

Explaining Reward Functions to Humans for Better Human-Robot Collaboration

Lindsay Sanneman and Julie A. Shah

CSAIL, Massachusetts Institute of Technology
lindsays, julie_a_shah@csail.mit.edu

Abstract

Explainable AI techniques that describe agent reward functions can enhance human-robot collaboration in a variety of settings. One context where human understanding of agent reward functions is particularly beneficial is in the value alignment setting. In the value alignment context, an agent aims to infer a human’s reward function through interaction so that it can assist the human with their tasks. If the human can understand where gaps exist in the agent’s reward understanding, they will be able to teach more efficiently and effectively, leading to quicker human-agent team performance improvements. In order to support human collaborators in the value alignment setting and similar contexts, it is first important to understand the effectiveness of different reward explanation techniques in a variety of domains. In this paper, we introduce a categorization of information modalities for reward explanation techniques, propose a suite of assessment techniques for human reward understanding, and introduce four axes of domain complexity. We then propose an experiment to study the relative efficacy of a broad set of reward explanation techniques covering multiple modalities of information in a set of domains of varying complexity.

Introduction

Effective explainable AI systems are critical to constructive human-robot collaboration in a variety of settings. Humans performing separate roles in distinct contexts require different types of information about their AI teammates in order to effectively perform their tasks (?). One context in which explainable AI is particularly important is the value alignment setting in which a human and an autonomous agent work together to maximize some reward, but only the human knows the true reward function (??). Through interaction, the agent infers the reward in order to become a better collaborator. It is ideal for the human to behave “pedagogically” in this circumstance, taking actions that best teach the agent about the true reward, but this requires the human to track the agent’s beliefs about the reward over the course of the interaction (?). This might be difficult or intractable in some settings given human cognitive limitations. Therefore, enabling an agent to provide feedback to a human about its current understanding of the reward function, as depicted in Figure 1, could be of value.

Copyright © 2021, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.

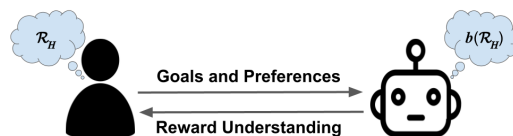


Figure 1: Bidirectional Communication for Value Alignment

In order to understand how to best explain agent reward functions in a value alignment setting, it is first important to understand which approaches for explaining reward functions are most effective in which contexts. To our knowledge, no comprehensive study comparing reward explanation techniques in different types of domains has previously been performed. In addition, no comprehensive way of assessing human reward understanding has been proposed. In this paper, we first outline two overarching categories of reward explanations and a subset of explanation modalities within each category. We then suggest a suite of assessment techniques and metrics for human reward understanding, define a set of axes characterizing domain complexity, and discuss a planned human subject experiment designed to better understand which modalities of reward explanations are most effective in domains of varying complexity. We scope this work to consider human understanding of linear reward functions in particular.

Related Work

Previous works have studied the efficacy of a variety of explanation techniques through human subject experiments in different settings. For example, ? assessed whether human participants could identify optimal versus satisficing plans after receiving explanations intended to reconcile their models with a robot’s. The authors also asked post-hoc Likert scale questions about whether the explanations were helpful and easy to understand and whether participants were satisfied with the explanations. In another experiment, ? asked Likert scale-based questions about the helpfulness, sociability, and intelligence of a robot that provided explanations about its reward function to human participants. ? further assessed human-agent team performance, the percentage of correct human decisions, and a human’s understanding of an agent’s decisions given explanations related to the dif-

ferent components of the agent’s POMDP-based representation of a task. Finally, ? measured a person’s understanding of explanations of various sizes and that provided different types of information using a combination of assessment techniques including simulation of the system’s actions, verification of a system’s response, and counterfactual reasoning.

Other works have compared multiple explanation techniques in the context of a single domain. For example, ? compared a person’s understanding of an agent’s reward function given both saliency maps and decomposed reward bars provided at each decision point in a simple Real-Time Strategy game. They measured the person’s reward understanding through the accuracy of the person’s predictions of the agent’s actions coupled with an open-ended questionnaire asking participants to describe the agent’s approach or method for making decisions. In another study, ? assessed a person’s reward understanding by asking them to identify an agent’s optimal trajectory after being provided with demonstrations of the agent’s behavior which were generated either assuming that the human will perform exact inference or approximate inference of the agent’s objectives. In their experiment, the human is assumed to know the correct set of features that the agent is using to make decisions. So far, we have not identified any work that has compared a broad set of reward explanation techniques provided through multiple explanation modalities in multiple domains in an experimental setting with human subjects. Further, while some preliminary assessment techniques for human reward understanding have been applied in a subset of these studies, no comprehensive way of assessing human reward understanding exists.

