Agent Strategy Summarization

Blue Sky Ideas Track

Ofra Amir
Technion IE&M
oamir@technion.ac.il

Finale Doshi-Velez
Harvard University
finale@seas.harvard.edu

David Sarne
Bar-Ilan University
sarned@cs.biu.ac.il

ABSTRACT
Intelligent agents and AI-based systems are becoming increasingly prevalent. They support people in different ways, such as providing users with advice, working with them to achieve goals or acting on users’ behalf. One key capability missing in such systems is the ability to present their users with an effective summary of their strategy and expected behaviors under different conditions and scenarios. This capability, which we see as complimentary to those currently under development in the context of “interpretable machine learning” and “explainable AI”, is critical in various settings. In particular, it is likely to play a key role whenever a user needs to understand the strategy of an agent she is working along with, when having to choose between different available agents to act on her behalf, or when requested to determine the level of autonomy to be granted to the agent or approve its strategy. In this paper, we pose the challenge of developing capabilities for strategy summarization, which is not addressed by current theories and methods in the field. We propose a conceptual framework for strategy summarization, which we envision as a collaborative process that involves both agents and people. Last, we suggest possible testbeds that could be used to evaluate progress in research on strategy summarization.

KEYWORDS
Strategy summarization; Explainable AI

1 INTRODUCTION
Intelligent systems play a growing role in our daily lives, from voice-controlled assistants and online ordering aides to tools for recognizing cancerous tumors and computer-assisted driving [38]. Many of these systems go even further, autonomously carrying out tasks on behalf of their user rather than simply providing advice. These can either take the form of virtual agents (e.g., Poker bots that play on real money, automatic news feed generators) or physical ones (e.g., autonomous cars, vacuum robots). The behavior of these systems is often opaque to human users. For example, a robotic vacuum may be equipped with several coverage algorithms and the choice of which to be used at a time may depend on environment conditions, which might be beyond the user’s reach.

Users’ familiarity with the strategies and expected behaviors of agents under different conditions and scenarios is essential for many purposes. First, an understanding of agents’ behaviors can facilitate choosing between interchangeable systems (e.g., Siri, Cortana, Alexa). Second, knowing the agent’s strengths and weaknesses can improve the ability of people to collaborate with agents (e.g., with a surgical robot). Last, users may need to determine how much autonomy to grant to an agent, and knowing its expected behavior can help them make more informed decisions, and trust that the agent could perform its designated role.

However, explaining complex system behavior to users is challenging because the behavior of these systems is often determined using sophisticated computational techniques (e.g., machine-learning models, deep learning, Markov decision processes and in many cases an ensemble of methods). People are inherently bounded-rational and find it difficult to map from a design and logic to actual behavior of the system. It has been shown that users’ mental models of system behaviors are incomplete, parsimonious and unstable; that people are limited in their ability to “run” these models to predict expected behavior; and that people often confuse different mental models [33]. Moreover, attempting to specify the system’s actual behavior in each world state is typically infeasible because the space of possible world states the system may run into is often far more immense than what a human can manage. For example, the state space in which autonomous vehicles make decisions is based on speed, weather, road conditions, distance and much other data gathered by a variety of sensors, including cameras, LiDARS (Light Detection and Ranging), and radars. While the user may be a very experienced driver, it is very likely that she has never experienced or ever considered many of the possible states in this space (e.g., spotting a child running out to retrieve a bouncing ball or spotting a tire of the car in front of you exploding).

Supporting users in understanding and anticipating agents’ behavior thus poses significant computational problems. While there has been growing recent discussion of the need for “explainable AI” and “human-aware AI” — which all relate to the problems specified above — these concepts are very broad and are not immediately translatable to concrete research problems, making it hard to measure progress in these areas. Therefore, we pose a more specific challenge: the development of core capabilities for agent strategy summarization. This challenge is not addressed by current state-of-the-art theories and methods. However, it is more concrete than the high-level goal of “explainable AI” and thus allows us to identify specific open problems that need to be solved in order to meet this challenge. These include the development of algorithms that generate summaries of agent behaviors, as well as the design of collaborative interfaces through which users can review and explore these summaries. We further consider methodologies and testbeds

for proper experimental evaluation of the effectiveness of such methods in improving people’s understanding of agent behavior.

