

A Survey on Large Language Model based Autonomous Agents

Lei Wang, Chen Ma*, Xueyang Feng*, Zeyu Zhang, Hao Yang, Jingsen Zhang,
Zhiyuan Chen, Jiakai Tang, Xu Chen, Yankai Lin, Wayne Xin Zhao, Zhewei Wei,
Ji-Rong Wen

Gaoling School of Artificial Intelligence, Renmin University of China, Beijing, China

Abstract

Autonomous agents have long been a prominent research topic in the academic community. Previous research in this field often focuses on training agents with limited knowledge within isolated environments, which diverges significantly from the human learning processes, and thus makes the agents hard to achieve human-like decisions. Recently, through the acquisition of vast amounts of web knowledge, large language models (LLMs) have demonstrated remarkable potential in achieving human-level intelligence. This has sparked an upsurge in studies investigating autonomous agents based on LLMs. To harness the full potential of LLMs, researchers have devised diverse agent architectures tailored to different applications. In this paper, we present a comprehensive survey of these studies, delivering a systematic review of the field of autonomous agents from a holistic perspective. More specifically, our focus lies in the construction of LLM-based agents, for which we propose a unified framework that encompasses a majority of the previous work. Additionally, we provide a summary of the various applications of LLM-based AI agents in the domains of social science, natural science, and engineering. Lastly, we discuss the commonly employed evaluation strategies for LLM-based AI agents. Based on the previous studies, we also present several challenges and future directions in this field. To keep track of this field and continuously update our survey, we maintain a repository for the related references at <https://github.com/Paitesanshi/LLM-Agent-Survey>.

1 Introduction

“An autonomous agent is a system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to effect what it senses in the future.”

Franklin and Graesser (1997)

Autonomous agents have long been seen as a promising path toward artificial general intelligence (AGI), capable of accomplishing tasks through self-directed planning and instructions. In earlier paradigms, the policy functions that dictated the agent’s actions were conceived through heuristic methodologies and subsequently refined through environmental engagements [101, 86, 120, 55, 9, 116]. A discernible gap has emerged wherein these functions often fall short of replicating human-level proficiency, particularly in unconstrained, open-domain settings. Such discrepancies can be traced back to potential inaccuracies inherent in the heuristic designs and the circumscribed knowledge furnished by the training environments.

*These authors contribute equally to this paper.

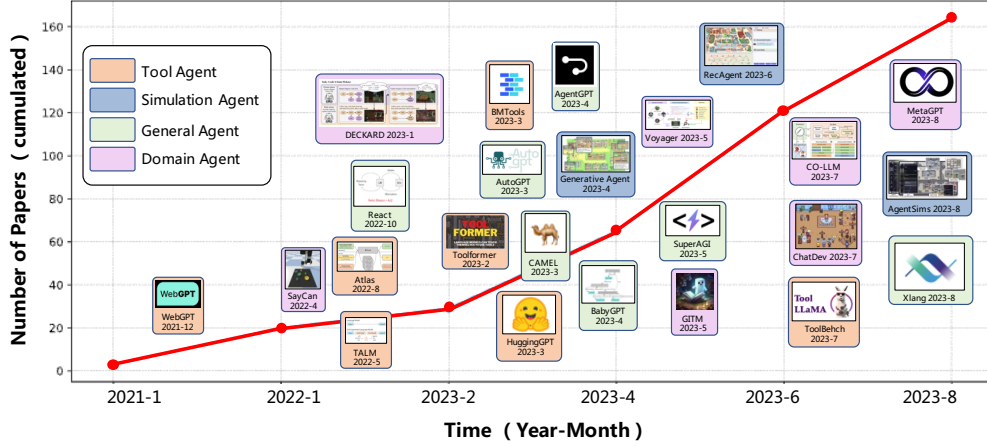


Figure 1: Illustration of the growth trend on the field of LLM-based autonomous agents.

In recent years, large language models (LLMs) have achieved remarkable success, indicating their potential for achieving human-like intelligence [108, 116, 9, 4, 130, 131]. This capability emerges from the utilization of comprehensive training datasets coupled with a substantial array of model parameters. Motivated by this capability, a burgeoning trend has emerged in recent years (see Figure 1 for the growth trend of this field), wherein LLMs are harnessed as core orchestrators in the creation of autonomous agents [19, 125, 123, 115, 119, 161]. This strategic employment aims to emulate human-like decision-making processes, thereby providing a pathway towards more sophisticated and adaptive artificial intelligence systems. Along the direction of LLM-based autonomous agents, people have designed many promising models, focusing on enhancing LLMs with essential capabilities, such as memory and planning, enabling them to stimulate human actions and proficiently undertake a range of tasks. However, these models are proposed independently, and there have been limited efforts in summarizing and comparing them holistically. It is crucial to construct a holistic summarization analysis for existing LLM-based autonomous agents works, which holds great significance in developing a comprehensive understanding of this field and serving as inspiration for future research.

In this paper, we conduct a comprehensive survey of the field of LLM-based autonomous agents. Specifically, we organize our survey based on three aspects including the construction, application, and evaluation of LLM-based autonomous agents. For the agent construction, we present a unified framework composed of four components, that is, a profile module to represent agent attributes, a memory module to store historical information, a planning module to strategize future actions, and an action module to execute the planned decisions. By disabling one or more modules, the majority of previous studies can be viewed as specific examples of this framework. After introducing the typical agent modules, we also provide a summary of the commonly-used fine-tuning strategies to enhance the adaptability of the agent for different application scenarios. In addition to constructing the agent, we provide an overview of the potential applications of autonomous agents, exploring how these agents can enhance the fields of social science, natural science, and engineering. Finally, we discuss the methods for evaluating autonomous agents, focusing on both subjective and objective strategies.

In summary, this survey provides a systematic review and establishes clear taxonomies for existing studies in the field of LLM-based autonomous agents. It focuses on three aspects including the agent construction, application, and evaluation. Based on the previous studies, we identify several challenges in this field and discuss potential future directions. We believe this field is still at its early stages, and therefore, we maintain a repository to continually keep track of the studies in this field at <https://github.com/Paitesanshi/LLM-Agent-Survey>.

2 LLM-based Autonomous Agent Construction

LLM-based autonomous agents are expected to effectively accomplish different tasks based on the human-like capabilities of LLMs. In order to achieve this goal, there are two significant aspects, that is, (1) which architecture should be designed to better use LLMs and (2) how to learn the parameters

of the architecture. Within the context of architectural design, we contribute a systematic synthesis of existing research, culminating in a comprehensive unified framework. As for the second aspect, we summarize three commonly employed strategies including (1) learning from examples, where the model is fine-tuned based on curated datasets, (2) learning from environment feedback, leveraging real-time interactions and observations, and (3) learning from human feedback, capitalizing on human expertise and intervention for refinement.

2.1 Agent Architecture Design

Recent advancements in Language Models (LLMs) have demonstrated their potential to accomplish a wide range of tasks. However, only based on LLMs, it is hard to effectively realize an autonomous agent due to their architecture limitations. To bridge this gap, previous work has developed a number of modules to inspire and enhance the capabilities of LLMs for building autonomous agents. In this section, we propose a unified framework to summarize the architectures proposed in the previous work*. In specific, the overall structure of our framework is illustrated Figure 2, which is composed of a profiling module, a memory module, a planning module, and an action module. The purpose of the profiling module is to identify the role of the agent. The memory and planning modules place the agent into a dynamic environment, enabling it to recall past behaviors and plan future actions. The action module is responsible for translating the agent’s decisions into specific outputs. Within these modules, the profiling module impacts the memory and planning modules, and collectively, these three modules influence the action module. In the following, we detail these modules.

2.1.1 Profiling Module

autonomous agents typically perform tasks by assuming specific roles, such as coders, teachers and domain experts [113, 35]. The profiling module aims to indicate the role profiles of the agents, which are usually written into the prompt to influence the LLM behaviors. In existing work, there are three commonly used strategies for generating agent profiles.

Handcrafting Method: in this method, the profiles of agents are manually specified. For instance, if one would like to design agents with different personalities, he can use "you are an outgoing person" or "you are an introverted person" to profile the agent. The handcrafting method has been leveraged in a lot of previous work to indicate the agent profiles. In specific, Generative Agent [156] describes the agent by the information like name, objectives, and relationships with other agents. MetaGPT [58], ChatDev [113], and Self-collaboration [29] predefine various roles and their corresponding responsibilities in software development, manually assigning distinct profiles to each agent to facilitate collaboration. A recent work [27] demonstrates that manually assigning different personas significantly impacts LLM’s generation, including toxicity. By assigning specific personas, they show increased toxicity versus default personas. In general, the handcrafting method is very flexible. However, it can be labor-intensive, particularly when dealing with a large number of agents.

LLM-generation Method: in this method, the agent profiles are automatically generated based on LLMs. Typically, it begins by providing manual prompts that outline specific generation rules and elucidates the composition and attributes of the agent profiles within the target population. In addition, it may specify initial seed agent profiles to serve as few-shot examples. These profiles then serve as the foundation for generating other agent information based on LLMs. For example, RecAgent [134] first creates seed profiles for a small number of agents by manually crafting details like age, gender, personal traits, and movie preferences. Then, it leverages ChatGPT to generate more agent profiles based on the seed information. The LLM-generation method can save significant time when the number of agents is large, but it may lack precise control over the generated profiles.

Dataset Alignment Method: in this method, the agent profiles are indicated based on real-world datasets. The basic information of real humans is fully or selectively leveraged to describe the agents. For example, the agents in [5] are initialized based on the participant demographic backgrounds in real-world survey datasets. The dataset alignment method can accurately capture the attributes of the real population, effectively bridging the gap between the virtual and real worlds.

In addition to the profile generation strategies, another important problem is how to specify the information for profiling the agents. Examples of information include demographic information, which introduces the characteristics of a population (e.g., age, gender, and income), psychology

*Our framework is also inspired by a pioneer work at <https://lilianweng.github.io/posts/2023-06-23-agent/>

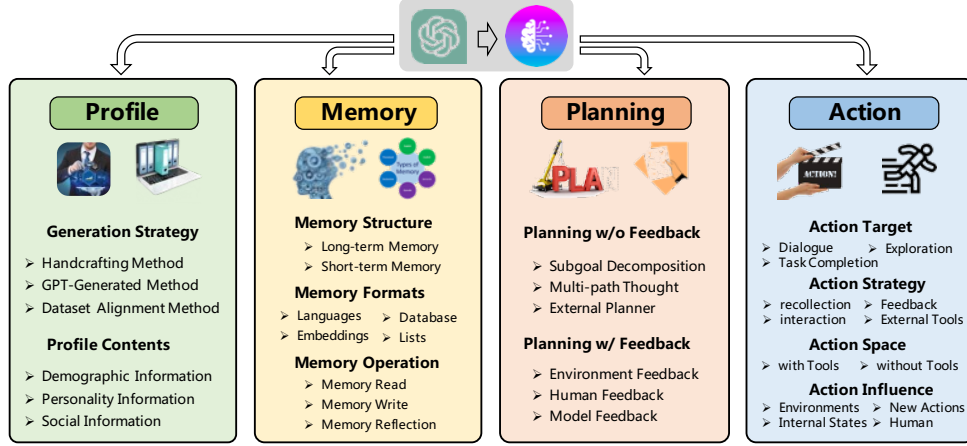


Figure 2: A unified framework for the architecture design of LLM-based autonomous AI agent.

information, which indicates the personalities of the agents, and social information, which describes the relationships between agents. The choice of information to profile the agent is largely determined by the specific application scenarios. For instance, if the study focuses on user social behaviors, social profile information becomes pivotal. However, establishing the relationship between the profile information and downstream tasks is not always straightforward. A potential solution would be to input all possible profile information initially and then develop automatic methods (e.g., based on LLMs) to select the most suitable one.

2.1.2 Memory Module

The memory module plays a very important role in the construction of AI agents. It stores information perceived from the environment and leverages the recorded memories to facilitate future actions. The memory module can help the agent to accumulate experiences, self-evolve, and behave in a more consistent, reasonable, and effective manner. This section provides a comprehensive overview of the memory module, focusing on its structures, formats, and operations.

Memory Structures: LLM-based autonomous agents usually incorporate principles and mechanisms derived from cognitive science research on human memory processes. Human memory follows a general progression from sensory memory that registers perceptual inputs, to short-term memory that maintains information transiently, to long-term memory that consolidates information over extended periods. When designing memory architectures for AI agents, researchers take inspiration from these aspects of human memory while also recognizing key differences in capabilities. Short-term memory in AI agents is analogous to learning capacities supported within the context window constraints of the Transformer architecture. Long-term memory resembles the external vector storage that agents can rapidly query and retrieve from as needed. Thus, while humans gradually transfer perceived information from short-term to long-term stores via reinforcement, AI agents can engineer more optimized writing and reading processes between their algorithmically implemented memory systems. By emulating aspects of human memory, designers can create agents that leverage memory processes for improved reasoning and autonomy. In the following, we introduce two types of commonly used memory structures.

- **Unified Memory.** In this structure, the memories are organized into a single framework, and there are no distinctions between the short- and long-term memories. The framework has unified interfaces for memory reading, writing, and reflection. For example, Atlas [65] stores document memories based on universal dense vectors, which are generated from a dual-encoder model. Augmented LLM [121] employs a unified external storage for its memory, which can be accessed via prompts. Voyager [133] also utilizes a unified memory architecture, where skills of different complexities are gathered in a central library. During code generation, skills can be indexed based on their relevance for matching and retrieval. ChatLog [132] maintains a unified memory stream, which allows the model to retain important historical information and adaptively adjust the agents themselves for different environments.

- *Hybrid Memory.* Hybrid memory clearly differentiates between short-term and long-term functions. The short-term component temporarily buffers recent perceptions, while long-term memory consolidates important information over time. For instance, [109] employs a dual-layered memory structure to store an agent’s experiences and knowledge, comprising a long-term memory and a short-term memory. Long-term memory is utilized to preserve the agent’s understanding and summarization of the entire world, while short-term memory is employed to retain the agent’s comprehension and annotations of individual events. AgentSims [89] also implements a hybrid memory architecture. The long-term memory utilizes a vector database to efficiently store and retrieve the episodic memories of each agent. LLMs are employed to realize the short-term memory and perform abstraction, validation, correction, and simulation tasks. In GITM [161], the short-term memory stores the current trajectory, and the long-term memory saves reference plans summarized from successful prior trajectories. Long-term memory provides stable knowledge, while short-term memory allows flexible planning. Reflexion [125] utilizes a short-term sliding window to capture recent feedback and incorporates persistent long-term storage to retain condensed insights. This combination allows for the utilization of both detailed immediate experiences and high-level abstractions. SCM [84] selectively activates the most relevant long-term knowledge to combine with short-term memory, enabling reasoning over complex contextual dialogues. SWIFTSAGE [87] employs a small LM to manage short-term memory for generating intuition and associative thinking, while utilizing a LLM for handling long-term memory to generate well-considered decisions.

Memory Formats: Information can be stored in memory using various formats, each offering unique advantages. For example, natural languages can retain comprehensive semantic information, while embeddings can enhance the efficiency of memory reading. In the following, we present four types of commonly used memory formats.

- *Natural Languages.* Using natural languages for task reasoning/programming enables flexible, semantic-rich storage/access. For instance, Reflexion [125] stores experiential feedback in natural language within a sliding window. Voyager [133] employs natural language descriptions to represent skills within the Minecraft game, which are directly stored in memory.