Reward Explanation Techniques

We group reward explanation techniques into two categories: feature space techniques and policy space techniques. Feature space techniques explain the reward function in terms of the individual features that comprise the reward function and their relative weights. Policy space techniques explain the reward function through demonstrations of actions in the environment along with how the demonstrated state-action pairs relate to the policy (best/worst actions, important states, etc.). Note that the goal in both cases is to communicate information about the features and their weights and to support understanding of what this means in terms of action in the environment, but the modality of communication differs between the two categories. Feature space techniques may be most applicable when the reward function can be easily represented by a limited number of interpretable features, while policy space techniques may be ideal when reward functions are uninterpretable or otherwise difficult to reason about in terms of translation into actions in the environment. Here we introduce sub-categories of feature and policy space techniques as well as examples from the literature that fall into each category. These categories represent a broad range of common reward explanation modalities. We intend to select one technique from each category for our future human subject experiment.

Feature Space Techniques

Direct Reward Function One straightforward approach to communicating reward information to humans is to show them the reward function, including all features and their weights, directly. While this might be the most direct and complete way of communicating reward information, there are a number of potential shortcomings of this approach. First, if the domain involves a large number of features, it might be difficult for a person to reason over all of these features simultaneously. Second, in cases in which features are uninterpretable to humans (as with deep reinforcement learning), explaining reward information directly may be infeasible. Finally, even if humans are able to understand and reason over all features and their weights, they may not be able to convert this information into an optimal plan or otherwise use the information for their tasks.

Feature Subset Reward information can also be communicated to humans in feature space through subsets of features and their relative weights. This might be a better approach if there are too many features for the human to reason over simultaneously or in order to help the human to focus only on the most important aspects of robot decision-making, for example. Displaying subsets of features has previously been applied in the context of classification tasks, including producing prototypes of different classes (?) and identifying the optimal feature subset given a budget of information to display (?). While these explanation techniques show users subsets of features, they are not directly applied to reward functions, which we study in this work. ? introduce a technique that infers a human’s reward function based on their actions and explains expected missing information. While this technique inherently provides humans with a subset of reward features, in this experiment we are interested in cases in which the reward function is explained from scratch. In our assessment, we will apply a similar approach to that introduced by ?.

Reward Abstractions Finally, reward functions can be explained to humans in feature space using abstractions of features and their relative weights. For example, multiple features may be combined to create one feature or high-level concepts can be combined to create an alternate representation of the reward function. This approach may be especially beneficial if there are too many features for a human to reason over simultaneously or if the features are uninterpretable to humans in some way. Previous works have leveraged user-defined interpretable concepts to learn human-understandable representations of the reward function (??). In our assessment of reward explanation techniques, we intend to pre-define a set of concepts such as those introduced by ? and ? and learn the appropriate weights via regression.

Policy Space Techniques

Trajectory Demonstrations Another way of revealing information about the robot’s reward function to human teammates is through trajectory demonstrations. Trajectory demonstrations could include one or multiple sequences of states and actions generated based on the robot’s reward function or policy. For example, the robot could demonstrate

the optimal trajectory based on its reward function, much as humans are often assumed to do when teaching a robot through learning from demonstration (?). The robot could also provide the most legible trajectory, where a legible trajectory is defined by ? as a trajectory that enables an observer to confidently infer the correct robot goal. Finally, the robot could demonstrate the least optimal trajectory based on its reward function in order to illustrate examples of unfavorable state-action pairs. Note that in many cases, there are many optimal or otherwise equivalent trajectories that could be provided to users, and strategies exist to down-select from these multiple possibilities, for example through the selection of maximally informative trajectories (???). In our assessment, we will provide users with the most and least optimal trajectories as a simple baseline.

