,a]_n = \arg\min_{(s',a') \in D_n(S\times A)} \|(s,a) - (s',a')\|_2$.

Proof. For any $(s,a) \in S \times A$,

$$
\begin{aligned}
&\|f(s,a) - \mu_n(s,a)\|_2 \\
&= \sqrt{\sum_{i=1}^{d} (\tilde{f}(s,a,i) - \mu_n(s,a,i))^2} && (18)\\
&= \sqrt{\sum_{i=1}^{d} |\tilde{f}(s,a,i) - \tilde{f}([s,a]_n,i) + \tilde{f}([s,a]_n,i) - \mu_n([s,a]_n,i) + \mu_n([s,a]_n,i) - \mu_n(s,a,i)|^2} \\
&\le \sum_{i=1}^{d} |\tilde{f}(s,a,i) - \tilde{f}([s,a]_n,i)| + |\tilde{f}([s,a]_n,i) - \mu_n([s,a]_n,i)| + |\mu_n([s,a]_n,i) - \mu_n(s,a,i)| && (19)\\
&\le \sum_{i=1}^{d} (|\tilde{f}([s,a]_n,i) - \mu_n([s,a]_n,i)|) + \frac{2d}{\sqrt{n}} && (20)\\
&\le \beta_n(\delta) \sum_{i=1}^{d} (\sigma_n([s,a]_n,i)) + \frac{2d}{\sqrt{n}} && (21)\\
&\le \beta_n(\delta)\sqrt{d}\sqrt{\sum_{i=1}^{d} (\sigma_n([s,a]_n,i))^2} + \frac{2d}{\sqrt{n}} && (22)\\
&\le \beta_n(\delta)\sqrt{d}\,\|\sigma_n([s,a]_n)\|_2 + \frac{2d}{\sqrt{n}}. && (23)
\end{aligned}
$$

In Equation (19), Equation (22) we use $\|x\|_2 \le \|x\|_1 \le \sqrt{d}\|x\|_2$. And Equation (20) and Equation (21) follow from Assumption 1 (since $\tilde{f}, \mu_n \in H_k(S \times A \times I)$) and Lemma 4, respectively.

□

A.3 Sample Complexity Guarantees

Our objective is to obtain a uniform upper bound on the model precision$\| _n(s,a) - f(s,a)\|_2$ for all state-action pairs (s,a) while accounting for the errors induced by discretization. Here, $_n(\cdot,\cdot)$ is obtained from Algorithm 1. We achieve this by using Lemma 5 to obtain a bound in terms of maximum information gain (Equation (9)).

Lemma 1. For $_n(\cdot,\cdot)$ set as in Lemma 4 andI_d denoting $\{1,2,\ldots,d\}$, the MVR algorithm (Algorithm 1) outputs the dynamics estimate$\hat{f}_n(\cdot,\cdot) \quad _n(\cdot,\cdot)$ such that the following holds uniformly for all$(s,a) \in S \quad A$ with probability at least $1 \quad$,

$$\| _n(s,a) \quad f(s,a)\|_2 \le O\left(\frac{_n(\cdot,\cdot)\sqrt{d}}{\bar{n}}\sqrt{\frac{\log(nd|S \quad A \quad I_d|)}{}}\right).$$

Proof. From Lemma 5, it holds that with probability at least $1 \quad$ uniformly for all $(s,a) \in S \quad A$:

$$\begin{aligned}
\| _n(s,a) \quad f(s,a)\|_2 &\le \quad _n(\cdot,\cdot) + \sqrt{d}\,\| _n(s,a) - _n(s,a)\|_2 \quad \frac{2d}{\sqrt{\bar{n}}} \\
&\le \quad _n(\cdot,\cdot) + \sqrt{d}\max_{(s,a)\in S \quad A}\| _n(s,a) - _n(s,a)\|_2 \quad \frac{2d}{\sqrt{\bar{n}}} \\
&\le \quad _n(\cdot,\cdot) + \sqrt{d}\,\| _n(s_n,a_n) - _n(s_n,a_n)\|_2 \quad \frac{2d}{\sqrt{\bar{n}}} \\
&\le \frac{2d}{\sqrt{\bar{n}}} \quad \frac{_n(\cdot,\cdot)}{n}\sqrt{d}\sum_{j=1}^{n}\| _j(s_n,a_n) - _j(s_n,a_n)\|_2 \\
&\le \frac{2d}{\sqrt{\bar{n}}} \quad \frac{_n(\cdot,\cdot)}{n}\sqrt{d}\sum_{j=1}^{n}\| _j(s_j,a_j) - _j(s_j,a_j)\|_2 \qquad (24) \\
&\le \frac{_n(\cdot,\cdot)}{\sqrt{\bar{n}}}\sqrt{d}\exp\left(\frac{1}{n}\sum_{j=1}^{n}\| _j(s_j,a_j) - _j(s_j,a_j)\|_2^2\right) \quad \frac{2d}{\sqrt{\bar{n}}} \\
&\le \frac{_n(\cdot,\cdot)\sqrt{2ed}}{\sqrt{\bar{n}}}\sqrt{\frac{\log(nd|S \quad A \quad I_d|)}{}} \quad \frac{2d}{\sqrt{\bar{n}}} \qquad (25) \\
&\le O\left(\frac{_n(\cdot,\cdot)\sqrt{d}}{\sqrt{\bar{n}}}\sqrt{\frac{\log(nd|S \quad A \quad I_d|)}{}}\right). \qquad (26)
\end{aligned}$$

Here, Equation (24) follows from the decision rule in line-4 of Algorithm 1 and Equation (25) is obtained using standard bound for the sum of variances in the case of multi-output GPs from Curi et al. (2021, Lemma-7) and Chowdhury and Gopalan (2019, Lemma-11). □

B Sample Complexity Bounds for KL Uncertainty Sets

Theorem 2. (Sample Complexity of MVR under KL uncertainty set) Consider a robust MDP with nominal transition dynamics f satisfying the regularity assumptions from Section 2 and with uncertainty set defined as in Equation (2) w.r.t. KL divergence. For π^* denoting the robust optimal policy w.r.t. nominal transition dynamics f and $\hat{\pi}_N$ denoting the robust optimal policy w.r.t. learned nominal transition dynamics $\hat{f}_N$ via MVR (Algorithm 1), and $P_0 \in (0, 1]$, $P_0 \in (0, \frac{1}{1-\gamma}]$, it holds that $\max_s |V^R_{\hat{\pi}_N, f}(s) - V^R_{\pi^*, f}(s)| \leq \epsilon$ with probability at least $1 - \delta$ for any N such that

$$N = O\left(e^{\frac{2}{(P_1 - P_0)^2 \rho_{KL}}} \frac{2^2 N^2 (P_0 + P_1)^2 S A}{(P_1 - P_0)^4 \epsilon^2} \log \frac{Nd}{\delta}\right). \tag{27}$$

Proof. Step (i): As detailed in the proof outline of Section 4, in order to bound $|V^R_{\hat{\pi}_n, f}(s) - V^R_{\pi^*, f}(s)|$, we begin by adding and subtracting $V^R_{\hat{\pi}_n, \hat{f}_n}(s)$ which is the robust value function w.r.t. the nominal transition dynamics $\hat{f}_n$ and its corresponding optimal policy $\hat{\pi}_n$. Then, we split the difference into two terms as follows:

$$|V^R_{\hat{\pi}_n, f}(s) - V^R_{\pi^*, f}(s)| \leq \underbrace{|V^R_{\hat{\pi}_n, f}(s) - V^R_{\hat{\pi}_n, \hat{f}_n}(s)|}_{(i)} + \underbrace{|V^R_{\hat{\pi}_n, \hat{f}_n}(s) - V^R_{\pi^*, f}(s)|}_{(ii)}. \tag{28}$$

In order to not disturb the flow of the proof we bound (i) and (ii) separately Lemma 6 and Lemma 7 respectively. From Lemma 6, we obtain that

$$\begin{aligned}(i) &\leq \max_s |V^R_{\hat{\pi}_n, f}(s) - V^R_{\hat{\pi}_n, \hat{f}_n}(s)| \\ &\leq \frac{\gamma}{1-\gamma} \max_s \left| \inf_{KL(p \| P_f(s, \hat{\pi}_n(s))) \leq \rho} \mathbb{E}_{s' \sim p}\left[V^R_{\hat{\pi}_n, f}(s')\right] - \inf_{KL(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \leq \rho} \mathbb{E}_{s' \sim p}\left[V^R_{\hat{\pi}_n, f}(s')\right] \right|.\end{aligned} \tag{29}$$

And from Lemma 7, we obtain that

$$\begin{aligned}(ii) &\leq \max_s |V^R_{\hat{\pi}_n, \hat{f}_n}(s) - V^R_{\pi^*, f}(s)| \\ &\leq \frac{\gamma}{1-\gamma} \max_s \left| \inf_{KL(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \leq \rho} \mathbb{E}_{s' \sim p}\left[V^R_{\pi^*, f}(s')\right] - \inf_{KL(p \| P_f(s, \hat{\pi}_n(s))) \leq \rho} \mathbb{E}_{s' \sim p}\left[V^R_{\pi^*, f}(s')\right] \right|.\end{aligned} \tag{30}$$

Note that both these terms in Equations (29) and (30) are of the form mentioned in the Step (i) of Section 4.

Step (ii): Next, corresponding to Step (ii) of the proof outline in Section 4, we use Lemma 2 to bound Equations (29) and (30). Denote $M := \frac{1}{1-\gamma} \cdot \max_s V^R(s)$ for convenience. Using Equation (29) and Lemma 9 (internally using Lemma 2), conditioned on the event of Lemma 9 holding true, it holds that

$$\begin{aligned}(i) &\leq \max_s |V^R_{\hat{\pi}_n, f}(s) - V^R_{\hat{\pi}_n, \hat{f}_n}(s)| \\ &\leq \frac{1}{1-\gamma} \max_s \left| \inf_{KL(p \| P_f(s, \hat{\pi}_n(s))) \leq \rho} \mathbb{E}_{s' \sim p}\left[V^R_{\hat{\pi}_n, f}(s')\right] - \inf_{KL(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \leq \rho} \mathbb{E}_{s' \sim p}\left[V^R_{\hat{\pi}_n, f}(s')\right] \right| \\ &\leq \max_{s,a} 2 M^2 e^{\frac{M}{\alpha}} \max_{Pr_\alpha(\cdot) \leq \frac{M}{\alpha}} \left| \mathbb{E}_{s' \sim P_{\hat{f}_n}(s,a)}\left[e^{-\frac{V^R_{\hat{\pi}_n, f}(s')}{\alpha}}\right] - \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V^R_{\hat{\pi}_n, f}(s')}{\alpha}}\right] \right| \quad : \end{aligned} \tag{31}$$

$$\leq \max_{V \in \mathcal{V}} \max_{s,a} 2 M^2 e^{\frac{M}{\alpha}} \max_{Pr_\alpha(\cdot) \leq \frac{M}{\alpha}} \left| \mathbb{E}_{s' \sim P_{\hat{f}_n}(s,a)}\left[e^{-\frac{V(s')}{\alpha}}\right] - \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\alpha}}\right] \right| \quad : \tag{32}$$

We can bound (ii) similarly.

$$(ii) \leq \max_s |V^R_{\hat{\pi}_n, \hat{f}_n}(s) - V^R_{\pi^*, f}(s)| \tag{33}$$

$$\leq \max_{V \in \mathcal{V}} \max_{s,a} 2 M^2 e^{\frac{M}{\alpha}} \max_{Pr_\alpha(\cdot) \leq \frac{M}{\alpha}} \left| \mathbb{E}_{s' \sim P_{\hat{f}_n}(s,a)}\left[e^{-\frac{V(s')}{\alpha}}\right] - \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\alpha}}\right] \right| \quad : \tag{34}$$

Step (iii): Next, we want to utilize the learning error bound (Equation (26)) that bounds the di erence between the means of true nominal transition dynamics P_f and learned nominal transition dynamics $P_{\hat{f}_n}$ to bound Equations (32) and (34).

We begin by bounding the di erence $E_{s^1 \sim P_{\hat{f}_n}(\cdot|s,a)}[r e^{\frac{V(s^1)}{\tau}}] - E_{s^1 \sim P_f(\cdot|s,a)}[r e^{\frac{V(s^1)}{\tau}}]$, by the di erence in means of P_f and $P_{\hat{f}_n}$ in Lemma 10. Since Equation (32) has a max over all value functions, we introduce a covering number argument in Lemma 12 to reform it to a max over the functions in the covering set. We then use Lemma 10 to obtain bounds in terms of maximum information gain γ_{Nd} (Equation (9)) and . Further details regarding the covering number argument are deferred to Lemma 12. Then, we apply the result of Lemma 12 with 1 (de ned in Lemma 12) on Equation (32). Then, it holds that

$$(i) \le \max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{n},\hat{f}_n}(s)| \le O\left(2M^2 e^{\frac{M}{\kappa_{kl}}} e^{\frac{1}{\kappa_{kl}}} \frac{\gamma_n \sqrt{2e\sigma^2 \gamma_{nd}}}{\bar{n}}\right), \tag{35}$$

where κ_{kl} is a problem-dependent constant denoting the minimum value of $\underline{\ }$ de ned in Lemma 9. A similar constant also appears in the sample complexity bounds provided in Panaganti and Kalathil (2022); Zhou et al. (2021). Note that γ_n, which appears in Lemma 3, has a logarithmic dependence on n. Similarly, from Equation (34) and Lemmas 10 and 12, we obtain

$$(ii) \le \max_s |V^R_{\hat{n},\hat{f}_n}(s) - V^R_{\hat{f}}(s)| \le O\left(2^{\frac{M^2}{\kappa_{kl}}} e^{\frac{M}{\kappa_{kl}}} e^{\frac{1}{\kappa_{kl}}} \frac{\gamma_n \sqrt{2e\sigma^2 \gamma_{nd}}}{\bar{n}}\right). \tag{36}$$

Note that we want to bound $|V^R_{\hat{n},f}(s) - V^R_{\hat{f}}(s)| \le (i) + (ii)$ over all $s \in S$. Using $\max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{f}}(s)| \le \max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{n},\hat{f}_n}(s)| + \max_s |V^R_{\hat{n},\hat{f}_n}(s) - V^R_{\hat{f}}(s)|$ and substituting M by $1/\{(1-\rho)\sigma\}$, we obtain from Equation (35) and Equation (36)

$$\max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{f}}(s)| \le O\left(e^{\frac{1}{(1-\rho)\sigma\kappa_{kl}}} e^{\frac{1}{\kappa_{kl}}} \frac{\gamma_n \sqrt{2e\gamma_{nd}}}{(1-\rho)\sigma^2 \sqrt{\bar{n}}}\right).$$

Finally, to ensure that $\max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{f}}(s)| \le \varepsilon$, it su ces to have

$$\max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{f}}(s)| \le O\left(e^{\frac{1}{(1-\rho)\sigma\kappa_{kl}}} e^{\frac{1}{\kappa_{kl}}} \frac{\gamma_n \sqrt{2e\gamma_{nd}}}{(1-\rho)\sigma^2 \sqrt{\bar{n}}}\right) \le \varepsilon.$$

By inverting the previously obtained result, we arrive at

$$n \ge O\left(e^{\frac{2}{(1-\rho)\sigma\kappa_{kl}}} e^{\frac{2}{\kappa_{kl}}} \frac{\gamma_n^2 (1-\rho)\sigma^2 \gamma_{nd}}{(1-\rho)^4 \varepsilon^2}\right).$$

