

# A SURVEY OF SELF-EVOLVING AGENTS: ON PATH TO ARTIFICIAL SUPER INTELLIGENCE

Huan-ang Gao<sup>γ†</sup>, Jiayi Geng<sup>α†</sup>, Wenyue Hua<sup>ε†</sup>, Mengkang Hu<sup>ω†</sup>, Xinzhe Juan<sup>σμ†</sup>, Hongzhang Liu<sup>ξ†</sup>, Shilong Liu<sup>α†</sup>, Jiahao Qiu<sup>αδ†</sup>, Xuan Qi<sup>γ†</sup>, Yiran Wu<sup>ρ†</sup>, Hongru Wang<sup>τα†✉</sup>, Han Xiao<sup>τ†</sup>, Yuhang Zhou<sup>λ†</sup>, Shaokun Zhang<sup>ρ†</sup>, Jiayi Zhang<sup>π</sup>, Jinyu Xiang, Yixiong Fang<sup>θ</sup>, Qiwen Zhao<sup>ζ</sup>, Dongrui Liu<sup>σ</sup>, Qihan Ren<sup>σ</sup>, Cheng Qian<sup>β</sup>, Zhenghailong Wang<sup>β</sup>, Minda Hu<sup>τ</sup>, Huazheng Wang<sup>η</sup>, Qingyun Wu<sup>ρ</sup>, Heng Ji<sup>β</sup>, Mengdi Wang<sup>αδ✉</sup>

<sup>α</sup>Princeton University, <sup>δ</sup>Princeton AI Lab, <sup>γ</sup>Tsinghua University, <sup>ξ</sup>Carnegie Mellon University,

<sup>ε</sup>University of Sydney, <sup>π</sup>Shanghai Jiao Tong University, <sup>ρ</sup>Pennsylvania State University, <sup>μ</sup>University of Michigan,

<sup>η</sup>Oregon State University, <sup>τ</sup>The Chinese University of Hong Kong, <sup>λ</sup>Fudan University,

<sup>β</sup>The Hong Kong University of Science and Technology (Guangzhou), <sup>ω</sup>The University of Hong Kong,

<sup>ε</sup>University of California, Santa Barbara, <sup>ζ</sup>University of California San Diego,

<sup>β</sup>University of Illinois Urbana-Champaign,

**Github Repo:** <https://github.com/CharlesQ9/Self-Evolving-Agents>

<sup>†</sup>Equal contribution and the order is determined alphabetically, <sup>✉</sup>Corresponding Author

## ABSTRACT

Large Language Models (LLMs) have demonstrated remarkable capabilities across diverse tasks but remain fundamentally static, unable to adapt their internal parameters to novel tasks, evolving knowledge domains, or dynamic interaction contexts. As LLMs are increasingly deployed in open-ended, interactive environments, this static nature has become a critical bottleneck, necessitating agents that can adaptively reason, act, and evolve in real time. This paradigm shift—from scaling static models to developing self-evolving agents—has sparked growing interest in architectures and methods enabling continual learning and adaptation from data, interactions, and experiences. This survey provides the first systematic and comprehensive review of self-evolving agents, organizing the field around three foundational dimensions—*what to evolve, when to evolve, and how to evolve*. We examine evolutionary mechanisms across agent components (e.g., models, memory, tools, architecture), categorize adaptation methods by stages (e.g., intra-test-time, inter-test-time), and analyze the algorithmic and architectural designs that guide evolutionary adaptation (e.g., scalar rewards, textual feedback, single-agent and multi-agent systems). Additionally, we analyze evaluation metrics and benchmarks tailored for self-evolving agents, highlight applications in domains such as coding, education, and healthcare, and identify critical challenges and research directions in safety, scalability, and co-evolutionary dynamics. By providing a structured framework for understanding and designing self-evolving agents, this survey establishes a roadmap for advancing adaptive, robust, and versatile agentic systems in both research and real-world deployments, ultimately shedding lights to pave the way for the realization of Artificial Super Intelligence (ASI), where agents evolve autonomously, performing at or beyond human-level intelligence across a wide array of tasks.

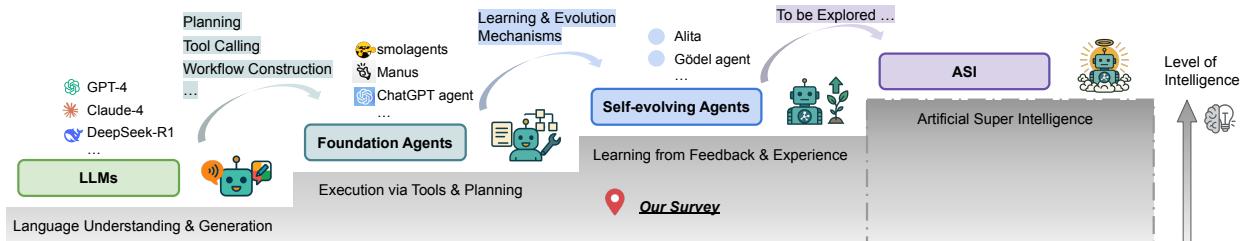


Figure 1: A conceptual trajectory illustrating the progression from large language models (LLMs) to foundation agents, advancing to self-evolving agents—our focus, and ultimately toward hypothetical Artificial Super Intelligence (ASI). Along this path, intelligence and adaptivity increase, marking a shift toward more autonomous and agentic AI systems.

## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Definitions and Foundations</b>	<b>5</b>
2.1	Definitions . . . . .	5
2.2	Relationships with Other Works . . . . .	7
<b>3</b>	<b>What to Evolve?</b>	<b>9</b>
3.1	Models . . . . .	9
3.2	Context . . . . .	10
3.2.1	Memory Evolution . . . . .	11
3.2.2	Prompt Optimization . . . . .	11
3.3	Tools . . . . .	12
3.4	Architecture . . . . .	13
3.4.1	Single-Agent System Optimization . . . . .	13
3.4.2	Multi-Agent System Optimization . . . . .	13
<b>4</b>	<b>When to Evolve</b>	<b>14</b>
4.1	Intra-test-Time Self-Evolution . . . . .	15
4.2	Inter-Test-Time Self-Evolution . . . . .	16
<b>5</b>	<b>How to Evolve</b>	<b>16</b>
5.1	Reward-based Self-Evolution . . . . .	18
5.2	Imitation and Demonstration Learning . . . . .	19
5.2.1	Self-Generated Demonstration Learning . . . . .	19
5.2.2	Cross-Agent Demonstration Learning . . . . .	20
5.2.3	Hybrid Demonstration Learning . . . . .	20
5.3	Population-based and Evolutionary Methods . . . . .	20
5.3.1	Single Agent Evolution . . . . .	21
5.3.2	Multi-Agent Evolution . . . . .	21
5.4	Cross-cutting Evolutionary Dimensions . . . . .	22
5.4.1	Online and Offline Learning . . . . .	23
5.4.2	On-policy and Off-policy Learning . . . . .	23
5.4.3	Reward Granularity . . . . .	24
5.5	Other Dimensions of Self-Evolution Methods . . . . .	25
<b>6</b>	<b>Where to Evolve?</b>	<b>25</b>
6.1	General Domain Evolution . . . . .	25
6.2	Specialized Domain Evolution . . . . .	26
<b>7</b>	<b>Evaluation of Self-evolving Agents</b>	<b>28</b>

7.1	Evaluation Goals and Metrics . . . . .	28
7.2	Evaluation Paradigm . . . . .	30
7.2.1	Static Assessment . . . . .	30
7.2.2	Short-Horizon Adaptive Assessment . . . . .	31
7.2.3	Long-Horizon Lifelong Learning Ability Assessment . . . . .	33
<b>8</b>	<b>Future Direction</b>	<b>34</b>
8.1	Personalize AI Agents . . . . .	34
8.2	Generalization . . . . .	34
8.3	Safe and Controllable Agents . . . . .	35
8.4	Ecosystems of Multi-Agents . . . . .	35
<b>9</b>	<b>Conclusion</b>	<b>36</b>

## 1 Introduction

*"It is not the most intellectual of the species that survives; it is not the strongest that survives; but the species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself."*

— Charles Darwin<sup>1</sup>

Large Language Models (LLMs) have demonstrated remarkable capabilities across a wide range of tasks. Yet, they remain fundamentally static [1], unable to adapt their internal parameters when encountering novel tasks, evolving knowledge domains, or dynamic interaction contexts. As LLMs are increasingly deployed in open-ended, interactive environments, this limitation becomes a critical bottleneck. In such settings, conventional knowledge retrieval mechanisms prove inadequate, giving rise to agents capable of dynamically adapting their perception, reasoning, and actions in real time. This emerging need for dynamic, continual adaptation signals a conceptual shift in artificial intelligence: *from scaling up static models to developing self-evolving agents*, such agents are capable of continuously learn from new data, interactions, and experiences in real-time, leading to systems that are more robust, versatile, and capable of tackling complex, dynamic real-world problems [2]. This shift is currently driving us toward a promising and transformative path to Artificial Super Intelligence (ASI), where the agents not only can learn and evolve from experience with an unpredictable speed but also perform at or above human-level intelligence across a wide array of tasks [3].

Unlike static LLMs, which remain constrained by their inability to adapt to novel and evolving contexts, self-evolving agents are designed to overcome these limitations by continuously learning from real-world feedback. This progression reshapes our understanding of agents. Self-evolving agents, as a core concept, will be the precursors to ASI, acting as intermediaries that pave the way for the ultimate evolution of intelligence, as shown in Figure 1. Recent research initiatives have increasingly focused on developing adaptive agent architectures capable of continually learning and adapting from experience, such as recent advancements in agent frameworks [4], prompting strategies [5], and different optimization ways to evolve. Notwithstanding these advances, existing surveys predominantly address agent evolution as a subsidiary component within comprehensive agent taxonomies. Previous surveys primarily provide systematic overviews of general agent development, while offering limited coverage of self-evolving mechanisms across constrained scenarios in self-evolving agents [1, 6]. For example, Luo et al. [1] discuss several ways to evolve, such as self-learning and multi-agent co-evolution, while Liu et al. [6] explicitly introduce the evolution in terms of different components of agents, such as tools and prompts. Moreover, some studies focus specifically on the evolution of language models themselves [7], rather than on the broader concept of agents. Yet, there is no systematic survey devoted to a dedicated, comprehensive investigation of self-evolving agents as a first-class research paradigm. This gap has left fundamental questions underexplored: *What aspects of an agent should evolve? When should adaptation occur? And how should that evolution be implemented in practice?*

To the best of our knowledge, this is the first systematic and comprehensive survey focusing on self-evolving agents, offering a clear roadmap for both theoretical inquiry and practical deployment. We organize our analysis around three foundational questions — *what, when, and how to evolve* — and provide a structured framework for understanding each. Specifically, we systematically examine individual agent components, including the model, memory, tools and corresponding workflow, investigating their distinct evolutionary mechanisms (what to evolve of agent in Section 3); then we divide existing evolving methods according to different temporal stages with different learning paradigms such as supervised fine-tuning, reinforcement learning and inference-time evolving (when to evolve in Section 4). We finally summarize different signals to guide the evolution of agents, such as textual feedback or scalar rewards, and also different architectures of agents to evolve, such as single-agent and multi-agent evolution (how to evolve in Section 5). Furthermore, we review certain evaluation metrics and benchmarks to track existing advancements of self-evolving agents, emphasizing the importance of co-evolution between evaluation and agents (Section 6). We also examine emerging applications in domains such as coding, education, and healthcare, where continual adaptation and evolution are essential (Section 7). Finally, we identify persistent challenges and outline promising research directions to guide the development of self-evolving agents (Section 8). Through this systematic decomposition of self-evolutionary processes across orthogonal dimensions, we provide a structured and practical framework enabling researchers to systematically analyze, compare, and design more robust and adaptive agentic systems. To sum up, our key contributions are as follows:

- We establish a unified theoretical framework for characterizing self-evolutionary processes in agent systems, anchored around three fundamental dimensions: what evolves, how it evolves, and when it evolves, providing clear design guidance for future self-evolving agentic systems.

---

<sup>1</sup>This quote is widely attributed to Charles Darwin, but it does not appear verbatim in his writings. The phrasing is believed to originate from Professor Leon C. Megginson, who paraphrased Darwin's ideas. Despite its frequent misattribution, the quote effectively captures the essence of Darwinian evolution and has since been popularized in both scientific and managerial literature.

- We further investigate the evaluation benchmark or environment tailored for self-evolving agents, highlighting emerging metrics and challenges related to adaptability, robustness, and real-world complexity.
- We showcase several key real-world applications across various domains, including autonomous software engineering, personalized education, healthcare, and intelligent virtual assistance, illustrating the practical potential of self-evolving agents.
- We identify critical open challenges and promising future research directions, emphasizing aspects like safety, personalization, multi-agent co-evolution, and scalability.

In doing so, our survey provides researchers and practitioners with a more structured taxonomy for understanding, comparing, and advancing research of self-evolving agents from different perspectives. As LLM-based agents are increasingly integrated into mission-critical applications, understanding their evolutionary dynamics becomes essential, extending beyond academic research to encompass industrial applications, regulatory considerations, and broader societal implications.

## 2 Definitions and Foundations

Before delving into a comprehensive survey, we first present a formal definition of self-evolving agents and introduce a taxonomy of the key aspects in self-evolving agents. We also discuss the relationships between self-evolving agents and other renowned learning paradigms, such as curriculum learning, lifelong learning, model editing, and unlearning, highlighting the adaptive, dynamic, and autonomous nature of self-evolving agents.

### 2.1 Definitions

**Environment** We first define the environment (including the user and the execution environment, e.g., Linux shell) of an agent system as a partially observable Markov Decision Process (POMDP), represented as a tuple  $E = (\mathcal{G}, \mathcal{S}, \mathcal{A}, T, R, \Omega, O, \gamma)$ , where:

- $\mathcal{G}$  is a set of potential goals. Each  $g \in \mathcal{G}$  is a task objective that the agent needs to achieve, e.g., a user query.
- $\mathcal{S}$  is a set of states. Each  $s \in \mathcal{S}$  represents the internal state of the environment.
- $\mathcal{A}$  is a set of actions. Each action  $a \in \mathcal{A}$  can be a combination of textual reasoning, retrieval of external knowledge, and tool calls.
- $T$  is the state transition probability function which takes a state-action pair  $(s, a)$  and outputs the probability distribution  $T(s'|s, a)$  of the next state.
- $R : \mathcal{S} \times \mathcal{A} \times \mathcal{G} \rightarrow \mathcal{R}$  is the feedback/reward function, conditioned on the specific goal  $g \in \mathcal{G}$ . The feedback  $r = R(s, a, g)$  typically takes the form of a scalar score or textual feedback.
- $\Omega$  is a set of observations accessible to the agent.
- $O$  is the observation probability function which takes a state-action pair  $(s, a)$  and outputs the probability distribution  $O(o'|s, a)$  of the next observation for the agent.
- $\gamma$  is the discount factor.

**Agent system** We define a (multi-)agent system as  $\Pi = (\Gamma, \{\psi_i\}, \{C_i\}, \{\mathcal{W}_i\})$ . The architecture  $\Gamma$  determines the control flow of the agent system or collaborative structures between multiple agents. It is typically represented as a sequence of nodes ( $N_1, N_2, \dots$ ) organized by graph or code structures. Each node  $N_i$  consists of the following components:

- $\psi_i$ : the underlying LLM/MLLM.
- $C_i$ : the context information, e.g., prompt  $P_i$  and memory  $M_i$ .
- $\mathcal{W}_i$ : the set of available tools/APIs.

At each node, the agent policy is a function  $\pi_{\theta_i}(\cdot|o)$  that takes an observation and outputs the probability distribution of the next action, where  $\theta_i = (\psi_i, C_i)$ . The actual action space here is the union of the natural language space and the tool space  $\mathcal{W}_i$ .

For a given task  $\mathcal{T} = (E, g)$ , represented by an environment  $E$  and a corresponding goal  $g \in \mathcal{G}$ , the agent system follows the topology  $\Gamma$  to generate a trajectory  $\tau = (o_0, a_0, o_1, a_1, \dots)$ , and receives a feedback  $r$  either from the external environment or from internal signals (e.g., self-confidence or feedback from an evaluator).

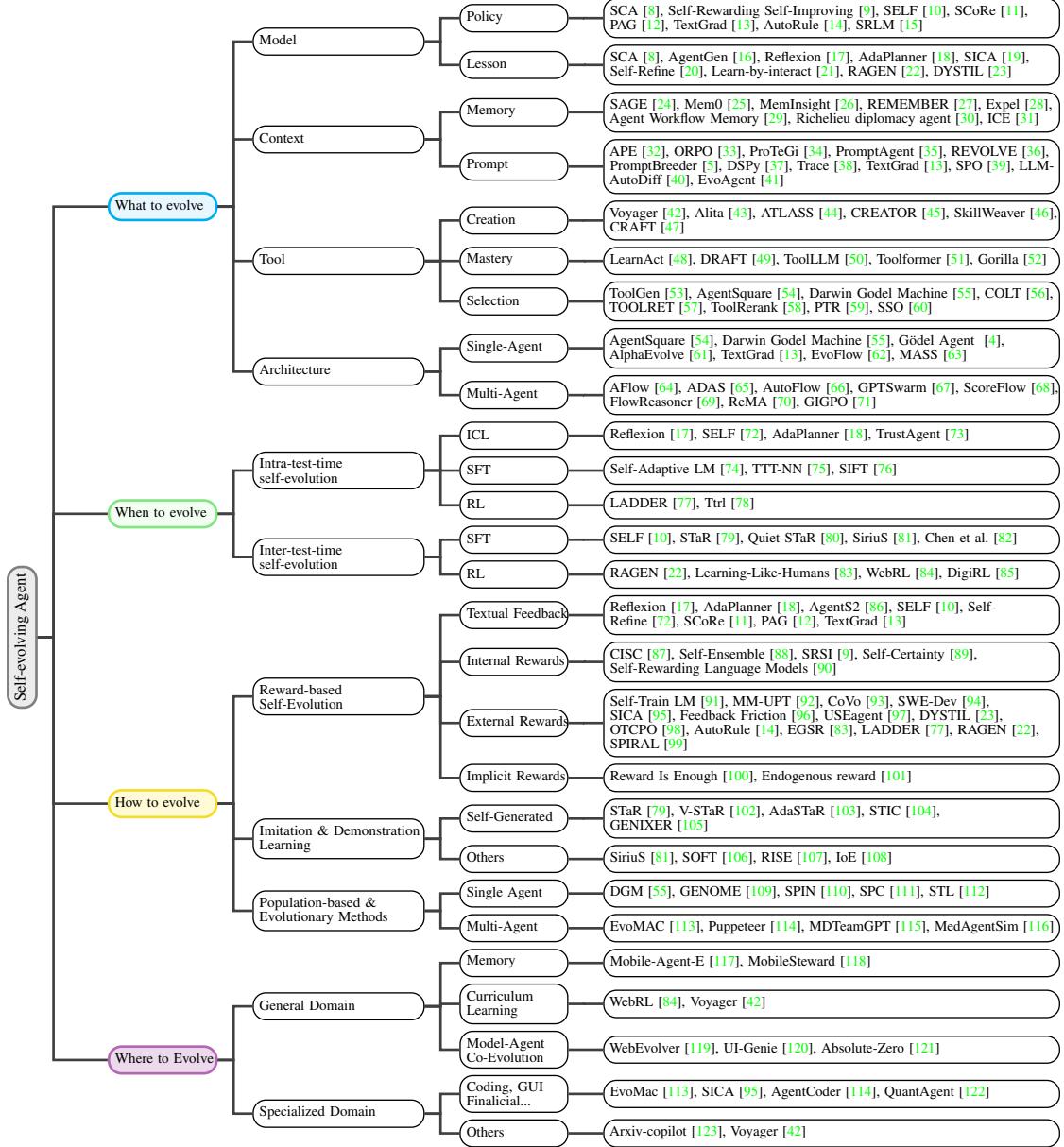


Figure 2: Taxonomy of self-evolving agents, in which agents are analyzed along the *what*, *when*, *how*, and *where* dimensions, with selected representative methods and systems annotated at each leaf node.

**Self-evolving strategy** A self-evolving strategy is a transformation  $f$  that maps the current agent system to a new state, conditioned on the generated trajectory  $\tau$  and the external/internal feedback  $r$ :

$$f(\Pi, \tau, r) = \Pi' = (\Gamma', \{\psi'_i\}, \{C'_i\}, \{\mathcal{W}'_i\}) \quad (1)$$

**Objective of self-evolving agents** Let  $U$  be a utility function that measures the performance of an agent system  $\Pi$  on a given task  $\mathcal{T}$  by assigning a scalar score  $U(\Pi, \mathcal{T}) \in \mathbb{R}$ . The utility may be derived from the task-specific feedback  $r$ , such as a reward signal or textual evaluation, possibly combined with other performance indicators (e.g., completion time, accuracy, or robustness). Given a sequence of tasks  $(\mathcal{T}_0, \mathcal{T}_1, \dots, \mathcal{T}_n)$  and an initial agent system  $\Pi_0$ , a self-evolving strategy  $f$  recurrently generates an evolving sequence of agent systems  $(\Pi_1, \Pi_2, \dots, \Pi_n)$  via

$$\Pi_{j+1} = f(\Pi_j, \tau_j, r_j), \quad (2)$$

where  $\tau_j$  and  $r_j$  are the trajectory and feedback on task  $\mathcal{T}_j$ .

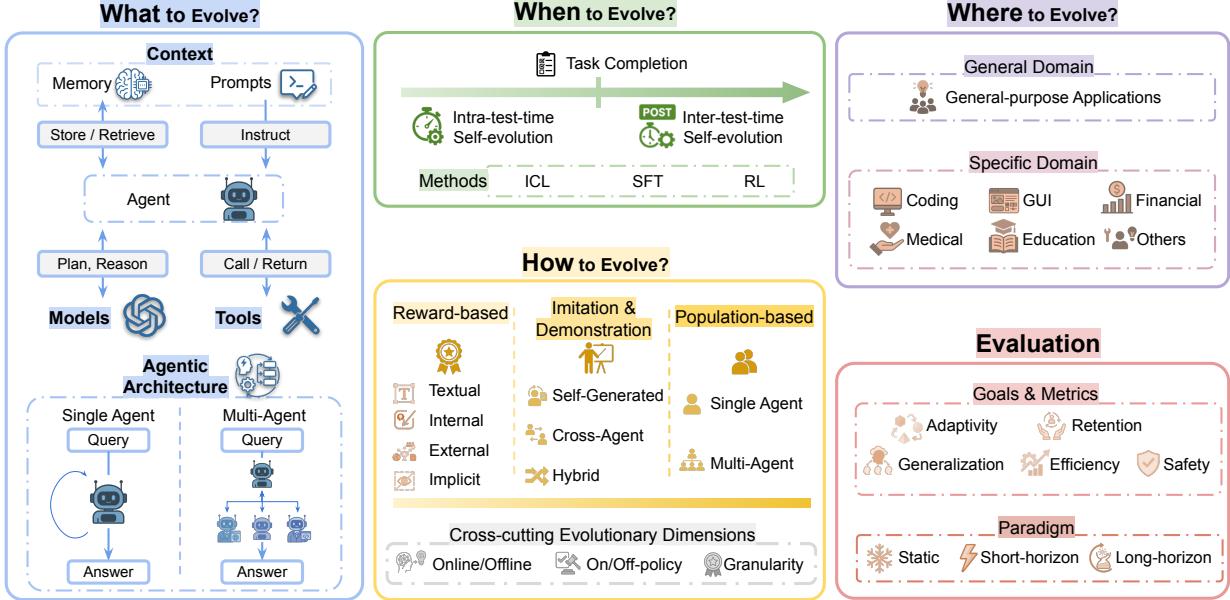


Figure 3: A comprehensive overview of self-evolving agents across key dimensions: **What to evolve**: covering four major categories—Model, Context, Tool, and Architecture; **When to evolve**: differentiating intra-test-time and inter-test-time self-evolution, via in-context learning (ICL), supervised fine-tuning (SFT), or reinforcement learning (RL); **How to evolve**: centered on three main paradigms—reward-based, imitation and demonstration, and population-based methods. These are complemented by cross-cutting dimensions. **Where to evolve**: ranging from general-purpose domains to specific domains; **Evaluation**: focusing on goals (e.g., adaptivity, safety, generalization) and evaluation paradigms (static, short-horizon, or long-horizon).

The overarching objective in designing a self-evolving agent is to construct a strategy  $f$  such that the cumulative utility over tasks is maximized:

$$\max_f \sum_{j=0}^n U(\Pi_j, \mathcal{T}_j) \quad (3)$$

## 2.2 Relationships with Other Works

Table 1 summarizes the key distinctions between self-evolving agents and other paradigms (including curriculum learning, lifelong learning, model editing, and unlearning). Unlike these existing paradigms that primarily focus on updating model parameters, self-evolving agents expand the scope of updating targets to include non-parametric components, such as context (prompts and memory) and toolset. This expanded space provides greater flexibility, enabling self-evolving agents to operate effectively in sequential task settings and adapt at test time. More crucially, self-evolving agents uniquely demonstrate the ability of active exploration (e.g., searching for open-source tools online [43]), structural modification of their own topology (e.g., iteratively modifying the workflow [64] or code [55]), and self-reflection and self-evaluation capabilities (e.g., providing verbal feedback using an internal evaluator LLM [17]), which are absent in previous paradigms.

We provide a brief introduction to each paradigm below, highlighting the differences among these paradigms, as well as the differences with self-evolving agents.

