000 001 002 003 004 MITIGATING OVERESTIMATION IN OFFLINE REINFORCEMENT LEARNING WITH ANOMALY **DETECTION**

Anonymous authors

Paper under double-blind review

ABSTRACT

Reinforcement Learning (RL) encounters substantial challenges in real-world applications, due to the time-consuming, costly, and risky nature of interacting with the environment. Offline Reinforcement Learning addresses this limitation by training models on static datasets, allowing an optimal policy to be learned from pre-collected data without requiring additional interactions with the environment. However, in this setting, when the agent queries actions outside the training data distribution, it can lead to overestimation of Q-values for OOD (Out-of-distribution) actions, ultimately hindering policy optimization. Previous works attempted to address this problem using explicit constraints such as penalty terms or support restriction. But these methods often fail to identify OOD actions or result in overly conservative Q-value estimates. We propose a novel solution that adjusts weights during training by using an anomaly detection model to identify the distribution of the offline dataset and employing anomaly scores to guide the offline RL process. Our method(RLAD) not only effectively mitigates the overestimation of OOD actions but also achieves near state-of-the-art performance on continuous D4RL tasks. Additionally, this framework is highly flexible, allowing for integration with various off-policy or offline RL algorithms and Anomaly Detection models to enhance performance.

1 INTRODUCTION

035 036 037 038 039 040 041 042 Reinforcement Learning (RL) has become a pivotal field in artificial intelligence, demonstrating significant achievements in areas such as natural language processing (NLP) [\(Ouyang et al., 2022\)](#page-10-0) and computer vision ([\(Furuta et al., 2019\)](#page-9-0), [\(Liu et al., 2023\)](#page-10-1)). Its ability to enable agents to interact with environments and perform human-like sequential decision-making has made RL particularly valuable in fields such as robotics [\(Vecerik et al., 2018\)](#page-10-2), medical diagnosis, and autonomous driving [\(Gu et al., 2023\)](#page-9-1). However, applying reinforcement learning (RL) to real-world problems poses significant challenges due to the time-consuming, costly, and risky nature of continuous environment interactions.

043 044 045 046 047 048 049 050 051 052 053 To address these challenges, offline Reinforcement Learning (Offline RL) has emerged, focusing on leveraging static datasets for training. Unlike traditional RL, Offline RL lacks the continuous exploration that helps the agent converge to an optimal policy. Additionally, Offline RL must work with limited datasets, often failing to provide sufficient coverage of all possible state-action pairs above given offline dataset leading to a phenomenon known as distributional shift. This limitation leads to a prominent issue: the overestimation of the Q-function, especially for state-action pairs not present in the training dataset, as highlighted by the work of [\(Kumar et al., 2019\)](#page-10-3). Methods like CQL, BCQ, and BRAC ([\(Kumar et al., 2020\)](#page-10-4), [\(Fujimoto et al., 2019\)](#page-9-2), [\(Wu et al., 2019\)](#page-11-0) have been developed to tackle this problem by making value functions pessimistic or restrict the action space of a policy, which can result in overly pessimistic evaluations or overly restrictive regions. Therefore, many works try to make the agent not too conservative or to address distributional shift and OOD actions while maintaining trading off with the previous distributional shift and OOD repression to obtain an optimal policy. ([\(Lyu et al., 2022\)](#page-10-5), [\(Hong et al., 2023\)](#page-9-3))

054 055 056 057 058 059 060 Inspired by the analysis of [\(Kumar et al., 2019\)](#page-10-3), which highlights that overestimation mainly occurs with data outside the training distribution, and the fact that explicit constraints can result in overpessimistic value estimation, we have focused on the following point: How can we better utilize the distribution of the training dataset to avoid overestimation caused by OOD data? While we aim to prevent the agent from querying out-of-distribution actions, we also recognize that not every out-of-distribution action leads to a sub-optimal policy. Therefore, we seek to avoid imposing hard or explicit constraints.

061 062 063 064 065 066 We propose that anomaly detection models, which are highly effective modules for identifying out-of-distribution or novel data, can be a possible novel solution. These models adept at classifying binary problems based on anomaly scores, which typically quantify how much a data point deviates from the training distribution. These scores can provide useful guidance for the agent during training, so we can plug-in any off-policy algorithm without the need to introduce additional regularizers into their objective function.

067 068 069 070 071 072 073 074 In this context, we propose approaching the Offline RL problem through the lens of a Anomaly Detection, classifying data as either in-distribution (normal) or out-of-distribution (abnormal). Our proposed method, Reinforcement Learning with Anomaly Detection (RLAD), addresses these challenges by leveraging deep learning-based anomaly detection models ([\(Zong et al., 2018\)](#page-11-1), [\(Ruff](#page-10-6) [et al., 2018\)](#page-10-6)) to efficiently and accurately estimate whether unseen data belongs to the in-distribution or out-of-distribution. This approach capitalizes on the expressive power of neural network networks without the need for specialized regularizer to match distributions, support or underestimate Q-value. Our algorithm operates in two stages:

- 1) Anomaly Detection Model Training: Train the anomaly detection model on the training dataset. During this phase, the model learns which data points are close to the training distribution and assigns an anomaly score as an indicator.
	- 2) Anomaly Score-Based Weight Adjustment: Use the anomaly score of the given data to inform the agent, adjusting the importance of each sample during learning through the application of different sample weights.

