Towards Interpretable Deep Reinforcement Learning Models via Inverse Reinforcement Learning

Sean Xie  
Department of Computer Science  
Dartmouth College  
Hanover, NH 03755  
yuansheng.xie.gr@dartmouth.edu

Soroush Vosoughi  
Department of Computer Science  
Dartmouth College  
Hanover, NH 03755  
soroush.vosoughi@dartmouth.edu

Saeed Hassanpour  
Department of Biomedical Data Science  
Dartmouth College  
Hanover, NH 03755  
saeed.hassanpour@dartmouth.edu

Abstract—Artificial Intelligence, particularly through recent advancements in deep learning (DL), has achieved exceptional performances in many tasks in fields such as natural language processing and computer vision. For certain high-stake domains, in addition to desirable performance metrics, a high level of interpretability is often required in order for AI to be reliably utilized. Unfortunately, the black box nature of DL models prevents researchers from providing explicative descriptions for a DL model's reasoning process and decisions. In this work, we propose a novel framework utilizing Adversarial Inverse Reinforcement Learning that can provide global explanations for decisions made by a Reinforcement Learning model and capture intuitive tendencies that the model follows by summarizing the model's decision-making process.

Index Terms—Adversarial Inverse Reinforcement Learning, Natural Language Processing, Abstractive Summarization

I. INTRODUCTION

The utilization of deep learning (DL) models has become increasingly prevalent in a variety of domains such as smart city [1], [2], criminal justice [3], [4], [5], drug discovery [6], [7] and healthcare [8], [9], [10]. In these domains, the successful adoption of predictive models in assisting with high-stake decisions depends not only on the performance of these models but also on how well the process by which these models are making their decisions can be understood by their users [11], [12]. Only when users clearly understand the behavior of a model, can they determine how much they should rely on the a model's decisions. The complexity of DL models, however, make it an extremely difficult task to explain or reason about their behaviors [13], [14]. The crux of the problem rests with the basis of DL, the Multi-Layer Perceptron (MLP). Since their inception, MLPs have been widely regarded as being capable of inferring and modeling complex relationships in data. However, due to the structure and the enormous number of parameters in MLPs, MLPs are not by their nature interpretable. The necessity of model interpretability means that MLP and deep learning models, including model simplification approaches, feature relevance estimators, text explanations, local explanations and model visualizations [15]. The most popular interpretability methods, however, are all local, i.e. they are based on single instances of model decisions and provide explanations for those instances individually. Current global methods, i.e. methods that summarize and describe a model, are often task-specific or not suited for deep learning models with a wide range of features. Inverse Reinforcement Learning (IRL) is a class of methods that seeks to learn the policies of trained models (experts) by inferring the reward function from demonstrations [16]. A particular subclass of IRL methods, named Adversarial Inverse Reinforcement Learning (AIRL), learns and encapsulates the reward function in the form of a discriminator that can discern expert trajectories from non-expert trajectories [17]. This discriminator is then used as an approximation for the true reward function in order to train a novice agent from scratch. The discriminator captures the training objective and induces expert-like output from the novice agent. Therefore, the discriminator is of interest from the viewpoint of interpretability because it can be utilized to explain the decision-making process of a model globally. In this work, we introduce a novel interpretability framework to provide explanations for deep reinforcement learning models. This framework leverages AIRL to generate a discriminator and then utilizes the discriminator to discover patterns and tendencies that are latent in the decision-making process of a Deep Reinforcement Learning (DRL) model. Our framework has three main contributions:

1) In contrast to existing interpretability methods, our framework provides a comprehensive global summarization of a model without focusing on a singular input.
2) Our framework, to the best of our knowledge, is the first attempt at using Inverse Reinforcement Learning to explain and interpret abstractive summarization
3) Our framework is inherently interpretable in that the explanations produced by the framework are easy to understand.
II. RELATED WORK

The field of Explainable Artificial Intelligence (XAI) is a rapidly evolving field [13]. Current methods in XAI that focus on the interpretability of machine learning models can generally be categorized as either global (i.e., summarizing the model and its behavior under different settings) or local (deciphering the process that produced the prediction for a single instance). There also exist three main popular approaches for machine learning models to attribute importance to different parts of the input.

