Learning Two-Step Hybrid Policy for Graph-Based Interpretable Reinforcement Learning

Tongzhou Mu ∗
Department of Computer Science and Engineering
University of California San Diego
t3mu@eng.ucsd.edu

Kaixiang Lin
Amazon
kaixianl@amazon.com

Feiyang Niu
Amazon
nfeiyan@amazon.com

Govind Thattai
Amazon
thattg@amazon.com

Reviewed on OpenReview: https://openreview.net/forum?id=OzStmhFBrc

Abstract

We present a two-step hybrid reinforcement learning (RL) policy that is designed to generate interpretable and robust hierarchical policies on the RL problem with graph-based input. Unlike prior deep reinforcement learning policies parameterized by an end-to-end black-box graph neural network, our approach disentangles the decision-making process into two steps. The first step is a simplified classification problem that maps the graph input to an action group where all actions share a similar semantic meaning. The second step implements a sophisticated rule-miner that conducts explicit one-hop reasoning over the graph and identifies decisive edges in the graph input without the necessity of heavy domain knowledge. This two-step hybrid policy presents human-friendly interpretations and achieves better performance in terms of generalization and robustness. Extensive experimental studies on four levels of complex text-based games have demonstrated the superiority of the proposed method compared to the state-of-the-art.

1 Introduction

Recent years have witnessed the rapid developments of deep reinforcement learning across various domains such as mastering board games Silver et al. (2016); Schrittwieser et al. (2020) playing video games Mnih et al. (2015), and chip design Mirhoseini et al. (2021), etc. The larger and complicated architecture of deep reinforcement learning models empowered the capabilities of resolving challenging tasks while brought in significant challenges of interpreting the decision making process of those complex policies Punetta & Veith (2020). This trade-off between performance and interpretability becomes an inevitable issue when DRL is applied to high stakes applications such as health care Rudin (2019). In this work, we focus on graph-based interpretable reinforcement learning Zambaldi et al. (2018); Waradpande et al. (2020) as the graph representation is expressive in various domains including drug discovery Patel et al. (2020), visual question answering Hildebrandt et al. (2020), and embodied AI Chaplot et al. (2020); Huang et al. (2019), etc. Especially in robotics and embodied AI, the scene graph Zhou et al. (2019) of the environment is a general representation, which is widely used not only in building the environment Puig et al. (2020); Kolve et al. (2017), but also very effective when building the planning module Jia et al. (2022); Min et al. (2021).

∗Work done during an internship at Amazon Alexa AI.

1
Another benefit of studying graph-based RL is that the graph structure can provide natural explanations of the decision-making process without the necessity of introducing new programs or heavy domain knowledge for interpretation. Prior works in interpretable reinforcement learning either work on restricted policy class that leads to downgraded performance, or the interpretability is limited. Another common issue of interpretable RL is that the provided explanation is generally difficult to comprehend for non-experts.

In this work, we seek to obtain a human-understandable interpretation for the decision making process in graph-based tasks. To better illustrate the desired interpretability in graph-based tasks, we borrow the ideas from the visual recognition community, where people interpret how CNN works by analyzing which region gets the most attention. Similarly, in graph-based tasks, we want to figure out the most crucial sub-graphs (or edges) used in decision making.

We refer to this kind of interpretation as “interpretability” in graph-based RL, not only because this kind of “interpretability” is similar to the one in the visual recognition community, but also because it is easily understood by humans. A crucial sub-graph also has several desirable characteristics of explanation defined by Molnar (2020), e.g., it is contrastive and selected.

To obtain the desired interpreability and resolve the challenges mentioned above, we propose a novel two-step hybrid decision-making process for general deep reinforcement learning methods with graph input. Our approach is inspired by the observation of human decision-making. When confront complicated tasks that involve expertise from multiple domains, we typically identify which domain of expert we would like to consult first and then search for specific knowledge or solutions to solve the problem. Recognizing the scope of the problem significantly reduces the search space of downstream tasks, which leads to a more simplified problem compared to find the exact solution in all domains directly. As an analogy of this procedure, we disentangle a complicated deep reinforcement learning policy into a classification the problem for problem type selection and rule-miner. The classification establishes a mapping from complex graph input into an action type, which handles high-order logical interactions among node and edge representations with graph neural network. The rule miner conducts explicit one-hop reasoning over the graph and provides user-friendly selective explanations by mining several decisive edges. This two-step decision making is essential not only for providing interpretability, but also for generalization and robustness. It is intuitive to see that the simplified classification is easier to achieve better generalization and robustness than the original complicated RL policy. Furthermore, the rule-miner identifying key edges in the graph is much more robust to the noisy perturbations on the irrelevant graph components.