**Curriculum Learning** Curriculum learning is a training strategy for AI models in which data are presented in order of increasing difficulty [124, 125]. This strategy resembles human curricula where concepts are introduced progressively from simple to complex. Curriculum learning has been widely adopted across diverse domains, including computer vision [126, 127, 128], natural language processing [129, 130], speech recognition [131, 132], etc. Recently, several curriculum learning-based methods have been proposed to fine-tune LLMs during the post-training phase [133, 134, 135, 83, 136]. The framework for curriculum learning generally comprises two key components: a difficulty measurer that quantifies the difficulty level of each training data point, and a training scheduler that reorganizes the order of data points received by the model according to the difficulty level. Unlike curriculum learning, which operates on a

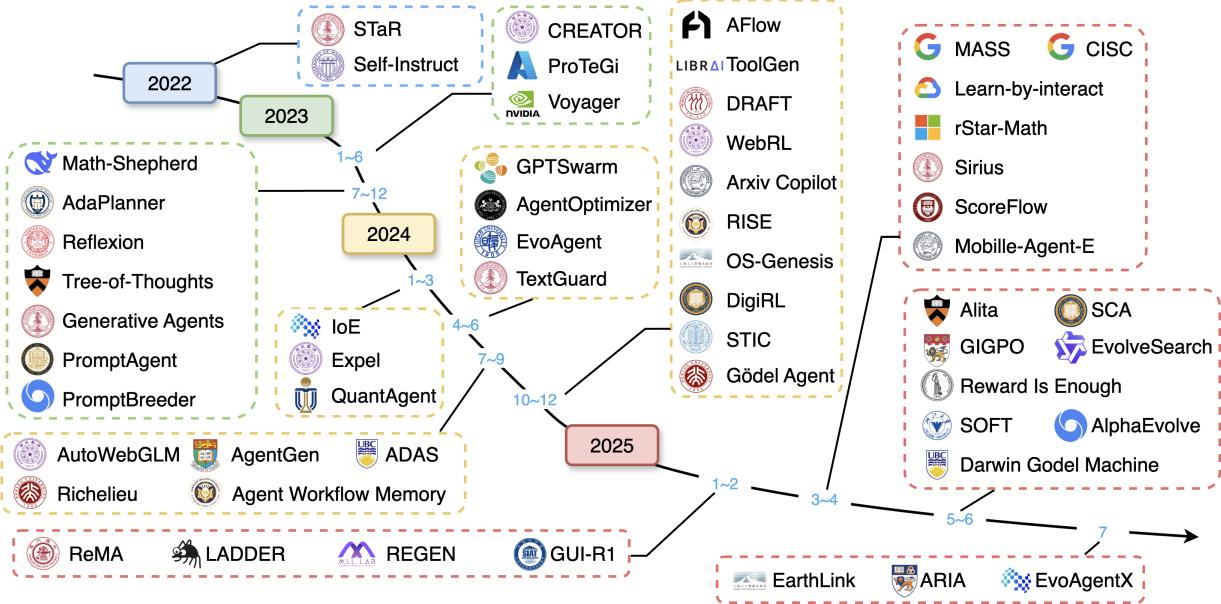


Figure 4: An evolutionary landscape of several representative self-evolving agent frameworks from 2022 to 2025. The figure chronologically organizes major research milestones in the development of self-evolving agents with capabilities such as autonomous planning, tool use, and continual self-improvement.

static dataset, self-evolving agents aim to handle sequential tasks in dynamic environments. Additionally, curriculum learning updates only model parameters, whereas self-evolving agents are able to adjust non-parametric components like memory and tools.

**Lifelong Learning** Lifelong learning refers to the ability of AI models to continuously and adaptively learn when exposed to new tasks and environments, while retaining previously acquired knowledge and abilities. This learning paradigm, also known as continual learning or incremental learning, is crucial for AI models to operate in dynamic and complex environments [137, 138, 139, 140, 141, 142]. The primary goal of lifelong learning for AI models is to achieve a balance between preserving existing knowledge (stability) and acquiring new knowledge (plasticity) when exposed to new data or tasks [143, 138, 144, 145]. Though it shares the sequential task setting with self-evolving agents, lifelong learning differs in two ways: (1) like curriculum learning, lifelong learning typically updates only model parameters, lacking the ability to modify non-parametric components; (2) lifelong learning primarily acquires knowledge passively through external feedback or manual guidance, whereas self-evolving agents actively explore their environment and may incorporate internal reflection or self-evaluation mechanisms.

**Model Editing and Unlearning** Model editing and unlearning aim to efficiently and precisely modify specific knowledge in AI models while preserving irrelevant knowledge and avoiding full retraining [146, 147, 148, 147, 149, 150]. A canonical application of model editing is to perform efficient and precise localized factual updates (e.g., modifying the answer to “2021 Olympics host city” from “Tokyo” to “Paris”). Early methods focused on triples of atomic knowledge and later expanded into various trustworthy-related tasks [151, 152]. Recent studies also propose lifelong model editing [153] that sequentially performs model editing. For model unlearning, early efforts mainly focus on the removal of privacy-related information [154]. With the rapid development of LLMs, model unlearning is also used to enhance LLMs’ safety [155, 156, 157, 158]. Compared to lifelong learning, model editing shares an aligned objective: both aim to acquire new knowledge or capabilities while mitigating catastrophic forgetting. However, lifelong learning typically relies on extensive gradient-based fine-tuning across all model parameters, whereas model editing often modifies only a small subset of parameters in a targeted manner. Compared to self-evolving agents, model editing (1) cannot modify non-parametric components such as memory or tools, and (2) relies on a pre-defined pipeline from the algorithm designer, whereas self-evolving agents can spontaneously employ more diverse and flexible strategies based on the observation of the environment or internal feedback signals.

Table 1: Comparison between self-evolving agents and other renowned paradigms, including curriculum learning, lifelong learning, model editing and unlearning.

Paradigm	Evolving Context	Evolving Toolset	Dynamic Tasks	Test-time Adaptation	Active Exploration	Structural Change	Self-reflect & Eval
Curriculum Learning	✗	✗	✗	✗	✗	✗	✗
Lifelong Learning	✗	✗	✓	✗	✗	✗	✗
Model Editing	✗	✗	✓	✓	✗	✗	✗
<b>Self-evolving Agents</b>	✓	✓	✓	✓	✓	✓	✓

### 3 What to Evolve?

The transition from pre-programmed, static systems to genuinely autonomous intelligent agents hinges on one critical capability: self-evolution. This capability for continuous improvement is not monolithic; instead, it manifests across various facets of an agent’s being. Therefore, the first key aspect of a self-evolving agent is identifying the *evolving components* – which components in the agent system  $\Pi = (\Gamma, \{\psi_i\}, \{C_i\}, \{\mathcal{W}_i\})$  can be explicitly changed over time?

Following the formulation in Section 2.1, we can decompose the agent system into four fundamental, evolvable pillars. Our investigation starts at the agent’s cognitive core, namely the **Models**  $\{\psi_i\}$ , and examines how the fundamental parameters that govern its reasoning and behavior are continuously updated through its own experiences[8, 22]. We then consider the **Context**  $\{C_i\}$  that shapes its actions, exploring the evolution of both the instructions[39, 37] it follows and the long-term memory[25, 29] it draws upon to stay informed and adapt. From this internal foundation, we shift to the agent’s external capabilities, analyzing how it evolves its set of **Tools**  $\{\mathcal{W}_i\}$  by autonomously creating[43], mastering[49], and managing new skills[53] to overcome its innate limitations. Finally, we scale our perspective to the Agentic System itself, investigating how the agentic system’s **architecture**[65, 64] and collaborative structures[70] are dynamically optimized to enhance overall performance and efficiency. We present a subset of these evolving dimensions in Table 2.

#### 3.1 Models

Models constitute the central substrate of intelligent agents, directly determining their reasoning, planning, and decision-making behaviors. The ability of these models to evolve by continually adapting their internal parameters and expanding their functional capabilities is essential for the development of autonomous, general-purpose agents. Unlike static systems that rely heavily on human-annotated datasets and fixed training regimes, self-evolving models can improve through interaction, self-supervised data generation, and dynamic learning loops, thereby achieving greater efficiency, adaptability, and scalability. In detail, we outline the principal axes along which model evolution unfolds. These include learning from self-generated supervision to refine model weights, evolving through interaction with constructed or external environments. Together, these strategies represent a shift from passive learning paradigms toward active, continual, and self-directed improvement.

**Policy** A self-evolving agent can refine its parameters to perform better on targeted tasks. Traditional methods of data collection for training agents on tool-use benchmarks are costly and often yield limited coverage, while purely synthetic data-generation pipelines typically suffer from inadequate quality. Consequently, recent studies emphasize enabling agents to autonomously generate data to improve their own model weights. One representative approach is the Self-Challenging Agent (SCA)[8], where a language model alternates roles between a challenger generating executable Code-as-Task problems and an executor solving them. The model then fine-tunes its parameters using trajectories derived from successful solutions, resulting in significant performance gains on complex, multi-step tasks. Similarly, the Self-Rewarding Self-Improving framework[9] implements an internal self-judging mechanism, allowing the model to autonomously generate problems, solve them, and assess its performance, thus producing self-contained fine-tuning data without external annotations. This method demonstrated notable improvements, particularly in complex reasoning tasks. Beyond task creation, another promising research direction involves leveraging interaction feedback directly for parameter updates. For instance, SELF [10], SCoRe [11], and PAG [12] interpret execution traces or natural-language critiques as reward signals within an online Supervised Fine-Tuning (SFT) combined with Reinforcement Learning (RL) framework, enabling continuous policy improvement. TextGrad [13] further extends this concept by treating unstructured textual feedback as a differentiable training signal capable of directly influencing both prompt design and model parameters. Additionally, AutoRule [14] converts language-model reasoning traces and preference feedback into explicit rule-based training rewards, enhancing the quality of model outputs through structured reward signals. Collectively, these advancements chart a clear trajectory—from agents autonomously crafting their training

Table 2: Representative self-evolving agent methods positioned along four evolutionary pillars; a filled bullet (●) marks dimensions where the approach actively evolves.

Method	Model		Context		Tool			Architecture	
	Policy	Experience	Prompt	Memory	Creation	Mastery	Selection	Single	Multi
SCA [8]	●	●	○	○	●	○	○	○	○
RAGEN [22]	●	●	●	○	○	○	○	●	○
AgentGen [16]	○	●	●	●	●	○	○	●	○
Promptbreeder [5]	○	○	●	○	○	○	○	●	○
Expel [28]	○	●	○	●	○	○	○	○	○
Agent Workflow Memory [29]	○	○	○	●	○	○	●	○	○
Mem0 [25]	○	○	○	●	○	○	○	○	○
MAS-Zero [159]	○	○	●	○	○	○	○	○	●
Multi-Agent Design [63]	○	○	●	○	○	○	●	○	●
SPO [39]	○	○	●	○	○	○	○	○	○
Alita [43]	○	○	○	○	●	○	●	○	○
TextGrad [13]	○	○	●	○	○	●	●	●	○
DGM [55]	○	○	●	○	○	○	○	●	○
AlphaEvolve [61]	○	○	●	○	●	●	○	●	○
ADAS [65]	○	○	●	○	●	○	○	●	●
AFlow [64]	○	○	●	○	●	○	●	●	●
ReMA [70]	○	○	○	○	○	○	○	●	●
SkillWeaver [46]	○	○	○	●	●	●	●	○	○
LearnAct [48]	○	○	○	●	●	○	●	○	○
DRAFT [49]	○	○	●	○	●	●	○	○	○
ToolGen [53]	○	○	○	●	●	●	○	○	○
CRAFT [47]	○	○	○	○	●	●	●	○	○
CREATOR [45]	○	○	○	○	●	●	○	○	○
Voyager [42]	○	○	●	●	●	●	●	○	●

tasks to directly refining their parameters based on execution feedback, highlighting the capacity of models to evolve continuously by learning from the data they produce.

**Experience** Agents can evolve not only by adjusting their internal parameters but also by actively interacting with or even constructing their environments, capturing experiences, and transforming them into learning signals that drive iterative improvement. This environmental loop provides agents with the complexity and diversity required for scalable self-adaptation. The Self-Challenging Agent (SCA)[8] exemplifies this dynamic at the task level, where the agent autonomously generates novel Code-as-Task problems, executes them, and then filters successful trajectories for retraining itself. AgentGen[16] extends this concept to full-environment generation, synthesizing diverse simulation worlds (in PDDL or Gym-style formats) derived from an initial corpus. It implements a bidirectional evolution loop that progressively adjusts task difficulty, enabling the agent to continuously grow within a dynamically structured curriculum. Reflexion [17] complements this by introducing self-reflective mechanisms, where agents iteratively record natural-language critiques of their previous actions, guiding future behavior to avoid recurring mistakes. Additionally, AdaPlanner [18] introduces closed-loop adaptive planning, allowing agents to refine their strategies on-the-fly based on environmental feedback, effectively reshaping action sequences in response to immediate outcomes. Similarly, Self-Refine [20] employs an iterative refinement loop in which the agent repeatedly critiques and revises its initial outputs, significantly improving task accuracy without explicit retraining. SICA (Self-Improving Coding Agent) [19] further pushes the boundary by enabling agents to autonomously edit their underlying code and tools, iteratively enhancing their core reasoning abilities through direct self-modification. From a reinforcement learning perspective, frameworks such as RAGEN [22] and DYSTIL [23] conceptualize multi-step tool-use tasks as Markov Decision Processes, optimizing agent policies through rich environmental rewards and strategy induction loops. RAGEN leverages dense feedback from the environment to iteratively fine-tune action policies, while DYSTIL utilizes high-level strategy advice generated by language models to progressively internalize complex decision-making skills into reinforcement learning agents. Collectively, these approaches highlight a compelling paradigm where self-evolving agents not only leverage self-generated data but actively reshape their environments and internal mechanisms to fuel ongoing learning. Such dynamic interaction loops point toward autonomous, open-ended improvement cycles deeply grounded in experiential adaptation.

### 3.2 Context

An essential component of an LLM agent to be evolved is the context, which shapes how an agent behaves. To start with, we want to interpret two terms, "prompt optimization" and "memory evolution", which have been used in different literature. In most cases, these two terms can be used interchangeably because they both refer to what is included in

the context window. Prompt optimization asks "how can we phrase or structure the instructions so the LLM behaves better?", and attends to details such as the wording, ordering. On the other hand, memory evolution asks "how should we store, forget, and retrieve context so that the agent can stay informed and perform better?", which focuses on what past information to surface or archive.

### 3.2.1 Memory Evolution

LLM-based agents are increasingly designed with long-term memory mechanisms that grow and adapt as the agent continues to solve tasks and interacts with its environment [160, 161]. An evolving memory enables the agent to accumulate knowledge, recall past events, and adjust its behavior based on experience. Many works stress that effective memory management is crucial for agent performance [162, 163, 164]. SAGE [24] uses the Ebbinghaus forgetting curve to decide what to remember or forget. A-mem[165] updates the agent memory structure to create interconnected knowledge networks through dynamic indexing and linking, following the basic principles of the Zettelkasten method. Mem0 [25] introduces a two-phase pipeline where the agent first extracts salient facts from recent dialogue and then decides how to update the long-term memory: the agent can ADD new facts, MERGE/UPDATE redundant ones, or DELETE contradictions. Such a mechanism ensures the agent's long-term memory is coherent and up-to-date. MemInsight [26] augments raw memories with semantic structure, which summarizes and tags past interactions for retrieval later. REMEMBER [27] combines an LLM with a memory of experiences and uses reinforcement learning signals to decide how to update that memory after each episode.

A critical aspect of memory evolution is enabling agents to learn heuristics or skills from past experiences. Rather than only retrieving exact past instances, advanced agents distill experiences into more general guidance [28, 166]. Expel [28] processes past trajectories to generate insights and rules to guide further interactions. This experiential knowledge accumulation leads to measurable gains, as the agent steadily performs better with more experience. Other systems focus on storing higher-level building blocks of problem-solving. For instance, Agent Workflow Memory [29] records common sub-task sequences (workflows) so that an agent solving a complex task can retrieve and reuse a proven sequence of actions rather than plan from scratch. In the Richelieu diplomacy agent, the system improves its negotiation strategies by augmenting its memory through self-play games, storing the insights from simulated interactions to refine future decisions [30]. By generalizing from specific episodes to reusable knowledge, these approaches illustrate how memory evolution turns an agent's one-time experiences into long-term competencies, which leads to agents evolving.

### 3.2.2 Prompt Optimization

While memory evolution focused on what knowledge an agent retains, Prompt Optimization (PO) enables LLM agents to self-evolve by refining the instructions it feeds to the backbone model, which directly alters the model's behavior without modifying model weights [167]. Early research treats instruction design as a search problem. APE [32] generates candidate prompts, scores them on validation examples, and selects the best. ORPO [33] extends this idea by letting the model iteratively rewrite its own prompt, guided by feedback on prior outputs. ADO [168] introduces DSP that imposes semantic constraints on iteratively proposed prompts to facilitate finding the optimal prompt. ProTeGi [34] generates natural language "corrections" that are applied as edits to the prompt, forming a textual analogue of gradient descent. PromptAgent [35] casts prompt discovery as Monte-Carlo Tree Search, exploring instruction space strategically, while evolutionary approaches like PromptBreeder [5] maintain a population to discover increasingly effective instructions. REVOLVE [36] further stabilizes long optimization runs by tracking the trajectory of model responses and applying smoothed updates. Pushing this autonomy to its limit, SPO [39] creates a fully self-contained loop where the model generates its training data and uses pairwise preference comparison on its outputs to refine the prompt, eliminating the need for any external labeled data or human feedback. Collectively, these techniques demonstrate that an agent can autonomously improve its prompting policy, turning prompt text into a learnable component that co-evolves with the agent's experience.

In complex systems, an agent often orchestrates a sequence of LLM calls or collaborates with other agents, making prompt design a multi-node problem. Frameworks such as DSPy represent an entire workflow as a graph whose sub-prompts are jointly tuned for a global objective [37]. Trace [38], TextGrad [13], and LLM-AutoDiff [40] generalize this idea by treating each prompt as a parameter in a differentiable program and propagating natural-language "gradients" to refine every step. In collaborative scenarios, Multi-Agent System Search (MASS) [63] first optimizes individual role prompts and then refines inter-agent communication patterns, while MAS-ZERO [159] dynamically proposes and revises role prompts to assemble an effective team for each new problem. Evolutionary systems such as EvoAgent [41] and AgentSquare [54] treat each agent along with prompts as the modules and use mutation and selection to discover specialized teams that outperform hand-crafted designs. These approaches extend PO from a single instruction to the language that defines whole workflows or societies of agents.

### 3.3 Tools

An agent's capabilities are fundamentally defined by the tools it can wield. The trajectory of agent development is marked by a crucial evolution: from being mere tool users to becoming autonomous tool makers. This transition from relying on predefined, static toolsets to enabling agents to autonomously expand and refine their own skills is a critical leap towards cognitive self-sufficiency. This paradigm, where agents dynamically adapt their capabilities, allows them to solve a long tail of complex problems not envisioned by their initial designers. This evolution unfolds across three interconnected fronts: tool discovery, mastery, and management, as detailed in the subsections below.

**Autonomous Discovery and Creation** The primary impetus for autonomous tool creation is to overcome the inherent limitations of a fixed toolset, granting agents the flexibility to innovate on demand. Methodologies for this now span a spectrum from opportunistic discovery to formalized synthesis. At one end, agents like Voyager build an ever-expanding library of skills through emergent trial-and-error, driven by an intrinsic motivation to explore complex, open-ended environments like Minecraft [42]. This exploratory approach is powerful for generating a wide array of skills but may lack precision. In contrast, systems like Alita and ATLASS take a more reactive approach, often employing retrieval-augmented generation (RAG) to search open-source code repositories or write new functions from scratch the moment a capability gap is identified [43, 44]. At the other end of the spectrum lie highly structured frameworks that treat tool creation as a deliberate engineering process. CREATOR, for example, disentangles abstract tool creation (e.g., reasoning about the general structure of a reusable function for averaging temperatures over N days) from concrete tool usage (e.g., deciding how to apply that function to a specific city and time range), which enhances modularity and reusability [45]. Even more formally, SkillWeaver analyzes successful human or agent task trajectories to propose, synthesize, and hone new skills into robust, reusable APIs, ensuring a higher degree of initial quality [46]. Furthermore, frameworks like CRAFT demonstrate that creating specialized toolsets for specific domains is essential to complement general-purpose models, enabling expert-level performance without sacrificing adaptability [47]. However, this burgeoning autonomy introduces significant challenges, particularly around safety and security. The unconstrained generation of code risks creating tools with exploitable vulnerabilities or unintended harmful behaviors, making automated verification and sandboxing critical areas for future research.

**Mastery Through Iterative Refinement** The proliferation of self-created tools necessitates a robust mechanism for their mastery; a newly generated tool is often a brittle script, not a reliable function. This is where iterative refinement becomes essential. Frameworks like LearnAct and From Exploration to Mastery establish a critical self-correction loop where the agent learns from its own experience [48, 49]. This involves tackling the difficult "credit assignment" problem: determining precisely which line of code or which parameter was responsible for a failure. To do this, the agent analyzes a rich variety of feedback signals—including compiler errors, unexpected API return values, environmental state changes, or even implicit signals from a user's subsequent actions. The goal is not only to debug the tool's underlying code but also to refine its documentation (e.g., its docstring and argument descriptions), which is crucial for improving the agent's ability to understand and correctly use the tool in the future. This refinement process also opens the door for valuable human-agent collaboration. While full autonomy is the ultimate goal, many systems can be designed with a "human in the loop," where a human expert can provide corrections, offer high-level suggestions, or validate a newly created tool. This collaborative approach can significantly accelerate the mastery process and ensure that the agent's skills align with human intentions and safety standards. Ultimately, this self-honing process is what elevates a nascent skill into a dependable capability, ensuring the agent's growing skill library increases not just in quantity, but more importantly, in quality and robustness.

**Scalable Management and Selection** As an agent's mastered skill library grows into the hundreds or thousands, it faces a "curse of abundance." The challenge shifts from creating tools to efficiently managing and selecting from them. A large library creates a massive search space, making traditional retrieval methods slow and inaccurate. To overcome this, ToolGen represents a fundamental paradigm shift by encoding tools as unique tokens within the language model's vocabulary. This elegantly reframes tool retrieval as a generation problem, leveraging the transformer's immense pattern-recognition capabilities to predict the most appropriate tool as a natural continuation of its thought process [53]. Beyond selecting a single tool, advanced agents must also excel at tool composition—learning to chain multiple tools in novel sequences to solve multi-step problems. This is a higher-order management task. Architectural approaches like AgentSquare engage in a form of meta-learning, automatically searching the modular design space of an agent—including its planning, memory, and tool-use components—to find an optimal configuration for complex task execution [54]. As a logical endpoint to this evolutionary trend, visionary concepts like the Darwin Godel Machine propose a framework for open-ended evolution, where the agent can fundamentally rewrite its own core code. In this vision, the distinction between the agent and its tools blurs, leading to a recursive cascade of self-improvement that transcends tool enhancement alone [55]. In essence, this entire evolutionary path aims to establish a closed and virtuous

cycle: a truly autonomous agent that can perceive gaps in its capabilities, create novel solutions, master them through practice, and seamlessly integrate them into a coherently managed and ever-expanding repertoire.

### 3.4 Architecture

The defining feature of next-generation agentic systems is their intrinsic capacity for self-improvement. This marks a fundamental shift from systems with fixed capabilities to those that can autonomously enhance their performance[169]. By treating their own internal logic and collaborative structures as optimizable components, these systems can adapt their behavior and design in response to feedback, achieving a level of efficiency and effectiveness that static designs cannot match. This section details how this self-optimization is realized, first by examining improvements within single-agent systems and then by exploring the co-evolution of complex multi-agent systems.

#### 3.4.1 Single-Agent System Optimization

**LLM-Invoking Node Optimization** Optimizing a single LLM call is straightforward in isolation, but within an agentic system, it becomes a difficult credit assignment problem, as the effect of any single change is obscured by subsequent steps. Research addresses this by making node-level components optimizable, following two main strategies. The first focuses on refining nodes within a fixed agentic topology. A prime example is TextGrad [13], which, inspired by backpropagation, uses "textual gradients" to propagate feedback from the final output backward through the workflow, guiding systematic, local refinements at each node without altering the system's overall structure. The second, parallel strategy integrates this component-level optimization directly into the search for the system's architecture itself. Under this approach, node characteristics become tunable parameters in a larger search space. For instance, frameworks can embed prompt engineering directly into the search loop, allowing the system to discover not just the optimal workflow but also the most effective instruction for each agent simultaneously [63]. Similarly, EvoFlow [62] uses evolutionary algorithms to construct heterogeneous workflows by selecting the most suitable LLM for each task from a diverse pool. This holistic strategy enables the discovery of systems that are co-optimized for both their structure and individual agent capabilities, effectively balancing metrics like overall performance and cost [170].

**Autonomous-Agent Optimization** Building upon the optimization of individual LLM-invoking nodes, a more profound level of self-improvement targets the autonomous agent as a holistic entity. This evolution proceeds along two main fronts: optimizing the agent's high-level architectural design and enabling the agent to directly modify its own source code. The first approach focuses on discovering the optimal agent structure. AgentSquare [54] exemplifies this by defining a modular design space of components like planners and memory modules, then using an evolutionary algorithm to find the most effective combination for a given task. The second front involves agents that dynamically rewrite their own operational code. This is seen in radical systems like the Darwin Gödel Machine [55], which recursively modifies its own Python codebase, and AlphaEvolve [61], which uses evolutionary coding to improve specific algorithms. Similarly, Gödel Agent [4] provides a self-referential framework for agents to analyze and alter their logic. Together, these two directions (optimizing the agent's architectural "blueprint" and its functional code) demonstrate a key trend toward turning the agent's fundamental structure and logic into learnable components.

#### 3.4.2 Multi-Agent System Optimization

How agents are organized and communicate within a system (its topology) fundamentally determines its capacity for solving complex problems. The field has evolved from using fixed, human-designed communication structures to creating dynamic systems that automatically adapt their organization to a given task, allowing them to discover and exploit the most effective collaboration patterns. This evolution is explored along two major fronts: the optimization of static, explicit workflows and the co-evolution of dynamic, internal policies.

**Agentic Workflow Optimization** The optimization of agentic workflows focuses on finding the most effective, often static, structure of communication and task delegation for a given problem. Early research established important foundations, with studies like AutoFlow [66] demonstrating the automated creation of linear workflows from natural language, and GPTSwarm [67] proposing a unifying graph-based framework. Concurrently, other foundational work explored how agents could evolve by using symbolic learning to distill their interaction experiences into an explicit, interpretable set of logical rules to guide future decisions [171]. This abstraction of systems into tunable components—whether nodes, edges, or symbolic rules—was crucial. However, these early systems often lacked a formal method for efficiently navigating the vast space of possible configurations and interactions.

The major breakthrough came when ADAS [65] and AFlow [64] formally defined this challenge as a search and optimization problem. ADAS set a theoretical vision by framing system design as a search through a Turing-complete space of code-based configurations. Building on this, AFlow made it practical by introducing reusable operators that

represent common agentic patterns and by employing Monte Carlo Tree Search (MCTS) to efficiently navigate the enormous design space. Together, these works established a core methodology for treating agent system design as a tractable optimization problem, proving that automatically discovered workflows could outperform human-designed ones.

Following this formalization, research rapidly diversified toward creating customized agent systems for each specific query. Two primary strategies emerged: search-based and learning-based generation. Search-based methods, such as MaAS [172], create a "supernet" of potential architectures and then sample a specialized system from it. In parallel, learning-based methods train models to directly generate effective topologies. ScoreFlow [68], for instance, trains a generator using a novel preference optimization method, while FlowReasoner [69] uses reinforcement learning to train a meta-agent that constructs a bespoke workflow on the fly. This line of query-specific generation continues to be an active area of research [173, 159]. Furthermore, it is important to note that this process is not limited to the topology alone; many of these frameworks also perform node-level optimization in tandem, such as co-optimizing prompts or selecting heterogeneous models as an integral part of the architectural generation process [64, 63, 62].