Our experiments aim to demonstrate about anomaly scores(weight) and estimated Q-values. Our algorithm performs well in continuous environments, achieving state-of-the-art performance in several tasks. Our contributions are as follows:

- 1) Framework: We present a simple, easily implementable framework that can be integrated with various off-policy or offline RL algorithms and anomaly detection models, especially according to the environment.
- 2) Q-value Estimation: We demonstrate that Anomaly Score-Based Weight Adjustment significantly contribute to accurate Q-value estimation and the mitigation of overestimation.
- 3) Empirical Performance: We show good empirical performance, particularly in MuJoCo environments, achieving state-of-the-art results.

2 RELATED WORKS

097 098 099 100 101 Policy Constraints Several works have proposed imposing constraints on actor-critic algorithms by constraining the learned policy to remain close to the behavior policy that generated the offline dataset D. [\(Fujimoto et al., 2019\)](#page-9-2) directly estimates the behavior policy π_β and constrains the learned policy π_{θ} to stay close to the estimated π_{β} . In contrast, [\(Kumar et al., 2019\)](#page-10-3) argues that support matching using Maximum Mean Discrepancy (MMD) is more effective than direct matching of distributions.

102 103 104 105 106 107 Additionally, [\(Wu et al., 2019\)](#page-11-0) brings π_β closer to the target policy by penalizing the critic, leading to more pessimistic evaluations. Methods like [\(Peng et al., 2019\)](#page-10-7) and [\(Nair et al., 2021\)](#page-10-8) use the advantage term to construct an implicitly weighted maximum likelihood objective, while others, such as (Fujimoto $\&$ Gu, 2021), operate without the actor-critic structure. These approaches aim to fundamentally prevent OOD actions from being selected by the learned policy π_{θ} , thus mitigating overestimation and providing relatively stable performance. However, these strategies can sometimes excessively constrain or regularize actions of the agent.

108 109 110 111 112 113 114 115 Conservative Value Estimation Rather than restricting the policy, some methods focus on conservatively estimating the value function of state-action pairs by explicitly penalizing unseen OOD actions in D [\(Kumar et al., 2020\)](#page-10-4) or by avoiding directly querying unseen actions in the dataset using expectile regression to maximize the advantage [\(Kostrikov et al., 2021\)](#page-10-9). Additionally, model-based approaches such as [\(Yu et al., 2022\)](#page-11-2) learn dynamic models to interpolate and augment data, combined with conservative Q-value estimation. While these works aim to avoid the OOD overestimation problem by penalizing or ignoring unseen OOD actions in D , they often suffer from overly pessimistic value estimates.

116 117 118 119 Other approaches, such as [\(Gal & Ghahramani, 2016\)](#page-9-5), [\(Wu et al., 2021\)](#page-11-3), [\(An et al., 2021\)](#page-9-6), [\(Bai](#page-9-7) [et al., 2022\)](#page-9-7), utilize uncertainty measures—like Bayesian methods, MC-dropout, and ensemble to adaptively adjust the level of OOD suppression. These strategies can operate without explicit policy constraints, but the computational cost of measuring uncertainty can be high and incorrect.

120 121 122 123 124 125 Trajectory Optimization Recently, Conditional Sequence Modeling (CSM) has emerged as a novel paradigm for RL tasks, associating individual trajectories with return-to-go (RTG) tokens, enabling the handling of long sequences with large model sizes, such as in [\(Janner et al., 2021\)](#page-9-8) and [\(Chen et al.,](#page-9-9) [2021\)](#page-9-9). However, due to the intrinsic stochasticity of state transitions, approaches like [\(Yamagata](#page-11-4) [et al., 2023\)](#page-11-4) and [\(Chebotar et al., 2023\)](#page-9-10) have been proposed to address these limitations, particularly in offline settings.

126 127 128 129 130 131 132 133 Anomaly Detection Anomaly Detection (AD) is the task of identifying samples that deviate significantly from the majority of the data, often signaling irregular, fake, rare, or fraudulent observations [\(Wang et al., 2019\)](#page-10-10). Particularly, semi-supervised AD is defined as the task of detecting samples that are out of distribution by using only normal samples in the training dataset. To estimate the normal distribution and detect exceptional samples from that distribution, a wide range of models is available, spanning from statistical to deep-learning based AutoEncoder ([\(Ruff et al., 2018\)](#page-10-6), [\(Zong et al., 2018\)](#page-11-1)) Transformer [\(Xu, 2021\)](#page-11-5), and flow-based[\(Zhou et al., 2024\)](#page-11-6). These methods have been improved to handle various problem of each data types, including images, video, and time-series data.