- *Embeddings.* Using embeddings to store information can enhance memory retrieval and reading efficiency. For example, MemoryBank [158] encodes each memory segment into an embedding vector, building an indexed corpus for retrieval. GITM [161] represents reference plans as embeddings to facilitate matching and reuse. ChatDev [113] encodes dialogue history into vectors for retrieval.

- *Databases.* External databases provide structured storage, and one can manipulate the memories with efficient and comprehensive operations. For example, ChatDB [61] utilizes a database as symbolic long-term memory. SQL statements generated by the LLM controller can accurately operate on the database.

- *Structured Lists.* Another type of memory format is the structured list, based on which the information can be delivered in a more concise and efficient manner. For example, GITM [161] stores action lists for sub-goals in a hierarchical tree structure. The hierarchical structure explicitly captures the relationships between goals and corresponding plans. RET-LLM [102] initially converts natural language sentences into triplet phrases, and subsequently stores them in memory.

Above, we mainly discuss the internal designs of the memory module. In the following, we turn our focus to memory operations, which are used to interact with external environments.

Memory Operations: There are three critical memory operations include reading, writing, and self-reflection. In the following, we introduce these operations more in detail.

- *Memory Reading.* The key to memory reading lies in extracting information from the memory. Usually, there three commonly used criteria for information extraction, that is, the recency, relevance, and importance [109]. Memories that are more recent, relevant, and important are more likely to be extracted. Formally, we conclude the following equation to extract information:

$$m^* = \arg \min_{m \in M} \alpha s^{rec}(q, m) + \beta s^{rel}(q, m) + \gamma s^{imp}(m), \quad (1)$$

where q is the query, for example, the task that the agent should address or the context in which the agent is situated. M is the set of all memories. $s^{rec}(\cdot)$, $s^{rel}(\cdot)$ and $s^{imp}(\cdot)$ are the scoring functions for measuring the recency, relevance, and importance of the memory m . It should be noted that s^{imp} only reflects the characters of the memory itself, thus it is unrelated to the query q . α , β and γ are balancing parameters. By assigning them with different values, one can obtain various memory

reading strategies. For example, by setting $\alpha = \gamma = 0$, many studies [102, 161, 133, 49] only consider the relevance score s^{rel} for memory reading. By assigning $\alpha = \beta = \gamma = 1.0$, [109] equally weights all the above three metrics to extract information from the memory.

- *Memory Writing.* Agents can acquire knowledge and experiences by storing significant information in their memories. During the writing process, there are two potential problems that should be carefully addressed. On one hand, it is crucial to address how to store information that is similar to existing memories (*i.e.*, memory duplicated). On the other hand, it is important to consider how to remove information when the memory reaches its storage limit (*i.e.*, memory overflow). These problems can be resolved based on the following strategies. (1) *Memory Duplicated.* To incorporate similar information, people have developed various methods for integrating new and previous records. For instance, in [108], the successful action sequences related to the same sub-goal are stored in a list. Once the size of the list reaches $N(=5)$, all the sequences in it are condensed into a unified plan solution using LLMs. The original sequences in the memory are replaced with the newly generated one. Augmented LLM [121] aggregates duplicate information via count accumulation, avoiding redundant storage. Reflexion [125] consolidates related feedback into high-level insights, replacing raw experiences. (2) *Memory Overflow.* In order to write information into the memory when it is full, people design different methods to delete existing information to continue the memorizing process. For example, in ChatDB [61], memories can be explicitly deleted based on the user’s command. RET-LLM [102] uses a fixed-size cyclic buffer for memory, overwriting the oldest entries based on a first-in-first-out (FIFO) scheme.

- *Memory Reflection.* This operation seeks to empower agents with the ability to condense and deduce more advanced information, or verify and correct their own actions autonomously. It assists agents in comprehending their own and others’ attributes, preferences, objectives, and connections, which in turn directs their behaviors. Previous studies have studied various forms of memory reflection, that is, (1) *Self-summarization.* Reflection can be utilized to condense the agent’s memories into higher-level concepts. In [109], the agent has the capability to summarize its past experiences stored in memory into broader and more abstract insights. Specifically, the agent first generates three key questions based on its recent memories. Then, these questions are used to query the memory to obtain relevant information. Building upon the acquired information, the agent generates five insights, which reflect the agent high-level ideas. Additionally, reflection can occur hierarchically, meaning that insights can be generated based on existing insights. (2) *Self-verification.* Another form of reflection involves evaluating the effectiveness of the agent’s actions. In [133], the agent aims to accomplish tasks in Minecraft. During each execution round, the agent utilizes GPT-4 as a critic to assess whether the current action is sufficient to achieve the desired task. If the task fails, the critic offers feedback by suggesting approaches for completing the task. Replug [124] employs a training scheme to further adapt the retrieval model to the target language model. Specifically, it utilizes a language model as a scoring function to assess the contribution of each document towards reducing the perplexity of the language model. The retrieval model parameters are updated by minimizing the KL divergence between the retrieval probabilities and the language model scores. This approach effectively evaluates the relevance of the retrieved results and adjusts them based on feedback from the language model. (3) *Self-correction.* In this type of reflection, the agent can correct its behaviors by incorporating feedback from the environment. In MemPrompt [96], the model can adjust its understanding of the tasks based on user feedback for generating more accurate answers. In [137], the agent is designed to play Minecraft, and it takes actions based on predefined plans. When the plan fails, the agent rethinks its plan and changes it to continue the exploration process. (4) *Empathy.* Memory reflection can also be leveraged to enhance the agent’s empathy capability. In [49], the agent is a chatbot, but it generates utterances by considering the human cognition process. After each round of conversation, the agent evaluates the impact of his words on the listener and updates his beliefs about the listener’s states.

2.1.3 Planning Module

When humans face a complex task, they first break it down into simple subtasks and then solve each subtask one by one. The planning module empowers LLM-based agents with the ability to think and plan for solving complex tasks, which makes the agent more comprehensive, powerful, and reliable. In the following, we present two types of planning modules.

Planning without Feedback: In this method, the agent does not receive feedback in the planning process. The plans are generated in a monolithic manner. The following are many representative planning strategies in this direction.

- *Subgoal Decomposition.* Some researchers intend to let LLMs think step by step to solve complex tasks. Chain of Thought (CoT) [138] has become a standard technique for allowing large models to solve complex tasks. It proposes a simple but effective prompting method, which takes the process of solving complex reasoning problems step by step with a small number of language examples in the prompt. Zero-shot-CoT [72] allows LLMs to autonomously generate reasoning processes for complex problems by prompting the model to "think step by step", and experimentally proves that LLMs are decent zero-shot reasoners. In [63], the LLMs act as Zero-Shot Planners to make goal-driven decisions in an interactive simulation environment. [53] further uses environmental objects and object relationships as additional inputs for LLMs action plan generation, providing the system with a sense of its surroundings to generate plans. ReWOO [147] introduces a paradigm of separating planning from external observations, enabling the LLM to act as a planner that directly generates a series of independent plans without requiring external feedback. In summary, by decomposing complex tasks into executable sub-tasks, the ability of the large language model to make plans and decisions is significantly improved.

- *Multi-path Thought.* Based on CoT, some researchers suggest that the process of human thinking and reasoning is a tree-like structure with multiple paths to the final result. Self-consistent CoT (CoT-SC) [135] assumes that each complex problem has multiple ways of thinking to deduce the final answer. In specific, CoT is utilized to generate several paths and answers of reasoning, where the answer with the most occurrences will be selected as the final answer output. Tree of Thoughts (ToT) [150] assumes that humans tend to think in a tree-like way, when making decisions on complex problems for planning purposes, where each tree node is a thinking state. It uses LLM to generate evaluations or votes of thoughts, which can be searched using BFS or DFS. These methods improve the performance of LLMs on complex reasoning tasks. [153] discusses the constrained language planning problem. It generates extra scripts and filtering them to improve the quality of script generation. Among the several generated scripts, the script selection is determined by (1) the cosine similarity between the script and the goal, (2) whether the script contains the goal constraint keywords. DEPS [137] uses vision-language models as selectors to choose the optimal path in optional subtasks. SayCan [2] combines the probability from the language model (the probability that an action will be useful for the high-level instruction) with the probability from the value function (the probability of successfully executing the said action) and selects the action to take. Then, it appends to the robot response and queries the model again to repeat the process until the output step terminates. In conclusion, multi-path thought further empowers the agent to solve more complex planning tasks, but it also brings additional computational burden.

- *External Planner.* LLMs, even if having significant zero-sample planning power, are not as reliable as traditional planners in many cases, especially when faced with domain-specific long-term planning problems. LLM+P [90] transforms natural language descriptions into a formal Planning Domain Definition Language (PDDL). Then, results are computed using an external planner and transformed into natural language by the LLMs finally. Likewise, LLM-DP [24] utilizes the LLM to convert observation, current world state, and target objectives into PDDL format. This information is then passed to an external symbolic planner, which efficiently determines the optimal sequence of actions from the current state to the target state. MRKL [71] is a modular, neural-symbolic AI architecture, where LLMs process the input texts, routes them to each of the experts, and then pass them through the LLMs' outputs. CO-LLM [156] consider that LLMs are good at generating high-level plans, but not good at low-level controlling. They use a heuristically designed low-level planner to robustly implement base actions according to high-level plans. With expert planners in the sub-task domains, it is possible for LLM to navigate the planning of complex tasks in specific domains. LLM-based agents' generalized knowledge is difficult to perform best on tasks in all domains, but combining it with the expert knowledge from external planners can be effective to improve performance.

Planning with Feedback: When humans deal with tasks, the experience of success or failure directs them to reflect on themselves and improves their planning ability. The experiences are often obtained and accumulated based on external feedback. To simulate such human capability, many researchers have designed planning modules, which can receive feedback from the environment, humans, and models, significantly improving the planning ability of the agents.

- *Environmental Feedback.* In many studies, the agents make plans based on environmental feedback. For example, ReAct [151] extends the agent's action space to a collection of actions and language space. Explicit reasoning and actions are performed sequentially, and when the feedback

from an action does not have the correct answer, reasoning will be performed again until obtaining the correct answer. Voyager [133] self-refines the agent generation scripts by acting on three types of feedback until it passes self-validation and is deposited in the skills library. Ghost [161], DEPS [137] can receive feedback from the environment, including information about the current state of the agent in the environment, and the information about the success or failure of each action performed. By integrating this feedback, the agents can update their understanding of the environment, improve their strategy and adapt their behaviors. Based on Zero-Shot Planners [63], Re-prompting [117] uses the pre-condition errors information to detect whether the agent is capable of completing the current planning. It also uses the precondition information to re-prompt the LLM to complete the closed-loop control. Inner Monologue [64] appends three types of environmental feedback: successful execution of sub-tasks, passive scene description, and active scene description to instruction, thus enabling closed-loop planning for LLM-based agents. Introspective Tips [17] allows LLM to introspect through the history of the environmental feedback. LLM-Planner [127] introduces a grounded re-planning algorithm that dynamically updates plans generated by LLMs when encountering object mismatches and unattainable plans during task completion. In Progprompt [126], assertions are incorporated into the generated script to provide environment state feedback, allowing for error recovery in case the action’s preconditions are not satisfied. In summary, environmental feedback serves as a direct indicator of planning success or failure, thereby enhancing the efficiency of closed-loop planning.

- *Human Feedback.* The agent can make plans with the help of real human feedback. Such signal can help the agent to better align with practical settings, and may also alleviate the hallucination problem. In Voyager [133], it is mentioned that human can act as a critic to ask Voyager to change the previous round of code through multi-model feedback. OpenAGI [51] proposes a reinforcement learning with task feedback (RLTF) mechanism that utilizes manual or benchmark evaluation to improve the capabilities of the LLM-based agent.

- *Model Feedback.* Language models can be used as critics to criticise and improve the generated plans. Self-Refine [97] introduces the self-refine mechanism to improve the output of LLMs by iterating feedback and improvement. Specifically, the LLM is utilized as a generator, feedback provider, and refiner. First, the generator is used to generate an initial output, then the feedback provider presents specific and actionable feedback for the output, and finally, the refiner is used to improve the output using the feedback. The reasoning power of LLM is improved by an iterative feedback loop between the generator and the critic. Reflexion [125] is a framework for enhancing agent through verbally feedback, which introduces memory mechanism. The actor first generates the action, then the evaluator generates the evaluation, and finally a summary of the past experience is generated by a self-reflective model. The summary will be stored in memory to further improving the generation of the actor through the past experience. World model typically refers to an agent’s internal representation of the environment, which is utilized for internal simulation and abstraction of the environment. It aids agents in reasoning, planning, and predicting the effects of different actions on the environment. RAP [57] involves utilizing LLMs both as the world model and as the agent. During the reasoning process, the agent constructs a reasoning tree, while the world model provides rewards as feedback. The agent performs MCTS (Monte Carlo Tree Search) on the reasoning tree to obtain the optimal plan. Similarly, REX [103] introduces an accelerated MCTS approach where rewards feedback are furnished by either the environment or the LLM. Tips [17] can learn from demonstrations of other expert models. In the MAD(Multi-Agent Debate) [83] framework, multiple agents express their arguments in an "eye-for-an-eye" fashion, and a judge manages the debate process to reach a final solution. The MAD framework encourages divergent thinking in LLM, which facilitates tasks requiring deeper thinking.

In summary, the planning module is important for the agents to solve complex tasks. While external feedback can always help to make informed plans, it does not always exist. Planning with and without feedback are both important for building LLM-based agents.

2.1.4 Action Module

The action module aims to translate the agent’s decisions into specific outcomes. It directly interacts with the environment, determining the agent’s effectiveness in completing tasks. This section offers an overview of the action module, primarily examining the action target, strategy, space, and influence.

Action Target: Action target means the goal of the action, which is usually specified by the real-humans or the agent itself. The three main action targets include task completion, dialogue interaction, and environment exploration and interaction.

- *Task Completion.* A fundamental goal of the action module is to complete a specific task in a logical manner. The type of tasks varies in different scenarios, leading to the necessary design of the action module. For example, Voyager [133] utilizes LLMs as action module to guide agents in exploring and collecting resources to complete sophisticated tasks in Minecraft. GITM [161] decomposes an overall task into executable actions, enabling the agents to complete the routine activities step by step. Generative Agents [109] similarly conducts executable action sequences by hierarchically decomposing high-level task planning.

- *Dialogue Interaction.* The ability of LLM-based autonomous agents to conduct a natural language dialogue with humans is essential since human users usually need to obtain the agent status or complete collaborative tasks with agents. Previous work has improved the dialogue interaction ability of agents in diverse domains. For example, ChatDev [113] conducts related dialogues among employees of a software development company. DERA [104] enhances the dialogue interaction in an iterative manner. [31, 139] utilizes interaction dialogues between different agents, and therefore encourages them have similar opinions about certain topic.

- *Environment Exploration and Interaction.* Agents are able to acquire new knowledge through interacting with the environment and enhance themselves by summarizing recent experiences. In this way, the agent can generate novel behaviors which are increasingly attuned to the environment and aligned with common sense. For example, Voyager [133] conducts continual learning by allowing the agent to explore in the open-ended environment. Memory-enhanced reinforcement learning (MERL) framework in SayCan [2] continuously accumulates the textual knowledge and then adjusts the agent action scheme based on external feedback. Similarly, GITM [161] allows agents to continually collect the textual knowledge and therefore adapt their behaviors based on the environment feedback.

Action Strategy: Action strategy means the methods that the agent produces the actions. In existing work, these strategies may be memory recollection, multi-round interaction, feedback adjustment and incorporating external tools. In the following, we detail these strategies one by one.