Our contributions can be summarized as below:

- We propose a general framework for two-step hybrid decision making, which is able to combine neural network and rule-based method together to make a decision while yielding human-friendly interpretations.
- We instantiate our proposed framework in the setting of text-based games with graph input by proposing a novel rule miner for knowledge graphs.
- Extensive experiments on several text-based games demonstrated that the proposed approach achieves a new state-of-the-art performance for both generalization and robustness.

2 Related Works

2.1 Interpretable RL

Instead of using deep RL as a black box, researchers also worked on making deep RL more interpretable. Mott et al. (2019) and Zambaldi et al. (2018) introduce some sorts of attention mechanism into policy networks. The idea of the crucial sub-graph is also similar to the crucial point set used in PointNet, which is essentially a graph neural network.
and explain decision making process by analyzing attention weights. Verma et al. (2018) combines program synthesis and PIDs in classic control to solve continuous control problems, while keep the decision making interpretable by explicitly writing the program. Combining symbolic planning and deep RL has similar effects, like Lyu et al. (2019). Tree-based policies Bastani et al. (2018) are favorable in interpretable RL, since they are more human-readable and easy to verify. Bonaert et al. (2020) introduces goal-based interpretability, where the agent produces goals which show the reason for its current actions. However, many existing works of interpretable RL sacrifices the performance for the interpretability. In contrast, our method achieves even better generalization and robustness while providing interpretability.

2.2 Hierarchical RL

Hierarchical RL focuses on decomposing a long-horizon tasks into several sub-tasks, and applying a policy with hierarchical structure to solve the task. Vezhnevets et al. (2017); Frans et al. (2018) try to solve generic long-horizon tasks with a two-level policy, where a high-level policy will generate a latent sub-goal for low-level policies, or directly select a low-level policy, and the low-level policy is responsible for generating the final action. In some robot locomotion tasks, people usually manually define the choices of sub-goals to boost the performance and lower the learning difficulty, like Nachum et al. (2018); Levy et al. (2018). In Multi-agent RL, hierarchical structure is a commonly adopted policy structure to provide certain interpretability Gupta et al. (2021); Mahajan et al. (2019); Wang et al. (2020). However, those approaches can not explain how specific decision is associated with the state space as their low-level policy is still a black box policy. Our two-step hybrid policy is reminiscent of the two-level policy architecture in hierarchical RL. Unlike the high-level policy in hierarchical RL is mainly used to generate a sub-goal, the action pruner in our hybrid policy is also used to reduce the number of action candidates. And the motivations of our method and hierarchical RL are also different: hierarchical RL targets at decomposing a long-horizon tasks into several pieces, but our method focuses on interpretability, generalizability and robustness.

2.3 Refactoring Policy

Given a trained neural network-based policies, one may want to refactor the policy into another architecture, so as to improve the generalizibility or interpretability. And this refactoring process is usually done by imitation learning. The desired architectures of the new policy can be decision tree Bastani et al. (2018), symbolic policy Landajuela et al. (2021), a mixture of program and neural networks Sun et al. (2018), a graph neural networks Mu et al. (2020), or a hierarchical policy Bonaert et al. (2020). In our method, we also use similar techniques to refactor a reinforcement learning policy into a two-step hybrid policy.

2.4 Combine Neural Networks with Rule-Based Models

Neural networks and rule-based models excel at different aspects, and many works have explored how to bring them together, like Chiu et al. (1997); Goodman et al. (1990); Ray & Chakrabarti (2020); Okajima & Sadamasa (2019); Greenspan et al. (1992). There are various ways to combine neural networks with rule-based models. For example, Wang (2019) combines them in a "horizontal" way, i.e., some of the data are assigned to rule-based models while the others are handled by neural networks. In contrast, our work combines neural networks and rule-based models in a "vertical" way, i.e., the two models collaborate to make decisions in a two-step manner.

3 A General Framework for Two-Step Hybrid Decision Making

In this section, we first describe our problem setting including key assumptions and a general framework that formulates the decision-making process in a two-step manner.

