Visual Adversarial Imitation Learning using Variational Models

Anonymous Author(s)
Affiliation
Address
email

Abstract

Reward function specification, which requires considerable human effort and iteration, remains a major impediment for learning behaviors through deep reinforcement learning. In contrast, providing visual demonstrations of desired behaviors presents an easier and more natural way to teach agents. We consider a setting where an agent is provided a fixed dataset of visual demonstrations illustrating how to perform a task, and must learn to solve the task using the provided demonstrations and unsupervised environment interactions. This setting presents a number of challenges including representation learning for visual observations, sample complexity due to high dimensional spaces, and learning instability due to the lack of a fixed reward or learning signal. Towards addressing these challenges, we develop a variational model-based adversarial imitation learning (V-MAIL) algorithm. The model-based approach provides a strong signal for representation learning, enables sample efficiency, and improves the stability of adversarial training by enabling on-policy learning. Through experiments involving several vision-based locomotion and manipulation tasks, we find that V-MAIL learns successful visuomotor policies in a sample-efficient manner, has better stability compared to prior work, and also achieves higher asymptotic performance. We further find that by transferring the learned models, V-MAIL can learn new tasks from visual demonstrations without any additional environment interactions. All results including videos can be found online at https://sites.google.com/view/variational-mail.

1 Introduction

The ability of reinforcement learning (RL) agents to autonomously learn by interacting with the environment presents a promising approach for learning diverse skills. However, reward specification has remained a major challenge in the deployment of RL in practical settings [2, 9, 37]. The ability to imitate humans or other expert trajectories allows us to avoid the reward specification problem, while also circumventing challenges related to exploration in RL. Visual demonstrations are also a more natural way to teach robots various tasks and skills in real-world applications. However, this setting is also fraught with a number of technical challenges including representation learning for visual observations, sample complexity due to the high dimensional observation spaces, and learning instability [35, 25, 32] due to lack of a stationary learning signal. We aim to overcome these challenges and to develop an algorithm that can learn from limited demonstration data as well as scale to high-dimensional observation and action spaces often encountered in robotics applications.

Behaviour cloning (BC) is a classic algorithm to imitate expert demonstrations [34], which uses supervised learning to greedily match the expert behaviour at demonstrated expert states. Due to environment stochasticity, covariate shift, and policy approximation error, the agent may drift away from the expert state distribution and ultimately fail to mimic the demonstrator [40]. While a wide initial state distribution [41] or the ability to interactively query the expert policy [40] can

Submitted to 35th Conference on Neural Information Processing Systems (NeurIPS 2021). Do not distribute.

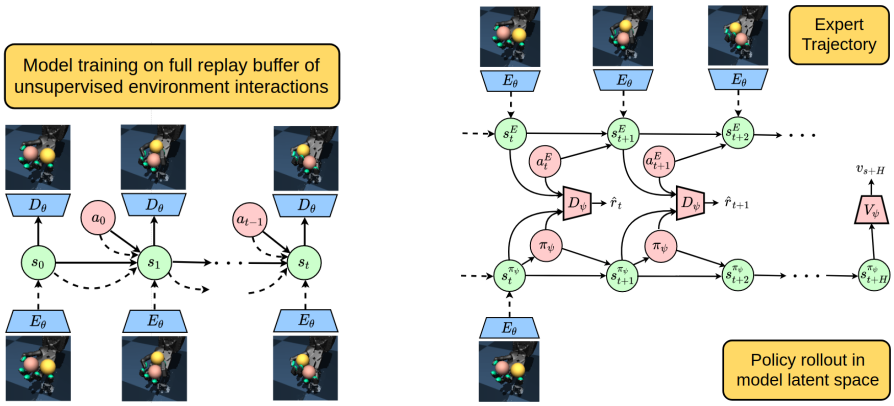

Figure 1: **Left**: the variational dynamics model, which enables joint representation learning from visual inputs and a latent space dynamics model, and the discriminator which is trained to distinguish latent states of expert demonstrations from that of policy rollouts. Dashed lines represent inference and solid lines represent the generative model. **Right**: the policy training, which uses the discriminator as the reward function, so that the policy induces a latent state visitation distribution that is indistinguishable from that of the expert. The learned policy network is composed with the image encoder from the variational model to recover a visuomotor policy.

circumvent these difficulties, such conditions require additional supervision and are difficult to meet in practical applications. An alternate line of work based on inverse RL [13, 14] and adversarial imitation learning [22, 12] aims to not only match actions at demonstrated states, but also the long term visitation distribution [16]. These approaches explicitly train a GAN-based classifier [17] to distinguish the visitation distribution of the agent from the expert, and use it as a reward signal for training the agent with RL. While these methods have achieved substantial improvement over behaviour cloning without additional expert supervision, they are difficult to deploy in realistic scenarios, primarily due to three reasons: (1) the objective requires on-policy data collection leading to high sample complexity; (2) the non-stationarity reward function changes as the RL agent learns; and (3) high-dimensional observation spaces require representation learning and exacerbate the optimization challenges.

Our main contribution in this work is the development of a new algorithm, variational model-based adversarial imitation learning (V-MAIL), which aims to overcome each of the aforementioned challenges within a single framework. As illustrated in Figure 1, V-MAIL trains a variational latent-space dynamics model and a discriminator that provides a learning reward signal by distinguishing latent rollouts of the agent from the expert. The key insight of our approach is that variational models can address these challenges simultaneously by (a) making it possible to collect on-policy roll-outs inside the model without environment interaction, leading to an efficient and stable optimization process and (b) providing a rich auxiliary objective for efficiently learning compact state representations and which regularizes the discriminator. Furthermore, the variational model also allows V-MAIL to perform zero-shot transfer to new imitation learning tasks. By generating on-policy rollouts within the model, and training the discriminator using these rollouts along with demonstrations of a new task, V-MAIL can learn policies for new tasks without any additional environment interactions.

Through experiments on a collection of vision-based locomotion and manipulation tasks, we find that V-MAIL can learn successful visuomotor control policies through imitation learning. In particular, V-MAIL exhibits stable and near-monotonic learning, is highly sample efficient, and asymptotically matches the expert level performance on most tasks. In contrast, prior algorithms exhibit unstable learning and poor asymptotic performance, often achieving less that 20% of expert level performance. We further show the ability to transfer our models to novel task and acquire qualitatively new behaviors using only a few demonstrations and no additional environment interactions. To our knowledge this is the first approach to use variational model-based training for zero-shot or few-shot imitation learning.