**Gradient-based** approaches measure the amount of change around a neighborhood in the model that is necessary to induce a change in the output. The importance of features is determined through derivative calculations with respect to the input of the models [18], [19]. The popularity of this method is due to the fact that the attribution of importance to different features, which naturally lends itself to interpretability, and can be computed conveniently via backpropagation [20]. Although methods that use this approach are straightforward, they are, by definition, only local. In addition, some methods using this approach can only reproduce a subset of the original features and their corresponding relevance [21].

**Surrogate-based** approaches [22], [14], [23], [24], [25] aim to develop a secondary model that can approximate the primary model but the secondary model is constructed in a way that is more easily interpretable. Additive feature attribution methods, where features are assigned a coefficient and the approximation of the original model is calculated through a linear combination of the features and their corresponding coefficients, is a well-known and prominent surrogate-based method. It should be noted that the most popular interpretability methods used today (e.g., Local Interpretable Model-agnostic Explanations (LIME)) all utilize some combinations of gradient-based and surrogate-based approaches. Also, they are all local and do not offer a general comprehension of the model itself. Current global methods [26], [27] for these two approaches rely on decision trees and decision sets, which become difficult to utilize and interpret as the number of features in the inputs increases and the nature of inputs becomes more abstract as the case in NLP text-generation tasks.

**Perturbation-based** approaches [28], [29], [30], [31] modify certain parts of the input and use detected change in the output to assess the importance of features in the input. Although perturbation-based methods directly estimate feature importance with relative clarity, they become computationally prohibitive as the number of features in the input increases [32]. In addition, the product of perturbation-based methods is highly contingent upon the number of features that are modified in the process [33]. Finally, perturbation-based methods are usually employed in such a way that they are local to each individual instance.

Our framework is categorized as global as it does not fixate on a single instance but rather produces results that can generalize and summarize the behavior of the model as a whole. Policy extraction and summarization methods via IRL have been explored by [34], [35], and [36] before. However, none of those works were employed in the NLP domain and utilized the Adversarial method of IRL in their approaches. Our framework is also similar to surrogate-based approaches in that it works by approximating the reward function under which the expert was trained with a discriminator and mines information from this reward function. In contrast to existing global surrogate methods such as [26], [27] and [37], the rules and input-output relationships mined by our framework are easily interpretable for users even as the number of features substantially increases.

III. METHODOLOGY

Our three-step framework relies on the techniques of Reinforcement Learning, Inverse Reinforcement Learning, and Adversarial Inverse Reinforcement Learning. The detailed usages of each of them are provided below.

**A. Reinforcement Learning**

A Markov Decision Process (MDP) [38] is defined as a tuple \( M = (S, A, T, r, \gamma, \rho) \), where \( S \) and \( A \) are, respectively, the state and action spaces, \( \gamma \in (0, 1) \) is the discount factor, \( T(s', a, s) \) is the transition model that defines the conditional distribution of the next state, \( s' \), given the current state \( s \) and action \( a \), \( r(s, a) \) is the reward function that defines a reward for performing action \( a \) while in state \( s \), and \( \rho \) is the initial state distribution. Reinforcement Learning seeks to find the optimal policy \( \pi^* \), which is defined as the policy that maximizes the discounted sum of rewards [39].

\[
E \left[ \sum_{t=0}^{\infty} \gamma^t R(s_t, a_t) | \pi \right]
\]

**B. Inverse Reinforcement Learning (IRL)**

Under the same MDP \( M \) but without the reward function \( r(s, a) \), the goal of IRL is to infer the reward function \( r(s, a) \) given a set of demonstration trajectories \( D = \{ \tau_1, \ldots, \tau_N \} \). We assume these demonstration trajectories are produced by an agent operating under optimal policy \( \pi^* \) (an expert). Solving the IRL problem can be framed as solving the maximum likelihood problem:

\[
\max_{\theta} E_{\tau \sim D} [\log p_\theta(\tau)]
\]

where

\[
p_\theta(\tau) \propto p(s_0) \prod_{t=0}^{\infty} p(s_{t+1} | s_t, a_t) e^{\gamma^t r_\theta(s_t, a_t)}
\]

parameterizes the reward function \( r_\theta(s, a) \) but fixes the dynamics and initial state distribution to that of \( M \) [17].