134 135 136 137 Given the dimension reduction capabilities and generalizability of AutoEncoders in handling the varying space sizes of reinforcement learning datasets, we select two models for the AD module to capture distributional information: Deep SVDD ([\(Ruff et al., 2018\)](#page-10-6)) and DAGMM ([\(Zong et al.,](#page-11-1) [2018\)](#page-11-1)).

138 139 140 141 142 143 Deep SVDD Deep SVDD [\(Ruff et al., 2018\)](#page-10-6) is a deep learning-based extension of the classical Support Vector Data Description method.[\(Tax & Duin, 2004\)](#page-10-11) Unlike SVDD, which uses hand-crafted kernels such as the Gaussian kernel, Deep SVDD learns the appropriate feature space through a deep neural network with an AutoEncoder architecture. The goal of Deep SVDD is to find the smallest hypersphere that encloses most of the normal data in the feature space by mapping inputs through the model.

144 145 146 147 DAGMM Similar to Deep SVDD, DAGMM also utilizes an AutoEncoder to encode data into a feature space.[\(Zong et al., 2018\)](#page-11-1) However, unlike Deep SVDD, which seeks to find the optimal hypersphere for normal data, DAGMM estimates the distribution of data in the latent space by utilizing a Gaussian Mixture Model.

148 149 150

151 152

3 PRELIMINARIES

3.1 REINFORCEMENT LEARNING

153 154 155 156 157 We formulate Reinforcement Learning using the standard Markov Decision Process (MDP), (S, A, P, R, γ) , where S represents the state space, A denotes the action space, $P(s'|s, a)$ is the transition probability, $R(s, a) : S \times A \to \mathbb{R}$ is the reward function, and $\gamma \in (0, 1]$ is the discount factor. Reinforcement Learning aims to find an optimal policy that maximizes the expected cumulative discounted reward, $\mathbb{E}_{\tau}[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t)]$, where τ is a trajectory.

158 159 160 There are several approaches to finding an optimal policy, such as Policy Gradient [\(Sutton et al.,](#page-10-12) [1999\)](#page-10-12), Q-learning [\(Sutton & Barto, 2018\)](#page-10-13), and Actor-Critic methods [\(Konda & Tsitsiklis, 1999\)](#page-9-11). Among them, Q-learning and Actor-Critic methods are based on the Bellman Equation:

$$
Q^{\pi}(s, a) = R(s, a) + \gamma \mathbb{E}_{P(s'|s, a)}[V^{\pi}(s')]
$$

162 163 164 165 where $Q^{\pi}(s, a) = \mathbb{E}_{\pi}[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t) | s = s_t, a = a_t]$ is the state-action value function, and $V^{\pi}(s) = \mathbb{E}_{\pi} \left[\sum_{t=0}^{\infty} \gamma^{t} R(s_t, a_t) | s = s_t \right]$ is the state value function. Both methods update the Qfunction via the Bellman operator B :

$$
(\mathcal{B}Q^{\pi})(s,a) = R(s,a) + \gamma \mathbb{E}_{P(s'|s,a)} [\mathbb{E}_{\pi}[Q^{\pi}(s',a')]]
$$

In this paper, we utilize the Actor-Critic method, a widely used approach that alternates between policy evaluation and policy improvement, which demonstrates faster and more efficient convergence towards finding the optimal policy.

169 170 171

172

166 167 168

3.2 OFFLINE REINFORCEMENT LEARNING

173 174 175 176 177 In real-world applications, interacting with the environment can often be risky, expensive, and time-consuming. To address these challenges, Offline Reinforcement Learning (Offline RL) has been developed, which leverages a pre-collected dataset to learn an optimal policy without additional environment interaction. The pre-collected dataset consists of multiple trajectories $\tau = (s_0, a_0, r_0, s_1, a_1, r_1, \ldots).$

178 179 180 181 182 183 184 However, the lack of interaction with the environment makes it difficult for the agent to explore new state-action pairs, leading to the domain shift problem, which results in a sub-optimal policy. Additionally, standard off-policy algorithms often perform poorly in the offline setting, leading to a need for new methods. Many approaches focus on mitigating the overestimation problem caused by out-of-distribution actions through value function or policy constraints, uncertainty-based methods, or model-based approaches. In this paper, we aim to address this issue using anomaly scores from independently trained anomaly detection module.

- **185**
- **186 187**

4 REINFORCEMENT LEARNING WITH ANOMALY DETECTION (RLAD)

188 189 190 191 192 In this paper, we propose addressing the Offline RL problem through the lens of Anomaly Detection, which we refer to as Reinforcement Learning with Anomaly Detection (RLAD). Offline Reinforcement Learning encounters the overestimation problem primarily when the agent bootstraps actions that are not present in the training dataset. As a result, the accumulation of bootstrapping errors can significantly degrade performance.