□

Lemma 6. (Simpli cation using robust Bellman equation) Denote $(i) := |V^R_{\hat{n},f}(s) - V^R_{\hat{n},\hat{f}_n}(s)|$ for $V^R_{\hat{n},f}$ being the robust value function of policy $\hat{\pi}_n$ w.r.t. true nominal transition dynamics f and $V^R_{\hat{n},\hat{f}_n}$ being the robust value function of policy $\hat{\pi}_n$ w.r.t. learned nominal transition dynamics $\hat{f}$. Then the following holds,

$$\begin{aligned}
(i) &= |V^R_{\hat{n},f}(s) - V^R_{\hat{n},\hat{f}_n}(s)| \\
&\le \max_s |V^R_{\hat{n},f}(s) - V^R_{\hat{n},\hat{f}_n}(s)| \\
&\le \frac{1}{\underline{\ }} \max_s \Big| \inf_{D(p||P_f(s,\hat{\pi}_n(s)))} E_{s^1 \sim p}[V^R_{\hat{n},f}(s^1)] - \inf_{D(p||P_{\hat{f}_n}(s,\hat{\pi}_n(s)))} E_{s^1 \sim p}[V^R_{\hat{n},f}(s^1)] \Big| .
\end{aligned} \tag{37}$$

Proof. Since both the quantities are w.r.t. the same policy, using the de nition of the robust Q-function and the robust Bellman equation (see Equation (4)), we obtain:

$$(i) \quad |V^R_{\hat{n},f}(s) - V^R_{\hat{n},\hat{f}_n}(s)| \tag{38}$$

$$
\begin{aligned}
&| Q^R_{\hat{\pi}_n;f}(s,\hat{\pi}_n(s),a) - Q^R_{\hat{\pi}_n;\hat{f}_n}(s,\hat{\pi}_n(s),a)| \\
&| r(s,\hat{\pi}_n(s),a) - r(s,\hat{\pi}_n(s),a) \\
&\quad + \inf_{D(p\|P_f(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;\hat{f}_n}(s')| \\
&| \inf_{D(p\|P_f(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;\hat{f}_n}(s')| \qquad (39)
\end{aligned}
$$

Adding and subtracting $\inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s')$ to Equation (39), we obtain the following two terms:

$$
\begin{aligned}
(i_a) \quad & | \inf_{D(p\|P_f(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s')|; \\
(i_b) \quad & | \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;\hat{f}_n}(s')|:
\end{aligned}
$$

Now, we use Lemma 8 to bound(i_b). We have:

$$
\begin{aligned}
(i_b) \quad & | \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;\hat{f}_n}(s')| \\
& \overset{\text{Lemma 8}}{\le} \max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)| \qquad (\text{Lemma 8}) \qquad (40)
\end{aligned}
$$

Plugging Equation (40) into Equation (38) and using the fact that $(i) \le (i_a) + (i_b)$, we have

$$
\begin{aligned}
(i) \quad & |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)| \qquad (41) \\
& \le (i_a) + \max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)| \\
& \quad + | \inf_{D(p\|P_f(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s')| \\
& \quad \max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)|: \qquad (42)
\end{aligned}
$$

Taking maximum over states in Equation (41) and Equation (42) we have

$$
\begin{aligned}
&\max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)| \\
&\le \max_s \inf_{D(p\|P_f(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') \\
&\quad \max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)|:
\end{aligned}
$$

Moving $\max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)|$ to the LHS and dividing $(1-\gamma)$ on both sides, it holds that

$$
\begin{aligned}
&(i) \le \max_s |V^R_{\hat{\pi}_n;f}(s) - V^R_{\hat{\pi}_n;\hat{f}_n}(s)| \\
&\le \frac{1}{1-\gamma} \max_s \inf_{D(p\|P_f(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') - \inf_{D(p\|P_{\hat{f}_n}(s,\hat{\pi}_n(s),a))\le\rho} \mathbb{E}_{s'\sim p}\, V^R_{\hat{\pi}_n;f}(s') : \qquad (43)
\end{aligned}
$$

□

Lemma 7. (Simplification using robust Bellman equation) Denote $(ii): |V^R_{\hat{\pi}_n;\hat{f}_n}(s) - V^R_{\hat{\pi}_n;f}(s)|$ for $V^R_{\hat{\pi}_n;\hat{f}_n}$ being the robust value function of policy $\hat{\pi}_n$ w.r.t. learned nominal transition dynamics $\hat{f}_n$ and $V^R_{\hat{\pi}_n;f}$ being the robust value function of policy $\hat{\pi}_n$ w.r.t. true nominal transition dynamics f. Then the following holds,

$$
(ii) \le |V^R_{\hat{\pi}_n;\hat{f}_n}(s) - V^R_{\hat{\pi}_n;f}(s)|
$$

$$
\begin{aligned}
&\le \max_s V^{R}_{\hat{\pi}_n, \hat{f}_n}(s) - V^{R}_{\pi, f}(s) \\
&\le \frac{\gamma}{1-\gamma} \max_s \left(\inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') - \inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') \right). \qquad (44)
\end{aligned}
$$

Proof. We first note that $Q^{R}_{\pi, f}(s, \hat{\pi}_n(s)) \le Q^{R}_{\pi, f}(s, \pi(s))$ as π is the robust optimal policy for the nominal transition dynamics f (see Equation (3)). As a result, we have

$$
\begin{aligned}
(ii) &= | V^{R}_{\hat{\pi}_n, \hat{f}_n}(s) - V^{R}_{\pi, f}(s) | \qquad (45) \\
&= | Q^{R}_{\hat{\pi}_n, \hat{f}_n}(s, \hat{\pi}_n(s)) - Q^{R}_{\pi, f}(s, \pi(s)) | \\
&\le | Q^{R}_{\hat{\pi}_n, \hat{f}_n}(s, \hat{\pi}_n(s)) - Q^{R}_{\pi, f}(s, \hat{\pi}_n(s)) | \\
&= | r(s, \hat{\pi}_n(s)) - r(s, \hat{\pi}_n(s)) \\
&\quad + \gamma \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\hat{\pi}_n, \hat{f}_n}(s') - \gamma \inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') |. \\
&= \gamma | \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\hat{\pi}_n, \hat{f}_n}(s') - \inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') | \qquad (46)
\end{aligned}
$$

Adding and subtracting $\gamma \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s')$ to Equation (46), we obtain the following two terms:

$$
(ii_a) = \gamma | \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\hat{\pi}_n, \hat{f}_n}(s') - \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') |;
$$

$$
(ii_b) = \gamma | \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') - \inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') |.
$$

Now, we use Lemma 8 to bound (ii_a). We have:

$$
\begin{aligned}
(ii_a) &= \gamma | \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\hat{\pi}_n, \hat{f}_n}(s') - \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') | \\
&\le \gamma \max_s V^{R}_{\pi, f}(s) - V^{R}_{\hat{\pi}_n, \hat{f}_n}(s). \qquad (47)
\end{aligned}
$$

Plugging Equation (47) into Equation (45) and using the fact that $(ii) = (ii_a) + (ii_b)$, we have

$$
\begin{aligned}
(ii) &= | V^{R}_{\pi, f}(s) - V^{R}_{\hat{\pi}_n, \hat{f}_n}(s) | \qquad (48) \\
&\le (ii_b) + \gamma \max_s V^{R}_{\pi, f}(s) - V^{R}_{\hat{\pi}_n, \hat{f}_n}(s) \\
&= \gamma | \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') - \inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') | \\
&\quad + \gamma \max_s V^{R}_{\pi, f}(s) - V^{R}_{\hat{\pi}_n, \hat{f}_n}(s). \qquad (49)
\end{aligned}
$$

Taking maximum over states in Equation (48) and Equation (49) and following similar steps as in Equation (43), we have

$$
\begin{aligned}
(ii) \le \max_s V^{R}_{\pi, f}(s) - V^{R}_{\hat{\pi}_n, \hat{f}_n}(s) &\le \gamma \max_s \left(\inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\hat{\pi}_n, f}(s') - \inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\hat{\pi}_n, f}(s') \right) \\
&\quad + \gamma \max_s V^{R}_{\pi, f}(s) - V^{R}_{\hat{\pi}_n, \hat{f}_n}(s) \\
&\le \frac{\gamma}{1-\gamma} \max_s \left(\inf_{D(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') - \inf_{D(p \| P_f(s, \hat{\pi}_n(s))) \le \delta} \mathbb{E}_{s' \sim p} V^{R}_{\pi, f}(s') \right). \qquad (50)
\end{aligned}
$$

□

Lemma 8. (from Panaganti and Kalathil (2022, Lemma 1)) Let V_1 and V_2 be two value functions from $S \tilde{N} r 0; 1\{p1 \quad qs$ Let D be any distance measure between probability distributions (e.g., KL-divergence,^{2} divergence, or variation distance de ned in Equation (2)). The following inequality (1-Lipschitz w.r.t. V) holds true

$$\inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \qquad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_2ps^1q \qquad \cdot \qquad \max_{s^1}|V_2ps^1q \qquad V_1ps^1q|:$$

Proof. We want to bound

$$\inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \qquad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_2ps^1q\ :$$

Notice that

$$\begin{aligned}
&\inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \qquad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_2ps^1q \\
&\quad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} \sup_{D\,pp^1||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \quad E_{s^1\ p^1}\ V_2ps^1q \\
&¥ \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \quad E_{s^1\ p}\ V_2ps^1q \\
&\quad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \quad V_2ps^1q\ ;
\end{aligned}$$

where the inequality follows from the property of supremum. By the de nition of inf, for any ¡ 0, there exists some distribution q s.t. $D\,pq||P_{f\sim}ps;aqq\cdot$ satisfying

$$E_{s^1\ q}\ V_1ps^1q \quad V_2ps^1q \qquad \cdot \inf_{D\,pp||P_{f\sim}ps;a\,qqq\cdot} E_{s^1\ p}\ V_1ps^1q \quad V_2ps^1q\ :$$

Then, we have

$$\begin{aligned}
&\inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_2ps^1q \qquad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \\
&\cdot \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \quad V_2ps^1q \\
&\cdot E_{s^1\ q}\ V_1ps^1q \quad V_2ps^1q \\
&\cdot E_{s^1\ q}\ V_2ps^1q \quad V_1ps^1q \\
&\cdot \max_{s^1}|V_2ps^1q \quad V_1ps^1q| \quad : \qquad (51)
\end{aligned}$$

Let $\tilde{N}$ 0, we obtain one side of the desired bound.

One can similarly bound $\inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \quad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_2ps^1q$ by just interchanging V_1 and V_2 everywhere. Combining this argument with Equation (51), we obtain

$$\inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_1ps^1q \qquad \inf_{D\,pp||P_{f\sim}ps;a\,qq\cdot} E_{s^1\ p}\ V_2ps^1q \qquad \cdot \qquad \max_{s^1}|V_2ps^1q \qquad V_1ps^1q|:$$

□

Lemma 9. (Simpli cation using Lemma 2 reformulation) For any value function $V\,p\,q: S \tilde{N} r 0; 1\{p1 \quad qs$ de ne the event E as follows:

$$\max_s \inf_{KL\ pp||P_{f\hat{}n}\ ps;\hat{}n\ psqqq\cdot} E_{s^1\ p}\ V\,ps^1q \qquad \inf_{KL\ pp||P_f\ ps;\hat{}n\ psqqq\cdot} E_{s^1\ p}\ V\,ps^1q \quad \cdot$$

$$\max_{s;a} 2\frac{M}{-}e^{\frac{M}{-}} \max_{Pr_{-};\bar{-}s} E_{s^1\ P_{f\hat{}n\ ps;a\ q}}re^{-\frac{V\,ps^1q}{}}s \quad E_{s^1\ P_f\ ps;a\,q}re^{-\frac{V\,ps^1q}{}}s\ :$$

Then, for any $n \geq t$ $\max_{s,a} N^{1}(p, P_f(s,a)q) \max_{s,a} N^{2}(p, P_f(s,a)q)u$where $N^{1}(p, P_f(s,a)q) \leq \frac{\frac{2}{n} p\, q2ed^{2}\ nd}{p - \frac{e}{2} q^{2}}$ and $N^{2}(p, P_f(s,a)q) \leq \frac{4M^{2} e^{\frac{2M}{-}} \frac{2}{n} p\, q2ed^{2}\ nd}{p\ q^{2}}$ with $- \frac{M}{}$, $M \frac{1}{1}$, de ned in Equation (67), de ned in Equation (70), and $\_ \{2$ de ned in Equation (56), the event E holds true with probability at least 1 .

Proof. (A similar proof as in Zhou et al. (2021, Lemma-4)). First note that,

$$\max_{s} \inf_{KL(p\|P_{f^{\wedge}_n}(s,\hat{}_n(s)qqq)\leq} E_{s^{1}\sim p} V(s^{1}q \inf_{KL(p\|P_f(s,\hat{}_n(s)qqq)\leq} E_{s^{1}\sim p} V(s^{1}q \leq$$

$$\max_{s,a} \inf_{KL(p\|P_{f^{\wedge}_n}(s,a)qq)\leq} E_{s^{1}\sim p} V(s^{1}q \inf_{KL(p\|P_f(s,a)qq)\leq} E_{s^{1}\sim p} V(s^{1}q : \quad (52)$$

Recall (Hu and Hong, 2013, Theorem-1) for distributionally robust optimization with a random variable X and a random function H. One can rewrite an in nite-dimensional optimization problem as a scalar optimization problem:

$$\sup_{P:KL(p\|P_0)q\leq} E_{X\sim P}(H(X)qs) = \inf_{\geq 0} t\ \log(pE_{X\sim P_0}(e^{\frac{H(X)q}{}})sq) - u. \quad (53)$$

For now, we focus on bounding $\inf_{KL(p\|P_{f^{\wedge}_n}(s,a)qq)\leq} E_{s^{1}\sim p} V(s^{1}q \inf_{KL(p\|P_f(s,a)qq)\leq} E_{s^{1}\sim p} V(s^{1}q$ for one particular $(s,a)q$. For brevity, we write $P_f(s,a)q$ and $P_{f^{\wedge}_n}(s,a)q$ as P_f and $P_{f^{\wedge}_n}$, respectively. By Equation (53), we have

$$\inf_{P:KL(p\|P_f)q\leq} E_{s^{1}\sim P}(V(s^{1}q)s) = \max_{\geq 0} t\ \log(pE_{s^{1}\sim P_f}(e^{\frac{V(s^{1}q)}{}})sq) - u; \quad (54)$$

$$\inf_{P:KL(p\|\hat{P}_{f^{\wedge}_n})q\leq} E_{s^{1}\sim P}(V(s^{1}q)s) = \max_{\geq 0} t\ \log(pE_{s^{1}\sim P_{f^{\wedge}_n}}(e^{\frac{V(s^{1}q)}{}})sq) - u. \quad (55)$$

For the nite state-action space setting, Zhou et al. (2021, Lemma-4) characterizes the property of the optimal . Following a similar proof strategy, we denote

$$\arg\max_{\geq 0} t\ \log(pE_{s^{1}\sim P_f}(e^{\frac{V(s^{1}q)}{}})sq) - u; \quad (56)$$

and

$$\hat{}_n \arg\max_{\geq 0} t\ \log(pE_{s^{1}\sim P_{f^{\wedge}_n}}(e^{\frac{V(s^{1}q)}{}})sq) - u. \quad (57)$$

To ensure that $\max_{\geq 0} t\ \log(pE_{s^{1}\sim P_f}(e^{\frac{V(s^{1}q)}{}})sq) - u$ $\max_{\geq 0} t\ \log(pE_{s^{1}\sim P_{f^{\wedge}_n}}(e^{\frac{V(s^{1}q)}{}})sq) - u$ is small enough, we need to show that and $\hat{}_n$ are close enough. For this, one considers two di erent cases, 0 and $\neq 0$.

Case-1: In Case-1, we investigate the conditions for$\hat{}_n$ 0 given that 0. According to (Hu and Hong, 2013, Proposition-2), for 0 to occur, the random variable $Y : V(s^{1}q)$ where $s^{1} N(f(s,a)q, {}^{2}I)q$ must satisfy three conditions namely, (i) Y must be bounded, (ii) Y must have nite mass at its essential in mum, and (iii) the nite mass at essential in mum should be greater than e . So we want to verify whether these conditions hold true for $\hat{Y}_n : V(s^{1}q)$ where $s^{1} N(f^{\wedge}_n(s,a)q, {}^{2}I)q$ when Y satis es these conditions.