2 Related Work

Here, we review the relevant literature on imitation learning and image-based RL.

Imitation Learning. Recent model-free imitation learning can be categorized as either adversarial or non-adversarial. Adversarial methods inspired by GANs [17] train an explicit classifier between

expert and policy behaviour and optimize the agent in a two-player minimax game. GAIL [22] and AIRL [14] are two such algorithms; however they often have poor sample efficiency due to the requirement of on-policy rollouts in the environment. To address sample efficiency issues, off-policy variants such as DAC [27] and SAM [5] have been developed, however they suffer from an objective mismatch when using off-policy data [28], often resulting in learning instability [6].

An alternate line of research attempts to forego adversarial training: SQIL [39] frames the problem as regularized behaviour cloning and trains an off-policy algorithm with rewards of 1 for expert trajectories and 0 for policy ones. RCE [10] uses a very similar approach, but derives it as maximizing probability of task success, which they show is equivalent to minimizing the Hellinger distance between the policy occupation distribution and a particular target distribution. ValueDICE [28] uses the same key result for iterative distribution matching as RCE in conjunction with the Donsker-Varadhan representation to obtain an off-policy distribution matching algorithm. In Swamy et al. [42] the authors derive distribution matching as a bound on policy under-performance, similar to our analysis in Section 4.1 and propose a practical non-adversarial algorithm AdVIL, however in reported experiments it does not outperform behaviour cloning. A few papers have considered model-based imitation learning as well: Baram et al. [3] is an adversarial algorithm conceptually similar to our approach, but only focuses on low-dimensional state-based tasks and train the discriminator using off-policy replay buffer, which does not allow it to generalize to new tasks. Related to our method is Finn et al. [13] which uses a similar reward learning in combination with a locally linear dynamics model, which leads to trajectory centric algorithms and the inability to transfer the model to new tasks. Das et al. [8] considers a similar setting for inverse RL using a simplified parameterization of the cost function. In this work we develop end-to-end model for adversarial imitation learning in high-dimensional POMDPs and generalization to novel tasks without hand-designed features.

Reinforcement Learning From Images with Variational Models. Reinforcement learning from images is an inherently difficult task, since the agent needs to learn meaningful visual representations to support policy learning. A recent line of research [15, 19, 30, 20, 36] train a variational model of the image-based environment as an auxiliary task, either for representation learning only [15, 30] or for additionally generating on-policy data by rolling out the model [20]. Our method builds upon these ideas, but unlike these prior works, considers the problem of learning from visual demonstrations without access to rewards.

3 Preliminaries

We consider the problem setting of learning in partially observed Markov decision processes (POMDPs), which can be described with the tuple: $\mathcal{M} = (\mathcal{S}, \mathcal{A}, \mathcal{X}, \mathcal{R}, \mathcal{T}, \mathcal{U}, \gamma)$, where $\boldsymbol{s} \in \mathcal{S}$ is the state space, $\boldsymbol{a} \in \mathcal{A}$ is the action space, $\boldsymbol{x} \in \mathcal{X}$ is the observation space and $r = \mathcal{R}(\boldsymbol{s}, \boldsymbol{a})$ is a reward function. The state evolution is Markovian and governed by the dynamics as $\boldsymbol{s}' \sim \mathcal{T}(\cdot|\boldsymbol{s}, \boldsymbol{a})$. Finally, the observations are generated through the observation model $\boldsymbol{x} \sim \mathcal{U}(\cdot|\boldsymbol{s})$. The widely studied Markov decision process (MDP) is a special case of this 7-tuple where the underlying state is directly observed in the observation model.

In this work, we study imitation learning in unknown POMDPs. Thus, we do not have access to the underlying dynamics, the true state representation of the POMDP, or the reward function. In place of the rewards, the agent is provided with a fixed set of expert demonstrations collected by executing an expert policy π^E, which we assume is optimal under the unknown reward function. The agent can interact with the environment and must learn a policy $\pi(\boldsymbol{a}_t|\boldsymbol{x}_{\leq t})$ that mimics the expert.

3.1 Imitation learning as divergence minimization

In line with prior work, we interpret imitation learning as a divergence minimization problem [22, 16, 24]. For simplicity of exposition, we consider the MDP case in this section, and discuss POMDP extensions in Section 4.2. Let $\rho^\pi_{\mathcal{M}}(\boldsymbol{s}, \boldsymbol{a}) = (1-\gamma)\sum_{t=0}^{\infty} \gamma^t P(\boldsymbol{s}_t = \boldsymbol{s}, \boldsymbol{a}_t = \boldsymbol{a})$ be the discounted state-action visitation distribution of a policy π in MDP $\mathcal{M}$. Then, a divergence minimization objective for imitation learning corresponds to

$$\min_{\pi} \; \mathbb{D}(\rho^\pi_{\mathcal{M}}, \rho^E_{\mathcal{M}}), \tag{1}$$

where $\rho^E_{\mathcal{M}}$ is the discounted visitation distribution of the expert policy π^E, and $\mathbb{D}$ is a divergence measure between probability distributions such as KL-divergence, Jensen-Shannon divergence, or a generic $f-$divergence. To see why this is a reasonable objective, let $J(\pi, \mathcal{M})$ denote the expected

value of a policy π in $\mathcal{M}$. Inverse RL [46, 22, 12] interprets the expert as the optimal policy under some unknown reward function. With respect to this unknown reward function, the sub-optimality of any policy π can be bounded as:

$$\Big|J(\pi^E, \mathcal{M}) - J(\pi, \mathcal{M})\Big| \leq \frac{R_{\max}}{1-\gamma}\, \mathbb{D}_{TV}(\rho^{\pi}_{\mathcal{M}}, \rho^{E}_{\mathcal{M}}),$$

since the policy performance is $J(\pi, \mathcal{M}) = \mathbb{E}_{(\boldsymbol{s},\boldsymbol{a})\sim\rho^{\pi}_{\mathcal{M}}}\big[r(\boldsymbol{s},\boldsymbol{a})\big]$. We use $\mathbb{D}_{TV}$ to denote total variation distance. Since various divergence measures are related to the total variation distance, optimizing the divergence between visitation distributions in state space amounts to optimizing a bound on the policy sub-optimality.

