A Survey on Generalization in Deep Reinforcement Learning

Ezgi Korkmaz
University College London
ezgikorkmazmail@gmail.com

Abstract

Reinforcement learning research obtained significant success and attention with the utilization of deep neural networks to solve problems in high dimensional state or action spaces. While deep reinforcement learning policies are currently being deployed in many different fields from medical applications to self driving vehicles, there are still ongoing questions the field is trying to answer on the generalization capabilities of deep reinforcement learning policies. In this paper, we will go over the fundamental reasons why deep reinforcement learning policies encounter overfitting problems that limit their generalization capabilities. Furthermore, we will formalize and unify the diverse solution approaches to increase generalization, and overcome overfitting in deep reinforcement learning policies. We believe our study can provide a compact systematic unified analysis for the current advancements in deep reinforcement learning, and help to construct robust deep neural policies with improved generalization abilities.

1 Introduction

The performance of reinforcement learning algorithms has been boosted with the utilization of deep neural networks as function approximators (Mnih et al., 2015). Currently, it is possible to learn deep reinforcement learning policies that can operate in large state and/or action space MDPs. This progress consequently resulted in building reasonable deep reinforcement learning policies that can play computer games with high dimensional state representations (e.g. Atari, StarCraft), solve complex robotics control tasks, design algorithms (Mankowitz et al., 2023; Fawzi et al., 2022), and play some of the most complicated board games (e.g. Chess, Go) (Schrittwieser et al., 2020). However, deep reinforcement learning algorithms also experience several problems caused by their overall generalization capabilities. Some studies demonstrated these problems via adversarial perturbations introduced to the state observations of the policy (Huang et al., 2017; Kos & Song, 2017; Korkmaz, 2022), several focused on exploring the fundamental issues with function approximation, estimation biases in the state-action value function (Hasselt et al., 2016), or with new architectural design ideas (Wang et al., 2016).

The fact that we are not able to explore the whole MDP for high dimensional state representation MDPs, even with deep neural networks as function approximators, is one of the root problems that limits generalization. On top this, some portion of the problems are directly caused by the utilization of deep neural networks and thereby the intrinsic problems inherited from their utilization (Goodfellow et al., 2015; Szegedy et al., 2014).

In this paper we will focus on generalization in deep reinforcement learning and underlying causes of the limitations deep reinforcement learning research currently faces. In particular, we will try to answer the following questions:

• What is the role of exploration in overfitting for deep reinforcement learning?
To answer these questions we go through research from several subfields on overfitting and generalization in reinforcement learning. We introduce a categorization of the different methods used to both achieve and test generalization, and use it to systematically summarize and consolidate the current body of research. We further describe the issue of value function overestimation, and the role of exploration in overfitting in reinforcement learning. Furthermore, we explain new emerging research areas that can potentially target these questions in the long run including meta-reinforcement learning and lifelong learning. We hope that our paper can provide a compact overview and unification of the current advancements and limitations in the field.

2 Preliminaries on Deep Reinforcement Learning

The aim in deep reinforcement learning is to learn a policy via interacting with an environment in a Markov Decision Process (MDP) that maximize expected cumulative discounted rewards. An MDP is represented by a tuple \( M = (S, A, P, r, \rho_0, \gamma) \), where \( S \) represents the state space, \( A \) represents the action space, \( r : S \times A \to \mathbb{R} \) is a reward function, \( P : S \times A \to \Delta(S) \) is a transition probability kernel, \( \rho_0 \) represents the initial state distribution, \( \gamma \) represents the discount factor. The objective in reinforcement learning is to learn a policy \( \pi : S \to \Delta(A) \) which maps states to probability distributions on actions in order to maximize the expected cumulative reward \( R = \mathbb{E} \sum_{t=0}^{T-1} \gamma^t r(s_t, a_t) \) where \( a_t \sim \pi(s_t), s_{t+1} \sim P(s_t, a_t) \). In \( Q \)-learning the goal is to learn the optimal state-action value function \(^8\text{Watkins (1989)}\)

\[
Q^*(s, a) = R(s, a) + \sum_{s' \in S} P(s'|s, a) \max_{a' \in A} Q^*(s', a').
\]

This is achieved via iterative Bellman update which updates \( Q(s_t, a_t) \) by

\[
Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha [R_{t+1} + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)].
\]

Thus, the optimal policy is determined by choosing the action \( a^*(s) = \arg \max_a Q(s, a) \) in state \( s \).

In high dimensional state space or action space MDPs the optimal policy is decided via a function-approximated state-action value function represented by a deep neural network. In a parallel line of algorithm families the policy itself is directly parametrized by \( \pi_\theta \), and the gradient estimator used in learning is

\[
g = \mathbb{E}_t [\nabla_\theta \log \pi_\theta(s_t, a_t)(Q(s_t, a_t) - \max_a Q(s_t, a))]\]

where \( Q(s_t, a_t) \) refers to the state-action value function at timestep \( t \).