- *Memory Recollection.* Memory recollection techniques facilitate agents in making informed decisions based on stored experiences in memory modules [109, 78, 161]. Generative Agents [109] maintain a memory stream of dialogues and experiences. When taking actions, relevant memory snippets are retrieved as conditional inputs for the LLMs to ensure consistent actions. GITM [161] uses memories to guide actions, like moving towards previously discovered locations. CAMEL [78] constructs a memory stream of historical experiences, enabling the LLMs to generate informed actions based on these memories.

- *Multi-round Interaction.* This method seeks to leverage dialogue context across multiple rounds for agents to determine appropriate responses as actions [113, 104, 31]. ChatDev [113] encourages the agents to act based on their dialogue histories with others. DERA [104] proposes a novel dialogue agent, where during the communication process, the researcher agent can provide useful feedback to guide the action of the decider agent. [31] constructs a multi-agent debate (MAD) system, where each LLM-based agent engages in iterative rounds of interaction, exchanging challenges and insights, with the ultimate aim of achieving consensus. ChatCot [20] employs a multi-round dialogue framework to model the process of chain-of-thought reasoning, seamlessly integrating reasoning and tool usage through conversational interactions.

- *Feedback Adjustment.* The effectiveness of human feedback or engagement with the external environment has been demonstrated in facilitating agents to adapt and enhance their action strategies [133, 99, 2]. For instance, Voyager [133] enables agents to improve their policies after experiencing action failures or validate successful strategies using feedback mechanisms. The Interactive Construction Learning Agent (ICLA) [99] utilizes user feedback on initial actions to iteratively enhance plans, leading to the development of more precise strategies. SayCan [2] employs a reinforcement learning framework where the agent continuously adjusts actions based solely on environment feedback, enabling automated trial-and-error based enhancement.

- *Incorporating External Tools.* LLM-based autonomous agents can be enhanced through the incorporation of external tools and the expansion of knowledge sources. On the one hand, the agents can be equipped with the ability to access and employ a variety of APIs, databases, web applications, and other external resources during the training or inference stage. For example, Toolformer [119] is trained to determine the appropriate APIs to call upon, the timing for these calls, and the optimal method of integrating the returned results into future token prediction. ChemCrow [8] designs a

chemistry-oriented LLM-based agent, which incorporates seventeen expert-designed tools, to perform tasks including organic synthesis, drug discovery, and materials design. ViperGPT [128] presents a code-generation framework, which assembles vision-and-language models into subroutines that is able to return results for any given query. HuggingGPT [123] employs LLMs to connect diverse AI models in machine learning communities (*e.g.*, Hugging Face) to resolve AI tasks. In specific, HuggingGPT proposes a meta-learning approach to train LLMs to generate code snippets, and then use these snippets to call upon the desired AI models from the external community hub. On the other hand, the scope and quality of knowledge that agents directly access can be broadened with the help of external knowledge sources. In previous work, the external knowledge sources contains databases, knowledge graphs, web pages, and so on. For example, Gorilla [111] is able to effectively provide appropriate API calls, since it is trained on three extra machine learning hub datasets: Torch Hub, TensorFlow Hub, and HuggingFace. WebGPT [105] proposes an extension that can incorporate the relevant results retrieved from websites into prompts when using ChatGPT, thus leading to more accurate and timely conversations. ChatDB [61] is an AI database assistant that utilizes SQL statements generated by the LLM controller to operate the external database accurately. GITM [161] uses LLMs to generate explainable results of text mining tasks, which employs a novel text mining pipeline that integrates LLMs, knowledge extraction and topic modeling modules.

Action Space: The action space of LLM-based agents refers to the set of possible actions that can be performed by the agent. This stems from two main sources: external tools that expand the action capabilities, and the agent’s own knowledge and skills such as language generation and memory-based decision making. Specifically, external tools include search engines, knowledge bases, computing tools, other language models, and visual models. By interfacing with these tools, agents can execute diverse realistic actions like information retrieval, data querying, mathematical computations, sophisticated language production, and image analysis. The agent’s self-acquired knowledge based on the language model can empower the agent to plan, generate language, and make decisions, further expanding its action potential.

- *Tools.* Various external tools or knowledge sources provide much richer action capabilities for agents, including APIs, knowledge bases, visual models, language models, and so on. (1) *APIs.* Leveraging external APIs to complement and expand action space is a popular paradigm in recent years. For example, HuggingGPT [123] uses search engines, transforming queries into search request to fetch relevant code. [105, 118] propose to automatically generate queries to extract relevant content from external web pages when responding to user request. TPTU [118] interfaces with both Python interpreters and LaTeX compilers to execute sophisticated computations such as square roots, factorials and matrix operations. Another type of APIs is the ones that can be directly invoked by LLMs based on natural language or code inputs. For instance, ToolFormer [119] is an LLM-based tool transformation system that can automatically convert a given tool into another one with different functionalities or formats based on natural language instructions. API-Bank [80] is an LLM-based API recommendation agent that can automatically search and generate appropriate API calls for various programming languages and domains. API-Bank also provides an interactive interface for users to easily modify and execute the generated API calls. Similarly, ToolBench [115] is an LLM-based tool generation system that can automatically design and implement various practical tools based on natural language requirements. The tools generated by ToolBench include calculators, unit converters, calendars, maps, charts, etc. All these agents utilize external APIs as their external tools, and provide interactive interfaces for users to easily modify and execute the generated or transformed tools. (2) *Knowledge Bases.* Connecting to external knowledge bases can help the agents to obtain specific domain information for generating more realistic actions. For example, ChatDB [61] employs SQL statements to query databases, facilitating actions by the agents in a logical manner. ChemCrow [8] presents an LLM-based chemical agent aimed at accomplishing tasks in the fields of organic synthesis, drug discovery, and material design, with the help of seventeen expert-designed tools. MRKL Systems [71], OpenAGI [51] incorporates various expert systems such as knowledge bases and planners, invoking them to access domain-specific information in a systematic manner. (3) *Language Models.* Language models can also act as tools to enrich the action spaces. For example, MemoryBank [158] employs two language models, one aims to encode input text while the other is responsible to match the arrived query statements to provide auxiliary textual retrieval. ViperGPT [128] firstly uses Codex, which is based on language model, to generate Python code from text descriptions, and then executes the code to complete the given tasks. TPTU [118] incorporates various LLMs to accomplish a wide range of language generation tasks such as generating code, producing lyrics, and more. (4) *Visual Models.* Integrating visual models with agents can broaden the

action space into the multi-modal domain. ViperGPT [128] leverages models like GLIP to extract image features for visual content-related actions. HuggingGPT [123] proposes to use visual models for image processing and generation.

- *Agent’s Self Knowledge.* An agent’s self-acquired knowledge also affords diverse behaviors, such as leveraging LLM’s generative powers for planning and language production, making decisions based on memories, etc. An agent’s self-acquired knowledge such as memories, experiences, and language capabilities enable diverse tool-free actions. For instance, Generative Agents [109] maintains comprehensive memory logs of all past dialogues. When taking actions, it retrieves relevant memory snippets as conditional inputs to guide the LLM in autoregressively generating logical and consistent language plans. GITM [161] constructs a memory base of experiences like discovered villages or collected resources. When acting, it queries the memory base for relevant entries, such as recalling a previous village direction to move towards that location again. SayCan [2] develops a reinforcement learning framework where the agent repeatedly adjusts actions like motions purely based on environment feedback for automated trial-and-error improvements, without any human demonstrations or interventions. Voyager [133] leverages the LLM’s broad language generation capabilities to synthesize free-form textual solutions like Python code snippets or conversational responses tailored to current needs. Similarly, LATM [10] empowers LLMs to utilize Python code for crafting its own reusable tools, fostering a flexible approach to problem-solving. CAMEL [78] records all historical experiences in a memory stream. The LLM then draws from relevant memories to autoregressively generate high-level textual plans outlining intended future courses of action. ChatDev [113] equips LLM agents with a dialogue history memory to determine appropriate conversational responses and actions based on context. In summary, an agent’s internal knowledge enables a diverse repertoire of tool-free actions via approaches like memory recollection, feedback adjustment, and open-ended language generation.

Action Influence: Action influence refers to the consequences of an action, which encompass changes in the environment, alterations in the internal states of the agent, triggering of new actions, and impacts on human perceptions. In the following, we elaborate on these consequences.

- *Changing Environments.* Actions can directly alter environment states, such as moving agent positions, collecting items, constructing buildings, etc. For instance, GITM[161] and Voyager [133] change environment states by executing action sequences that complete tasks.

- *Altering Internal States.* Actions taken by agent can also change the agent itself, including updating memories, forming new plans, acquiring novel knowledge, and more. For example, in Generative Agents [109], memory streams are updated after performing actions within the system. SayCan [2] enables agents to take actions to update understandings of the environment and thus adapt the subsequent behaviors.

- *Triggering New Actions.* For most LLM-based autonomous agents, actions are usually taken in a sequential manner, that is, the former action can trigger the next new action. For example, Voyager [133] seeks to construct buildings after collecting the environmental resources in Minecraft scenario. Generative Agents[109] firstly decomposes the plans into sub-goals, and then conducts a series of related actions to complete each sub-goal.

- *Impacting Human Perceptions.* The language, imagery and other modalities from actions directly influence user perceptions and experiences. For example, CAMEL [78] generates utterances that are coherent, informative, and engaging for conversational agents. ViperGPT [128] produces visuals that are realistic, diverse, and relevant for image generation tasks. HuggingGPT [123] can generate visual outputs, such as images, to extend human perceptions into the realm of visual experiences. Moreover, HuggingGPT can also generate multimodal outputs, such as code, music, and video, to enrich human interactions with different media forms.

2.2 Learning Strategy

Learning stands as an essential mechanism for humans to attain both knowledge and skills, fostering the augmentation of their capabilities—a significance extended profoundly to the realm of LLM-based agents. Through the process of learning, these agents are imbued with the capacity to demonstrate heightened mastery in adhering to instructions, deftly navigating intricate tasks, and seamlessly adapting to unprecedented and diverse environments. This transformative process empowers these agents to evolve beyond their initial programming, enabling them to perform tasks with greater finesse

Table 1: Summary of the construction strategies of representative agents (more agents can be seen on <https://github.com/Paitesanshi/LLM-Agent-Survey>). For the profile module, we focus on the profile generation strategies, and use ①, ② and ③ to represent the handcrafting method, LLM-generation method, and dataset alignment method, respectively. For the memory module, we focus on the implementation strategies for memory operation and memory structure. For memory operation, we use ① and ② to indicate that the model only has read/write operations and has read/write/reflection operations, respectively. For memory structure, we use ① and ② to represent unified and hybrid memories, respectively. For the planning module, we use ① and ② to represent planning w/o feedback and w/ feedback, respectively. For the action module, we use ① and ② to represent that the model does not use tools and use tools, respectively. Beyond the above agent design strategies, we also present the learning strategies (LS) of these agents. In specific, we use ①, ② and ③ to represent learning from examples, human feedback and environment feedback, respectively.

Model	Profile	Memory		Planning	Action	LS	Time
		Operation	Structure				
WebGPT[105]	-	-	-	-	②	②	12/2021
SayCan[2]	-	-	-	①	②	③	04/2022
MRKL[71]	-	-	-	①	②	-	05/2022
Inner Monologue[64]	-	-	-	②	②	③	07/2022
Social Simulacra[110]	②	-	-	-	①	-	08/2022
ReAct[151]	-	-	-	②	②	③	10/2022
REPLUG[124]	-	②	①	-	①	-	01/2023
MALLM[121]	-	②	②	-	①	-	01/2023
DEPS[137]	-	-	-	②	②	③	02/2023
Toolformer[119]	-	-	-	①	②	①	02/2023
Reflexion[125]	-	②	②	②	①	③	03/2023
CAMEL[78]	① ②	-	-	②	①	-	03/2023
ViperGPT[128]	-	-	-	-	②	-	03/2023
HuggingGPT[123]	-	①	①	①	②	-	03/2023
Generative Agents[109]	①	②	②	①	①	-	04/2023
LLM+P[90]	-	-	-	①	②	-	04/2023
ChemCrow[8]	-	-	-	②	②	-	04/2023
API-Bank[80]	-	-	-	②	②	①	04/2023
OpenAGI[51]	-	-	-	②	②	①	04/2023
AutoGPT[45]	-	①	②	②	②	③	04/2023
SCM[84]	-	①	②	-	①	-	04/2023
Socially Alignment[92]	-	①	②	-	①	①	05/2023
GITM[161]	-	②	②	②	①	③	05/2023
Voyager[133]	-	②	①	②	①	③	05/2023
Introspective Tips[17]	-	②	①	②	①	①③	05/2023
RET-LLM[102]	-	②	①	-	①	①	05/2023
ChatDB[61]	-	②	①	②	②	-	06/2023
S^3 [50]	③	②	②	①	①	-	07/2023
ChatDev[113]	①	②	①	②	①	-	07/2023
ToolBench[115]	-	-	-	②	②	①	07/2023
MemoryBank[158]	-	②	②	-	①	-	07/2023
MetaGPT[58]	①	②	②	②	②	-	08/2023

and flexibility. In this chapter, we will delve into various learning strategies employed by LLM-based agents and explore their far-reaching impacts.

Learning from Example: Learning from examples is a foundational process that underpins human and AI learning. In the realm of LLM-based agents, this principle is embodied in fine-tuning, where these agents refine their skills through exposure to real-world data.

- *Learning from Human-Annotations.* In the pursuit of harmony with human values, integrating human-generated feedback data becomes a cornerstone of fine-tuning LLMs. This practice is particularly crucial in shaping intelligent agents designed to complement or even replace human involvement in specific tasks. The CoH approach, proposed by Liu et al. [91], involves a multi-step

process where the LLM generates responses, assessed by human reviewers to differentiate favorable from unfavorable outcomes. This amalgamation of responses and evaluations contributes to the fine-tuning process, arming the LLM with a comprehensive understanding of errors and the ability to rectify them while staying aligned with human preferences. Despite the simplicity and directness of this approach, it is encumbered by substantial annotation costs and time, posing challenges in rapid adaptation to disparate scenarios. MIND2WEB [26] fine-tunes using human-annotated real-world website task data from diverse domains, resulting in a general agent that performs effectively across actual websites.

- *Learning from LLMs' Annotations.* During pre-training, LLMs acquire a wealth of world knowledge from extensive training data. After fine-tuning and alignment with humans, they exhibit capabilities akin to human judgment, as exemplified by models like ChatGPT and GPT-4. Hence, we can utilize LLMs for annotation tasks, which can significantly reduce costs compared to human annotation, offering the potential for extensive data acquisition. Liu et al. [92] proposed a stable alignment approach for fine-tuning LLMs based on social interaction. They devised a sandbox environment containing multiple agents, each responding to a probing question. These responses are then evaluated and scored by nearby agents and ChatGPT. Subsequently, the responding agent refines their answer based on these evaluations, which is then re-scored by ChatGPT. This iterative process yields a substantial corpus of interactive data, which is subsequently employed for fine-tuning LLMs using contrastive supervised learning. In Refiner [112], the generator is asked to generate intermediate steps and a critic model is introduced to generate structured feedback. Then, the feedback records is used to fine-tune the generator model to improve inference ability. In ToolFormer [119], a pre-training corpus is marked with potential API calls using LLMs. Then, LLMs are fine-tuned on this annotated data to learn how and when to use APIs, and integrate API results into their text generation. Similarly, ToolBench [115] is also a dataset entirely generated using ChatGPT, designed for fine-tuning and enhancing LLMs' proficiency in utilizing tools. ToolBench comprises an extensive collection of API descriptions, accompanied by directives that outline tasks to be accomplished using specific APIs, along with the corresponding sequences of actions to fulfill these directives. The fine-tuning process using ToolBench results in a model termed ToolLLaMA, which demonstrates performance comparable to ChatGPT. Notably, ToolLLaMA exhibits robust generalization capabilities even when confronted with previously unseen APIs.