193 194 195 196 To address the issue of out-of-distribution actions being bootstrapped, we provide an anomaly score as guidance to the agent to indicate how far a data point is from the distribution of the training dataset. Specifically, anomaly scores are used as weights for the objective functions of both the Actor and Critic. Our approach has empirically shown promising results.

197 198

4.1 WHY ANOMALY DETECTION?

199

200 201 202 203 204 As mentioned earlier, previous works in offline reinforcement learning algorithms often solve the overestimation problem by imposing constraints on value functions or policies. However, these methods can lead to overly conservative value estimates or overly restrictive action spaces, resulting in sub-optimal policies. Moreover, approaches based on ensemble or dropout-based uncertainty measures, being suggested to solve this problem, have inevitable problem of high computational cost or inaccurate estimation of uncertainty.

205

206 207 208 In contrast, Anomaly Detection models are effective at detecting out-of-distribution data with respect to the normal training dataset. These models typically determine whether data points are in-distribution or out-of-distribution based on anomaly scores.

209 210 211 In this reason, we propose that anomaly scores can serve as efficient and effective guidance for the agent to determine whether a given action is out-of-distribution, helping the agent adjust its policy accordingly.

212

- **213** 4.2 PRETRAINING THE ANOMALY DETECTION MODEL
- **215** To inform the agent of how far the data is from the training set, we first train an anomaly detection model. In this paper, we use Deep SVDD and DAGMM with state-action pairs as the input. Although

Figure 1: This figure illustrates the overall pipeline. Anomaly Detection Train(left) First train the Anomaly Detection(AD) module using offline Reinforcement Learning dataset D . **RL Train(right)** Then weighted update is performed for RL algorithm update for every iteration with anomaly score from AD module and scaling function f. For offline update, every sample is bootstrapped from offline Dataset D.

we considered using full trajectories, capturing the features of each trajectory proved challenging, so we opted for state-action pairs to simplify assumptions and efficiently capture features. We denote the anomaly score for a state-action pair (s, a) as anomaly score (s, a) . When the state s is fixed, this can be roughly interpreted with behavior policy. Additionally, we assume that the further a state-action pair is from the dataset, the higher the *anomaly_score(s, a)*.

246

247

4.3 TRAINING THE RL AGENT

248 249 250 251 252 253 Using the previously trained Anomaly Detection model, we compute the anomaly score for each state-action pair. This score is then used to weight the value function training and policy optimization. Since we want the agent to focus more on data points that are closer to the training distribution, the weight should increase as the anomaly score decreases. A higher weight indicates a lower likelihood of being OOD, encouraging more learning. Conversely, a lower weight indicates a higher likelihood of being OOD, reducing its impact on learning.

254 255 256 This approach avoids imposing strict penalties or limiting the agent to the training distribution, effectively mitigating the overestimation problem caused by OOD data while still allowing for accurate estimation of OOD actions. The overall algorithm can be summarized as follows:

- 1) Calculate Anomaly Score: Use the trained Anomaly Detection model to calculate the anomaly score for the next state-action pair. Since the agent only queries the next action, we need to train the network based on the next state-action pair.
- 2) Compute Weight: Determine the weight from pretrained Anomaly Detection model as follows:

 $weight(s, a) := f(anomaly_score(s, a))$

where $f(\cdot)$ is a non-negative, monotonically decreasing function bounded within the range of anomaly_score(\cdot , \cdot). The specific form of $f(\cdot)$ may vary depending on the model used to compute the anomaly score. In our implementation, we use $f(x) = \frac{1}{x}$ for Deep SVDD and $f(x) = sigmoid(-x)$ for DAGMM.

267 268 269 3) Weighted Q-Function Training: Train the Q-function using the computed weights with the following objective function:

$$
\nabla_{\theta} \mathcal{L}(\theta) = \mathbb{E}[weight(s', a') (Q_{\theta}(s, a) - r - Q^*(s', a')) \nabla_{\theta} Q_{\theta}(s, a)]
$$

5 EXPERIMENTAL RESULTS

In this section, our experiments try to address the following questions:

- 1. Does our framework achieve better performance with various combinations of Anomaly Detection models and Reinforcement Learning algorithms?
- 2. Does our framework estimate Q values correctly in the training distribution and do not estimate Q values too conservative in the out-of-distribution?

To answer the above questions we present two experiments : First, we analyze Q value errors (between the true value and the estimated value from offline algorithms) with weights on the training distribution and the out-of-distribution. Second, we compare normalized returns with some baselines in some tasks MuJoCo environment including medium, medium-replay and medium-expert and Adroit environment including human and cloned. Also we compare Q-value distributions among Soft Actor-Critic, RLAD-SAC-SVDD, and CQL in 'Pendulum-v1' environment.

 In this section, we analyze the relationship between the weight and the $Q_{\text{difference}}$ to demonstrate the effectiveness of our method.