3 How to Achieve Generalization?

To be able to categorize different paths to achieve generalization first we will provide a definition meant to capture the behavior of a generic reinforcement learning algorithm.

Definition 3.1. A reinforcement learning training algorithm \( \mathcal{A} \) learns a policy \( \pi \) by interacting with an MDP \( \mathcal{M} \). We divide up the execution of \( \mathcal{A} \) into discrete time steps as follows. At each time \( t \), the algorithm chooses a state \( s_t \), takes an action \( a_t \), observes a transition to state \( s'_t \) with corresponding reward \( r_t = r(s_t, a_t, s'_t) \). We define the history of algorithm \( \mathcal{A} \) in MDP \( \mathcal{M} \) to be the sequence \( H_t = (s_0, a_0, s'_0, r_0), \ldots, (s_t, a_t, s'_t, r_t) \) of all the transitions observed by the algorithm so far. We require that state and action \((s_t, a_t)\) chosen at time \( t \) are a function only of \( H_{t-1} \), i.e., the transitions observed so far by \( \mathcal{A} \). At time \( t = T \), the algorithm stops and outputs a policy \( \pi \).

\(^8\text{DeepMind Control Suite}\)
Intuitively, a reinforcement learning algorithm performs a sequence of queries \((s_t, a_t)\) to the MDP, and observes the resulting state transitions and rewards. In order to be as generic as possible, the definition makes no assumptions about how the algorithm chooses the sequence of queries. Notably, if taking action \(a_t\) in state \(s_t\) leads to a transition to state \(s'_t\), there is no requirement that \(s_{t+1} = s'_t\). Indeed, the only assumption is that \((s_{t+1}, a_{t+1})\) depends only on \(H_t\), the history of transitions observed so far. This allows the definition to capture deep reinforcement learning algorithms, which may choose to query states and actions in a complex way based on previously observed state transitions. Based on this definition of generic reinforcement learning algorithm, we will now further define the different techniques proposed to achieve generalization.

**Definition 3.2.** Let \(A\) be a training algorithm that takes as input an MDP and outputs a policy. Given an MDP \(M = (S, A, P, r, \rho_0, \gamma)\), a rewards transforming generalization method \(G_R\) is given by a sequence of functions \(F_t : (S \times A \times S \times \mathbb{R})^t \rightarrow \mathbb{R}\). The method attempts to achieve generalization by running \(A\) on MDP \(M\), but modifying the rewards at each time \(t\) to be \(\tilde{r}_t(s_t, a_t, s'_t) = F_{t-1}(H_{t-1})\), where \(H_{t-1}\) is the history of algorithm \(A\) when running with the perturbed rewards.

In summary, a rewards transforming generalization methods simply runs the original algorithm, but modifies the observed rewards. Similarly, we define two additional generalization methods which run the original algorithm while modifying states and transition probabilities respectively.

**Definition 3.3.** Let \(A\) be a training algorithm that takes as input an MDP and outputs a policy. Given an MDP \(M = (S, A, P, r, \rho_0, \gamma)\), a state transforming generalization method \(G_S\) is given by a sequence of functions \(F_t : (S \times A \times S \times \mathbb{R})^t \times S \rightarrow S\). The method attempts to achieve generalization by running \(A\) on MDP \(M\), but modifying the state chosen at time \(t\) to be \(\tilde{s}_t = F_{t-1}(H_{t-1}, s_t)\), where \(H_{t-1}\) is the history of algorithm \(A\) when running with the perturbed states.

**Definition 3.4.** Let \(A\) be a training algorithm that takes as input an MDP and outputs a policy. Given an MDP \(M = (S, A, P, r, \rho_0, \gamma)\), a transition probability transforming generalization method \(G_T\) is given by a sequence of functions \(F_t : (S \times A \times S \times \mathbb{R})^t \times (S \times A) \rightarrow \mathbb{R}\). The method attempts to achieve generalization by running \(A\) on MDP \(M\), but modifying the transition probabilities at time \(t\) to be \(\tilde{P}(s_t, a_t, s'_t) = F_{t-1}(H_{t-1}, s_t, a_t, s'_t)\), where \(H_{t-1}\) is the history of algorithm \(A\) when running with the perturbed transition probabilities.

The last type of generalization method we define is based on directly modifying the way in which the training algorithm chooses the state and action pair for the next time step. While this definition is broad enough to capture very complex changes to the training algorithm, in practice the choice of modification generally has a simple description.

**Definition 3.5.** Let \(A\) be a training algorithm that takes as input an MDP and outputs a policy. Given an MDP \(M = (S, A, P, r, \rho_0, \gamma)\), a policy transforming generalization method \(G_P\) is given by a sequence of functions \(F_t : (S \times A \times S \times \mathbb{R})^t \rightarrow S \times A\). The method attempts to achieve generalization by running \(A\) on MDP \(M\), but modifying the policy by which \(A\) chooses the next state and action to be \((\tilde{s}_t, \tilde{a}_t) = F_{t-1}(H_{t-1})\), where \(H_{t-1}\) is the history of algorithm \(A\) when running with the perturbed policy.