**C. Adversarial Inverse Reinforcement Learning**

Optimizing (4) can be formulated as a generative adversarial network (GAN) [40] optimization problem with the discriminator taking the form of

\[
Disc(s, a, s') = \frac{\exp(f_{\theta,\phi}(s, a, s'))}{\exp(f_{\theta,\phi}(s, a, s') + \pi(a|s))}
\]
where \( f_{\theta, \phi}(s, a, s') = g_\theta(s, a) + \gamma h_\phi(s') - h_\phi(s) \) (5)

The discriminator is trained via binary logistic regression to discern expert data trajectories from non-expert (novice) trajectories. The output of the discriminator can be viewed as the reward for the transition from state \( s \) to state \( s' \) by taking action \( a \). The discriminator’s output rewards are then used to train the novice to be more expert-like. For details on AIRL, we refer the reader to [17] and [40].

D. Our Framework

We break down our framework (Fig. 1) into three steps:

- **Step 1:** The RL Training part of our framework involves training a model via reinforcement learning and obtaining an expert model that operates under \( \pi^* \).
- **Step 2:** The AIRL Training part of our framework involves first initializing an untrained model (which will become the novice agent) that has the same model architecture as the expert. We then utilize the AIRL algorithm to pit the expert and the novice against each other by having the discriminator discern trajectories produced by the expert from trajectories produced by the novice. The discriminator, defined in (4) by the end of this step will be able to reward expert-like behavior by generating a higher numerical output for expertlike trajectories. By the end of this step the novice will also be able to produce expert-like trajectories up to a certain level.
- **Step 3:** This step of our framework is about analyzing the discriminator’s rewards. We define a trajectory \( \tau = (s_0, a_0, s_1, a_1, \ldots, s_t, a_t) \) as a sequence of states and actions produced by a model during its prediction process for a single instance. We define \( D = \{\tau_1, \ldots, \tau_N\} \) to be trajectories of a model over all instances in the dataset. We take trajectories produced by a model (in our case, the expert model) and feed them to the discriminator to produce outputs for each \( \tau \in D \). The outputs of the discriminator over all \( D \) can then be and analyzed to capture trends and patterns in the discriminator’s reward data. Because the discriminator’s output is the reward for transitioning from state \( s \) to state \( s' \) by taking action \( a \), we can use this output to rate a model’s decisions and empirically compute aggregate information to gain an understanding over all the decisions the model has made — thus giving us a global summarization of the model’s decision-making process. Intuitively, because the novice is trained using only reward data from the discriminator, the discriminator’s output should provide valuable information regarding how the novice (or any RL model with the same architecture as the expert) prefers to transition and the underlying decision-making pattern when taking these transitions. In the following sections we describe our specific experiment and the methods we used to collect and aggregate the necessary information to find patterns for our specific dataset and application. Please note that, for a different task in a different domain, the reward analysis part will need to be adapted to gather appropriate information.

IV. EXPERIMENT

A. Dataset

The dataset we utilized in our experiment is the CNN/Daily Mail dataset introduced by [41]. A single sample in the dataset contains a news article sourced from CNN/Daily Mail and its corresponding ground truth summary. 287,113 such samples in the dataset were used for training, 13,368 samples for validation and 11,490 samples for testing.

B. Our Task

We tested our framework on an abstractive summarization task. Our expert (denoted here as \( \pi^* \) is a self-attentive model...
trained via deep reinforcement learning. Our novice model (denoted here as $\pi$) is of the same architecture as the expert but trained via AIRL. The models take as input a tokenized news article and abstractly produces a summary for that article, which we then evaluate against the human-generated ground truth summary using ROUGE [42]. We chose abstractive summarization in the NLP domain as our representative RL-based task because textual data is interesting in that each unit of datum (i.e., each word) has many characteristics to be analyzed. In our experiment, for each word, we chose to analyze its frequency of appearance, its complexity (length in characters), and its part of speech.

### C. Model Architecture and Implementation

The architectures of our expert and novice models are both encoder-decoder that employs intra-temporal attention in the encoder (bi-directional LSTM) and intra-decoder attention in the decoder (uni-directional LSTM) [43]. These mechanisms have been shown by [44] to produce good summaries that contain fewer repetitions in a DRL environment. We limit the vocabulary to 50,000 words. For each input article, at each time step $t$, our model generates probability distribution $P^t$ from which the next word in the summary is sampled. We train our expert model that is fed into the framework first with the loss function specified in the next section. For additional details on the architecture of the model and hyper parameters used during training, we refer the reader to the technical appendix in the supplementary materials.

