ADVERSARIAL STYLE TRANSFER FOR ROBUST POLICY OPTIMIZATION IN REINFORCEMENT LEARNING

Anonymous authors
Paper under double-blind review

ABSTRACT

This paper proposes an algorithm that aims to improve generalization for reinforcement learning agents by removing overfitting to confounding features. Our approach consists of a max-min game theoretic objective. A generator transfers the style of observation during reinforcement learning. An additional goal of the generator is to perturb the observation, which maximizes the agent's probability of taking a different action. In contrast, a policy network updates its parameters to minimize the effect of such perturbations, thus staying robust while maximizing the expected future reward. Based on this setup, we propose a practical deep reinforcement learning algorithm, Adversarial Robust Policy Optimization (ARPO), to find an optimal policy that generalizes to unseen environments. We evaluate our approach on visually enriched and diverse Procgen benchmarks. Empirically, we observed that our agent ARPO performs better in generalization and sample efficiency than a few state-of-the-art algorithms.

1 INTRODUCTION

The reinforcement learning (RL) environments often provide observation, which is a high-dimensional projection of the true state, complicating policy learning as the deep neural network model might mistakenly correlate reward with irrelevant information. Thus deep neural networks might overfit irrelevant features in the training data due to their high flexibility and the long-stretched time duration of the RL training process, which leads to poor generalization (Hardt et al., 2016; Zhang et al., 2018a; Cobbe et al., 2019; 2020; Zhang et al., 2018b; Machado et al., 2018; Gamrian & Goldberg, 2019). These irrelevant features (e.g., background color) usually do not impact the reward; thus, an optimal agent should avoid focusing on them during policy learning. Even worse, this might lead to incorrect state representations, which prevents deep RL agents from performing well even in slightly different environments. Thus, to learn a correct state representation, the agent needs to avoid those features that are not important for optimal policy learning.

In recent times, generalization in RL has been explored extensively. In zero-shot generalization framework (Zhang et al., 2018b; Song et al., 2020; Wang et al., 2019; Packer et al., 2018) the agent is trained on a finite training set of MDP levels and then evaluated on the full distribution of the MDP levels. The distribution of the MDP levels can be generated in various ways, including changing dynamics, exploit determinism, and adding irrelevant confounders to high-dimensional observation. An agent trained in these setups can overfit any of these factors, resulting in poor generalization performance. Many approaches have been proposed to address this challenges including various data augmentation approaches such as random cropping, adding jitter in image-based observation (Cobbe et al., 2019; Laskin et al., 2020a; Raileanu et al., 2020; Kostrikov et al., 2020; Laskin et al., 2020b),random noise injection (Igl et al., 2019), network randomization (Osband et al., 2018; Burda et al., 2018; Lee et al., 2020), and regularization (Cobbe et al., 2019; Kostrikov et al., 2020; Igl et al., 2019; Wang et al., 2020) have shown to improve generalization. The common theme of these approaches is to increase diversity in the training data so as the learned policy would better generalize. However, this perturbation is primarily done in isolation of the RL reward function, which might change an essential aspect of the observation, resulting in sub-optimal policy learning. Moreover, the random perturbation in various manipulations of observations such as cropping, blocking, or combining two random images from different environment levels might result in unrealistic observations that the agent will less likely observe during testing. Thus these techniques might work poorly in the setup where agents depend on realistic observation for policy learning. It is also de-

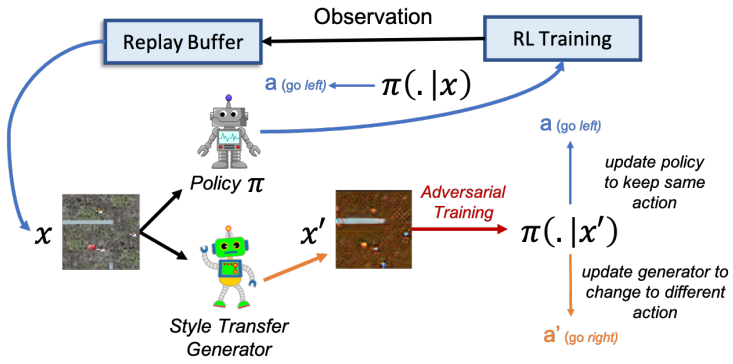


Figure 1: Overview of our approach. The method consists of a minimax game theoretic objective. It first applies a clustering approach to generate n group of clusters based on the different visual features in the observation. A generator is then used to style translate observation from one cluster to another while maximizing the change in action probabilities of the policy. In contrast, the policy network updates its policy parameters to minimize the translation effect while optimizing for the RL objective that maximizes the expected future reward.

sirable to train the agent with realistic observations, which helps it understand the environments' semantics. Otherwise, the agent might learn unexpected and unsafe behaviors while entirely focusing on maximizing rewards even by exploiting flaws in environments such as imperfect reward design.

This paper focuses on a particular form of generalization where the agent gets to observe a high-dimensional projection of the true state. In contrast, the latent state dynamics remain the same across all the MDP levels. This assumption has been shown to affect generalization (Song et al., 2020) in well studied benchmarks (Nichol et al., 2018) . It has been observed that the agent overfit the scoreboard or timer and sometimes achieves the best training performance even without looking at the other part of the observation. Consequently, this policy completely fails to generalize in test environments. The high-capacity model even can memorize the whole training environment, thus severely affecting the generalization (Zhang et al., 2018b).