All the definitions so far categorize methods to modify training algorithms in order to achieve generalization. However, many such methods for modifying training algorithms have a corresponding method which can be used to test the generalization capabilities of a trained policy. Our final definition captures this correspondence.

**Definition 3.6.** Let \(\pi\) be a trained policy for an MDP \(M\). Let \(F_t\) be a sequence of functions corresponding to a generalization method from one of the previous definitions. The generalization testing method of \(F_t\) is given by executing the policy \(\pi\) in \(M\), but in each time step applying the modification \(F_t\) where the history \(H_t\) is given by the transitions executed by \(\pi\) so far. When both a generalization method and a generalization testing method are used concurrently, we will use subscripts to denote the generalization method and superscripts to denote the testing method. For instance, \(G_S^{\pi}\) corresponds to training with a state transforming method, and testing with a policy transforming method.

### 4 Roots of Overestimation in Deep Reinforcement Learning

Many reinforcement learning algorithms compute estimates for the state-action values in an MDP. Because these estimates are usually based on a stochastic interaction with the MDP, computing
Table 1: Environment and algorithm details for different exploration strategies for generalization.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Proposed Method</th>
<th>Environment</th>
<th>Reinforcement Learning Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bellemare et al. (2016)</td>
<td>Count-based</td>
<td>ALE</td>
<td>A3C and DQN</td>
</tr>
<tr>
<td>Osband et al. (2016b)</td>
<td>RLSVI</td>
<td>Tetris Tabular</td>
<td>Q-learning</td>
</tr>
<tr>
<td>Osband et al. (2016a)</td>
<td>Bootstrapped DQN</td>
<td>ALE</td>
<td>DQN</td>
</tr>
<tr>
<td>Houthooft et al. (2017)</td>
<td>VIME</td>
<td>DeepMind Control Suite</td>
<td>TRPO</td>
</tr>
<tr>
<td>Fortunato et al. (2018)</td>
<td>NoisyNet</td>
<td>ALE</td>
<td>A3C and DQN</td>
</tr>
<tr>
<td>Lee et al. (2021)</td>
<td>SUNRISE</td>
<td>DCS and Atari</td>
<td>Soft Actor-Critic and Rainbow DQN</td>
</tr>
</tbody>
</table>

Accurate estimates that correctly generalize to further interactions is one of the most fundamental tasks in reinforcement learning. A major challenge in this area has been the tendency of many classes of reinforcement learning algorithms to consistently overestimate state-action values. Initially, the overestimation bias for Q-learning is discussed and theoretically justified by Thrun & Schwartz (1993) as a byproduct of using function approximators for state-action value estimates. Following this initial discussion, it has been shown that several parts of the deep reinforcement learning process can cause overestimation bias. Learning overestimated state-action values can be caused by statistical bias of utilizing a single max operator (van Hasselt, 2010), coupling between value function and the optimal policy (Kakade & Fergus, 2021; Cobbe et al., 2021), or caused by the accumulated function approximation error (Boyan & Moore, 1994).

Several methods have been proposed to target overestimation bias for value iteration algorithms. In particular, to solve this overestimation bias introduced by the max operator (van Hasselt, 2010) proposed to utilize a double estimator for the state-action value estimates. Later, the authors also created a version of this algorithm that can solve high-dimensional state space problems (Hasselt et al., 2016). Some of the work on this line of research targeting overestimation bias for value iteration algorithms is based on simply averaging the state-action values with previously learned state-action value estimates during training time (Anschel et al., 2017).

While overestimation bias was demonstrated to be a problem and discussed over a long period of time (Thrun & Schwartz, 1993; van Hasselt, 2010), recent studies also further demonstrated that actor-critic algorithms also suffer from this issue (Fujimoto et al., 2018).

5 The Role of Exploration in Overfitting

The fundamental trade-off of exploration vs exploitation is the dilemma that the agent can try to take actions to move towards more unexplored states by sacrificing the current immediate rewards. While there is a significant body of studies on provably efficient exploration strategies, the results from these studies do not necessarily directly transfer to the high-dimensional state or action MDPs. The most prominent indication of this is that, even though it is possible to use deep neural networks as function approximators for large state spaces, the agent will simply not be able to explore the full state space. The fact that the agent is able to only explore a portion of the state space simply creates a bias in the learnt value function (Baird, 1995).