We consider a discrete time Markov Decision Process (MDP) with a discrete state space $\mathcal{S}$ and the action space $\mathcal{A}$ is finite. The environment dynamics is denoted as $P = \{p(s'|s,a), \forall s,s' \in \mathcal{S}, a \in \mathcal{A}\}$. Given an action set $\mathcal{A}$ and the current state $s_t \in \mathcal{S}$, our goal is to learn a policy ($\pi$) that select an action $a_t \in \mathcal{A}$ to maximize the long-term reward $E_\pi[\sum_{t=1}^{T} r(s_t, a_t)]$. Assume we are able to group the actions into
several mutual exclusive action types \( (A_k) \) according to its semantic meanings. More concretely, the \( k \)-th action type \( A_k = \{a_{k1}, \ldots, a_{kn} \} \) denotes a subset of actions in original action space \( A_k \subseteq A \). Then we have \( A_1, A_2, \ldots, A_K \subseteq A, A_i \cap A_j = \emptyset (i \neq j), \bigcup_{i=1}^{K} A_i = A \). It is worth noting that the number of action type \( K \) is usually much smaller than original actions \( (K \ll |A|) \).

Let the policy \( \pi = (f_p, f_s) \) represented by a hybrid model that consists of action pruner \( f_p \) and action selector \( f_s \). The action pruner is used to prune all available action candidates to a single action type, i.e., \( f_p(s_i) = k \), where \( k \) is the index of chosen action type and \( A_k \in \{A_1, A_2, \ldots, A_K \} \). Then the action selector is used to select a specific action given the action type chosen by the action pruner, i.e., \( f_s(s_i, A_k) = a_i \), where \( a_i \in A_k \) and \( k = f_p(s_i) \).

Intuitively, this design intends to disentangle different phases in decision-making process to two different modules. On the one hand, determining the action type typically involves high-order relationships and needs a model with strong expressive power, then neural network is a good candidate in this regard. On the other hand, selecting an action within a specific action type can resort to rule-based approaches, which is essential in providing strong interpretablility, generazability and robustness.

Figure 1 shows the overall pipeline of our two-step hybrid decision making. The agent will receive a state \( s_i \) at each time step \( i \). At time step \( i \), we will first call the action pruner \( f_p(s_i) \) to select the action type \( A_k \). Then the rule-based action selector \( f_s(s_i, A_k) \) will take as inputs the current state \( s_i \) and the action type \( A_k \) given by action pruner to select the specific action to be executed in this step.

Figure 1: Overall pipeline of the two-step hybrid decision making.

4 Two-Step Hybrid Policy for Text-Based Games with Graph Input

4.1 Overview

In this section, we first discuss our considerations for investigating the interpretability of graph-based tasks and the reasons for using text-based games as our testbed. Firstly, graph is a powerful data structure, and it has been widely adopted in many real-world applications such as drug discovery [Patel et al. (2020), visual question answering [Hildebrandt et al. (2020)], and embodied AI [Chaplot et al. (2020), Huang et al. (2019)], etc. Meanwhile, the discrete nature and the explicit semantic meaning of graphs (e.g., the relationship of related nodes) provide an easily understandable format for elaborating the decision-making process even for a non-expert. However, the interpretability of graph-based RL tasks is still rarely explored. On the other hand, it is challenging to provide interpretability without any assumption on the action space, even for graph-based RL. We focus on tasks with hierarchical/compositional action spaces as a starting point, which is a common setting in embodied AI. Considering the text-based scene graph has been a general representation of embodied AI tasks [Shridhar et al. (2020)], we instantiate our proposed framework in the setting of text-based games [Côté et al. (2018)] with graph input. In text-based games, the agent receives a knowledge graph (as shown in Figure 3) that describes the current state of the environment and the task to be completed, e.g., the task can be represented by several edges like (‘potato’, ‘needs’, ‘diced’). Our goal is to learn a policy that maps the input knowledge graph to an action from the provided action set \( A \). Each action \( a_i \in A \) is a short sentence, e.g., “take apple from fridge”.

In this setting, we use graph neural networks (GNNs) as the action pruner \( f_p \), and a rule-based model as the action selector \( f_s \). We will elaborate the details of the action pruner and the action selector in Sec 4.4 and Sec 4.5 respectively. A brief description of GNNs can be found in Sec 4.2.
Training the GNN-based action pruner and the rule-based action selector by reinforcement learning is nontrivial since the whole pipeline is not end-to-end differentiable. Therefore, we propose to learn both models separately from a demonstration dataset, and the demonstration dataset can be obtained by a trained reinforcement learning agent. We will elaborate the details in Sec 4.3.1. This process is inspired by existing works like Bastani et al. (2018); Landajuela et al. (2021); Sun et al. (2018); Mu et al. (2020), where policies trained by reinforcement learning can be refactorized into other forms.