3.2 Generative Adversarial Imitation Learning (GAIL)

With the divergence minimization viewpoint, any standard generative modeling technique including density estimation, VAEs, GANs etc. can in principle be used to minimize Eq. 1. However, in practice, use of certain generative modeling techniques can be difficult. A standard density estimation technique would involve directly parameterizing $\rho^{\pi}_{\mathcal{M}}$, say through auto-regressive flows, and learning the density model. However, a policy that induces the learned visitation distribution in $\mathcal{M}$ is not guaranteed to exist and may prove hard to recover. Similar challenges prevent the direct application of a VAE based generative model as well. In contrast, GANs allow for a policy based parameterization, since it only requires the ability to sample from the generative model and does not require the likelihood. This approach was followed in GAIL, leading to the optimization

$$\max_{\pi}\ \min_{D_\psi}\ \mathbb{E}_{(\boldsymbol{s},\boldsymbol{a})\sim\rho^{E}_{\mathcal{M}}}\big[-\log D_\psi(\boldsymbol{s},\boldsymbol{a})\big]\ +\ \mathbb{E}_{(\boldsymbol{s},\boldsymbol{a})\sim\rho^{\pi}_{\mathcal{M}}}\Big[-\log\big(1 - D_\psi(\boldsymbol{s},\boldsymbol{a})\big)\Big], \tag{2}$$

where D_ψ is a discriminative classifier used to distinguish between samples from the expert distribution and the policy generated distribution. Results from Goodfellow et al. [17] and Ho & Ermon [22] suggest that the learning objective in Eq. 2 corresponds to the divergence minimization objective in Eq. 1 with Jensen-Shannon divergence. In order to estimate the second expectation in Eq. 2 we require on-policy samples from π, which is data-inefficient. Adversarial off-policy algorithms, such as [27, 5] replace the expectation under the policy distribution with expectation under the current replay buffer distribution, which allows for off-policy training, but no longer guarantee that the policy marginal distribution will match the expert.

4 Variational Model-Based Adversarial Imitation Learning

Generative modeling in the context of imitation learning poses unique challenges. Improving the generative distribution (policy in our case) requires samples from $\rho^{\pi}_{\mathcal{M}}$, which requires rolling out π in the environment. Furthermore, the complex optimization landscape of a saddle point problem requires many iterations of learning, each of which requires on-policy rollouts. This is unlike typical generative modeling applications where generating samples from the generator is cheap and does not require any environment interactions. To overcome this challenge, we present a model-based imitation learning algorithm. For conceptual clarity and ease of exposition, we will first present our conceptual algorithm in the MDP setting in Section 4.1. Subsequently, we will extend this algorithm to the POMDP case in Section 4.2. Finally, we present a practical version of our algorithm in Section 4.3.

4.1 Model-Based Adversarial Imitation Learning

Model-based algorithms for RL and IL involve learning an approximate dynamics model $\widehat{\mathcal{T}}$ using environment interactions. The learned dynamics model can be used to construct an approximate MDP $\widehat{\mathcal{M}}$. In our context of imitation learning, learning a dynamics model allows us to generate samples from $\widehat{\mathcal{M}}$ as a surrogate for samples from $\mathcal{M}$, leading to the objective:

$$\min_{\pi}\ \ \mathbb{D}(\rho^{\pi}_{\widehat{\mathcal{M}}}, \rho^{E}_{\mathcal{M}}), \tag{3}$$

which can serve as a good proxy to Eq. 1 as long as the model approximation is accurate. In particular, with an α-approximate dynamics model given by $\mathbb{D}_{TV}(\widehat{\mathcal{T}}(\boldsymbol{s},\boldsymbol{a}), \mathcal{T}(\boldsymbol{s},\boldsymbol{a})) \leq \alpha\ \forall(\boldsymbol{s},\boldsymbol{a})$, we can bound the policy suboptimality with respect to the expert as:

$$\Big|J(\pi^E, \mathcal{M}) - J(\pi, \mathcal{M})\Big| \leq \frac{R_{\max}}{1-\gamma}\, \mathbb{D}_{TV}(\rho^{\pi}_{\widehat{\mathcal{M}}}, \rho^{E}_{\mathcal{M}}) + \frac{\alpha \cdot R_{\max}}{(1-\gamma)^2}. \tag{4}$$

Thus, the divergence minimization in Eq. 3 serves as an approximate bound on the sub-optimality with a bias that is proportional to the model error. Thus, we ultimately propose to solve the following saddle point optimization problem:

$$\max_{\pi} \min_{D_\psi} \mathbb{E}_{(\boldsymbol{s},\boldsymbol{a})\sim\rho^E_{\mathcal{M}}}\left[-\log D_\psi(\boldsymbol{s},\boldsymbol{a})\right] + \mathbb{E}_{(\boldsymbol{s},\boldsymbol{a})\sim\rho^\pi_{\widehat{\mathcal{M}}}}\left[-\log\left(1-D_\psi(\boldsymbol{s},\boldsymbol{a})\right)\right], \tag{5}$$

which requires generating on-policy samples only from the learned model $\widehat{\mathcal{M}}$. We can interleave policy learning according to Eq. 5 with performing policy rollouts in the real environment to iteratively improve the model. Provided the policy is updated sufficiently slowly, Rajeswaran et al. [38] show that such interleaved policy and model learning corresponds to a stable and convergent algorithm, while being highly sample efficient.

4.2 Extension to POMDPs

In POMDPs, the underlying state is not directly observed, and thus cannot be directly used by the policy. In this case, we typically use the notion of *belief state*, which is defined to be the filtering distribution $P(\boldsymbol{s}_t|\boldsymbol{h}_t)$, where we denote history with $\boldsymbol{h}_t := (\boldsymbol{x}_{\leq t}, \boldsymbol{a}_{<t})$. By using the historical information, the belief state provides more information about the current state, and can enable the learning of better policies. However, learning and maintaining an explicit distribution over states can be difficult. Thus, we consider learning a latent representation of the history $\boldsymbol{z}_t = q(\boldsymbol{h}_t)$, so that $P(\boldsymbol{s}_t|\boldsymbol{h}_t) \approx P(\boldsymbol{s}_t|\boldsymbol{z}_t)$.

To develop an algorithm for the POMDP setting, we first make the key observation that imitation learning in POMDPs can be reduced to divergence minimization in the latent belief state representation. To formalize this, we introduce the following theorem. A formal version of the theorem and proof are provided in the appendix.