In this section, we will go through several exploration strategies in deep reinforcement learning and how they affect policy overfitting. A quite simple version of this is based on adding noise in action selection during training e.g. ε-greedy exploration. Note that this is an example of a policy transforming generalization method \( G_\epsilon \) in Definition 3.5 in Section 3. Yet it has been proven that to explore the state space these algorithms may take exponentially long (Kakade, 2003). Several others focused on randomizing different components of the reinforcement learning training algorithms. In particular, Osband et al. (2016b) proposes the randomized least-squared value iteration algorithm to explore more efficiently in order to increase generalization in reinforcement learning for linearly parametrized value functions. This is achieved by simply adding Gaussian noise as a function of state visitation frequencies to the training dataset. Later, the authors also propose the bootstrapped DQN algorithm (i.e. adding temporally correlated noise) to increase generalization with non-linear function approximation (Osband et al., 2016a).

Houthooft et al. (2017) proposed an exploration technique centered around maximizing the information gain on the agent’s belief of the environment dynamics. In practice, the authors use Bayesian neural networks for effectively exploring high-dimensional action space MDPs. Following this line of work on increasing efficiency during exploration, Fortunato et al. (2018) proposes to add parametric
Table 2: Environment and algorithm details for data augmentation techniques for state observation generalization. All of the studies in this section focuses on state transformation methods $G_S$ defined in Section 3.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Proposed Method</th>
<th>Environment</th>
<th>Reinforcement Learning Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yarats et al. 2021</td>
<td>DrQ</td>
<td>DeepMind Control Suite, ALE</td>
<td>DQN</td>
</tr>
<tr>
<td>Laskin et al. 2020b</td>
<td>CuRL</td>
<td>DeepMind Control Suite, ALE</td>
<td>Soft Actor Critic and DQN</td>
</tr>
<tr>
<td>Laskin et al. 2020a</td>
<td>RAD</td>
<td>DeepMind Control Suite, ProcGen</td>
<td>Soft Actor Critic and PPO</td>
</tr>
<tr>
<td>Wang et al. 2020</td>
<td>Mixreg</td>
<td>ProcGen</td>
<td>DQN and PPO</td>
</tr>
</tbody>
</table>

...noise to the deep reinforcement learning policy weights in high dimensional state MDPs. While several methods focused on ensemble state-action value function learning (Osband et al., 2016a), [Lee et al., 2021] proposed reweighting target Q-values from an ensemble of policies (i.e. weighted Bellman backups) combined with highest upper-confidence bound action selection. Another line of research in exploration strategies focused on *count-based methods* that use the direct count of state visitations. In this line of work, [Bellemare et al., 2016] tried to lay out the relationship between count based methods and intrinsic motivation, and used count-based methods for high dimensional state MDPs (i.e. Arcade Learning Environment). Yet it is worthwhile to note that most of the current deep reinforcement learning algorithms use very simple exploration techniques such as $\epsilon$-greedy which is based on taking the action maximizing the state-action value function with probability $1 - \epsilon$ and taking a random action with probability $\epsilon$ (Mnih et al., 2015; Hasselt et al., 2016; Wang et al., 2016; Hamrick et al., 2020; Kapturowski et al., 2023).

It is possible to argue that the fact that the deep reinforcement learning policy obtained higher score with the same number of samples by a particular type of training method $A$ compared to method $B$ is by itself evidence that the technique $A$ leads to more generalized policies. Even though the agent is trained and tested in the same environment, the explored states during training time are not exactly the same states visited during test time. The fact that the policy trained with technique $A$ obtains a higher score at the end of episode is sole evidence that the agent trained with $A$ was able to visit further states in the MDP and thus succeed in them. Yet, throughout the paper we will discuss different notions of generalization investigated in different subfields of reinforcement learning research. While exploration vs exploitation stands out as one of the main problems in reinforcement learning policy performance most of the work conducted in this section still is not able to obtain policies that perform as well as those in the studies described in Section 6.

### 6 Regularization

In this section we will focus on different regularization techniques employed to increase generalization in deep reinforcement learning policies. We will go through these works by categorizing under data augmentation, adversarial training, and direct function regularization. Under each category we will connect these different line of approaches to increase generalization in deep reinforcement learning to the settings we defined in Section 3.

#### 6.1 Data Augmentation

Several studies focus on diversifying the observations of the deep reinforcement learning policy to increase generalization capabilities. A line of research in this regard focused on simply employing versions of data augmentation techniques (Laskin et al., 2020a,b; Yarats et al., 2021) for high dimensional state representation environments. In particular, these studies involve simple techniques such as cropping, rotating or shifting the state observations during training time. While this line of work got considerable attention, a quite recent study (Agarwal et al., 2021b) demonstrated that when the number of random seeds is increased to one hundred the relative performance achieved and reported in the original papers of (Laskin et al., 2020b; Yarats et al., 2021) on data augmentation training in deep reinforcement learning decreases to a level that is significant to mention.