Learning from Environment Feedback: In many cases, intelligent agents need to proactively explore their surroundings and interact with the environment. Therefore, they require the ability to adapt to the environment and enhance their capabilities from environmental feedback. In the field of reinforcement learning, agents learn by continuously exploring the environment and adapting based on environmental feedback [68, 82, 98, 152]. This principle also holds for intelligent agents based on LLMs. Voyager [133] follows an iterative prompting method, where agents perform actions, gather environment feedback, and continuously iterate until newly acquired skills are validated and added to the skill repository through self-verification. Similarly, LMA3 [22] autonomously sets goals and executes actions in interactive environments, with LLM scoring its performance as a reward function. By iterating this process, LMA3 independently learns a wide range of skills. Meanwhile, GITM [161] and Inner Monologue [64] integrate environmental feedback into the closed-loop process of planning based on large-scale language models. Furthermore, creating an environment that closely mirrors reality also contributes significantly to enhancing the agent's performance. WebShop [149] has developed a simulated e-commerce environment where the agent can engage in activities such as searching and making purchases, receiving corresponding rewards and feedback in return. In [145], an embodiment simulator is utilized to enable agents to interact within a simulated real-world environment, facilitating physical engagements that lead to the acquisition of embodied experiences. Subsequently, these experiences are employed to fine-tune the model, thereby enhancing its performance in downstream tasks.

Contrastive to learning from annotations, learning from environmental feedback distinctly encapsulates the autonomy and independence characteristic of LLM-based agents. This divergence exemplifies a profound interplay between environmental responsiveness and autonomous learning, fostering a nuanced understanding of agent behavior and adaptation.

Learning from Interactive Human Feedback: Interactive human feedback provides the agent with the opportunities to adapt, evolve, and refine their behaviors under human guidance in a dynamic manner. Compared to one-shot feedback, interactive feedback is more aligned with real-world scenarios. As the agents are learned in a dynamic process, they do more than just process static data

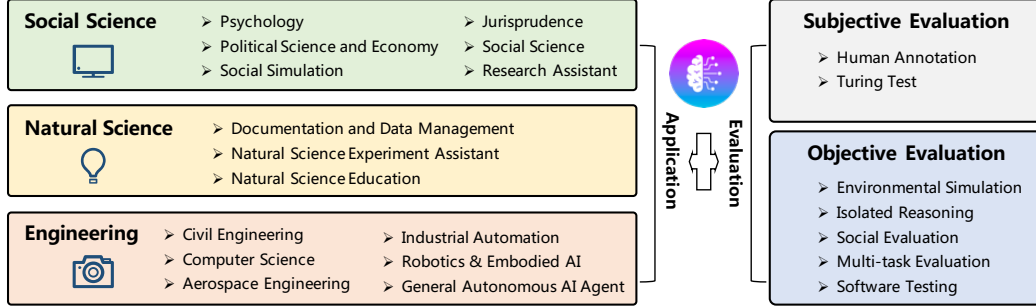


Figure 3: The applications (left) and evaluation strategies (right) of LLM-based agents.

- they participate in a continual refinement of their understanding, adaptation, and alignment with humans. For example, [156] incorporates a communication module that enables collaborative task completion via chat-based interaction and feedback from humans. As highlighted by [122], interactive feedback fosters key aspects such as reliability, transparency, immediacy, task characteristics, and the evolution of trust over time when learning the agents.

In the above sections, we summarize the previous work based on the agent construction strategies, where we focus on two aspects including the architecture design and parameter optimization. We present the correspondence between the previous work and our taxonomy in Table 1.

3 LLM-based Autonomous Agent Application

The application of LLM-based autonomous agents across various fields represents a paradigm shift in how we approach problem-solving, decision-making, and innovation. These agents, endowed with the capabilities of language comprehension, reasoning, and adaptation, are revolutionizing industries and disciplines by offering unprecedented insights, assistance, and solutions. In this section, we explore the transformative impact of LLM-based autonomous agents in three distinct domains: social science, natural science, and engineering (see the left part of Figure 3 for a global overview).

3.1 Social Science

Computational social science involves the development and application of computational methods to analyze complex human behavioral data, often at a large scale, including data from simulated scenarios [74]. Recently, LLMs have shown impressive human-like capabilities, which hold promise for research in social computational science [54]. In the following, we present many representative domains that LLM-based agents have been applied to.

Psychology: LLM-based agents can be used in Psychology for conducting psychological experiments [1, 3, 95, 163]. In [1], LLM-based agents are leveraged to simulate psychological experiments including the ultimatum game, garden path sentence, Milgram shock experiment, and capacity for group intelligence. In the first three experiments, the LLM-based agent can reproduce current psychological findings, while the last experiment reveals "hyperaccuracy distortions" in some language models (including ChatGPT and GPT-4), which may affect downstream applications. In [3], the authors employ LLM-based agents to simulate two prototypical repeated games in the field of game theory: the Prisoner's dilemma and the battle of the sexes. They find that LLM-based agents show a psychological tendency to prioritize self-interest over coordination. As for the application on mental health, [95] discusses the advantages and disadvantages associated with the utilization of LLM-based agent to provide mental health support.

Political Science and Economy: Recent studies have employed LLM-based agents in the fields of political science and economics [5, 59, 163]. These agents are utilized to analyze partisan impressions and explore how political actors modify agendas, among other applications. Additionally, LLM-based agents can be utilized for ideology detection and predicting voting patterns [5]. Furthermore, recent research endeavors have focused on understanding the discourse structure and persuasive elements of political speech through the assistance of LLM-based agents [163]. In the study conducted by Horton et al. [59], LLM-based agents are provided with specific traits such as talents, preferences,

and personalities. This allows researchers to explore economic behavior in simulated scenarios and gain novel insights into the field of economics.

Social Simulation: Conducting experiments with human societies is often expensive, anti-ethical, anti-moral, or even unachievable. In contrast, agent-based simulation enables researchers to construct hypothetical scenarios under specific rules to simulate a range of social phenomena, e.g., the propagation of harmful information. The researcher engages in both observes and intervenes within the system at both macro and micro levels, which enables them to study counterfactual events [110, 81, 76, 109, 89, 73, 50, 140]. This process allows decision makers to develop more rational rules or policies. For example, Social Simulacra [110] simulates an online social community and explores the potential of utilizing LLM-based agent simulations to aid decision-makers to improve community regulations. [81, 76] investigates the behavioral characteristics of LLM-based agents in social networks and the potential impact on social networks. In addition, Generative Agents [109] and AgentSims[89] construct towns comprising multiple agents. SocialAI School [73] employs simulations to investigate fundamental social cognitive skills that manifest during the course of child development. S³ [50] focuses on Propagation of information, emotion and attitude, while [140] concentrates on the transmission of infectious diseases.

Jurisprudence: LLM-based agent can serve as aids in legal decision-making processes, facilitating judges in rendering more informed judgements [23, 56]. Blind Judgement [56] employs several language models to simulate the decision-making processes of multiple judges. It gathers diverse opinions and consolidates the outcomes through a voting mechanism. ChatLaw [23] is a prominent Chinese legal fine-tuned LLM. To address the issue of model hallucination, ChatLaw incorporates a fusion of database search and keyword search techniques to enhance accuracy. Concurrently, a self-attention mechanism is employed to augment the LLM’s capability in mitigating the impact of inaccuracies in the reference data.

Social Science Research Assistant : Apart from conducting specialized research within distinct domains of social computing, LLM-based agent can play the role of research assistants [6, 163]. They have the potential to aid researchers in tasks like generating article abstracts, extracting keywords and generating scripts. [163]. Additionally, LLM-based agent can serve as a writing aids, and they even possess the capability to identify novel research inquiries for social scientists [6].

The development of LLM-based agents holds great promise for bringing new research methods to the field of computational social science research. However, the application of LLM-based agent on social computing still presents several challenges and limitations [163, 6]. Two primary concerns are bias and toxicity, as LLMs are trained from real-world datasets, which makes them susceptible to inherent biases, discrimination content, and unfairness. When LLM is introduced, it may produce biased information, which is further taken to train LLM, leading to the amplification of bias. Causality and interpretability pose another challenge, particularly in the context of social science where robust causal relationships are often required. Probability-based LLMs tend to lack clear interpretability.

3.2 Natural Science

The application of LLM-based agents in the field of natural sciences is on the rise due to the rapid advancement of large language models. These agents bring new opportunities for scientific research in the natural sciences. In the following, we present many representative domains, where LLM-based agents can play important roles.

Documentation and Data Management: In the realm of natural scientific research, a substantial amount of literature and data often necessitates meticulous collection, organization, and extraction, entailing significant time and human resources. LLM-based agents exhibit robust natural language processing capabilities, enabling them to effectively access a wide array of tools to browse the Internet, documents, databases, and other information sources. This capacity empowers them to attain vast amounts of data, seamlessly integrate and manage it, and thereby provide valuable assistance in scientific research [7, 70, 8]. By utilizing APIs to access the Internet, agents in [7] can efficiently query and retrieve real-time, relevant information, aiding in tasks such as question answering and experiment planning. ChatMOF [70] leverages LLMs to extract key points from human-written textual descriptions and formulate a plan to invoke necessary toolkits in order to predict properties and structures of metal-organic frameworks. The utilization of databases further enhances the agent’s performance in specific domains, owing to the wealth of tailored data they contain. For instance,

when accessing chemistry-related databases, ChemCrow [8] can verify the accuracy of compound representations or identify hazardous substances, thereby contributing to more accurate and informed scientific investigations.

Natural Science Experiment Assistant: LLM-based agents can operate autonomously, conducting experiments independently, as well as serve as a valuable tool to support scientists in their research projects [7, 8]. For example, [7] introduces an innovative agent system that leverages LLMs to automate the design, planning, and execution of scientific experiments. When provided with the experimental objectives as input, the system accesses the Internet and retrieves relevant documents to acquire the necessary information. Subsequently, it employs Python code to perform the essential calculations and ultimately executes the sequential steps of the experiment. Additionally, the ChemCrow [8] incorporates 17 meticulously crafted tools specifically designed to aid researchers in chemical research. Upon receiving the input objectives, ChemCrow offers insightful recommendations for experimental procedures while carefully highlighting potential safety risks associated with the proposed experiments.

Natural Science Education: Benefiting from the natural language capabilities, LLMs facilitate seamless communication with humans through natural language interactions, making them exciting educational tools that offer real-time question-answering and knowledge dissemination [7, 129, 30, 18]. For example, [7] proposes agent systems that serve as valuable educational tools for students and researchers to learn experimental design, methodologies, and analysis. They help foster critical thinking and problem-solving skills while encouraging a deeper comprehension of scientific principles. Math Agents [129] are entities that use artificial intelligence techniques to explore, discover, solve and prove mathematical problems. Math Agents can also communicate with humans and help them understand and use mathematics. [30] utilize the capabilities of CodeX [18] to achieve human-level automatic solving, explanation, and generation of university-level mathematical problems through few-shot learning. This achievement bears significant implications for higher education, offering advantages such as curriculum design and analysis tools, as well as automated content generation.

The utilization of LLM-based agents in supporting natural scientific research also entails certain risks and challenges. On one hand, LLMs themselves may be susceptible to illusions and other issues, occasionally providing erroneous answers, leading to incorrect conclusions, experimental failures, or even posing risks to human safety in hazardous experiments. Therefore, during experimentation, users must possess the necessary expertise and knowledge to exercise appropriate caution. On the other hand, LLM-based agents could potentially be exploited for malicious purposes, such as the development of chemical weapons, necessitating the implementation of security measures, such as human alignment, to ensure responsible and ethical use.

3.3 Engineering

LLM-based autonomous agents have shown great potential in assisting and enhancing engineering research and applications. In this section, we review and summarize the applications of LLM-based agents in several major engineering domains.

Civil Engineering: In civil engineering, LLM-based agents can be used to design and optimize complex structures such as buildings, bridges, dams, roads, etc. [99] proposes an interactive framework where human architects and AI agents collaborate to construct structures in a 3D simulation environment. The interactive agent can understand natural language instructions, place blocks, detect confusion, seek clarification, and incorporate human feedback, showing the potential for human-AI collaboration in engineering design.

Computer Science & Software Engineering: In the field of computer science and software engineering, LLM-based agents offer potential for automating coding, testing, debugging, and documentation generation [115, 113, 58, 29, 33, 44, 41]. ChatDev [113] proposes an end-to-end framework, where multiple agent roles communicate and collaborate through natural language conversations to complete the software development life cycle. This framework demonstrates efficient and cost-effective generation of executable software systems. ToolBench [115] can be used for tasks such as code autocompletion and code recommendation. For example, ToolBench can automatically complete function names and variable names in code, as well as to recommend code snippets. MetaGPT [58] abstracts multiple roles, such as product managers, architects, project managers, and engineers, to internally supervise code generation and enhance the quality of the final output code. This enables

low-cost software development. [29] presents a self-collaboration framework for code generation using LLMs, exemplified by ChatGPT. In this framework, multiple LLMs assume distinct "expert" roles for specific subtasks within a complex task. They collaborate and interact according to specified instructions, forming a virtual team that facilitates each other's work. Ultimately, the virtual team collaboratively addresses code generation tasks without requiring human intervention. GPT-Engineer [33], SmolModels [44] and DemoGPT [41] are open-source projects that focus on automating code generation through prompts to complete development tasks. LLMs can also be applied to code bug testing and correction. LLIFT [79] utilizes LLMs to aid in static analysis for detecting code vulnerabilities, striking a balance between precision and scalability.

Aerospace Engineering: In aerospace engineering, early work explores using LLM-based agents to model physics, solve complex differential equations, and optimize design. [107] shows promising results in solving problems related to aerodynamics, aircraft design, trajectory optimization, etc. With further development, LLM-based agents may innovatively design spacecraft, simulate fluid flows, perform structural analysis, and even control autonomous vehicles by generating executable code that integrates with engineering systems.

Industrial Automation: In the field of industrial automation, LLM-based agents can be used to achieve intelligent planning and control of production processes. [144] proposes a novel framework that integrates large language models (LLMs) with digital twin systems to accommodate flexible production needs. The framework leverages prompt engineering techniques to create LLM agents that can adapt to specific tasks based on the information provided by digital twins. These agents can coordinate a series of atomic functionalities and skills to complete production tasks at different levels within the automation pyramid. This research demonstrates the potential of integrating LLMs into industrial automation systems, providing innovative solutions for more agile, flexible and adaptive production processes.

Robotics & Embodied Artificial Intelligence: Recent works have developed more efficient reinforcement learning agents for robotics and embodied artificial intelligence [25, 160, 106, 143, 133, 161, 60, 142, 154, 28, 2]. The focus is on enhancing autonomous agents' abilities for planning, reasoning, and collaboration in embodied environments. Some approaches such as [25] combine complementary strengths into unified systems for embodied reasoning and task planning. High-level commands enable improved planning while low-level controllers translate commands into actions. Dialogue for information gathering as in [160] can accelerate training. Other works such as [106, 143] employ autonomous agents for embodied decision-making and exploration guided by internal world models. Considering physical constraints, agents can generate executable plans and accomplish long-term tasks requiring multiple skills. In terms of control policies, SayCan [2] focuses on investigating a wide range of manipulation and navigation skills utilizing a mobile manipulator robot. Taking inspiration from typical tasks encountered in a kitchen environment, it presents a comprehensive set of 551 skills that cover seven skill families and 17 objects. These skills encompass various actions such as picking, placing, pouring, grasping, and manipulating objects, among others. Additional frameworks such as VOYAGAR [133] and GITM [161] propose autonomous agents that communicate, collaborate, and accomplish complex tasks. This demonstrates the promise of natural language understanding, motion planning, and human interaction for real-world robotics. As capabilities advance, adaptive autonomous agents may accomplish increasingly complex embodied tasks. In summary, complementing conventional methods with reasoning and planning abilities as in [60, 142, 154, 28] significantly improves autonomous agent performance in embodied environments. The focus is on holistic systems that enhance sample efficiency, generalization, and accomplish long-horizon tasks.