Theorem 1. *(Divergence bound in latent space; Informal) Consider a POMDP $\mathcal{M}$, and let $\boldsymbol{z}_t$ be a latent space representation of the history and belief state such that $P(\boldsymbol{s}_t|\boldsymbol{x}_{\leq t}, \boldsymbol{a}_{<t}) = P(\boldsymbol{s}_t|\boldsymbol{z}_t)$. Let D_f be a generic $f-$divergence. Then the following inequalities hold:*

$$D_f(\rho^\pi_{\mathcal{M}}(\boldsymbol{x},\boldsymbol{a})||\rho^E_{\mathcal{M}}(\boldsymbol{x},\boldsymbol{a})) \leq D_f(\rho^\pi_{\mathcal{M}}(\boldsymbol{s},\boldsymbol{a})||\rho^E_{\mathcal{M}}(\boldsymbol{s},\boldsymbol{a})) \leq D_f(\rho^\pi_{\mathcal{M}}(\boldsymbol{z},\boldsymbol{a})||\rho^E_{\mathcal{M}}(\boldsymbol{z},\boldsymbol{a}))$$

Theorem 1 suggests that the divergence of visitation distributions in the latent space represents an upper bound of the divergence in the state and observation spaces. This is particularly useful, since we do not have access to the ground-truth states of the POMDP and matching the expert marginal distribution in the high-dimensional observation space (such as images) could be difficult. Furthermore, based on the results in Section 3.1, minimizing the state divergence results in minimizing a bound on policy sub-optimality as well. These results provide a direct way to extend the results from Section 4.1 to the POMDP setting. If we can learn an encoder $\boldsymbol{z}_t = q(\boldsymbol{x}_{\leq t}, \boldsymbol{a}_{<t})$ that captures sufficient statistics of the history, and a latent state space dynamics model $\boldsymbol{z}_{t+1} \sim \widehat{\mathcal{T}}(\cdot|\boldsymbol{z}_t, \boldsymbol{a}_t)$, then we can learn the policy by extending Eq. 5 to the induced MDP in the latent space as:

$$\max_{\pi} \min_{D_\psi} \mathbb{E}_{(\boldsymbol{z},\boldsymbol{a})\sim\rho^E_{\mathcal{M}}(\boldsymbol{z},\boldsymbol{a})}\left[-\log D_\psi(\boldsymbol{z},\boldsymbol{a})\right] + \mathbb{E}_{(\boldsymbol{z},\boldsymbol{a})\sim\rho^\pi_{\widehat{\mathcal{M}}}(\boldsymbol{z},\boldsymbol{a})}\left[-\log\left(1-D_\psi(\boldsymbol{z},\boldsymbol{a})\right)\right]. \tag{6}$$

Once learned, the policy can be composed with the encoder for deployment in the POMDP.

4.3 Practical Algorithm with Variational Models

The divergence bound of Theorem 1 allows us to develop a practical algorithm if we can learn a good belief state representation. Towards that end we turn to the theory of deep Bayesian filters [23] and begin with the likelihood:

$$\log P(\boldsymbol{x}_{1:T}|\boldsymbol{a}_{1:T}) = \log \int \prod_{t=1}^{T} \mathcal{U}(\boldsymbol{x}_t|\boldsymbol{s}_t)\mathcal{T}(\boldsymbol{s}_t|\boldsymbol{a}_{t-1}, \boldsymbol{s}_{t-1}) d\boldsymbol{s}_{1:T}$$

We can introduce the belief distribution $q(\boldsymbol{z}_{1:T}|\boldsymbol{x}_{1:T}, \boldsymbol{a}_{1:T-1}) = \prod_{t=1}^{T} q(\boldsymbol{z}_t|\boldsymbol{x}_t, \boldsymbol{z}_{t-1}, \boldsymbol{a}_{t-1})$, which considers only model classes that satisfy the the sufficient statistics requirement. Using the introduced belief distribution as the variational distribution, we derive the evidence lower bound (ELBO) [4, 26]:

Algorithm 1 V-MAIL: Variational Model-Based Adversarial Imitation Learning

Require: Expert demos $\mathcal{B}_E$, environment buffer $\mathcal{B}_\pi$.
Randomly initialize variational model $\{q_\theta, \widehat{\mathcal{T}}_\theta\}$, policy π_ψ and discriminator D_ψ
for number of iterations **do**
    `// Environment Data Collection`
    for timestep $t = 1 : T$ **do**
        Estimate latent state from the belief distribution $\boldsymbol{z}_t \sim q_\theta(\cdot|\boldsymbol{x}_t, \boldsymbol{z}_{t-1}, \boldsymbol{a}_{t-1})$
        Sample action $\boldsymbol{a}_t \sim \pi_\psi(\boldsymbol{a}_t|\boldsymbol{z}_t)$
        Step environment and get observation $\boldsymbol{x}_{t+1}$
    Add data $\{\boldsymbol{x}_{1:T}, \boldsymbol{a}_{1:T-1}\}$ to policy replay buffer $\mathcal{B}_\pi$
    for number of training iterations **do**
        `// Dynamics Learning`
        Sample a batch of trajectories $\{\boldsymbol{x}_{1:T}, \boldsymbol{a}_{1:T-1}\}$ from the joint buffer $\mathcal{B}_E \cup \mathcal{B}_\pi$
        Optimize the variational model $\{q_\theta, \widehat{\mathcal{T}}_\theta\}$ using Equation 7
        `// Adversarial Policy Learning`
        Sample trajectories from expert buffer $\{\boldsymbol{x}^E_{1:T}, \boldsymbol{a}^E_{1:T-1}\} \sim \mathcal{B}_E$
        Infer expert latent states $\boldsymbol{z}^E_{1:T} \sim q_\theta(\cdot|\boldsymbol{x}^E_{1:T}, \boldsymbol{a}^E_{1:T-1})$ using the belief model q_θ
        Generate latent rollouts $\boldsymbol{z}^{\pi_\psi}_{1:H}$ using the policy π_ψ from the forward model $\widehat{\mathcal{T}}_\theta$
        Update the discriminator D_ψ with data $\boldsymbol{z}^E_{1:T}, \boldsymbol{z}^{\pi_\psi}_{1:H}$ using Equation 6
        Update the policy π_ψ to improve the value function in Equation 8

$$\log P(\boldsymbol{x}_{1:T}|\boldsymbol{a}_{1:T}) \geq \mathbb{E}_{q(\boldsymbol{z}_{1:T}|\boldsymbol{x}_{1:T}, \boldsymbol{a}_{1:T-1})} \left[\log \prod_{t=1}^{T} \mathcal{U}(\boldsymbol{x}_t|\boldsymbol{z}_t) \frac{\mathcal{T}(\boldsymbol{z}_t|\boldsymbol{a}_{t-1}, \boldsymbol{z}_{t-1})}{q(\boldsymbol{z}_t|\boldsymbol{x}_t, \boldsymbol{z}_{t-1}, \boldsymbol{a}_{t-1})} \right]$$