This paper proposes a style transfer-based observation translation method that considers the observation's content and reward signal. In particular, a generator performs the style transfer while the policy tries to be robust toward such style changes. Note that, style transfer-based approach has been used to target generalization in Anonymous (2021) where the authors propose to train style transfer and reinforcement learning in isolation. In contrast, in this paper, we propose a unified learning approach where the style transfer is integrated into the reinforcement learning training. Thus the generator produces more effective translation targeted toward RL objective, making the RL policy more robust. The trajectory data from the agent's replay buffer is first clustered into different categories, and then observation is translated from one cluster's style to another cluster's style. Here the style is determined by the attribute commonality of observation features in a cluster. The agent should be robust toward changes of such features. Moreover, the translated trajectories correspond to those that possibly appear in testing environments, assisting the agent in adapting to unseen scenarios.

Figure 1 shows an overview of our method. Our approach consists of a max-min game theoretic objective where a generator network modifies the observation by style transferring it to maximize the agent's probability of taking a different action. In contrast, the policy network (agent) updates its parameters to minimize the effect of perturbation while maximizing the expected future reward. Based on this objective, we propose a practical deep reinforcement learning algorithm, Adversarial Robust Policy Optimization (ARPO), that aims to find an optimal policy by mitigating the observational overfitting and eventually generalizes to test environments.

We empirically show that our method performs better in generalization to test environments than state-of-the-art algorithms. We conduct experiments on visually enriched challenging Procgen (Cobbe et al., 2020) benchmarks with image observation and compare our proposed method with

other strong baselines standard PPO (Schulman et al., 2017), and data augmentation RAD (Laskin et al., 2020a). The experiments show that our algorithm outperforms the baselines in most of the Procgen environments both generalization and sample efficiency.

In summary, our contributions are listed as follows:

- We propose Adversarial Robust Policy Optimization (ARPO), a deep reinforcement learning algorithm to find an optimal policy that generalizes to test environments in a zero-shot generalization framework.
- We evaluate our approach on visually enriched, and diverse Procgen (Cobbe et al., 2020) benchmark in generalization settings.
- Empirically, we observed that our agent ARPO performs better generalization and sample efficiency performance compared to state-of-the-art algorithms: PPO (Schulman et al., 2017), and data augmentation technique (RAD) (Laskin et al., 2020a) on most of the Procgen environments.

2 Preliminaries and Problem Settings

Markov Decision Process (MDP) An MDP is denoted by $\mathcal{M} = (\mathcal{S}, \mathcal{A}, \mathcal{P}, r)$ where at every timestep t, from an state $s_t \in \mathcal{S}$, the agent takes an action a_t from a set of actions $\mathcal{A}$. The agent then receives a reward r_t and the environment and move to a new state $s_{t+1} \in \mathcal{S}$ based on the transition probability $P(s_{t+1}|s_t, a_t)$.

Reinforcement Learning. Reinforcement learning aims to learn a policy $\pi \in \Pi$ that maps state to actions. The policy's objective is to maximize cumulative reward in an MDP, where Π is the set of all possible policies. Thus, the policy which achieves the highest possible cumulative reward is the optimal policy $\pi^* \in \Pi$.

Generalization in Reinforcement Learning. In the zero-shot generalization framework (Song et al., 2020), we assume the existence of a distribution of levels $\mathcal{D}$ over an MDP and a fixed optimal policy π^* which can achieve maximal return over levels generated from the distribution $\mathcal{D}$. The levels may differ in observational variety, such as different background colors. In this setup, the agent has access to a fixed set of MDP levels during training the policy. The trained agent is then tested on the unseen levels to measure the generalization performance of the agent.

Style Transfer. The task of image-to-image translation is to change a particular aspect of a given image to another, such as red background to green background. Generative adversarial network (GAN)-based method has achieved tremendous success in this task (Kim et al., 2017; Isola et al., 2017; Zhu et al., 2017; Choi et al., 2018). Given training data from two domains, these models learn to style translate images from one domain to another. The domain is defined as a set of images sharing the same attribute value, such as similar background color and texture. The shared attributes in a domain are considered as the "style" of that domain. Many translation methods require paired images from two domains, which is not feasible in the reinforcement learning setup. The agent collects the data during policy learning, and annotating them in pairs is not feasible. Thus, we leverage unpaired image to image translation, which does not require a one-to-one mapping of annotated images from two domains.

In particular, we build upon the work of StarGAN (Choi et al., 2018) which is capable of learning mappings among multiple domains efficiently. The model takes in training data of multiple domains and learns the mappings between each pair of available domains using only a single generator. This method automatically captures special characteristics of one image domain and figures out how these characteristics could be translated into the other image collection, making it appealing in the reinforcement learning setup. However, the RL agent generates experience trajectory data which is not separated into domains. Thus, we further apply a clustering approach which first clusters the trajectory observation into domains, and then we train the generator, which style translates among those domains.

3 ADVERSARIAL ROBUST POLICY OPTIMIZATION (ARPO)

Our approach consists of a max-min game theoretic objective where a generator network modifies the observation by style transferring it to maximize the agent's probability of taking a different action. In contrast, the policy network (agent) updates its parameters to minimize the effect of perturbation while maximizing the expected future reward. Based on this objective, we propose a practical deep reinforcement learning algorithm, Adversarial Robust Policy Optimization (ARPO), to find an optimal policy that generalizes to test environments. We now discuss the details of the policy network and generator.

3.1 POLICY NETWORK

The objective of the policy network is two-fold: maximize the cumulative RL return during training and be robust to the perturbation on the observation imposed by the generator. Ideally, the action probability of the translated image should not change from the original image, as the translated observation is assumed to represent the same semantic as the original observation.