 To estimate $Q^*(s, a)$, we used the critic network of an SAC model trained in online setting for proxy. We then compared the $Q(s, a)$ values from both our model and the baseline model, CQL, with simple qunaitifing measure defined as $Q_{difference}(s, a) := Q(s, a) - Q^*(s, a)$. Additionally, we extracted an OOD dataset using AutoEncoder and MC-Dropout, independent of the offline dataset and Anomaly Detection module, to analyze OOD actions and Q-value differences. For the validity of these datasets, please refer to t-SNE visualizations in Appendix, figure [5.](#page-15-0)

 The figure shows the distribution of weight as a function of $Q_{difference}$ for both normal and OOD samples across our model(RLAD-SAC) and CQL in the 'halfcheetah-medium-v2' environment. Notably, both models display a peak at negative $Q_{\text{difference}}$ values, with a long tail extending toward positive values. However, our model exhibits a more concentrated peak near $Q_{difference} = 0$, while CQL shows more spread in the positive direction, indicating more frequent overestimations.

 For OOD samples, the distribution of our model shows that $Q_{\text{difference}}$ are near zero and weights from the anomaly detection module are smaller than normal data, which demonstrates that the anomaly detection module performs well. In contrast, $Q_{\text{difference}}$ of CQL are far from zero for OOD samples, suggesting overly conservative estimation.

378

379 380 381 Table 1: Comparison of normalized average returns of RLAD against original SAC model (offline) and Behavior Cloning(BC) on the D4RL MuJoCo Gym datasets. Normalized returns of RLAD are averaged over 5 random seeds, and baseline values are taken from each paper.

392 393 394

In comparing the two methods, our model shows a more accurate Q-value estimation, particularly around $Q_{difference} = 0$, where weight peaks closer to this value indicate higher accuracy in policy learning. CQL, however, suffers from both under- and overestimation, as evidenced by its broader distribution and more pronounced presence of large positive $Q_{\text{difference}}$ values, even for normal data.

399 400 401 402 403 Also, as shown in table [1,](#page-7-0) this indicates that AD modules like Deep SVDD and DAGMM can capture the characteristics of the data and successfully estimate Q-values for samples not present in D, without directly imposing constraints on policy or value estimation. Moreover, the superior performance of RLAD-SAC (with Deep SVDD and DAGMM) over standard SAC highlights the potential for exploring a broader range of AD models.

404 405

406

5.2 BRIEF ANALYSIS ON Q-FUNCTIONS

407 408 409 410 411 We analyze the Q-functions of Online Soft Actor-Critic, RLAD-SAC-SVDD (Offline), and CQL (Offline) in the Pendulum-v1 environment, where the offline dataset is obtained by a random policy. The Pendulum environment is chosen for visualization on a 1D plane, eliminating the need for dimensionality reduction methods for clearer interpretation.

412 413 414 As shown in Figure [3,](#page-6-0) both our model and CQL estimate the Q-values conservatively. However, CQL exhibits more conservative estimates than our model, while our model provides more accurate Q-value estimations.

415

416 417 5.3 COMPARISON WITH D4RL

418 419 420 421 422 Based on the above analysis showing the effectiveness of our model, we compare our method to prior offline RL methods on continuous domains and dataset compositions. We implement our method based on Soft Actor-Critic[\(Haarnoja et al., 2018\)](#page-9-12) and BEAR[\(Kumar et al., 2019\)](#page-10-3) for Reinforcement Learning algorithms and Deep-SVDD[\(Ruff et al., 2018\)](#page-10-6) and DAGMM [\(Zong et al., 2018\)](#page-11-1) for Anomaly Detection model.

423 424 425 426 427 428 429 430 431 Evaluation on D4RL Results for the MuJoCo tasks and Adroit tasks [\(Rajeswaran et al., 2018\)](#page-10-14) in the D4RL benchmarks [\(Fu et al., 2021\)](#page-9-13) are shown in [2](#page-8-0) and [3,](#page-8-1) respectively. The results for other baselines are based on their respective papers ([\(Kang et al., 2023\)](#page-9-14), [\(Kidambi et al., 2020\)](#page-9-15), [\(Rigter et al., 2022\)](#page-10-15), [\(Kumar et al., 2019\)](#page-10-3), [\(Cheng et al., 2022\)](#page-9-16), [\(Kumar et al., 2020\)](#page-10-4), [\(Kostrikov et al., 2021\)](#page-10-9), [\(Chen et al.,](#page-9-9) [2021\)](#page-9-9)). We evaluate three environments of MuJoCo tasks, hopper, walker2d, and halfcheetah, with three dataset types, medium, medium-replay, and medium-expert, for each environment. Also, we evaluate four environments of Adroit tasks, pen, hammer, door, and relocate, with two data types, human and cloned. We achieve the best performance on most environments. Especially, we obtain good performance on the multimodal datasets such as medium-expert or medium-replay. This implies that our method is robust to the complex distribution.

433 434 435 Table 2: Comparison of normalized average returns of RLAD against baselines on the D4RL MuJoCo Gym datasets. Normalized returns of RLAD are averaged over 5 random seeds, and baseline values are taken from each paper.