We restate de nition of the essential in mum for a real-valued random variable Y, denoted as$ESI(pY)q$,

$$ESI(pY)q \sup\{t \in R : P(t Y) \quad u\} \quad 0u. \quad (58)$$

We rst show that $Y V(s^{1}q)$ where $s^{1} N(f(s,a)q, {}^{2}I)q$ and $\hat{Y}_n V(s^{1}q)$ where $s^{1} N(f^{\wedge}_n(s,a)q, {}^{2}I)q$ have the same essential in mum. By the de nition of $ESI(pY)q$, for any $\neq 0$, it holds that

$$P(t ESI(pY)q \in Y \quad ESI(pY)q \quad u \neq 0; \quad P(t Y \quad ESI(pY)qu \quad 0. \quad (59)$$

It implies for $Y \in V(s^{-1})$ and $s^{-1} \in N(f(s); a(\cdot), \sigma^2 I(\cdot))$ that

$$P_{s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : ESI_p(Y) \in V(s^{-1}) \setminus ESI_p(Y)\} > 0, \tag{60}$$

$$P_{s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : Y \in V(s^{-1}) \setminus ESI_p(Y)\} = 0. \tag{61}$$

It further implies that, the set $\{s^{-1} \in P \mid R^d : ESI_p(Y) \in V(s^{-1}) \setminus ESI_p(Y)\}$ must have a Lebesgue measure greater than 0 and $\{s^{-1} \in P \mid R^d : V(s^{-1}) \setminus ESI_p(Y)\}$ must have a Lebesgue measure equal to 0 since $s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))$ is a continuous distribution.

Due to this fact that the set $\{s^{-1} \in P \mid R^d : ESI_p(Y) \in V(s^{-1}) \setminus ESI_p(Y)\}$ has a Lebesgue measure greater than zero and noting that $N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))$ is also a continuous distribution with the same support as of $N(f(s); a(\cdot), \sigma^2 I(\cdot))$ (i.e., the probability density function of $N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))$ is positive whenever probability density function of $N(f(s); a(\cdot), \sigma^2 I(\cdot))$ is positive), it holds that

$$P_{s^{-1} \sim N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : ESI_p(Y) \in \hat{Y}_n \setminus V(s^{-1}) \setminus ESI_p(Y)\} > 0. \tag{62}$$

A similar argument follows for

$$P_{s^{-1} \sim N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : \hat{Y}_n \setminus V(s^{-1}) \setminus ESI_p(Y)\} = 0. \tag{63}$$

In essence, Equations (62) and (63) imply,

$$Pt\,ESI_p(Y) \in \hat{Y}_n \setminus ESI_p(Y) > 0; \quad Pt\,\hat{Y}_n \setminus ESI_p(Y) = 0.$$

Hence, from the definition of ESI_p in Equations (58) and (59), we have $ESI_p(Y) \subseteq ESI_p(\hat{Y}_n)$.

As a result, for $\epsilon = 0$ to occur and for $Y \in V(s^{-1}) \cap s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))$ to have finite mass at the essential infimum (condition-(ii)), i.e, $Pt\,Y \setminus ESI_p(Y) > 0$, it requires that

$$P_{s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : Y \in V(s^{-1}) \setminus ESI_p(Y)\} > 0.$$

This will further require that the set $\{s^{-1} \in P \mid R^d : Y \in V(s^{-1}) \setminus ESI_p(Y)\}$ must have a Lebesgue measure greater than 0. Following a similar argument as to have obtained Equation (62) (the probability density function of $N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))$ is positive whenever probability density function of $N(f(s); a(\cdot), \sigma^2 I(\cdot))$ is positive), the set $\{s^{-1} \in P \mid R^d : Y \in V(s^{-1}) \setminus ESI_p(Y)\}$ having Lebesgue measure greater than 0, will imply

$$P_{s^{-1} \sim N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : \hat{Y}_n \setminus V(s^{-1}) \setminus ESI_p(Y)\} > 0, \tag{64}$$

and

$$Pt\,\hat{Y}_n \setminus ESI_p(Y) > 0 \tag{65}$$

Since $ESI_p(Y) \subseteq ESI_p(\hat{Y}_n)$, Equations (64) and (65) imply

$$Pt\,\hat{Y}_n \setminus ESI_p(\hat{Y}_n) > 0, \tag{66}$$

Hence, if $Pt\,Y \setminus ESI_p(Y) > 0$ holds true, it also holds that $Pt\,\hat{Y}_n \setminus ESI_p(\hat{Y}_n) > 0$. This implies that whenever Y has a finite mass at its essential infimum, $\hat{Y}_n$ also has finite mass at its essential infimum (condition-(ii) satisfied).

But, recall that according to (Hu and Hong, 2013, Proposition-2) for $\epsilon = 0$ to occur, the finite mass which Y has at its essential infimum should also be greater than ϵ (condition-(iii)). Hence, one has to check if Y satisfies

$$P_{s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : Y \in V(s^{-1}) \setminus ESI_p(Y)\} > \epsilon, \tag{67}$$

what is the condition that Y_n satisfies

$$P_{s^{-1} \sim N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : \hat{Y}_n \setminus V(s^{-1}) \setminus ESI_p(\hat{Y}_n)\} > \epsilon,$$

so that $\hat{\epsilon}_n = 0$ whenever $\epsilon = 0$. Denote : $P_{s^{-1} \sim N(f(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : Y \in V(s^{-1}) \setminus ESI_p(Y)\} = \epsilon$, $P_{s^{-1} \sim N(\hat{f}_n(s); a(\cdot), \sigma^2 I(\cdot))}\{s^{-1} \in P \mid R^d : \hat{Y}_n \setminus V(s^{-1}) \setminus ESI_p(\hat{Y}_n)\} = \hat{\epsilon}_n$ and $S_{min} = \{s^{-1} \in P \mid R^d : V(s^{-1}) \setminus ESI_p(Y) \setminus ESI_p(\hat{Y}_n)\}$. If $\hat{\epsilon}_n < \epsilon$ and $\epsilon_n \leq \frac{\epsilon}{2}$, then it will hold that $\epsilon_n < \epsilon$.

$$|\epsilon - \hat{\epsilon}_n| \leq \int_{S_{min}} \frac{1}{\sqrt{(2\pi)^2 \sigma^4}} \left(e^{-\frac{\{s^{-1}(f(s)) - a(\cdot)\}^2}{2}} - e^{-\frac{\{s^{-1}(\hat{f}_n(s)) - a(\cdot)\}^2}{2}} \right) d(\cdot)$$

$$\begin{aligned}
&\leq \int_{S_{min}}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\{s^{-1}(f(s,a)-q)\}^2}{2}} \, e^{-\frac{\{s^{-1}(\hat{f}_n(s,a)-q)\}^2}{2}} \, dx \\
&\leq \int_{R^d}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\{s^{-1}(f(s,a)-q)\}^2}{2}} \, e^{-\frac{\{s^{-1}(\hat{f}_n(s,a)-q)\}^2}{2}} \, dx \\
&\leq \|f(s,a) - \hat{f}_n(s,a)\|_2 \quad \text{(Lemma 10)} \\
&\leq O\left(\frac{\sqrt{2ed^2\sigma^2 nd}}{n}\right);
\end{aligned}$$

We need $O\left(\frac{\sqrt{2ed^2\sigma^2 nd}}{n}\right) \leq \frac{\epsilon}{2}$, which in turn requires $n \geq O\left(\frac{2\sigma^2(2ed^2\sigma^2 nd)}{(\frac{\epsilon}{2})^2}\right) \geq N^{-1}(\epsilon; P_f(s,a))$. Hence, for $n \geq \max_{s,a} N^{-1}(\epsilon; P_f(s,a))$ with probability at least $1-\delta$, it holds that

$$\|\hat{P}_n - P_f\| \leq \epsilon;$$

for all $(s,a) \in S \times A$ whenever $\epsilon \geq \epsilon_n$, implying $\epsilon_n \to 0$ whenever $\epsilon \to 0$.

Case-2: Consider the case of $\epsilon_n > 0$. The idea is to bound both ρ^π and $\hat{\rho}^\pi_n$ by a set $\{\underline{\rho}, \bar{\rho}\}$ and bound $\max_{\theta \geq 0} |\log(\mathbb{E}_{s' \sim P_f(s,a)}[e^{-\theta V^\pi(s')}]) - \log(\mathbb{E}_{s' \sim P_{f'}(s,a)}[e^{-\theta V^\pi(s')}])|$ for $f, f' \in \{\underline{f}, \bar{f}\}$ taking values within set $\{\underline{\rho}, \bar{\rho}\}$. We first provide a upper bound for θ as $\frac{M}{\sigma^2}$ where $M = \frac{1}{1-\gamma}$ denoting the maximum value of $V^\pi(s')$.

$$\begin{aligned}
&\max_{\theta \geq 0} \left| \log(\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]) - \log(\mathbb{E}_{s' \sim P_{f'}}[e^{-\theta V^\pi(s')}]) \right| \\
&\geq \lim_{\theta \to 0} \left| \log(\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]) - \log(\mathbb{E}_{s' \sim P_{f'}}[e^{-\theta V^\pi(s')}]) \right| \\
&= |\mathrm{ESI}(V^\pi(s'); s' \sim P_f) - \mathrm{ESI}(V^\pi(s'); s' \sim P_{f'})| \quad \text{(Lemma 11)} \\
&> 0. \qquad (68)
\end{aligned}$$

Since $\max_s V^\pi(s) \leq M$, we have

$$\log(\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]) \geq \log(e^{-M\theta}) = -M\theta.$$

It implies for $\theta < \frac{M}{\sigma^2}$ that

$$\log(\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]) > 0. \qquad (69)$$

By Equation (68), since $\max_{\theta \geq 0} |\log(\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]) - \log(\mathbb{E}_{s' \sim P_{f'}}[e^{-\theta V^\pi(s')}])| > 0$, $\arg\max_{\theta \geq 0} |\log(\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]) - \log(\mathbb{E}_{s' \sim P_{f'}}[e^{-\theta V^\pi(s')}])|$ cannot be greater than $\frac{M}{\sigma^2}$ due to Equation (69) holding for all $\theta < \frac{M}{\sigma^2}$. Hence, we have $\underline{\rho} \leq \frac{M}{\sigma^2}$. A similar argument holds for $\hat{\rho}_n$ and it holds that $\hat{\rho}_n \leq \frac{M}{\sigma^2}$.

Denote $\underline{\rho} := \{\underline{f}, \bar{f}\} := \frac{M}{\sigma^2}$, and

$$\Delta := \min\left(\underline{\rho} |\log(\mathbb{E}_{s' \sim P_f}[e^{-\underline{\rho} V^\pi(s')}]) - \underline{\rho}|, \bar{\rho} |\log(\mathbb{E}_{s' \sim P_f}[e^{-\bar{\rho} V^\pi(s')}]) - \bar{\rho}|\right) \log(\mathbb{E}_{s' \sim P_f}[e^{-\underline{\rho} V^\pi(s')}]) - \log(\mathbb{E}_{s' \sim P_f}[e^{-\bar{\rho} V^\pi(s')}]).$$

We first show that,

$$\left|\log\frac{\mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}]}{\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]}\right| \leq e^{M\theta} \left|\mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}] - \mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]\right|. \qquad (70)$$

Consider 2 cases $\mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}] \geq \mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]$ and $\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}] > \mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}]$

Case-1: $\mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}] \geq \mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]$:

$$\left|\log\frac{\mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}]}{\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]}\right| \quad \log\frac{\mathbb{E}_{s' \sim P_{\hat{f}_n}}[e^{-\theta V^\pi(s')}]}{\mathbb{E}_{s' \sim P_f}[e^{-\theta V^\pi(s')}]}$$

$$\log\Big(1+\frac{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}\Big)$$

$$\leq \frac{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}$$

$$\leq e^{\frac{M}{\eta}}\big(E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)$$

Case-2: $E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big] \leq E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]$.

$$\Big|\log\Big(\frac{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}\Big)\Big| \leq \log\Big(\frac{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}\Big)$$

$$\log\Big(1+\frac{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}\Big)$$

$$\leq \frac{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}$$

$$\leq e^{\frac{M}{\eta}}\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)$$

Hence, Equation (70) holds. Then, for $P(r,\bar{s})$, we have

$$\Big|\log\big(E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)-\log\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)\Big| \tag{71}$$

$$\Big|\log\Big(1+\frac{E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}{E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]}\Big)\Big|$$

$$\overset{(i)}{\leq} e^{\frac{M}{\eta}}\Big|E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]-E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\Big|$$

$$\overset{(ii)}{\leq} e^{\frac{M}{\eta}}\big\{f(ps,a)-f'_n(ps,a)\big\} \quad (\text{Lemma 10})$$

$$\overset{(iii)}{\leq} O\Big(e^{\frac{M}{\eta}}\epsilon_n(p,q)\sqrt{\frac{2ed^2\ln d}{n}}\Big) \quad (\text{from Equation (26)}); \tag{72}$$

Here (i) holds from Equation (70), (ii) from Lemma 10 and (iii) from Equation (26).

We further show that $\hat{\epsilon}_n(P(r,\bar{s}))$. The first step in achieving that is to restrict $n \geq N^2(p,P_f(ps,aq))$ $O\Big(4\frac{M^2e^{\frac{2M}{\eta}-\frac{2}{n}}(p,q)2ed^2\ln d}{\epsilon^2(p,q)}\Big)$. It implies that if $O\Big(e^{\frac{M}{\eta}}\epsilon_n(p,q)\sqrt{\frac{2ed^2\ln d}{n}}\Big) \leq \epsilon/2$ and for $n \geq \max_{s,a} N^2(p,P_f(ps,aq))$ from Equation (72) with probability at least $1-\delta$, for all $(ps,aq)\in S\times A$, we have

$$\max_{r,\bar{s}}\Big|\log\big(E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)-\log\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)\Big| \leq \epsilon/2. \tag{73}$$

It further implies that

$$\max_{P(r,\bar{s})}\Big(\log\big(E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)-\log\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)\Big)$$

$$\overset{(i)}{\leq} \log\big(E_{s^{(1)}\sim P_{f'_n}}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)$$

$$\overset{(ii)}{\leq} \log\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)+\epsilon/2$$

$$\overset{(iii)}{\leq} \max\Big\{r+\log\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)-r,\ \bar{r}+\log\big(E_{s^{(1)}\sim P_f}\big[re^{\frac{V_{ps}(1)}{\eta}}s\big]\big)-\bar{r}\Big\}+\epsilon/2$$

$$\overset{(iv)}{\geq} \max\{-\underline{\lambda}\log(\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\underline{\lambda}}]), -\bar{\lambda}\log(\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\bar{\lambda}}])\}. \tag{74}$$

where (i) follows from the fact that $\lambda^* \in [\underline{\lambda}, \bar{\lambda}]$, (ii) follows from Equation (73), (iii) follows from the definition of $\underline{\lambda}$ in Equation (70) and (iv) again follows from Equation (73).