### D. Loss Function

Our loss function during RL training incorporates the ROUGE function as part of the reward. For a given input sequence $y^{in}$, in our models output two sequences, $y^s$ and $y^g$. Sequence $y^s$ is the sequence the model produces by sampling from the distribution $P^t$ each time step $t$. Sequence $y^g$ is the sequence the model produces by greedily selecting the token that would maximize the output probability at each time step $t$. We use the ROUGE function as the reward function for output sequences and incorporate its output into our loss function. Specifically, we define the ground truth summarization for a particular sample as $y^g$ and function $R(y^g)$ as a function that returns the ROUGE score between the outputted sequence of $y^g$ and the ground truth sequence $y^g$. Our RL model’s loss function is shown in (6). During training, minimizing (6) is the same as increasing the reward expectation in (1) of our expert model.

$$\mathcal{L} = (R(y^g) - R(y^s)) \sum_{t=1}^{N} \log P^t(y^s_t|y^s_1,...,y^g_{t-1},y^{in}) \quad (6)$$

### E. Training the Novice and the Discriminator

The expert, untrained novice, and untrained discriminator are used together in the AIRL algorithm. In our application, the two functions $g_\theta$ and $h_\phi$ that make up the discriminator $f_{\theta,\phi}$ are both MLPs. The discriminator takes as input trajectories of the expert or the novice and outputs a reward for the input trajectories. For the purpose of inputting into the discriminator, we reformatted $\tau$ as defined in the Methodology section into sequences of tuples that represent actions that caused a transition of states, i.e., $\tau = ((s_0, a_0, s_1), (s_1, a_1, s_2), \ldots, (s_{T-1}, a_T, s_T))$. By the end of step 2 in Fig. 1, our discriminator can discern between expert and non-expert trajectories and correspondingly reward expert-like trajectories. We show through our experimentation that the novice is able to reproduce the expert’s trajectories up to a certain degree.

### F. Aggregate Analysis of Rewards

After training our discriminator we run the expert’s trajectories through the discriminator and obtain rewards for all trajectories in the dataset. We then take the softmax of rewards within each singular trajectory to obtain normalized rewards for each singular trajectory. For this particular task, to get a general description of our model, we calculated the most rewarding parts of speech (with two methods) and the normalized mutual information (MI) score between word characteristics and rewards, which we discuss below.

## V. RESULTS

### A. Model Evaluation

shows a summary of the results of our expert and novice models on the testing set. We also include the performance of three State-of-the-Art (SOTA) models for reference.

### B. Most Rewarding Parts of Speech

We summed up the rewards by parts of speech over all trajectories and calculated the average for each tag to find the most rewarding the POS tags. The 36 tags we use here are from The Penn Treebank [48]. We treat words that have different parts of speech as different words, i.e. (run, noun) and (run, verb) are treated as different words. We took the averages through two methods. For Method 1, we first grouped the rewards by words and divided by the number of times those words appeared before dividing by the number of times that particular parts of speech appeared. This is done to prevent words that appear more frequent from having an unfair impact on the rewards. For method 2, we forwent normalizing by the number of times those words appeared before dividing by the number of times that particular parts of speech appeared. We define the symbols below in Table

| TABLE I ROUGE SCOR ES OF MODELS ON CNN/DAILY MIL DATASE T |
|-----------------|-----------------|-----------------|-----------------|
| Model           | ROUGE-1 F1      | ROUGE-2 F1      | ROUGE-1 F1      |
| Expert          | 42.80           | 19.12           | 27.96           |
| Novice          | 14.21           | 8.23            | 8.11            |
| BART [45]       | 44.16           | 21.28           | 40.96           |
| TS [46]         | 43.52           | 21.55           | 40.69           |
| UniLMv2 [47]    | 43.16           | 20.43           | 40.34           |
TABLE II
DEFINITIONS OF SYMBOLS USED IN (7)

| Symbol | Definition |
|--------|------------|
| $S$    | the set of all parts of speech in the Penn Tree Bank |
| $D$    | the set of all expert trajectories |
| $V$    | the set of all words that appeared in $D$ |
| $n_s$  | number of times a POS $s \in S$ appeared in $D$ |
| $w_s$  | a word that has part of speech $s$ |
| $n_{w,s}$ | the number of times $w_s$ appeared in $D$ |
| $r_{w,s,\tau}$ | the total reward of $w_s$ in a trajectory $\tau \in D$ |