General Autonomous AI Agent: A number of open source projects based on LLM development have conducted preliminary explorations of Artificial General Intelligence (AGI), they are dedicated to the autonomous universal AI agent framework [45, 43, 38, 40, 35, 36, 42, 15, 32, 39, 34, 114, 47, 41, 37, 46, 141], enabling developers to build, manage, and run useful autonomous agents quickly and reliably. For example, LangChain [15] is an open-source framework that automates coding, testing, debugging, and documentation generation tasks. By integrating language models with data sources and facilitating interaction with the environment, LangChain enables efficient and cost-effective software development through natural language communication and collaboration among multiple agent roles. Based on LangChain, XLang [36] comes with a comprehensive set of tools, a complete user interface, and support for three different agent scenarios, namely data processing, plugin usage, and web agent. AutoGPT [45] is a fully automated, networkable agent that simply sets one or more goals and automatically breaks them down into corresponding tasks and cycles

Table 2: Representative applications of LLM-based autonomous agents.

	Domain	Work
	Psychology	TE[1], Akata et al. [3], Ziems et al [163]
Social Science	Political Science and Economy	Out of One [5], Horton[59], Ziems et al [163]
	Social Simulation	Social Simulacra [110], Generative Agents [109], SocialAI School [73], AgentSims [89], S^3 [50], Williams et al. [140], Li et al. [81], Chao et al. [76]
	Jurisprudence Research Assistant	ChatLaw [23], Blind Judgement [56] Ziems et al [163], Bail et al. [6]
Natural Science	Documentation, Data Managent	ChemCrow[8], Boiko et al.[7], ChatMOF [70]
	Experiment Assistant	ChemCrow [8], Boiko et al. [7]
	Science Education	ChemCrow [8], Boiko et al. [7], MathAgent [129], Drori et al. [30]
Engineering	Civil Engineering	IGLU [99]
	CS & SE	ToolBench [115], ChatDev [113], MetaGPT [58], SCG [29], GPTEngineer [33], SmolModels [44], DemoGPT [41]
	Aerospace Engineering	IELLM [107]
	Industrial Automation	GPT4IA [144]
	Robotics & Embodied AI	Planner-Actor-Reporter [25], Dialogue Shaping [160], DECKARD [106], TaPA [143], Voyager [133], GITM [161], LLM4RL[60], PET [142], REMEMBERER [154], Unified Agent [28], SayCan [2]
	General Autonomous Agents	AutoGPT [45], AgentGPT [43], Allegion [38], AGiXT [40], AgentVerse [35], XLang[36], BabyAGI [42], LangChain [15], WorkGPT [32], LoopGPT [39], GPTresearcher [34], BMTools[114], TransformersAgent [47], DemoGPT [41], MiniAGI [37], SuperAGI [46], AutoGen [141]

through them until the goal is reached. WorkGPT [32] is an agent framework similar to AutoGPT and LangChain. By providing it with an instruction and a set of APIs, it engages in back-and-forth conversations with AI until the instruction is completed. AGiXT [40] is a dynamic AI automation platform designed to orchestrate efficient AI command management and task execution across many providers. AgentVerse [35] is a versatile framework that helps researchers quickly create customized multiple LLM-based agent simulations. GPT Researcher [34] is an experimental application that leverages large language models to efficiently develop research questions, trigger web crawls to gather information, summarize sources, and aggregate summaries. BMTools [114] is an open-source repository that extends LLMs with tools and provides a platform for community-driven tool building and sharing. It supports various types of tools, enables simultaneous task execution using multiple tools, and offers a simple interface for loading plugins via URLs, fostering easy development and contribution to the BMTools ecosystem.

In summary, LLM-based autonomous agents are opening up new possibilities across diverse engineering domains to enhance human creativity and productivity. As LLMs continue to advance in their reasoning and generalization capabilities, we expect that symbiotic human-AI teams will unlock new horizons and capabilities in engineering innovation and discovery. However, questions around trust, transparency, and control remain when deploying LLM-based agents in safety-critical engineering systems. Finding the right balance between human and AI capabilities while ensuring robustness will enable realizing the full potential of this technology.

In the above sections, we introduce the previous work on LLM-based autonomous agents according to their applications. For more clear understanding, we summarize the these applications in Table 3.

4 LLM-based Autonomous Agent Evaluation

This section introduces the evaluation methods for assessing the effectiveness of LLM-based autonomous agents. Similar to LLM itself, the evaluation of AI agent is not an easy problem. Here, we present two commonly used evaluation strategies for assessing AI agents: subjective and objective evaluation. (Refer to the right part of Figure 3 for an overview.)

4.1 Subjective Evaluation

LLM-based agents have a wide range of applications. However, in many scenarios, there lacks general metrics to evaluate the performance of agents. Some potential properties, like agent’s intelligence and user-friendliness, cannot be measured by quantitative metrics as well. Therefore, subjective evaluation is indispensable for current research.

Subjective evaluation refers to the testing of the capabilities of LLM-based agents by humans through various means such as interaction, scoring, and so on. In this case, the participating testers are often recruited through crowdsourcing platforms [75, 110, 109, 5, 156]; while some researchers believe that crowdsourced personnel are unstable due to individual differences and use expert annotations to conduct the tests [163]. In the following, we present two commonly leveraged strategies.

Human Annotation: In some studies, the human evaluators directly rank or score the generated results of the LLM-based agents based on some specific perspectives [163, 5, 156]; Another evaluation type is user-centred, which asks human evaluators to response whether the LLM-based agents system is helpful to them [110] and whether it is user-friendly [75], and so on. In specific, one possible evaluation can be whether a social simulation system can effectively contribute to the enhancement of rule design for online communities [110].

Turing Test: In this method, human evaluators are always asked to distinguish between agent and human behaviours. In Generative Agents [109], the first cohort of human evaluators are asked to assess agents’ key competencies in five areas by interviewing. After two days of play time, another cohort of human evaluators will be asked to differentiate between agents and human responses under the same conditions. In the Free-form Partisan Text experiment[5], human evaluators are asked to guess whether responses are from human or LLM-based agent.

Because the LLM-based agent system ultimately serves humans, manual evaluation plays an irreplaceable role at this stage, but it also suffers from expensive costs, low efficiency, and population bias. With advances in LLM, it can somewhat play the role of a human for assessment tasks.

In some of the current studies, additional LLM-agents can be employed as subjective evaluators of the results. In ChemCrow [8], EvaluatorGPT evaluates the outcomes of the experiment by assigning grades that consider both the successful completion of tasks and the accuracy of the underlying thought processes. ChatEval [12] assembles a panel of multiple agent referees based on LLMs to evaluate the results generated by models through debates. We believe that with the progress of LLM, the results of model evaluation will be more credible and the application will be more extensive.

4.2 Objective Evaluation

Objective evaluation offers several benefits over human evaluations. Quantitative metrics enable clear comparisons between different methods and tracking of progress over time. Large-scale automated testing is feasible, allowing evaluation on thousands of tasks rather than a handful [113, 5]. Results are also more objective and reproducible. However, human evaluations can assess complementary qualities like naturalness, nuance, and social intelligence that are difficult to quantify objectively. The two approaches can therefore be used in conjunction.

Objective evaluation refers to assessing the capabilities of LLM-based autonomous agents using quantitative metrics that can be computed, compared and tracked over time. In contrast to subjective or human evaluations, objective metrics aim to provide concrete, measurable insights into agent performance. In this section, we review and synthesize objective evaluation approaches from the perspectives of metrics, strategies and benchmarks.

Metrics: In order to objectively evaluate the effectiveness of the agents, designing proper metrics is significant, which may influence the evaluation accuracy and comprehensiveness. Ideal evaluation

Table 3: Summary on the evaluation strategies of LLM-based autonomous agents (more details can be seen on <https://github.com/Paitesanshi/LLM-Agent-Survey>). For subjective evaluation, we use ① and ② to represent human annotation and the Turing test, respectively. For objective evaluation, we use ①, ②, ③, ④, and ⑤ to represent environment simulation, isolated reasoning, social evaluation, multi-task evaluation, and software testing, respectively. We also summarize whether these agents use benchmarks for evaluation.

Model	Subjective	Objective	Benchmark	Time
WebShop [149]	-	① ② ④	✓	07/2022
Social Simulacra [110]	①	③	-	08/2022
TE [1]	-	③	-	08/2022
LIBRO [69]	-	⑤	-	09/2022
ReAct[151]	-	①	✓	10/2022
Out of One, Many[5]	②	② ④	-	02/2023
DEPS[137]	-	①	✓	02/2023
Jalil et al.[66]	-	⑤	-	02/2023
Reflexion[125]	-	②	-	03/2023
IGLU[99]	-	①	✓	04/2023
LLM+P[90]	-	②	-	04/2023
Generative Agents[109]	①②	-	-	04/2023
ToolBench[114]	-	④	✓	04/2023
GITM[161]	-	①	✓	05/2023
Two-Failures[16]	-	①	-	05/2023
Voyager[133]	-	①	✓	05/2023
SocKET [21]	-	② ③ ④	✓	05/2023
MobileEnv [155]	-	① ② ④	✓	05/2023
clmbench [11]	-	①	✓	05/2023
Dialop [88]	-	③	✓	06/2023
ChatDB[61]	-	②	-	06/2023
Feldt et al.[48]	-	⑤	-	06/2023
CO-LLM [156]	①	①	-	07/2023
Tachikuma[85]	①	①	✓	07/2023
ChatDev[113]	-	②	-	07/2023
WebArena [159]	-	①	✓	07/2023
AgentSims[89]	-	③	-	08/2023
AgentBench[93]	-	④	✓	08/2023
BOLAA[94]	-	① ④ ⑤	✓	08/2023
Gentopia [146]	-	② ④	✓	08/2023

metrics should precisely reflect the quality of the agents, and align with the human feelings when using them in real-world scenarios. In existing work, we can see the following representative evaluation metrics. (1) *Task success metrics*: These metrics measure how well an agent can complete tasks and achieve goals. Common metrics include success rate [156, 151, 125, 90], reward/score [156, 151, 99], coverage [161], and accuracy [113, 1, 61]. Higher values indicate greater task completion ability. (2) *Human similarity metrics*: These metrics quantify the degree to which agent behavior closely resembles that of humans. Typical examples include trajectory/location accuracy [16, 133], dialogue similarities [110, 1], and mimicry of human responses [1, 5]. Higher similarity suggests more human-like reasoning. (3) *Efficiency metrics*: In contrast to the aforementioned metrics used to evaluate agent effectiveness, these metrics assess agent efficiency from various perspectives. Typical metrics include planning length [90], development cost [113], inference speed [161, 133], and number of clarification dialogues [99].

Strategies: Based on the methods employed for evaluation, we can identify several common strategies: (1) *Environmental simulation*: In this method, the agents are assessed in immersive 3D environments such as games and interactive fiction using metrics for task success and human similarity, which incorporate factors like trajectories, language usage, and completed objectives [16, 156, 161, 151, 133, 99, 137, 85, 149, 155]. This showcases the agents’ practical abilities in real-world scenarios. (2) *Isolated reasoning*: In this method, the researchers concentrate on fundamental cognitive abilities by employing limited tasks such as accuracy, passage completion rate, and ablation measures [113, 5, 125, 90, 61, 21, 149, 155]. This approach simplifies the analysis of individual skills. (3) *Social evaluation*: [110, 1, 21, 89, 94] directly probe social intelligence using human studies and mimicry metrics. This assesses higher-order social cognition. (4) *Multi-task*: [5, 21, 114, 93, 94, 149, 155] use suites of diverse tasks from different domains with zero/few-shot evaluation. This measures generalizability. (5) *Software testing*: [66, 69, 48, 94] explore the use of LLMs for various software testing tasks, such as generating test cases, reproducing bugs, debugging code, and interacting with developers and external tools. They use metrics such as test coverage, bug detection rate, code quality, and reasoning ability to measure the effectiveness of LLM-based agents.

Benchmarks: In addition to metrics, objective evaluation relies on benchmarks, controlled experiments, and statistical significance testing. Many papers construct benchmarks with datasets of tasks and environments to systematically test agents, such as ALFWorld [151], IGLU [99], and Minecraft [161, 133, 137]. Clembench [11] is a game-based approach for evaluating chat-optimized language models as conversational agents, which explores the possibility of meaningfully evaluating LLMs by exposing them to restricted, game-like settings designed to challenge specific capabilities. Tachikuma [85] is a benchmark that leverages TRPG game logs to evaluate LLMs’ ability to understand and infer complex interactions with multiple characters and novel objects. AgentBench [93] provides a comprehensive framework for evaluating LLMs as autonomous agents across diverse environments, which enables standardized benchmarking of LLM agents by adopting F1 as the primary metric. It represents the first systematic assessment of pretrained LLMs as agents on real-world challenges across diverse domains. SocKET [21] is a comprehensive benchmark for evaluating the social knowledge capabilities of large language models (LLMs) across 58 tasks covering five categories of social information such as humor and sarcasm, emotions and feelings, credibility, etc. AgentSims [89] is a versatile infrastructure for building testing sandboxes for large-scale language models, facilitating diverse evaluation tasks and applications in data generation and social science research. ToolBench [114] is an open-source project that aims to facilitate the construction of powerful large language models (LLMs) with general tool-use capability by providing an open platform for training, serving, and evaluating LLMs for tool learning. Dialop [88] was designed with three tasks: optimisation, planning, and mediation, to evaluate the decision-making ability of the LLM-based agent. WebShop [149] Benchmark evaluates LLM agents on product search and retrieval from a collection of 1.18 million real-world items through search queries and clicks, using rewards based on attribute overlap and recall performance. Mobile-Env [155] is an easily-extendable interaction platform, which provides a foundation for assessing the multi-step interaction abilities of LLM-based agents in interacting with information user interfaces (InfoUI). WebArena [159] has established a comprehensive website environment encompassing common domains. This environment serves as a platform for evaluating agents in an end-to-end manner, assessing the functional correctness of completed task. GentBench [146] is a benchmark designed to evaluate various capabilities of agents, including reasoning, safety, efficiency, and more. Additionally, it supports the assessment of agents’ competence in utilizing tools to address complex tasks.

In summary, objective evaluation enables quantitative assessment of LLM-based agent capabilities through metrics like task success, human similarity, efficiency, and ablation studies. A diverse toolbox of objective techniques has emerged targeted at different competencies, from environmental simulation to social evaluation. While current techniques have limitations in measuring general capabilities, objective evaluation provides crucial insights complementing human assessment. Continued progress in objective evaluation benchmarks and methodology will further advance the development and understanding of LLM-based autonomous agents.

In the above sections, we introduce both subjective and objective evaluation strategies for LLM-based autonomous agents. The evaluation of the agents play significant roles in this domain. However, both subjective and objective evaluation have their own strengths and weakness. Maybe, in practice, they should be combined together to comprehensively evaluate the agents. We summarize the correspondence between the previous work and these evaluation strategies in Table 3.