Table 3: Comparison of normalized average returns of RLOCC against baselines on the D4RL Adroit datasets. Normalized returns of RLAD are averaged over 5 random seeds, and baseline values are taken from each paper.

5.4 CONCLUSION

458 459 460 461 462 463 464 465 466 467 By analyzing Q differences, we demonstrate that our model which utilizes Anomaly Detection(AD) models, effectively mitigates the overestimation of OOD samples compared to prior offline RL algorithms, also do not estimate Q-values overly conservative. Moreover, in the D4RL benchmarks, our model achieves near state-of-the-art performance across various environments, for several combinations of Reinforcement Learning algorithms and Anomaly Detection models. These experiments highlight the potential of integrating Anomaly Detection modules to detect OOD samples and leveraging their quantitative anomaly scores as guidance to enhance performance. Because of the independence of AD module, this allows for the flexible integration of various models without imposing explicit constraints on policy or value functions, facilitating the exploration of optimal combinations between various branches of Anomaly Detection and powerful RL algorithms.

468 469 470 471 472 473 474 For future work, we aim to find the way how to choose the best combination of an Anomaly Detection module and a Reinforcement Learning algorithm according to the characteristic of the dataset or the environment. This research will enable more effective selection of an anomaly detection model and a reinforcement learning algorithm. We believe that our work provides a deeper empirical understanding of the relationship between accurate Q-value estimation and overall performance across various environments and RL algorithms. Additionally, we see potential for our approach to be further developed, much like data type-specific AD research in areas such as images and time series.

475

432

- **476**
- **477**
- **478 479**
- **480**
- **481**
- **482**
- **483**
- **484**
- **485**

486 487 REFERENCES

501

515

521

532

538

491 492 Chenjia Bai, Lingxiao Wang, Zhuoran Yang, Zhihong Deng, Animesh Garg, Peng Liu, and Zhaoran Wang. Pessimistic bootstrapping for uncertainty-driven offline reinforcement learning, 2022.

493 494 495 496 497 498 499 500 Yevgen Chebotar, Quan Vuong, Karol Hausman, Fei Xia, Yao Lu, Alex Irpan, Aviral Kumar, Tianhe Yu, Alexander Herzog, Karl Pertsch, Keerthana Gopalakrishnan, Julian Ibarz, Ofir Nachum, Sumedh Anand Sontakke, Grecia Salazar, Huong T. Tran, Jodilyn Peralta, Clayton Tan, Deeksha Manjunath, Jaspiar Singh, Brianna Zitkovich, Tomas Jackson, Kanishka Rao, Chelsea Finn, and Sergey Levine. Q-transformer: Scalable offline reinforcement learning via autoregressive q-functions. In Jie Tan, Marc Toussaint, and Kourosh Darvish (eds.), *Proceedings of The 7th Conference on Robot Learning*, volume 229 of *Proceedings of Machine Learning Research*, pp. 3909–3928. PMLR, 06–09 Nov 2023. URL [https://proceedings.mlr.press/v229/](https://proceedings.mlr.press/v229/chebotar23a.html) [chebotar23a.html](https://proceedings.mlr.press/v229/chebotar23a.html).

- **502 503 504** Lili Chen, Kevin Lu, Aravind Rajeswaran, Kimin Lee, Aditya Grover, Misha Laskin, Pieter Abbeel, Aravind Srinivas, and Igor Mordatch. Decision transformer: Reinforcement learning via sequence modeling. *Advances in neural information processing systems*, 34:15084–15097, 2021.
- **505 506 507** Ching-An Cheng, Tengyang Xie, Nan Jiang, and Alekh Agarwal. Adversarially trained actor critic for offline reinforcement learning, 2022.
- **508 509** Justin Fu, Aviral Kumar, Ofir Nachum, George Tucker, and Sergey Levine. D4rl: Datasets for deep data-driven reinforcement learning, 2021.
- **510 511 512** Scott Fujimoto and Shixiang Shane Gu. A minimalist approach to offline reinforcement learning. In *Thirty-Fifth Conference on Neural Information Processing Systems*, 2021.
- **513 514** Scott Fujimoto, David Meger, and Doina Precup. Off-policy deep reinforcement learning without exploration, 2019.
- **516 517 518** Ryosuke Furuta, Naoto Inoue, and Toshihiko Yamasaki. Pixelrl: Fully convolutional network with reinforcement learning for image processing. *IEEE Transactions on Multimedia*, 22(7):1704–1719, 2019.
- **519 520** Yarin Gal and Zoubin Ghahramani. Dropout as a bayesian approximation: Representing model uncertainty in deep learning, 2016.
- **522 523 524** Ziqing Gu, Lingping Gao, Haitong Ma, Shengbo Eben Li, Sifa Zheng, Wei Jing, and Junbo Chen. Safe-state enhancement method for autonomous driving via direct hierarchical reinforcement learning. *IEEE Transactions on Intelligent Transportation Systems*, 2023.
- **525 526** Tuomas Haarnoja, Aurick Zhou, Pieter Abbeel, and Sergey Levine. Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor, 2018.
- **527 528 529** Joey Hong, Aviral Kumar, and Sergey Levine. Confidence-conditioned value functions for offline reinforcement learning, 2023. URL <https://arxiv.org/abs/2212.04607>.
- **530 531** Michael Janner, Qiyang Li, and Sergey Levine. Offline reinforcement learning as one big sequence modeling problem. In *Advances in Neural Information Processing Systems*, 2021.
- **533 534** Bingyi Kang, Xiao Ma, Chao Du, Tianyu Pang, and Shuicheng Yan. Efficient diffusion policies for offline reinforcement learning, 2023. URL <https://arxiv.org/abs/2305.20081>.
- **535 536 537** Rahul Kidambi, Aravind Rajeswaran, Praneeth Netrapalli, and Thorsten Joachims. Morel: Modelbased offline reinforcement learning. *Advances in neural information processing systems*, 33: 21810–21823, 2020.
- **539** Vijay Konda and John Tsitsiklis. Actor-critic algorithms. *Advances in neural information processing systems*, 12, 1999.