4.2 Backgrounds on Graph Neural Networks

We briefly describe a commonly used class of GNNs that encompasses many state-of-art networks, including GCN (Kipf & Welling (2016), GAT (Veličković et al. (2017), GIN (Xu et al. (2018), etc. The class of GNNs generalizes the message-passing framework (Gilmer et al. (2017) to handle edge attributes. Each layer of it can be written as

$$h_{v}^{l+1} = f_{\theta}^{l}(h_{v}^{l}, \{x_{e} : e \in \mathcal{N}_{E}(v)\}, \{h_{v'}^{l} : v' \in \mathcal{N}_{V}(v)\})$$

, where $h_{v}^{l}$ is the node feature vector of node $v$ at layer $l$, $\mathcal{N}_{V}(v)$ and $\mathcal{N}_{E}(v)$ denote the sets of nodes and edges that are directly connected to node $v$ (i.e. its 1-hop neighborhood). $f_{\theta}^{l}$ is a parameterized function, which is usually composed of several MLP modules and aggregation functions (e.g. sum/max) in practice.

4.3 Preparing Datasets for Learning Two-Step Hybrid Policy

4.3.1 Demonstration Acquisition

Given a set of interactive training environments, the goal of this step is to obtain a demonstration dataset, which contains state-action pairs from a policy achieving high reward in the training environment. Specifically, we aim at generating a demonstration dataset $D = \{(s_{i}, \pi(s_{i}))\}_{i=1}^{N}$, where $s_{i}$ is the input state (a knowledge graph in our cases) from the training environments, and $\pi(s_{i})$ is the output of demonstration policy on the state $s_{i}$. The representation of $\pi(s_{i})$ is flexible: it can be an action, the logits, or any latent representation, which indicates the demonstration action distribution. This dataset will be used for learning our two-step hybrid policy.

We refer the policy used to generate demonstration as teacher policy. It can be obtained in any way, as long as it provides reasonable and good supervision on how to solve the task in the training environments, and it is not necessary to have strong interpretability, generalizability or robustness. Therefore, deep reinforcement learning is a great tool to learn such a policy.

After obtaining the teacher policy, we use it to interact with the training environments to collect states and label them with the output of the teacher policy. During the interaction, we add action noise to perturb the state distribution in the demonstration dataset. A more diversified state distribution is beneficial to the performance of our two-step hybrid approach.

4.3.2 Action Grouping and Demonstration Splits

As mentioned above, the action pruner is responsible for selecting the correct type of actions for the current state, so that the action candidates will be pruned to a smaller set. Then, a rule-based model will work on this specific action type to select the action to be executed. Therefore, we need to label each state with the action type. Since the action for each state is already in the dataset, we just need to convert each action into an action type. In other words, we need to group all possible actions into several action types.

In text-based games, each action is a short sentence with semantic meaning, e.g., “take apple from fridge”. Intuitively, we can group the actions by their semantic meaning. For example, if the actions are “take apple from fridge”, “slice potato with knife”, “dice cheese with knife”, “cook carrot with oven”, and “cook onion with stove”, we can group them into three types: “take” actions, “cut” actions, and “cook” actions. And we make sure all the actions with the same action type follow the same template, e.g., the template of “take” action can be written as “take object from receptacle”, where object and receptacle can be instantiated by appropriate words.
Grouping actions by semantic meanings also aligns with our motivation: 1) After we obtained $K$ group of actions, we substantially alleviate the workload of neural networks from learning a policy that maps states to an action in a varying size and high-dimensional action space to a simplified classification with a much smaller number of classification categories. This simplification could greatly reduces the sample-complexity. 2) Furthermore, this step also creates a much smaller search space to enable the rule-miner to search within a feasible candidates set.