Policy Summarization Policy summarization techniques demonstrate agent behavior in a subset of informative states given different conditions and scenarios (?). Such techniques may be beneficial when the state and action space is large and when it might be difficult for a human user to extrapolate important aspects of the agent’s behavior based solely on one or a few optimal or legible trajectories. Given a budget of trajectory segments to provide in a summary, the state-action pairs to include in each segment can be determined based on the importance and diversity of states (?). Multiple definitions of important states have been proposed, including both Q-function-based (?) and entropy-based (?) definitions. ? define important states as states from which taking a wrong action can lead to a significant decrease in future rewards, as determined by the agents Q-values. In particular, they consider the most important states to be states in which the difference between the Q-values associated with the best and worst actions is maximized. We will leverage this definition and the approach introduced by ? in providing policy summaries.

Factored Policies via Reward Decomposition Finally, reward functions can be explained in policy space through factored policies derived from factored rewards (?). In these approaches, the reward function is broken into individual components (in a linear reward function, these might correspond to each feature, for example). A decomposed Q-function with components corresponding to each individual reward component is then learned. With this decomposed Q-function, the contribution of each state-action pair to the individual reward components can be displayed. In our assessment, we will display factored Q-function information for different state-action pairs. We will select states for which we will display factored Q-function information by leveraging a similar approach to the state importance-based selection strategy described by ?.

Reward Understanding Assessments

In order to assess a person’s reward understanding, we suggest the use of a suite of four different assessment techniques: free response, feature sub-selection, preference elicitation, and best demonstration elicitation. Since a variety of assessment techniques have been applied in the past and there is not currently a standard way of assessing a human’s

reward understanding, using a suite of techniques will allow us to consider multiple types of human input and compare the results from each. The following are descriptions of the assessment techniques along with the associated metric for each. We also introduce three composite metrics that are based on the four individual metrics proposed here.

Free Response (FR)

For the free response assessment, subjects will be asked how they think the robot makes decisions in each domain. They will be able to provide free-form answers about the factors they think the robot uses in decision-making and how important each factor is relative to the others. Their responses will be coded in a similar way as in previous literature (???), and the coded response will be used to produce the set of features that the human believes are important, F_H^{fr} , as well as the set of pairwise comparisons of their relative weights, W_H^{fr} (e.g. $w_A > w_B$, where w_i is the weight of feature i). Given the robot’s ground truth set of features, F_R^{fr} , and pairwise comparisons of its relative weights, W_R^{fr} , the metric for the free response assessment, based on the similarity metrics used by ?, can be defined as the intersection over union of the set of human features and pairwise rankings and the ground truth set of robot features and pairwise rankings:

$$FR = \frac{(F_H^{fr} \cup W_H^{fr}) \cap (F_R^{fr} \cup W_R^{fr})}{(F_H^{fr} \cup W_H^{fr}) \cup (F_R^{fr} \cup W_R^{fr})}$$

Feature Sub-selection (FS)

For the feature sub-selection assessment, subjects will be provided with a list of possible features (only a subset of which are actually used by the robot), and they will be asked to select the ones they believe are relevant to the scenario and assign relative weights to each. F_H^{fs} , W_H^{fs} , F_R^{fs} , and W_R^{fs} are defined as in the previous section and yield the following metric for feature sub-selection (also based on the previously-discussed similarity metric):

$$FS = \frac{(F_H^{fs} \cup W_H^{fs}) \cap (F_R^{fs} \cup W_R^{fs})}{(F_H^{fs} \cup W_H^{fs}) \cup (F_R^{fs} \cup W_R^{fs})}$$

Preference Elicitation (PE)

Preference elicitation involves presenting subjects with multiple trajectories and asking them to select the best, similar to an active learning approach (Settles 2012). We generate queries using the maximum information gain strategy proposed by ?. We define the set of human responses to these queries as q_H and the set of ground truth correct responses from the robot as q_R . Given these, the metric for preference elicitation is defined as the percent of correct human responses (i.e. recall):

$$PE = \frac{|q_H \cap q_R|}{|q_R|}$$

Best Demonstration (BD)

For the best demonstration assessment, subjects will be asked to provide demonstrations that they believe are optimal given what they know about the agents reward function.

This assessment is similar to the “simulation” assessment used by ?. The metric we consider for the best demonstration is the complement of the normalized regret:

$$BD = 1 - \frac{R(\xi^*) - R(\xi^H)}{R(\xi^*)}$$

$R(\xi^*)$ is the reward for the optimal trajectory ξ^* and $R(\xi^H)$ is the reward for the human’s demonstration ξ^H . We normalize regret in this case, because all of the other assessment metrics are normalized, and we take the complement, since larger values indicate better understanding for the other assessments. These two steps allowed us to combine the four assessment metrics into composite metrics more readily.