A key challenge for all search and learning methods is the computational cost of evaluating each potential workflow [54]. To address this, researchers have developed lightweight prediction models. Agentic Predictor [174] is a prime example, training a model to accurately estimate a workflow's performance based on its structural and semantic features without a full execution. By providing a fast and inexpensive evaluation proxy, these predictors significantly accelerate the optimization process, making the exploration of vast design spaces feasible [175].

**Multi-Autonomous-Agent Optimization** Distinct from optimizing a system's explicit workflow structure, this line of research focuses on how multiple autonomous agents can co-evolve their internal behavioral policies through interaction. This approach enables emergent capabilities like coordination, task delegation, and beneficial competition. For instance, ReMA [70] uses multi-agent reinforcement learning (MARL) to collaboratively train a high-level meta-thinker and a low-level executor, significantly improving performance on reasoning benchmarks. Building on this, GiGPO [71] enhances MARL training by aggregating trajectories to provide more precise credit assignment, boosting success rates on long-horizon tasks. To support this direction, platforms like MARTI [176] provide open-source infrastructure for orchestrating and scaling the training of these language-model collectives. Collectively, these studies underscore multi-agent reinforcement learning as a promising route for cultivating group-level competencies unattainable by individual agents alone.

## 4 When to Evolve

The temporal dimension of self-evolution in LLM-based agents mainly concerns the relationship between learning processes and task execution. Therefore, the second key aspect of a self-evolving agent is identifying the *evolving timing*, i.e., at which stage the self-evolving strategy  $f$  is invoked and applied to the agent system. To this end, we propose a taxonomy that distinguishes between two temporal modes of self-evolution: Intra-test-time self-evolution and inter-test-time self-evolution.

**Intra-test-time self-evolution** refers to adaptive processes that occur during task execution, where agents recognize their limitations on a specific problem and initiate targeted learning mechanisms to enhance their capabilities in real-time [177, 178]. This mode of evolution is characterized by its immediate coupling with the task at hand: the agent improves its problem-solving abilities for a specific problem encountered, creating a dynamic interplay between performance and adaptation.

**Inter-test-time self-evolution** refers to learning processes that occur between task completions, leveraging accumulated experiences to improve future performance. This category encompasses diverse methodological approaches: offline learning paradigms that extract knowledge from pre-collected datasets through iterative refinement [79, 80], and online learning paradigms that continuously adapt based on streaming interaction data [84, 43, 179, 117].

The implementation of self-evolution across these temporal phases leverages three fundamental learning paradigms in LLMs: in-context learning (ICL) [180, 181, 182], which adapts behavior through contextual examples without modifying parameters; supervised fine-tuning (SFT), which updates model weights through gradient-based optimization on labeled data [183, 184, 185]; and reinforcement learning (RL), which shapes behavior through reward-driven policy optimization [186, 187, 188]. While these learning paradigms remain conceptually consistent across temporal contexts, their instantiation differs in terms of data availability and learning objectives:

Intra-test-time is characterized by its online nature: learning data emerges dynamically during task execution, with optimization directly targeting performance enhancement on the immediate problem instance. This real-time coupling necessitates rapid adaptation mechanisms that can process learning data and feedback signals and modify behavior

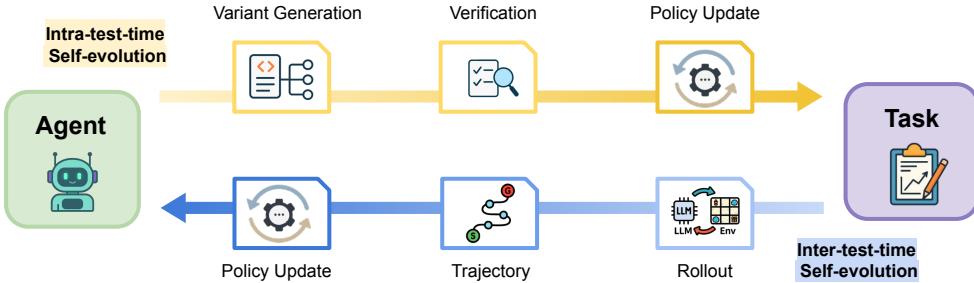


Figure 5: An overview of when to evolve. The top pathway illustrates intra-test-time self-evolution, where adaptation (e.g., variant generation, verification, and policy update) occurs within task execution. The bottom pathway depicts inter-test-time self-evolution, where learning happens retrospectively through rollout, trajectory analysis, and policy updates.

within the temporal constraints of active task-solving. On the other hand, inter-test-time is characterized by its retrospective nature: learning algorithms operate on historical data, whether from curated datasets or accumulated behavioral trajectories, with optimization objectives oriented toward improving expected performance across the task distribution rather than maximizing success on any specific problem instance. This temporal decoupling enables more sophisticated learning procedures that can identify cross-task patterns, consolidate diverse experiences, and develop generalizable capabilities without the immediacy constraints of active task execution.

#### 4.1 Intra-test-Time Self-Evolution

In intra-test-time self-evolution, agents engage in self-improvement processes that are intrinsically coupled with solving the immediate task at hand. The distinguishing characteristic of this temporal phase is its synchronous nature: feedback signals are generated and processed during task execution, with optimization objectives specifically targeted at improving performance on the current problem instance rather than generalizing to future tasks. Here, we introduce how the three learning paradigms are realized in this temporal phase.

**In-Context Learning** Intra-test-time ICL methods leverage the model’s context window as a dynamic memory system for immediate adaptation without parameter modification. These approaches typically employ self-reflective mechanisms where agents analyze their own performance, generate verbal critiques or insights, and maintain these reflections in episodic memory buffers to guide subsequent decisions within the same task context [17, 72]. Some methods extend beyond simple reflection to include dynamic planning revision, where agents can modify their entire approach based on environmental feedback, switching between action execution and plan modification as needed. For instance, AdaPlanner [18] decomposes tasks into manageable sub-goals and predicts environmental feedback for each. During execution, its refiner component distinguishes between in-plan feedback (observations aligning with predictions) and out-of-plan feedback (deviating observations). For in-plan feedback, the refiner dynamically queries the LLM through a specialized `ask_LLM()` action to parse observations and extract pertinent information. For out-of-plan feedback, the refiner proactively revises the entire plan and resumes solving from an intermediate point, rather than restarting from scratch. This adaptive closed-loop framework eliminates the need for prior knowledge about feedback structures and enables more efficient decision-making. Similarly, TrustAgent [73] employs rule-based plan revision during execution, modifying its approach based on language feedback to evolve toward safer planning strategies. These ICL methods demonstrate how test-time adaptation can achieve sophisticated behavioral modification without permanent model changes, maintaining flexibility while preserving the model’s general capabilities.

**Supervised Fine-Tuning.** Intra-test-time SFT represents a paradigm shift where models perform immediate self-modification through learned meta-adaptation strategies. Self-adaptive language modeling [74] exemplifies this approach by generating “self-edits”, which are meta-level instructions that can restructure information representations, specify optimization hyperparameters, or invoke tools for data augmentation and gradient computation. These self-edits trigger immediate supervised fine-tuning, resulting in persistent weight updates that adapt the model to the current task. The key innovation lies in the meta-learning phase, where reinforcement learning trains models to produce effective self-edits by using the downstream performance of the updated model as the reward signal, essentially teaching models how to teach themselves.

**Reinforcement Learning.** Intra-test-time RL enables models to develop new capabilities on-demand when encountering problems beyond their current competence. LADDER [77] demonstrates this through its test-time reinforcement learning (TTRL) mechanism: upon identifying a particularly challenging problem, the system generates a focused set of related problem variants and conducts intensive, targeted reinforcement learning specifically for that problem class. This approach transforms insurmountable challenges into learning opportunities, allowing models to expand their problem-solving repertoire during deployment rather than failing or providing suboptimal solutions. The method represents a form of just-in-time skill acquisition, where computational resources are invested precisely when and where they are needed most.

## 4.2 Inter-Test-Time Self-Evolution

Inter-test-time self-evolution represents the predominant learning process in autonomous agents, wherein adaptation occurs following task execution rather than during it. In this temporal mode, agents complete a given task, extract feedback signals, including explicit rewards [189], gradients [190, 191], and performance metrics [192], and subsequently leverage this information to enhance their capabilities for future problem-solving. This retrospective learning process decouples task performance from capability improvement, allowing agents to consolidate experiences, identify patterns of success and failure, and systematically refine their behavioral policies without the computational constraints imposed by real-time task demands.

**In-Context Learning.** Inter-test-time in-context learning has emerged as a widely adopted approach for agent self-improvement. This paradigm leverages execution results and feedback from previous tasks as contextual information for future problem-solving. Wang et al. [29] demonstrate this principle by inducing workflows from agent action histories and incorporating them into the context for subsequent tasks. The field of in-context reinforcement learning (ICRL) [193, 194, 195] extends this concept by maintaining histories of observations and actions within the agent’s context window. These methods exploit the hypothesis that pre-trained neural networks can implement implicit reinforcement learning algorithms within their forward pass, processing contextual information to adapt behavior without parameter updates [196]. A defining characteristic of ICRL is in-context improvement: the phenomenon whereby agent performance progressively enhances as task-relevant information accumulates in the context, enabling sophisticated adaptation through attention mechanisms rather than gradient-based learning.

**Supervised Fine-Tuning.** Inter-test-time SFT [82] methods establish a paradigm of iterative self-improvement through synthetic data generation and self-evaluation. SELF [10] pioneered meta-cognitive training, where models first acquire self-feedback and self-refinement capabilities, then iteratively generate responses to unlabeled instructions and enhance them through self-critique. STaR [79] and Quiet-STaR [80] focus on reasoning improvement through rationalization—models attempt problems, then generate explanations for correct answers they initially failed to solve, creating augmented training data that combines successful attempts with post-hoc reasoning. SiriusS [81] extends this to sequential problem-solving, maintaining repositories of correct solutions while augmenting failures through multi-stage refinement involving feedback incorporation, regeneration, and rephrasing. These methods share a core insight: models can bootstrap their own improvement by learning to evaluate and enhance their outputs, creating high-quality training signals from initially imperfect attempts without extensive human supervision.

**Reinforcement Learning.** Inter-test-time RL leverages unconstrained computational resources to optimize agents through extensive environmental interaction and sophisticated curriculum design. RAGEN [22] and DYSTIL [23] employ online reinforcement learning for multi-turn interactive tasks, continuously refining policies through on-policy learning in simulated dialogues. Learning Like Humans [83] introduces cognitive-inspired training with adaptive difficulty progression, combining on-policy exploration with off-policy efficiency and expert demonstrations to accelerate learning. Domain-specific applications demonstrate the versatility of inter-test-time RL: WebRL [84] develops web navigation agents through self-evolving curricula that automatically adjust task complexity based on performance, while DigiRL [85] enables device-control agents to master in-the-wild interactions through autonomous reinforcement learning. These approaches exploit the pre-deployment phase to engage in extensive trial-and-error learning, developing robust policies through thousands of interactions that would be impractical during real-time deployment.

## 5 How to Evolve

The pursuit of self-evolution lies at the heart of building advanced, autonomous, and increasingly general artificial intelligence. For large language models (LLMs) and their agentic extensions, the question of how to continually, autonomously, and efficiently evolve their capabilities has become a central challenge. Therefore, the third key aspect

Table 3: Overview of Reward-based, Imitation/Demonstration, and Population-based Learning Methods for Self-Evolving Agents. This table categorizes key approaches based on the following criteria: (1) Feedback Type: the type of feedback used, including language-based rationales and numerical rewards. (2) Feedback Source: the origin of the feedback, either internal (model-generated) or external (provided externally). (3) Learning Method: the learning paradigm applied, such as in-context learning (ICL), supervised fine-tuning (SFT), reinforcement learning (RL), and evolutionary algorithms; (4) Updated Components: which parts of the model are updated, either full parameters or a subset of the model. (5) Update Timing: the stage during the agent’s evolution when updates are applied, such as pre-training, pre-test, or test-time.

Method	Feedback Type	Feedback Source	Learning Method	Updated Components	Update Timing
<i>Reward-based Evolution Methods</i>					
Reflexion [17]	language	internal	ICL	context	test-time
AdaPlanner [18]	language	external + internal	ICL	context	test-time
AgentS2 [86]	language	external	ICL	context	test-time
SELF [10]	language	external + internal	SFT	full params	pre-test time + test-time
SELF-REFINE [72]	language	internal	ICL	context	test-time
SCoRe [11]	numerical	external	RL	full params	pre-test time
PAG [12]	numerical	external	RL	full params	pre-test time
TextGrad [13]	language	external	ICL	context	pre-test time / test-time
SRSI [9]	language	internal	RL	full params	pre-test time
Self-Train LM [91]	numerical	internal	RL	full params	pre-test time
MM-UPt [92]	numerical	internal	RL	full params	pre-test time
CoVo [93]	numerical	internal	RL	full params	pre-test time
SWE-agent [94]	language	external	ICL	context	test-time
SICA [95]	numerical	external	ICL	codebase(tools, workflows, prompts)	test-time
Feedback Friction [96]	language	external	ICL	context	test-time
USEagent [97]	language	external	ICL	context	test-time
DYSTIL [23]	language + numerical	external + internal	SFT+RL	full params	pre-test time + test-time
OTC-PO [98]	numerical	external	RL	full params	pre-test time
AUTORULE [14]	language + numerical	external + internal	RL	full params	pre-test time
EGSR [83]	numerical	external	RL	full params	pre-test time
LADDER [77]	numerical	external	RL	full params	pre-test time
RAGEN [22]	numerical	external	RL	full params	test-time
SPIRAL [99]	numerical	internal	RL	full params	pre-test time
ICRL Prompting [100]	numerical	external + internal	RL	full params	test-time
MATH-SHEPHERD [197]	numerical	external	RL	full params	pre-test time
AgentPRM [198]	numerical	external	SFT+RL	full params	pre-test time
Agent Q [199]	numerical	external	RL	full params	pre-test time
GiGPO [200]	numerical	external	RL	full params	pre-test time
SPA-RL [201]	numerical	external	RL	full params	pre-test time
Self-Instruct [202]	language	internal	SFT	full params	pre-test time
WizardLM [203]	language	internal	SFT	full params	pre-test time
OS-Genesis [204]	numerical	external	SFT	full params	pre-test time
UI-Genie [120]	numerical	external	SFT	partial params	pre-test time
GUI-R1 [205]	numerical	external	SFT+RL	full params	pre-test time
InfiGUI-R1 [206]	numerical	external	SFT+RL	full params	pre-test time
Voyager [42]	language	external	ICL	context	test-time
SwiftSage [207]	language	external	ICL	context	test-time
AutoWebGLM [208]	language	external	SFT+RL	full params	pre-test time
DigiRL [85]	language	external	RL	partial params	pre-test time
WebRL [84]	language	external	SFT+RL	full params	pre-test time
Let’s Verify Step-by-Step [209]	language	external	SFT	full params	pre-test time
AlphaMath [210]	numerical	external	SFT	full params	pre-test time
rStar-Math [211]	numerical	external	SFT	full params	pre-test time
DistRL [212]	language	external	RL	full params	pre-test time
MobileGUI-RL [213]	language	external	RL	full params	pre-test time
<i>Imitation and Demonstration Learning Methods</i>					
STaR [79]	language + numerical	internal	SFT	full params	pre-test time
V-STaR [102]	numerical	external + internal	SFT + RL	partial params	pre-test time
AdaSTaR [103]	numerical	internal	SFT	full params	pre-test time
STIC [104]	language	internal	RL + SFT	partial params	pre-test time
GENIXER [105]	language	external	SFT	full params	pre-training
SiriuS [81]	language + numerical	internal	SFT	full params	pre-test time
SOFT [106]	language	internal	SFT	not specified	pre-test time
RISE [107]	language + numerical	internal + external	SFT	full params	pre-test time
IoE [108]	numerical	internal	/	/	test-time
<i>Population-based and Evolutionary Methods</i>					
DGM [55]	numerical	external	ICL	codebase (tools, workflows, prompts)	test-time
EvoMAC [113]	language	external	ICL	team composition, workflow, prompts	test-time
SPIN [110]	language	internal	RL	full params	pre-test time
GENOME [109]	numerical	external	Evolution Alg.	partial params	pre-test time
SPC [111]	numerical	internal		critic params	pre-test time + test-time
Puppeteer [114]	numerical	external		planner policy	pre-test time / between tasks
MedAgentSim [116]	language	external		context (knowledge base)	test-time
STL [112]	language + numerical	internal	SFT	value model	pre-test time
MDTeamGPT [115]	language	external	ICL	context (knowledge base)	test-time

of a self-evolving agent is to instantiate an effective *evolving strategy*  $f$ , i.e., how to transform an agent system  $\Pi = (\Gamma, \{\psi_i\}, \{C_i\}, \{\mathcal{W}_i\})$  to its new state  $\Pi' = (\Gamma', \{\psi'_i\}, \{C'_i\}, \{\mathcal{W}'_i\})$ . Unlike traditional approaches that rely



Figure 6: Overview of reward-based self-evolution strategies, categorized into textual, implicit, internal, and external rewards, each associated with distinct feedback sources and mechanisms.

on static datasets or one-time supervised fine-tuning, self-evolution emphasizes an ongoing process where models learn from real-world interactions, actively seek feedback, self-reflect, generate or curate new data, and adapt their strategies in response to dynamic environments. This continuous evolution is not merely a matter of scaling up data or computation; it requires the agent to acquire a spectrum of meta-capabilities, including self-correction, autonomous data generation, knowledge transfer, and multi-agent collaboration. As a result, the landscape of self-evolution has become increasingly rich and multi-faceted, with each methodological branch exploring different axes of feedback, learning paradigms, data sources, and evolutionary scales.

This chapter aims to systematically map and analyze the major families of self-evolution methods, providing a unified framework for understanding their principles, mechanisms, and interactions. We begin with **reward-based evolution**, which centers on the design of reward signals—ranging from natural language feedback and internal confidence metrics to external or implicit signals—to guide iterative self-improvement. Next, we examine **imitation and demonstration learning**, where agents improve by learning from high-quality exemplars, either self-generated or provided by other agents or external sources. This paradigm is particularly powerful when demonstrations are abundant or can be autonomously synthesized, and it has driven significant progress in both reasoning and multimodal domains. Finally, we introduce **population-based and evolutionary methods**, which draw inspiration from biological evolution and collective intelligence. These approaches maintain populations of agent variants or collaborating agents, leveraging mechanisms such as selection, mutation, crossover, and competition to explore the solution space in parallel, foster diversity, and enable the emergence of novel strategies or architectural innovations.

## 5.1 Reward-based Self-Evolution

The capacity for self-improvement is a cornerstone of advanced intelligence. In the context of Large Language Models (LLMs), this manifests as a dynamic process of reward-driven evolution, where models iteratively learn from their own outputs and interactions to refine their capabilities. The design of the reward signal, which serves as the guiding feedback, is crucial; it determines the nature, efficiency, and effectiveness of the learning process. In this section, we systematically review the main methodologies for reward design, categorized by the nature of the feedback: textual feedback, internal confidence, external rewards, and implicit rewards.

**Textual Feedback** Textual Feedback leverages the native modality of LLMs—natural language—to provide detailed, interpretable instructions for refinement. Unlike scalar rewards, textual feedback encapsulates nuanced critiques and actionable suggestions. Recent frameworks such as Reflexion [17], AdaPlanner [18], AgentS2 [86], SELF [10], Self-Refine [72], SCoRe [11], PAG [12], and TextGrad [13] exemplify this direction. For instance, Reflexion proposes “verbal reinforcement learning,” where agents reflect in natural language on their past trials, storing these reflections as episodic memory to guide future decisions. AdaPlanner enables closed-loop adaptive planning by allowing LLM agents to revise their plans based on both in-plan and out-of-plan feedback, while also mitigating hallucination via code-style prompts and leveraging skill discovery. Self-Refine and SELF further explore iterative self-feedback and self-correction, demonstrating that even state-of-the-art models can be improved via multi-turn, language-based self-critique, without additional supervised data or external reinforcement. Such frameworks highlight the power of language as a reward channel, enabling nuanced, flexible, and sample-efficient self-improvement.

**Internal Rewards** Internal Confidence-based rewards move away from external signals and instead exploit internal metrics such as the model’s probability estimates or certainty. This paradigm leverages the model’s intrinsic understanding to guide improvement without relying on external supervision. Methods such as Confidence-Informed Self-Consistency (CISC) [87], Self-Ensemble [88], Self-Rewarding Self-Improving [9], scalable best-of-N selection

via self-certainty [89], and Self-Rewarding Language Models [90] allow models to self-evaluate and calibrate their responses based on internal confidence metrics. For example, CISC weights reasoning paths by confidence scores to improve both accuracy and computational efficiency, effectively filtering high-quality solutions from multiple candidates. Self-Ensemble mitigates confidence distortion by dividing choices into smaller, more manageable groups and aggregating predictions to reduce overconfidence bias. Self-Rewarding Language Models demonstrate that models can act as their own reward function, generating training data through self-instruction and self-evaluation cycles. These approaches can reduce reliance on human labels and external evaluators, enabling scalable and autonomous self-improvement loops that can operate continuously without human intervention.

**External Rewards** External Rewards are derived from sources outside the model, such as the environment, majority voting, or explicit rules. Majority voting [91, 92, 93] uses consensus among multiple model outputs as a proxy for correctness, providing a self-generated but grounded reward signal. Environment feedback, including tool-based signals, is central to agentic LLM research (e.g., SWE-Dev [94], SICA [95], Feedback Friction [96], USEAgent [97], DYSTIL [23]), where agents learn through direct interaction with real-world environments and tools. Rule-based rewards [98, 14, 83, 77, 22, 99] use explicit constraints or logical rules as verifiable signals, particularly effective in the domains of mathematical reasoning, game play, and structured problem solving. These methods offer objective, reliable supervision but may require significant engineering or be limited in expressiveness.

**Implicit Rewards** Implicit Reward frameworks hypothesize that LLMs can learn from feedback signals even when not explicitly labeled as rewards. For instance, “Reward Is Enough” [100] demonstrates that LLMs can perform in-context reinforcement learning using simple scalar signals embedded in the context window, improving their responses over rounds without explicit RL fine-tuning or supervision. This reveals an inherent capacity for models to interpret and learn from implicit feedback cues present in their input context. Recent work has expanded this concept by showing that LLMs inherently encode reward-like signals through their standard training objectives. Endogenous reward [101] reveal that standard next-token prediction implicitly learns a generalist reward function, which can be extracted from model logits without additional training. Moreover, ImPlicit Self-ImprovementT (PIT) framework [214] implicitly learns the improvement goal from human preference data without extra human efforts by maximizing the quality gap of the response conditioned on a reference response. Unlike rule-based or environment-derived external rewards, implicit reward methods offer unique advantages by discovering and utilizing reward signals that are inherently present in language modeling.

## 5.2 Imitation and Demonstration Learning

Imitation and demonstration learning is a paradigm in which self-evolving agents improve their capabilities by learning from high-quality exemplars, which may be generated by the agents themselves, other agents, or external sources. Unlike reward-based methods that rely on explicit reward signals, imitation-based approaches focus on reproducing and refining successful behavioral patterns through iterative self-training and bootstrapping mechanisms. This approach is particularly effective when high-quality demonstrations are available or can be autonomously generated, allowing agents to bootstrap their capabilities with minimal external supervision.

### 5.2.1 Self-Generated Demonstration Learning

Self-generated demonstration learning involves agents creating their own training data through iterative refinement processes, where the models learn to improve by generating and selecting high-quality examples from their own outputs.

**Bootstrapping Reasoning Capabilities.** [79] introduces the foundational framework for self-generated demonstration learning, enabling language models to bootstrap their reasoning capabilities through iterative self-training. This process involves generating reasoning chains for problems, fine-tuning on correct solutions, and repeating this cycle to progressively improve performance without the need for ground-truth reasoning paths. Building on this framework, recent advancements have refined the bootstrapping process through more sophisticated training strategies. For instance, [102] proposes a verifier-guided self-training approach, where separate verifier models assess the quality of generated reasoning chains before they are incorporated into the training data, enhancing the reliability of self-improvement. Additionally, [103] introduces adaptive data sampling strategies that dynamically adjust the composition of training data based on model performance across various reasoning tasks, thereby mitigating overfitting to specific problem types.

**Multimodal Self-Training.** Extending self-training to multimodal domains presents unique challenges in generating high-quality demonstrations that span both visual and textual modalities. [104] demonstrates how vision-language models can improve iteratively by training on their own generated image descriptions and visual reasoning chains. The approach leverages the model’s existing visual understanding to generate detailed image descriptions, which are subsequently used to fine-tune the model’s visual perception in a bootstrapping manner. [105] builds on this concept

by empowering multimodal large language models to serve as powerful data generators, producing diverse training examples across different modalities and tasks through advanced prompt engineering and quality filtering mechanisms.

### 5.2.2 Cross-Agent Demonstration Learning

Cross-agent demonstration learning involves agents learning from demonstrations provided by other agents, either within the same system or from external sources, enabling knowledge transfer and collaborative improvement.

**Multi-Agent Bootstrapped Reasoning.** [81] presents a framework for multi-agent systems to learn from each other's successful demonstrations through bootstrapped reasoning. The system maintains an experience library containing successful interaction trajectories generated by different agents, facilitating efficient knowledge sharing and collaborative improvement. Each agent can leverage the collective experience of the entire system, thereby accelerating the learning process and enabling the discovery of diverse solution strategies. This framework illustrates how agents can specialize in different aspects of complex tasks while benefiting from the accumulated knowledge of the entire system.

**Domain-Specific Demonstration Learning.** Domain-specific applications of demonstration learning have proven especially effective in specialized fields where expert knowledge can be effectively transferred through demonstrations. In recommendation systems, techniques such as self-optimized fine-tuning [106] enable LLM-based recommender systems to learn from their own successful recommendation patterns, creating a feedback loop that enhances personalization over time. The system generates high-quality recommendation demonstrations from successful user interactions and uses these to fine-tune the underlying language model, ultimately leading to more accurate and personalized recommendations.

### 5.2.3 Hybrid Demonstration Learning

Hybrid demonstration learning combines both self-generated and external demonstrations to create more robust and diverse training regimens that leverage the strengths of each approach.