To estimate the expectation, we can use sequential sampling from the belief distribution $\boldsymbol{z}_t \sim q(\cdot|\boldsymbol{x}_t, \boldsymbol{z}_{t-1}, \boldsymbol{a}_{t-1}), t = 1 : T$ and the reparameterization trick [26]. This ultimately leads to the empirical variational model training objective:

$$\max_\theta \widehat{\mathbb{E}}_{q_\theta} \Big[\sum_{t=1}^{T} \underbrace{\log \widehat{\mathcal{U}}_\theta(\boldsymbol{x}_t|\boldsymbol{z}_t)}_{\text{reconstruction}} - \underbrace{\mathbb{D}_{KL}(q_\theta(\boldsymbol{z}_t|\boldsymbol{x}_t, \boldsymbol{z}_{t-1}, \boldsymbol{a}_{t-1}) || \widehat{\mathcal{T}}_\theta(\boldsymbol{z}_t|\boldsymbol{z}_{t-1}, \boldsymbol{a}_{t-1}))}_{\text{forward model}} \Big]. \tag{7}$$

That is, we jointly train a belief representation q_θ and a Markovian dynamics model $\widehat{\mathcal{T}}$, which allows us to optimize Eq. 5 in our learned belief space. A number of recent works have considered similar models [44, 45, 30, 15, 19, 20]. We base our architectural choice on the recurrent state space model [19, 20], as it has shown strong performance in RL tasks from images. In principle, any on-policy RL algorithm can be used to train the policy using Eq. 6. In our setup, the RL objective is a differentiable function of the policy, model, and discriminator parameters. Based on this, we setup a K step value expansion objective [11, 7] given below, and use it for policy learning.

$$V^K_{\theta,\psi}(\boldsymbol{z}_t) = \mathbb{E}_{\pi_\psi, \widehat{\mathcal{T}}_\theta} \left[\sum_{\tau=t}^{t+K-1} \gamma^{\tau-t} \log D_\psi(\boldsymbol{z}^{\pi_\psi}_\tau, \boldsymbol{a}^{\pi_\psi}_\tau) + \gamma^K V_\psi(\boldsymbol{z}^{\pi_\psi}_{t+K}) \right] \tag{8}$$

Finally, we train the discriminator D_ψ using Eq. 5 with on-policy rollots from the model $\widehat{\mathcal{T}}$. Our full approach is outlined in Algorithm 1.

4.4 Zero-Shot Transfer to New Imitation Tasks

Our model-based approach is well suited to the problem of zero-shot transfer to new imitation learning tasks, i.e. transferring to a new task using a modest number of demonstrations and no additional samples collected in the environment.. In particular, we assume a set of source tasks $\{\mathcal{T}^i\}$, each with a buffer of expert demonstrations $\mathcal{B}^i_E$. Each source task corresponds to a different POMDP with different underlying rewards, but shared dynamics. The underlying state space may also change

Algorithm 2 Zero-Shot Transfer with V-MAIL

Require: Expert demos $\mathcal{B}_E^i$ for each source task, expert demos $\mathcal{B}_E$ for target task
Randomly initialize policy π_ψ, and discriminator D_ψ
Train Alg 1 on source tasks, yielding shared model $\{q_\theta, \widehat{\mathcal{T}}_\theta\}$ and aggregated replay buffer $\mathcal{B}_\pi$
for number of training iterations **do**
    `// Dynamics Fine-Tuning using Expert Trajectories`
    Update the variational model $\{q_\theta, \widehat{\mathcal{T}}_\theta\}$ using Equation 7 with data from $\mathcal{B}_E \cup \mathcal{B}_\pi$
    `// Adversarial Policy Learning`
    Update discriminator D_ψ and policy π_ψ with Equations 6 and 8.

across tasks, but the dynamics and observation model are shared across tasks. During training, the agent can interact with each source environment and collect additional data. At test time, we're introduced with a new target task $\mathcal{T}$ with corresponding expert demonstrations $\mathcal{B}_E$ and the goal is to obtain a policy that achieves high reward without additional interaction with the environment.

Our key observation is that we can optimize Eq. 6 under our model and still obtain an upper bound on policy sub-optimality via Eq. 4. Furthermore, the sub-optimality is bound by the accuracy of our model over the marginal state-action distribution of the target task expert. Specifically, we first train on all of the source tasks using Algorithm 1, training a single shared variational model across the tasks. By fine-tuning that model on data that includes the target task expert demonstrations our hope is that we can get an accurate model and thus a high-quality policy. Similarly to Algorithm 1, we then train a discriminator and policy for the target task using only model rollouts. This approach is outlined in Algorithm 2.

5 Experiments

In our experiments, we aim to answer several questions: (1) can V-MAIL successfully scale to environments with image observations, (2) how does V-MAIL compare to state of the art model-free imitation approaches, (3) can V-MAIL solve realistic manipulation tasks and environments with complex physical interactions, and (4) can V-MAIL enable zero-shot transfer to new tasks? All experiments were carried out on a single Titan RTX GPU using an internal cluster for about 1000 GPU hours.

5.1 Single-Task Experiments

Comparisons. To answer question (2), we choose to compare V-MAIL to model-free adversarial and non-adversarial imitation learning methods. For the former, we choose DAC [27] as a representative approach, which we equip with DrQ data augmentation for greater performance on vision-based tasks. For the latter, we consider SQIL [39], also equipped with DrQ training. We refer to each approach with data augmentation as DA-DAC and DA-SQIL respectively. Both of these methods are off-policy algorithms, which we expect to be considerably more sample efficient than on-policy methods like GAIL [22] and AIRL [14].

Environments and Demonstration Data. To answer the above questions, we consider the five visual control environments illustrated in Figure 2. We first evaluate our method on the visual Cheetah and visual Walker tasks from the DeepMind Control Suite [43]. Following SQIL [39] we also consider the classic Car Racing environment, which is difficult to solve even with ground-truth rewards. In addition, we benchmark our method on a custom D'Claw environment from the Robel

Figure 2: Illustration of the environments used in our experiments: Cheetah, Walker, Car Racing, D'Claw, and Baoding Balls. In all environments, the agent has access only to the RGB image frames as observations, except with additional access to proprioception in the Baoding Balls environment.