Thus $\hat{\lambda}_n \in [\underline{\lambda}, \bar{\lambda}]$ follows from Equation (74) and concavity of $-\lambda\log(\mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]) - \lambda\rho$ w.r.t. λ. Note that λ^* also belongs in this set. We bound $\max_{\lambda\geq 0}\{-\lambda\log(\mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]) - \lambda\rho\} - \max_{\lambda\geq 0}\{-\lambda\log(\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\lambda}]) - \lambda\rho\}$ only between $\lambda \in [\underline{\lambda}, \bar{\lambda}]$ instead of all $\lambda > 0$. As a result, it holds that

$$\max_{\lambda\in[\underline{\lambda},\bar{\lambda}]}\{-\lambda\log(\mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]) - \lambda\rho\} - \max_{\lambda\in[\underline{\lambda},\bar{\lambda}]}\{-\lambda\log(\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\lambda}]) - \lambda\rho\} \tag{75}$$

$$\begin{aligned}
&\leq \max_{\lambda\in[\underline{\lambda},\bar{\lambda}]}\Big(\{-\lambda\log(\mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]) - \lambda\rho\} - \{-\lambda\log(\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\lambda}]) - \lambda\rho\}\Big) \\
&= \max_{\lambda\in[\underline{\lambda},\bar{\lambda}]} \lambda\Big|\log\Big(1 + \frac{\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\lambda}] - \mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]}{\mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]}\Big)\Big| \\
&\leq \max_{\lambda\in[\underline{\lambda},\bar{\lambda}]} 2\lambda e^{M/\lambda}\big|\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\lambda}] - \mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]\big| \\
&\leq 2\frac{M}{\rho}e^{\frac{M}{\underline{\lambda}}} \max_{\lambda\in[\underline{\lambda},\bar{\lambda}]}\big|\mathbb{E}_{s'\sim P_{\hat{f}_n}}[e^{-V(s')/\lambda}] - \mathbb{E}_{s'\sim P_f}[e^{-V(s')/\lambda}]\big|,
\end{aligned}$$

where the first inequality follows from Equation (70) and second inequality follows from the bounds of λ. Taking a maximum over all (s, a) gets the desired result.

□

Lemma 10. (Bound by difference between estimated model $\hat{f}_n$ and true f) For any value function $V(s'): \mathcal{S} \to [0, 1/(1-\gamma)]$ and any $\lambda > 0$, it holds that

$$|\mathbb{E}_{s'\sim P_{\hat{f}_n}(s,a)}[e^{-V(s')/\lambda}] - \mathbb{E}_{s'\sim P_f(s,a)}[e^{-V(s')/\lambda}]| \leq \sigma^{-1}\|f(s,a) - \hat{f}_n(s,a)\|,$$

where $P_{\hat{f}_n}(s,a) = \mathcal{N}(\hat{f}_n(s,a), \sigma^2 I)$ and $P_f(s,a) = \mathcal{N}(f(s,a), \sigma^2 I)$.

Proof.

$$\begin{aligned}
\mathbb{E}_{s'\sim P_{\hat{f}_n}(s,a)}[e^{-V(s')/\lambda}] - \mathbb{E}_{s'\sim P_f(s,a)}[e^{-V(s')/\lambda}] &= \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi\sigma^2)^d}} e^{-V(s')/\lambda}\Big(e^{-\frac{\|x - f(s,a)\|^2}{2\sigma^2}} - e^{-\frac{\|x - \hat{f}_n(s,a)\|^2}{2\sigma^2}}\Big) \\
&\leq \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi\sigma^2)^d}} e^{-V(s')/\lambda}\Big|e^{-\frac{\|x - f(s,a)\|^2}{2\sigma^2}} - e^{-\frac{\|x - \hat{f}_n(s,a)\|^2}{2\sigma^2}}\Big| \\
&\leq \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi\sigma^2)^d}} \Big|e^{-\frac{\|x - f(s,a)\|^2}{2\sigma^2}} - e^{-\frac{\|x - \hat{f}_n(s,a)\|^2}{2\sigma^2}}\Big| \\
&\overset{(i)}{\leq} 2\,\mathrm{TV}(P_{\hat{f}_n}(s,a), P_f(s,a)) \\
&\overset{(ii)}{\leq} 2\sqrt{\mathrm{KL}(P_{\hat{f}_n}(s,a), P_f(s,a))/2} \\
&\overset{(iii)}{\leq} 2\sqrt{\|f(s,a) - \hat{f}_n(s,a)\|^2/4\sigma^2} \\
&\leq \|f(s,a) - \hat{f}_n(s,a)\|/\sigma;
\end{aligned}$$

where (i) follows from the definition of Total Variation (TV) distance between any two multivariate Gaussians, (ii) uses the Pinsker's inequality, (iii) uses the formula for KL-divergence between multivariate Gaussian distributions.

□

Lemma 11. (Proposition-2 in Hu and Hong (2013)) For any function $V(\cdot): S \to [0,1]$ and random variable $Y \sim P_f(s,a)$, we have

$$\lim_{\epsilon \to 0} \epsilon \log \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] = -\mathrm{ESInf}(Y),$$

where $\mathrm{ESInf}(Y) = \sup\{t \in \mathbb{R} : \Pr(Y \geq t) = 1\}$ (essential infimum).

Proof. Consider the case when $M > \mathrm{ESInf}(Y)$. Let $\delta_M = \Pr(V(s') > M) \geq \int_{s'} \mathbb{1}(V(s') > M) e^{-\frac{\|s'-f(s,a)\|^2}{2}}$. It holds that

$$\begin{aligned}
&\log \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] && (76)\\
&\quad \leq \log \mathbb{E}_{s' \sim P_f(s,a)}\left[\mathbb{1}(V(s') \leq M) e^{-\frac{V(s')}{\epsilon}} + \mathbb{1}(V(s') > M) e^{-\frac{V(s')}{\epsilon}}\right]\\
&\quad \leq \log \mathbb{E}_{s' \sim P_f(s,a)}\left[\mathbb{1}(V(s') \leq M) e^{-\frac{V(s')}{\epsilon}}\right] + \delta_M\\
&\quad \leq \log \mathbb{E}_{s' \sim P_f(s,a)}\left[\mathbb{1}(V(s') \leq M) e^{-\frac{M}{\epsilon}}\right] + \delta_M\\
&\quad \leq \log\left[e^{-\frac{M}{\epsilon}}\right] + \delta_M\\
&\quad \leq -\frac{M}{\epsilon} + \log(1+\delta_M) && (77)
\end{aligned}$$

Thus for any $M > \mathrm{ESInf}(Y)$, we have

$$\lim_{\epsilon \to 0} \epsilon \log \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] \leq -M.$$

Combining with the fact that $\lim_{\epsilon \to 0} \epsilon \log \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] \geq -\mathrm{ESInf}(Y)$, we get the desired result. □

Lemma 12. (cover construction) For $\mathcal{V}$ denoting the set of value functions from $S \to [0, 1/(1-\gamma)]$, τ as defined in Lemma 9 we have with probability at least $1-\delta$,

$$\max_{V \in \mathcal{V}} \max_{s,a} 2\epsilon e^{-\frac{M}{\epsilon}} \max_{\mathrm{Pr}_\tau, \tau_s} \left|\mathbb{E}_{s' \sim P_{\hat{f}_n}(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] - \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right]\right| \leq O\left(2p^{M}\epsilon e^{\frac{M}{k_l}} e^{-\frac{\tau}{k_l}} \frac{\sqrt{2ed^2 \log(nd)}}{\sqrt{n}}\right).$$

Proof. Let $N_\epsilon(\mathcal{V})$ be the cover of the set $\mathcal{V}$. By definition, there exists $V' \in N_\epsilon(\mathcal{V})$ such that $\|V' - V\| \leq \epsilon$ for every $V \in \mathcal{V}$.

$$\begin{aligned}
&\left|\mathbb{E}_{s' \sim P_{\hat{f}_n}(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] - \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right]\right|\\
&\leq \left|\int_{\mathbb{R}^d} \frac{1}{\sqrt{2\pi\sigma^2}^d} e^{-\frac{V(s')}{\epsilon}} \left(e^{-\frac{\|s'-\hat{f}_n(s,a)\|^2}{2}} - e^{-\frac{\|s'-f(s,a)\|^2}{2}}\right)\right|\\
&\leq \int_{\mathbb{R}^d} \frac{1}{\sqrt{2\pi\sigma^2}^d} e^{-\frac{V(s')}{\epsilon}} \left|e^{-\frac{\|s'-\hat{f}_n(s,a)\|^2}{2}} - e^{-\frac{\|s'-f(s,a)\|^2}{2}}\right|\\
&\leq \int_{\mathbb{R}^d} \frac{1}{\sqrt{2\pi\sigma^2}^d} e^{-\frac{V(s')-V'(s')}{\epsilon}} e^{-\frac{V'(s')}{\epsilon}} \left|e^{-\frac{\|s'-\hat{f}_n(s,a)\|^2}{2}} - e^{-\frac{\|s'-f(s,a)\|^2}{2}}\right|\\
&\leq e^{\frac{\epsilon}{k_l}} \int_{\mathbb{R}^d} \frac{1}{\sqrt{2\pi\sigma^2}^d} e^{-\frac{V'(s')}{\epsilon}} \left|e^{-\frac{\|s'-\hat{f}_n(s,a)\|^2}{2}} - e^{-\frac{\|s'-f(s,a)\|^2}{2}}\right|\\
&\leq \max_{V' \in N_\epsilon(\mathcal{V})} \max_{s,a} \max_{\mathrm{Pr}_{k_l}, \tau_s} e^{\frac{\epsilon}{k_l}} \int_{\mathbb{R}^d} \frac{1}{\sqrt{2\pi\sigma^2}^d} e^{-\frac{V'(s')}{\epsilon}} \left|e^{-\frac{\|s'-\hat{f}_n(s,a)\|^2}{2}} - e^{-\frac{\|s'-f(s,a)\|^2}{2}}\right| && (78)
\end{aligned}$$

Here (i) is obtained using the fact that $\|V' - V\| \leq \epsilon$ and k_l is the minimum value of τ as defined in Lemma 9. Using Equation (78), we bound uniformly over all $V \in \mathcal{V}$, we have

$$\max_{V \in \mathcal{V}} \max_{s,a} 2\epsilon e^{-\frac{M}{k_l}} \max_{\mathrm{Pr}_{k_l}, \tau_s} \left|\mathbb{E}_{s' \sim P_{\hat{f}_n}(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right] - \mathbb{E}_{s' \sim P_f(s,a)}\left[e^{-\frac{V(s')}{\epsilon}}\right]\right|$$

$$\begin{aligned}
&\leq \max_{V\in[0,\frac{1}{1-\gamma}]^{|\mathcal{S}|}} \max_{s,a} \max_{\Pr_{kl}(\cdot,\cdot)\leq\varepsilon_s} 2\varepsilon e^{\frac{M}{kl}} e^{\frac{1}{kl}} \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi)^2|\Sigma|}} e^{-\frac{(V-\mathbb{E}_{P_{sa}}[V])^2}{2}} \left| e^{\frac{(s-f(s,a))^2}{2}} - e^{\frac{(s-\hat{f}_n(s,a))^2}{2}} \right| \\
&\leq \max_{V\in[0,\frac{1}{1-\gamma}]^{|\mathcal{S}|}} \max_{s,a} \max_{\Pr_{kl}(\cdot,\cdot)\leq\varepsilon_s} 2\varepsilon e^{\frac{M}{kl}} e^{\frac{1}{kl}} \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi)^2|\Sigma|}} \left| e^{\frac{(s-f(s,a))^2}{2}} - e^{\frac{(s-\hat{f}_n(s,a))^2}{2}} \right| \qquad (79) \\
&\overset{(i)}{\leq} \max_{s,a} 4\varepsilon^{-1} e^{\frac{M}{kl}} e^{\frac{1}{kl}} \{f(s,a) - \hat{f}_n(s,a)\} \\
&\overset{(ii)}{=} O\left(2\varepsilon^{-1} M e^{\frac{M}{kl}} e^{\frac{1}{kl}} \frac{\sqrt{n(\delta,n)}\sqrt{2\sigma d^2 \log nd}}{n}\right)
\end{aligned}$$

Here (i) follows from Lemma 10 and by the fact that none of the remaining terms inside $\max$ depend on V^{-1} or s. And (ii) follows from $\varepsilon \leq \frac{M}{1-\gamma}$ and Equation (26).

□

C Other Uncertainty Sets

C.1 Chi-Square Uncertainty Set

The f-divergence (Ali and Silvey (1966); Csiszár (1967)) between probability measures P and P_0 defined over X for a convex function $f : \mathbb{R}^+ \to \mathbb{R} \cup \{+\infty\}$ satisfying $f(1) = 0$ and $f(t) < \infty$ for any $t < 0$ is defined as follows:

$$D_f(P\|P_0) := \int f\left(\frac{dP}{dP_0}\right) dP_0. \qquad (80)$$

Specifically Duchi and Namkoong (2021) considers the Cressie-Read family of f-divergences (Cressie and Read (1984), see Appendix C.1) which includes χ^2 divergence ($k = 2$), etc. This family of f-divergences can be parametrized by $k \in (1, \infty)$, with $f_k(t) := \frac{t^k - kt + k - 1}{k(k-1)}$. Using this, we state the reformulation result from Duchi and Namkoong (2021, Lemma-1).

Lemma 13. For $k \in (1, \infty)$, $k = \frac{k}{k-1}$, any $\rho > 0$ and $c_k(\rho) = 1 + (k-1)(\rho^k - 1)^{\frac{1}{k}}$ and $X \sim P_0$ where P_0 is any probability distribution over X with $H : X \to \mathbb{R}$, we have

$$\sup_{P : D_{f_k}(P\|P_0) \leq \rho} \mathbb{E}_P[H(X)] = \inf_{\eta \in \mathbb{R}} \{c_k(\rho)(\mathbb{E}_{P_0}[(H(X) - \eta)_+^k])^{\frac{1}{k}} + \eta\}. \qquad (81)$$

Theorem 3. (Sample Complexity under χ^2 uncertainty set) Consider a robust MDP (see Section 2) with nominal transition dynamics f and uncertainty set defined as in Equation (2) w.r.t. χ^2 divergence. For denoting the robust optimal policy w.r.t. nominal transition dynamics f and π_N denoting the robust optimal policy w.r.t. learned nominal transition dynamics $\hat{f}_N$ via Algorithm 1, and $\varepsilon \in (0, 1]$, $\delta \in (0, \frac{1}{1-\gamma}]$, it holds that $\max_s |V^R_{N,f}(s) - V^R_{\pi,f}(s)| \leq \varepsilon$ with probability at least $1 - \delta$ for any $N \geq N_{\chi^2}$, where

$$N_{\chi^2} = O\left(\frac{1}{(1-\gamma)^2} \frac{\sqrt{n(\delta,n)}\sigma^2 d^2 \log nd}{\varepsilon^2 (1-\gamma)^3}\right). \qquad (82)$$

Proof. Step (i): As detailed in the proof outline of Section 4, in order to bound $V^R_{\hat{\pi}_n,f}(s) - V^R_{\pi,f}(s)$, we begin by adding and subtracting $V^R_{\hat{\pi}_n,\hat{f}_n}(s)$ which is the robust value function w.r.t. the nominal transition dynamics $\hat{f}_n$ and its corresponding optimal policy $\hat{\pi}_n$. Then, we split the difference into two terms as follows:

$$V^R_{\hat{\pi}_n,f}(s) - V^R_{\pi,f}(s) = \underbrace{V^R_{\hat{\pi}_n,f}(s) - V^R_{\hat{\pi}_n,\hat{f}_n}(s)}_{(i)} + \underbrace{V^R_{\hat{\pi}_n,\hat{f}_n}(s) - V^R_{\pi,f}(s)}_{(ii)}. \qquad (83)$$

In order to not disturb the flow of the proof we bound (i) and (ii) separately Lemma 6 and Lemma 7 respectively. From Lemma 6, we obtain that

$$(i) \leq \max_s V^R_{\hat{\pi}_n,f}(s) - V^R_{\hat{\pi}_n,\hat{f}_n}(s)$$

$$\text{(i)} \le \frac{1}{1-\gamma}\max_{s}\Big[\inf_{\hat{P}\in B(P_f(s,a),\hat{\eta}_n(s,a))} \mathbb{E}_{s'\sim\hat{P}}\big[V^{R}_{\hat{\eta}_n,f}(s')\big] - \inf_{\hat{P}\in B(P_{\hat{f}_n}(s,a),\hat{\eta}_n(s,a))} \mathbb{E}_{s'\sim\hat{P}}\big[V^{R}_{\hat{\eta}_n,f}(s')\big]\Big]. \tag{84}$$

And from Lemma 7, we obtain that

$$\begin{aligned}\text{(ii)} &= \max_{s} V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) - V^{R}_{\hat{\eta}_n,f}(s)\\ &\le \frac{1}{1-\gamma}\max_{s}\Big[\inf_{\hat{P}\in B(P_{\hat{f}_n}(s,a),\hat{\eta}_n(s,a))} \mathbb{E}_{s'\sim\hat{P}}\big[V^{R}_{\hat{\eta}_n,f}(s')\big] - \inf_{\hat{P}\in B(P_f(s,a),\hat{\eta}_n(s,a))} \mathbb{E}_{s'\sim\hat{P}}\big[V^{R}_{\hat{\eta}_n,f}(s')\big]\Big]. \end{aligned}\tag{85}$$

Note that both these terms in Equations (84) and (85) are of the form mentioned in the Step (i) of Section 4.