**Recursive Self-Improvement.** [107] demonstrates how agents can be trained to systematically improve their behavior through structured self-reflection and demonstration generation. This approach enables language model agents to introspect on their reasoning processes, identify areas for improvement, and generate corrective demonstrations to address these weaknesses. This recursive process establishes a continuous improvement loop, where agents become increasingly skilled at self-diagnosis and self-correction, leading to more robust and adaptable behavior.

**Confidence-Guided Demonstration Selection.** Recent developments have focused on more sophisticated mechanisms for selecting high-quality demonstrations from both self-generated and external sources. Confidence-based approaches [108] utilize the model's uncertainty estimates to determine which demonstrations are most likely to contribute positively to learning, filtering out potentially detrimental or low-quality examples. This method addresses a critical challenge in demonstration learning: poor-quality demonstrations can degrade performance. By ensuring that only high-confidence, high-quality examples are used for training, this approach helps to maintain the integrity of the learning process.

The effectiveness of imitation and demonstration learning approaches is highly dependent on the quality and diversity of the available demonstrations. While these methods can yield impressive results when high-quality exemplars are present, they face challenges in domains where good demonstrations are scarce or where the optimal behavior is not well-represented in the available data. Future research directions include developing more sophisticated demonstration selection and generation strategies, improving the robustness of learning from imperfect demonstrations, and creating better mechanisms for combining demonstrations from multiple sources.

## 5.3 Population-based and Evolutionary Methods

Population-based and evolutionary methods represent a fundamentally different paradigm for agent evolution compared to the reward-based and imitation-based approaches discussed in previous sections. While reward-based methods typically optimize individual agents through iterative reward signals and imitation learning relies on learning from demonstrations, population-based methods draw inspiration from biological evolution and collective intelligence. These approaches maintain multiple agent variants simultaneously, allowing for parallel exploration of the solution space and the emergence of diverse capabilities through mechanisms such as selection, mutation, crossover, and competitive interaction [109]. This enables broader search coverage and the discovery of novel solutions that might be missed by gradient-based optimization. This approach is particularly valuable when the solution space is complex, multimodal, or when the optimal strategy requires fundamental architectural changes rather than parameter fine-tuning.

### 5.3.1 Single Agent Evolution

Single-agent evolutionary approaches focus on evolving individual agents through population-based mechanisms, where multiple variants of an agent compete and evolve over time. These methods can be broadly categorized into two main paradigms: learning from evolution and self-play from multiple rollouts.

**Learning from Evolution.** This paradigm draws directly from biological evolution, maintaining populations of agent variants and applying evolutionary operators to discover improved capabilities. The Darwin Gödel Machine (DGM) [55] exemplifies this approach through open-ended evolution of self-improving agents that maintain an archive of all historical versions, enabling branching from any past "species" rather than linear optimization. The system achieves self-referential improvement by allowing agents to directly modify their own Python codebase, with evolution driven by empirical performance on coding benchmarks and parent selection balancing performance scores with novelty rewards for diverse exploration. Complementing this code-level evolution, the Nature-Inspired Population-Based Evolution (GENOME) framework [109] directly applies genetic algorithms to language model parameter evolution, maintaining populations and using crossover, mutation, and selection operators on model weights. GENOME+ extends this with particle swarm optimization concepts, adding inheritance mechanisms and ensemble methods that demonstrate gradient-free evolutionary optimization can effectively improve model capabilities through parameter space exploration.

**Self-Play from Multiple Rollouts.** This paradigm focuses on agents improving through iterative self-competition and rollout-based learning, where agents generate multiple trajectories and learn from their own exploration. Self-Play Fine-Tuning (SPIN) [110] establishes the foundation by having current models compete against previous versions, creating evolutionary pressure where only improving strategies survive without external annotations. SPC [111] advances this through sophisticated adversarial co-evolution, where a "sneaky generator" learns to create deceptive errors while a "step critic" evolves to detect increasingly subtle mistakes, using automated validation to sustain improvement without human step-level annotations. STL [112] demonstrates self-teaching evolution through iterative lookahead search, where value models generate training data from their own exploratory rollouts, combining numerical value learning with natural language reasoning chains to bootstrap continuous improvement. These approaches share the principle of using agents' own generated experiences as learning signals, creating self-sustaining improvement cycles that evolve without external supervision.

### 5.3.2 Multi-Agent Evolution

Multi-agent evolutionary methods extend population-based approaches to evolving entire teams or networks of agents, focusing on optimizing collective behavior, coordination strategies, and collaborative architectures. These approaches can be categorized into two main paradigms based on their evolution mechanisms: System Architecture Evolution and Knowledge-Based Evolution.

**System Architecture Evolution.** This paradigm focuses on evolving the structural and coordination aspects of multi-agent systems, including team composition, orchestration strategies, and workflow optimization. EvoMAC [113] introduces a framework that mimics neural network training for multi-agent systems, implementing "textual backpropagation" where compilation errors and test failures serve as loss signals to drive iterative modifications of agent team composition and individual prompts. A specialized "updating team" analyzes textual feedback to identify problematic agents and generate modification instructions, effectively implementing gradient-based optimization in the space of agent configurations rather than model parameters. Building on this structural evolution concept, Puppeteer [114] takes a different approach by focusing on coordination strategy evolution rather than team composition changes. The system employs a centralized orchestrator that evolves its decision policy through reinforcement learning, dynamically selecting which agents to activate at each step while balancing task performance with computational cost. This "puppeteer-puppet" paradigm demonstrates how architectural evolution can occur at the coordination level, discovering efficient collaboration patterns and emergent behaviors such as tighter coordination among core agents and sophisticated cyclic interaction patterns.

**Knowledge-Based Evolution.** This paradigm emphasizes evolving the collective knowledge and experience of multi-agent teams through memory accumulation and case-based learning, primarily operating through in-context learning rather than parameter updates. MDTeamGPT [115] establishes the foundation for this approach through a dual knowledge base system, implementing CorrectKB for storing successful cases and ChainKB for capturing failure reflections, enabling the system to learn from both successes and mistakes through structured case retrieval and reasoning enhancement. Extending this medical consultation framework, MedAgentSim [116] demonstrates how such knowledge-based evolution can be applied to real-world diagnostic scenarios, accumulating experience from patient interactions and using retrieval-augmented generation to improve consultation quality over time.

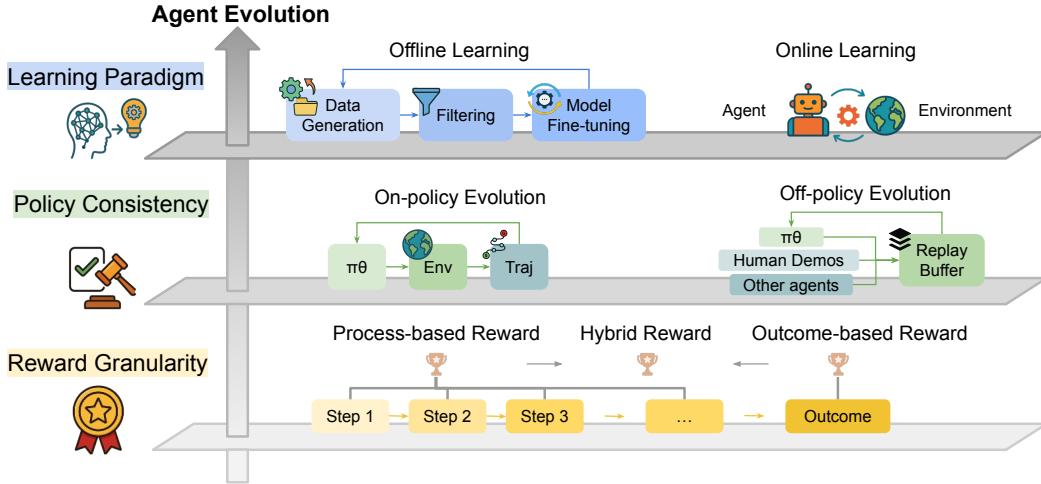


Figure 7: Illustration of cross-cutting evolutionary dimensions in agent self-evolution, structured along three key axes: learning paradigm (offline/online), policy consistency (on/off-policy), and reward granularity (process-based, outcome-based, and hybrid). These dimensions jointly characterize how autonomous agents generate data, interact with environments, adapt policies, and receive feedback, providing a structured lens for analyzing reward-based, imitation-based, and population-based evolution strategies.

Table 4: Comparison of self-evolution method families along key dimensions.

Dimension	Reward-based	Imitation/Demonstration	Population-based
<b>Feedback Type</b>	Scalar reward, natural language, confidence, external signals	Demonstration trajectories, exemplars, rationales	Fitness scores, task success, competitive signals
<b>Data Source</b>	Self-generated, environment, external rules	Self-generated or other agents, humans	Population generations, multi-agent systems
<b>Reward Granularity</b>	Outcome/process/hybrid (flexible)	Usually outcome/process (via demo steps)	Often outcome-level, sometimes process via competition
<b>Online/Offline</b>	Both (reward learning, RL, DPO, SFT)	Typically offline, sometimes online demo mining	Online evolution or batch population updates
<b>On/Off-policy</b>	Both (DPO, Reflexion, GRPO)	Primarily off-policy, but online variants can be on-policy	Off-policy (population); self-play is on-policy
<b>Sample Efficiency</b>	Moderate (depends on reward sparsity)	High (if demo quality is high)	Usually low (needs many trials)
<b>Stability</b>	Sensitive to reward design	Sensitive to demo quality/diversity	Sensitive to population size/diversity
<b>Scalability</b>	Good with automation	Limited by demo collection	High but resource-intensive

#### 5.4 Cross-cutting Evolutionary Dimensions

Agent self-evolution is a multifaceted process characterized by a number of cross-cutting dimensions that shape how agents learn, adapt, and improve over time. Beyond any single learning algorithm or supervision signal, these dimensions define the core principles underlying the design and analysis of autonomous agents. In this section, we systematically compare the major families of self-evolution methods—reward-based, imitation/demonstration-based, and population-based—along several key axes, such as learning paradigm (online vs. offline), policy consistency (on-policy vs. off-policy), and reward granularity (process-based, outcome-based, or hybrid). We further highlight additional dimensions, including feedback types, data sources, sample efficiency, stability, and scalability, as summarized in Table 4. This comprehensive comparison provides a unified perspective for understanding the strengths, limitations, and design trade-offs inherent in different approaches to agent evolution.

#### 5.4.1 Online and Offline Learning

Another fundamental dimension in the design of self-evolving agents is the learning paradigm, which can be broadly categorized as either offline or online. This distinction depends on whether the agent’s evolutionary updates are performed on a static, pre-collected dataset of experiences (offline) or through continuous, direct interaction with a live environment (online).

**Offline Learning** In the offline learning paradigm, the learning phase is decoupled from live task execution. The offline process typically involves cycles of offline data generation, filtering, and model fine-tuning, focusing on building a powerful and generalist foundational model before deployment. A primary strategy in this domain is LLM bootstrapping, where a model enhances its own capabilities using its self-generated content. For example, Self-Instruct [202] shows how a language model can bootstrap its own instruction-following ability by generating new instructions, paired with its own responses, creating a synthetic dataset for fine-tuning. Building on this, WizardLM [203] demonstrates how to progressively evolve the complexity of these self-generated instructions, pushing the model’s capabilities on more challenging tasks. In the context of GUI and Web agents, offline learning often involves leveraging pre-collected high-quality trajectories for supervised fine-tuning (SFT). OS-Genesis [204] introduced a reverse task synthesis method for automatic trajectory creation. Similarly, UI-Genie [120] employs a unified reward model for trajectory evaluation and a self-improving loop to generate high-quality trajectories iteratively. Both approaches focus on curating a rich SFT dataset to enhance the agent’s capabilities to solve complex tasks. Beyond SFT, offline methods also incorporate reinforcement learning performed on a static dataset of agent-environment interactions. For example, GUI-R1 [205] and InfiGUI-R1 [206] utilize rule-based rewards and apply R1-style [215] training on offline GUI datasets.

**Online Learning** In contrast, online learning enables an agent to learn and adapt continuously while it interacts with a live or simulated environment. Feedback from each action is used to update the agent’s policy, plan, or knowledge base in real-time. This allows for greater adaptability to dynamic or unseen situations. Some agents evolve online not by updating their model weights, but by refining their plans and skill libraries on the fly. For example, Voyager [42] presents an LLM-powered agent that learns to play Minecraft by continuously exploring, generating its own curriculum of tasks, and building a persistent skill library from direct experience. AdaPlanner [18] focuses on adapting its plan within a task; it generates an initial plan, receives feedback from the environment, and refines the plan online. Similarly, SwiftSage [207] operates with a fast-and-slow thinking process, where it can reflect on failures of its fast, intuitive mode and switch to a more deliberate, tool-using slow mode, adapting its strategy online based on task difficulty. Reinforcement Learning serves as a fundamental mechanism for online learning, enabling agents to learn from environmental reward signals. DigiRL [85] demonstrates how to train device-control agents in the wild using autonomous RL, while DistRL [212] proposes an asynchronous distributed framework to make such on-device training feasible. MobileGUI-RL [213] addresses the specific challenges of training GUI agents in online mobile environments by introducing a synthetic task generation pipeline combined with group relative policy optimization (GRPO) through trajectory-aware rewards.

#### 5.4.2 On-policy and Off-policy Learning

While the previous section examined the timing of data collection and learning (online vs offline), this section focuses on the policy consistency aspect of agent evolution - specifically, whether agents learn from experiences generated by the same policy they are trying to improve (on-policy) or from experiences generated by different policies (off-policy). This distinction is crucial for understanding how agents utilize their experiential data and manage the trade-offs between learning stability and sample efficiency during the evolutionary process.

**On-policy Learning.** On-policy approaches require agents to learn exclusively from experiences generated by their current policy, ensuring policy consistency but often at the cost of sample efficiency. Reflexion [17] exemplifies this approach through its iterative self-reflection mechanism. The agent generates responses using its current policy, receives feedback on failures, and immediately incorporates this feedback to update its reasoning process for the next iteration. GRPO [216] and DAPO [217] continue this path and show the effectiveness of multiple rollouts. The agent always learns from its current behavior, maintaining strict policy consistency. In agent settings, on-policy methods provide excellent learning stability and avoid distribution mismatch issues that plague off-policy methods. However, they suffer from low sample efficiency, as each policy update requires fresh data collection, making them computationally expensive for complex multi-step reasoning or tool use scenarios where generating high-quality trajectories is costly.

**Off-policy Learning.** Off-policy approaches allow agents to learn from experiences generated by different policies, including previous versions, other agents, or human demonstrations, significantly improving sample efficiency at the cost of potential distribution mismatch. [218] demonstrates a sophisticated off-policy approach where model  $M_{t+1}$  learns from preference data generated by the previous version  $M_t$ . The system handles distribution shift through DPO’s built-in KL divergence constraint with the reference policy, preventing the new policy from deviating too far from the data-generating policy. [219] showcases another powerful off-policy paradigm by learning from diverse response

sources—including other models, humans, and different sampling strategies—through ranking-based supervision. The method elegantly sidesteps distribution shift by treating alignment as a ranking problem rather than requiring policy consistency. [81] illustrates off-policy learning in multi-agent settings, where agents learn from an "experience library" containing successful interaction trajectories generated by previous policy versions, enabling efficient reuse of expensive multi-agent coordination data. In agent settings, off-policy methods excel in sample efficiency, allowing agents to leverage historical data, expert demonstrations, and cross-agent learning. They are particularly valuable for multi-step reasoning where successful trajectories are rare and expensive to generate, and for tool use scenarios where agents can learn from diverse execution examples without repeated environmental interaction. However, they face challenges with distribution shift, reward hacking (where agents exploit inconsistencies between training and deployment policies), and the need for careful regularization to maintain training stability.

### 5.4.3 Reward Granularity

Another critical choice in the reward design is its granularity, which determines at what level of detail the agent receives its learning signal. Reward granularity ranges from coarse-grained outcome-based rewards, which evaluate the overall task completion, to fine-grained process-based rewards that assess each step of the agent's trajectory. Current self-evolution frameworks adopt these varying levels of granularity to tailor feedback mechanisms according to task complexity and the desired learning outcomes.

**Outcome-based Reward** Outcome-based Reward is a feedback mechanism that evaluates an agent based on the successful completion of predefined tasks. This reward is determined solely by the final state of the agent's trajectory, regardless of the intermediate steps. A central challenge, particularly in dynamic environments like web or GUI navigation, is to effectively learn from both successful trajectories and the much more frequent failure trajectories. To address this, Direct Preference Optimization (DPO) [220] is designed to directly maximize the likelihood of preferred responses while minimizing the KL-divergence with the reference policy. Similarly, RRHF [219] employs a ranking loss approach that aligns model probabilities of multiple responses with human preferences by ranking response probabilities without requiring auxiliary value models. Moreover, several works have developed specialized frameworks for agent self-evolution that are built upon outcome-based rewards. A straightforward approach is rejection sampling finetuning, as used in AutoWebGLM [208]. This method employs a pre-designed reward model to evaluate trajectory outcomes, identify the successful trajectories, and update the model with this high-quality data. DigiRL [85] models the GUI navigation task as a Markov Decision Process (MDP) and obtains a final, sparse reward at the end of an episode using a VLM-based evaluator. WebRL [84] develops a robust outcome-supervised reward model (ORM) to address the feedback sparsity inherent in dynamic web environments. The ORM evaluates task success within a self-evolving curriculum framework, enabling agents to learn from unsuccessful attempts and progressively improve.

**Process-based Reward** In contrast to outcome-based rewards, which provide a single, delayed signal, the process-based reward paradigm offers more precise and granular feedback by evaluating each step in an agent's trajectory. Process-supervised reward models (PRMs) have been demonstrated to be significantly more reliable than outcome-supervised reward models (ORMs), particularly in domains requiring complex reasoning like solving math problems [209]. However, obtaining such fine-grained step-level feedback traditionally requires extensive human annotations, which are both time-consuming and expensive to scale. To address this annotation bottleneck, Math-Shepherd [197] proposes an automatic process annotation framework that utilizes Monte Carlo Tree Search (MCTS) to gather step-wise supervision by assessing each step's potential to derive the correct final answer. Similarly, AlphaMath [210] trains a value model to evaluate the step correctness in solution paths and updates both the policy and value model through exploration and exploitation within an MCTS framework. By leveraging process-based rewards, agents can improve their capabilities in a progressive, step-by-step manner. rStar-Math [211] and AgentPRM [198] both propose methods to iteratively evolve the policy and the process reward model, generating progressively higher-quality reasoning paths without manual labels. Agent Q [199] integrates a step-wise verification mechanism into its MCTS process to collect high-quality trajectories, which are then used to iteratively refine the policy via DPO training.

**Hybrid Reward** The hybrid methods aim to provide more comprehensive learning signals by incorporating both the clarity of final task success (outcome-based) and the granular guidance of intermediate steps (process-based). These methods overcome the sparsity of outcome-only signals while grounding the agent's step-by-step reasoning in the ultimate task goal. For example, GiGPO [200] addresses the instability of training long-horizon agents by introducing a dual-level reward mechanism. It provides an episode-level reward based on the final success of entire trajectories, while simultaneously assigning a localized, step-level reward for intermediate actions. This dual signal provides both a high-level directional goal and low-level corrective guidance. Similarly, SPA-RL [201] proposes a reward decomposition method that bridges the gap between sparse outcome signals and dense process feedback. It attributes incremental progress to each step within multi-step trajectories based on the final task completion, effectively distributing the outcome-based reward across the process steps. This approach creates dense intermediate progress rewards that enhance reinforcement learning effectiveness while maintaining alignment with the ultimate task objectives.

## 5.5 Other Dimensions of Self-Evolution Methods

In addition to the core axes of learning paradigm, policy consistency, and reward granularity, Table 4 highlights several other important dimensions that differentiate self-evolution methods:

**Feedback Type.** The nature of feedback varies widely: reward-based methods leverage scalar rewards, natural language signals, or model confidence; imitation methods focus on demonstration trajectories and rationales; population-based methods use fitness scores or competitive signals. The feedback type fundamentally determines what information the agent uses to improve.

**Data Source.** Reward-based methods typically generate data through agent-environment interaction or engineered rules, while imitation learning often relies on human or expert-generated demonstrations. Population-based approaches draw from the collective experience of multiple agents or generations, enabling diverse exploration but requiring significant coordination.

**Sample Efficiency.** Imitation learning is generally the most sample-efficient, provided high-quality demonstrations are available, as agents can directly mimic expert behavior. Reward-based methods are moderately efficient, with efficiency highly sensitive to reward sparsity. Population-based evolution tends to be sample-inefficient, as it often requires evaluating a large number of agent variants through many trials.

**Stability.** Reward-based learning is sensitive to the quality and design of reward functions, risking reward hacking or unintended behaviors. Imitation learning depends heavily on the quality and diversity of demonstrations. Population-based methods are sensitive to population size and diversity, with small or homogeneous populations at risk of premature convergence.

**Scalability.** Scalability is determined by the feasibility of data or feedback collection and the ability to parallelize learning. Reward-based methods scale well when feedback is automated (e.g., via simulators). Imitation learning is often bottlenecked by the cost of collecting demonstrations. Population-based approaches can scale to large compute but are highly resource-intensive.

Together, these dimensions offer a more nuanced, multidimensional view of self-evolution strategies, guiding practitioners in selecting and designing agent learning pipelines that are best matched to the challenges of their specific domains.

## 6 Where to Evolve?

Self-evolving agents have facilitated advancements across a diverse array of domains and applications. Broadly, most of these applications can be systematically categorized into two groups: (1) general domain evolution, where agent systems evolve to expand their capabilities across a wide variety of tasks, mostly within the digital realm, and (2) specialized domain evolution, which evolves specifically to enhance their proficiency within particular task domains. In essence, evolution in general-purpose assistants focuses on transferring learned experience to a broader set of tasks, while evolution in specialized agents emphasizes deepening expertise within a specific domain.

### 6.1 General Domain Evolution

The first category, general domain evolution, refers to self-evolving agents designed for general-purpose applications, particularly as versatile digital assistants. These agents progressively enhance their capabilities to address a broad spectrum of user queries, especially in dynamic and diverse digital environments. Technically speaking, these general assistant agents enhance their abilities primarily via three mechanisms: memory optimization, curriculum-driven training, and model-agent co-evolution. These mechanisms collectively enable the agents to continuously adapt and effectively respond to increasingly complex user demands.

**Memory Mechanism.** The most common mechanism facilitating agent evolution is the memory mechanism, wherein agents summarize historical success/failure experiences [42, 221] into memory representations [222], anticipating that these distilled experiences will be beneficial when addressing previously unseen tasks. For instance, Mobile-Agent-E [117] employs a long-term memory structure consisting of "Tips," which provide general guidelines, and "Shortcuts," representing reusable action sequences derived from past experiences. This self-evolutionary module supports the continuous enhancement of performance on complex smartphone tasks. Another typical example is MobileSteward [118], which coordinates multiple app-specific Agents under a central Agent, with specialized modules for task scheduling, execution, and evaluation. It also incorporates a memory-based self-evolution mechanism that summarizes successful executions to improve future cross-app instruction handling. Meanwhile, Generative Agents [223] store

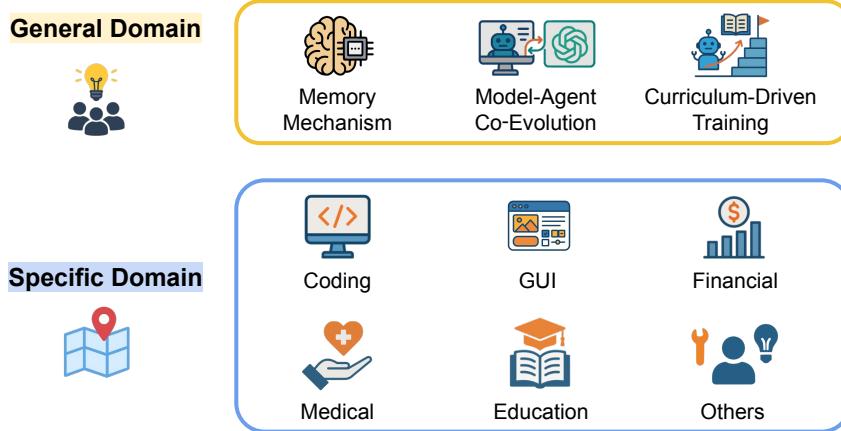


Figure 8: Categorization of where to evolve into two major types: General Domain Evolution, which focuses on broad capability enhancement across diverse tasks (e.g., memory mechanisms, co-evolution, curriculum training), and Specific Domain Evolution, which targets domain-specific expertise in areas such as coding, GUI, finance, medical, education, and others.

episodic memories of their experiences, synthesize higher-level reflections, and condition future planning on this self-reflection. In these examples, memory serves as the foundation that enables agents to internalize past experiences, abstract high-level patterns, and refine their future behavior.

**Model-Agent Co-Evolution.** Another line of work is to perform Model-Agent Co-evolution for LLM agents. UI-Genie [120] constructs a specialized image-text reward model that scores trajectories at both step and task levels. It jointly fine-tunes the agent and reward model using synthetic trajectories—generated by controlled corruption and hard-negative mining—across multiple generations. WebEvolver [119] introduces a co-evolving world model LLM that simulates web environments. It generates synthetic training data by predicting next observations and enables look-ahead reasoning during inference, which greatly improves real-web task success. Absolute Zero [121] co-evolves a reasoning agent and its internal self-reward model through reinforced self-play. By adversarially generating increasingly challenging reasoning problems and optimizing the agent using internal self-certainty as a reward signal, the framework simultaneously updates both the agent’s policy and the self-rewarding mechanism. Together, these methods demonstrate the effectiveness of co-evolving agents and auxiliary models (e.g., reward or world models) to achieve more robust, generalizable, and scalable learning in LLM agentic systems.

**Curriculum-Driven Training.** Curriculum-driven training also serves as a critical mechanism for building a self-evolving general assistant. For example, WebRL [84] uses a self-evolving curriculum: when an agent fails, similar but manageable tasks are automatically generated. Coupled with a learned reward model and adaptive policy updates, this yields a success rate uplift on WebArena benchmarks. Voyager [42] similarly leverages an automatic, bottom-up curriculum in Minecraft, where GPT-4 proposes appropriate next tasks based on agent progress, building a growing code-based skill library through iterative prompting and environmental feedback. These approaches highlight how curriculum learning enables agents to autonomously expand their capabilities through iterative task adaptation.

## 6.2 Specialized Domain Evolution

In addition to general digital agents, self-evolving agents have also been effectively applied within specialized domains, where their evolution is tailored to significantly enhance performance within narrower task sets.