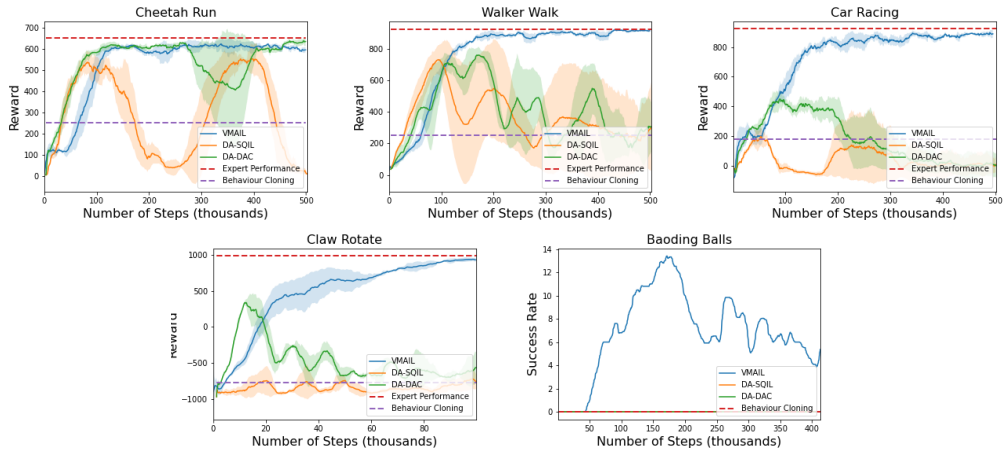

Figure 3: Learning curves showing ground truth reward versus number of environment steps for V-MAIL (ours), prior model-free imitation learning approaches, and behavior cloning on five visual imitation tasks. We find that V-MAIL consistently outperforms prior methods in terms of sample efficiency, final performance, and stability, particularly for the first four environments where V-MAIL reaches near-expert performance. In the most challenging visual Baoding Balls task, which is notably difficult even with ground-truth state, only V-MAIL is able to make some progress, but all methods struggle. Confidence intervals are shown with 1 SD over 3 runs.

suite [1], entirely from images without proprioception. This makes the task challenging due to a complex action dynamics, contact dynamics, and occlusions from the robot fingers. Our final environment is the Baoding balls task from Nagabandi et al. [33]. This is an extremely challenging task for policy learning, even in the state-based case. All tasks are from raw RGB images, while the Baoding balls task additionally includes robot proprioception. All methods receive access to use 10 expert demonstrations, with the exception of the Baoding environment, which uses 25 demonstrations. The demonstrations for the DeepMind Control and D'Claw tasks are generated using a policy trained with SAC [18], the expert data for the Car Racing environment is generated using Dreamer [20], and the demonstrations for the Baoding task is generated using PDDM [33] from low-dimensional states. Additional details on the experimental set-up are provided in the appendix.

Results. Experiment results are shown in Figure 3. To answer questions (1) and (2), we compare V-MAIL to DA-SQIL and DA-DAC on the Cheetah and Walker tasks. We find that V-MAIL efficiently and reliably solves both tasks; in contrast, the model-free methods initially outperform V-MAIL, but their performance has high variance across random seeds and exhibits significant instability. Such stability issues have also been observed by Swamy et al. [42], which provides some theoretical explanation in the case of SQIL and the suggestion of early stopping as a mitigation technique. In the case of DAC, the reasons for instability are less clear. Motivated by instability we observed in the critic loss for DA-DAC, we experimented with a number of mitigation strategies in an attempt to improve DA-DAC, including constraining the discriminator, varying the buffer and batch sizes, and separating the convolutional encoders of the discriminator and the actor/critic; however, these techniques didn't fully prevented the degradation in performance.

On the Car Racing environment, we find that DA-SQIL and DA-DAC can reach or outperform behavior cloning, but struggle to reach expert-level performance. In contrast, V-MAIL stably and reliably achieves near-expert performance in about 200k environment steps. Note that Reddy et al. [39] report expert-level performance on this task, but in an easier setting with double the number of expert demonstrations available (20 vs. 10). Given that tracks are randomly generated per episode demanding significant generalization, it is not surprising that the problem becomes considerably more difficult with only 10 demonstrations.

Finally, to answer question (3), we consider the D'Claw and Baoding Balls tasks. In the D'Claw environment, SQIL fails to make progress, while DA-DAC makes significant progress initially but quickly degrades. V-MAIL solves the task in less than 100k environment steps. In the most challenging visual Baoding Balls problem, involving a 26-dimensional control space, V-MAIL is the only algorithm to reach any success.

5.2 Transfer Experiments

Transfer Scenarios. To evaluate V-MAIL's ability to learn new imitation tasks in a zero-shot way (i.e. without any additional environment samples) we deploy Algorithm 2 on two domains: in a locomotion experiment we train on the Walker Stand and Walker Run (target speed greater than 8) tasks and and evaluate transfer to the Walker Walk (target speed between 2 and 4) task from the DeepMind Control suite. In a manipulation scenario, we use a set of custom D'Claw Screw tasks from the Robel suite [1]. We train our model on the 3-prong tasks with clockwise and counter-clockwise rotation, as well as the 4-prong task with counter-clockwise rotation and evaluate transfer to the 4-prong task with clockwise rotation.

Comparisons. To our knowledge, no prior work has considered this zero-shot transfer scenario previously. Thus, we devise several points of comparison. First, we compare to directly applying the policy learned in the most related source task to the target task. This tests whether the target task demands qualitatively distinct behavior. Second, we compare to an offline version of DAC, augmented with the CQL approach [29], where samples collected from the source task are used to update the policy, with the target task demonstrations used to learn the reward. Finally, we also compare to behavior cloning on the target task demonstrations (without leveraging any source task data), and an oracle that performs V-MAIL on the target task directly.

Results. Our results are shown in Table 1. Policy transfer performs poorly, suggesting that the target task indeed requires qualitatively different behaviour from the few training tasks available. Further, behavior cloning on the target demonstrations is not sufficient to learn the task. Offline DAC also shows poor performance. Finally, we see that V-MAIL almost matches the performance of the agent explicitly trained on task, indicating the learned model and the algorithm for training within that model can be used not just for efficient visual imitation learning, but also for zero-shot transfer to new tasks.