551

572

- **540 541 542** Ilya Kostrikov, Ashvin Nair, and Sergey Levine. Offline reinforcement learning with implicit q-learning, 2021. URL <https://arxiv.org/abs/2110.06169>.
- **543 544** Aviral Kumar, Justin Fu, George Tucker, and Sergey Levine. Stabilizing off-policy q-learning via bootstrapping error reduction, 2019.
- **545 546 547** Aviral Kumar, Aurick Zhou, George Tucker, and Sergey Levine. Conservative q-learning for offline reinforcement learning. *Advances in Neural Information Processing Systems*, 33:1179–1191, 2020.
- **548 549 550** Yinhe Liu, Sunan Shi, Junjue Wang, and Yanfei Zhong. Seeing beyond the patch: Scale-adaptive semantic segmentation of high-resolution remote sensing imagery based on reinforcement learning, 2023.
- **552 553 554** Jiafei Lyu, Xiaoteng Ma, Xiu Li, and Zongqing Lu. Mildly conservative q-learning for offline reinforcement learning. In *Thirty-sixth Conference on Neural Information Processing Systems*, 2022.
	- Ashvin Nair, Abhishek Gupta, Murtaza Dalal, and Sergey Levine. Awac: Accelerating online reinforcement learning with offline datasets, 2021. URL [https://arxiv.org/abs/2006.](https://arxiv.org/abs/2006.09359) [09359](https://arxiv.org/abs/2006.09359).
- **559 560 561 562** Long Ouyang, Jeffrey Wu, Xu Jiang, Diogo Almeida, Carroll Wainwright, Pamela Mishkin, Chong Zhang, Sandhini Agarwal, Katarina Slama, Alex Ray, et al. Training language models to follow instructions with human feedback. *Advances in neural information processing systems*, 35:27730– 27744, 2022.
- **563 564 565** Xue Bin Peng, Aviral Kumar, Grace Zhang, and Sergey Levine. Advantage-weighted regression: Simple and scalable off-policy reinforcement learning, 2019. URL [https://arxiv.org/](https://arxiv.org/abs/1910.00177) [abs/1910.00177](https://arxiv.org/abs/1910.00177).
	- 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, 2018.
- **570 571** Marc Rigter, Bruno Lacerda, and Nick Hawes. Rambo-rl: Robust adversarial model-based offline reinforcement learning, 2022.
- **573 574 575 576 577** Lukas Ruff, Robert Vandermeulen, Nico Goernitz, Lucas Deecke, Shoaib Ahmed Siddiqui, Alexander Binder, Emmanuel Müller, and Marius Kloft. Deep one-class classification. In Jennifer Dy and Andreas Krause (eds.), *Proceedings of the 35th International Conference on Machine Learning*, volume 80 of *Proceedings of Machine Learning Research*, pp. 4393–4402. PMLR, 10–15 Jul 2018. URL <https://proceedings.mlr.press/v80/ruff18a.html>.
- **578** Richard S Sutton and Andrew G Barto. *Reinforcement learning: An introduction*. MIT press, 2018.
- **579 580 581 582** Richard S Sutton, David McAllester, Satinder Singh, and Yishay Mansour. Policy gradient methods for reinforcement learning with function approximation. *Advances in neural information processing systems*, 12, 1999.
- **583 584** David MJ Tax and Robert PW Duin. Support vector data description. *Machine learning*, 54:45–66, 2004.
	- Laurens Van der Maaten and Geoffrey Hinton. Visualizing data using t-sne. *Journal of machine learning research*, 9(11), 2008.
- **588 589 590 591** Mel Vecerik, Todd Hester, Jonathan Scholz, Fumin Wang, Olivier Pietquin, Bilal Piot, Nicolas Heess, Thomas Rothörl, Thomas Lampe, and Martin Riedmiller. Leveraging demonstrations for deep reinforcement learning on robotics problems with sparse rewards, 2018.
- **592 593** Hongzhi Wang, Mohamed Jaward Bah, and Mohamed Hammad. Progress in outlier detection techniques: A survey. *IEEE Access*, 7:107964–108000, 2019. doi: 10.1109/ACCESS.2019. 2932769.