Composite Metrics

Finally, we propose three composite metrics based on combinations of four individual metrics. Just as we divided reward explanation techniques into feature space techniques and policy space techniques, we can similarly divide our assessment metrics into feature space metrics, which ask directly about features and their weights (FR and FS), and policy space metrics, which ask about the behaviors that result from reward functions (PE and BD). All four individual metrics are normalized, and so we weight them equally in combining them to form the composite metrics. Accordingly, we propose the composite feature space metric: $F = FR + FS$. We also propose the composite policy space metric: $P = PE + BD$. Finally, we propose the overall composite metric: $C = F + P$.

Axes of Domain Complexity

In characterizing domains, we consider four different axes of complexity: reward function complexity, feature complexity, environment complexity, and situational complexity. When considering reward functions that are linear in features, we can vary reward function complexity by considering reward functions with more or fewer features. Feature complexity is related to how complex each individual feature within the linear reward function is. While there might be many ways to characterize feature complexity, we consider the interpretability of individual features as a measure of their complexity. Environment complexity includes factors such as the size of the state and action spaces, whether the state and action spaces are discrete or continuous, or whether a domain is Markovian or non-Markovian. Finally, situational complexity indicates whether a person will need to perform other tasks at the same time as receiving the explanation and the number and difficulty of those tasks.

Proposed Experiment

We propose an experiment to test each of the different explanation techniques in domains of varying complexity as defined by the four axes outlined in the previous section. We have selected four domains in order to cover a broad range of complexities. Our domains include a simple grid world scenario, OpenAI Gym’s Lunar Lander (?), the threats and waypoints domain proposed by ?, and the threats and waypoints domain combined with a secondary task in which the human needs to monitor a robot traversing in rocky terrain.

Hypotheses

Our hypotheses for the proposed experiment include those listed below. We intend to assess our hypotheses using the proposed metrics for reward understanding.

Hypothesis 1 *Feature space techniques will lead to better reward understanding than policy space techniques in domains of low versus high reward, feature, and environment complexity.*

Hypothesis 2 *Policy space techniques will lead to better reward understanding than feature space techniques in domains of high versus low reward, feature, and environment complexity.*

Hypothesis 3 *The best modality of information (feature versus policy space) will not change between scenarios with low versus high situational complexity in domains of the same reward, feature, and environment complexities.*

Hypothesis 4 *Reward understanding will be worse in scenarios with high versus low situational complexity for both feature space techniques and policy space techniques.*

Conclusion

In this paper, we define categories of existing reward explanation techniques representing a broad set of explanation modalities, and we identify a specific approach we plan to implement in the context of a human subject experiment from each category. We also suggest a suite of assessment techniques and metrics for human reward understanding. These techniques and metrics integrate multiple modalities of human information understanding, including both feature-based information and behavior/policy-based information. Finally, we define four axes of domain complexity and outline a future experiment to better understand which reward explanation techniques are most effective in which contexts. We hope that the proposed characterization of reward explanation techniques along with the assessment techniques and metrics will contribute to a more systematic understanding of which reward explanation techniques are most beneficial in different contexts through future human subject experiments. Minima esse illo deserunt praesentium, eum recusandae tenetur assumenda voluptatem quas illo fugit, deleniti saepe aspernatur totam consequuntur cumque error velit, explicabo officiis incidunt rerum ipsum voluptatum expedita, rerum tempora veritatis voluptatum culpa. Molestias voluptates ex tenetur doloremque repellat doloribus aut, deleniti numquam odit adipisci quo nihil. Cupiditate nobis obcaecati est nemo repellat vitae maiores nisi, ipsum culpa ullam expedita eaque blanditiis ratione qui nostrum? Quasi a rem dolorum porro at laboriosam provident, voluptatibus natus vitae accusamus harum laborum laboriosam fugit, atque nostrum odit quas provident voluptatibus nobis nam at modi, corrupti officiis praesentium quod possimus, odit veniam nesciunt perspicui? Earum deleniti quaerat dicta nam cupiditate reprehenderit delectus expedita alias, nam minima labore vitae animi quasi obcaecati fugit architecto, esse iure exercitationem debitis? Aut possimus deserunt officia ut nulla

maxime assumenda omnis numquam iusto, mollitia explicabo quisquam nisi provident libero?Accusantium soluta hic illum quos maiores deserunt blanditiis, culpa fugiat vel doloribus ipsa sunt magnam consectetur ipsam