While some of the work on this line of research simply focuses on using a set of data augmentation methods (Laskin et al., 2020a,b; Yarats et al., 2021), other work focuses on proposing new environments to train in (Cobbe et al., 2020). The studies on designing new environments to train deep reinforcement learning policies basically aim to provide high variation in the observed environment...
Table 3: Environment and algorithm details for different direct function regularization strategies for trying to overcome overfitting problems in reinforcement learning. Note that most of the methods based on direct function regularization are a form of policy perturbation method $G_{\pi}$ to overcome overfitting as described in Section 3.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Proposed Method</th>
<th>Environment</th>
<th>Reinforcement Learning Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Igl et al. (2019)</td>
<td>SNI and IBAC</td>
<td>GridWorld and CoinRun</td>
<td>Proximal Policy Optimization</td>
</tr>
<tr>
<td>Vieillard et al. 2020b</td>
<td>Munchausen RL</td>
<td>Atari</td>
<td>DQN and IQN</td>
</tr>
<tr>
<td>Lee et al. 2020</td>
<td>Network Randomization</td>
<td>2D CoinRun and 3D DeepMind Lab</td>
<td>Proximal Policy Optimization</td>
</tr>
<tr>
<td>Amit et al. 2020</td>
<td>Discount Regularization</td>
<td>GridWorld and Mujoco</td>
<td>Twin Delayed DDPG (TD3)</td>
</tr>
<tr>
<td>Agarwal et al. 2021</td>
<td>PSM</td>
<td>DDMC and Rectangle Game</td>
<td>DQ</td>
</tr>
<tr>
<td>Lau et al. 2021</td>
<td>BN and dropout and $L_2/L_1$</td>
<td>Mujoco</td>
<td>PPO, TRPO, SAC, A2C</td>
</tr>
</tbody>
</table>

such as changing background colors and changing object shapes in ways that are meaningful in the game, in order to increase test time generalization.

Within this category some work focuses on producing more observations by simply blending in (e.g. creating a mixture state from multiple different observations) several observations to increase generalization (Wang et al., 2020). While most of the studies trying to increase generalization by data augmentation techniques are primarily conducted in the DeepMind Control Suite or the Arcade Learning Environment (ALE) (Bellemare et al., 2013), some small fraction of these studies (Wang et al., 2020) are conducted in relatively recently designed training environments like ProcGen (Cobbe et al., 2020). Cobbe et al. (2019) focuses on decoupling the training and testing set for reinforcement learning via simply proposing a new game environment CoinRun.

6.2 Direct Function Regularization

While some of the work we have discussed so far focuses on regularizing the data (i.e. state observations) as in Section 6.1 some focuses on directly regularizing the function learned with the intention of simulating techniques from deep neural network regularization like batch normalization and dropout (Igl et al., 2019). While some studies have attempted to simulate these known techniques in reinforcement learning, some focus on directly applying them to overcome overfitting. In this line of research, Liu et al. (2021) proposes to use known techniques from deep neural network regularization to apply in continuous control deep reinforcement learning training. In particular, these techniques are batch normalization (BN) (Ioffe & Szegedy, 2015), weight clipping, dropout, entropy and $L_2/L_1$ weight regularization.

Lee et al. (2020) proposes to utilize a random network to randomize the input observations to increase generalization skills of deep reinforcement learning policies, and tests the proposal in 2D CoinRun game proposed by Cobbe et al. (2019) and 3D DeepMind Lab. In particular, the authors basically introduce a random convolutional layer to perturb the state observations. Hence, this study is also a clear example of a state transformation generalization method $G_S$ described in Definition 3.3. While this is another example of random state perturbation methods we will further explain in Section 6.3 the worst-case perturbation methods to target generalization in reinforcement learning policies.

Some work employs contrastive representation learning to learn deep reinforcement learning policies from state observations that are close to each other (Agarwal et al., 2021a). The authors of this study leverage the temporal aspect of reinforcement learning and propose a policy similarity metric. The main goal of the paper is to lay out the sequential structure and utilize representation learning to learn generalizable abstractions from state representations. One drawback of this study is that most of the experimental study is conducted in a non-baseline environment (Rectangle game). Even though the authors show surprising results for this particular game, it is not clear how the proposed method would work for high dimensional state representation MDPs such as the Arcade Learning Environment.

Malik et al. (2021) studies query complexity of reinforcement learning policies that can generalize to multiple environments. The authors of this study focus on an example of the transition probability transformation setting $G_P$ in Definition 3.4 and the reward function transformation setting $G_R$ in Definition 3.2.