The idea behind strategy summarization is to provide users with some form of a summary (either textual or visual, through an interactive interface) that demonstrates system behavior in carefully selected world states. With this new paradigm, users gain a better understanding of the system in a range of diverse world states, in a relatively short time. While recent efforts developed methods for explaining one-shot decisions made by autonomous agents (e.g., Khan et al. [23]) or machine learning algorithms (e.g., [34]) in retrospect, or ex-post, strategy summarization offers a complementary important capability, which is the cohesive description of the behavior an agent is likely to exhibit, ex-ante. Few recent works propose user interface designs enabling users to query an agent’s policy (e.g., Hayes & Shah [20]), yet these require much sophistication, knowledge and effort from users in order to properly understand the system, and do not generate automated summaries. In contrast, the strategy summarization approach aims to communicate the actual agent behavior in a scenario-based manner, rather than conveying its underlying decision-making model (e.g., a decision tree, the coefficients of a logit regression model). It reduces user effort in that it presents agent behavior in a range of scenarios rather than requiring users to specify many queries on their own.

The study of strategy summarization will contribute to theories and methods in the areas of decision making under uncertainty, human-agent interaction, explainable AI and multi-agent literature. It requires expertise in diverse fields, in particular human-agent interaction, planning and learning algorithms and representations, interpretability, and machine learning. Still, we argue it is both feasible and worth pursuing, as methods that help people better understand agents are expected to have an impact in many areas, including domains of societal importance such as healthcare, education and transportation.

2 RELATED WORK
While there is relatively little work on ex-ante descriptions of agent strategy, there is a broader literature of summarizing hierarchical plans, explaining robot behavior, explaining decisions in Markov Decision Processes, interpretable machine learning, as well studies concerned with users’ mental models of systems. We review works in these areas, which strategy summarization research can and should draw on.

Summarizing hierarchical plans. Recent research has considered several new approaches for enabling users understand the strategy of the systems they use. For example, Myers [31] proposed a method for summarizing plans represented as Hierarchical task networks (HTNs) to help people in reviewing and comparing them, emphasizing features such as the allocation of roles to agents, tasks included in the plan and tasks absent. However, this approach is limited in the sense that it is only appropriate for short-term plans toward achieving a specific goal and relies on an HTN model.

Explaining robot and agent behavior. In the context of human-robot interaction, prior work has developed methods for supporting users in debugging a robot or to improve the ability of the human and the robot to collaborate effectively. For example, Nikolaidis et al. [32] proposed a cross-training approach to help parties develop a better understanding of their teammate. Lomas et al. [27] developed a system that enables a user to ask robots questions. Brooks et al. [5] developed a system that visualizes all the past actions of a robot and includes explanations for the actions. Hayes & Shah [20] proposed several methods for explaining robot policies to people using past execution traces, enabling users to query the agent’s behavior in different states and request explanations. In other work, animation techniques depicting anticipation and reaction of robots were used to help people predict what a robot will do next [40]. Recently, Zhang et al. [51] proposed methods for plan explicability and predictability which can be used to generate plans that are more understandable to people. Other works have used argumentation approaches to explain agent behavior [1, 37]. These approaches are complementary to the strategy summarization approach, in that they provide different ways of examining the behaviors of agents, yet they do not attempt to generate summaries of the agent’s behavior. Instead, they present complete plans or attempt to explain the logic underlying specific decisions.

Several prior works suggested methods for explaining recommendations given by MDP-based intelligent assistants [9, 11, 12, 22, 23] or explaining plans [36]. Wang et al. generated explanations of robot reasoning based on Partially Observable Markov Decision Problems (POMDPs) [47] and similar approaches have been developed for explaining decisions in the context of HTN planning, explaining an agent’s actions based on its task model [29, 30]. The problem we address differs from the problem of generating explanations for specific decisions, as rather than explaining an action taken (or a suggested action), we aim to describe which actions would be taken in information-critical states, before the agent actually acts.

Interpretable machine learning. Recently, many approaches have been proposed for developing interpretable machine learning models, that is, models that are understandable to people [10, 26, 35, 44]. These approaches typically seek to explain a decision made by a machine learning model (e.g., by showing a simpler locally correct model [34] that explains the classification of a sample). Similar to the methods for explaining MDP decisions, these approaches explain a single decision after the fact, rather than provide a description of a strategy or behavior of an agent in different situations. While some methods suggest complete decision-making models that can be more intuitive to people [24, 50], they do not account for sequential decision-making settings.

Users’ understanding of system behavior. The strategy summarization idea relates to the literature on users’ mental models of systems (software, robots). In a study of users’ trust in personal assistants, Glass et al [16] found that system transparency is important to users and suggested that explanations of system behavior can facilitate trust. More accurate mental models of users about robots’ behavior can result in improved performance when collaborating with robots [8]. However, research in HCI has shown that people face difficulties in forming accurate mental models of systems and in practice their models of system behaviors are incomplete, parsimonious and unstable; and they are limited in their ability to predict a system’s behavior [33]. Letting users interact with a robot’s behavior has been shown to help them establish appropriate mental model[39]. We hypothesize that presenting users with summaries of agent strategies will also help them establish mental models of these agents, facilitating trust and collaboration.
3 A CONCEPTUAL FRAMEWORK FOR STRATEGY SUMMARIZATION

While strategy summarization is a complex task, we argue that it can be broken down into manageable subcomponents. We suggest a conceptual framework for the process of strategy summarization, illustrated in Figure 1, which we envision as a collaborative effort that involves both agents and people. We next describe the main components required for generating and presenting summaries, as well as how they interact.