The reinforcement learning loss $\mathcal{L}_\pi$ can be optimized with various reinforcement learning mechanisms, such as policy gradient (optimization). However, we do not make any assumption the type of RL algorithms to use for optimizing $\mathcal{L}_\pi$; thus, any algorithms can be incorporated with our method. Here we discuss the policy optimization formulation, which is based on the proximal policy optimization (PPO) (Schulman et al., 2017) objective:

$$\mathcal{L}_\pi = -\mathbb{E}_t[\frac{\pi_\theta(a_t|s_t)}{\pi_{\theta_{old}}(a_t|s_t)}A_t] \tag{1}$$

$$A_t = -V(s_t) + r_t + \gamma r_{r+1} + ... + \gamma^{T-t+1} r_{T-1} + \gamma^{T-t} V(s_T). \tag{2}$$

where, π_θ is the current policy and $\pi_{\theta_{old}}$ is the old policy; A_t is estimated from the sampled trajectory by policy $\pi_{\theta_{old}}$ leveraging a value function estimator denoted as V. Here, both the policy π and value network V are represented as neural networks.

An additional objective of the policy is to participate in the adversarial game with the style transfer generator. Thus the final policy loss $\mathcal{L}_\theta$ is defined as follows:

$$\mathcal{L}_\theta = \mathcal{L}_\pi + \beta_1 KL[\pi_\theta(.|x_t), \pi_\theta(.|x'_t)] \tag{3}$$

The policy parameter θ is updated to minimize equation 3. For the observation x_t at timestep t, the KL-component measure the distortion in the action distribution of the policy π_θ due to the perturbation (x'_t). The hyperparameter β_1 determines the participation in an adversarial objective with the generator. By minimizing the KL-part, the policy becomes robust to the change in perturbation proposed by the generator.

3.2 GENERATOR NETWORK

It takes the observation x_t as input and outputs the style translated observation x'_t. The objective of this network is to change the agent's (policy network's) probability of taking a different action for the corresponding input observation. However, the content or semantic of the observations needs to be intact, and the only style of the images will differ.

The first step of this process is to curate a dataset with different style features such as background color and texture of objects present in the observation. We first use experience trajectory observation data from the environment and separate them into different classes based on visual features (Figure 2). The task of the generator is then to translate the images from one class images to another class images. In this case, the "style" is defined as the commonality among images in a single class. We now discuss details about how we separate the trajectory observation to get different clusters.

Clustering Trajectory Observation. The trajectory data is first clustered into n clusters. Then, we use the Gaussian Mixture Model (GMM) for clustering and ResNet (He et al., 2016) for feature extraction and dimension reduction. Firstly, a pre-trained (on ImageNet) ResNet model reduces an RGB image into a 1000 dimensional vector. This step extracts useful information from the raw image and reduces the dimension, allowing faster cluster training. Note that this process focuses

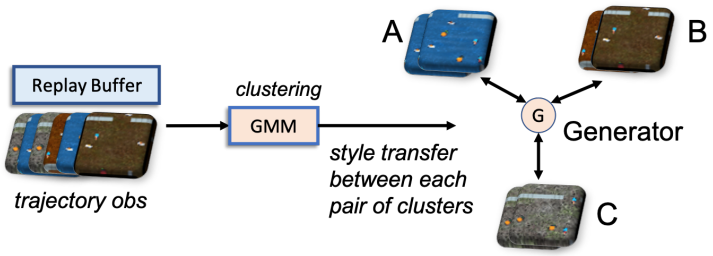


Figure 2: Overview of style transfer generator module. The experience trajectory observation data for the task environment are separated into different classes based on visual features using Gaussian Mixture Model (GMM) clustering algorithm. The task of the generator is then to translate the image from one class image to another classes images. In this case, the "style" is defined as the commonality among images in a single class. Given a new observation, it first infers into its (source) cluster using GMM, and then the generator translated it to (target) another cluster style. The target cluster is taken randomly from the rest of the cluster.

entirely on the visual aspect of the observation. After passing through the ResNet, the observation dataset is clustered using GMM.

Generator Training. Generator G tries to fool discriminator D in an adversarial setting by generating a realistic image represented by the true image distribution. We extend the generator's ability, and an additional objective of the generator is to fool the RL agent (policy network) by transforming the style of the original observation. For example, changing the background color to a different one does not change the semantic of the observation, but the image style would be different. Ideally, the action mapping of the policy needs to be the same on both the original and translated observation. However, a policy that focuses on the irrelevant background color will suffer from this translation, and thus its probability distribution deviates because of the style translation. This is defined as the KL-divergence $KL(\pi_\theta(.|x_t), \pi_\theta(.|x'_t))$, where x_t is the given observation and x'_t is the translated observation by the generator.

The generator tries to generate a style that eventually increases the KL quantity. On the other hand, the policy should learn to be robust toward such changes. The policy training described above addresses this and tries to minimize the KL-divergence due to the style transfer, which eventually allows robust policy learning and ultimately prevents the agent from overfitting irrelevant features from the high-dimensional observation.

We build on the generator on previous works (Choi et al., 2018; Zhu et al., 2017) which is a unified framework for a multi-domain image to image translation. The discriminator loss is

$$\mathcal{L}_D = -\mathcal{L}_{adv} + \lambda_{cls}\mathcal{L}^r_{cls}, \tag{4}$$

which consist of the adversarial loss $\mathcal{L}_{adv}$ and domain classification loss $\mathcal{L}^r_{cls}$. The discriminator detects a fake image generated by the generator G from the real image in the given class data.