1 Low dimensional setting of Mujoco is used for this study.
2 Rectangle game is a simple video game with only two actions, "Right" and "Jump". The game has black background and two rectangles where the goal of the game is to avoid white obstacles and reach to the right side of the screen. Agarwal et al. (2021a) is the only paper we encountered experimenting with this particular game.
Table 4: Environment and algorithm details for adversarial policy regularization and attack techniques in deep reinforcement learning. Note that most of the methods based on adversarial policy regularzation are a form of state observation perturbation method $G^S$ as described in Definition 3.6.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Proposed Method</th>
<th>Environment</th>
<th>Reinforcement Learning Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huang et al. (2017)</td>
<td>FGSM</td>
<td>ALE</td>
<td>DQN, TRPO, A3C</td>
</tr>
<tr>
<td>Kos &amp; Song (2017)</td>
<td>FGSM</td>
<td>ALE</td>
<td>DQN and IQN</td>
</tr>
<tr>
<td>Lan et al. (2017)</td>
<td>Strategically-Timed Attack</td>
<td>ALE</td>
<td>A3C and DQN</td>
</tr>
<tr>
<td>Gleave et al. (2020)</td>
<td>Adversarial Policies</td>
<td>Mujoco</td>
<td>Proximal Policy Optimization</td>
</tr>
<tr>
<td>Huan et al. (2020)</td>
<td>SA-DQN</td>
<td>ALE and $L_{\text{Mujoco}}$</td>
<td>DDQN and PPO</td>
</tr>
<tr>
<td>Korkmaz (2020)</td>
<td>KMAP and HMAP</td>
<td>ALE</td>
<td>DDQN</td>
</tr>
<tr>
<td>Korkmaz (2022)</td>
<td>Adversarial Framework</td>
<td>ALE</td>
<td>DDQN and A3C</td>
</tr>
<tr>
<td>Korkmaz (2023)</td>
<td>Natural Attacks</td>
<td>ALE</td>
<td>DDQN and A3C</td>
</tr>
<tr>
<td>Korkmaz &amp; Brown-Cohen (2023)</td>
<td>Adversarial Detection</td>
<td>ALE</td>
<td>DDQN</td>
</tr>
</tbody>
</table>

Another line of study in direct function generalization investigates the relationship between reduced discount factor and adding an $\ell_2$-regularization term to the loss function (weight decay) (Amit et al., 2020). The authors in this work demonstrate the explicit connection between reducing the discount factor and adding an $\ell_2$-regularizer to the value function for temporal difference learning. In particular, this study demonstrates that adding an $\ell_2$-regularization term to the loss function is equal to training with a lower discount term, which the authors refer to as discount regularization. The results of this study however are based on experiments from tabular reinforcement learning, and the low dimensional setting of the Mujoco environment.

On the reward transformation for generalization setting $G_R$ defined in Definition 3.2, Vieillard et al. (2020b) adds the scaled log policy to the current rewards. To overcome overfitting some work tries to learn explicit or implicit similarity between the states to obtain a reasonable policy Lan et al. (2021). In particular, the authors in this work try to unify the state space representations by providing a taxonomy of metrics in reinforcement learning. Several studies proposed different ways to include Kullback-Leibler (KL) divergence between the current policy and the pre-updated policy to add as a regularization term in the reinforcement learning objective (Schulman et al., 2015). Recently, some studies argued that utilizing Kullback-Leibler regularization implicitly averages the state-action value estimates (Vieillard et al., 2020a).

6.3 The Adversarial Perspective for Deep Neural Policy Generalization

One of the ways to regularize the state observations is based on considering worst-case perturbations added to state observations (i.e. adversarial perturbations). This line of work starts with introducing perturbations produced by the fast gradient sign method proposed by Goodfellow et al. (2015) into deep reinforcement learning observations at test time Huang et al. (2017) Kos & Song (2017), and compares the generalization capabilities of the trained deep reinforcement learning policies in the presence worst-case perturbations and Gaussian noise. These gradient based adversarial methods are based on taking the gradient of the cost function used to train the policy with respect to the state observation. Several other techniques have been proposed on the optimization line of the adversarial alteration of state observations. In this line of work, Korkmaz (2020) suggested a Nesterov momentum-based method to produce adversarial perturbations for deep reinforcement learning policies. Korkmaz (2022) showed that deep reinforcement learning policies learn shared adversarial features across MDPs. In this work the authors investigate the root causes of this problem, and demonstrate that policy high-sensitivity directions and the perceptual similarity of the state observations are uncorrelated. Furthermore, the study demonstrates that the current state-of-the-art adversarial training techniques also learn similar high-sensitivity directions as the vanilla trained deep reinforcement learning policies. While some studies focused on state observation alterations to assess policy resilience with respect to these changes, some studies focused on interpretability and explainability of these changes in these state observation alterations and how these alterations

---

4Low dimensional state Mujoco refers to the setting of Mujoco where the state dimensions are not represented by pixels and dimensions of the state observations range from 11 to 117.

5From the security point of view, this adversarial framework is under the category of black-box adversarial attacks in which this is the first study that demonstrated that the deep reinforcement learning policies are vulnerable to black-box adversarial attacks Korkmaz (2023). Furthermore, note that black-box adversarial perturbations are more generalizable global perturbations that can effect many different policies.
have different effects on standard deep reinforcement learning training algorithms and certified (i.e.
adversarial) training algorithms.\cite{Korkmaz2021b}\footnote{See an initial and preliminary version of the paper by Korkmaz \cite{Korkmaz2021b} here.} Note that this line of work falls under the state observation generalization testing category $\mathcal{G}^S$ provided in Definition 3.6.