**Coding.** The power of self-evolving agents extends directly to practical applications like coding, where their ability to autonomously adapt and improve offers a transformative approach to software development. SICA [95] demonstrates that a self-improving coding agent can autonomously edit its own codebase and improve its performance on benchmark tasks. EvoMAC [113] introduces a self-evolving paradigm on multi-agent collaboration networks, which automatically optimizes individual agent prompts and multi-agent workflows, significantly improving code generation performance by overcoming the limitations of manually designed systems. AgentCoder [224] also focuses on a multi-agent code generation framework that self-evolves through iterative refinement. A programmer agent continuously improves code based on feedback from a test executor agent, validated against independent test cases from a test designer, significantly

boosting effectiveness and efficiency. Zhang et al. [225] enable LLM agents to continuously evolve by filtering high-quality answers, stratifying earned experiences by difficulty, and adaptively selecting demonstrations from self-generated data, leading to significant performance improvements and the construction of ML libraries. While these instances differ in their specific mechanisms—ranging from single-agent self-editing to complex multi-agent collaborative networks and experience-based learning—they commonly share the core principle of iterative self-improvement and autonomous adaptation to enhance coding capabilities. These advancements highlight how self-evolving agents can dramatically enhance coding efficiency and code quality by continuously learning and optimizing.

**Graphical User Interfaces (GUI).** Self-evolving GUI agents extend LLM capabilities from pure text reasoning to direct manipulation of desktop, web, and mobile interfaces, where they must cope with large discrete action spaces, heterogeneous layouts, and partial visual observability. Yuan *et al.* couple pixel-level vision with self-reinforcement, enabling the agent to iteratively refine click-type grounding accuracy without additional human labels [226]. On real desktop software, the Navi agent from *WindowsAgentArena* replays and critiques its own failure trajectories, ultimately doubling its task-completion rate across 150 Windows challenges [227]. For open-web automation, *WebVoyager* fuses screenshot features with chain-of-thought reflection; successive self-fine-tuning raises its end-to-end success on unseen sites from 30 % to 59 % [228], while ReAP adds episodic memories of past outcomes, recovering a further 29-percentage-point margin on previously failed queries [229]. Beyond RL and memory, *AutoGUI* continuously mines functionality annotations from live interfaces to expand a reusable skill library each training cycle [230], and *MobileUse* deploys a hierarchical self-reflection stack that monitors, verifies, and revises smartphone actions *in situ* [231]. Collectively, these systems epitomize the full triad of self-evolution—what evolves (grounding modules, skill memories), when it evolves (offline consolidation vs. online reflection), and how it evolves (reinforcement learning, synthetic data, hierarchical monitoring)—charting a path toward universally competent interface agents.

**Financial.** The primary bottleneck in customizing agents for specialized domains like financial tasks lies in efficiently constructing and integrating a domain-specific knowledge base into the agent’s learning process—a challenge that can be effectively mitigated by incorporating self-evolving mechanisms. QuantAgent [122] proposed a two-layer framework that iteratively refines the agent’s responses and automatically enhances its domain-specific knowledge base using feedback from simulated and real-world environments. This iterative process helps the agent progressively approximate optimal behavior, reduces reliance on costly human-curated datasets, and demonstrably improves its predictive accuracy and signal quality in trading tasks. TradingAgents [232] incorporates dynamic processes such as reflection, reinforcement learning, and a feedback loop from real-world trading results, alongside collaborative debates, to continuously refine its strategies and enhance trading performance. These developments underscore the potential of self-evolving agents to revolutionize the financial domain by autonomously building domain expertise, adapting to dynamic market conditions, and continuously improving decision-making and trading performance.

**Medical.** Self-evolving agents have become a powerful paradigm in medical AI, where adaptability and the ability to evolve are essential for managing the complexity and ever-changing nature of real-world clinical practice. One of the most prominent applications is hospital-scale simulation. For example, Agent Hospital [233] creates closed environments with LLM-driven doctors, patients, and nurses, allowing the doctor agent to treat thousands of virtual cases. This process helps these agents autonomously refine and evolve their diagnostic strategies without manual labeling, ultimately achieving strong performance on USMLE-style exams. Similarly, MedAgentSim [234] integrates an LLM doctor, patient, and tool agent. It records successful consultations as reusable trajectories and employs chain-of-thought reflection and consensus to drive self-evolution, improving success rates over successive interactions. Another example is EvoPatient [235] places a doctor agent and a patient agent in continuous dialogue. With each generation, they update their memory with high-quality exchanges: the patient develops more realistic symptom narratives, while the doctor learns to ask sharper questions. Notably, this happens without explicit gradient updates or hand-crafted rewards. Reinforcement learning is also central to building adaptive medical agents. For instance, DoctorAgent-RL [236] models consultations as a Markov decision process, using a reward function that scores diagnostic accuracy, coverage, and efficiency. This guides policy-gradient updates that help the agent ask more relevant questions and reach correct diagnoses faster than imitation-based approaches, thus achieving self-improvement. In addition, automated architecture-search approaches like *Learning to Be a Doctor* treat the workflow itself as an evolvable object, iteratively inserting specialist sub-agents or new reasoning hops to cover observed failure modes and improve multimodal diagnostic accuracy [237]. Finally, beyond clinical decision-making, self-evolving agents have also been extended to biomedical discovery. OriGene [238] functions as a virtual disease biologist that evolves by iteratively refining its analytical process. It leverages human and experimental feedback to update core reasoning templates, adjust tool usage strategies, and refine analytical protocols. Similarly, STELLA [239] is a self-evolving biomedical research agent that improves over time by distilling successful reasoning workflows into reusable templates through its Template Library and expanding its Tool Ocean with external or newly assembled tools to meet emerging analytical needs.

**Education.** Self-evolving LLM agents have also found strong applications in the education domain. At the learner level, self-evolving agents like the personalized tutor PACE [240] adjust their prompts based on detailed student profiles and continually refine their questioning during conversations. Meanwhile, an LLM-to-LLM self-play framework generates diverse tutor–student dialogues that further fine-tune the agent, allowing its teaching strategies to evolve both during and after interactions. Another example is MathVC [241], which employs symbolic persona profiles for virtual students and a meta-planner that orchestrates realistic problem-solving stages. This setup enables the agent’s conversational process to evolve step by step toward correct solutions, closely mirroring how collaborative learning naturally unfolds. On the instructor side, self-evolving agent systems like the professional-development platform i-vip [242] deploy a team of cooperating LLM agents—a coach, assessor, and feedback generator—that critique and enhance each other’s outputs in real time. These agents adapt their explanations based on teacher-learners’ responses and continue to evolve by incorporating expert feedback after deployment, thereby refining their prompt strategies over time. Similarly, EduPlanner [243] frames lesson-plan creation as an adversarial loop where a planner’s draft is repeatedly reviewed and refined by evaluator and optimizer agents until it meets diverse educational goals. Similarly, SEFL [244] uses teacher–student self-play to generate large sets of homework–feedback examples, which then fine-tune a lightweight feedback model. This self-evolving process significantly improves the clarity and usefulness of the comments. Collectively, these examples illustrate how self-evolving LLM agents can dynamically adapt to both learners and instructors, driving more personalized, effective, and scalable educational experiences.

**Others.** Beyond the four major verticals discussed above, self-evolving agents demonstrate broader applicability, delivering superior adaptability and performance in specialized domains where conventional agents often fall short. For instance, Arxiv Copilot [123] learns and adapts by incorporating historical user interactions, including generated answers, research trends, and ideas, into its thought database, enhancing its ability to provide personalized and augmented academic assistance. In a very different context, Voyager [42], an agent in the game Minecraft, excels at solving novel tasks from scratch in new worlds through a process of self-evolution. It continually refines its task goals via an automatic curriculum, expands its skill library, and enhances its actions using an iterative prompting mechanism without human intervention. Transitioning to domains that require explicit strategic planning, Agents-of-Change [245] autonomously refines prompts and rewrites code based on iterative performance analysis and strategic research, thereby helping agents overcome inherent limitations in long-term strategic planning and achieve consistently superior and more coherent gameplay in complex environments like Settlers of Catan. Lastly, in the realm of diplomacy, Richelieu [246] introduces AI diplomacy agents that can self-evolve through their self-play mechanism, which allows the agent to augment its memory by acquiring diverse experiences without human data, thereby enhancing its strategic planning, reflection, and overall performance in diplomacy activities. While these diverse examples operate in distinct environments—from academic research and virtual game worlds to strategic board games and complex diplomatic negotiations—they all share the fundamental characteristic of leveraging continuous learning, self-refinement, and autonomous adaptation to achieve increasingly sophisticated and effective performance within their respective domains. These diverse examples reinforce the versatility of self-evolving agents, showcasing their growing potential to excel in a wide range of complex, dynamic, and human-like tasks beyond traditional domains.

## 7 Evaluation of Self-evolving Agents

Evaluating self-evolving agents presents a unique set of challenges that extend beyond the traditional assessment of static AI systems. Unlike conventional agents typically evaluated on a fixed set of tasks at a single point in time, self-evolving agents are designed to continuously learn, adapt, and improve through ongoing interaction with dynamic environments. Consequently, their evaluation must capture not only immediate task success but also crucial aspects such as adaptation over time, knowledge accumulation and retention, long-term generalization, and the ability to transfer learned skills across sequential or novel tasks, all while mitigating catastrophic forgetting. This demands a fundamental shift from conventional “single-shot” assessments to a longitudinal view of their growth trajectory.

### 7.1 Evaluation Goals and Metrics

To effectively evaluate self-evolving agents, we must move beyond traditional metrics and establish a comprehensive framework that captures their dynamic, adaptive, and long-term learning capabilities. A truly capable and desirable self-evolving agent must not only **learn and improve** but also **remember** past knowledge, **transfer** it to new situations, operate **sustainably**, and behave **responsibly**. Grounded in these critical requirements for continuous and robust AI, we categorize the key evaluation goals into five core dimensions: **Adaptivity**, **Retention**, **Generalization**, **Efficiency**, and **Safety**, as illustrated in Table 5. Each dimension addresses a vital aspect of an agent’s self-evolutionary process, providing a holistic view of its performance.

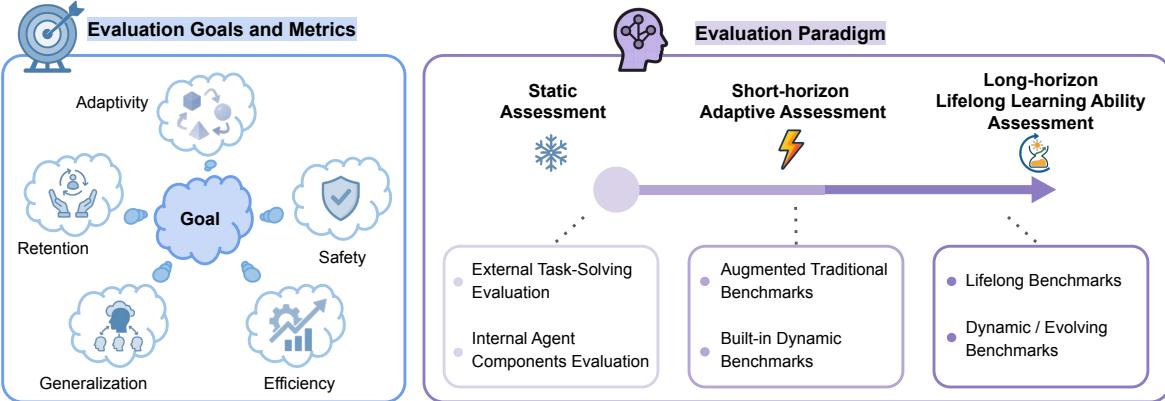


Figure 9: Overview of evaluation angles for self-evolving agents, encompassing core Evaluation Goals and Metrics—such as adaptivity, retention, generalization, safety, and efficiency—and a continuum of Evaluation Paradigms spanning from static assessment to short-term adaptability and long-horizon lifelong learning evaluation.

**Adaptivity** Adaptivity serves as a foundational evaluation criterion for any self-evolving agent, measuring its ability to improve performance on in-domain tasks through experience. This dimension focuses on quantifying the learning curve and the extent of performance enhancement as an agent iterates and evolves within a specific domain. Rather than a static success rate, adaptivity is gauged over time, steps, or iterations. Typical metrics include the Success Rate by Iteration Steps [65, 29, 247], which tracks performance in downstream tasks as a function of the agent’s interaction history.

**Retention** Retention is a crucial criterion for evaluating the stability of a self-evolving agent’s knowledge base. This dimension specifically focuses on the challenge of catastrophic forgetting, a common issue in lifelong learning where new knowledge acquisition erodes previously learned information, and knowledge retention within extended interactions. Two key metrics can be used to quantify this stability from different perspectives: Forgetting (FGT) and Backward Transfer (BWT) [138]. Specifically, Let  $J_{i,t}$  be the performance of LLM agents on task  $i$  after completing  $t$  tasks. FGT and BWT can be calculated as follows:

$$FGT_t = \frac{1}{t-1} \sum_{i=1}^{t-1} [\max_{j \in \{i, i+1, \dots, t\}} (\{J_{j,i}\}_j) - J_{t,i}] \quad BWT_t = \frac{1}{t-1} \sum_{i=1}^{t-1} (J_{t,i} - J_{i,i})$$

FGT evaluates the average accuracy drop on old tasks after an agent learns a new one, thereby measuring whether useful experience is successfully maintained. In contrast, BWT assesses the average accuracy improvement on old tasks due to the experience gained from a new task. A positive BWT indicates that new learning positively benefits old tasks, signifying successful knowledge transfer and a more robust, stable learning process.

**Generalization** While Adaptivity and Retention focus on in-domain performance, Generalization is a pivotal measure of a self-evolving agent’s ability to apply its accumulated knowledge to new, unseen domains or tasks. A truly intelligent agent should not only perform well within its familiar territory but also demonstrate a capacity for cross-domain generalization. This capability can be evaluated by assessing an agent’s performance on a diverse set of tasks that span multiple task distributions and domains. Common approaches include computing aggregate performance metrics (e.g., mean success rates) across multi-domain test suites [248], [18], and conducting out-of-domain evaluations using held-out task distributions that simulate real-world novelty scenarios [16, 249].

**Efficiency** Efficiency quantifies the resourcefulness of a self-evolving agent. As agents operate continuously and make decisions autonomously, it is essential to evaluate the cost and speed of their evolutionary process. These metrics are particularly important for practical, real-world applications where resources like computation and time are finite. Key indicators include token consumption [250], which measures the computational cost of an agent’s reasoning and generation steps), time consumption [251], the number of steps [42] and the number of interaction with the tools (e.g. tool productivity) [98] required to complete a task, which rewards agents for completing tasks in the fewest possible resource consumption. Several key metrics quantify agent efficiency in task execution, including token consumption (measuring computational overhead in reasoning and generation) [250], time expenditure [251], the number of required steps[42], and tool interaction frequency [98]. These indicators collectively assess an agent’s ability to minimize resource utilization while maintaining task performance, with lower values generally reflecting more efficient operation.

Table 5: Overview of Agent Evaluation Metrics Across Core Dimensions

Goal	Metric	Description
Adaptivity	Success Rate by Iteration Steps [65, 29, 247]	Performance in downstream tasks as a function of the agent's interaction history
	Adaptation Speed [42]	How quickly an agent reaches a certain performance threshold or converges to an optimal strategy within a given adaptation period
Retention	Forgetting (FGT) [138]	The average accuracy drop on old tasks after an agent learns a new one, measuring whether useful experience is successfully maintained
	Backward Transfer (BWT) [138]	The average accuracy improvement on old tasks due to the experience gained from new tasks
Generalization	Aggregate Performance [248, 18]	Mean success rates or other performance indicators across multi-domain test suites to gauge overall proficiency
	Out-of-Domain (OOD) Performance [16, 249]	The agent's performance in held-out task distributions
Efficiency	Token Consumption [250]	Computational overhead in reasoning and generation steps
	Time Expenditure [251]	Total duration required for task completion
	Number of Steps [42]	Minimal actions needed to accomplish objectives
	Tool Productivity [98]	The ratio between task benefit (e.g., answer accuracy) and tool usage cost (e.g., number of tool calls)
Safety	Safety Score [252]	Proportion of test cases where agent behavior meets predefined safety criteria
	Harm Score [253]	Graded assessment of harmful outputs based on violation severity
	Completion Under Policy (CuP) [254]	Task success rate while complying with specified constraints
	Risk Ratio [254]	Frequency of policy violations per interaction opportunity
	Refusal Rate [255, 253]	Percentage of tasks declined due to safety concerns
	Leakage Rate [256]	Incidence of unintended sensitive information disclosure

**Safety** From the perspective of self-evolving, the Safety domain critically examines whether these agents develop unsafe or undesirable behavioral patterns throughout their continuous evolution. This dimension assesses an agent's adherence to predefined rules and its propensity for harmful actions. Key metrics in evaluating safety of self-evolving agents may include: (1) Safety Score [252], measures the proportion of test cases where the agent's behavior is labeled “safe” ; (2) Harm Score [253], computes via a detailed manually written grading rubric where outputs earn partial credit whenever some but not all harmful criteria are triggered; (3) Completion Under Policy (CuP) [254], assesses whether an agent successfully completes a task while strictly adhering to a given set of rules or policies ; (4) Risk Ratio [254], calculates the frequency of an agent's rule violations along a specific dimension, providing a quantitative measure of non-compliance ; (5) Refusal Rate [255, 253], evaluates the proportion of tasks an agent refuses to perform due to their aggressive, malicious, or otherwise unsafe nature; (6) Leakage Rate [256], tracks how often an agent unintentionally leaks sensitive or private information.

## 7.2 Evaluation Paradigm

The evaluation of self-evolving agents, given their continuous learning paradigm, necessitates a multi-faceted approach that extends beyond traditional static assessments. Current evaluation paradigm can be broadly categorized based on the temporal scope of the assessment: **Static Assessment**, **Short-horizon Adaptive Assessment**, and **Long-horizon Lifelong Learning Ability Assessment**. Each category addresses different aspects of an agent's evolving capabilities, from its instantaneous performance to its long-term learning trajectory.

### 7.2.1 Static Assessment

Static assessment evaluates the instantaneous performance of self-evolving agents at a specific point in time. Although these agents are designed for continuous improvement, static methods remain crucial for establishing baseline performance, comparing different agent architectures on fixed task sets, or evaluating capabilities after discrete training phases. This approach aligns with conventional AI evaluation, focusing on immediate performance in fixed environments. While useful for assessing generalization in an “in-domain evolving, out-of-domain evaluation” paradigm, static assessment inherently does not capture the dynamic, continuous learning, or long-term evolutionary aspects central to self-evolving agents.

Table 6: Differences between Short-horizon Adaptive Assessment and Long-horizon Lifelong Learning Ability Assessment

Dimension	Short-horizon Adaptation Assessment	Long-horizon Lifelong Learning Ability Assessment
<b>Primary Focus</b>	Immediate learning and incremental improvement within consistent or slightly varying tasks	Continuous knowledge accumulation and sustained performance across diverse, evolving tasks and environments.
<b>Core Challenges</b>	Rapid adaptation to minor changes; Improving on similar, repeated tasks	Mitigating catastrophic forgetting; Robust knowledge transfer; Maintaining efficiency/safety over time; handling true novelty and significant distribution shifts
<b>Temporal Scope</b>	Small number of sequential tasks or iterations over a short period; Improvement on the same or similar task types.	Large, potentially unbounded sequence of diverse, cross-domain tasks; Very long interaction periods requiring integration of new skills with old

For evaluating an agent’s general capabilities at a given moment, standard benchmarks designed for static AI systems are often employed. These benchmarks offer diverse task domains and test various core agent competencies, providing a snapshot of an agent’s proficiency before or at specific stages of its evolution. These assessments can be systematically categorized into **External Task-Solving Evaluation** and **Internal Agent Components Evaluation**, where External Task-Solving Evaluation measures end-to-end performance in completing domain-specific or cross-domain tasks, and Internal Capability Evaluation focuses on fundamental components in the agent, including planning, tool utilization, memory management, multi-agent coordination, etc.

**External Task-Solving Evaluation** This category assesses an agent’s end-to-end proficiency in completing tasks across various real-world or simulated environments. In **scientific data analysis and machine learning engineering**, benchmarks like ScienceAgentBench[257] and MLE-Bench[258] test agents’ ability to generate and execute code for data analysis and solve Kaggle-style problems. For **web search/Browse**, environments such as WebShop[259], WebArena[260], X-WebAgentBench [261], Mind2Web[262], and BrowseComp[263] simulate realistic web interactions, complex Browse scenarios, and task completion under security constraints. In **software engineering**, the SWE-bench series[264, 265, 266, 267] uses real GitHub issues to assess agents’ code repair capabilities. For **computer-use interactions**, OSWorld[268] offers a unified environment for open-ended tasks involving various desktop and web applications. Specialized domains like **marketing** also feature benchmarks such as xbench[269]. Beyond specific domains, **generalist agent benchmarks** like AgentBench[248], GAIA[270], and TheAgentCompany[271] evaluate broad problem-solving abilities across multiple knowledge domains and professional tasks, simulating real-world demands on general AI assistants.

**Internal Agent Components Evaluation** Beyond end-to-end task completion, assessing an agent’s underlying core competencies is crucial. These benchmarks evaluate fundamental capabilities that contribute to an agent’s overall intelligence and self-evolutionary potential. As for **Planning**, Benchmarks such as PlanBench[272], Natural Plan[273], AutoPlanBench[274], and ACPBench[275] comprehensively evaluate an agent’s ability to understand dynamic environments, devise strategies, decompose complex problems, and execute reasoning in various planning domains. For **Tool Usage**, simple benchmarks like ToolAlpaca[276] and ToolBench[50] test basic selection and parameter mapping, while more complex ones like ToolSandbox[277], Seal-Tools[278], API-Bank[279], T-Eval[280],  $\tau$ -Bench[281], AceBench[282]) simulate real-world scenarios involving multi-turn interactions, implicit state dependencies, and nested calls. **Memory Management** benchmarks such as LTMbenchmark[283], MemoryAgentBench[284], and StoryBench[285] evaluate the agent’s capacity to retain and utilize information across multi-turn interactions, dynamic scenarios, and long-range dependencies. For evaluating **Multi-Agent Collaboration**, benchmarks such as MultiAgentBench[286] and SwarmBench[287] assess coordination, communication, and emergent swarm intelligence in both collaborative and competitive settings.

**Metrics for Static Assessment** Typical metrics for static assessment include accuracy, success rate, progress rate, completion rate, and various domain-specific performance indicators (e.g., CodeBertScore, Valid Execution Rate, Pass Rate, F1 score). These metrics provide a singular performance score for an isolated invocation or a fixed set of tasks.

## 7.2.2 Short-Horizon Adaptive Assessment

Short-horizon adaptations extend beyond static evaluations by assessing an agent’s ability to adapt and improve over a relatively short period or a limited number of interactions. The agent might improve performance on the same task instance with more attempts, or adapt to new instances of the same task type. This category focuses on capturing the capacity of the self-evolving agent for immediate adaptability and incremental learning within a relatively consistent or slightly varying task distribution. These evaluation schemes can be broadly categorized into two ways: (1) augment

Table 7: Representative Benchmarks for Evaluating Self-Evolving Agents

Benchmark Name	Task Domain	Goal	Core Metrics	Task Quantity	Temporal Scope
ScienceAgentBench [257]	Scientific Data Analysis	Adaptivity, Efficiency	Valid Execution Rate, Success Rate, CodeBERTScore, API Cost	102	Static
MLE-Bench [258]	ML-Engineering	Adaptivity	-	75	Static
DS-Bench [288]	Data Science	Adaptivity	Task Success Rate, Cost, Inference Time, Competition-level Accuracy	540	Static
SWE-bench [264]	Software Engineering	Adaptivity	Pass Rate	2,294	Static
OSWorld [268]	Computer-Use / GUI	Adaptivity	Success Rate	369	Static
Mobile-Eval-E [117]	Computer-Use / GUI	Adaptivity, Efficiency	Action Accuracy, Reflection Accuracy, Termination Error	25	Static, Short-horizon
WebShop [259]	Web Search / Browse	Adaptivity	Success Rate	12,087	Static
WebArena [260]	Web Search / Browse	Adaptivity	Success Rate	812	Static
WebWalkerQA [289]	Web Search / Browse	Adaptivity, Efficiency	Accuracy, Action Count	680	Static
ST-WebAgentBench [254]	Web Search / Browse	Safety	Completion under Policy	235	Static
xbench [269]	Web Search / Browse	Adaptivity	LLM-Judge Score	100	Static
BrowseComp [263]	Web Search / Browse	Adaptivity	Accuracy	1,266	Static
Agent-SafetyBench [252]	General	Safety	Safety Sore	20,000	Static
LifelongAgentBench [247]	General	Adaptivity, Retention, Generalization	Success Rate	1396	Long-horizon
AgentBench [248]	General	Adaptivity, Generalization	Success Rate, F1, Reward, Game Progress	1360	Static
GAIA [270]	General	Adaptivity	Accuracy	466	Static
TheAgentCompany [271]	General	Adaptivity, Efficiency	Completion Score, Steps, Cost per Instance	175	Static
EvaLearn [290]	General	Adaptivity, Efficiency	Accuracy, Slope, Position of 1st solution, Num of consecutive solutions	648	Long-Horizon
PlanBench [272]	Planning	Adaptivity	Accuracy	~26,250	Static, Short-horizon
Natural Plan [273]	Planning	Adaptivity	Exact Match	3,600	Static
ACPBench [275]	Planning	Adaptivity, Generalization	Accuracy	3,720	Static
AppBench [291]	Planning	Adaptivity	Success Rate, F1	800	Static
ToolBench [50]	Tool Usage	Adaptivity	Pass Rate, Win Rate	126,486	Static
ToolSandbox [277]	Tool Usage	Adaptivity	Similarity Score	1,032	Static
Seal-Tools [278]	Tool Usage	Adaptivity	Accuracy, P/R/F1	14,076	Static
API-Bank [279]	Tool Usage	Adaptivity	Accuracy, Rouge	4,125	Static
T-Eval [280]	Tool Usage	Adaptivity	Domain-Specific Score	23,305	Static
$\tau$ -Bench [281]	Tool Usage	Adaptivity	Pass^k	165	Static
AceBench [282]	Tool Usage	Adaptivity	Accuracy	2,000	Static
LTMBenchmark [283]	Agent Memory	Retention, Efficiency	Score, Accuracy, GoodAI LTM Score, Speed, Cost, Verbosity	30	Long-Horizon
StoryBench [285]	Agent Memory	Retention, Efficiency	Accuracy, First-Try Accuracy, Longest Corr, Retry Count, Runtime Cost, Token Cons,	311 scene nodes, 86 choice nodes	Short-Horizon, Long-Horizon
MemoryAgentBench [284]	Agent Memory	Adaptivity	SubEM, Recall, ROUGE F1, Accuracy, Recall@5, Model Based Acc/F1	2200	Static, Short-horizon
MultiAgentBench [286]	Multi-Agent Collaboration	Adaptivity	KPI, Text-Based Score, Communication Score, Planing Score, Coordination Score	100	Static
SwarmBench [287]	Multi-Agent Collaboration	Adaptivity	Perspective-specific Metrics	5	Short-horizon

traditional benchmarks with a temporal dimension, and (2) specially design benchmarks and metrics that can inherently support Short-Horizon dynamic learning.