On the other hand, the generator loss is

$$\mathcal{L}_G = \mathcal{L}_{adv} + \lambda_{cls}\mathcal{L}^f_{cls} + \lambda_{rec}\mathcal{L}_{rec} - \beta_2 KL(\pi_\theta(.|x_t), \pi_\theta(.|x'_t)) \tag{5}$$

which consists of image translation components and policy component which is the KL-part. From the translation side, the $\mathcal{L}_{adv}$ is adversarial loss with discriminator $\mathcal{L}^f_{cls}$ is the loss of detecting fake image. Finally, a cycle consistency loss (Choi et al., 2018; Zhu et al., 2017) $\mathcal{L}_{rec}$ is used which makes sure the translated input can be translated back to the original input, thus only changing the domain related part and not the semantic. Some more details of these losses can be found in the supplementary materials.

Our addition to the generator objective is the KL-part in equation 5 which tries to challenge the RL agent and fool its policy by providing a more challenging translation. However, the eventual goal of this adversarial game is to help the agent to be robust to any irreverent features in the observations. The hyperparameter β_2 control the participation in the adversarial objective of the generator network.

Now we discuss a practical RL algorithm based on the above objectives.

3.3 ARPO ALGORITHM

The training of the policy network and the generator network happen in an alternating way. First, the policy is trained on a batch of replay buffer trajectory observation, and then the generator parameters are updated based on the objectives discussed above. The more overall training progresses, the better the generator at translating observation, and the policy also becomes better and becomes robust to irrelevant style changes. For stable training, the input images data for the generator is kept fixed initially, and we apply the GMM cluster only at the beginning to generate different class images (distribution). The pseudocode of the algorithm is given in Algorithm 1.

Algorithm 1 Adversarial Robust Policy Optimization (ARPO)

```
Initialize parameter vectors for policy network and generator network
for each iteration do
    for each environment step do
        a_t ~ π_θ(a_t|x_t)
        x_{t+1} ~ P(x_{t+1}|x_t, a_t)
        r_t ~ R(x_t, a_t)
        D ← D ∪ {(x_t, a_t, r_t, x_{t+1})}
    end for
    for each observation x_t in D do
        x'_t ← Generator(x_t) // generate translated observation
        Compute L_π from data D using Equation 1, and 2 // update policy for RL objective
        Compute L_θ using Equation 3 // update policy with adversarial KL part
        Update generator by computing Equation 6, and 5
    end for
end for
```

4 EXPERIMENTS

In this section, we empirically analyze the effectiveness of our proposed method. We first discuss the experiment setup, including the details of the environment used. Then we analyze the results.

4.1 SETUP

Procgen Environment We evaluate our proposed agent ARPO on the challenging RL generalization benchmark Procgen (Cobbe et al., 2020). We allow the agent to train on only 200 levels of each environment, with the difficulty level set as *easy*. Then the agents are tested over more than 100K levels, full distribution. Thus, to better generalize to the test environment, the agent must master the skill and avoid overfitting to spurious features in the training environment. The observations are raw pixel images, and the environment varies drastically between levels; some snippets are given in Figure 3.

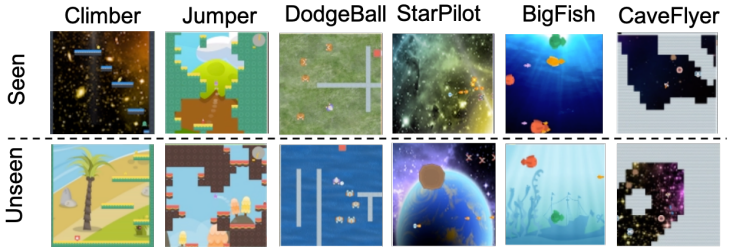


Figure 3: Some snippets of different Procgen environments (Cobbe et al., 2020). The training (seen) levels vary drastically from the testing (unseen) environment. The agent must master the skill without overfitting irrelevant non-generalizable aspects of the environment to perform better in unseen levels.

Baselines. We compare our algorithm with Proximal Policy Optimization (PPO), an on-policy algorithm motivated by how we can quickly optimize our policy while staying close to the current

policy. PPO performs effectively in many RL benchmarks, which includes the Procgen environments (Cobbe et al., 2020). Furthermore, we evaluated our method with a state-of-the-art data augmentation technique, RAD (Laskin et al., 2020a). RAD is a plug-and-play module that can be used with existing RL algorithms and shows effective empirical performance in complex RL benchmarks, including some Procgen environments. In particular, we evaluated *Cutout Color* augmentation technique which has shown better results in many Procgen environments compared to other augmentation techniques evaluated in Laskin et al. (2020a). This augmentation is applied on top of standard PPO.

Note that our ARPO algorithm can be easily plugged in with these data augmentation-based methods. However, in this paper, we evaluated how our ARPO agent performs even when no augmentation is used.

Implementation. We implemented our ARPO on the Ray RLlib framework (Liang et al., 2018) and used a CNN-based model for the policy network for these experiments. For Procgen we set the $\beta_1 = \beta_2 = 20$ (in equation 3, and 5). The generator's hyperparameters are set to $\lambda_{cls} = 1$, and $\lambda_{rec} = 10$. Number of cluster is set to 3. Details of model configurations and parameters are given in the supplementary materials.

4.2 Results

Generalization. The results in Figure 4 show the test results of ARPO and baselines PPO and RAD on visually enriched and diverse 16 Procgen environments with image observation. Overall, ARPO performs better in most environments where it consistently outperforms the baselines. We observe that, almost in half of the environments, our agent ARPO consistently outperforms both baselines. It also performs comparably in a few other environments. Note that in some environments such as Ninja, Plunder, Chaser, Heist, all the agents fail to obtain a reasonable training accuracy and thus perform poorly on generalization. The results are averaged over 3 seed runs.