While several studies focused on improving optimization techniques to compute optimal perturbations, a line of research focused on making deep neural policies resilient to these perturbations. \cite{Pinto2017} proposed to model the dynamics between the adversary and the deep neural policy as a zero-sum game where the goal of the adversary is to minimize expected cumulative rewards of the deep reinforcement learning policy. This study is a clear example of transition probability perturbation to achieve generalization $\mathcal{G}_P$ in Definition 3.4 of Section 3. \cite{Gleave2020} approached this problem with an adversary model which is restricted to take natural actions in the MDP instead of modifying the observations with $\ell_p$-norm bounded perturbations. The authors model this dynamic as a zero-sum Markov game and solve it via self play Proximal Policy Optimization (PPO). Some recent studies, proposed to model the interaction between the adversary and the deep reinforcement learning policy as a state-adversarial MDP, and claimed that their proposed algorithm State Adversarial Double Deep Q-Network (SA-DDQN) learns theoretically certified robust policies against natural noise and perturbations. In particular, these certified adversarial training techniques aim to add a regularizer term to the temporal difference loss in deep $Q$-learning.

$$\mathcal{H}(r_i + \gamma \max_a \hat{Q}_\theta(s_i, a; \theta) - Q_\theta(s_i, a_i; \theta)) + \kappa \mathcal{R}(\theta)$$

where $\mathcal{H}$ is the Huber loss, $\hat{Q}$ refers to the target network and $\kappa$ is to adjust the level of regularization for convergence. The regularizer term can vary for different certified adversarial training techniques yet the baseline technique uses

$$\mathcal{R}(\theta) = \max\{ \max_{\hat{s} \in B(s)} \max_{a \neq \text{arg maxi} Q(s, a')} Q_\theta(\hat{s}, a) - Q_\theta(\hat{s}, \text{arg maxi} Q(s, a'), -c).$$

where $B(s)$ is an $\ell_p$-norm ball of radius $\epsilon$. While these certified adversarial training techniques drew some attention from the community, more recently manifold concerns have been raised on the robustness of theoretically certified adversarially trained deep reinforcement learning policies \cite{Korkmaz2021a} in Definition 3.6. In these studies, the authors argue that adversarially trained (i.e. certified robust) deep reinforcement learning policies learn inaccurate state-action value functions and non-robust features from the environment. In particular, in \cite{Korkmaz2021a} the authors use action manipulation to investigate worst-case perturbation training. This study is also a clear example of a policy perturbation generalization testing method $\mathcal{G}^\mathcal{P}$ in Definition 3.6. More importantly, recently it has been shown that adversarially trained deep reinforcement learning policies have worse generalization capabilities compared to vanilla trained reinforcement learning policies in high dimensional state space MDPs \cite{Korkmaz2023}. While this study provides a contradistinction between adversarial directions and natural directions that are intrinsic to the MDP, it further demonstrates that the certified adversarial training techniques block generalization capabilities of standard deep reinforcement learning policies. Furthermore note that this study is also a clear example of a state observation perturbation generalization testing method $\mathcal{G}^S$ the Definition 3.6 in Section 3.

7 Meta-Reinforcement Learning and Meta Gradients

A quite recent line of research directs its research efforts to discovering reinforcement learning algorithms automatically, without explicitly designing them, via meta-gradients \cite{Oh2020,Xu2020}. This line of study targets learning the "learning algorithm" by only interacting with a set of environments as a meta-learning problem. In particular,

$$\eta^* = \arg \max_{\eta} \mathbb{E}_{\epsilon \sim \rho(\epsilon)} \mathbb{E}_{\theta_0 \sim \rho(\theta_0)} [\mathbb{E}_{\theta_N} \sum_{t=0}^{\infty} \gamma^t r_t]]$$

here the optimal update rule is parameterized by $\eta$, for a distribution on environments $\rho(\epsilon)$ and initial policy parameters $\rho(\theta_0)$ where $\mathbb{E}_{\theta_N} \sum_{t=0}^{\infty} \gamma^t r_t$ is the expected return for the end of the lifetime of the agent.