Method	Walker Walk	Claw Rotate
Offline DAC	8.8%	-0.7%
Behavior cloning	26.8%	8.3%
Policy transfer	21.3%	5.6%
V-MAIL (ours)	**92.7%**	**97.9%**
Target task IL (oracle)	98.2%	102.3%

Table 1: Performance on zero-shot transfer to a new imitation learning task as percent of expert return. Each method is provided with 10 demonstrations of the target task, and zero additional samples in the environment. V-MAIL can solve the target tasks within its learned model without any additional samples, while model-free transfer learning approaches fail.

6 Conclusion

In this work we presented V-MAIL, a model-based imitation learning algorithm that works from high-dimensional image observations. V-MAIL learns a model of the environment, which serves a strong supervision signal for visual representation learning, as well as allowing us to train an imitation learning algorithm on-policy, without sacrificing sample efficiency. V-MAIL achieves better asymptotic returns, is more stable, and matches the sample efficiency of off-policy model-free approaches. We also find that by training a policy using only model rollouts, our approach is a strong procedure for zero-shot transfer to novel imitation learning tasks.

Future Work. We believe this work opens the door for many potential developments. One direction is to use recent developments in variational models to train our procedure using only expert observations without access to expert actions, which is an even more realistic scenario. This setup is quite difficult for model-free approaches, since expert actions usually serve as a strong supervision. Another direction is to use on-policy model based rollouts to efficiently train other algorithms that inherently require on-policy data, such as multi-modal imitation [31, 21]. Finally, the experiments suggest that this algorithm is efficient enough to be applied to real robots, an interesting direction for future work.

Limitations. Although successful in domains with complex dynamics, crucially our approach relies on variational models with compact, single-level, latent state spaces. It is possible that this model class could not have the capacity to represent complex realistic scenes such as large-scale cluttered environments, cloth and deformable object dynamics, realistic city scenes or home environments, which would limit real world applications.

Negative Societal Impacts. We do not anticipate any negative societal impacts that are unique to this paper compared to prior imitation learning works.

References

[1] Michael Ahn, Henry Zhu, Kristian Hartikainen, Hugo Ponte, Abhishek Gupta, Sergey Levine, and Vikash Kumar. ROBEL: RObotics BEnchmarks for Learning with low-cost robots. In *Conference on Robot Learning (CoRL)*, 2019.

[2] Dario Amodei, Chris Olah, J. Steinhardt, Paul F. Christiano, John Schulman, and Dan Mané. Concrete problems in ai safety. *ArXiv*, abs/1606.06565, 2016.

[3] Nir Baram, Oron Anschel, and Shie Mannor. Model-based adversarial imitation learning. *Conference on Neural Information Processing Systems*, 2016.

[4] David M. Blei, A. Kucukelbir, and Jon D. McAuliffe. Variational inference: A review for statisticians. *Journal of the American Statistical Association*, 112:859 – 877, 2016.

[5] Lionel Blondé and Alexandros Kalousis. Sample-efficient imitation learning via generative adversarial nets. *AISTATS*, 2019.

[6] Lionel Blondé, Pablo Strasser, and Alexandros Kalousis. Lipschitzness is all you need to tame off-policy generative adversarial imitation learning, 2020.

[7] Jacob Buckman, Danijar Hafner, George Tucker, Eugene Brevdo, and Honglak Lee. Sample-efficient reinforcement learning with stochastic ensemble value expansion. *Conference on Neural Information Processing Systems*, 2019.

[8] Neha Das, Sarah Bechtle, Todor Davchev, Dinesh Jayaraman, Akshara Rai, and Franziska Meier. Model-based inverse reinforcement learning from visual demonstrations. *Conference on Robot Learning*, 2020.

[9] Tom Everitt and Marcus Hutter. Reward tampering problems and solutions in reinforcement learning: A causal influence diagram perspective. *ArXiv*, abs/1908.04734, 2019.

[10] Benjamin Eysenbach, Sergey Levine, and Ruslan Salakhutdinov. Replacing rewards with examples: Example-based policy search via recursive classification, 2021.

[11] Vladimir Feinberg, Alvin Wan, Ion Stoica, Michael I. Jordan, Joseph E. Gonzalez, and Sergey Levine. Model-based value estimation for efficient model-free reinforcement learning. *International Conference on Machine Learning*, 2018.

[12] Chelsea Finn, Paul Christiano, Pieter Abbeel, and Sergey Levine. A connection between generative adversarial networks, inverse reinforcement learning, and energy-based models. *ArXiv Preprint*, 2016.

[13] Chelsea Finn, Sergey Levine, and Pieter Abbeel. Guided cost learning: Deep inverse optimal control via policy optimization. In *International conference on machine learning*, pp. 49–58. PMLR, 2016.

[14] Justin Fu, Katie Luo, and Sergey Levine. Learning robust rewards with adversarial inverse reinforcement learning. *International Conference on Learning Representations*, 2018.

[15] Carles Gelada, Saurabh Kumar, Jacob Buckman, Ofir Nachum, and Marc G. Bellemare. Deepmdp: Learning continuous latent space models for representation learning. *International Conference on Machine Learning*, 2019.

[16] Seyed Kamyar Seyed Ghasemipour, Richard Zemel, and Shixiang Gu. A divergence minimization perspective on imitation learning methods. *Conference on Robot Learning*, 2019.

[17] Ian J. Goodfellow, Jean Pouget-Abadie, M. Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron C. Courville, and Yoshua Bengio. Generative adversarial nets. In *NIPS*, 2014.

[18] Tuomas Haarnoja, Aurick Zhou, Pieter Abbeel, and Sergey Levine. Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor. *International Conference on Machine Learning*, 2018.

[19] Danijar Hafner, Timothy Lillicrap, Ian Fischer, Ruben Villegas, David Ha, Honglak Lee, and James Davidson. Learning latent dynamics for planning from pixels. *International Conference on Machine Learning*, 2019.

[20] Danijar Hafner, Timothy Lillicrap, Jimmy Ba, and Mohammad Norouzi. Dream to control: Learning behaviors by latent imagination. *International Conference on Learning Representations*, 2020.

[21] Karol Hausman, Yevgen Chebotar, Stefan Schaal, Gaurav Sukhatme, and Joseph Lim. Multi-modal imitation learning from unstructured demonstrations using generative adversarial nets, 2017.