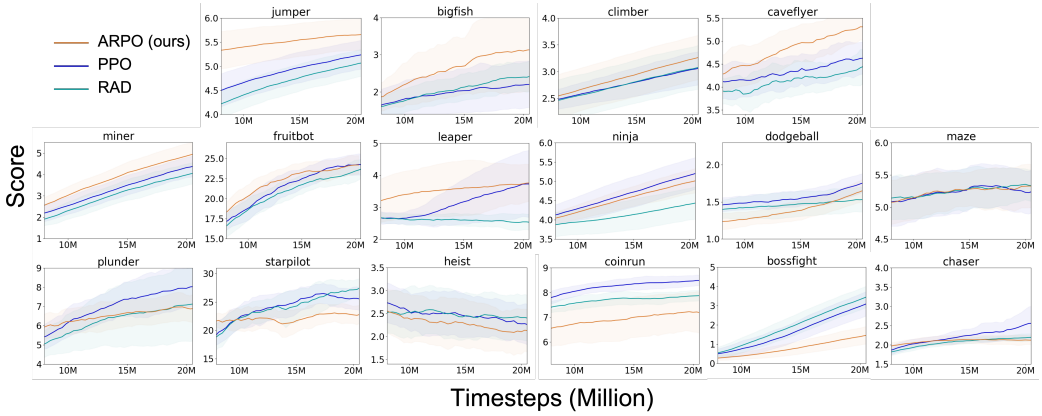


Figure 4: Generalization results. Test performance comparison on visually enriched and diverse Procgen environments with image observation. ARPO performs better in most environments where it consistently outperforms the baselines (one or both). The results are averaged over 3 seeds.

This result shows that our proposed agent ARPO achieves a strong performance and reduces the generalization gap compared to the tested baselines on generalization.

We further show how each agent achieves generalization during the entire timesteps. Consequently, we compute the maximum score achieved by each agent in the entire duration and take the average best score across 3 seed runs. The generalization results are computed by evaluating the trained agents on test levels (full distribution). The performance is computed by evaluating each agent for 10 random episode trials after a training interval of 10. All agents ran for 22 million timesteps for training.

Table 1 shows the results comparison for all the agents on Procgen environments. The results are averaged over 3 seeds. Similar to the previous discussion, we see that in most of the environments,

Table 1: Generalization results on Procgen environments. The results are the **mean of best test result** achieved by each agent in each environment and standard deviation across 3 seeds. ARPO achieves the best generalization results in most of the environments compared to PPO and RAD. ARPO (ours) results: **Bold & underscore** when better than PPO, and RAD, **Bold** when better than at least of the baselines (PPO or RAD).

Env	ARPO (ours)	PPO	RAD
jumper	**6.5** $\pm$ 0.06	6.49 $\pm$ 0.15	6.35 $\pm$ 0.04
bigfish	**4.18** $\pm$ 1.59	2.82 $\pm$ 0.75	3.22 $\pm$ 0.23
climber	**5.88** $\pm$ 0.42	5.22 $\pm$ 0.59	5.53 $\pm$ 0.55
caveflyer	**5.91** $\pm$ 0.08	5.5 $\pm$ 0.25	5.46 $\pm$ 0.34
miner	**7.2** $\pm$ 0.71	6.8 $\pm$ 0.17	6.21 $\pm$ 0.36
fruitbot	**27.04** $\pm$ 0.49	26.53 $\pm$ 0.57	26.99 $\pm$ 0.97
leaper	**4.19** $\pm$ 0.55	4.33 $\pm$ 0.97	3.22 $\pm$ 0.06
ninja	**6.49** $\pm$ 0.41	6.96 $\pm$ 0.5	5.82 $\pm$ 0.29
dodgeball	**2.32** $\pm$ 0.22	2.28 $\pm$ 0.05	1.85 $\pm$ 0.17
maze	**6.1** $\pm$ 0.14	6.23 $\pm$ 0.32	5.98 $\pm$ 0.04
plunder	**8.37** $\pm$ 0.95	9.39 $\pm$ 0.47	8.34 $\pm$ 2.19
starpilot	29.0 $\pm$ 3.04	31.13 $\pm$ 0.27	31.59 $\pm$ 1.28
heist	**3.93** $\pm$ 0.41	3.7 $\pm$ 0.35	3.75 $\pm$ 0.13
coinrun	7.67 $\pm$ 0.68	8.81 $\pm$ 0.12	8.25 $\pm$ 0.22
bossfight	4.08 $\pm$ 1.27	7.63 $\pm$ 0.6	7.99 $\pm$ 0.39
chaser	2.32 $\pm$ 0.09	3.11 $\pm$ 0.69	2.36 $\pm$ 0.04

our ARPO agents perform consistently better than the baselines. ARPO performs better than both the baselines in half of the environment, and in 12 out 16 environments, ARPO performs better than at least on baselines. This result shows that our agent consistently outperforms the baselines in the generalization results on Procgen benchmarks.

Sample Efficiency. We evaluate and compare our agent on the sample efficiency during training. This result shows how quickly our agent achieves a better score during training. Figure 5 shows the results of all the agents during training. In most environments, we see our agent ARPO consistently