\footnote{A short and preliminary version of the paper \cite{Korkmaz2023} can also be found here.}
The overarching objective of meta-reinforcement learning is to be able to build agents that can learn how to learn over time, thus allowing these policies to adapt to a changing environment or even any other changing conditions of the MDP. Quite recently, a significant line of research has been conducted to achieve this objective, particularly Oh et al. (2020) proposes to discover the value function in reinforcement learning. Following this work, Xu et al. (2020) proposed a joint meta-learning framework to learn what the policy should predict and how these predictions should be used in updating the policy. Recently, Kirsch et al. (2022) proposes to use symmetry information in discovering reinforcement learning algorithms and discusses meta-generalization. There is also some work on enabling reinforcement learning algorithms to discover temporal abstractions (Veeriah et al., 2021). In particular, temporal abstraction refers to the ability of the policy to abstract a sequence of actions to achieve certain sub-tasks. As it stands now meta-reinforcement learning can be considered to be a promising research direction that could enable us to build deep reinforcement learning policies that can generalize to different environments, to changing environments over time, or even to different tasks.

8 Transfer in Reinforcement Learning

Transfer in reinforcement learning is a subfield heavily discussed in certain applications of reinforcement learning algorithms e.g. robotics. In current robotics research there is not a safe way of training a reinforcement learning agent by letting the robot explore in real life. Hence, the way to overcome this is to train policies in a simulated environment, and install the trained policies in the actual application setting. The fact that the simulation environment and the installation environment are not identical is one of the main problems for reinforcement learning application research. This is referred to as the sim-to-real gap.

Another subfield in reinforcement learning research focusing on obtaining generalizable policies investigates this concept through transfer in reinforcement learning. The consideration in this line of research is to build policies that are trained for a particular task with limited data and to try to make these policies perform well on slightly different tasks. An initial discussion on this starts with (Taylor & Stone, 2007) to obtain policies initially trained in a source task and transferred to a target task in a more sample efficient way. Later, Tirinzoni et al. (2018) proposes to transfer value functions that are based on learning a prior distribution over optimal value functions from a source task. However, this study is conducted in simple environments with low dimensional state spaces. (Barreto et al., 2017) considers the reward transformation setting $G_R$ in Definition 3.2 from Section 3. In particular, the authors consider a policy transfer between a specific task with a reward function $r(s, a)$ and a different task with reward function $r'(s, a)$. The goal of the study is to decouple the state representations from the task. In the setting of state transformation for generalization $G_S$ in Definition 3.3 Gamrian & Goldberg (2019) focuses on state-wise differences between source and target task. In particular, the authors use unaligned generative adversarial networks to create target task states from source task states. In the setting of policy transformation for generalization $G_\pi$ in Definition 3.5 Jain et al. (2020) focuses on zero-shot generalization to a newly introduced action set to increase adaptability.

While transfer learning is a promising research direction for reinforcement learning, the studies in this subfield still remain oriented only towards reinforcement learning applications, and it is possible to consider the research centered on this subfield as not at the same level of maturity as the previously discussed line of research in Section 6 in terms of being able to test the claims or propositions in complex established baselines.

9 Lifelong Reinforcement Learning

Lifelong learning is a subfield closely related to transfer learning that has recently drawn attention from the reinforcement learning community. Lifelong learning aims to build policies that can sequentially solve different tasks by being able to transfer knowledge between tasks. On this line of research, Lecarpentier et al. (2021) provide an algorithm for value-based transfer in the Lipschitz continuous task space with theoretical contributions for lifelong learning goals. In the setting of action transformation for generalization $G_\pi$ in Definition 3.5 Chandak et al. (2020) focuses on temporally varying (e.g. variations between source task and target task) the action set in lifelong learning. In lifelong reinforcement learning some studies focus on different exploration strategies. In particular,
Garcia & Thomas (2019) models the exploration strategy problem for lifelong learning as another MDP, and the study uses a separate reinforcement learning agent to find an optimal exploration method for the initial lifelong learning agent. The lack of benchmarks limits the progress of lifelong reinforcement learning research by restricting the direct comparison between proposed algorithms or methods. However, quite recent work proposed a new training environment benchmark based on robotics applications for lifelong learning to overcome this issue (Wolczyk et al., 2021).

10 Conclusion

In this paper we tried to answer the following questions: (i) What are the explicit problems limiting reinforcement learning algorithms from obtaining high-performing policies that can generalize? (ii) How can we categorize the different techniques proposed so far to achieve generalization in reinforcement learning? (iii) What are the similarities and differences of these different techniques proposed by different subfields of reinforcement learning research to build reinforcement learning policies that generalize? To answer these questions first we explain the importance of exploration strategies in overfitting, and explain the manifold causes of overestimation bias in reinforcement learning. In the second part of the paper we propose a framework to unify and categorize the various techniques to achieve generalization in reinforcement learning. Starting from explaining all the different regularization techniques in either state representations or in learnt value functions from worst-case to average-case, we provide a current layout of the wide range of reinforcement learning subfields that are essentially working towards the same objective, i.e. generalizable deep reinforcement learning policies. Finally, we provided a discussion for each category on the drawbacks and advantages of these algorithms. We believe our study can provide a compact unifying formalization on recent reinforcement learning generalization research.

References


*The state dimension for this benchmark is 12. Hence, the state space is quite low dimensional.*