II. and provide equations for the two ways of averaging parts of speeches in (7).

\[
\forall s \in S \begin{cases} 
\text{Avg. Method 1} = \frac{1}{n_s} \sum_{w_s \in V} \frac{1}{n_{w,s}} \sum_{\tau \in D} r_{w,s,\tau} \\
\text{Avg. Method 2} = \frac{1}{n_s} \sum_{w_s \in V} \sum_{\tau \in D} r_{w,s,\tau}
\end{cases}
\] (7)

C. Mutual Information

Mutual Information (MI) is a measure of dependency between two variables. We calculate the normalized MI score between 3 characteristics of words and the discriminator’s rewards for transitions involving these words and present them in Table III. The 3 characteristics that we analyzed are:

- The number of appearances is the number of times the word has appeared throughout the expert-generated summaries.
- The complexity of a word is the number of letters in the word.
- The part of speech of a word. We also use the POSs from the Penn Treebank here.

VI. DISCUSSION

A. Model Evaluation

Our expert model achieved near SOTA performance and our novice model was able to reproduce the expert’s behavior up to the degree that AIRM and IRL usually perform. It is worth noting that the goal of this work is to introduce a novel interpretability framework for RL-based models rather than improving on existing SOTA abstractive summarization approaches. To that end, the presented models’ performances show the efficacy of our framework. We also would like to point out, that, although we chose to train our expert model to achieve a high performance and use the expert model for our interpretability experiment, our framework does not require a model to achieve any threshold of performance in order to explain its decisions. For our task, we found it intuitive and appealing to explain the decisions of a well-performing model.

B. Discussion of Results

We find possessive wh-pronouns, possessive pronouns, superlative adverbs, determiners, modal verbs, symbols, adverbs, singular nouns, plural nouns and wh-adverbs, in that order, to be the top 10 most rewarding parts of speech among words generated by the expert in its summaries. We show that the two different methods to calculate average rewards only make a difference on the magnitude of average rewards but do not make a difference on the ranking of most to least rewarding parts of speech. We also find a non-zero amount of dependence between the number of appearances of a word, the complexity of a word, the parts of speech of a word, and
the rewards given by the discriminator for transitions involving these words. Out of these three characteristics examined, the number of appearances of a word has the most correlation with the reward given by the discriminator for that word, followed by the word complexity and its part of speech.

C. Our Contribution to Interpretability

Our framework’s strength lies in its ability to generate summaries that explain the model’s behavior over a large set of data and be examined in the entire scope of a task. Our method instead finds global trends and patterns that underlie the model’s decision-making processes over the entire dataset. With our framework, we can make statements that do not pertain to single samples of data, but instead broadly describe the decisions of a model, such as:

- The model prefers using pronouns over nouns in writing its summaries.
- Possessive wh-pronouns are, in this dataset, the most rewarding and most preferred decisions by the model in writing its summaries.
- The complexity of a word has slightly more to do with how rewarding a word is than the word’s part of speech.

Therefore, word complexity is more influential in the model’s decision-making process than parts of speech. These global summaries are important because they help researchers gain an intuitive, qualitative and/or quantitative understanding of the model’s overall decision-making process for a specific task.

For DRL models that are not easily interpretable and tasks such as abstractive summarization for which very little amount of interpretation is usually provided, our framework can provide us with some overarching principles that guide the model in its predictions over the samples in the dataset. For models and tasks for which researchers already have an intuition or understanding on how a model should work, our framework can be applied to gauge the fidelity of the model by extracting patterns and comparing them to the established understanding. In either cases, our framework offers practical value by helping researchers and deep learning practitioners gain more confidence and trust in the utilization of their models. An IRL-based interpretability framework has yet to be adopted by the research community at large. IRL has also not been utilized widely for an abstractive summarization task. Our framework is the first attempt to utilize IRL, specifically Adversarial IRL, to tackle both problems. Through our novel framework and our experiments, we showed that IRL can be utilized to increase model interpretability and achieve promising results for abstractive summarization. In addition to abstractive summarization, our framework has the potential to be applied for model interpretability in other generative NLP tasks. We would also like to note that our framework’s output is inherently interpretable. Specifically, our framework outputs rewards for specific transitions taken by the model, which are easily understood. Although not required, with additional processing of the output rewards, we can obtain metrics and statistics that can be used to create more detailed descriptions of the model and thus increase interpretability.