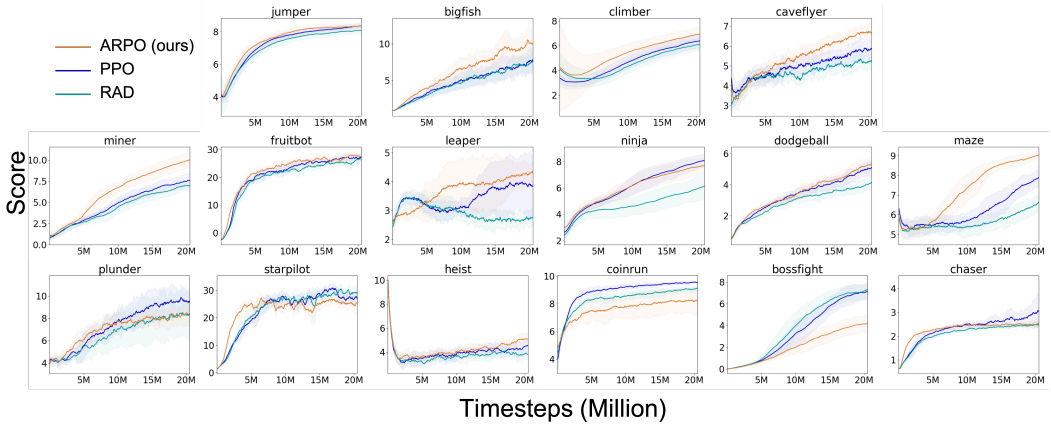
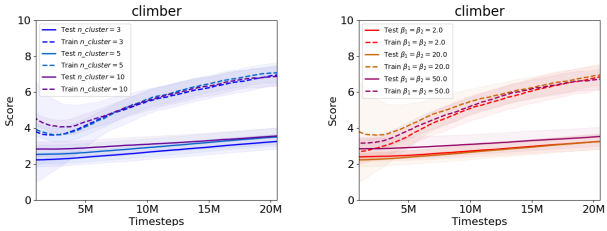


Figure 5: Sample efficiency results. Train performance (learning curve) comparison on visually enriched and diverse Procgen environments with image observation. Despite using perturbation on the observation, our agent ARPO consistently outperforms the baselines in many environments, thus achieving better sample efficiency during training. The results are averaged over 3 seeds.

perform better than the baselines PPO and RAD. These results show that despite optimizing for the generalization, our adversarial training helps the ARPO agent learn a robust policy which is also better during training.

Ablation Study. We conduct a study on how ARPO agent's performance varies due to its hyperparameters: (a) the number of clusters generated by the GMM model for generator training, and (b) β_1, β_2 which indicate the amount of participation of policy and generator in the adversarial objective.

Figure 6 shows the ablation results. We observe that our ARPO agent shows improvement in generalization (test) performance with the increase in number of cluster on Climber environment (Figure 6a). As the number of cluster increase, the generator has more option to choose for translation, and thus the policy might face a hard challenge and thus learn a more robust policy. In this paper, we report the ARPO agent's results on cluster $n_cluster = 3$. On the other hand, and ablation results on different β values are shown in Figure 6b. When β values are large the test performance goes up; however, training performance suffer a bit. In this paper, we report the results on $\beta_1 = \beta_2 = 20$, which shows a balance in train and test performance.



(a) (b)

Figure 6: Ablation results. The results are averaged over 3 seeds. **(a)** Our ARPO agent's results on different cluster numbers. It improves generalization (test) performance with the increase in cluster number in the Climber environment. **(b)** Our ARPO agent's results on different β values which determine participation on adversarial optimization.

5 Related Work

In recent time, many approaches have been proposed to address this challenges including various data augmentation approaches (Cobbe et al., 2019; Laskin et al., 2020a; Kostrikov et al., 2020; Raileanu et al., 2020; Kostrikov et al., 2020; Laskin et al., 2020b; Igl et al., 2019; Osband et al., 2018; Burda et al., 2018; Lee et al., 2020; Cobbe et al., 2019; Kostrikov et al., 2020; Wang et al., 2020; Zhang et al., 2021) have shown to improve generalization. The common theme of these approaches is to increase diversity in the training data; however, these perturbations are primarily conducted in isolation of the RL reward function, which might change crucial aspects of the observation, resulting in sub-optimal policy learning. Furthermore, state learning approaches (Higgins et al., 2017; Agarwal et al., 2021; Zhang et al., 2020) and auto-encoder based latent state learning (Lange et al., 2012; Lange & Riedmiller, 2010; Hafner et al., 2019) with reconstruction loss have been proposed. The sequential structure in RL (Agarwal et al., 2021) and behavioral similarity between states (Zhang et al., 2020) to learn invariant states have been leveraged to improve RL robustness and generalization. In contrast, we learn the invariant state by providing the RL agent with an additional variant of the same observation while retaining the reward structure using an adversarial max-min objective.

6 Conclusion

We proposed an algorithm, Adversarial Robust Policy Optimization (ARPO), to improve generalization for reinforcement learning agents by removing the effect of overfitting in high-dimensional observation space. Our method consists of a max-min game theoretic objective where a generator is used to transfer the style of high-dimensional observation (e.g., image), thus perturb original observation while maximizing the agent's probability of taking a different action for the corresponding input observation. In contrast, a policy network updates its parameters to minimize the effect of such translation, thus being robust to the perturbation while maximizing the expected future reward. We tested our approaches on Procgen benchmarks in generalization setup and confirm the effectiveness of our proposed algorithm. Empirical results show that our method generalizes better in unseen test environments than state-of-the-art algorithms: standard PPO and data augmentation technique RAD.

REFERENCES

Rishabh Agarwal, Marlos C. Machado, Pablo Samuel Castro, and Marc G. Bellemare. Contrastive behavioral similarity embeddings for generalization in reinforcement learning. In *International Conference on Learning Representations*, 2021.

Anonymous. Bootstrap state representations for better generalization in deep reinforcement learning. In *Under review*, 2021.

Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *International conference on machine learning*, pp. 214–223. PMLR, 2017.

Yuri Burda, Harrison Edwards, Amos Storkey, and Oleg Klimov. Exploration by random network distillation. *arXiv preprint arXiv:1810.12894*, 2018.