**Augmented Traditional Benchmarks** Many studies leverage existing benchmarks but introduce a new dimension to track performance over time. This typically involves analyzing performance as a function of the number of iterations, steps, or examples. For example, ADAS[65] evaluated the held-out test accuracy with the number of agent system iterations on the ARC benchmark [292]; AWM[29] studied the cumulative success rate over the process of online evaluation under WebArena map test split[260], using a number of examples to mark the evolution progress; WebEvolver[119] studied the success rate with self-improving iterations under Mind2web-Live [293]. This approach allows for tracking the Adaptivity of the agent within a confined scope.

**Benchmarks with Built-in Dynamic Evaluation** Some benchmarks are designed with short-horizon dynamic learning in mind. MemoryAgentBench [284], for example, includes a “Test-Time Learning” (TTL) dimension that evaluates an agent’s ability to learn new tasks directly from conversation within a single interaction session. In practice, TTL is evaluated through two types of tasks: Multi-Class Classification and Recommendation. In these settings, the agent must utilize previously provided information—such as labeled examples in context or a long movie-related dialogue history—to perform new tasks like mapping sentences to class labels or recommending relevant movies. This assesses immediate adaptation and knowledge acquisition during ongoing interaction.

**Metrics and Methods for Evaluating Short-Horizon Adaptations** The primary metrics and methods for short-horizon adaptations are designed to quantify Adaptivity. These include: (1) Success Rate by Iteration Steps [65, 29, 247], which tracks performance improvements as the agent interacts more with the environment or attempts a task multiple times. (2) Learning Curve Analysis, visualizing how performance (e.g., success rate, accuracy) changes over a limited number of training steps, episodes, or interactions [65, 29]. (3) Adaptation Speed [42], measuring how quickly an agent reaches a certain performance threshold or converges to an optimal strategy within the short horizon.

Short-horizon adaptations are well-suited for evaluating the initial learning capabilities and immediate adaptability of self-evolving agents. They can effectively demonstrate whether an agent can learn from recent experiences and improve its performance on in-domain tasks. This category is widely used for current self-evolving agents. However, the limited temporal window makes it challenging to assess long-term knowledge retention (mitigating catastrophic forgetting) and true lifelong learning capabilities across vastly different or sequentially presented tasks.

### 7.2.3 Long-Horizon Lifelong Learning Ability Assessment

Long-horizon lifelong learning ability assessment is crucial for truly assessing self-evolving agents, as they focus on the agent’s ability to continuously acquire, retain, and reuse knowledge across diverse environments and over extended periods. As shown in Table 7.2.1, it mainly focuses on continuous learning, knowledge accumulation, and sustained performance across a diverse and potentially ever-changing stream of tasks or environments over an extended period. This is a nascent but critical area, where unique challenges include catastrophic forgetting, robust knowledge transfer across disparate tasks, efficient resource management over extended durations, and mitigating data leakage when continuously evaluating on evolving data distributions. Specialized benchmarks are emerging to tackle these complexities.

Currently, there are few benchmarks of this type. LTMBenchmark [283] is a specialized benchmark focusing on long-term memory (LTM) evaluation. It assesses LLM agents’ memory retention and continual learning through dynamic conversational tests, using interleaved dialogues with controlled distractions to simulate real-world recall challenges. Key metrics include task accuracy, memory-span-weighted LTM Score, and efficiency measures (tests/hour, cost) for cross-architecture comparison. LifelongAgentBench [247] is another pioneering benchmark specifically designed to evaluate agent lifelong learning. It constructs sequences of interdependent tasks across domains like Database (DB), Operating System (OS), and Knowledge Graph (KG), requiring agents to progressively build upon previously acquired skills. This allows for systematic tracking of performance improvement and knowledge retention across a prolonged learning trajectory. In addition, there is a solution that constructs a dynamic benchmark through continuously updating benchmark datasets [294, 295] or evolving the benchmark itself by reconstructing original benchmarks to evaluate self-evolving agents, which can alleviate data leakage to some extent [296]. Benchmark Self-Evolving [297], for example, proposes a solution to continuously update the existing benchmark through iteration. Preliminary findings from such dynamic benchmark scenarios have shown that model performance can degrade as the benchmark evolves, highlighting the difficulty of continuous adaptation.

Metrics for long-horizon lifelong learning go beyond simple success rates to quantify the agent’s evolving ability, such as Forgetting (FGT), Backward Transfer (BWT) [138], Cost-per-Gain. Long-term Generalization metrics could involve assessing performance on a continuously evolving set of out-of-distribution tasks or measuring the breadth of tasks an agent can still perform effectively after prolonged learning across many domains.

Long-horizon lifelong learning ability assessment is essential for comprehensively evaluating the core promise of self-evolving agents: their ability to learn continuously, retain knowledge, and generalize effectively over extended periods. They are critical for assessing Retention, Generalization to truly novel scenarios, and the Efficiency of long-term operation. This area remains a key frontier for research in evaluating self-evolving agents.

## 8 Future Direction

### 8.1 Personalize AI Agents

With the increasing interest in self-evolving agents, deploying personalized agents has become a crucial and increasingly significant objective for the research community [298]. For instance, in applications such as chatbots, digital twins, and emotional support dialogues, a key challenge is enabling AI agents to accurately capture and adapt to users' unique behavioral patterns or preferences over extended interactions. Existing personalized agents typically depend heavily on labeled data and post-training methodologies [299]. Recent work by [300] proposes a self-generated preference data approach aimed at rapidly personalizing LLMs. TWIN-GPT [301] leverages electronic health records to create digital twins of patients, enhancing the accuracy of clinical trial outcome predictions. However, these existing strategies hinge on the critical assumption that LLMs can consistently obtain high-quality, large-scale user data. In practical deployment scenarios, the primary challenge remains the cold-start problem: agents need to progressively refine their personalized understanding, accurately interpret user intentions, and effectively construct user profiles, even when initial data is limited. Additionally, significant challenges persist in personalized planning and execution, such as effective long-term memory management, external tool integration, and personalized generation (ensuring outputs consistently align with individual user facts and preferences) [302]. Moreover, it is essential to ensure that self-evolving agents do not inadvertently reinforce or exacerbate existing biases and stereotypes, highlighting another critical direction for future research.

With the integration of personalized data, evaluation metrics for personalizing self-evolving agents should extend beyond intrinsic evaluations (e.g., directly assessing personalized generated text quality using metrics such as ROUGE [303] and BLEU [304]) or extrinsic evaluations (e.g., indirect assessments of personalization effects through recommendation systems, classification tasks, and other specific applications). Traditional personalization evaluation metrics often fail to adequately capture the evolving dynamics inherent in self-evolving agents. Consequently, future research calls for more lightweight and adaptive evaluation metrics [298]. Additionally, to better assess self-evolving personalized agents, there is a clear need for flexible, dynamic benchmarks capable of accurately evaluating agents' performance, particularly in managing long-tailed personalization data throughout their self-evolving processes.

### 8.2 Generalization

Self-evolving agents also face considerable challenges in achieving robust generalization across diverse task domains and environments. The fundamental tension between specialization and broad adaptability remains one of the most pressing challenges in the field, with significant implications for scalability, knowledge transfer, and collaborative intelligence.

**Scalable Architecture Design:** A central challenge in developing generalizable self-evolving agents lies in designing scalable architectures capable of maintaining performance as complexity and scope increase. Current agent systems frequently encounter a trade-off between specialization and generalization, where agents optimized for specific tasks struggle to transfer their learned behaviors to novel environments [305]. Additionally, the computational cost associated with dynamic reasoning in LLM-based agents grows non-linearly with the complexity of adaptation mechanisms, imposing practical constraints on achievable generalization within realistic resource limitations [306]. Recent studies indicate that self-evolving agents equipped with reflective and memory-augmented capabilities show substantial promise for enhancing generalization, particularly in smaller, resource-constrained models [24]. Nonetheless, these approaches continue to encounter limitations when addressing complex real-world scenarios that require sustained adaptation over prolonged periods.

**Cross-Domain Adaptation:** Achieving generalization across domains represents a critical frontier for self-evolving agents. Current methods frequently rely on domain-specific fine-tuning, restricting agents' adaptability to new environments without retraining [245]. Recent advancements in test-time scaling and inference-time adaptation provide promising pathways for enhancing cross-domain generalization [307, 308]. These techniques allow agents to dynamically allocate additional reasoning capacity to unfamiliar scenarios by scaling computational resources during inference, avoiding the need for increasing model parameters. Additionally, meta-learning strategies have demonstrated considerable potential in facilitating rapid few-shot adaptation to new domains [309]. However, their effectiveness critically depends on an agent's capability to accurately determine when supplementary computational resources are necessary and efficiently distribute these resources across diverse reasoning tasks.

**Continual Learning and Catastrophic Forgetting:** Self-evolving agents must continuously adapt to new tasks while retaining previously acquired knowledge, a challenge exacerbated by the catastrophic forgetting phenomenon [310] of

continual memorization [311] inherent in LLMs [312]. The stability-plasticity dilemma becomes particularly acute in foundation model-based agents, where the computational costs of retraining for every new task are prohibitive [138]. Recent research has explored parameter-efficient fine-tuning methods, selective memory mechanisms, and incremental learning strategies to mitigate catastrophic forgetting while preserving adaptability [137]. Nonetheless, achieving an optimal balance between efficiency and preventing model drift remains a significant open challenge, especially when agents operate under resource constraints or manage streaming data with stringent privacy considerations.

**Knowledge Transferability:** Recent studies have identified critical limitations in knowledge transfer among AI agents. [313] emphasized that knowledge integration and transfer capabilities in current agents still require significant optimization. In particular, [314] found that LLM-based agents often fail to effectively propagate newly acquired knowledge from interactions to other agents, restricting their collaborative potential. Furthermore, [315] revealed that foundation models might depend heavily on shallow pattern matching, rather than developing robust and transferable internal world models. These findings indicate several important future research directions: 1) it is essential to better understand the conditions under which knowledge acquired by one agent can be reliably generalized and communicated to others; 2) developing methods to quantify the limitations in agents' knowledge transferability could lead to clearer insights into agent collaboration bottlenecks; 3) we need to have an explicit mechanism that encourage the formation of robust, generalizable world models could significantly improve the collaborative effectiveness of self-evolving agents.

### 8.3 Safe and Controllable Agents

As autonomous AI agents become increasingly capable of learning, evolving, and performing complex tasks independently, more agent-based studies are shifting their focus towards the deployment of safer and more controllable agents. These safety concerns arise primarily from user-related risks, such as vague or misleading instructions that lead agents to execute harmful actions, as well as environmental risks, including exposure to malicious content, such as phishing website links [316].

Many studies aimed to address safety concerns about the automatic adaptation of agents. For instance, TrustAgent [73] implements pre-planning, in-planning, and post-planning strategies to foster safer agent behavior. However, as highlighted in [317], current agents based on LLM still struggle to accurately differentiate between sensitive information that is necessary and irrelevant information. A major challenge here is the precise identification and understanding of task-related versus unrelated information. Furthermore, managing agent actions when goals involve deceptive or unethical methods presents further difficulties, as ongoing learning uncertainty exacerbates these safety challenges for the deployment of controllable agents [318]. This uncertainty is reflected similarly in ambiguous contexts [319] and poorly designed memory modules [320]. Therefore, deploying a reliable, controllable, and safe self-evolving system has become a critical issue. Future research should focus on collecting larger-scale, more diverse real-world scenario data to support comprehensive learning of safe behaviors. Further refining the Agent Constitution by developing clearer, more understandable rules and case libraries is essential. Furthermore, exploring safer training algorithms and thoroughly investigating the impacts of privacy-protection measures on agent efficiency are necessary steps toward achieving a more balanced and secure deployment of autonomous AI agents.

### 8.4 Ecosystems of Multi-Agents

Multi-agent self-evolving systems face several unique challenges that require further exploration.

**Balancing Individual and Collective Reasoning:** Recent studies highlight the difficulty of balancing independent reasoning with effective group decision-making in multi-agent environments [321, 322]. While collective discussions can significantly enhance diagnostic reasoning, agents often risk becoming overly reliant on group consensus, thereby diminishing their independent reasoning capabilities. To mitigate this issue, future research should explore dynamic mechanisms that adjust the relative weight of individual versus collective input. Such an approach would help prevent decision-making from being dominated by a single or a small subset of agents, ultimately promoting robust, balanced consensus-building and innovation. Additionally, developing explicit knowledge bases and standardized updating methodologies—leveraging agents' successes and failures—could further improve the agents' self-evolution abilities and strengthen their individual reasoning contributions within collaborative contexts.

**Efficient Frameworks and Dynamic Evaluation:** Another crucial challenge lies in developing efficient algorithms and adaptive frameworks that allow agents to collaborate effectively while preserving their individual decision-making strengths. [113] introduced adaptive reward models and optimized dynamic network structures, which can significantly enhance cooperative self-improvement among agents. However, a major gap identified by [322] is the absence of clear mechanisms for agents to dynamically manage and update their knowledge. Addressing this issue will require

new frameworks that explicitly integrate continuous learning and adaptive collaboration mechanisms. Furthermore, existing benchmarks for multi-agent evaluation are predominantly static [286] and therefore fail to capture the long-term adaptability and continuous evolution of agent roles. Future benchmarks should incorporate dynamic assessment methods, reflecting ongoing adaptation, evolving interactions, and diverse contributions within multi-agent systems, thus providing more comprehensive evaluation metrics for self-evolving agents.

## 9 Conclusion

The emergence of self-evolving agents marks a paradigm shift in artificial intelligence, moving beyond static, monolithic models toward dynamic agentic systems capable of continual learning and adaptation. As language agents are increasingly deployed in open-ended, interactive environments, the ability to evolve, adapting reasoning processes, tools, and behaviors in response to new tasks, knowledge, and feedback, has become essential for building the next generation of agentic systems. In this survey, we provide the first comprehensive and systematic review of self-evolving agents, organized around three foundational questions: *what aspects of an agent should evolve, when evolution should occur, and how to implement evolutionary processes effectively*. Moreover, we discuss several methods for evaluating the progress of self-evolving agents in terms of metrics and benchmarks, followed by corresponding applications and future directions. Looking ahead, realizing the full potential of self-evolving agents will be critical in laying the groundwork for Artificial Super Intelligence (ASI). The evolution of these agents will require significant advancements in models, data, algorithms, and evaluation practices, and so on. Addressing issues such as catastrophic forgetting, human preference alignment during autonomous evolution, and the co-evolution of agents and environments will be key to unlocking agents that are not only adaptive but also trustworthy and aligned with human values. We hope this survey provides a foundational framework for researchers and practitioners to design, analyze, and advance the development and progress of self-evolving agents.

## References

- [1] Junyu Luo, Weizhi Zhang, Ye Yuan, Yusheng Zhao, Junwei Yang, Yiyang Gu, Bohan Wu, Binqi Chen, Ziyue Qiao, Qingqing Long, Rongcheng Tu, Xiao Luo, Wei Ju, Zhiping Xiao, Yifan Wang, Meng Xiao, Chenwu Liu, Jingyang Yuan, Shichang Zhang, Yiqiao Jin, Fan Zhang, Xian Wu, Hanqing Zhao, Dacheng Tao, Philip S. Yu, and Ming Zhang. Large language model agent: A survey on methodology, applications and challenges, 2025.
- [2] Hongru Wang, Yujia Qin, Yankai Lin, Jeff Z. Pan, and Kam-Fai Wong. Empowering large language models: Tool learning for real-world interaction. In *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR ’24, page 2983–2986, New York, NY, USA, 2024. Association for Computing Machinery.
- [3] Hongru Wang, Cheng Qian, Manling Li, Jiahao Qiu, Boyang Xue, Mengdi Wang, Heng Ji, and Kam-Fai Wong. Toward a theory of agents as tool-use decision-makers, 2025.
- [4] Xunjian Yin, Xinyi Wang, Liangming Pan, Li Lin, Xiaojun Wan, and William Yang Wang. Gödel agent: A self-referential agent framework for recursive self-improvement, 2025.
- [5] Chrisantha Fernando, Dylan Banarse, Henryk Michalewski, Simon Osindero, and Tim Rocktäschel. Prompt-breeder: Self-referential self-improvement via prompt evolution. *arXiv preprint arXiv:2309.16797*, 2023.
- [6] Bang Liu, Xinfeng Li, Jiayi Zhang, Jinlin Wang, Tanjin He, Sirui Hong, Hongzhang Liu, Shaokun Zhang, Kaitao Song, Kunlun Zhu, Yuheng Cheng, Suyuchen Wang, Xiaoqiang Wang, Yuyu Luo, Haibo Jin, Peiyan Zhang, Ollie Liu, Jiaqi Chen, Huan Zhang, Zhaoyang Yu, Haochen Shi, Boyan Li, Dekun Wu, Fengwei Teng, Xiaojun Jia, Jiawei Xu, Jinyu Xiang, Yizhang Lin, Tianming Liu, Tongliang Liu, Yu Su, Huan Sun, Glen Berseth, Jianyun Nie, Ian Foster, Logan Ward, Qingyun Wu, Yu Gu, Mingchen Zhuge, Xiangru Tang, Haohan Wang, Jiaxuan You, Chi Wang, Jian Pei, Qiang Yang, Xiaoliang Qi, and Chenglin Wu. Advances and challenges in foundation agents: From brain-inspired intelligence to evolutionary, collaborative, and safe systems, 2025.
- [7] Zhengwei Tao, Ting-En Lin, Xiancai Chen, Hangyu Li, Yuchuan Wu, Yongbin Li, Zhi Jin, Fei Huang, Dacheng Tao, and Jingren Zhou. A survey on self-evolution of large language models. *arXiv preprint arXiv:2404.14387*, 2024.
- [8] Yifei Zhou, Sergey Levine, Jason Weston, Xian Li, and Sainbayar Sukhbaatar. Self-challenging language model agents, 2025.
- [9] Toby Simonds, Kevin Lopez, Akira Yoshiyama, and Dominique Garmier. Self rewarding self improving, 2025.
- [10] Jianqiao Lu, Wanjun Zhong, Wenyong Huang, Yufei Wang, Qi Zhu, Fei Mi, Baojun Wang, Weichao Wang, Xingshan Zeng, Lifeng Shang, Xin Jiang, and Qun Liu. SELF: Self-evolution with language feedback. *arXiv preprint arXiv:2310.00533*, 2023.

- [11] Aviral Kumar, Rishabh Agarwal, Disha Shrivastava, Feryal Behbahani, Aleksandra Faust, et al. Training language models to self-correct via reinforcement learning. [arXiv preprint arXiv:2409.12917](#), 2024.
- [12] Yuhua Jiang, Yuwen Xiong, Yufeng Yuan, Chao Xin, Wenyuan Xu, Yu Yue, Qianchuan Zhao, and Lin Yan. PAG: Multi-turn reinforced llm self-correction with policy as generative verifier. [arXiv preprint arXiv:2506.10406](#), 2025.
- [13] S. Yellamraju, , et al. TextGrad: Automatic "differentiation" via text. [arXiv preprint arXiv:2406.07496](#), 2024.
- [14] Tevin Wang and Chenyan Xiong. Autorule: Reasoning chain-of-thought extracted rule-based rewards improve preference learning. [arXiv preprint arXiv:2506.15651](#), 2025.
- [15] Hongru Wang, Deng Cai, Wanjun Zhong, Shijue Huang, Jeff Z. Pan, Zeming Liu, and Kam-Fai Wong. Self-reasoning language models: Unfold hidden reasoning chains with few reasoning catalyst, 2025.
- [16] Mengkang Hu, Pu Zhao, Can Xu, Qingfeng Sun, Jianguang Lou, Qingwei Lin, Ping Luo, and Saravan Rajmohan. Agentgen: Enhancing planning abilities for large language model based agent via environment and task generation. [arXiv preprint arXiv:2408.00764](#), 2024.
- [17] Noah Shinn, Federico Cassano, Edward Berman, Ashwin Gopinath, Karthik Narasimhan, and Shunyu Yao. Reflexion: Language agents with verbal reinforcement learning. In [Advances in Neural Information Processing Systems](#), 2023.
- [18] Haotian Sun, Yuchen Zhuang, Lingkai Kong, Bo Dai, and Chao Zhang. AdaPlanner: Adaptive planning from feedback with language models. In [Advances in Neural Information Processing Systems](#), 2023.
- [19] Maxime Robeyns, Martin Szummer, and Laurence Aitchison. A self-improving coding agent, 2025.
- [20] Aman Madaan, Niket Tandon, Prakhar Gupta, Skyler Hallinan, Luyu Gao, Sarah Wiegreffe, Uri Alon, Nouha Dziri, Shrimai Prabhumoye, Yiming Yang, Shashank Gupta, Bodhisattwa Prasad Majumder, Katherine Hermann, Sean Welleck, Amir Yazdanbakhsh, and Peter Clark. Self-refine: Iterative refinement with self-feedback. In A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, editors, [Advances in Neural Information Processing Systems](#), volume 36, pages 46534–46594. Curran Associates, Inc., 2023.
- [21] Hongjin Su, Ruoxi Sun, Jinsung Yoon, Pengcheng Yin, Tao Yu, and Sercan Ö. Arık. Learn-by-interact: A data-centric framework for self-adaptive agents in realistic environments, 2025.
- [22] Zihan Wang, Kangrui Wang, Qineng Wang, Pingyue Zhang, Linjie Li, Zhengyuan Yang, Xing Jin, Kefan Yu, Minh Nhat Nguyen, Licheng Liu, Eli Gottlieb, Yiping Lu, Kyunghyun Cho, Jiajun Wu, Li Fei-Fei, Lijuan Wang, Yejin Choi, and Manling Li. Ragen: Understanding self-evolution in llm agents via multi-turn reinforcement learning. [arXiv preprint arXiv:2504.20073](#), 2025.
- [23] Borui Wang, Kathleen McKeown, and Rex Ying. Dystil: Dynamic strategy induction with large language models for reinforcement learning, 2025.
- [24] Xuechen Liang, Yangfan He, Yinghui Xia, Xinyuan Song, Jianhui Wang, Meiling Tao, Li Sun, Xinhang Yuan, Jiayi Su, Keqin Li, Siyuan Chen, and Tianyu Shi. Self-evolving agents with reflective and memory-augmented abilities. [arXiv preprint arXiv:2409.00872](#), 2024.
- [25] Prateek Chhikara, Dev Khant, Saket Aryan, Taranjeet Singh, and Deshraj Yadav. Mem0: Building production-ready ai agents with scalable long-term memory. [arXiv preprint arXiv:2504.19413](#), 2025.
- [26] Rana Salama, Jason Cai, Michelle Yuan, Anna Currey, Monica Sunkara, Yi Zhang, and Yassine Benajiba. Memindsight: Autonomous memory augmentation for llm agents. [arXiv preprint arXiv:2503.21760](#), 2025.
- [27] Danyang Zhang, Lu Chen, Situo Zhang, Hongshen Xu, Zihan Zhao, and Kai Yu. Large language models are semi-parametric reinforcement learning agents. [Advances in Neural Information Processing Systems](#), 36, 2024.
- [28] Andrew Zhao, Daniel Huang, Quentin Xu, Matthieu Lin, Yong-Jin Liu, and Gao Huang. Expel: Llm agents are experiential learners. In [Proceedings of the AAAI Conference on Artificial Intelligence](#), volume 38, pages 19632–19642, 2024.
- [29] Zora Zhiruo Wang, Jiayuan Mao, Daniel Fried, and Graham Neubig. Agent workflow memory. [arXiv preprint arXiv:2409.07429](#), 2024.
- [30] Zhenyu Guan, Xiangyu Kong, Fangwei Zhong, and Yizhou Wang. Richelieu: Self-evolving llm-based agents for ai diplomacy. [Advances in Neural Information Processing Systems](#), 37:123471–123497, 2024.
- [31] Cheng Qian, Shihao Liang, Yujia Qin, Yining Ye, Xin Cong, Yankai Lin, Yesai Wu, Zhiyuan Liu, and Maosong Sun. Investigate-consolidate-exploit: A general strategy for inter-task agent self-evolution. [arXiv preprint arXiv:2401.13996](#), 2024.