Formally, given a dataset $\mathcal{D} = \{(s_i, \pi(s_i))\}_{i=1}^{N}$, we will generate an action type for each state, policy output $(s_i, \pi(s_i))$ pair. The action type $k_i$ is determined by $k_i = h(\pi(s_i))$, where $h(\pi(s_i))$ is a domain-specific function which takes the semantic meaning of the action into consideration. As a result of the clustering process, we will get a new demonstration dataset with action types $\mathcal{D} = \{(s_i, \pi(s_i), k_i)\}_{i=1}^{N}$. In addition, we can also split the demonstration dataset based on the action types to get $K$ subset of the original demonstration dataset, $\mathcal{D}_1, \mathcal{D}_2, ..., \mathcal{D}_K$, where $\mathcal{D}_k = \{s_i, \pi(s_i)|h(\pi(s_i)) = k\}$.

### 4.4 GNN-based Action Pruner

The action pruner needs to output an action type based on the input knowledge graph, so it is essentially a classifier. Given the demonstration dataset $\mathcal{D} = \{(s_i, k_i)\}_{i=1}^{N}$ obtained in the last step, we want to train a classifier $f_\theta(s; \theta) = k$, where $k \in \{1, 2, ..., K\}$ is an action type. This is a conventional classification problem which can be solved by minimizing cross entropy loss:

$$
\theta = \arg \min \theta \sum_i \sum_j k_i^j \log(f_\theta^j(s_i)),
$$

where $f_\theta(s_i)$ outputs a probability distribution over the $K$ action types, $f_\theta^j(s_i)$ denotes the $j$-th action type’s probability. $k_i^j \in \{0, 1\}$ denotes denotes whether the action type $j$ was chosen in the demonstration dataset at state $i$.

### 4.5 Rule-Based Action Selector

#### 4.5.1 Abstract Supporting Edge Sets

When the input is a knowledge graph, the action is naturally strongly correlated with some critical edges. For example, (“potato”, “needs”, “diced”) and (“potato”, “in”, “player”) can lead to the action “dice potato”. We refer those decisive edges correlating to an action as the abstract supporting edge set. The abstract supporting edge set indicates the decisive edges for an action type, and it can be instantiated for each specific action. For example, to check whether the action “dice apple” should be executed, the abstract edge (“object”, “in”, “player”) will be instantiated to edge (“apple”, “in”, “player”). Then, the existence of (“apple”, “in”, “player”) in input knowledge graph becomes an evidence for selecting the action “dice apple”. We aim at finding an abstract supporting edge set for each action type, and it will be used during inference.

#### 4.5.2 Mine Abstract Supporting Edge Sets from Demonstrations

Finding the abstract supporting edge set for each action type is actually a rule mining process. There are several off-the-shelf rule miners like FP-Growth [Han et al. 2004], Apriori Agrawal et al. [1994], Eclat Zaki.
Figure 2: An example of using supporting edge set to score an action. Based on the knowledge graph, the action pruner first predict the action type (e.g., cook) that needs to be taken at current state, then instantiate the abstract supporting edge set to a concrete supporting edge set. Comparing the input knowledge graph with the supporting edge set, we can compute action score for each action and select the action with highest score accordingly.

To find the Abstract Supporting Edge set $ASE(A_k)$ for each action type $A_k$, we designed a numerical statistic that is intended to reflect the importance of an edge when taking an action $a \in A$, and this numerical statistic is inspired by tf-idf [Rajaraman & Ullman (2011)]. Formally, for action type $A_k$, we have a corresponding subset of demonstration dataset $D_k = \{s_i\}$ (ignoring $\pi_i$ here) where all the actions are within the action type $A_k$. Under the abstraction mentioned above, we can count the edge frequency for every (abstract) edge $e$ in $D_k$:

$$freq_k(e) = \frac{|\{s_i|s_i \in D_k, e \in s_i\}|}{|D_k|}.$$  

Similarly, we can also count the edge frequency for the entire demonstration dataset:

$$freq(e) = \frac{|\{s_i|s_i \in \mathcal{D}, e \in s_i\}|}{|\mathcal{D}|}.$$  

And we can define an importance score of an edge w.r.t to the action type $A_k$:

$$I_k(e) = freq_k(e) \cdot \log\left(\frac{1}{freq(e)}\right),$$

where the term $freq_k(e)$ is similar to the term-frequency (tf), and the term $\log\left(\frac{1}{freq(e)}\right)$ is similar to the inverse document frequency (idf).

Then we can get the $ASE(A_k)$ by selecting the edges with the importance higher than a threshold, i.e., $ASE(A_k) = \{e|I_k(e) > \tau\}$, where $\tau$ is a hyperparameter shared across all action types.
4.5.3 Inference Based on Supporting Edges

During inference, we use the supporting edge sets to score each action within the action type provided by action pruner, and select the action with the highest score. Figure 2 shows a concrete example of using supporting edge set to score an action.