Yunjey Choi, Minje Choi, Munyoung Kim, Jung-Woo Ha, Sunghun Kim, and Jaegul Choo. Stargan: Unified generative adversarial networks for multi-domain image-to-image translation. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 8789–8797, 2018.

Karl Cobbe, Oleg Klimov, Chris Hesse, Taehoon Kim, and John Schulman. Quantifying generalization in reinforcement learning. In *International Conference on Machine Learning*, pp. 1282–1289. PMLR, 2019.

Karl Cobbe, Chris Hesse, Jacob Hilton, and John Schulman. Leveraging procedural generation to benchmark reinforcement learning. In *International conference on machine learning*, pp. 2048–2056. PMLR, 2020.

Lasse Espeholt, Hubert Soyer, Remi Munos, Karen Simonyan, Volodymir Mnih, Tom Ward, Yotam Doron, Vlad Firoiu, Tim Harley, Iain Dunning, et al. Impala: Scalable distributed deep-rl with importance weighted actor-learner architectures. *arXiv preprint arXiv:1802.01561*, 2018.

Shani Gamrian and Yoav Goldberg. Transfer learning for related reinforcement learning tasks via image-to-image translation. In *International Conference on Machine Learning*, pp. 2063–2072. PMLR, 2019.

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

Moritz Hardt, Ben Recht, and Yoram Singer. Train faster, generalize better: Stability of stochastic gradient descent. In *International Conference on Machine Learning*, pp. 1225–1234. PMLR, 2016.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770–778, 2016.

Irina Higgins, Arka Pal, Andrei A Rusu, Loic Matthey, Christopher P Burgess, Alexander Pritzel, Matthew Botvinick, Charles Blundell, and Alexander Lerchner. Darla: Improving zero-shot transfer in reinforcement learning. *arXiv preprint arXiv:1707.08475*, 2017.

Maximilian Igl, Kamil Ciosek, Yingzhen Li, Sebastian Tschiatschek, Cheng Zhang, Sam Devlin, and Katja Hofmann. Generalization in reinforcement learning with selective noise injection and information bottleneck. In *Advances in neural information processing systems*, pp. 13978–13990, 2019.

Phillip Isola, Jun-Yan Zhu, Tinghui Zhou, and Alexei A Efros. Image-to-image translation with conditional adversarial networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 1125–1134, 2017.

Taeksoo Kim, Moonsu Cha, Hyunsoo Kim, Jung Kwon Lee, and Jiwon Kim. Learning to discover cross-domain relations with generative adversarial networks. In *International Conference on Machine Learning*, pp. 1857–1865. PMLR, 2017.

Ilya Kostrikov, Denis Yarats, and Rob Fergus. Image augmentation is all you need: Regularizing deep reinforcement learning from pixels. *arXiv preprint arXiv:2004.13649*, 2020.

Sascha Lange and Martin Riedmiller. Deep auto-encoder neural networks in reinforcement learning. In *The 2010 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8. IEEE, 2010.

Sascha Lange, Martin Riedmiller, and Arne Voigtländer. Autonomous reinforcement learning on raw visual input data in a real world application. In *The 2012 international joint conference on neural networks (IJCNN)*, pp. 1–8. IEEE, 2012.

Michael Laskin, Kimin Lee, Adam Stooke, Lerrel Pinto, Pieter Abbeel, and Aravind Srinivas. Reinforcement learning with augmented data. In *Advances in neural information processing systems*, 2020a.

Michael Laskin, Aravind Srinivas, and Pieter Abbeel. Curl: Contrastive unsupervised representations for reinforcement learning. In *International Conference on Machine Learning*, pp. 5639–5650. PMLR, 2020b.

Kimin Lee, Kibok Lee, Jinwoo Shin, and Honglak Lee. Network randomization: A simple technique for generalization in deep reinforcement learning. In *International Conference on Learning Representations*, 2020. URL `https://openreview.net/forum?id=HJgcvJBFvB`.

Eric Liang, Richard Liaw, Robert Nishihara, Philipp Moritz, Roy Fox, Ken Goldberg, Joseph Gonzalez, Michael Jordan, and Ion Stoica. Rllib: Abstractions for distributed reinforcement learning. In *International Conference on Machine Learning*, pp. 3053–3062. PMLR, 2018.

Marlos C Machado, Marc G Bellemare, Erik Talvitie, Joel Veness, Matthew Hausknecht, and Michael Bowling. Revisiting the arcade learning environment: Evaluation protocols and open problems for general agents. *Journal of Artificial Intelligence Research*, 61:523–562, 2018.

Alex Nichol, Vicki Pfau, Christopher Hesse, Oleg Klimov, and John Schulman. Gotta learn fast: A new benchmark for generalization in rl. *arXiv preprint arXiv:1804.03720*, 2018.

Ian Osband, John Aslanides, and Albin Cassirer. Randomized prior functions for deep reinforcement learning. In *Advances in Neural Information Processing Systems*, pp. 8617–8629, 2018.

Charles Packer, Katelyn Gao, Jernej Kos, Philipp Krähenbühl, Vladlen Koltun, and Dawn Song. Assessing generalization in deep reinforcement learning. *arXiv preprint arXiv:1810.12282*, 2018.

Roberta Raileanu, Max Goldstein, Denis Yarats, Ilya Kostrikov, and Rob Fergus. Automatic data augmentation for generalization in deep reinforcement learning. *arXiv preprint arXiv:2006.12862*, 2020.

John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*, 2017.

Xingyou Song, Yiding Jiang, Stephen Tu, Yilun Du, and Behnam Neyshabur. Observational overfitting in reinforcement learning. In *International Conference on Learning Representations*, 2020. URL `https://openreview.net/forum?id=HJli2hNKDH`.