[22] Jonathan Ho and Stefano Ermon. Generative adversarial imitation learning. *Conference on Neural Information Processing Systems*, 2016.

[23] Maximilian Karl, Maximilian Soelch, Justin Bayer, and Patrick van der Smagt. Deep variational bayes filters: Unsupervised learning of state space models from raw data. *International Conference on Machine Learning*, 2017.

[24] Liyiming Ke, Matt Barnes, W. Sun, Gilwoo Lee, Sanjiban Choudhury, and S. Srinivasa. Imitation learning as f-divergence minimization. *ArXiv*, abs/1905.12888, 2019.

[25] Khimya Khetarpal, Matthew Riemer, I. Rish, and Doina Precup. Towards continual reinforcement learning: A review and perspectives. *ArXiv*, abs/2012.13490, 2020.

[26] Diederik P Kingma and Max Welling. Auto-encoding variational bayes, 2014.

[27] Ilya Kostrikov, Kumar Krishna Agrawal, Debidatta Dwibedi, Sergey Levine, and Jonathan Tompson. Discriminator-actor-critic: Addressing sample inefficiency and reward bias in adversarial imitation learning. *International Conference on Learning Representations*, 2019.

[28] Ilya Kostrikov, Ofir Nachum, and Jonathan Tompson. Imitation learning via off-policy distribution matching. *International Conference on Learning Representations*, 2020.

[29] Aviral Kumar, Aurick Zhou, George Tucker, and Sergey Levine. Conservative q-learning for offline reinforcement learning. *Conference on Neural Information Processing Systems*, 2020.

[30] Alex X. Lee, Anusha Nagabandi, Pieter Abbeel, and Sergey Levine. Stochastic latent actor-critic: Deep reinforcement learning with a latent variable model. *Conference on Neural Information Processing Systems*, 2020.

[31] Yunzhu Li, Jiaming Song, and Stefano Ermon. Infogail: Interpretable imitation learning from visual demonstrations. *Conference on Neural Information Processing Systems*, 2017.

[32] Ryan Lowe, Yi Wu, Aviv Tamar, Jean Harb, P. Abbeel, and Igor Mordatch. Multi-agent actor-critic for mixed cooperative-competitive environments. In *NIPS*, 2017.

[33] Anusha Nagabandi, Kurt Konolige, Sergey Levine, and Vikash Kumar. Deep dynamics models for learning dexterous manipulation. *Conference on Robot Learning*, 2019.

[34] Dean A Pomerleau. Alvinn: an autonomous land vehicle in a neural network. In *Proceedings of the 1st International Conference on Neural Information Processing Systems*, pp. 305–313, 1988.

[35] Rémy Portelas, Cédric Colas, Lilian Weng, Katja Hofmann, and Pierre-Yves Oudeyer. Automatic curriculum learning for deep rl: A short survey. *ArXiv*, abs/2003.04664, 2020.

[36] Rafael Rafailov, Tianhe Yu, Aravind Rajeswaran, and Chelsea Finn. Offline reinforcement learning from images with latent space models. *arXiv preprint arXiv:2012.11547*, 2020.

[37] Aravind Rajeswaran, Vikash Kumar, Abhishek Gupta, Giulia Vezzani, John Schulman, Emanuel Todorov, and Sergey Levine. Learning Complex Dexterous Manipulation with Deep Reinforcement Learning and Demonstrations. In *Proceedings of Robotics: Science and Systems (RSS)*, 2018.

[38] Aravind Rajeswaran, Igor Mordatch, and Vikash Kumar. A Game Theoretic Framework for Model-Based Reinforcement Learning. In *ICML*, 2020.

[39] Siddharth Reddy, Anca D. Dragan, and Sergey Levine. Sqil: Imitation learning via reinforcement learning with sparse rewards. *International Conference on Learning Representations*, 2020.

[40] Stephane Ross, Geoffrey J. Gordon, and J. Andrew Bagnell. A reduction of imitation learning and structured prediction to no-regret online learning. *AISTATS*, 2011.

[41] Jonathan Spencer, Sanjiban Choudhury, Arun Venkatraman, Brian Ziebart, and J. Andrew Bagnell. Feedback in imitation learning: The three regimes of covariate shift. *ArXiv Preprint*, 2021.

[42] Gokul Swamy, Sanjiban Choudhury, Zhiwei Steven Wu, and J. Andrew Bagnell. Of moments and matching: Trade-offs and treatments in imitation learning. 2021.

[43] Yuval Tassa, Yotam Doron, Alistair Muldal, Tom Erez, Yazhe Li, Diego de Las Casas, David Budden, Abbas Abdolmaleki, Josh Merel, Andrew Lefrancq, Timothy Lillicrap, and Martin Riedmiller. Deepmind control suite, 2018.

[44] Manuel Watter, Jost Tobias Springenberg, Joschka Boedecker, and Martin Riedmiller. Embed to control: A locally linear latent dynamics model for control from raw images, 2015.

[45] Marvin Zhang, Sharad Vikram, Laura Smith, Pieter Abbeel, Matthew J. Johnson, and Sergey Levine. Solar: Deep structured representations for model-based reinforcement learning. *International Conference on Machine Learning*, 2019.

[46] Brian D. Ziebart, Andrew L. Maas, J. Bagnell, and A. Dey. Maximum entropy inverse reinforcement learning. In *AAAI*, 2008.

Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper's contributions and scope? [Yes]
   (b) Did you describe the limitations of your work? [Yes] Limitations are discussed in the conclusion.
   (c) Did you discuss any potential negative societal impacts of your work? [Yes] This is addressed in the conclusion.
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes]
2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [Yes] The complete assumptions and full proofs are included as an Appendix with the supplemental materials.
   (b) Did you include complete proofs of all theoretical results? [Yes] The complete assumptions and full proofs are included as an Appendix with the supplemental materials.
3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] Our codebase is available with the supplemental materials.
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] Training details are available as an appendix with the supplemental materials.
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [Yes] Consult Figure 3.
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] Refer to Experiments section.
4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] We build our codebases on top of several publicly available developments, more details are included in the supplement materials.
   (b) Did you mention the license of the assets? [N/A]
   (c) Did you include any new assets either in the supplemental material or as a URL? [Yes] Our codebase is included with the supplement materials.
   (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? [N/A]
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [N/A]
5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A]

(b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A]

(c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A]