Firstly, the action pruner outputs an action type based on the input knowledge graph, and we can retrieve the abstract supporting edge set of this action type. Secondly, given an action within the action type, we can instantiate the abstract supporting edge set to a specific supporting edge set by replacing the abstract names by the concrete words according to the action, e.g, (“object”, “in”, “player”) will be instantiated to (“potato”, “in”, “player”) if the action is “cook potato with oven”. Finally, we can compare the input knowledge graph with the supporting edge set of each action to figure out which supporting edge set is best covered by the input knowledge graph. The number of overlapped edges between the supporting edge set and the input knowledge graph will be regarded as the score of the action.

Formally, the inference process of our rule-based action selector can be described as follows

\[ f_s(s, A) = \arg \max_{a \in A} |s \cap \text{SE}(a)|, \]

where \( \text{SE}(a) \) is the supporting edge set associated with action \( a \), which is obtained by instantiating the abstract supporting edge set of action type \( A \).

5 Experiments

5.1 Dataset Setup

<table>
<thead>
<tr>
<th>Difficulty Level</th>
<th>Recipe Size</th>
<th>Number of Locations</th>
<th>Need Cut</th>
<th>Need Cook</th>
<th>Number of Action Candidates</th>
<th>Number of Objects</th>
<th>Number of Sub-tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>No</td>
<td>11.5</td>
<td>17.1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>11.8</td>
<td>17.5</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>9</td>
<td>No</td>
<td>No</td>
<td>7.2</td>
<td>34.1</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>6</td>
<td>Yes</td>
<td>Yes</td>
<td>28.4</td>
<td>33.4</td>
<td>11</td>
</tr>
</tbody>
</table>

Table 1: TextWorld games statistics (averaged across all games within a difficulty level). The games and statistics are generated by Adhikari et al. (2020).

We evaluate our method on TextWorld, which is a framework for designing text-based interactive games. More specifically, we use the TextWorld games generated by GATA Adhikari et al. (2020). In these games, the agent is asked to cook a meal according to given recipes. It requires the agent to navigate among different rooms to locate and collect food ingredients specified in the recipe, process the food ingredients appropriately, and finally cook and eat a meal.

The state received by the agent is a knowledge graph describing all the necessary information about the game. All the nodes and edges in the knowledge graph are represented in text. Figure 3 shows a partial example of input knowledge graph. The actions are also represented in text. Note that the number of available actions vary from state to state, so most of of existing network architecture used deep reinforcement learning cannot be directly used here.

The games have four different difficulty levels, and each difficulty level contains 20 training, 20 validation, and 20 test environments, which are sampled from a distribution based on the difficulty level. The higher the difficulty levels are, the more complicated recipe will be and the more rooms food ingredients will be distributed among. For easier games, the recipe might only require a single ingredient, and the world is limited to a single location, whereas harder games might require an agent to navigate a map of six locations to collect and appropriately process up to three ingredients. Statistics of the games are shown in Table 1. For evaluating model generalizability, we select the top-performing agent on validation sets and report its test scores; all validation and test games are unseen in the training set.
5.2 Implementation Details

5.2.1 Process Knowledge Graphs by GNNs

Graph neural networks (GNNs) serve as backbone networks in both our RL teacher policy and the action pruner in our two-step hybrid policy. More specifically, we use the Relational-GCN to take edge attributes into consideration, and the Relational-GCN is also the backbone architecture used in GATA Adhikari et al. (2020), which is the baseline method in the TextWorld games we used. Actually, the choice of the network architecture is not very important in our method. This is because both the RL teacher policy and the action pruner are only used to fit the training environments or the demonstration dataset. We did not really expect them to have strong interpretability, because this is the job of the rule-based action selector. Therefore, most graph-based networks with sufficient capacity should be good in our cases. We will also perform an ablation study about network architecture in Sec. 5.4.

The relations and nodes of the input knowledge graphs are initially represented in text (words or short sentences). We use fastText Mikolov et al. (2017), pre-trained on Common Crawl, to convert each token to an embedding, and then average all the token embeddings to obtain the mean fastText embedding of the entire text string. These mean fastText embeddings are pre-computed and fixed during training. For each relation and node, we append their corresponding mean fastText embedding with a trainable embedding vector. The concatenated embeddings are then used as the numerical representation of each relation and node. Finally, a graph with numerical node/relation features is passed through GNNs to get the latent embedding of the entire input knowledge graph.