A APPENDIX

A.1 IMPLEMENTATION DETAILS

This is hyper-parameters for SAC and BEAR.

Table 4: Hyperparameters

A.3 EXPERIMENT DESIGN : ANALYSIS OF WEIGHT AND Q DIFFERENCE

 In [5.1,](#page-6-1) our experiment procedure is as the following: we train the Anomaly Detection model and train two agents based on SAC which are in online setting and offline setting, respectively.

- 1. Offline Learning and Proxy for Optimal Q-Value: Online Learning To estimate $Q^*(s, a)$, we utilized the critic network of a Soft Actor-Critic (SAC) model trained with a large amount of online data as a proxy for the optimal policy and the optimal policy evaluation network (critic).
	- 2. Sampling and calculating Q difference Afterward, we trained both our proposed model and the baseline model, CQL, in an offline setting. We then compared the difference between the $Q(s, a)$ values obtained from the critic networks of both offline models with the $Q^*(s, a)$ values from the online SAC critic, visualizing these differences in a graph[\(2\)](#page-6-2).

 $Q_{\text{difference}} = (f(anomaly_score(s, a)), Q^*(s, a) - Q(s, a))$

- 3. **Sampling** D_{ood} Furthermore, to analyze the anomaly scores of OOD actions and the differences in Q -values, we extracted an OOD dataset, D_{ood} , using Autoencoder(AE) and Monte Carlo Dropout(MC-Dropout). For ensuring the objectivity of test, the extraction of D_{ood} is performed independently of both the offline dataset D and the Anomaly methods. Detailed procedure is:
	- Training the autoencoder model with dropout layers using the normal set D .
	- For each data in the training dataset, calculate the variance of the reconstruction error with Monte Carlo(MC) Dropout. Set the threshold as 10 times of the maximum of the variance of the reconstruction error within the training dataset.
	- With the random policy, calculate the variance of the reconstruction error for each state, action pairs in an episode with MC dropout. If the variance exceeds the threshold, we classify that state-action pair as out-of-distribution data and include it in the out-ofdistribution dataset.
	- Each D and D_{ood} is visualized by TSNE[\(Van der Maaten & Hinton, 2008\)](#page-10-16) for the high and varying dimensionality of each environment[\(5\)](#page-15-0)

 As you can see in the figure [4,](#page-14-0) both CQL and our model estimate Q-values accurately in the training dataset. Meanwhile, in the out-of-distribution, our model estimates Q-values more accurate than CQL, that is Q values of the most of data in the out-of distribution are close to 0. This result shows that our model effectively mitigates Q values and estimates accurately.

-
-
-
-

-
-
-
-
-

Figure 4: $Q_{difference}$ and Weight for each D4RL mujoco environments.

 To describe the results of other mujoco environment, please see this figure [4.](#page-14-0) In the Hopper environment, the overall pattern is similar to the main figure, with the only difference being the gap between normal-CQL and normal-RLAD. For the halfcheetah-medium-replay environment, the results demonstrate that CQL's estimations for both the normal and OOD sets deviate significantly from the online proxy Q^* , whereas our model (green and pink) overlaps near the zero region, indicating more accurate estimations.

 An exception to this pattern is observed in the halfcheetah-medium-expert environment, where the performance gap between RLAD-SAC and CQL is smaller than in other datasets. This could suggest that the dynamics of the expert dataset reduce the model's reliance on anomaly detection, partially explaining why RLAD-SAC's advantage is less pronounced in this setting. However, even in this case, RLAD-SAC avoids significant overestimation, particularly for the OOD set, which still provides a performance edge over CQL[\(2\)](#page-8-0). Lastly, in the walker2d environment, both models perform well on the training dataset D , with our model showing a tendency toward underestimation, while CQL exhibits overestimation for D_{ood} samples. This may further explain the performance gap between our model and CQL.

 Interestingly, in the walker2d-medium-expert environment, the overall weight distribution is higher than in other environments. However, the AD module appears to be functioning well, as the OOD set still exhibits a lower peak in weight values compared to the training set. In this environment, not only our model could avoid overstimation of D_{ood} , but also estimate Q values for normal set D more exactly.

A.4 HARDWARES

 For the Mujoco experiments, we use the medium, medium-replay, and medium-expert datasets for the hopper, walker2d, and halfcheetah environments, respectively. And for Adroit experiments, we use human and cloned for pen, hammer, door and relocate. To operate experiments, we use the following hardwares:

Table 7: Specifications of the Hardware Used for Experiments