D. Limitations

Popular IRL techniques can only partially achieve the performance of the expert model involved in the imitation learning process. The performance of our novice is therefore bounded by the performance of the expert and the effectiveness of IRL as a technique. We believe that although there are inherent challenges in training IRL (and GAN) models, the advantages of these techniques outweigh the difficulties. Our framework currently only helps with the interpretability of models in a task if that task can be framed as a Reinforcement Learning task. This framework would need to be expanded to fit more general tasks before achieving wide adoption for broader purposes. In addition, training the novice and the discriminator requires a large amount of data in the form of expert trajectories. Building interpretable few-shot learning models and discovering interpretability methods or frameworks with few-shot learning models remain an ongoing area of research in the field [49], [50], [51], [52], [53]. Nonetheless, our framework shows the promise of IRL in both the field of XAI as well as the field of NLP. We hope this effort motivates future work and experiments with IRL in both fields.

VII. CONCLUSION

Increased interpretability of deep learning models leads to increased confidence and trust in deep learning models, which then lead to the wider adoption of deep learning models in practice. Therefore, interpretability frameworks are of significant value and interest to the deep learning community. In this paper, we introduced a novel interpretability framework based on Adversarial Inverse Reinforcement Learning (AIRL) that can increase the interpretability of a Reinforcement Learning (RL) based model by providing global descriptions of a model. We then experimented with the framework over an abstractive summarization task. Our models achieved promising performance on the abstractive summarization task and we showed that our framework can be utilized to discover latent patterns and valuable information that help us better understand the decision-making process of these models.

VIII. ACKNOWLEDGEMENTS

We would like to thank Joseph DiPalma, Naofumi Tomita, Wayner Barrios Quiroga, Yiren Jian, Alex DeJournett, Maxwell Aladago and Timothy Daniel Irwin for their feedback on the experimental setup in this work as well as their comments during the writing of this paper.
[46] C. Raffel, N. Shazeer, A. Roberts, K. Lee, S. Narang, M. Matena, Y. Zhou, W. Li, and P. J. Liu, “Exploring the limits of transfer learning with a unified text-to-text transformer,” arXiv preprint arXiv:1910.10683, 2019.

[47] H. Bao, L. Dong, F. Wei, W. Wang, N. Yang, X. Liu, Y. Wang, J. Gao, S. Piao, M. Zhou et al., “Unilmv2: Pseudo-masked language models for unified language model pre-training,” in International Conference on Machine Learning. PMLR, 2020, pp. 642–652.

[48] M. Marcus, G. Kim, M. A. Marcinkiewicz, R. MacIntyre, A. Bies, M. Ferguson, K. Katz, and B. Schasberger, “The penn treebank: Annotating predicate argument structure,” in Human Language Technology: Proceedings of a Workshop held at Plainsboro, New Jersey, March 8-11, 1994, 1994.

[49] M. R. Zarei and M. Komeili, “Interpretable concept-based prototypical networks for few-shot learning,” 2022. [Online]. Available: https://arxiv.org/abs/2202.13474

[50] A. Asadulaev, I. Kuznetsov, and A. Filchenkov, “Linear distillation learning,” CoRR, vol. abs/1906.05431, 2019. [Online]. Available: http://arxiv.org/abs/1906.05431

[51] Y. Jian, C. Gao, and S. Vosoughi, “Embedding hallucination for few-shot language learning,” Conference of the North American Chapter of the Association for Computational Linguistics (NAACL), 2022.

[52] ——, “Contrastive learning for prompt-based few-shot language learners,” Conference of the North American Chapter of the Association for Computational Linguistics (NAACL), 2022.

[53] L. Zhang, Y. Chen, W. Wu, B. Wei, X. Luo, X. Chang, and J. Liu, “Interpretable few-shot learning with contrastive constraint,” Journal of Computer Research and Development, vol. 58, no. 12, p. 2573, 2021.