- [32] Yongchao Zhou, Andrei Ioan Muresanu, Ziwen Han, Keiran Paster, Silviu Pitis, Harris Chan, and Jimmy Ba. Large language models are human-level prompt engineers. In *The Eleventh International Conference on Learning Representations*, 2022.
- [33] Chengrun Yang, Xuezhi Wang, Yifeng Lu, Hanxiao Liu, Quoc V Le, Denny Zhou, and Xinyun Chen. Large language models as optimizers. *arXiv preprint arXiv:2309.03409*, 2023.
- [34] Reid Pryzant, Dan Iter, Jerry Li, Yin Tat Lee, Chenguang Zhu, and Michael Zeng. Automatic prompt optimization with "gradient descent" and beam search. *arXiv preprint arXiv:2305.03495*, 2023.
- [35] Xinyuan Wang, Chenxi Li, Zhen Wang, Fan Bai, Haotian Luo, Jiayou Zhang, Nebojsa Jojic, Eric P Xing, and Zhiting Hu. Promptagent: Strategic planning with language models enables expert-level prompt optimization. *arXiv preprint arXiv:2310.16427*, 2023.
- [36] Peiyang Zhang, Haibo Jin, Leyang Hu, Xinnuo Li, Liying Kang, Man Luo, Yangqiu Song, and Haohan Wang. Revolve: Optimizing ai systems by tracking response evolution in textual optimization. *arXiv preprint arXiv:2412.03092*, 2024.
- [37] Omar Khattab, Arnav Singhvi, Paridhi Maheshwari, Zhiyuan Zhang, Keshav Santhanam, Sri Vardhamanan, Saiful Haq, Ashutosh Sharma, Thomas T Joshi, Hanna Moazam, et al. Dspy: Compiling declarative language model calls into self-improving pipelines. *arXiv preprint arXiv:2310.03714*, 2023.
- [38] Xiao Wang, Yuansen Zhang, Tianze Chen, Songyang Gao, Senjie Jin, Xianjun Yang, Zhiheng Xi, Rui Zheng, Yicheng Zou, Tao Gui, et al. Trace: A comprehensive benchmark for continual learning in large language models. *arXiv preprint arXiv:2310.06762*, 2023.
- [39] Jinyu Xiang, Jiayi Zhang, Zhaoyang Yu, Fengwei Teng, Jinhao Tu, Xinbing Liang, Sirui Hong, Chenglin Wu, and Yuyu Luo. Self-supervised prompt optimization. *arXiv preprint arXiv:2502.06855*, 2025.
- [40] Li Yin and Zhangyang Wang. Llm-autodiff: Auto-differentiate any llm workflow. *arXiv e-prints*, pages arXiv–2501, 2025.
- [41] Siyu Yuan, Kaitao Song, Jiangjie Chen, Xu Tan, Dongsheng Li, and Deqing Yang. Evoagent: Towards automatic multi-agent generation via evolutionary algorithms. *arXiv preprint arXiv:2406.14228*, 2024.
- [42] Guanzhi Wang, Yuqi Xie, Yunfan Jiang, Ajay Mandlekar, Chaowei Xiao, Yuke Zhu, Linxi Fan, and Anima Anand-kumar. Voyager: An open-ended embodied agent with large language models. *arXiv preprint arXiv:2305.16291*, 2023.
- [43] Jiahao Qiu, Xuan Qi, Tongcheng Zhang, Xinzhe Juan, Jiacheng Guo, Yifu Lu, Yimin Wang, Zixin Yao, Qihan Ren, Xun Jiang, Xing Zhou, Dongrui Liu, Ling Yang, Yue Wu, Kaixuan Huang, Shilong Liu, Hongru Wang, and Mengdi Wang. Alita: Generalist agent enabling scalable agentic reasoning with minimal predefinition and maximal self-evolution. *CoRR*, abs/2505.20286, 2025.
- [44] Mohd Ariful Haque, Justin Williams, Sunzida Siddique, Md. Hujaifa Islam, Hasmot Ali, Kishor Datta Gupta, and Roy George. Advanced tool learning and selection system (ATLASS): A closed-loop framework using LLM. *CoRR*, abs/2503.10071, 2025.
- [45] Cheng Qian, Chi Han, Yi Fung, Yujia Qin, Zhiyuan Liu, and Heng Ji. CREATOR: Tool Creation for Disentangling Abstract and Concrete Reasoning of Large Language Models. In *The 2023 Conference on Empirical Methods in Natural Language Processing*, 2023.
- [46] Boyuan Zheng, Michael Y. Fatemi, Xiaolong Jin, Zora Zhiruo Wang, Apurva Gandhi, Yueqi Song, Yu Gu, Jayanth Srinivasa, Gaowen Liu, Graham Neubig, and Yu Su. Skillweaver: Web agents can self-improve by discovering and honing skills. *CoRR*, abs/2504.07079, 2025.
- [47] Lifan Yuan, Yangyi Chen, Xingyao Wang, Yi Fung, Hao Peng, and Heng Ji. CRAFT: Customizing LLMs by Creating and Retrieving from Specialized Toolsets. In *12th International Conference on Learning Representations*, 2024.
- [48] Haiteng Zhao, Chang Ma, Guoyin Wang, Jing Su, Lingpeng Kong, Jingjing Xu, Zhi-Hong Deng, and Hongxia Yang. Empowering large language model agents through action learning. *CoRR*, abs/2402.15809, 2024.
- [49] Changle Qu, Sunhao Dai, Xiaochi Wei, Hengyi Cai, Shuaiqiang Wang, Dawei Yin, Jun Xu, and Ji-Rong Wen. From exploration to mastery: Enabling llms to master tools via self-driven interactions. In *ICLR*. OpenReview.net, 2025.
- [50] 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.

- [51] Timo Schick, Jane Dwivedi-Yu, Roberto Dessì, Roberta Raileanu, Maria Lomeli, Eric Hambro, Luke Zettlemoyer, Nicola Cancedda, and Thomas Scialom. Toolformer: Language models can teach themselves to use tools. In *NeurIPS*, 2023.
- [52] Shishir G. Patil, Tianjun Zhang, Xin Wang, and Joseph E. Gonzalez. Gorilla: Large language model connected with massive apis. In *NeurIPS*, 2024.
- [53] Renxi Wang, Xudong Han, Lei Ji, Shu Wang, Timothy Baldwin, and Haonan Li. Toolgen: Unified tool retrieval and calling via generation. In *ICLR*. OpenReview.net, 2025.
- [54] Yu Shang, Yu Li, Keyu Zhao, Likai Ma, Jiahe Liu, Fengli Xu, and Yong Li. Agentsquare: Automatic LLM agent search in modular design space. In *ICLR*. OpenReview.net, 2025.
- [55] Jenny Zhang, Shengran Hu, Cong Lu, Robert Lange, and Jeff Clune. Darwin Godel Machine: Open-Ended Evolution of Self-Improving Agents. *arXiv preprint arXiv:2505.22954*, 2025.
- [56] Changle Qu, Sunhao Dai, Xiaochi Wei, Hengyi Cai, Shuaiqiang Wang, Dawei Yin, Jun Xu, and Ji-Rong Wen. Towards completeness-oriented tool retrieval for large language models. In *CIKM*, pages 1930–1940. ACM, 2024.
- [57] Zhengliang Shi, Yuhang Wang, Lingyong Yan, Pengjie Ren, Shuaiqiang Wang, Dawei Yin, and Zhaochun Ren. Retrieval models aren't tool-savvy: Benchmarking tool retrieval for large language models. *CoRR*, abs/2503.01763, 2025.
- [58] Yuanhang Zheng, Peng Li, Wei Liu, Yang Liu, Jian Luan, and Bin Wang. Toolrank: Adaptive and hierarchy-aware reranking for tool retrieval. In *LREC/COLING*, pages 16263–16273. ELRA and ICCL, 2024.
- [59] Hang Gao and Yongfeng Zhang. PTR: precision-driven tool recommendation for large language models. *CoRR*, abs/2411.09613, 2024.
- [60] Kolby Nottingham, Bodhisattwa Prasad Majumder, Bhavana Dalvi Mishra, Sameer Singh, Peter Clark, and Roy Fox. Skill set optimization: Reinforcing language model behavior via transferable skills. In *ICML*. OpenReview.net, 2024.
- [61] Alexander Novikov, Ngân Vũ, Marvin Eisenberger, Emilien Dupont, Po-Sen Huang, Adam Zsolt Wagner, Sergey Shirobokov, Borislav Kozlovskii, Francisco JR Ruiz, Abbas Mehrabian, et al. Alphaevolve: A coding agent for scientific and algorithmic discovery. *arXiv preprint arXiv:2506.13131*, 2025.
- [62] Guanghui Zhang, Kang Chen, Guohao Wan, Hao Chang, Hao Cheng, et al. Evoflow: Evolving diverse agentic workflows on the fly. *arXiv preprint arXiv:2502.07373*, 2025.
- [63] Han Zhou, Xingchen Wan, Ruoxi Sun, Hamid Palangi, Shariq Iqbal, Ivan Vulić, Anna Korhonen, and Sercan Ö. Arik. Multi-agent design: Optimizing agents with better prompts and topologies, 2025.
- [64] Jiayi Zhang, Jinyu Xiang, Zhaoyang Yu, Fengwei Teng, Xionghui Chen, Jiaqi Chen, Mingchen Zhuge, Xin Cheng, Sirui Hong, Jinlin Wang, et al. Aflow: Automating agentic workflow generation. *arXiv preprint arXiv:2410.10762*, 2024.
- [65] Shengran Hu, Cong Lu, and Jeff Clune. Automated design of agentic systems. *arXiv preprint arXiv:2408.08435*, 2024.
- [66] Zelong Li, Shuyuan Xu, Kai Mei, Wenyue Hua, Balaji Rama, Om Raheja, Hao Wang, He Zhu, and Yongfeng Zhang. Autoflow: Automated workflow generation for large language model agents. *arXiv preprint arXiv:2407.12821*, 2024.
- [67] Mingchen Zhuge, Wenyi Wang, Louis Kirsch, Francesco Faccio, Dmitrii Khizbulin, and Jürgen Schmidhuber. Gptswarm: Language agents as optimizable graphs. In *ICML*. OpenReview.net, 2024.
- [68] Yinjie Wang, Ling Yang, Guohao Li, Mengdi Wang, and Bryon Aragam. Scoreflow: Mastering LLM agent workflows via score-based preference optimization. *arXiv preprint arXiv:2502.04306*, 2025.
- [69] Hongcheng Gao, Yue Liu, Yufei He, Longxu Dou, Chao Du, Zhijie Deng, Bryan Hooi, Min Lin, and Tianyu Pang. Flowreasoner: Reinforcing query-level meta-agents. *arXiv preprint arXiv:2504.15257*, 2025.
- [70] Ziyu Wan, Yunxiang Li, Xiaoyu Wen, Yan Song, Hanjing Wang, Linyi Yang, Mark Schmidt, Jun Wang, Weinan Zhang, Shuyue Hu, and Ying Wen. Rema: Learning to meta-think for llms with multi-agent reinforcement learning, 2025.
- [71] Lang Feng, Zhenghai Xue, Tingcong Liu, and Bo An. Group-in-group policy optimization for llm agent training, 2025.

- [72] Aman Madaan, Niket Tandon, Prakhar Gupta, Skyler Hallinan, Luyu Gao, Sarah Wiegreffe, Uri Alon, Nouha Dziri, Shrimai Prabhumoye, Yiming Yang, Shashank Gupta, Bodhisattwa Prasad Majumder, Katherine Hermann, Sean Welleck, Amir Yazdanbakhsh, and Peter Clark. Self-Refine: Iterative refinement with self-feedback. In *Advances in Neural Information Processing Systems*, 2023.
- [73] Wenyue Hua, Xianjun Yang, Mingyu Jin, Zelong Li, Wei Cheng, Ruixiang Tang, and Yongfeng Zhang. Trustagent: Towards safe and trustworthy llm-based agents through agent constitution. In *Trustworthy Multi-modal Foundation Models and AI Agents (TiFA)*, 2024.
- [74] Adam Zweiger, Jyothish Pari, Han Guo, Ekin Akyürek, Yoon Kim, and Pulkit Agrawal. Self-adapting language models. *arXiv preprint arXiv:2506.10943*, 2025.
- [75] Moritz Hardt and Yu Sun. Test-time training on nearest neighbors for large language models. *arXiv preprint arXiv:2305.18466*, 2023.
- [76] Jonas Hübotter, Sascha Bongni, Ido Hakimi, and Andreas Krause. Efficiently learning at test-time: Active fine-tuning of llms. *arXiv preprint arXiv:2410.08020*, 2024.
- [77] Toby Simonds and Akira Yoshiyama. Ladder: Self-improving llms through recursive problem decomposition. *arXiv preprint arXiv:2503.00735*, 2025.
- [78] Yuxin Zuo, Kaiyan Zhang, Li Sheng, Shang Qu, Ganqu Cui, Xuekai Zhu, Haozhan Li, Yuchen Zhang, Xinwei Long, Ermo Hua, et al. Ttrl: Test-time reinforcement learning. *arXiv preprint arXiv:2504.16084*, 2025.
- [79] Eric Zelikman, Yuhuai Wu, Jesse Mu, and Noah Goodman. Star: Bootstrapping reasoning with reasoning. *Advances in Neural Information Processing Systems*, 35:15476–15488, 2022.
- [80] Eric Zelikman, Georges Harik, Yijia Shao, Varuna Jayasiri, Nick Haber, and Noah D Goodman. Quiet-star: Language models can teach themselves to think before speaking. *arXiv preprint arXiv:2403.09629*, 2024.
- [81] Wanjia Zhao, Mert Yuksekgonul, Shirley Wu, and James Zou. Sirius: Self-improving multi-agent systems via bootstrapped reasoning. *arXiv preprint arXiv:2502.04780*, 2025.
- [82] Hardy Chen, Haoqin Tu, Fali Wang, Hui Liu, Xianfeng Tang, Xinya Du, Yuyin Zhou, and Cihang Xie. Sft or rl? an early investigation into training r1-like reasoning large vision-language models. *arXiv preprint arXiv:2504.11468*, 2025.
- [83] Enci Zhang, Xingang Yan, Wei Lin, Tianxiang Zhang, and Qianchun Lu. Learning like humans: Advancing llm reasoning capabilities via adaptive difficulty curriculum learning and expert-guided self-reformulation. *arXiv preprint arXiv:2505.08364*, 2025.
- [84] Zehan Qi, Xiao Liu, Iat Long Iong, Hanyu Lai, Xueqiao Sun, Jiadai Sun, Xinyue Yang, Yu Yang, Shuntian Yao, Wei Xu, Jie Tang, and Yuxiao Dong. Webrl: Training llm web agents via self-evolving online curriculum reinforcement learning. *arXiv preprint arXiv:2411.02337*, 2024.
- [85] Hao Bai, Yifei Zhou, Jiayi Pan, Mert Cemri, Alane Suhr, Sergey Levine, and Aviral Kumar. Digirl: Training in-the-wild device-control agents with autonomous reinforcement learning. *Advances in Neural Information Processing Systems*, 37:12461–12495, 2024.
- [86] Saaket Agashe, Kyle Wong, Vincent Tu, Jiachen Yang, Ang Li, and Xin Eric Wang. Agent S2: A compositional generalist-specialist framework for computer use agents. *arXiv preprint arXiv:2504.00906*, 2025.
- [87] Amir Taubenfeld, Tom Sheffer, Eran Ofek, Amir Feder, Ariel Goldstein, Zorik Gekhman, and Gal Yona. Confidence improves self-consistency in llms. *arXiv preprint arXiv:2502.06233*, 2025.
- [88] Zicheng Xu, Guanchu Wang, Guangyao Zheng, Yu-Neng Chuang, Alexander Szalay, Xia Hu, and Vladimir Braverman. Self-ensemble: Mitigating confidence distortion for large language models, 2025.
- [89] Zhewei Kang, Xuandong Zhao, and Dawn Song. Scalable best-of-n selection for large language models via self-certainty, 2025.
- [90] Weizhe Yuan, Richard Yuanzhe Pang, Kyunghyun Cho, Xian Li, Sainbayar Sukhbaatar, Jing Xu, and Jason Weston. Self-rewarding language models, 2025.
- [91] Sheikh Shafayat, Fahim Tajwar, Ruslan Salakhutdinov, Jeff Schneider, and Andrea Zanette. Can large reasoning models self-train?, 2025.
- [92] Lai Wei, Yuting Li, Chen Wang, Yue Wang, Linghe Kong, Weiran Huang, and Lichao Sun. Unsupervised post-training for multi-modal llm reasoning via grpo, 2025.
- [93] Kongcheng Zhang, Qi Yao, Shunyu Liu, Yingjie Wang, Baisheng Lai, Jieping Ye, Mingli Song, and Dacheng Tao. Consistent paths lead to truth: Self-rewarding reinforcement learning for llm reasoning, 2025.

- [94] Yixin Du, Yuzhu Cai, Yifan Zhou, Cheng Wang, Yu Qian, Xianghe Pang, Qian Liu, Yue Hu, and Siheng Chen. Swe-dev: Evaluating and training autonomous feature-driven software development, 2025.
- [95] Maxime Robeyns, Martin Szummer, and Laurence Aitchison. A self-improving coding agent. *arXiv preprint arXiv:2504.15228*, 2025.
- [96] Dongwei Jiang, Alvin Zhang, Andrew Wang, Nicholas Andrews, and Daniel Khashabi. Feedback friction: Llms struggle to fully incorporate external feedback. *arXiv preprint arXiv:2506.11930*, 2025.
- [97] Leonhard Applis, Yuntong Zhang, Shanchao Liang, Nan Jiang, Lin Tan, and Abhik Roychoudhury. Unified software engineering agent as ai software engineer. *arXiv preprint arXiv:2506.14683*, 2025.
- [98] Hongru Wang, Cheng Qian, Jiahao Qiu, et al. OTC-PO: Optimal tool calls via reinforcement learning. *arXiv preprint arXiv:2504.14870*, 2025.
- [99] Bo Liu, Leon Guertler, Simon Yu, Zichen Liu, Penghui Qi, Daniel Balcells, Mickel Liu, Cheston Tan, Weiyan Shi, Min Lin, et al. Spiral: Self-play on zero-sum games incentivizes reasoning via multi-agent multi-turn reinforcement learning. *arXiv preprint arXiv:2506.24119*, 2025.
- [100] Kefan Song, Amir Moeini, Peng Wang, Lei Gong, Rohan Chandra, Yanjun Qi, and Shangtong Zhang. Reward is enough: Llms are in-context reinforcement learners. *arXiv preprint arXiv:2506.06303*, 2025.
- [101] Yi-Chen Li, Tian Xu, Yang Yu, Xuqin Zhang, Xiong-Hui Chen, Zhongxiang Ling, Ningjing Chao, Lei Yuan, and Zhi-Hua Zhou. Generalist reward models: Found inside large language models. *arXiv preprint arXiv:2506.23235*, 2025.
- [102] Arian Hosseini, Xingdi Yuan, Nikolay Malkin, Aaron Courville, Alessandro Sordoni, and Rishabh Agarwal. V-star: Training verifiers for self-taught reasoners. *arXiv preprint arXiv:2402.06457*, 2024.
- [103] Woosung Koh, Wonbeen Oh, Jaein Jang, MinHyung Lee, Hyeongjin Kim, Ah Yeon Kim, Joonkee Kim, Junghyun Lee, Taehyeon Kim, and Se-Young Yun. Adastar: Adaptive data sampling for training self-taught reasoners. *arXiv preprint arXiv:2505.16322*, 2025.
- [104] Yihe Deng, Pan Lu, Fan Yin, Ziniu Hu, Sheng Shen, Quanquan Gu, James Y Zou, Kai-Wei Chang, and Wei Wang. Enhancing large vision language models with self-training on image comprehension. *Advances in Neural Information Processing Systems*, 37:131369–131397, 2024.
- [105] Henry Hengyuan Zhao, Pan Zhou, and Mike Zheng Shou. Genixer: Empowering multimodal large language model as a powerful data generator. In *European Conference on Computer Vision*, pages 129–147. Springer, 2024.
- [106] Heng Tang, Feng Liu, Xinbo Chen, Jiawei Chen, Bohao Wang, Changwang Zhang, Jun Wang, Yuegang Sun, Bingde Hu, and Can Wang. Bridging the gap: Self-optimized fine-tuning for llm-based recommender systems. *arXiv preprint arXiv:2505.20771*, 2025.
- [107] Yuxiao Qu, Tianjun Zhang, Naman Garg, and Aviral Kumar. Recursive introspection: Teaching language model agents how to self-improve. *Advances in Neural Information Processing Systems*, 37:55249–55285, 2024.
- [108] Loka Li, Zhenhao Chen, Guangyi Chen, Yixuan Zhang, Yusheng Su, Eric Xing, and Kun Zhang. Confidence matters: Revisiting intrinsic self-correction capabilities of large language models. *arXiv preprint arXiv:2402.12563*, 2024.
- [109] Yiqun Zhang, Peng Ye, Xiaocui Yang, Shi Feng, Shufei Zhang, Lei Bai, Wanli Ouyang, and Shuyue Hu. Nature-inspired population-based evolution of large language models. *arXiv preprint arXiv:2503.01155*, 2025.
- [110] Zixiang Chen, Yihe Deng, Huizhuo Yuan, Kaixuan Ji, and Quanquan Gu. Self-play fine-tuning converts weak language models to strong language models. *arXiv preprint arXiv:2401.01335*, 2024.
- [111] Jiaqi Chen, Bang Zhang, Ruotian Ma, Peisong Wang, Xiaodan Liang, Zhaopeng Tu, Xiaolong Li, and Kwan-Yee K Wong. Spc: Evolving self-play critic via adversarial games for llm reasoning. *arXiv preprint arXiv:2504.19162*, 2025.
- [112] Ethan Mendes and Alan Ritter. Language models can self-improve at state-value estimation for better search. *arXiv preprint arXiv:2503.02878*, 2025.
- [113] Yue Hu, Yuzhu Cai, Yixin Du, Xinyu Zhu, Xiangrui Liu, Zijie Yu, Yuchen Hou, Shuo Tang, and Siheng Chen. Self-evolving multi-agent collaboration networks for software development. *arXiv preprint arXiv:2410.16946*, 2024.
- [114] Yufan Dang, Chen Qian, Xueheng Luo, Jingru Fan, Zihao Xie, Ruijie Shi, Weize Chen, Cheng Yang, Xiaoyin Che, Ye Tian, et al. Multi-agent collaboration via evolving orchestration. *arXiv preprint arXiv:2505.19591*, 2025.

- [115] Kai Chen, Ji Qi, Jing Huo, Pinzhuo Tian, Fanyu Meng, Xi Yang, and Yang Gao. A self-evolving framework for multi-agent medical consultation based on large language models. In ICASSP 2025-2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 1–5. IEEE, 2025.
- [116] Mohammad Almansoori, Komal Kumar, and Hisham Cholakkal. Self-evolving multi-agent simulations for realistic clinical interactions. arXiv preprint arXiv:2503.22678, 2025.
- [117] Zhenhailong Wang, Haiyang Xu, Junyang Wang, Xi Zhang, Ming Yan, Ji Zhang, Fei Huang, and Heng Ji. Mobile-agent-e: Self-evolving mobile assistant for complex tasks. arXiv preprint arXiv:2501.11733, 2025.
- [118] Yuxuan Liu, Hongda Sun, Wei Liu, Jian Luan, Bo Du, and Rui Yan. Mobilesteward: Integrating multiple app-oriented agents with self-evolution to automate cross-app instructions. arXiv preprint arXiv:2502.16796, 2025.
- [119] Tianqing Fang, Hongming Zhang, Zhisong Zhang, Kaixin Ma, Wenhao Yu, Haitao Mi, and Dong Yu. Webevolver: Enhancing web agent self-improvement with coevolving world model. arXiv preprint arXiv:2504.21024, 2025.
- [120] Han Xiao, Guozhi Wang, Yuxiang Chai, Zimu Lu, Weifeng Lin, Hao He, Lue Fan, Liuyang Bian, Rui Hu, Liang Liu, et al. Ui-genie: A self-improving approach for iteratively boosting mllm-based mobile gui agents. arXiv preprint arXiv:2505.21496, 2025.
- [121] Andrew Zhao, Yiran Wu, Yang Yue, Tong Wu, Quentin Xu, Matthieu Lin, Shenzhi Wang, Qingyun Wu, Zilong Zheng, and Gao Huang. Absolute zero: Reinforced self-play reasoning with zero data. arXiv preprint arXiv:2505.03335, 2025.
- [122] Saizhuo Wang, Hang Yuan, Lionel M Ni, and Jian Guo. Quantagent: Seeking holy grail in trading by self-improving large language model. arXiv preprint arXiv:2402.03755, 2024.
- [123] Guanyu Lin, Tao Feng, Pengrui Han, Ge Liu, and Jiaxuan You. Arxiv copilot: A self-evolving and efficient LLM system for personalized academic assistance. In Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: System Demonstrations, pages 122–130, 2024. arXiv:2409.04593.
- [124] Yoshua Bengio, Jérôme Louradour, Ronan Collobert, and Jason Weston. Curriculum learning. In Proceedings of the 26th annual international conference on machine learning, pages 41–48, 2009.
- [125] Xin Wang, Yudong Chen, and Wenwu Zhu. A survey on curriculum learning. IEEE transactions on pattern analysis and machine intelligence, 44(9):4555–4576, 2021.
- [126] Sheng Guo, Weilin Huang, Haozhi Zhang, Chenfan Zhuang, Dengke Dong, Matthew R Scott, and Dinglong Huang. Curriculumnet: Weakly supervised learning from large-scale web images. In Proceedings of the European conference on computer vision (ECCV), pages 135–150, 2018.
- [127] Lu Jiang, Deyu Meng, Teruko Mitamura, and Alexander G Hauptmann. Easy samples first: Self-paced reranking for zero-example multimedia search. In Proceedings of the 22nd ACM international conference on Multimedia, pages 547–556, 2014.
- [128] Dongrui Liu, Huiqi Deng, Xu Cheng, Qihan Ren, Kangrui Wang, and Quanshi Zhang. Towards the difficulty for a deep neural network to learn concepts of different complexities. Advances in Neural Information Processing Systems, 36:41283–41304, 2023.
- [129] Emmanouil Antonios Platanios, Otilia Stretcu, Graham Neubig, Barnabas Poczos, and Tom M Mitchell. Competence-based curriculum learning for neural machine translation. arXiv preprint arXiv:1903.09848, 2019.
- [130] Yi Tay, Shuhang Wang, Luu Anh Tuan, Jie Fu, Minh C Phan, Xingdi Yuan, Jinfeng Rao, Siu Cheung Hui, and Aston Zhang. Simple and effective curriculum pointer-generator networks for reading comprehension over long narratives. arXiv preprint arXiv:1905.10847, 2019.
- [131] Stefan Braun, Daniel Neil, and Shih-Chii Liu. A curriculum learning method for improved noise robustness in automatic speech recognition. In 2017 25th European Signal Processing Conference (EUSIPCO), pages 548–552. IEEE, 2017.
- [132] Reza Lotfian and Carlos Busso. Curriculum learning for speech emotion recognition from crowdsourced labels. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 27(4):815–826, 2019.
- [133] Zhenting Wang, Guofeng Cui, Kun Wan, and Wentian Zhao. Dump: Automated distribution-level curriculum learning for rl-based llm post-training. arXiv preprint arXiv:2504.09710, 2025.
- [134] Xuemiao Zhang, Liangyu Xu, Feiyu Duan, Yongwei Zhou, Sirui Wang, Rongxiang Weng, Jingang Wang, and Xunliang Cai. Preference curriculum: Llms should always be pretrained on their preferred data. arXiv preprint arXiv:2501.13126, 2025.