5 Related Surveys

With the vigorous development of large language models, numerous comprehensive surveys have emerged, providing detailed insights into various aspects. [157] extensively introduces the background, main findings, and mainstream technologies of LLMs, encompassing a vast array of existing works. On the other hand, [148] primarily focus on the applications of LLMs in various downstream tasks and the challenges associated with their deployment. Aligning LLMs with human intelligence is an active area of research to address concerns such as biases and illusions. [136] have compiled existing techniques for human alignment, including data collection and model training methodologies. Reasoning is a crucial aspect of intelligence, influencing decision-making, problem-solving, and other cognitive abilities. [62] presents the current state of research on LLMs’ reasoning abilities, exploring approaches to improve and evaluate their reasoning skills. [100] propose that language models can be enhanced with reasoning capabilities and the ability to utilize tools, termed Augmented Language Models (ALMs). They conduct a comprehensive review of the latest advancements in ALMs. As the utilization of large-scale models becomes more prevalent, evaluating their performance is increasingly critical. [14] shed light on evaluating LLMs, addressing what to evaluate, where to evaluate, and how to assess their performance in downstream tasks and societal impact. [13] also discusses the capabilities and limitations of LLMs in various downstream tasks. The aforementioned research encompasses various aspects of large models, including training, application, and evaluation. However, prior to this paper, no work has specifically focused on the rapidly emerging and highly promising field of LLM-based Agents. In this study, we have compiled 100 relevant works on LLM-based Agents, covering their construction, applications, and evaluation processes.

6 Challenges

While previous work for LLM-based autonomous AI agent has shown many promising directions, this field is still at its initial stage, and many challenges exist on its development road. In the follow, we present several important challenges.

6.1 Role-playing Capability

Different from traditional LLMs, AI agent usually has to play as specific roles (*e.g.*, program coder, researcher and chemist) for accomplishing different tasks. Thus, the capability of the agent for role-playing is very important. While for many common roles (*e.g.*, movie reviewers), LLMs can well simulate them, there are still many roles and aspects that LLMs can be hard to capture. To begin with, LLMs are usually trained based on web-corpus, thus for the roles which are seldom discussed on the web or the newly emerging roles, LLMs may not simulate them well. In addition, previous research [49] has shown that existing LLMs may not well model the human cognitive psychology characters, leading to the lack of self-awareness in conversation scenarios. Potential solution to these problems may fine-tuning LLMs or carefully designing the agent prompts/architectures [77]. For example, one can firstly collect real-human data for uncommon roles or psychology characters, and then leverage it to fine-tune LLMs. However, how to ensure that fine-tuned model still perform well for the common roles may pose further challenges. Beyond fine-tuning, one can also design tailored agent prompts/architectures to enhance the capability of LLM on role-playing. However, finding the optimal prompts/architectures is not easy, since their designing spaces are too large.

6.2 Generalized Human Alignment

Human alignment has been discussed a lot for traditional LLMs. In the field of autonomous AI agent, especially when the agents are leveraged for simulation, we believe this concept should be discussed more in depth. In order to better serve human-beings, traditional LLMs are usually fine-tuned to be aligned with correct human values, for example, the agent should not plan to make a bomb for avenging society. However, when the agents are leveraged for real-world simulation, an ideal simulator should be able to honestly depict diverse human traits, including the ones with incorrect values. Actually, simulating the human negative aspects can be even more important, since an important goal of simulation is to discover and solve problems, and without negative aspects means no problem to be solved. For example, to simulate the real-world society, we may have to allow the agent to plan for making a bomb, and observe how it will act to implement the plan as well as the influence of its behaviors. Based on these observations, people can make better actions to stop

similar behaviors in real-world society. Inspired by the above case, maybe an important problem for agent-based simulation is how to conduct generalized human alignment, that is, for different purposes and applications, the agent should be able to align with diverse human values. However, existing powerful LLMs including ChatGPT and GPT-4 are mostly aligned with unified human values. Thus, an interesting direction is how to “realign” these models by designing proper prompting strategies.

6.3 Prompt Robustness

To ensure rational behavior in agents, designers often incorporate additional modules, such as memory and planning modules, into LLMs. However, the inclusion of these modules necessitates the development of more prompts in order to facilitate consistent operation and effective communication. Previous research [162, 52] has highlighted the lack of robustness in prompts for LLMs, as even minor alterations can yield substantially different outcomes. This issue becomes more pronounced when constructing autonomous agents, as they encompass not a single prompt but a prompt framework that considers all modules, wherein the prompt for one module has the potential to influence others. Moreover, the prompt frameworks can vary significantly across different LLMs. Developing a unified and robust prompt framework that can be applied to various LLMs is an important yet unresolved issue. There are two potential solutions to the aforementioned problems: (1) manually crafting the essential prompt elements through trial and error, or (2) automatically generating prompts using GPT.

6.4 Hallucination

Hallucination poses a fundamental challenge for LLMs, wherein the model erroneously outputs false information confidently. This issue is also prevalent in autonomous agents. For instance, in [67], it was observed that when confronted with simplistic instructions during code generation tasks, the agent may exhibit hallucinatory behavior. Hallucination can lead to serious consequences such as incorrect or misleading code, security risks, and ethical issues [67]. To address this problem, one possible approach is to incorporate human correction feedback within the loop of human-agent interaction [58]. More discussions on the hallucination problem can be seen in [157].

6.5 Knowledge Boundary

An important application of autonomous AI Agent is to simulate different real-world human behaviors [109]. The study of human simulation has a long history, and the recent surge in interest can be attributed to the remarkable advancements made by LLMs, which have demonstrated significant capabilities in simulating human behavior. However, it is important to recognize that the power of LLMs may not always be advantageous. Specifically, an ideal simulation should accurately replicate human knowledge. In this regard, LLMs can exhibit excessive power, as they are trained on an extensive corpus of web knowledge that surpasses the scope of ordinary individuals. The immense capabilities of LLMs can significantly impact the effectiveness of simulations. For instance, when attempting to simulate user selection behaviors for various movies, it is crucial to ensure that LLMs assume a position of having no prior knowledge of these movies. However, there is a possibility that LLMs have already acquired information about these movies. Without implementing appropriate strategies, LLMs may make decisions based on their extensive knowledge, even though real-world users would not have access to the contents of these movies beforehand. Based on the above example, we may conclude that for building believable agent simulation environment, an important problem is how to constrain the utilization of user-unknown knowledge of LLM.

6.6 Efficiency

Because of its auto-regressive architecture, LLMs typically have slow inference speeds. However, the agent may need to query LLMs for each action multiple times, such as extracting information from the memory module, make plans before taking actions and so on. Consequently, the efficiency of agent actions is greatly affected by the speed of LLM inference. Deploying multiple agents with the same API key can further significantly increase the time cost.

7 Conclusion

In this survey, we systematically summarize existing research in the field of LLM-based autonomous agents. We present and review these studies from three aspects including the construction, application,

and evaluation of the agents. For each of these aspects, we provide a detailed taxonomy to draw connections among the existing research, summarizing the major techniques and their development histories. In addition to reviewing the previous work, we also propose several challenges in this field, which are expected to guide potential future directions.

References

- [1] Gati V Aher, Rosa I Arriaga, and Adam Tauman Kalai. Using large language models to simulate multiple humans and replicate human subject studies. In *International Conference on Machine Learning*, pages 337–371. PMLR, 2023.
- [2] Michael Ahn, Anthony Brohan, Noah Brown, Yevgen Chebotar, Omar Cortes, Byron David, Chelsea Finn, Chuyuan Fu, Keerthana Gopalakrishnan, Karol Hausman, et al. Do as i can, not as i say: Grounding language in robotic affordances. *arXiv preprint arXiv:2204.01691*, 2022.
- [3] Elif Akata, Lion Schulz, Julian Coda-Forno, Seong Joon Oh, Matthias Bethge, and Eric Schulz. Playing repeated games with large language models. *arXiv preprint arXiv:2305.16867*, 2023.
- [4] Anthropic. Model card and evaluations for claude models. <https://www-files.anthropic.com/production/images/Model-Card-Claude-2.pdf?ref=maginataive.com>, 2023.
- [5] Lisa P Argyle, Ethan C Busby, Nancy Fulda, Joshua R Gubler, Christopher Rytting, and David Wingate. Out of one, many: Using language models to simulate human samples. *Political Analysis*, 31(3):337–351, 2023.
- [6] Christopher A Bail. Can generative AI improve social science? *SocArXiv*, 2023.
- [7] Daniil A Boiko, Robert MacKnight, and Gabe Gomes. Emergent autonomous scientific research capabilities of large language models. *arXiv preprint arXiv:2304.05332*, 2023.
- [8] Andres M Bran, Sam Cox, Andrew D White, and Philippe Schwaller. ChemCrow: Augmenting large-language models with chemistry tools. *arXiv preprint arXiv:2304.05376*, 2023.
- [9] Tom B Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, et al. Language models are few-shot learners. *arXiv preprint arXiv:2005.14165*, 2020.
- [10] Tianle Cai, Xuezhi Wang, Tengyu Ma, Xinyun Chen, and Denny Zhou. Large language models as tool makers. *arXiv preprint arXiv:2305.17126*, 2023.
- [11] Kranti Chalamalasetti, Jana Götze, Sherzod Hakimov, Brielen Madureira, Philipp Sadler, and David Schlangen. clembench: Using game play to evaluate chat-optimized language models as conversational agents. *arXiv preprint arXiv:2305.13455*, 2023.
- [12] Chi-Min Chan, Weize Chen, Yusheng Su, Jianxuan Yu, Wei Xue, Shanghang Zhang, Jie Fu, and Zhiyuan Liu. ChatEval: Towards better LLM-based evaluators through multi-agent debate. *arXiv preprint arXiv:2308.07201*, 2023.
- [13] Tyler A Chang and Benjamin K Bergen. Language model behavior: A comprehensive survey. *arXiv preprint arXiv:2303.11504*, 2023.
- [14] Yupeng Chang, Xu Wang, Jindong Wang, Yuan Wu, Kaijie Zhu, Hao Chen, Linyi Yang, Xiaoyuan Yi, Cunxiang Wang, Yidong Wang, et al. A survey on evaluation of large language models. *arXiv preprint arXiv:2307.03109*, 2023.
- [15] Harrison Chase. langchain. <https://docs.langchain.com/docs/>, 2023.
- [16] Angelica Chen, Jason Phang, Alicia Parrish, Vishakh Padmakumar, Chen Zhao, Samuel R Bowman, and Kyunghyun Cho. Two failures of self-consistency in the multi-step reasoning of LLMs. *arXiv preprint arXiv:2305.14279*, 2023.
- [17] Liting Chen, Lu Wang, Hang Dong, Yali Du, Jie Yan, Fangkai Yang, Shuang Li, Pu Zhao, Si Qin, Saravan Rajmohan, et al. Introspective tips: Large language model for in-context decision making. *arXiv preprint arXiv:2305.11598*, 2023.
- [18] Mark Chen, Jerry Tworek, Heewoo Jun, Qiming Yuan, Henrique Ponde de Oliveira Pinto, Jared Kaplan, Harri Edwards, Yuri Burda, Nicholas Joseph, Greg Brockman, et al. Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*, 2021.

- [19] Xinshi Chen, Shuang Li, Hui Li, Shaohua Jiang, Yuan Qi, and Le Song. Generative adversarial user model for reinforcement learning based recommendation system. In *International Conference on Machine Learning*, pages 1052–1061. PMLR, 2019.
- [20] Zhipeng Chen, Kun Zhou, Beichen Zhang, Zheng Gong, Wayne Xin Zhao, and Ji-Rong Wen. ChatCoT: Tool-augmented chain-of-thought reasoning on chat-based large language models. *arXiv preprint arXiv:2305.14323*, 2023.
- [21] Minje Choi, Jiaxin Pei, Sagar Kumar, Chang Shu, and David Jurgens. Do LLMs understand social knowledge? evaluating the sociability of large language models with socket benchmark. *arXiv preprint arXiv:2305.14938*, 2023.
- [22] Cédric Colas, Laetitia Teodorescu, Pierre-Yves Oudeyer, Xingdi Yuan, and Marc-Alexandre Côté. Augmenting autotelic agents with large language models. *arXiv preprint arXiv:2305.12487*, 2023.
- [23] Jiayi Cui, Zongjian Li, Yang Yan, Bohua Chen, and Li Yuan. ChatLaw: Open-source legal large language model with integrated external knowledge bases. *arXiv preprint arXiv:2306.16092*, 2023.
- [24] Gautier Dagan, Frank Keller, and Alex Lascarides. Dynamic planning with a LLM. *arXiv preprint arXiv:2308.06391*, 2023.
- [25] Ishita Dasgupta, Christine Kaeser-Chen, Kenneth Marino, Arun Ahuja, Sheila Babayan, Felix Hill, and Rob Fergus. Collaborating with language models for embodied reasoning. *arXiv preprint arXiv:2302.00763*, 2023.
- [26] Xiang Deng, Yu Gu, Boyuan Zheng, Shijie Chen, Samuel Stevens, Boshi Wang, Huan Sun, and Yu Su. Mind2web: Towards a generalist agent for the web. *arXiv preprint arXiv:2306.06070*, 2023.
- [27] Ameet Deshpande, Vishvak Murahari, Tanmay Rajpurohit, Ashwin Kalyan, and Karthik Narasimhan. Toxicity in ChatGPT: Analyzing persona-assigned language models. *arXiv preprint arXiv:2304.05335*, 2023.
- [28] Norman Di Palo, Arunkumar Byravan, Leonard Hasenclever, Markus Wulfmeier, Nicolas Heess, and Martin Riedmiller. Towards a unified agent with foundation models. In *Workshop on Reincarnating Reinforcement Learning at ICLR 2023*, 2023.
- [29] Yihong Dong, Xue Jiang, Zhi Jin, and Ge Li. Self-collaboration code generation via ChatGPT. *arXiv preprint arXiv:2304.07590*, 2023.
- [30] Iddo Drori, Sarah Zhang, Reece Shuttlesworth, Leonard Tang, Albert Lu, Elizabeth Ke, Kevin Liu, Linda Chen, Sunny Tran, Newman Cheng, Roman Wang, Nikhil Singh, Taylor L. Patti, Jayson Lynch, Avi Shporer, Nakul Verma, Eugene Wu, and Gilbert Strang. A neural network solves, explains, and generates university math problems by program synthesis and few-shot learning at human level. *Proceedings of the National Academy of Sciences*, 119(32), aug 2022.
- [31] Yilun Du, Shuang Li, Antonio Torralba, Joshua B Tenenbaum, and Igor Mordatch. Improving factuality and reasoning in language models through multiagent debate. *arXiv preprint arXiv:2305.14325*, 2023.
- [32] Alex MacCaw et al. WorkGPT. <https://github.com/team-openpm/workgpt>, 2023.
- [33] Anton Osika et al. GPT engineer. <https://github.com/AntonOsika/gpt-engineer>, 2023.
- [34] Assaf Elovic et al. GPT-researcher. <https://github.com/assafelovic/gpt-researcher>, 2023.
- [35] Chen et al. Agentverse. <https://github.com/OpenBMB/AgentVerse>, 2023.
- [36] Chen et al. Xlang. <https://github.com/xlang-ai/xlang>, 2023.
- [37] Enricoros et al. Miniagi. <https://github.com/muellerberndt/mini-agi>, 2023.
- [38] Eumemic et al. Ai-legion. <https://github.com/eumemic/ai-legion>, 2023.
- [39] Fayaz Rahman et al. LoopGPT. <https://github.com/farizrahman4u/loopgpt>, 2023.
- [40] Josh XT et al. Agixt. <https://github.com/Josh-XT/AGiXT>, 2023.