Step (ii): Next, corresponding to Step (ii) of the proof outline in Section 4, we use Lemma 13 to bound Equations (84) and (85). Denote $M := \frac{1}{1-\gamma} \cdot \max_s V^R(s)$ and $c_2(p,q) := \sqrt{\frac{1}{1-2}}$ for convenience. Using Equation (84) and Lemma 14 (internally using Lemma 13), it holds that

$$\begin{aligned}\text{(i)} &\le \max_{s} V^{R}_{\hat{\eta}_n,f}(s) - V^{R}_{\hat{\eta}_n,\hat{f}_n}(s)\\ &\le \frac{1}{1-\gamma}\max_{s}\Big[\inf_{\hat{P}\in B(P_f(s,a),\hat{\eta}_n(s,a))} \mathbb{E}_{s'\sim\hat{P}}\big[V^{R}_{\hat{\eta}_n,f}(s')\big] - \inf_{\hat{P}\in B(P_{\hat{f}_n}(s,a),\hat{\eta}_n(s,a))} \mathbb{E}_{s'\sim\hat{P}}\big[V^{R}_{\hat{\eta}_n,f}(s')\big]\Big]\\ &\le \max_{s,a}\frac{\sqrt{\frac{1}{1-2}}}{1-\gamma}\sup_{\Pr(0)\in\left[\frac{c_2(p,q)M}{c_2(p,q)-1},\,1\right]}\Big|\mathbb{E}_{P_f(s,a)}\big[V^{R}_{\hat{\eta}_n,f}(s')\big]\Pr(0) - \mathbb{E}_{P_{\hat{f}_n}(s,a)}\big[V^{R}_{\hat{\eta}_n,f}(s')\big]\Pr(0)\Big| \qquad (86)\\ &\le \max_{V(0)\in\mathcal{V}}\max_{s,a}\frac{\sqrt{\frac{1}{1-2}}}{1-\gamma}\sup_{\Pr(0)\in\left[\frac{c_2(p,q)M}{c_2(p,q)-1},\,1\right]}\Big|\mathbb{E}_{P_f(s,a)}\big[V(s')\big]\Pr(0) - \mathbb{E}_{P_{\hat{f}_n}(s,a)}\big[V(s')\big]\Pr(0)\Big| \qquad (87)\end{aligned}$$

We can bound (ii) similarly.

$$\begin{aligned}\text{(ii)} &= \max_{s} V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) - V^{R}_{\hat{\eta}_n,f}(s) \qquad (88)\\ &\le \max_{V(0)\in\mathcal{V}}\max_{s,a}\frac{\sqrt{\frac{1}{1-2}}}{1-\gamma}\sup_{\Pr(0)\in\left[\frac{c_2(p,q)M}{c_2(p,q)-1},\,1\right]}\Big|\mathbb{E}_{P_f(s,a)}\big[V(s')\big]\Pr(0) - \mathbb{E}_{P_{\hat{f}_n}(s,a)}\big[V(s')\big]\Pr(0)\Big| \qquad (89)\end{aligned}$$

Step (iii): Next, we want to utilize the learning error bound (Equation (26)) that bounds the difference between the means of true nominal transition dynamics P_f and learned nominal transition dynamics $P_{\hat{f}_n}$ to bound Equations (87) and (89).

We begin by bounding the difference $\big|\mathbb{E}_{P_f(s,a)}[V(s')]\Pr(0) - \mathbb{E}_{P_{\hat{f}_n}(s,a)}[V(s')]\Pr(0)\big|$, by the difference in means of P_f and $P_{\hat{f}_n}$ in Lemma 17. Since Equation (87) has a max over all value functions, we introduce a covering number argument in Lemma 15 to reform it to a max over the functions in the covering set. We then use Lemma 17 to obtain bounds in terms of maximum information gain γ_{Nd} (Equation (9)) and . Further details regarding the covering number argument are deferred to Lemma 15. Then, we apply the result of Lemma 15 with 1 (defined in Lemma 15) on Equation (87). Then, it holds that

$$\text{(i)} \le \max_{s} V^{R}_{\hat{\eta}_n,f}(s) - V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) \le O\left(\frac{c_2(p,q)\sqrt{q}M^2}{c_2(p,q)-1}\right)\left(\frac{\sqrt{\beta_n(p,q)}\sqrt{2\sigma^2\gamma_{Nd}}}{n}\right)^{\frac{1}{2}}. \tag{90}$$

Note that β_n, which appears in Lemma 3, has a logarithmic dependence on n. Similarly, from Equation (89), and Lemmas 15 and 17, we obtain

$$\text{(ii)} \le \max_{s} V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) - V^{R}_{\hat{\eta}_n,f}(s) \le O\left(\frac{c_2(p,q)\sqrt{q}M^2}{c_2(p,q)-1}\right)\left(\frac{\sqrt{\beta_n(p,q)}\sqrt{2\sigma^2\gamma_{Nd}}}{n}\right)^{\frac{1}{2}}. \tag{91}$$

Note that we want to bound $V^{R}_{\hat{\eta}_n,f}(s) - V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) \le \text{(i)} + \text{(ii)}$ over all $s \in S$. Using $\max_s V^{R}_{\hat{\eta}_n,f}(s) - V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) \le \max_s V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) - V^{R}_{\hat{\eta}_n,f}(s) + \max_s V^{R}_{\hat{\eta}_n,\hat{f}_n}(s) - V^{R}_{\hat{\eta}_n,f}(s)$ and substituting M by $1/(1-\gamma)$, we obtain from

Equation (90) and Equation (91)

$$\max_s V^R_{\hat{\wedge}_n;f}(s) - V^R_{;f}(s) \quad O\left(\frac{c_2(p,q)\sqrt{q^2M^2}}{c_2(p,q)-1}\right) \quad \left(\frac{\sqrt{n}(p,q)\sqrt{2\epsilon d^2 - nd}}{\bar{n}}\right)^{\frac{1}{2}} :$$

Finally, to ensure that $\max_s |V^R_{\hat{\wedge}_n;f}(s) - V^R_{;f}(s)| \leq$, it su ces to have

$$\max_s V^R_{\hat{\wedge}_n;f}(s) - V^R_{;f}(s) \quad O\left(\frac{c_2(p,q)\sqrt{q^2M^2}}{c_2(p,q)-1}\right) \quad \left(\frac{\sqrt{n}(p,q)\sqrt{2\epsilon d^2 - nd}}{\bar{n}}\right)^{\frac{1}{2}} :$$

Moving $\sqrt{\bar{n}}$ and to opposite sides and squaring both sides twice, we obtain

$$n \quad O\left(\frac{1}{1-2}\right)^4 \frac{^4(p,q)^2d^2 - nd}{^2(1-)^3} :$$

□

Lemma 14. (Simpli cation using Lemma 13 reformulation) For any value function V from $S \to [0, 1/(1-)]$, it holds that

$$\max_s \left| \inf_{\in(p||P_{\hat{f}_n}(s,a),\hat{}_n(s,a))} E_{s'\sim p}[V(s')] - \inf_{\in(p||P_f(s,a),\hat{}_n(s,a))} E_{s'\sim p}[V(s')] \right| \leq$$

$$\max_{s,a} c_2(p,q) \sup_{Pr(0;\frac{c_2(p,q)M}{c_2(p,q)-1}s)} t\left| E_{P_f(s,a)}[(p - V)(s')] - \sqrt{q^2 - s} - E_{P_{\hat{f}_n}(s,a)}[(p - V)(s')] - \sqrt{q^2 - s}\right|^{\frac{1}{2}} u, \quad (92)$$

where $c_2(p,q) \sqrt{1-2}$ and $M \quad 1/(1-)$.

Proof. First note that,

$$\max_s \left| \inf_{\in(p||P_{\hat{f}_n}(s,a),\hat{}_n(s,a))} E_{s'\sim p}[V(s')] - \inf_{\in(p||P_f(s,a),\hat{}_n(s,a))} E_{s'\sim p}[V(s')] \right| \leq$$

$$\max_{s,a} \left| \inf_{\in(p||P_{\hat{f}_n}(s,a),a)} E_{s'\sim p}[V(s')] - \inf_{\in(p||P_f(s,a),a)} E_{s'\sim p}[V(s')] \right| : \quad (93)$$

Using Lemma 13 and focusing to bound right side of Equation (93) for one particular(s,a) state-action pair, we obtain

$$\inf_{\in(p||P_{\hat{f}_n}(s,a),a)} E_{s'\sim p}[V(s')] - \inf_{\in(p||P_f(s,a),a)} E_{s'\sim p}[V(s')]$$

$$\sup_{P\in R} \left| c_2(p,q)\left(E_{P_f(s,a)}[(p - V)(s')] - \sqrt{q^2 - s}\right)^{\frac{1}{2}} u \right| - \sup_{P\in R} \left| c_2(p,q)\left(E_{P_{\hat{f}_n}(s,a)}[(p - V)(s')] - \sqrt{q^2 - s}\right)^{\frac{1}{2}} u \right|$$

$$\overset{(i)}{\leq} \sup_{P\in R} \left| c_2(p,q)\left(E_{P_f(s,a)}[(p - V)(s')] - \sqrt{q^2 - s}\right)^{\frac{1}{2}} u \right| - \sup_{P\in R} \left| c_2(p,q)\left(E_{P_{\hat{f}_n}(s,a)}[(p - V)(s')] - \sqrt{q^2 - s}\right)^{\frac{1}{2}} u \right| ; \quad (94)$$

where (i) is obtained by replacing with .

Let $g_{\in}(p; P_f(s,a)) \quad c_2(p,q)\left(E_{P_f(s,a)}[(p - V)(s')] - \sqrt{q^2 - s}\right)^{\frac{1}{2}}$. Note that $g_{\in}(p; P_f(s,a))$satis es the following: For ≥ 0 (implying $p - V(s') - q \geq 0$ and $p - V(s') - q \quad 0$),

$$g_{\in}(p; P_f(s,a)) \quad \geq 0: \quad (95)$$

And for $\frac{c_2(p,q)M}{c_2(p,q)-1} > 0$,

$$g\left(p\frac{c_2(p,q)M}{c_2(p,q)-1}; P_f(s,a)\right) \quad c_2(p,q)\left(E_{P_f(s,a)}[(p - V)(s')] - \frac{c_2(p,q)M}{c_2(p,q)-1}\sqrt{q^2 - s}\right)^{\frac{1}{2}} \quad \frac{c_2(p,q)M}{c_2(p,q)-1}$$

$$\overset{(i)}{\geq} \frac{c_2(p,q)M}{c_2(p,q)-1} \quad c_2(p,q)\left(E_{P_f(s,a)}[(p - V)(s')] \quad M\right)^{\frac{1}{2}} \quad \frac{c_2(p,q)M}{c_2(p,q)-1}\sqrt{q^2 - s}$$

$$\leq \frac{c_2(p,q)M}{c_2(p,q)-1} \quad c_2(p,q)\left|E_{P_f}(s,a)(p) - \frac{M}{c_2(p,q)-1}(q^2(s,a))^{\frac{1}{2}}\right|$$
$$\leq \frac{c_2(p,q)M}{c_2(p,q)-1} \quad \frac{c_2(p,q)M}{c_2(p,q)-1}$$
$$0, \tag{96}$$

where (i) follows from the fact that the random variable $V(s')$ is bounded by $M - 1/(1-)$. A similar result can be shown for $g(p) = P_{f_n}(s,a)(q)$ (or for any P). Along with the convexity of $\tilde{N}(g(p), P)$ (Duchi and Namkoong (2021)), and $\inf_{p \in P(\cdot)} E_{s' \sim p} V(s') \geq 0$, Equation (95) and Equation (96) imply that the sup is attained between $[0, \frac{c_2(p,q)M}{c_2(p,q)-1}]$ for both $\sup_{P \in R} g(p), P_f(s,a)(q)$ and $\sup_{P \in R} g(p), P_{f_n}(s,a)(q)$ Using this in Equation (94) we have,

$$\sup_{P \in R} t(g(p), P_f(s,a)(q)) - \sup_{P \in R} t(g(p), P_{f_n}(s,a)(q)) \tag{97}$$

$$\sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} t(g(p), P_f(s,a)(q)) - \sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} t(g(p), P_{f_n}(s,a)(q)) \tag{98}$$

$$\leq \sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} |t(g(p), P_f(s,a)(q)) - t(g(p), P_{f_n}(s,a)(q))| \tag{99}$$

$$\leq \sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} |c_2(p,q)\left|E_{P_f}(s,a)(p) - V(s')\right| - (q^2(s,a))^{\frac{1}{2}}| - |c_2(p,q)\left|E_{P_{f_n}}(s,a)(p) - V(s')\right| - (q^2(s,a))^{\frac{1}{2}}|| \tag{100}$$

$$\leq c_2(p,q) \sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} |\left|E_{P_f}(s,a)(p) - V(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V(s')\right| - (q^2(s,a))|^{\frac{1}{2}}. \tag{101}$$

The last step is obtained using the basic inequality $|\sqrt{a} - \sqrt{b}| \leq \sqrt{|a-b|}$.

□

Lemma 15. (cover construction) For V denoting the set of value functions from $S \tilde{N} [0, 1/(1-)]$ it holds with probability at least 1 ,

$$\max_{V \in V} \max_{s,a} \sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} |\left|E_{P_f}(s,a)(p) - V(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V(s')\right| - (q^2(s,a))|^{\frac{1}{2}}| \leq$$
$$O\left(\frac{c_2(p,q)M}{c_2(p,q)-1} \sqrt{\frac{n(p,q)}{2ed^2}}^{nd}\right)^{\frac{1}{2}}; \tag{102}$$

where $c_2(p,q) = \sqrt{1-2}$, $M - 1/(1-)$.