![Figure 1: A conceptual model of the summarization process.](image)

A key capability required for strategy summarization is identifying states that are likely to be of interest to people interacting with the agent, such that the behavior of the agent in this states can be conveyed to users. To this end, we suggest developing intelligent state extraction methods. These methods should take as input the strategy of the agent (or agents) that needs to be summarized and identify and prioritize a subset of states to include in the summary. The implementation of such methods requires a specification of the desired properties of a set of world-states to present in a summary. We discuss these in Section 3.1.

Another important capability required for the summarization process is the ability to properly represent world states (Section 3.2), meaning, how to encode states in a given application domain. We expect that internally, the agent may have a highly complex representation of the world that it uses for decision-making. For example, a decision to invest in a stock may depend not only on current stock prices but also on long-term and short-term trends as well as a variety of different types of external financial and political events. This representation likely does not match the human user’s notion of essential decision-making factors. A good world-state representation will substantially reduce the potentially immense and inscrutable space of agent internal representations to those that are meaningful to the user.

Finally, users will be the ultimate consumers of the strategy summary, and thus also essential in the process of determining what is relevant to them. We envision strategy summary interface, facilitating mixed-initiative interaction, where the exploration of the summary is guided by both the user and the system. We discuss key design and computational problems toward supporting this collaborative exploration in Section 3.3.

3.1 Intelligent State Extraction

While the specific requirements for an effective strategy summary will likely vary across problem domains, we hypothesize that there is a basic set of requirements that are common across different settings: the summary should provide a high coverage of states that are likely to be of interest to users and should be of reasonable length (such that it does not require too much time/cognitive effort to review). In addition, the summary should be relevant to the user’s goal (e.g., whether it is to choose between agent or work together with an agent), and should provide information that would help the user to contextualize the information presented (e.g., the likelihood of encountering different states).

We suggest two potential directions for the development of methods that determine which states (and the corresponding actions taken in those states) to include in the summary. The first approach draws on the agent’s own reasoning to identify states of interest. For example, states in which the agent could take an action that leads to a catastrophic outcome, or states where the agent is less confident might be considered as potentially interesting for the user. These can be identified by reasoning about the agent’s decision-making model. For instance, the distribution of Q-values in a certain state could be used to determine the importance of the choice of action in that state, as well as the uncertainty of the agent regarding its decision. Similar ideas have been used in the past in the context of student-teacher reinforcement learning to determine effective teaching opportunities for agents [3, 7, 41]. In preliminary work on strategy summarization, we used this approach to generate summaries and showed that these summaries helped people choose between different agents [2]. Distance between states can also be computed to avoid redundancy in the summary, and the likelihood of encountering a state can be computed to account for both common and rare states in a summary. If the goal is to distinguish between different users, their summaries can focus on states where their policies diverge.

The second approach utilizes people’s judgment to identify states that will likely be of importance to users. An example for possible methods that take this approach is the use of Peer-Designed Agents (PDAs) [6, 13, 14, 28]. These agents have been used in recent years for generating realistic behaviors for the purpose of predicting human behavior and their reaction to changes in their environment. The idea is to provide people with a skeleton agent equipped with all the required functionality except for its behavioral layer and have people (either directly or through the mediation of a programmer) design and program into them the strategy they would have used in similar decision situations. The PDAs’ logic can then be used as a reflection of what their developers considered to be important (or worth distinguishing) when reasoning about the strategy to be used. This could enable synthesizing the set of world states that are most relevant for demonstrating the system behavior, either through a manual code review, seeking for points of code divergence, or by applying standard clustering algorithms for identifying those states that are highly distinguishable in terms of the codes used in large by the population (when using several PDAs).

3.2 World-State Representation

Deciding how to encode the state representation such that states could be effectively conveyed to people and such that the space of states to consider for the summary will be reduced is a hard problem. We expect that this would require either analysis of large sets of strategies (e.g., a set of strategies programmed into PDAs for that application domain) or the design of effective processes for eliciting such state representation from domain experts. The idea in both approaches is to reason about what types of raw states can be logically aggregated to a single state, as far as the user is concerned.
and to what extent prior events as well as various measurable factors should be considered for distinguishing between states of interest. State representation encoding using experts is inherently a manual process, and designing a process for querying experts in an efficient way (e.g., using active learning approaches) will be key to making this process feasible. Extraction based on strategies could be made either based on manual code analysis or using unsupervised clustering over the raw world states to join states for which a similar action is used by a large subset of strategies.