- [41] Melih Unsal et al. DemoGPT. <https://github.com/melih-unsal/DemoGPT>, 2023.
- [42] Nakajima et al. Babyagi. <https://github.com/yoheinakajima>, 2023.
- [43] Reworkd et al. AgentGPT. <https://github.com/reworkd/AgentGPT>, 2023.
- [44] Swyxio et al. Smolmodels. <https://github.com/smol-ai/developer>, 2023.
- [45] Torantulino et al. Auto-GPT. <https://github.com/Significant-Gravitas/Auto-GPT>, 2023.
- [46] TransformerOptimus et al. Superagi. <https://github.com/TransformerOptimus/SuperAGI>, 2023.
- [47] Hugging Face. transformers-agent. https://huggingface.co/docs/transformers/transformers_agents, 2023.
- [48] Robert Feldt, Sungmin Kang, Juyeon Yoon, and Shin Yoo. Towards autonomous testing agents via conversational large language models. *arXiv preprint arXiv:2306.05152*, 2023.
- [49] Kevin A Fischer. Reflective linguistic programming (rlp): A stepping stone in socially-aware agi (socialagi). *arXiv preprint arXiv:2305.12647*, 2023.
- [50] Chen Gao, Xiaochong Lan, Zhihong Lu, Jinzhu Mao, Jinghua Piao, Huandong Wang, Depeng Jin, and Yong Li. S3: Social-network simulation system with large language model-empowered agents. *arXiv preprint arXiv:2307.14984*, 2023.
- [51] Yingqiang Ge, Wenyue Hua, Jianchao Ji, Juntao Tan, Shuyuan Xu, and Yongfeng Zhang. OpenAGI: When llm meets domain experts. *arXiv preprint arXiv:2304.04370*, 2023.
- [52] Zorik Gekhman, Nadav Oved, Orgad Keller, Idan Szpektor, and Roi Reichart. On the robustness of dialogue history representation in conversational question answering: a comprehensive study and a new prompt-based method. *Transactions of the Association for Computational Linguistics*, 11:351–366, 2023.
- [53] Maitrey Gramopadhye and Daniel Szafrir. Generating executable action plans with environmentally-aware language models. *arXiv preprint arXiv:2210.04964*, 2022.
- [54] Igor Grossmann, Matthew Feinberg, Dawn C Parker, Nicholas A Christakis, Philip E Tetlock, and William A Cunningham. Ai and the transformation of social science research. *Science*, 380(6650):1108–1109, 2023.
- [55] Tuomas Haarnoja, Aurick Zhou, Pieter Abbeel, and Sergey Levine. Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor. *arXiv preprint arXiv:1801.01290*, 2018.
- [56] Sil Hamilton. Blind judgement: Agent-based supreme court modelling with GPT. *arXiv preprint arXiv:2301.05327*, 2023.
- [57] Shibo Hao, Yi Gu, Haodi Ma, Joshua Jiahua Hong, Zhen Wang, Daisy Zhe Wang, and Zhiting Hu. Reasoning with language model is planning with world model. *arXiv preprint arXiv:2305.14992*, 2023.
- [58] Sirui Hong, Xiawu Zheng, Jonathan Chen, Yuheng Cheng, Ceyao Zhang, Zili Wang, Steven Ka Shing Yau, Zijuan Lin, Liyang Zhou, Chenyu Ran, et al. MetaGPT: Meta programming for multi-agent collaborative framework. *arXiv preprint arXiv:2308.00352*, 2023.
- [59] John J Horton. Large language models as simulated economic agents: What can we learn from homo silicus? Technical report, National Bureau of Economic Research, 2023.
- [60] Bin Hu, Chenyang Zhao, Pu Zhang, Zihao Zhou, Yuanhang Yang, Zenglin Xu, and Bin Liu. Enabling intelligent interactions between an agent and an llm: A reinforcement learning approach. *arXiv preprint arXiv:2306.03604*, 2023.
- [61] Chenxu Hu, Jie Fu, Chenzhuang Du, Simian Luo, Junbo Zhao, and Hang Zhao. Chatdb: Augmenting LLMs with databases as their symbolic memory. *arXiv preprint arXiv:2306.03901*, 2023.
- [62] Jie Huang and Kevin Chen-Chuan Chang. Towards reasoning in large language models: A survey. *arXiv preprint arXiv:2212.10403*, 2022.

- [63] Wenlong Huang, Pieter Abbeel, Deepak Pathak, and Igor Mordatch. Language models as zero-shot planners: Extracting actionable knowledge for embodied agents. In *International Conference on Machine Learning*, pages 9118–9147. PMLR, 2022.
- [64] Wenlong Huang, Fei Xia, Ted Xiao, Harris Chan, Jacky Liang, Pete Florence, Andy Zeng, Jonathan Tompson, Igor Mordatch, Yevgen Chebotar, et al. Inner monologue: Embodied reasoning through planning with language models. *arXiv preprint arXiv:2207.05608*, 2022.
- [65] Gautier Izacard, Patrick Lewis, Maria Lomeli, Lucas Hosseini, Fabio Petroni, Timo Schick, Jane Dwivedi-Yu, Armand Joulin, Sebastian Riedel, and Edouard Grave. Few-shot learning with retrieval augmented language models. *arXiv preprint arXiv:2208.03299*, 2022.
- [66] Sajed Jalil, Suzzana Rafi, Thomas D LaToza, Kevin Moran, and Wing Lam. ChatGPT and software testing education: Promises & perils. In *2023 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 4130–4137. IEEE, 2023.
- [67] Ziwei Ji, Nayeon Lee, Rita Frieske, Tiezheng Yu, Dan Su, Yan Xu, Etsuko Ishii, Ye Jin Bang, Andrea Madotto, and Pascale Fung. Survey of hallucination in natural language generation. *ACM Computing Surveys*, 55(12):1–38, 2023.
- [68] Leslie Pack Kaelbling, Michael L Littman, and Andrew W Moore. Reinforcement learning: A survey. *Journal of artificial intelligence research*, 4:237–285, 1996.
- [69] Sungmin Kang, Juyeon Yoon, and Shin Yoo. Large language models are few-shot testers: Exploring LLM-based general bug reproduction. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, pages 2312–2323. IEEE, 2023.
- [70] Yeonghun Kang and Jihan Kim. Chatmof: An autonomous ai system for predicting and generating metal-organic frameworks. *arXiv preprint arXiv:2308.01423*, 2023.
- [71] Ehud Karpas, Omri Abend, Yonatan Belinkov, Barak Lenz, Opher Lieber, Nir Ratner, Yoav Shoham, Hofit Bata, Yoav Levine, Kevin Leyton-Brown, et al. Mrkl systems: A modular, neuro-symbolic architecture that combines large language models, external knowledge sources and discrete reasoning. *arXiv preprint arXiv:2205.00445*, 2022.
- [72] Takeshi Kojima, Shixiang Shane Gu, Machel Reid, Yutaka Matsuo, and Yusuke Iwasawa. Large language models are zero-shot reasoners. *Advances in neural information processing systems*, 35:22199–22213, 2022.
- [73] Grgur Kovač, Rémy Portelas, Peter Ford Dominey, and Pierre-Yves Oudeyer. The socialai school: Insights from developmental psychology towards artificial socio-cultural agents. *arXiv preprint arXiv:2307.07871*, 2023.
- [74] David MJ Lazer, Alex Pentland, Duncan J Watts, Sinan Aral, Susan Athey, Noshir Contractor, Deen Freelon, Sandra Gonzalez-Bailon, Gary King, Helen Margetts, et al. Computational social science: Obstacles and opportunities. *Science*, 369(6507):1060–1062, 2020.
- [75] Mina Lee, Megha Srivastava, Amelia Hardy, John Thickstun, Esin Durmus, Ashwin Paranjape, Ines Gerard-Ursin, Xiang Lisa Li, Faisal Ladhak, Frieda Rong, et al. Evaluating human-language model interaction. *arXiv preprint arXiv:2212.09746*, 2022.
- [76] Chao Li, Xing Su, Chao Fan, Haoying Han, Cong Xue, and Chunmo Zheng. Quantifying the impact of large language models on collective opinion dynamics. *arXiv preprint arXiv:2308.03313*, 2023.
- [77] Cheng Li, Jindong Wang, Kaijie Zhu, Yixuan Zhang, Wenxin Hou, Jianxun Lian, and Xing Xie. Emotionprompt: Leveraging psychology for large language models enhancement via emotional stimulus. *arXiv preprint arXiv:2307.11760*, 2023.
- [78] Guohao Li, Hasan Abed Al Kader Hammoud, Hani Itani, Dmitrii Khizbullin, and Bernard Ghanem. Camel: Communicative agents for" mind" exploration of large scale language model society. *arXiv preprint arXiv:2303.17760*, 2023.
- [79] Haonan Li, Yu Hao, Yizhuo Zhai, and Zhiyun Qian. The hitchhiker’s guide to program analysis: A journey with large language models. *arXiv preprint arXiv:2308.00245*, 2023.
- [80] Minghao Li, Feifan Song, Bowen Yu, Haiyang Yu, Zhoujun Li, Fei Huang, and Yongbin Li. Api-bank: A benchmark for tool-augmented LLMs. *arXiv preprint arXiv:2304.08244*, 2023.

- [81] Siyu Li, Jin Yang, and Kui Zhao. Are you in a masquerade? exploring the behavior and impact of large language model driven social bots in online social networks. *arXiv preprint arXiv:2307.10337*, 2023.
- [82] Yuxi Li. Deep reinforcement learning: An overview. *arXiv preprint arXiv:1701.07274*, 2017.
- [83] Tian Liang, Zhiwei He, Wenxiang Jiao, Xing Wang, Yan Wang, Rui Wang, Yujiu Yang, Zhaopeng Tu, and Shuming Shi. Encouraging divergent thinking in large language models through multi-agent debate. *arXiv preprint arXiv:2305.19118*, 2023.
- [84] Xinnian Liang, Bing Wang, Hui Huang, Shuangzhi Wu, Peihao Wu, Lu Lu, Zejun Ma, and Zhoujun Li. Unleashing infinite-length input capacity for large-scale language models with self-controlled memory system. *arXiv preprint arXiv:2304.13343*, 2023.
- [85] Yuanzhi Liang, Linchao Zhu, and Yi Yang. Tachikuma: Understanding complex interactions with multi-character and novel objects by large language models. *arXiv preprint arXiv:2307.12573*, 2023.
- [86] Timothy P Lillicrap, Jonathan J Hunt, Alexander Pritzel, Nicolas Heess, Tom Erez, Yuval Tassa, David Silver, and Daan Wierstra. Continuous control with deep reinforcement learning. *arXiv preprint arXiv:1509.02971*, 2015.
- [87] Bill Yuchen Lin, Yicheng Fu, Karina Yang, Prithviraj Ammanabrolu, Faeze Brahman, Shiyu Huang, Chandra Bhagavatula, Yejin Choi, and Xiang Ren. Swiftsage: A generative agent with fast and slow thinking for complex interactive tasks. *arXiv preprint arXiv:2305.17390*, 2023.
- [88] Jessy Lin, Nicholas Tomlin, Jacob Andreas, and Jason Eisner. Decision-oriented dialogue for human-ai collaboration. *arXiv preprint arXiv:2305.20076*, 2023.
- [89] Jiaju Lin, Haoran Zhao, Aochi Zhang, Yiting Wu, Huqiyue Ping, and Qin Chen. Agentsims: An open-source sandbox for large language model evaluation. *arXiv preprint arXiv:2308.04026*, 2023.
- [90] Bo Liu, Yuqian Jiang, Xiaohan Zhang, Qiang Liu, Shiqi Zhang, Joydeep Biswas, and Peter Stone. LLM+P: Empowering large language models with optimal planning proficiency. *arXiv preprint arXiv:2304.11477*, 2023.
- [91] Hao Liu, Carmelo Sferrazza, and Pieter Abbeel. Chain of hindsight aligns language models with feedback. *arXiv preprint arXiv:2302.02676*, 3, 2023.
- [92] Ruibo Liu, Ruixin Yang, Chenyan Jia, Ge Zhang, Denny Zhou, Andrew M Dai, Diyi Yang, and Soroush Vosoughi. Training socially aligned language models in simulated human society. *arXiv preprint arXiv:2305.16960*, 2023.
- [93] Xiao Liu, Hao Yu, Hanchen Zhang, Yifan Xu, Xuanyu Lei, Hanyu Lai, Yu Gu, Hangliang Ding, Kaiwen Men, Kejuan Yang, et al. Agentbench: Evaluating LLMs as agents. *arXiv preprint arXiv:2308.03688*, 2023.
- [94] Zhiwei Liu, Weiran Yao, Jianguo Zhang, Le Xue, Shelby Heinecke, Rithesh Murthy, Yihao Feng, Zeyuan Chen, Juan Carlos Niebles, Devansh Arpit, et al. BOLAA: Benchmarking and orchestrating LLM-augmented autonomous agents. *arXiv preprint arXiv:2308.05960*, 2023.
- [95] Zilin Ma, Yiyang Mei, and Zhaoyuan Su. Understanding the benefits and challenges of using large language model-based conversational agents for mental well-being support. *arXiv preprint arXiv:2307.15810*, 2023.
- [96] Aman Madaan, Niket Tandon, Peter Clark, and Yiming Yang. Memory-assisted prompt editing to improve GPT-3 after deployment. In *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing*, pages 2833–2861, 2022.
- [97] Aman Madaan, Niket Tandon, Prakhar Gupta, Skyler Hallinan, Luyu Gao, Sarah Wiegrefe, Uri Alon, Nouha Dziri, Shrimai Prabhumoye, Yiming Yang, et al. Self-refine: Iterative refinement with self-feedback. *arXiv preprint arXiv:2303.17651*, 2023.
- [98] Roger McFarlane. A survey of exploration strategies in reinforcement learning. *McGill University*, 3:17–18, 2018.
- [99] Nikhil Mehta, Milagro Teruel, Patricio Figueroa Sanz, Xin Deng, Ahmed Hassan Awadallah, and Julia Kiseleva. Improving grounded language understanding in a collaborative environment by interacting with agents through help feedback. *arXiv preprint arXiv:2304.10750*, 2023.