Proof. Let $N_V(p,q)$ be the cover of the set V. By definition, there exists $V^1 \in N_V(p,q)$ such that $\|V^1 - V\| \leq$ for every $V \in V$.

$$\begin{aligned}
&\left|E_{P_f}(s,a)(p) - V(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V(s')\right| - (q^2(s,a))| \\
&\leq |\left|E_{P_f}(s,a)(p) - V(s')\right| - (q^2(s,a)) - \left|E_{P_f}(s,a)(p) - V^1(s')\right| - (q^2(s,a))| \\
&\quad + |\left|E_{P_f}(s,a)(p) - V^1(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V^1(s')\right| - (q^2(s,a))| \\
&\quad + |\left|E_{P_{f_n}}(s,a)(p) - V^1(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V(s')\right| - (q^2(s,a))|.
\end{aligned} \tag{103}$$

$$\overset{(i)}{\leq} 4\|V^1 - V\|^2 \quad 4\|V^1 - V\| + |\left|E_{P_f}(s,a)(p) - V^1(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V^1(s')\right| - (q^2(s,a))|, \tag{104}$$

where (i) follows from Lemma 16. Using Equation (104) we bound uniformly over all $V \in V$,

$$\max_{V \in V} \max_{s,a} \sup_{P \in [0, \frac{c_2(p,q)M}{c_2(p,q)-1}]} |\left|E_{P_f}(s,a)(p) - V(s')\right| - (q^2(s,a)) - \left|E_{P_{f_n}}(s,a)(p) - V(s')\right| - (q^2(s,a))|^{\frac{1}{2}} \tag{105}$$

$$\leq \max_{V^1 \in \mathcal{N}_V(p,q,s,a)} \sup_{\Pr(0,\frac{c_2(p,q)M}{c_2(p,q)-1}s)} \left[4\|V^1 - V\|_2^2 + 4\|V^1 - V\| \cdot \left| E_{P_f(s,a)}[(V^1(s^1) - q)^2] - E_{P_{\hat{f}_n}(s,a)}[(V^1(s^1) - q)^2] \right|^{\frac{1}{2}} + \left| E_{P_{\hat{f}_n}(s,a)}[(V^1(s^1) - q)^2] - E_{P_{\hat{f}_n}(s,a)}[(V^1(s^1) - q)^2] \right|^{\frac{1}{2}} \right]$$

$$\leq \max_{V^1 \in \mathcal{N}_V(p,q,s,a)} \sup_{\Pr(0,\frac{c_2(p,q)M}{c_2(p,q)-1}s)} \left[\frac{c_2(p,q)M}{c_2(p,q)-1} \|f(s,a) - \hat{f}_n(s,a)\| \right] + \frac{2}{4 - 4\frac{c_2(p,q)M}{c_2(p,q)-1}} \tag{iii}$$

$$\leq O\left(\frac{c_2(p,q)M}{c_2(p,q)-1} \sqrt{\frac{n(p,q)}{2ed^2 n_d}}^{\frac{1}{2}}\right) + \frac{2}{4 - 4\frac{c_2(p,q)M}{c_2(p,q)-1}} \tag{iv}$$

$$\leq O\left(\frac{c_2(p,q)M}{c_2(p,q)-1} \sqrt{\frac{n(p,q)}{2ed^2 n_d}}^{\frac{1}{2}}\right); \tag{v}$$

where (ii) follows from $\|V^1 - V\| \leq$ and $\leq \frac{c_2(p,q)M}{c_2(p,q)-1}$, (iii) follows from Lemma 17, (iv) follows from Equation (26), and (v) follows from substituing 1 (or any constant).

□

Lemma 16. For any two value functions V, V^1 from $S \to [0, 1/(1-\gamma)]$, it holds that

$$E_{P_f(s,a)}[(V^1(s^1) - q)^2] - E_{P_f(s,a)}[(V(s^1) - q)^2] \leq 2\|V^1 - V\|_2^2 + 2\|V^1 - V\|. \tag{108}$$

Proof. Let $p_{P_f(s,a)}(\cdot)$ denote the probability density function of $P_f(s,a)$. Then,

$$E_{P_f(s,a)}[(V^1(s^1) - q)^2] - E_{P_f(s,a)}[(V(s^1) - q)^2]$$

$$= \int_{s^1 \in P_f(s,a)} (V^1(s^1) - q)^2 p_{P_f(s,a)}(s^1) ds^1 - \int_{s^1 \in P_f(s,a)} (V(s^1) - q)^2 p_{P_f(s,a)}(s^1) ds^1$$

$$= \int_{s^1 \in P_f(s,a)} \underbrace{(V^1(s^1) - q + V(s^1) - q)(V^1(s^1) - V(s^1))}_{\text{(i)}} p_{P_f(s,a)}(s^1) ds^1$$

$$= \int_{s^1 \in P_f(s,a)} \underbrace{(V(s^1) - q + V^1(s^1) - q + V^1(s^1) - V(s^1))(V^1(s^1) - V(s^1))}_{\text{(ii)}} p_{P_f(s,a)}(s^1) ds^1. \tag{109}$$

where the last inequality is obtained by adding and subtracting $(V(s^1) - q)^2$.

We begin by bounding (ii). We have,

$$\text{(ii)} = \int_{s^1 \in P_f(s,a)} (V(s^1) - q + V^1(s^1) - q)(V^1(s^1) - V(s^1)) p_{P_f(s,a)}(s^1) ds^1$$

$$= \int_{s^1 \in P_f(s,a)} (V(s^1) - q)(V^1(s^1) - V(s^1)) + (V^1(s^1) - V(s^1))^2 p_{P_f(s,a)}(s^1) ds^1$$

$$\leq \int_{s^1 \in P_f(s,a)} (V(s^1) - q)(V^1(s^1) - V(s^1)) + (V^1(s^1) - V(s^1))(V^1(s^1) - V(s^1)) + (V^1(s^1) - V(s^1))^2 p_{P_f(s,a)}(s^1) ds^1$$

$$= \int_{s^1 \in P_f(s,a)} (V(s^1) - q)(V^1(s^1) - V(s^1)) + 2(V^1(s^1) - V(s^1))^2 p_{P_f(s,a)}(s^1) ds^1$$

»
¤ 1pV ps1q, V 1ps1q qp V 1ps1q V ps1qqp V 1ps1q V ps1q 2 qpPf ps;aqps1qds1
pii aq
» (110)
1pV ps1q ¤ V 1ps1qqp V 1ps1q V ps1qqp V 1ps1q V ps1q 2 qpPf ps;aqps1qds1:
pii bq

Bounding pii aq rst, we have,

»
pii aq 1pV ps1q, V 1ps1q qp V 1ps1q V ps1qqp V 1ps1q V ps1q 2 qpPf ps;aqps1qds1
paq »
¤ 1pV ps1q, V 1ps1q q V 1ps1q V ps1q p V 1ps1q V ps1q 2 qpPf ps;aqps1qds1
pbq »
¤ 1pV ps1q, V 1ps1q q V 1ps1q V ps1q 2 pPf ps;aqps1qds1
s1 Pf ps;aq
¤ 2 }V 1 V}; (111)

where (a) and (b) follows from p V 1ps1q V ps1q 2 q ¡ 0 as V ps1q, V 1ps1q . And pii bq can be bounded as,

»
pii bq 1pV ps1q ¤ V 1ps1qqp V 1ps1q V ps1qqp V 1ps1q V ps1q 2 qpPf ps;aqps1qds1
»
¤ 1pV ps1q ¤ V 1ps1qq V 1ps1q V ps1q V 1ps1q V ps1q 2 pPf ps;aqps1qds1
pcq »
¤ 1pV ps1q ¤ V 1ps1qq V 1ps1q V ps1q V ps1q V 1ps1q pPf ps;aqps1qds1
»
¤ 1pV ps1q ¤ V 1ps1qq V 1ps1q V ps1q 2 pPf ps;aqps1qds1
s1 Pf ps;aq
¤ } V 1 V}2; (112)

where (c) follows from ¤ V 1ps1q. Bounding (i) similarly,

»
i 1pV 1ps1q q 1pV ps1q q p V 1ps1q q2pPf ps;aqps1qds1
s1 Pf ps;aq
»
¤ 1pV 1ps1q ¤ V ps1qq p V 1ps1q q2pPf ps;aqps1qds1
s1 Pf ps;aq
»
¤ 1pV 1ps1q ¤ V ps1qq p V 1ps1q V ps1qq2pPf ps;aqps1qds1
s1 Pf ps;aq
¤ } V 1 V}2: (113)

Using Equations (109) to (113) we get the desired result. □

Lemma 17. (Bound by di erence between estimated model f̂n and true f) For any value function V ps1q : S Ñ r0; 1{p1 qs and any ¡ 0, it holds that

|EPf ps;aqrp V ps1q q2 s EPf̂n ps;aqrp V ps1q q2 s| ¤ 2 1 c2p qM / c2p q 1 2 }f ps; aq f̂n ps; aq};

where Pf̂n ps; aq N pf̂n ps; aq, 2I q and Pf ps; aq N pf ps; aq, 2I q, P r0; c2p qM / c2p q 1 s, c2p q ? 1 2 and M 1{p1 q.

Proof.

EPf ps;aqrp V ps1q q2 s EPf̂n ps;aqrp V ps1q q2 s

$$
\begin{aligned}
&\leq \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi)^d \det(\Sigma_1)}} \left| V(s_1) \right| \left| e^{-\frac{\|x - f(s,a)\|_2^2}{2\sigma^2}} - e^{-\frac{\|x - \hat{f}_n(s,a)\|_2^2}{2\sigma^2}} \right| dx \\
&\leq \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi)^d \det(\Sigma_1)}} \left| V(s_1) \right| \left| e^{-\frac{\|x - f(s,a)\|_2^2}{2\sigma^2}} - e^{-\frac{\|x - \hat{f}_n(s,a)\|_2^2}{2\sigma^2}} \right| dx \\
&\leq \left(\frac{c_2(p, q)M}{c_2(p, q) - 1} \right)^2 \int_{\mathbb{R}^d} \frac{1}{\sqrt{(2\pi)^d \det(\Sigma_1)}} \left| e^{-\frac{\|x - f(s,a)\|_2^2}{2\sigma^2}} - e^{-\frac{\|x - \hat{f}_n(s,a)\|_2^2}{2\sigma^2}} \right| dx \\
&\overset{(ii)}{\leq} 2 \left(\frac{c_2(p, q)M}{c_2(p, q) - 1} \right)^2 \mathrm{TV}\left(P_{\hat{f}_n}(s,a), P_f(s,a)\right) \\
&\overset{(iii)}{\leq} 2 \left(\frac{c_2(p, q)M}{c_2(p, q) - 1} \right)^2 \sqrt{\frac{1}{2} \mathrm{KL}\left(P_{\hat{f}_n}(s,a), P_f(s,a)\right)} \\
&\overset{(iv)}{\leq} 2 \left(\frac{c_2(p, q)M}{c_2(p, q) - 1} \right)^2 \sqrt{\frac{1}{2\sigma^2} \|f(s,a) - \hat{f}_n(s,a)\|_2^2} \\
&\leq \left(\frac{c_2(p, q)M}{c_2(p, q) - 1} \right)^2 \|f(s,a) - \hat{f}_n(s,a)\|_2 \, ;
\end{aligned}
$$

where (i) follows from $|V(s_1)| \leq \frac{c_2(p,q)M}{c_2(p,q)-1}$ as $\|x\|_2 \leq \frac{c_2(p,q)M}{c_2(p,q)-1}$, (ii) follows from the definition of Total Variation (TV) distance between any two multivariate Gaussians, (iii) uses the Pinsker's inequality, and (iv) uses the formula for KL-divergence between multivariate Gaussian distributions.

□

C.2 Total Variation Distance

Similar to lemma 13, we want a similar convex reformulation for the variation distance. We derive such a reformulation starting from the dual reformulation from Shapiro (2017) and Ben-Tal et al. (2013) stated as Proposition-1 in Duchi and Namkoong (2021).

Lemma 18. For $X \sim P_0$ where P_0 is any probability distribution over X with $H : X \to \mathbb{R}$, $\rho \geq 0$ and, $D_f(P||P_0)$ defined as in Equation (80), it holds that

$$
\sup_{P : D_f(P||P_0) \leq \rho} \mathbb{E}_P[H(X)] = \inf_{\lambda \geq 0,\ \lambda \in \mathbb{R}} \left(\mathbb{E}_{P_0}\left[f^* \left(\frac{H(X)}{\lambda} \right) \right] \lambda + \lambda \rho \right). \tag{114}
$$

Note that the total variation distance between two probability distributions P and P_0 is attained by substituting $f_{TV}(t) = |t - 1|$ in $D_f(P||P_0) = \int f\left(\frac{dP}{dP_0}\right) dP_0$. The corresponding Fenchel conjugate $f^*_{TV}(s)$ for $f_{TV}(t) = |t - 1|$ would be

$$
f^*_{TV}(s) = \begin{cases} -1, & s \leq -1 \\ s, & s \in [-1, 1] \\ \infty, & s \geq 1 \end{cases} \tag{115}
$$

As we require $\inf_{P : \mathrm{TV}(P||P_0) \leq \rho} \mathbb{E}_P[H(X)]$, using Equation (114) and replacing λ with α, we have

$$
\inf_{P : \mathrm{TV}(P||P_0) \leq \rho} \mathbb{E}_P[H(X)] = \sup_{\alpha \geq 0,\ \alpha \in \mathbb{R}} \left(\mathbb{E}_{P_0}\left[f^*_{TV}\left(\frac{H(X)}{\alpha} \right) \right] \alpha - \alpha \rho \right). \tag{116}
$$

Using Equation (116), we derive a convex reformulation in Lemma 19

Lemma 19. (Reformulation for total variation distance based on Yang et al. (2022)) For $\rho \geq 0$ and $X \sim P_0$ where P_0 is any probability distribution over X with $H : X \to \mathbb{R}$, for $0 \leq H(x) \leq \frac{1}{1-\gamma}$ and $\mathrm{ESI}(Y) = \sup\{t \in \mathbb{R} : P(Y \leq t) = 0\}$ (essential infimum), it holds that

$$
\inf_{P : \mathrm{TV}(P||P_0) \leq \rho} \mathbb{E}_P[H(X)] = \sup_{\alpha \in [0, \frac{p_2 - q}{p_1 - q}]} \left(\mathbb{E}_{P_0}\left[H(X) - \alpha \right] + \frac{\mathrm{ESI}(H(x)) - \alpha}{2} \rho \right). \tag{117}
$$

where TV denotes the total variation distance.

Proof. Substituting Equation (115) in Equation (116) to obtain the reformulation for total variation distance, we have

$$\inf_{P:TV(P\|P_0)\le\epsilon} E_P[H(X)] \tag{118}$$

$$\sup_{\lambda\ge 0,\ \mathrm{PR},\ \frac{H(x)}{2}\le 1} \lambda\epsilon + E_{P_0}\left[\max\left(\frac{H(X)}{2}, 1\right) - u\right] \tag{119}$$

$$\sup_{\lambda\ge 0,\ \mathrm{PR},\ \frac{H(x)}{2}\le 1} \lambda\epsilon + E_{P_0}\left[\max\left(H(X), \right) - u\right] \tag{120}$$

$$\sup_{\lambda\ge 0,\ \mathrm{PR},\ \frac{H(x)}{2}\le 2} \lambda\epsilon + E_{P_0}\left[\max\left(H(X), \right) - u\right] \tag{121}$$

$$\sup_{\lambda\ge 0,\ \mathrm{PR},\ \frac{H(x)}{2}\le 2} \lambda\epsilon + E_{P_0}\left[\max\left(H(X), 0\right) - u\right] \tag{122}$$

$$\sup_{\lambda\ge 0,\ \mathrm{PR},\ \frac{H(x)}{2}\le 2} \lambda\epsilon + E_{P_0}\left[H(X) - u\right]. \tag{123}$$

Here Equation (121) is obtained by substituting with . In order to optimize over , we need to choose the minimum satisfying the constraints. We require $\lambda \ge \frac{H(x)}{2}$ which translates to $\lambda \ge \frac{ESI(H(x))}{2}$ (as this constraint originates inside the expectation, points with zero mass, $t \in PR : P(Y) = u\}$, will have no effect). Substituting this, we have

$$\inf_{P:TV(P\|P_0)\le\epsilon} E_P[H(X)] \le \sup_{\mathrm{PR}} \left\{ E_{P_0}\left[H(X) - \frac{ESI(H(x))}{2}\right] - u \right\}. \tag{124}$$