5.2.2 Demonstration Acquisition

To collect demonstration dataset, we first train a teacher policy by DQN Mnih et al. (2015) in the training environments, which can converge to a near-optimal solution. To adopt variable number of available actions, we let the policy network take the state and an available action as input and output a score for this action. And we can select the action with maximum score as the final output.

The trained teacher policy is used to collect 300K samples through the interaction with the environment, and label them with the taken actions, as illustrated in Sec 4.3.1. When collecting the demonstration dataset, we use $\epsilon$-greedy exploration strategy to increase the diversity of states.

5.3 Results

5.3.1 Interpretability

The interpretability of our two-step policy is two-fold: 1) the transparent two-step decision making process; 2) the rule-based models make decisions in a way which is easy to interpret by human.

Table 2 shows some representative rules discovered by our rule miners. We observed that all of the four discovered abstract supporting edges are indeed prerequisites of the “cut” actions. In particular, the abstract supporting edge (“object”, “needs”, “verb_passive”) is a crucial prerequisite for the agent to select the correct verb in the “cut” actions. For example, if the input knowledge graph contains the edge (“potato”, “needs”, “sliced”), then the action “slice potato with knife” will get one more score than others because this edge is in the supporting edge set of action “slice potato with knife.”
Table 2: Discovered abstract supporting edges of the “cut” action type in difficulty level 1 of TextWorld environments. The importance of each edge is computed by the metric mentioned in Sec 4.5.2. The right column gives an example action and the corresponding supporting edge set, which is obtained by instantiating the abstract supporting edge set. The underlined words are abstract names for some certain words. For example, “verb” in action can be instantiated to “slice”, “dice” or “chop”, and “verb_passive” can be instantiated to “sliced”, “diced” or “chopped” accordingly.

Since we clearly see the rule-based model makes decisions based on these rules, it is not hard to check whether this model works in a correct way. In this way, the agent can certainly select the correct “cut” action even in unseen test environments.

5.3.2 Generalization

Table 3: Evaluation results on both training environments and test environment in TextWorld. The numbers show the agent’s normalized scores.

We compare with two baselines: GATA-GTF and vanilla RL. GATA-GTF is a variant from GATA [Adhikari et al. (2020)], and it uses the same ground-truth graph input as us. GATA-GTF processes the input graphs by relational graph convolutional networks (R-GCNs) [Schlichtkrull et al. (2018)], and the whole pipeline is trained by DQN [Mnih et al. (2015)]. Vanilla RL is essentially the same method with GATA-GTF, but implemented by ourselves. With better implementation and careful hyperparameter tuning, it performs better than the implementation released by the GATA authors. And vanilla RL also serves the teacher policy which used to generate demonstrations for our method.

Table 3 shows the normalized scores of different methods on both training environments and test environment in TextWorld. The result of GATA-GTF is obtained from its paper [Adhikari et al. 2020]. In all the environments, our agent achieves better generalization performance the vanilla RL (which is our RL teacher) and GATA-GTF baselines. Our agent can generalize pretty well to the unseen test environments in all difficulty levels, while the performance of GATA-GTF and vanilla RL performs poorly in unseen test environments.

5.3.3 Robustness

As mentioned above, our method also aims at robustness. To evaluate the robustness of our models, we add different levels of noises to input knowledge graphs and regard the performance of the agents under noisy inputs. In this paper, we define the noise on a knowledge graph as adding additional edges to the graph or dropping existing edges in the graph. Formally, we add noise at \((k, p)\)-level to input knowledge graph in the following way:
Table 4: Robustness analysis of our method and vanilla RL baseline. We evaluate the performance of agents on training environments under different noise levels, e.g., “add 0.2 drop 0.03” means we randomly add 20% additional edges while randomly dropping 3% existing edges in the graph. The numbers out of parentheses are normalized scores and the numbers in parentheses are relative performance change comparing to the performance without input noise. The bold numbers indicate which method performs better in each setting.

1. Add edges: ⌈k * |E|⌉ additional edges will be randomly generated and added to the graph, where E is the edge set of the graph. For each edge hi,t,i, head node hi and tail node ti are sampled from V_all and relation ri is sampled from R_all, where V_all means the set of all possible nodes and R_all is the set of all possible relations.