Huan Wang, Stephan Zheng, Caiming Xiong, and Richard Socher. On the generalization gap in reparameterizable reinforcement learning. In *International Conference on Machine Learning*, pp. 6648–6658. PMLR, 2019.

Kaixin Wang, Bingyi Kang, Jie Shao, and Jiashi Feng. Improving generalization in reinforcement learning with mixture regularization. *arXiv preprint arXiv:2010.10814*, 2020.

Amy Zhang, Nicolas Ballas, and Joelle Pineau. A dissection of overfitting and generalization in continuous reinforcement learning. *arXiv preprint arXiv:1806.07937*, 2018a.

Amy Zhang, Rowan McAllister, Roberto Calandra, Yarin Gal, and Sergey Levine. Learning invariant representations for reinforcement learning without reconstruction. *arXiv preprint arXiv:2006.10742*, 2020.

Amy Zhang, Rowan Thomas McAllister, Roberto Calandra, Yarin Gal, and Sergey Levine. Learning invariant representations for reinforcement learning without reconstruction. In *International Conference on Learning Representations*, 2021. URL https://openreview.net/forum?id=-2FCwDKRREu.

Chiyuan Zhang, Oriol Vinyals, Remi Munos, and Samy Bengio. A study on overfitting in deep reinforcement learning. *arXiv preprint arXiv:1804.06893*, 2018b.

Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A Efros. Unpaired image-to-image translation using cycle-consistent adversarial networks. In *Proceedings of the IEEE international conference on computer vision*, pp. 2223–2232, 2017.

A APPENDIX

Generator Training Loss.

The adversarial loss is calculated as the Wasserstein GAN (Arjovsky et al., 2017) objective with gradient penalty which is defined as

$$\mathcal{L}_{adv} = \mathbb{E}_x[D_{src}] - \mathbb{E}_{x,c}[D_{src}(G(x,c))] - \lambda_{gp}\mathbb{E}_{\hat{x}}[(||\nabla_{\hat{x}} D_{src}(\hat{x})|| - 1)^2], \tag{6}$$

where $\hat{x}$ is sampled uniformly along a straight line between a pair of real and generated fake images. We set the hyperparameter $\lambda_{gp} = 10$.

The classification loss of real image is defined as

$$\mathcal{L}^r_{cls} = \mathbb{E}_{x,c'}[-\log D_{cls}(c'|x)], \tag{7}$$

where $D_{cls}(c'|x)$ is the probability distribution over all clusteer labels. Similarly, the classification loss of fake generated image is defined as

$$\mathcal{L}^f_{cls} = \mathbb{E}_{x,c}[-\log D_{cls}(c|G(x,c))], \tag{8}$$

The reconstruction loss with the generator objective defined as

$$\mathcal{L}_{rec} = \mathbb{E}_{x,c,c'}[||x - G(G(x,c),c')||_1], \tag{9}$$

where we use the $L1$ norm.

A.1 ENVIRONMENT DETAILS

Procgen We conducted experiments on OpenAI Procgen Cobbe et al. (2020) benchmark, consisting of diverse procedurally-generated environments with different action sets. This environment has been used to measure how quickly (sample efficiency) a reinforcement learning agent learns generalizable skills. These environments greatly benefit from the use of procedural content generation, the algorithmic creation of a near-infinite supply of highly randomized content. The design principles consist of high diversity, tunable difficulty, shared action, shared observation space, and tunable dependence on exploration. Procedural generation logic directs the level layout and other game-specific details. Thus, to master any of these environments, agents must learn an effective policy across all environment variations. We use all 16 environments available in this benchmarks.

All environments use a discrete 15 dimensional action space which generates $64 \times 64 \times 3$ RGB image observations. Note that some environments may use no-op actions to accommodate a smaller subset of actions.

A.2 IMPLEMENTATION DETAILS

Procgen Experiments For experimenting on Procgen environments, we used RLlib Liang et al. (2018) to implement our ARPO, and baselines PPO and RAD cutour color algorithms. For all the agents' policy network (model), we use a CNN architecture used in IMPALA Espeholt et al. (2018). We use the same policy parameters for all agents for a fair comparison.

Policy learning hyperparameter settings for all the agents (ARPO, PPO, and RAD) are set same for fair comparison and detect the effect of our proposed method (max-min adversarial objective with perturbation network). These hyperparameters are given in Table 2.

Table 2: Hyperparameters for Procgen (RLlib) Experiments

Description	Hyperparameters
Discount factor of the MDP	$gamma : 0.999$
The GAE(lambda) parameter	$lambda : 0.95$
The default learning rate	$lr : 5.0e-4$
Number of epochs per train batch	$num_sgd_iter : 3$
Total SGD batch size	$sgd_minibatch_size : 2048$
Training batch size	$train_batch_size : 16384$
Initial coefficient for KL divergence	$kl_coeff : 0.0$
Target value for KL divergence	$kl_target : 0.01$
Coefficient of the value function loss	$vf_loss_coeff : 0.5$
Coefficient of the entropy regularizer	$entropy_coeff : 0.01$
PPO clip parameter	$clip_param : 0.2$
Clip param for the value function	$vf_clip_param : 0.2$
Clip the global amount	$grad_clip : 0.5$
Default preprocessors	$deepmind$
PyTorch Framework	$framework : torch$
Settings for Model	$custom_model : impala_cnn_torch$
Rollout Fragment	$rollout_fragment_length : 256$

A.3 COMPUTING DETAILS

We used the following machine configuration to run our experiments: 20 core-CPU with 256 GB of RAM, CPU Model Name: Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz, and a Nvidia A100 GPU.