Denote the inner function in Equation (124), as

$$g_{TV}(P, P_0) = E_{P_0}\left[H(X) - \frac{ESI(H(x))}{2}\right]. \tag{125}$$

Note that for $\lambda = 0$, the first two terms in $g_{TV}(P, P_0)$ will be 0 if $H(x) \ge 0$ for all x. This implies

$$g_{TV}(P, P_0) \ge 0 \quad @ \quad \lambda = 0. \tag{126}$$

Also, as $H(x) \le \frac{1}{1}$, we substitute $\frac{2}{p_1 \quad q}$ in $g_{TV}(P, P_0)$, and bound it as follows:

$$g_{TV}\left(\frac{p_2 \quad q}{p_1 \quad q}, P_0\right) = E_{P_0}\left[H(X) - \frac{p_2 \quad q}{p_1 \quad q}\right] - \frac{ESI(H(x))}{2}\left(\frac{p_2 \quad q}{p_1 \quad q}\right) \tag{127}$$

$$= E_{P_0}\left[H(X) - \frac{p_2 \quad q}{p_1 \quad q}\right] - \frac{ESI(H(x))}{2}\left(\frac{p_2 \quad q}{p_1 \quad q}\right) \tag{128}$$

$$= E_{P_0}\left[H(X) - \frac{ESI(H(x))}{2}\left(\frac{p_2 \quad q}{p_1 \quad q}\right)\right] \tag{129}$$

$$= E_{P_0}\left[H(X) - \frac{ESI(H(x))}{2}\left(\frac{p_2 \quad q}{p_1 \quad q}\right)\right] \tag{130}$$

$$\le E_{P_0}\left[H(X) - \frac{1}{1} - \frac{ESI(H(x))}{2}\frac{}{2p_1 \quad q}\right] \tag{131}$$

$$\le E_{P_0}\left[H(X) - \frac{1}{1} - \frac{1}{2}\left(ESI(H(x)) - \frac{1}{p_1 \quad q}\right)\right] \tag{132}$$

$$\le 0. \tag{133}$$

Here Equation (128), Equation (130) and Equation (133) are obtained from the fact that that $H(x) \le \frac{1}{1}$ ($H(x) - \frac{p_2 \quad q}{p_1 \quad q} \ge 0$) and $ESI(H(x)) \le \frac{1}{1}$ ($ESI(H(x)) - \frac{p_2 \quad q}{p_1 \quad q} \ge 0$). Along with the convexity of $g_{TV}(P, P_0)$, Equation (126) and Equation (133) imply that the $\sup_{\mathrm{PR}}\{g_{TV}(P, P_0)\}$ is attained in the range $[0; \frac{p_2 \quad q}{p_1 \quad q}]$. □

Theorem 4. (Sample Complexity under TV uncertainty set) Consider a robust MDP (see Section 2) with nominal transition dynamics f and uncertainty set defined as in Equation (2) w.r.t. TV distance. For π denoting the robust optimal policy w.r.t. nominal transition dynamics f and $\hat{\pi}_N$ denoting the robust optimal policy w.r.t. learned nominal transition dynamics $\hat{f}_N$ via Algorithm 1, and $\epsilon \in (0, 1)$, $\delta \in (0, \frac{1}{1-\gamma})$, it holds that $\max_s |V^R_{\hat{\pi}_N, f}(s) - V^R_{\pi, f}(s)| \leq \epsilon$ with probability at least $1 - \delta$ for any $N \geq N_{TV}$, where

$$N_{TV} = O\left(\frac{|S|^2 |A|^2}{\epsilon^2 (1-\gamma)^4} \ln\frac{|S|^2 |A|}{\delta^2}\right). \tag{134}$$

Proof. Step (i): As detailed in the proof outline of Section 4, in order to bound $V^R_{\hat{\pi}_n, f}(s) - V^R_{\pi, f}(s)$, we begin by adding and subtracting $V^R_{\hat{\pi}_n, \hat{f}_n}(s)$ which is the robust value function w.r.t. the nominal transition dynamics $\hat{f}_n$ and its corresponding optimal policy $\hat{\pi}_n$. Then, we split the difference into two terms as follows:

$$V^R_{\hat{\pi}_n, f}(s) - V^R_{\pi, f}(s) = \underbrace{V^R_{\hat{\pi}_n, f}(s) - V^R_{\hat{\pi}_n, \hat{f}_n}(s)}_{\text{(i)}} + \underbrace{V^R_{\hat{\pi}_n, \hat{f}_n}(s) - V^R_{\pi, f}(s)}_{\text{(ii)}}. \tag{135}$$

In order to not disturb the flow of the proof we bound (i) and (ii) separately Lemma 6 and Lemma 7 respectively. From Lemma 6, we obtain that

$$\begin{aligned}
\text{(i)} &\leq \max_s \left| V^R_{\hat{\pi}_n, f}(s) - V^R_{\hat{\pi}_n, \hat{f}_n}(s) \right| \\
&\leq \frac{\gamma}{1-\gamma} \max_s \left(\inf_{TV(p \| P_f(s, \hat{\pi}_n(s))) \leq \epsilon} \mathbb{E}_{s' \sim p} \left[V^R_{\hat{\pi}_n, f}(s') \right] - \inf_{TV(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \leq \epsilon} \mathbb{E}_{s' \sim p} \left[V^R_{\hat{\pi}_n, f}(s') \right] \right).
\end{aligned} \tag{136}$$

And from Lemma 7, we obtain that

$$\begin{aligned}
\text{(ii)} &\leq \max_s \left| V^R_{\hat{\pi}_n, \hat{f}_n}(s) - V^R_{\pi, f}(s) \right| \\
&\leq \frac{\gamma}{1-\gamma} \max_s \left(\inf_{TV(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \leq \epsilon} \mathbb{E}_{s' \sim p} \left[V^R_{\pi, f}(s') \right] - \inf_{TV(p \| P_f(s, \hat{\pi}_n(s))) \leq \epsilon} \mathbb{E}_{s' \sim p} \left[V^R_{\pi, f}(s') \right] \right).
\end{aligned} \tag{137}$$

Note that both these terms in Equations (136) and (137) are of the form mentioned in the Step (i) of Section 4.

Step (ii): Next, corresponding to step (ii) of the proof outline in Section 4, we use Lemma 19 to bound Equations (136) and (137). Denote $M := \frac{1}{1-\gamma} \geq \max_s V^R(s)$ for convenience. Using Equation (136) and Lemma 20 (internally using Lemma 19), it holds that

$$\begin{aligned}
\text{(i)} &\leq \max_s \left| V^R_{\hat{\pi}_n, f}(s) - V^R_{\hat{\pi}_n, \hat{f}_n}(s) \right| \\
&\leq \frac{1}{1-\gamma} \max_s \left(\inf_{TV(p \| P_f(s, \hat{\pi}_n(s))) \leq \epsilon} \mathbb{E}_{s' \sim p} \left[V^R_{\hat{\pi}_n, f}(s') \right] - \inf_{TV(p \| P_{\hat{f}_n}(s, \hat{\pi}_n(s))) \leq \epsilon} \mathbb{E}_{s' \sim p} \left[V^R_{\hat{\pi}_n, f}(s') \right] \right) \\
&\leq \frac{\gamma}{1-\gamma} \max_{s,a} \left(\sup_{Pr(0) : \frac{p_2 - q}{p_1 - q} \leq \epsilon} \left| \mathbb{E}_{P_f(s,a)}\left[V^R_{\hat{\pi}_n, \hat{f}_n}(s') \right] - \mathbb{E}_{P_{\hat{f}_n}(s,a)}\left[V^R_{\hat{\pi}_n, \hat{f}_n}(s') \right] \right| \right) \qquad (138) \\
&\leq \frac{\gamma}{1-\gamma} \max_{V : \|V\| \leq M} \max_{s,a} \left(\sup_{Pr(0) : \frac{p_2 - q}{p_1 - q} \leq \epsilon} \left| \mathbb{E}_{P_f(s,a)}\left[V(s') \right] - \mathbb{E}_{P_{\hat{f}_n}(s,a)}\left[V(s') \right] \right| \right). \qquad (139)
\end{aligned}$$

We can bound (ii) similarly.

$$\begin{aligned}
\text{(ii)} &\leq \max_s \left| V^R_{\hat{\pi}_n, \hat{f}_n}(s) - V^R_{\pi, f}(s) \right| \qquad (140) \\
&\leq \frac{\gamma}{1-\gamma} \max_{V : \|V\| \leq M} \max_{s,a} \left(\sup_{Pr(0) : \frac{p_2 - q}{p_1 - q} \leq \epsilon} \left| \mathbb{E}_{P_f(s,a)}\left[V(s') \right] - \mathbb{E}_{P_{\hat{f}_n}(s,a)}\left[V(s') \right] \right| \right). \qquad (141)
\end{aligned}$$

Step (iii): Next, we want to utilize the learning error bound (Equation (26)) that bounds the difference between the means of true nominal transition dynamics P_f and learned nominal transition dynamics $P_{\hat{f}_n}$ to bound Equations (139) and (141).

We begin by bounding the difference $\mathbb{E}_{P_f(s,a)}[(\ V(s')\ )\ ]\ \mathbb{E}_{P_{\hat{f}_n}(s,a)}[(\ V(s')\ )\ ]$, by the difference in means of P_f and $P_{\hat{f}_n}$ in Lemma 21. Since Equation (139) has a $\max$ over all value functions, we introduce a covering number argument in Lemma 22 to reform it to a $\max$ over the functions in the covering set. We then use Lemma 21 to obtain bounds in terms of maximum information gain $_{Nd}$ (Equation (9)) and . Further details regarding the covering number argument are deferred to Lemma 22. Then, we apply the result of Lemma 22 with 1 (defined in Lemma 22) on Equation (139). Then, it holds that

$$(i) \le \max_s V^R_{\hat{}_n;f}(s) \quad V^R_{\hat{}_n;\hat{f}_n}(s) \quad O\left(\frac{(2\ \ )}{(1\ \ )^2}\ \frac{_n(\ )\sqrt{2ed^2\ _{nd}}}{\sqrt{n}}\right). \tag{142}$$

Note that $_n$, which appears in Lemma 3, has a logarithmic dependence on n. Similarly, from Equation (141), and Lemmas 21 and 22, we obtain

$$(ii) \le \max_s V^R_{\hat{}_n;\hat{f}_n}(s) \quad V^R_{\ ;f}(s) \quad O\left(\frac{(2\ \ )}{(1\ \ )^2}\ \frac{_n(\ )\sqrt{2ed^2\ _{nd}}}{\sqrt{n}}\right). \tag{143}$$

Note that we want to bound $V^R_{\hat{}_n;f}(s)\ \ V^R_{\ ;f}(s)\ \ (i)\ \ (ii)$ over all $s \in S$. Using $\max_s V^R_{\hat{}_n;f}(s)\ \ V^R_{\ ;f}(s) \le \max_s V^R_{\hat{}_n;\hat{f}_n}(s)\ \ V^R_{\ ;f}(s)\ \ \max_s V^R_{\hat{}_n;\hat{f}_n}(s)\ \ V^R_{\ _n;f}(s)$ and substituting M by $1/(1\ \ )$, we obtain from Equation (142) and Equation (143)

$$\max_s V^R_{\hat{}_n;f}(s) \quad V^R_{\ ;f}(s) \quad O\left(\frac{(2\ \ )}{(1\ \ )^2}\ \frac{_n(\ )\sqrt{2ed^2\ _{nd}}}{\sqrt{n}}\right).$$

Finally, to ensure that $\max_s |V^R_{\hat{}_n;f}(s)\ \ V^R_{\ ;f}(s)| \le$, it suffices to have

$$\max_s V^R_{\hat{}_n;f}(s) \quad V^R_{\ ;f}(s) \quad O\left(\frac{(2\ \ )}{(1\ \ )^2}\ \frac{_n(\ )\sqrt{2ed^2\ _{nd}}}{\sqrt{n}}\right) \qquad .$$

Moving $\sqrt{n}$ and to opposite sides and squaring both sides, we obtain

$$n \quad O\left(\frac{(2\ \ )^2\ ^2}{^2(1\ \ )^4}\ \frac{_n(\ )^2 2ed^2\ _{nd}}{^2\ ^2}\right).$$

□

Lemma 20. *(Simplification using Lemma 19 reformulation) Let* V *be a value function from* $S \to [0, 1/(1\ \ )]$. *Then, it holds that*

$$\max_s \Big| \inf_{TV(p||P_{\hat{f}_n}(s;\hat{}_n(s))) \le} \mathbb{E}_{s' \sim p}\ V(s') \quad \inf_{TV(p||P_f(s;\hat{}_n(s))) \le} \mathbb{E}_{s' \sim p}\ V(s') \Big| \le$$
$$\max_{s;a} \sup_{\in[0;\frac{(2\ \ )}{(1\ \ )}]} \{|(\mathbb{E}_{P_f(s;a)}[(\ V(s')\ )\ ]\ \ \mathbb{E}_{P_{\hat{f}_n}(s;a)}[(\ V(s')\ )\ ]|\}.$$

Proof. First note that,

$$\max_s \inf_{TV(p||P_{\hat{f}_n}(s;\hat{}_n(s))) \le} \mathbb{E}_{s' \sim p}\ V(s') \quad \inf_{TV(p||P_f(s;\hat{}_n(s))) \le} \mathbb{E}_{s' \sim p}\ V(s') \quad \le$$
$$\max_{s;a} \inf_{TV(p||P_{\hat{f}_n}(s;a)) \le} \mathbb{E}_{s' \sim p}\ V(s') \quad \inf_{TV(p||P_f(s;a)) \le} \mathbb{E}_{s' \sim p}\ V(s') \tag{144}$$

Using Lemma 19 and focusing to bound right side of Equation (144) for one particular (s, a) state action pair, we obtain

$$\inf_{TV(p||P_{\hat{f}_n}(s;a)) \le} \mathbb{E}_{s' \sim p}\ V(s') \quad \inf_{TV(p||P_f(s;a)) \le} \mathbb{E}_{s' \sim p}\ V(s')$$

$$\sup_{\eta\in[0,\frac{(2+\rho)}{(1-\gamma)}]}\Big\{-\mathbb{E}_{P_f(s,a)}(\eta-V(s'))_+ - \frac{\rho(\eta-ESI_{P_f(s,a)}(V(s')))_+}{2}+\eta\Big\} - \sup_{\eta\in[0,\frac{(2+\rho)}{(1-\gamma)}]}\Big\{-\mathbb{E}_{P_{\hat f_n}(s,a)}(\eta-V(s'))_+ - \frac{\rho(\eta-ESI_{P_{\hat f_n}(s,a)}(V(s')))_+}{2}+\eta\Big\} \tag{145}$$

$$\leq \sup_{\eta\in[0,\frac{(2+\rho)}{(1-\gamma)}]}\Big\{\big|(\mathbb{E}_{P_f(s,a)}[(\eta-V(s'))_+]) - \mathbb{E}_{P_{\hat f_n}(s,a)}[(\eta-V(s'))_+]\big|\Big\}. \tag{146}$$

Here, Equation (146) is obtained using $ESI_{P_f(s,a)}(V(s')) = ESI_{P_{\hat f_n}(s,a)}(V(s'))$ as shown in proof of Lemma 9 (Case-1).

∎

Lemma 21. *(Bound by difference between estimated model $\hat f_n$ and true f) Let V be a value function from $\mathcal{S}\to[0,1/(1-\gamma)]$. Then, it holds that*

$$\big|\mathbb{E}_{P_f(s,a)}[(\eta-V(s'))_+] - \mathbb{E}_{P_{\hat f_n}(s,a)}[(\eta-V(s'))_+]\big| \leq \frac{(2+\rho)}{(1-\gamma)}\sigma^{-1}\|f(s,a)-\hat f_n(s,a)\|, \tag{147}$$

where $P_{\hat f_n}(s,a) = \mathcal{N}(\hat f_n(s,a),\sigma^2 I)$ *and* $P_f(s,a) = \mathcal{N}(f(s,a),\sigma^2 I)$ *and* $\eta\in[0,\frac{(2+\rho)}{(1-\gamma)}]$.