- [100] Grégoire Mialon, Roberto Dessì, Maria Lomeli, Christoforos Nalmpantis, Ram Pasunuru, Roberta Raileanu, Baptiste Rozière, Timo Schick, Jane Dwivedi-Yu, Asli Celikyilmaz, et al. Augmented language models: a survey. *arXiv preprint arXiv:2302.07842*, 2023.
- [101] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Andrei A Rusu, Joel Veness, Marc G Bellemare, Alex Graves, Martin Riedmiller, Andreas K Fidjeland, Georg Ostrovski, et al. Human-level control through deep reinforcement learning. *Nature*, 518(7540):529–533, 2015.
- [102] Ali Modarressi, Ayyoob Imani, Mohsen Fayyaz, and Hinrich Schütze. RET-LLM: Towards a general read-write memory for large language models. *arXiv preprint arXiv:2305.14322*, 2023.
- [103] Rithesh Murthy, Shelby Heinecke, Juan Carlos Niebles, Zhiwei Liu, Le Xue, Weiran Yao, Yihao Feng, Zeyuan Chen, Akash Gokul, Devansh Arpit, et al. Rex: Rapid exploration and exploitation for ai agents. *arXiv preprint arXiv:2307.08962*, 2023.
- [104] Varun Nair, Elliot Schumacher, Geoffrey Tso, and Anitha Kannan. Dera: enhancing large language model completions with dialog-enabled resolving agents. *arXiv preprint arXiv:2303.17071*, 2023.
- [105] Reiichiro Nakano, Jacob Hilton, Suchir Balaji, Jeff Wu, Long Ouyang, Christina Kim, Christopher Hesse, Shantanu Jain, Vineet Kosaraju, William Saunders, et al. WebGPT: Browser-assisted question-answering with human feedback. *arXiv preprint arXiv:2112.09332*, 2021.
- [106] Kolby Nottingham, Prithviraj Ammanabrolu, Alane Suhr, Yejin Choi, Hannaneh Hajishirzi, Sameer Singh, and Roy Fox. Do embodied agents dream of pixelated sheep?: Embodied decision making using language guided world modelling. *arXiv preprint arXiv:2301.12050*, 2023.
- [107] Oluwatosin Ogundare, Srinath Madasu, and Nathaniel Wiggins. Industrial engineering with large language models: A case study of ChatGPT’s performance on oil & gas problems. *arXiv preprint arXiv:2304.14354*, 2023.
- [108] OpenAI. GPT-4 technical report, 2023.
- [109] Joon Sung Park, Joseph C. O’Brien, Carrie J. Cai, Meredith Ringel Morris, Percy Liang, and Michael S. Bernstein. Generative agents: Interactive simulacra of human behavior. In *In the 36th Annual ACM Symposium on User Interface Software and Technology (UIST ’23)*, UIST ’23, New York, NY, USA, 2023. Association for Computing Machinery.
- [110] Joon Sung Park, Lindsay Popowski, Carrie Cai, Meredith Ringel Morris, Percy Liang, and Michael S Bernstein. Social simulacra: Creating populated prototypes for social computing systems. In *Proceedings of the 35th Annual ACM Symposium on User Interface Software and Technology*, pages 1–18, 2022.
- [111] Shishir G Patil, Tianjun Zhang, Xin Wang, and Joseph E Gonzalez. Gorilla: Large language model connected with massive apis. *arXiv preprint arXiv:2305.15334*, 2023.
- [112] Debjit Paul, Mete Ismayilzada, Maxime Peyrard, Beatriz Borges, Antoine Bosselut, Robert West, and Boi Faltings. Refiner: Reasoning feedback on intermediate representations. *arXiv preprint arXiv:2304.01904*, 2023.
- [113] Chen Qian, Xin Cong, Cheng Yang, Weize Chen, Yusheng Su, Juyuan Xu, Zhiyuan Liu, and Maosong Sun. Communicative agents for software development. *arXiv preprint arXiv:2307.07924*, 2023.
- [114] Yujia Qin, Shengding Hu, Yankai Lin, Weize Chen, Ning Ding, Ganqu Cui, Zheni Zeng, Yufei Huang, Chaojun Xiao, Chi Han, et al. Tool learning with foundation models. *arXiv preprint arXiv:2304.08354*, 2023.
- [115] Yujia Qin, Shihao Liang, Yining Ye, Kunlun Zhu, Lan Yan, Yaxi Lu, Yankai Lin, Xin Cong, Xiangru Tang, Bill Qian, et al. ToolLLM: Facilitating large language models to master 16000+ real-world apis. *arXiv preprint arXiv:2307.16789*, 2023.
- [116] Alec Radford, Jeff Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners. *OpenAI blog*, 1(8):9, 2019.
- [117] Shreyas Sundara Raman, Vanya Cohen, Eric Rosen, Ifrah Idrees, David Paulius, and Stefanie Tellex. Planning with large language models via corrective re-prompting. *arXiv preprint arXiv:2211.09935*, 2022.

- [118] Jingqing Ruan, Yihong Chen, Bin Zhang, Zhiwei Xu, Tianpeng Bao, Guoqing Du, Shiwei Shi, Hangyu Mao, Xingyu Zeng, and Rui Zhao. TPTU: Task planning and tool usage of large language model-based AI agents. *arXiv preprint arXiv:2308.03427*, 2023.
- [119] Timo Schick, Jane Dwivedi-Yu, Roberto Dessì, Roberta Raileanu, Maria Lomeli, Luke Zettlemoyer, Nicola Cancedda, and Thomas Scialom. Toolformer: Language models can teach themselves to use tools. *arXiv preprint arXiv:2302.04761*, 2023.
- [120] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*, 2017.
- [121] Dale Schuurmans. Memory augmented large language models are computationally universal. *arXiv preprint arXiv:2301.04589*, 2023.
- [122] Sivan Schwartz, Avi Yaeli, and Segev Shlomov. Enhancing trust in LLM-based AI automation agents: New considerations and future challenges. *arXiv preprint arXiv:2308.05391*, 2023.
- [123] Yongliang Shen, Kaitao Song, Xu Tan, Dongsheng Li, Weiming Lu, and Yueting Zhuang. HuggingGPT: Solving ai tasks with ChatGPT and its friends in huggingface. *arXiv preprint arXiv:2303.17580*, 2023.
- [124] Weijia Shi, Sewon Min, Michihiro Yasunaga, Minjoon Seo, Rich James, Mike Lewis, Luke Zettlemoyer, and Wen-tau Yih. Replug: Retrieval-augmented black-box language models. *arXiv preprint arXiv:2301.12652*, 2023.
- [125] Noah Shinn, Federico Cassano, Beck Labash, Ashwin Gopinath, Karthik Narasimhan, and Shunyu Yao. Reflexion: Language agents with verbal reinforcement learning. *arXiv preprint arXiv:2303.11366*, 2023.
- [126] Ishika Singh, Valts Blukis, Arsalan Mousavian, Ankit Goyal, Danfei Xu, Jonathan Tremblay, Dieter Fox, Jesse Thomason, and Animesh Garg. Progprompt: Generating situated robot task plans using large language models, 2022.
- [127] Chan Hee Song, Jiaman Wu, Clayton Washington, Brian M Sadler, Wei-Lun Chao, and Yu Su. LLM-Planner: Few-shot grounded planning for embodied agents with large language models. *arXiv preprint arXiv:2212.04088*, 2022.
- [128] Dídac Surís, Sachit Menon, and Carl Vondrick. ViperGPT: Visual inference via python execution for reasoning. *arXiv preprint arXiv:2303.08128*, 2023.
- [129] Melanie Swan, Takashi Kido, Eric Roland, and Renato P dos Santos. Math agents: Computational infrastructure, mathematical embedding, and genomics. *arXiv preprint arXiv:2307.02502*, 2023.
- [130] Hugo Touvron, Thibaut Lavril, Gautier Izacard, Xavier Martinet, Marie-Anne Lachaux, Timothée Lacroix, Baptiste Rozière, Naman Goyal, Eric Hambro, Faisal Azhar, et al. Llama: Open and efficient foundation language models. *arXiv preprint arXiv:2302.13971*, 2023.
- [131] Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, et al. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2307.09288*, 2023.
- [132] Shangqing Tu, Chunyang Li, Jifan Yu, Xiaozhi Wang, Lei Hou, and Juanzi Li. ChatLog: Recording and analyzing ChatGPT across time. *arXiv preprint arXiv:2304.14106*, 2023.
- [133] Guanzhi Wang, Yuqi Xie, Yunfan Jiang, Ajay Mandlekar, Chaowei Xiao, Yuke Zhu, Linxi Fan, and Anima Anandkumar. Voyager: An open-ended embodied agent with large language models. *arXiv preprint arXiv:2305.16291*, 2023.
- [134] Lei Wang, Jingsen Zhang, Xu Chen, Yankai Lin, Ruihua Song, Wayne Xin Zhao, and Ji-Rong Wen. Recagent: A novel simulation paradigm for recommender systems. *arXiv preprint arXiv:2306.02552*, 2023.
- [135] Xuezhi Wang, Jason Wei, Dale Schuurmans, Quoc Le, Ed Chi, Sharan Narang, Aakanksha Chowdhery, and Denny Zhou. Self-consistency improves chain of thought reasoning in language models. *arXiv preprint arXiv:2203.11171*, 2022.
- [136] Yufei Wang, Wanjun Zhong, Liangyou Li, Fei Mi, Xingshan Zeng, Wenying Huang, Lifeng Shang, Xin Jiang, and Qun Liu. Aligning large language models with human: A survey. *arXiv preprint arXiv:2307.12966*, 2023.

- [137] Zihao Wang, Shaofei Cai, Anji Liu, Xiaojian Ma, and Yitao Liang. Describe, explain, plan and select: Interactive planning with large language models enables open-world multi-task agents. *arXiv preprint arXiv:2302.01560*, 2023.
- [138] Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, Fei Xia, Ed Chi, Quoc V Le, Denny Zhou, et al. Chain-of-thought prompting elicits reasoning in large language models. *Advances in Neural Information Processing Systems*, 35:24824–24837, 2022.
- [139] Jimmy Wei, Kurt Shuster, Arthur Szlam, Jason Weston, Jack Urbanek, and Mojtaba Komeili. Multi-party chat: Conversational agents in group settings with humans and models. *arXiv preprint arXiv:2304.13835*, 2023.
- [140] Ross Williams, Niyousha Hosseinichimeh, Aritra Majumdar, and Navid Ghaffarzadegan. Epidemic modeling with generative agents. *arXiv preprint arXiv:2307.04986*, 2023.
- [141] Qingyun Wu, Gagan Bansal, Jieyu Zhang, Yiran Wu, Shaokun Zhang, Erkang Zhu, Beibin Li, Li Jiang, Xiaoyun Zhang, and Chi Wang. AutoGen: Enabling next-gen LLM applications via multi-agent conversation framework. *arXiv preprint arXiv:2308.08155*, 2023.
- [142] Yue Wu, So Yeon Min, Yonatan Bisk, Ruslan Salakhutdinov, Amos Azaria, Yuanzhi Li, Tom Mitchell, and Shrimai Prabhumoye. Plan, eliminate, and track—language models are good teachers for embodied agents. *arXiv preprint arXiv:2305.02412*, 2023.
- [143] Zhenyu Wu, Ziwei Wang, Xiuwei Xu, Jiwen Lu, and Haibin Yan. Embodied task planning with large language models. *arXiv preprint arXiv:2307.01848*, 2023.
- [144] Yuchen Xia, Manthan Shenoy, Nasser Jazdi, and Michael Weyrich. Towards autonomous system: flexible modular production system enhanced with large language model agents. *arXiv preprint arXiv:2304.14721*, 2023.
- [145] Jiannan Xiang, Tianhua Tao, Yi Gu, Tianmin Shu, Zirui Wang, Zichao Yang, and Zhiting Hu. Language models meet world models: Embodied experiences enhance language models. *arXiv preprint arXiv:2305.10626*, 2023.
- [146] Binfeng Xu, Xukun Liu, Hua Shen, Zeyu Han, Yuhan Li, Murong Yue, Zhiyuan Peng, Yuchen Liu, Ziyu Yao, and Dongkuan Xu. Gentopia: A collaborative platform for tool-augmented LLMs. *arXiv preprint arXiv:2308.04030*, 2023.
- [147] Binfeng Xu, Zhiyuan Peng, Bowen Lei, Subhabrata Mukherjee, Yuchen Liu, and Dongkuan Xu. Rewoo: Decoupling reasoning from observations for efficient augmented language models. *arXiv preprint arXiv:2305.18323*, 2023.
- [148] Jingfeng Yang, Hongye Jin, Ruixiang Tang, Xiaotian Han, Qizhang Feng, Haoming Jiang, Bing Yin, and Xia Hu. Harnessing the power of LLMs in practice: A survey on ChatGPT and beyond. *arXiv preprint arXiv:2304.13712*, 2023.
- [149] Shunyu Yao, Howard Chen, John Yang, and Karthik Narasimhan. Webshop: Towards scalable real-world web interaction with grounded language agents. *Advances in Neural Information Processing Systems*, 35:20744–20757, 2022.
- [150] Shunyu Yao, Dian Yu, Jeffrey Zhao, Izhak Shafran, Thomas L Griffiths, Yuan Cao, and Karthik Narasimhan. Tree of thoughts: Deliberate problem solving with large language models. *arXiv preprint arXiv:2305.10601*, 2023.
- [151] Shunyu Yao, Jeffrey Zhao, Dian Yu, Nan Du, Izhak Shafran, Karthik Narasimhan, and Yuan Cao. React: Synergizing reasoning and acting in language models. *arXiv preprint arXiv:2210.03629*, 2022.
- [152] Weiran Yao, Shelby Heinecke, Juan Carlos Niebles, Zhiwei Liu, Yihao Feng, Le Xue, Rithesh Murthy, Zeyuan Chen, Jianguo Zhang, Devansh Arpit, et al. Retroformer: Retrospective large language agents with policy gradient optimization. *arXiv preprint arXiv:2308.02151*, 2023.
- [153] Siyu Yuan, Jiangjie Chen, Ziquan Fu, Xuyang Ge, Soham Shah, Charles Robert Jankowski, Deqing Yang, and Yanghua Xiao. Distilling script knowledge from large language models for constrained language planning. *arXiv preprint arXiv:2305.05252*, 2023.
- [154] Danyang Zhang, Lu Chen, Situo Zhang, Hongshen Xu, Zihan Zhao, and Kai Yu. Large language model is semi-parametric reinforcement learning agent. *arXiv preprint arXiv:2306.07929*, 2023.

- [155] Danyang Zhang, Lu Chen, Zihan Zhao, Ruisheng Cao, and Kai Yu. Mobile-Env: An evaluation platform and benchmark for interactive agents in LLM era. *arXiv preprint arXiv:2305.08144*, 2023.
- [156] Hongxin Zhang, Weihua Du, Jiaming Shan, Qinzhong Zhou, Yilun Du, Joshua B Tenenbaum, Tianmin Shu, and Chuang Gan. Building cooperative embodied agents modularly with large language models. *arXiv preprint arXiv:2307.02485*, 2023.
- [157] Wayne Xin Zhao, Kun Zhou, Junyi Li, Tianyi Tang, Xiaolei Wang, Yupeng Hou, Yingqian Min, Beichen Zhang, Junjie Zhang, Zican Dong, et al. A survey of large language models. *arXiv preprint arXiv:2303.18223*, 2023.
- [158] Wanjun Zhong, Lianghong Guo, Qiqi Gao, and Yanlin Wang. Memorybank: Enhancing large language models with long-term memory. *arXiv preprint arXiv:2305.10250*, 2023.
- [159] Shuyan Zhou, Frank F Xu, Hao Zhu, Xuhui Zhou, Robert Lo, Abishek Sridhar, Xianyi Cheng, Yonatan Bisk, Daniel Fried, Uri Alon, et al. Webarena: A realistic web environment for building autonomous agents. *arXiv preprint arXiv:2307.13854*, 2023.
- [160] Wei Zhou, Xiangyu Peng, and Mark Riedl. Dialogue shaping: Empowering agents through npc interaction. *arXiv preprint arXiv:2307.15833*, 2023.
- [161] Xizhou Zhu, Yuntao Chen, Hao Tian, Chenxin Tao, Weijie Su, Chenyu Yang, Gao Huang, Bin Li, Lewei Lu, Xiaogang Wang, et al. Ghost in the minecraft: Generally capable agents for open-world environments via large language models with text-based knowledge and memory. *arXiv preprint arXiv:2305.17144*, 2023.
- [162] Terry Yue Zhuo, Zhuang Li, Yujin Huang, Yuan-Fang Li, Weiqing Wang, Gholamreza Haffari, and Fatemeh Shiri. On robustness of prompt-based semantic parsing with large pre-trained language model: An empirical study on codex. *arXiv preprint arXiv:2301.12868*, 2023.
- [163] Caleb Ziems, William Held, Omar Shaikh, Jiaao Chen, Zhehao Zhang, and Diyi Yang. Can large language models transform computational social science? *arXiv preprint arXiv:2305.03514*, 2023.