2. Drop edges: ⌈p * |E|⌉ edges will be dropped from the graph. Note that only original edges will be dropped, and the randomly added edges will not be dropped.

Table 4 shows the performance of vanilla RL and our method under noisy input graphs generated in the above mentioned way. Note that we test robustness in training environments instead of test environments, because the performance of both agents in test environments are not good enough and examining robustness of poor-performed agents does not make too much sense.

We observed that in difficulty level 1, both agents are very robust under the noisy inputs. However, in difficulty level 2 & 3 & 4, the performance of the RL agents are hurts a lot by the input noises, especially in the difficulty level 4. In contrast, the agents obtained by our method are still performs pretty good and the performance drops significantly less than the RL agents.

5.4 Ablation Study

In this section, we study the contributions of different modules in our method. Our proposed method mainly consists of three modules: 1) an RL teacher policy, 2) a GNN-based action pruner, 3) a rule-based action selector. Therefore, we replace each module with other alternatives and see how the generalization performance is influenced. All the experiments below are performed on the TextWorld games with difficulty level 1.

5.4.1 RL teacher policy

We first study how different kinds of teacher policies affects the performance. We consider the following three alternatives to our RL teacher policy: 1) an RL teacher policy with different backbone network: Graph Transformer Network (GTN) [Yun et al., 2019]; 2) a manually written ground truth policy which can perfectly solves the tasks; 3) a random policy. Note that we choose ground truth policy and random policy as teachers because they represent two extreme cases: a very good teacher and a very bad teacher.

Table 5 shows the results of this ablation study. From this table, we can observe the following things:
Table 5: Evaluation results on both training environments and test environment in TextWorld difficulty level 1. The numbers show the agent’s normalized scores.

- It does not make much difference by switching the backbone of the RL teacher policy from GCN to GTN. This verifies our expectation: any graph-based network should be good as long as it has sufficient capacity for the training environment / data, because the job of the RL teacher is only to provide a demonstration dataset.

- Using ground truth policy also does not really affect the performance of our method. Since our RL teacher policy actually achieves almost perfect performance on the training environments, the demonstrations generated by our RL teacher and the ground truth policy are almost equally good.

- Using a random policy does not work at all. This also meets our expectation that a good demonstration dataset is very important for learning the action pruner and the rule-based action selector.

5.4.2 GNN-based action pruner

In this section, we mainly assess the influences of the network architectures used in the GNN-based action pruner. Specifically, we replace the backbone of our action pruner with Graph Transformer Network (GTN) [Yun et al. 2019]. And we also study the case where the RL teacher also uses GTN as the backbone.

Table 6: Evaluation results on both training environments and test environment in TextWorld difficulty level 1. The numbers show the agent’s normalized scores.

From the Table 6, we can see that the architecture changes have minimal influence on the performance. This verifies our expectation again: any graph-based network should be good as long as it has sufficient capacity for the training environment / data. Though the “GTN teacher, GTN action pruner” variant does not get full scores on the training environment, the performance gap is very small.

5.4.3 Rule-based action selector

Finally, we study whether a rule-based action selector is crucial by replacing it with a network-based action selector. The resulting policy is somehow like a mixture of experts, where the gating function and the experts are all networks.

Table 7: Evaluation results on both training environments and test environment in TextWorld difficulty level 1. The numbers show the agent’s normalized scores.
From the Table 7, we can see that the network-based action selector does a good job in the training environments but performs poorly on the test environments. This is because the network-based action selector overfits the training data instead of really learning the underlying rules of decision making. In contrast, our rule-based action selector learns the real underlying rules that generalize well. Therefore, the rule-based action selector is a crucial component of our method.

6 Conclusion

In this work, we propose a two-step hybrid policy for graph-based reinforcement learning. The two-step hybrid policy disentangles complicated black-box deep reinforcement learning policy into an action pruner and an action selector. The joint effort of two modules can not only generate human-friendly explanations of each decision, but also provide significantly better performance in terms of generalization and robustness. We conduct comprehensive experiments on the representative text-based environments Côté et al. (2018) to demonstrate the effectiveness of our approach.
References


Jiawei Han, Jian Pei, Yiwen Yin, and Runyong Mao. Mining frequent patterns without candidate generation: A frequent-pattern tree approach. *Data mining and knowledge discovery*, 8(1):53–87, 2004.