Proof.

$$\begin{aligned}
&\mathbb{E}_{P_f(s,a)}[(\eta-V(s'))_+] - \mathbb{E}_{P_{\hat f_n}(s,a)}[(\eta-V(s'))_+]\\
&= \int_{\mathbb{R}^d}\frac{1}{\sqrt{(2\pi\sigma^2)^d}}(\eta-V(s'))_+\Big(e^{-\frac{\|x-f(s,a)\|^2}{2\sigma^2}} - e^{-\frac{\|x-\hat f_n(s,a)\|^2}{2\sigma^2}}\Big)\\
&\leq \int_{\mathbb{R}^d}\frac{1}{\sqrt{(2\pi\sigma^2)^d}}(\eta-V(s'))_+\Big|e^{-\frac{\|x-f(s,a)\|^2}{2\sigma^2}} - e^{-\frac{\|x-\hat f_n(s,a)\|^2}{2\sigma^2}}\Big|\\
&\overset{(i)}{\leq} \frac{(2+\rho)}{(1-\gamma)}\int_{\mathbb{R}^d}\frac{1}{\sqrt{(2\pi\sigma^2)^d}}\Big|e^{-\frac{\|x-f(s,a)\|^2}{2\sigma^2}} - e^{-\frac{\|x-\hat f_n(s,a)\|^2}{2\sigma^2}}\Big|\\
&\overset{(ii)}{\leq} 2\frac{(2+\rho)}{(1-\gamma)}\,\mathrm{TV}(P_{\hat f_n}(s,a),P_f(s,a))\\
&\overset{(iii)}{\leq} 2\frac{(2+\rho)}{(1-\gamma)}\sqrt{\mathrm{KL}(P_{\hat f_n}(s,a),P_f(s,a))/2}\\
&\overset{(iv)}{\leq} 2\frac{(2+\rho)}{(1-\gamma)}\sqrt{\|f(s,a)-\hat f_n(s,a)\|^2/4\sigma^2}\\
&\leq \frac{(2+\rho)}{(1-\gamma)}\|f(s,a)-\hat f_n(s,a)\|/\sigma;
\end{aligned}$$

where (i) follows from $(\eta-V(s'))^2\leq\frac{(2+\rho)}{(1-\gamma)}$ as $\eta\leq\frac{(2+\rho)}{(1-\gamma)}$, (ii) follows from the definition of Total Variation (TV) distance between any two multivariate Gaussians, (iii) uses the Pinsker's inequality, and (iv) uses the formula for KL-divergence between multivariate Gaussian distributions.

∎

Lemma 22. *(ϵ-cover construction) For $\mathcal{V}$ denoting the set of value functions from $\mathcal{S}\to[0,1/(1-\gamma)]$, with probability at least $1-\delta$ it holds that*

$$\max_{V\in\mathcal{V}}\max_{s,a}\sup_{\eta\in[0,\frac{(2+\rho)}{(1-\gamma)}]}\Big\{\big|\mathbb{E}_{P_f(s,a)}[(\eta-V(s'))_+] - \mathbb{E}_{P_{\hat f_n}(s,a)}[(\eta-V(s'))_+]\big|\Big\}$$

$$\leq \mathcal{O}\left(\frac{(2+\rho)}{(1-\gamma)}\cdot\frac{\beta_n(\delta)\sqrt{2ed^2\Gamma_{nd}}}{\sqrt{n}}\right). \tag{148}$$

Proof. Let $N_V(\varepsilon)$ be the cover of the set V. By definition, there exists $V^1 \in N_V(\varepsilon)$ such that $\|V^1 - V\| \leq$ for every $V \in V$.

$$\begin{aligned} &|\mathrm{E}_{P_f(s,a)}[V(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V(s^1)]| \\ &\leq |\mathrm{E}_{P_f(s,a)}[V(s^1)] - \mathrm{E}_{P_f(s,a)}[V^1(s^1)]| \\ &\quad + |\mathrm{E}_{P_f(s,a)}[V^1(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V^1(s^1)]| \\ &\quad + |\mathrm{E}_{P_{\hat{f}_n}(s,a)}[V^1(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V(s^1)]|. \end{aligned} \tag{149}$$

$$\overset{(i)}{\leq} 2\|V^1 - V\| + |\mathrm{E}_{P_f(s,a)}[V^1(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V^1(s^1)]|; \tag{150}$$

where (i) follows from Lemma 23. Using Equation (150), we bound uniformly over all $V \in V$. Using Equation (150) we bound uniformly over all $V \in V$,

$$\max_{V \in V} \max_{s,a} \sup_{\mathrm{Pr}(\cdot;\frac{p_2}{p_1},\frac{q}{q})} |\mathrm{E}_{P_f(s,a)}[V(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V(s^1)]| \tag{151}$$

$$\leq \max_{V^1 \in N_V(\varepsilon)} \max_{s,a} \sup_{\mathrm{Pr}(\cdot;\frac{p_2}{p_1},\frac{q}{q})} \Big(2\|V^1 - V\| + |\mathrm{E}_{P_f(s,a)}[V^1(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V^1(s^1)]| \Big)$$

$$\overset{(ii)}{\leq} \max_{V^1 \in N_V(\varepsilon)} \max_{s,a} \sup_{\mathrm{Pr}(\cdot;\frac{p_2}{p_1},\frac{q}{q})} \Big(|\mathrm{E}_{P_f(s,a)}[V^1(s^1)] - \mathrm{E}_{P_{\hat{f}_n}(s,a)}[V^1(s^1)]| \Big) + 2\varepsilon$$

$$\overset{(iii)}{\leq} \max_{V^1 \in N_V(\varepsilon)} \max_{s,a} \sup_{\mathrm{Pr}(\cdot;\frac{p_2}{p_1},\frac{q}{q})} \frac{p_2}{p_1} \|f(s,a) - \hat{f}_n(s,a)\|_1 + 2\varepsilon$$

$$\overset{(iv)}{\leq} \frac{p_2}{p_1} \sqrt{\frac{2ed^2}{\bar{n}} \ln\left(\frac{nd}{\delta}\right)} + 2\varepsilon \tag{152}$$

$$\overset{(v)}{=} \frac{p_2}{p_1} \sqrt{\frac{2ed^2}{\bar{n}} \ln\left(\frac{nd}{\delta}\right)}; \tag{153}$$

where (ii) follows from $\|V^1 - V\| \leq$, (iii) follows from Lemma 21, (iv) follows from Equation (26), and (v) follows from substituing 1 (or any constant).

□

Lemma 23. *For any two value functions $V, V^1 : S \to [0, \frac{1}{1-\gamma}]$, it holds that*

$$|\mathrm{E}_{P_f(s,a)}[V^1(s^1)] - \mathrm{E}_{P_f(s,a)}[V(s^1)]| \leq \|V^1 - V\|. \tag{154}$$

Proof. Noting that both the distributions are w.r.t. the same distribution $P_f(s,a)$ we have,

$$\mathrm{E}_{P_f(s,a)}[V^1(s^1)] - \mathrm{E}_{P_f(s,a)}[V(s^1)]$$

$$= \int_{s^1} \big(1(V^1(s^1) \geq V(s^1)) - 1(V(s^1) \geq V^1(s^1))\big) P_f(s,a)(s^1) \, ds^1. \tag{155}$$

Adding and subtracting $\int_{s^1} 1(V(s^1) \geq V^1(s^1)) P_{\hat{f}_n}(s,a)(s^1) \, ds^1$ to Equation (155), we obtain 2 terms,

$$i = \int_{s^1} \big(1(V^1(s^1) \geq V(s^1)) - 1(V(s^1) \geq V^1(s^1))\big) P_{\hat{f}_n}(s,a)(s^1) \, ds^1 \tag{156}$$

$$ii = \int_{s^1} 1(V(s^1) \geq V^1(s^1)) \big(P_{\hat{f}_n}(s,a)(s^1) - P_f(s,a)(s^1)\big) \, ds^1. \tag{157}$$

Bounding i first,

$$i = \int_{s^1} \big(1(V^1(s^1) \geq V(s^1)) - 1(V(s^1) \geq V^1(s^1))\big) P_{\hat{f}_n}(s,a)(s^1) \, ds^1 \tag{158}$$

$$\int_{s' \in P_f(s,a)} \mathbb{1}(V'(s') \le V(s))\,(V'(s') \;\;)\,p_{P_f(s,a)}(s')\,ds' \tag{159}$$
$$\int_{s' \in P_f(s,a)} \mathbb{1}(V(s') \;\; V'(s'))\,(V'(s') \;\;)\,p_{P_f(s,a)}(s')\,ds'$$
$$\le \int_{s' \in P_f(s,a)} \mathbb{1}(V'(s') \le V(s))\,(V'(s') \;\; V(s'))\,p_{P_f(s,a)}(s')\,ds' \tag{160}$$
$$\int_{s' \in P_f(s,a)} \mathbb{1}(V(s') \;\; V'(s'))\,(V'(s') \;\; V(s'))\,p_{P_f(s,a)}(s')\,ds'$$
$$\le \int_{s' \in P_f(s,a)} \mathbb{1}(V'(s') \le V(s))\,(V'(s') \;\; V(s'))\,p_{P_f(s,a)}(s')\,ds' \tag{161}$$
$$\int_{s' \in P_f(s,a)} \mathbb{1}(V(s') \;\; V'(s'))\,(V'(s') \;\; V(s'))\,p_{P_f(s,a)}(s')\,ds'$$
$$\le \|V' \;\; V\|. \tag{162}$$

Similarly bounding ii,

$$ii \;\; \int_{s' \in P_f(s,a)} \mathbb{1}(V(s') \;\;)\,(\,(V'(s') \;\;)\,(V(s') \;\;)\,)\,p_{P_f(s,a)}(s')\,ds' \tag{163}$$
$$\int_{s' \in P_f(s,a)} \mathbb{1}(V(s') \;\;)\,(V'(s') \;\; V(s'))\,p_{P_f(s,a)}(s')\,ds' \tag{164}$$
$$\le \int_{s' \in P_f(s,a)} \mathbb{1}(V(s') \;\;)\,(V'(s') \;\; V(s'))\,p_{P_f(s,a)}(s')\,ds' \tag{165}$$
$$\le \|V' \;\; V\|. \tag{166}$$

Using Equations (162) and (166) we get the desired result. □

D Additional Experiments and Details

In this section, we report additional experiments and discuss further details of our experimental setup. All experiments were run with GPU clusters: 10xNVidia 32Gb Tesla V100 with Intel(R) processors (2 cores, 2.50 GHz) and 256Gb RAM. For all the experiments, we use the environment implementations of Mehta et al. (2021) as done in https://github.com/fusion-ml/trajectory-information-rl/tree/main. Also, to learn the environment transition model, we use the same corresponding GP hyperparameters proposed by Mehta et al. (2021). For the offline RFQI/FQI algorithms we follow the implementation of Panaganti et al. (2022); Chen and Jiang (2019) in https://github.com/zaiyan-x/RFQI. We use the same default hyperparameters as used in their code except for training steps, batch size and robustness radius (for RFQI) which we tune depending on the environment as outlined next. For SAC in Pendulum experiments, we use the implementation and hyperparameters of https://github.com/DLR-RM/rl-baselines3-zoo. Whereas, for SAC in Reacher experiments, we use the implementation and hyperparameters of https://github.com/fusion-ml/bac-baselines, https://github.com/IanChar/rlkit2 (as done in (Mehta et al., 2021)).

Pendulum: In Pendulum experiments, we construct the learned model using 60 samples from the true environment. Then, we train a SAC policy on such a model for 2×10^4 steps and use it (with the probability of choosing a random action being 0.3 or 0.5) to generate 10^6 offline data (these are used both for MVR+RFQI and MVR+FQI). For training steps and batch size we consider the following combinations: $\{(2000, 100), (5000, 100), (10000, 100), (20000, 100), (35000, 100), (50000, 100), (5000, 500), (5000, 1000)\}$. We combine all these combinations with the following values of $\rho \in \{0.1, 0.2, 0.3, 0.5, 0.6, 0.7, 0.8, 0.9\}$. For each algorithm, we pick the best-performing combination in terms of average reward over 20 episodes for all (or most) perturbation values. We do this separately for length perturbations and action perturbations. In the length perturbation, the pendulum's length is changed from its nominal value to a new value depending on the perturbation percentage. In the action perturbation, a random action is chosen instead of the action chosen by the policy with various probabilities ranging from $[0, 1]$. We detail the optimal hyperparameters we realized for each algorithm in Table 2 for the

length and action perturbation, respectively. Moreover, we plot the average performance (over 20 episodes) of the different baselines w.r.t. length and action perturbations in Figure 3. We notice that in the case of length perturbation, the robust algorithms (RFQI and MVR+RFQI) outperform the corresponding non-robust baselines. In the case of action perturbations, we observe all algorithms except for SAC achieve similar performance.

	Training Steps	Batch-Size		Random Action Probability (Dataset)
MVR+RFQI	5000	100	0.3	0.5
MVR+FQI	2000	100	-	0.5
RFQI	2000	100	0.9	0.5
FQI	5000	500	-	0.5

	Training Steps	Batch-Size		Random Action Probability (Dataset)
MVR+RFQI	20000	100	0.5	0.3
MVR+FQI	50000	100	-	0.3
RFQI	50000	100	0.1	0.5
FQI	5000	500	-	0.5

Table 2: Hyperparameters for Pendulum - length perturbation (top) and action perturbation (bottom).

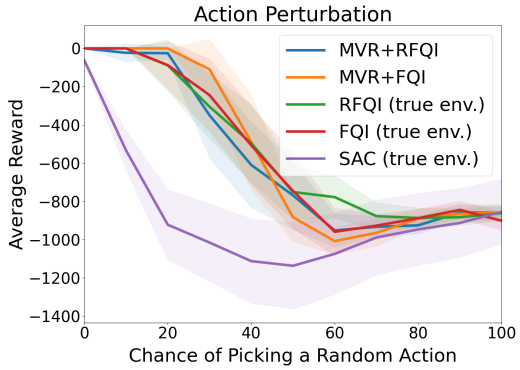


Figure 3: Pendulum experiments.

Cartpole: In Cartpole experiments, we construct the learned model using 150 samples from the true environment. Then, we run MPC on such a model following the implementation and hyperparameters of (Mehta et al., 2021; Pinneri et al., 2020) requiring 2250 samples to calculate the optimal action at each step and use it (with the probability of choosing a random action being 0.3) to generate 10^6 offline data for MVR+RFQI and MVR+FQI. For training steps and batch size, we test the following combinations: $\{1\}2000$ $100^{[1,1]}5000$ $100^{[1,1]}10000$ $100^{[1,1]}20000$ $100^{[1,1]}35000$ $100^{[1,1]}50000$ $100^{[1,1]}5000$ $500^{[1,1]}5000$ $1000^{[1]}$u, and consider radii in $\{0.1, 0.2, 0.3, 0.5, 0.6, 0.7, 0.8, 0.9\}$u. We consider perturbations of the force magnitude and the gravity, whereby the actuation force/gravity is changed from its nominal value to a new value depending on the perturbation percentage. We report the best-performing (average over 20 episodes) hyperparameters for each algorithm in Table 3. Such parameters were observed to be a good choice for both perturbation types. Finally, we plot the average performance (over 20 episodes) of the different baselines w.r.t. force magnitude and gravity perturbations in Figure 4. We notice that in both perturbations, the robust algorithms (RFQI and MVR+RFQI) outperform the corresponding non-robust baselines.

Reacher: In Reacher experiments, we construct the learned model using 2000 samples from the true environment. Then, we train a SAC policy on such a model for 10^6 steps and use it (with the probability of choosing a random action being 0.3) to generate 10^6 offline data for MVR+RFQI and MVR+FQI. For training steps and batch size, we consider the following combinations: $\{1\}10000$ $500^{[1,1]}20000$ $500^{[1,1]}40000$ $500^{[1,1]}80000$ $500^{[1,1]}160000$ $1000^{[1]}$u, while we consider radii in $\{0.1, 0.3, 0.5, 0.7, 0.9\}$u. We consider perturbations of the joint stiffness subject to different equilibrium positions, the latter represented by the 'Springref' parameter which we take to be 50 or 100. In both perturbation types, the joint stiffness is changed from its nominal value of 0 to a new value depending on