3.3 Strategy Summary Interface

Naturally, different forms of presenting summaries would be appropriate in different settings. For example, for physical agents such as self-driving cars or home robots, it might be more helpful to visually show their actual behavior (e.g., a video of their execution) than showing a textual summary of this behavior. However, for virtual agents such as a finance investment advising agent some form of a textual summary, typically in the form of rules to be applied over sets of world-states may be preferred. A key question is how to present summaries to people. There are additional important questions such as how to provide people with sufficient context about the states shown in the summary without overwhelming them with non-important low-level details.

As discussed in Section 3.1, there could be different criteria for deciding what information to include in the summary, and these criteria might be in conflict. Therefore, there is a need to design collaborative interfaces which will allow users to guide the generation of summaries by stating preferences. Such interfaces could also allow users to directly query the agent’s strategy and explore its behavior in situations that were not described in the summary. A key design challenge in developing these interaction methods is to ensure that users can express their needs in their own language, rather than being asked to specify low-level system parameters. Moreover, exploring the behavior of an agent can be tedious. To make the process more efficient, the design of mixed-initiative interactions [21] where the system tries to help the user in exploring the agent’s strategy will likely be required.

4 EVALUATION METHODOLOGIES

To assess progress in the area of strategy summarization and ensure that generated summaries are helpful for users, it is essential to thoroughly consider means of evaluation. To this end, there are numerous testbeds of common use in the AI-community which can be used for evaluation. Basic testbeds may include robotics applications, e.g., in exploration and search tasks [25, 43, 45, 46, 49]. More advanced testbeds include trading agents and automated negotiation infrastructures (e.g., TAC [17, 42, 48] or ANAC [4] simulators). Using such well-studied testbeds will enable drawing on already established agent repositories (with a variety of agent designs) and environments associated with these competitions. Route planning (and re-route planning as the congestion predictions change) is also an ideal testbed and there are various multi-layered multi-agent based implementations that can be used [18, 19].

Alongside experimentation with the above testbeds, it is important to have some real test-cases to validate. One ideal application on which strategy summarization can be tested is robotic vacuums. More complex domains include clinical decision-support (e.g., for treatment management [15]) and autonomous vehicles. The simpler domains will facilitate relatively fast cycles of testing and improvement of the developed methods, enabling gradual progress towards evaluation in the more complex domains, where substantial implementation and careful experimental design will be required.

Automated summarization should be assessed both in terms of computational aspects of the summarization methods and human-centered evaluation criteria. Metrics of the latter type can be both objective, e.g., people’s understanding of strategies (which could be measured by assessing their ability to predict agents’ actions or rank different agents in terms of the performance they are likely to achieve in a given environment) and their performance when collaborating with agents, as well as subjective, including the perceived usefulness of the methods and cognitive effort.

5 DISCUSSION

The study of strategy summarization will contribute much to theories and methods in the areas of decision making under uncertainty, human-agent interaction, explainable AI and multi-agent literature. However, more importantly, its deliverables will enable both novice and expert users to better understand the systems they use, in particular complex (AI-based) systems. With the growing use of AI-based agents and shift toward the design of intelligent agents that can collaborate effectively with people [38], we expect that improved user understanding of agents’ capabilities and limitations will lead to improved outcomes in many areas.

One key area in which we expect the developed methods to make a substantial impact is the emerging use of autonomous and semi-autonomous vehicles. There is no doubt that we are on the verge of a quantum shift in the way vehicles, humans and the transportation infrastructures interact. The successful operation of autonomous transportation systems (e.g., the autonomous car or Amazon’s UAVs) requires providing the highest level of assurance to legislators, authorities (e.g., highway authorities) and users (e.g., car buyers). With strategy summarization, both legislators and users will be able to better understand the way in which these systems work, potentially leading to shorter approval cycles and more effective use. For example, a better understanding of the expected behavior of an autonomous car will help drivers anticipate situations in which the car needs to transfer control to them.

Strategy summarization could also be beneficial in areas of vast societal importance such as education and healthcare. In education, the methods to be developed will enable parents and educators to make better choices when deciding on the educational systems kids will become engaged with, hence improving education development. In medical domains, patients will be able to better understand treatment protocols leading to a better state of mind while being treated, and professionals will be able to reason about the fit of such plans to patients, potentially improving patients’ outcomes.

ACKNOWLEDGMENTS

This research was partially supported by the ISRAEL SCIENCE FOUNDATION (grant No. 1162/17) and the ISF-NSFC joint research program (grant No. 2240/15).