- [135] Shubham Parashar, Shurui Gui, Xiner Li, Hongyi Ling, Sushil Vemuri, Blake Olson, Eric Li, Yu Zhang, James Caverlee, Dileep Kalathil, et al. Curriculum reinforcement learning from easy to hard tasks improves llm reasoning. [arXiv preprint arXiv:2506.06632](#), 2025.
- [136] Mengdi Li, Jiaye Lin, Xufeng Zhao, Wenhao Lu, Peilin Zhao, Stefan Wermter, and Di Wang. Curriculum-rlaif: Curriculum alignment with reinforcement learning from ai feedback. [arXiv preprint arXiv:2505.20075](#), 2025.
- [137] Liyuan Wang, Xingxing Zhang, Hang Su, and Jun Zhu. A comprehensive survey of continual learning: Theory, method and application. [IEEE transactions on pattern analysis and machine intelligence](#), 46(8):5362–5383, 2024.
- [138] Junhao Zheng, Chengming Shi, Xidi Cai, Qiuke Li, Duzhen Zhang, Chenxing Li, Dong Yu, and Qianli Ma. Lifelong learning of large language model based agents: A roadmap. [arXiv preprint arXiv:2501.07278](#), 2025.
- [139] German I Parisi, Ronald Kemker, Jose L Part, Christopher Kanan, and Stefan Wermter. Continual lifelong learning with neural networks: A review. [Neural networks](#), 113:54–71, 2019.
- [140] Haizhou Shi, Zihao Xu, Hengyi Wang, Weiyi Qin, Wenyuan Wang, Yibin Wang, Zifeng Wang, Sayna Ebrahimi, and Hao Wang. Continual learning of large language models: A comprehensive survey. [ACM Computing Surveys](#), 2024.
- [141] Yutao Yang, Jie Zhou, Xuanwen Ding, Tianyu Huai, Shunyu Liu, Qin Chen, Yuan Xie, and Liang He. Recent advances of foundation language models-based continual learning: A survey. [ACM Computing Surveys](#), 57(5):1–38, 2025.
- [142] Da-Wei Zhou, Hai-Long Sun, Jingyi Ning, Han-Jia Ye, and De-Chuan Zhan. Continual learning with pre-trained models: A survey. [arXiv preprint arXiv:2401.16386](#), 2024.
- [143] Michael McCloskey and Neal J Cohen. Catastrophic interference in connectionist networks: The sequential learning problem. In [Psychology of learning and motivation](#), volume 24, pages 109–165. Elsevier, 1989.
- [144] Roger Ratcliff. Connectionist models of recognition memory: constraints imposed by learning and forgetting functions. [Psychological review](#), 97(2):285, 1990.
- [145] David Rolnick, Arun Ahuja, Jonathan Schwarz, Timothy Lillicrap, and Gregory Wayne. Experience replay for continual learning. [Advances in neural information processing systems](#), 32, 2019.
- [146] Song Wang, Yaochen Zhu, Haochen Liu, Zaiyi Zheng, Chen Chen, and Jundong Li. Knowledge editing for large language models: A survey. [ACM Computing Surveys](#), 57(3):1–37, 2024.
- [147] Kun Wang, Guibin Zhang, Zhenhong Zhou, Jiahao Wu, Miao Yu, Shiqian Zhao, Chenlong Yin, Jinhu Fu, Yibo Yan, Hanjun Luo, et al. A comprehensive survey in llm (-agent) full stack safety: Data, training and deployment. [arXiv preprint arXiv:2504.15585](#), 2025.
- [148] Ningyu Zhang, Yunzhi Yao, Bozhong Tian, Peng Wang, Shumin Deng, Mengru Wang, Zekun Xi, Shengyu Mao, Jintian Zhang, Yuansheng Ni, et al. A comprehensive study of knowledge editing for large language models. [arXiv preprint arXiv:2401.01286](#), 2024.
- [149] Thanh Tam Nguyen, Thanh Trung Huynh, Zhao Ren, Phi Le Nguyen, Alan Wee-Chung Liew, Hongzhi Yin, and Quoc Viet Hung Nguyen. A survey of machine unlearning. [arXiv preprint arXiv:2209.02299](#), 2022.
- [150] Jiahui Geng, Qing Li, Herbert Woisetschlaeger, Zongxiong Chen, Fengyu Cai, Yuxia Wang, Preslav Nakov, Hans-Arno Jacobsen, and Fakhri Karray. A comprehensive survey of machine unlearning techniques for large language models. [arXiv preprint arXiv:2503.01854](#), 2025.
- [151] Junfeng Fang, Houcheng Jiang, Kun Wang, Yunshan Ma, Jie Shi, Xiang Wang, Xiangnan He, and Tat-Seng Chua. Alphaedit: Null-space constrained model editing for language models. In [The Thirteenth International Conference on Learning Representations](#), 2025.
- [152] Baixiang Huang, Zhen Tan, Haoran Wang, Zijie Liu, Dawei Li, Ali Payani, Huan Liu, Tianlong Chen, and Kai Shu. Model editing as a double-edged sword: Steering agent ethical behavior toward beneficence or harm. [arXiv preprint arXiv:2506.20606](#), 2025.
- [153] Qizhou Chen, Taolin Zhang, Xiaofeng He, Dongyang Li, Chengyu Wang, Longtao Huang, and Hui Xue. Lifelong knowledge editing for llms with retrieval-augmented continuous prompt learning. [arXiv preprint arXiv:2405.03279](#), 2024.
- [154] Min Chen, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert, and Yang Zhang. When machine unlearning jeopardizes privacy. In [Proceedings of the 2021 ACM SIGSAC conference on computer and communications security](#), pages 896–911, 2021.

- [155] Zhixin Zhang, Junxiao Yang, Pei Ke, Shiyao Cui, Chujie Zheng, Hongning Wang, and Minlie Huang. Safe unlearning: A surprisingly effective and generalizable solution to defend against jailbreak attacks. [arXiv preprint arXiv:2407.02855](#), 2024.
- [156] Nathaniel Li, Alexander Pan, Anjali Gopal, Summer Yue, Daniel Berrios, Alice Gatti, Justin D Li, Ann-Kathrin Dombrowski, Shashwat Goel, Long Phan, et al. The wmdp benchmark: Measuring and reducing malicious use with unlearning. [arXiv preprint arXiv:2403.03218](#), 2024.
- [157] Andy Zou, Long Phan, Justin Wang, Derek Duenas, Maxwell Lin, Maksym Andriushchenko, J Zico Kolter, Matt Fredrikson, and Dan Hendrycks. Improving alignment and robustness with circuit breakers. In [The Thirty-eighth Annual Conference on Neural Information Processing Systems](#), 2024.
- [158] Xiaoya Lu, Dongrui Liu, Yi Yu, Luxin Xu, and Jing Shao. X-boundary: Establishing exact safety boundary to shield llms from multi-turn jailbreaks without compromising usability. [arXiv preprint arXiv:2502.09990](#), 2025.
- [159] Zixuan Ke, Austin Xu, Yifei Ming, Xuan-Phi Nguyen, Caiming Xiong, and Shafiq Joty. Mas-zero: Designing multi-agent systems with zero supervision, 2025.
- [160] Lianlei Shan, Shixian Luo, Zezhou Zhu, Yu Yuan, and Yong Wu. Cognitive memory in large language models. [arXiv preprint arXiv:2504.02441](#), 2025.
- [161] Chen Qian, Yufan Dang, Jiahao Li, Wei Liu, Zihao Xie, Yifei Wang, Weize Chen, Cheng Yang, Xin Cong, Xiaoyin Che, et al. Experiential co-learning of software-developing agents. [arXiv preprint arXiv:2312.17025](#), 2023.
- [162] Wanjun Zhong, Lianghong Guo, Qiqi Gao, He Ye, and Yanlin Wang. Memorybank: Enhancing large language models with long-term memory. In [Proceedings of the AAAI Conference on Artificial Intelligence](#), volume 38, pages 19724–19731, 2024.
- [163] Guibin Zhang, Muxin Fu, Guancheng Wan, Miao Yu, Kun Wang, and Shuicheng Yan. G-memory: Tracing hierarchical memory for multi-agent systems. [arXiv preprint arXiv:2506.07398](#), 2025.
- [164] Cilin Yan, Jingyun Wang, Lin Zhang, Ruihui Zhao, Xiaopu Wu, Kai Xiong, Qingsong Liu, Guoliang Kang, and Yangyang Kang. Efficient and accurate prompt optimization: the benefit of memory in exemplar-guided reflection. [arXiv preprint arXiv:2411.07446](#), 2024.
- [165] Wujiang Xu, Kai Mei, Hang Gao, Juntao Tan, Zujie Liang, and Yongfeng Zhang. A-mem: Agentic memory for llm agents. [arXiv preprint arXiv:2502.12110](#), 2025.
- [166] Yao Fu, Dong-Ki Kim, Jaekyeom Kim, Sungryull Sohn, Lajanugen Logeswaran, Kyunghoon Bae, and Honglak Lee. Autoguide: Automated generation and selection of state-aware guidelines for large language model agents. [arXiv e-prints](#), pages arXiv–2403, 2024.
- [167] Kiran Ramnath, Kang Zhou, Sheng Guan, Soumya Smruti Mishra, Xuan Qi, Zhengyuan Shen, Shuai Wang, Sangmin Woo, Sullam Jeoung, Yawei Wang, et al. A systematic survey of automatic prompt optimization techniques. [arXiv preprint arXiv:2502.16923](#), 2025.
- [168] Sam Lin, Wenyue Hua, Lingyao Li, Zhenting Wang, and Yongfeng Zhang. Ado: Automatic data optimization for inputs in llm prompts. [arXiv preprint arXiv:2502.11436](#), 2025.
- [169] Bang Liu, Xinfeng Li, Jiayi Zhang, Jinlin Wang, Tanjin He, Sirui Hong, Hongzhang Liu, Shaokun Zhang, Kaitao Song, Kunlun Zhu, et al. Advances and challenges in foundation agents: From brain-inspired intelligence to evolutionary, collaborative, and safe systems. [arXiv preprint arXiv:2504.01990](#), 2025.
- [170] Rui Ye, Xiangru Liu, Qingyun Wu, Xinyuan Pang, Zhaopeng Yin, Lu Bai, et al. X-mas: Towards building multi-agent systems with heterogeneous llms. [arXiv preprint arXiv:2505.16997](#), 2025.
- [171] Wangchunshu Zhou, Yixin Ou, Shengwei Ding, Long Li, Jialong Wu, Tiannan Wang, Jiamin Chen, Shuai Wang, Xiaohua Xu, Ningyu Zhang, et al. Symbolic learning enables self-evolving agents. [arXiv preprint arXiv:2406.18532](#), 2024.
- [172] Guanghui Zhang, Li Niu, Jianwei Fang, Kun Wang, Lu Bai, et al. Multi-agent architecture search via agentic supernet. [arXiv preprint arXiv:2502.04180](#), 2025.
- [173] Rui Ye et al. Mas-gpt: Training llms to build llm-based multi-agent systems. [arXiv preprint](#), 2025.
- [174] Patara Trirat, Wonyong Jeong, and Sung Ju Hwang. Agentic predictor: Performance prediction for agentic workflows via multi-view encoding. [arXiv preprint arXiv:2505.19764](#), 2025.
- [175] Yuanshuo Zhang, Yuchen Hou, Bohan Tang, Shuo Chen, Muhan Zhang, Xiaowen Dong, and Siheng Chen. Gnn as predictors of agentic workflow performances. [arXiv preprint arXiv:2503.11301](#), 2025.
- [176] Junwei Liao, Muning Wen, Jun Wang, and Weinan Zhang. Marft: Multi-agent reinforcement fine-tuning, 2025.

- [177] Zhiheng Xi, Dingwen Yang, Jixuan Huang, Jiafu Tang, Guanyu Li, Yiwen Ding, Wei He, Boyang Hong, Shihan Do, Wenyu Zhan, et al. Enhancing llm reasoning via critique models with test-time and training-time supervision. *arXiv preprint arXiv:2411.16579*, 2024.
- [178] Zhenni Bi, Kai Han, Chuanjian Liu, Yehui Tang, and Yunhe Wang. Forest-of-thought: Scaling test-time compute for enhancing llm reasoning. *arXiv preprint arXiv:2412.09078*, 2024.
- [179] Lang Qian, Peng Sun, Yilei Wang, Jiayue Jin, Azzedine Boukerche, and Liang Song. A new online evolutive optimization method for driving agents. In *GLOBECOM 2024-2024 IEEE Global Communications Conference*, pages 2244–2249. IEEE, 2024.
- [180] Qingxiu Dong, Lei Li, Damai Dai, Ce Zheng, Jingyuan Ma, Rui Li, Heming Xia, Jingjing Xu, Zhiyong Wu, Tianyu Liu, et al. A survey on in-context learning. *arXiv preprint arXiv:2301.00234*, 2022.
- [181] Sewon Min, Mike Lewis, Luke Zettlemoyer, and Hannaneh Hajishirzi. Metaicl: Learning to learn in context. *arXiv preprint arXiv:2110.15943*, 2021.
- [182] Noam Wies, Yoav Levine, and Amnon Shashua. The learnability of in-context learning. *Advances in Neural Information Processing Systems*, 36:36637–36651, 2023.
- [183] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Bidirectional encoder representations from transformers. *arXiv preprint arXiv:1810.04805*, 15, 2018.
- [184] Ming Shen. Rethinking data selection for supervised fine-tuning. *arXiv preprint arXiv:2402.06094*, 2024.
- [185] Guanting Dong, Hongyi Yuan, Keming Lu, Chengpeng Li, Mingfeng Xue, Dayiheng Liu, Wei Wang, Zheng Yuan, Chang Zhou, and Jingren Zhou. How abilities in large language models are affected by supervised fine-tuning data composition. *arXiv preprint arXiv:2310.05492*, 2023.
- [186] Leslie Pack Kaelbling, Michael L Littman, and Andrew W Moore. Reinforcement learning: A survey. *Journal of artificial intelligence research*, 4:237–285, 1996.
- [187] Chuanneng Sun, Songjun Huang, and Dario Pompili. Llm-based multi-agent reinforcement learning: Current and future directions. *arXiv preprint arXiv:2405.11106*, 2024.
- [188] Shaokun Zhang, Yi Dong, Jieyu Zhang, Jan Kautz, Bryan Catanzaro, Andrew Tao, Qingyun Wu, Zhiding Yu, and Guilin Liu. Nemotron-research-tool-n1: Exploring tool-using language models with reinforced reasoning. *arXiv preprint arXiv:2505.00024*, 2025.
- [189] Jiaxuan Gao, Shusheng Xu, Wenjie Ye, Weilin Liu, Chuyi He, Wei Fu, Zhiyu Mei, Guangju Wang, and Yi Wu. On designing effective rl reward at training time for llm reasoning. *arXiv preprint arXiv:2410.15115*, 2024.
- [190] Shun-ichi Amari. Backpropagation and stochastic gradient descent method. *Neurocomputing*, 5(4-5):185–196, 1993.
- [191] Léon Bottou. Large-scale machine learning with stochastic gradient descent. In *Proceedings of COMPSTAT'2010: 19th International Conference on Computational StatisticsParis France, August 22-27, 2010 Keynote, Invited and Contributed Papers*, pages 177–186. Springer, 2010.
- [192] Yingqiang Ge, Wenyue Hua, Kai Mei, Juntao Tan, Shuyuan Xu, Zelong Li, Yongfeng Zhang, et al. Openagi: When llm meets domain experts. *Advances in Neural Information Processing Systems*, 36:5539–5568, 2023.
- [193] Amir Moeini, Jiuqi Wang, Jacob Beck, Ethan Blaser, Shimon Whiteson, Rohan Chandra, and Shangtong Zhang. A survey of in-context reinforcement learning. *arXiv preprint arXiv:2502.07978*, 2025.
- [194] Michael Laskin, Luyu Wang, Junhyuk Oh, Emilio Parisotto, Stephen Spencer, Richie Steigerwald, DJ Strouse, Steven Hansen, Angelos Filos, Ethan Brooks, et al. In-context reinforcement learning with algorithm distillation. *arXiv preprint arXiv:2210.14215*, 2022.
- [195] Jonathan Lee, Annie Xie, Aldo Pacchiano, Yash Chandak, Chelsea Finn, Ofir Nachum, and Emma Brunskill. Supervised pretraining can learn in-context reinforcement learning. *Advances in Neural Information Processing Systems*, 36:43057–43083, 2023.
- [196] Louis Kirsch, James Harrison, Daniel Freeman, Jascha Sohl-Dickstein, and Jürgen Schmidhuber. Towards general-purpose in-context learning agents. *Workshop on Distribution Shifts, 37th Conference on Neural Information ...*, 2023.
- [197] Peiyi Wang, Lei Li, Zhihong Shao, RX Xu, Damai Dai, Yifei Li, Deli Chen, Yu Wu, and Zhifang Sui. Math-shepherd: Verify and reinforce llms step-by-step without human annotations. *arXiv preprint arXiv:2312.08935*, 2023.
- [198] Sanjiban Choudhury. Process reward models for llm agents: Practical framework and directions. *arXiv preprint arXiv:2502.10325*, 2025.

- [199] Pranav Putta, Edmund Mills, Naman Garg, Sumeet Motwani, Chelsea Finn, Divyansh Garg, and Rafael Rafailev. Agent q: Advanced reasoning and learning for autonomous ai agents. [arXiv preprint arXiv:2408.07199](#), 2024.
- [200] Lang Feng, Zhenghai Xue, Tingcong Liu, and Bo An. Group-in-group policy optimization for llm agent training. [arXiv preprint arXiv:2505.10978](#), 2025.
- [201] Hanlin Wang, Chak Tou Leong, Jiashuo Wang, Jian Wang, and Wenjie Li. Spa-rl: Reinforcing llm agents via stepwise progress attribution. [arXiv preprint arXiv:2505.20732](#), 2025.
- [202] Yizhong Wang, Yeganeh Kordi, Swaroop Mishra, Alisa Liu, Noah A Smith, Daniel Khashabi, and Hanneh Hajishirzi. Self-instruct: Aligning language models with self-generated instructions. [arXiv preprint arXiv:2212.10560](#), 2022.
- [203] Can Xu, Qingfeng Sun, Kai Zheng, Xiubo Geng, Pu Zhao, Jiazhan Feng, Chongyang Tao, Qingwei Lin, and Daxin Jiang. Wizardlm: Empowering large pre-trained language models to follow complex instructions. In [The Twelfth International Conference on Learning Representations](#), 2024.
- [204] Qiushi Sun, Kanzhi Cheng, Zichen Ding, Chuanyang Jin, Yian Wang, Fangzhi Xu, Zhenyu Wu, Chengyou Jia, Liheng Chen, Zhoumianze Liu, et al. Os-genesis: Automating gui agent trajectory construction via reverse task synthesis. [arXiv preprint arXiv:2412.19723](#), 2024.
- [205] Run Luo, Lu Wang, Wanwei He, and Xiaobo Xia. Gui-rl: A generalist rl-style vision-language action model for gui agents. [arXiv preprint arXiv:2504.10458](#), 2025.
- [206] Yuhang Liu, Pengxiang Li, Congkai Xie, Xavier Hu, Xiaotian Han, Shengyu Zhang, Hongxia Yang, and Fei Wu. Infigui-rl: Advancing multimodal gui agents from reactive actors to deliberative reasoners. [arXiv preprint arXiv:2504.14239](#), 2025.
- [207] Bill Yuchen Lin, Yicheng Fu, Karina Yang, Faeze Brahman, Shiyu Huang, Chandra Bhagavatula, Prithviraj Ammanabrolu, Yejin Choi, and Xiang Ren. Swiftsage: A generative agent with fast and slow thinking for complex interactive tasks. [Advances in Neural Information Processing Systems](#), 36:23813–23825, 2023.
- [208] Hanyu Lai, Xiao Liu, Iat Long Iong, Shuntian Yao, Yuxuan Chen, Pengbo Shen, Hao Yu, Hanchen Zhang, Xiaohan Zhang, Yuxiao Dong, et al. Autowebglm: A large language model-based web navigating agent. In [Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining](#), pages 5295–5306, 2024.
- [209] Hunter Lightman, Vineet Kosaraju, Yuri Burda, Harrison Edwards, Bowen Baker, Teddy Lee, Jan Leike, John Schulman, Ilya Sutskever, and Karl Cobbe. Let’s verify step by step. In [The Twelfth International Conference on Learning Representations](#), 2023.
- [210] Guoxin Chen, Minpeng Liao, Chengxi Li, and Kai Fan. Alphamath almost zero: process supervision without process. [arXiv preprint arXiv:2405.03553](#), 2024.
- [211] Xinyu Guan, Li Lyra Zhang, Yifei Liu, Ning Shang, Youran Sun, Yi Zhu, Fan Yang, and Mao Yang. rstar-math: Small llms can master math reasoning with self-evolved deep thinking. [arXiv preprint arXiv:2501.04519](#), 2025.
- [212] Taiyi Wang, Zhihao Wu, Jianheng Liu, Jianye Hao, Jun Wang, and Kun Shao. Distrl: An asynchronous distributed reinforcement learning framework for on-device control agents. [arXiv preprint arXiv:2410.14803](#), 2024.
- [213] Yucheng Shi, Wenhao Yu, Zaitang Li, Yonglin Wang, Hongming Zhang, Ninghao Liu, Haitao Mi, and Dong Yu. Mobilegui-rl: Advancing mobile gui agent through reinforcement learning in online environment, 2025.
- [214] Ziqi Wang, Le Hou, Tianjian Lu, Yuexin Wu, Yunxuan Li, Hongkun Yu, and Heng Ji. Enabling lanuguage models to implicitly learn self-improvement. In [The Twelfth International Conference on Learning Representations](#), 2024.
- [215] Daya Guo, Dejian Yang, Haowei Zhang, Junxiao Song, Ruoyu Zhang, Runxin Xu, Qihao Zhu, Shirong Ma, Peiyi Wang, Xiao Bi, et al. Deepseek-rl: Incentivizing reasoning capability in llms via reinforcement learning. [arXiv preprint arXiv:2501.12948](#), 2025.
- [216] Zhihong Shao, Peiyi Wang, Qihao Zhu, Runxin Xu, Junxiao Song, Xiao Bi, Haowei Zhang, Mingchuan Zhang, YK Li, Y Wu, et al. Deepseekmath: Pushing the limits of mathematical reasoning in open language models. [arXiv preprint arXiv:2402.03300](#), 2024.
- [217] Qiying Yu, Zheng Zhang, Ruofei Zhu, Yufeng Yuan, Xiaochen Zuo, Yu Yue, Weinan Dai, Tiantian Fan, Gaohong Liu, Lingjun Liu, et al. Dapo: An open-source llm reinforcement learning system at scale. [arXiv preprint arXiv:2503.14476](#), 2025.
- [218] Weizhe Yuan, Richard Yuanzhe Pang, Kyunghyun Cho, Xian Li, Sainbayar Sukhbaatar, Jing Xu, and Jason Weston. Self-rewarding language models. [arXiv preprint arXiv:2401.10020](#).

- [219] Zheng Yuan, Hongyi Yuan, Chuanqi Tan, Wei Wang, Songfang Huang, and Fei Huang. Rrhf: Rank responses to align language models with human feedback without tears. [arXiv preprint arXiv:2304.05302](#), 2023.
- [220] Rafael Rafailov, Archit Sharma, Eric Mitchell, Christopher D Manning, Stefano Ermon, and Chelsea Finn. Direct preference optimization: Your language model is secretly a reward model. [Advances in Neural Information Processing Systems](#), 36:53728–53741, 2023.
- [221] Shaokun Zhang, Jieyu Zhang, Jiale Liu, Linxin Song, Chi Wang, Ranjay Krishna, and Qingyun Wu. Offline training of language model agents with functions as learnable weights. In [Forty-first International Conference on Machine Learning](#), 2024.
- [222] Zeyu Zhang, Xiaohe Bo, Chen Ma, Rui Li, Xu Chen, Quanyu Dai, Jieming Zhu, Zhenhua Dong, and Ji-Rong Wen. A survey on the memory mechanism of large language model based agents. [arXiv preprint arXiv:2404.13501](#), 2024.
- [223] Joon Sung Park, Joseph O’Brien, Carrie Jun Cai, Meredith Ringel Morris, Percy Liang, and Michael S Bernstein. Generative agents: Interactive simulacra of human behavior. In [Proceedings of the 36th annual ACM symposium on user interface software and technology](#), pages 1–22, 2023.
- [224] D Huang, JM Zhang, M Luck, Q Bu, Y Qing, and H Cui. Agentcoder: Multi-agent code generation with effective testing and self-optimization. [University of Hong Kong, King's College London, University of Sussex, Shanghai Jiao Tong University](#), 2024.
- [225] Genghan Zhang, Weixin Liang, Olivia Hsu, and Kunle Olukotun. Adaptive self-improvement llm agentic system for ml library development. [arXiv preprint arXiv:2502.02534](#), 2025.
- [226] Xinbin Yuan, Jian Zhang, Kaixin Li, Zhuoxuan Cai, Lujian Yao, Jie Chen, Enguang Wang, Qibin Hou, Jinwei Chen, Peng-Tao Jiang, and Bo Li. Enhancing visual grounding for gui agents via self-evolutionary reinforcement learning. [arXiv preprint arXiv:2505.12370](#), 2025.
- [227] Rogerio Bonatti, Dan Zhao, Francesco Bonacci, Dillon Dupont, Sara Abdali, Yinheng Li, Yadong Lu, Justin Wagle, Kazuhito Koishida, et al. Windows Agent Arena: Evaluating multi-modal OS agents at scale. [arXiv preprint arXiv:2409.08264](#), 2024.
- [228] Hongliang He, Wenlin Yao, Kaixin Ma, Wenhao Yu, Yong Dai, Hongming Zhang, Zhenzhong Lan, and Dong Yu. WebVoyager: Building an end-to-end web agent with large multimodal models. [arXiv preprint arXiv:2401.13919](#), 2024.
- [229] Ruhana Azam, Aditya Vempaty, and Ashish Jagmohan. Reflection-augmented planning (ReAP): Memory for web navigation agents. [arXiv preprint arXiv:2506.02158](#), 2025.
- [230] Hongxin Li, Jingfan Chen, Jingran Su, Yuntao Chen, Qing Li, and Zhaoxiang Zhang. AutoGUI: Scaling gui grounding with automatic functionality annotations from LLMs. [arXiv preprint arXiv:2502.01977](#), 2025.
- [231] Ning Li, Xiangmou Qu, Jiamu Zhou, Jun Wang, Muning Wen, Kounianhua Du, Xingyu Lou, Qiuying Peng, Jun Wang, and Weinan Zhang. MobileUse: A gui agent with hierarchical reflection for autonomous mobile operation. [arXiv preprint arXiv:2507.16853](#), 2025.
- [232] Yijia Xiao, Edward Sun, Di Luo, and Wei Wang. Tradingagents: Multi-agents llm financial trading framework. [arXiv preprint arXiv:2412.20138](#), 2024.
- [233] Junkai Li, Yunghwei Lai, Weitao Li, Jingyi Ren, Meng Zhang, Xinhui Kang, Siyu Wang, Peng Li, Ya-Qin Zhang, Weizhi Ma, and Yang Liu. Agent hospital: A simulacrum of hospital with evolvable medical agents. [arXiv preprint arXiv:2405.02957](#), 2024.
- [234] Mohammad Almansoori, Komal Kumar, and Hisham Cholakkal. Self-evolving multi-agent simulations for realistic clinical interactions. [arXiv preprint arXiv:2503.22678](#), 2025.
- [235] Zhuoyun Du, Lujie Zheng, Renjun Hu, Yuyang Xu, Xiawei Li, Ying Sun, Wei Chen, Jian Wu, Haolei Cai, and Haohao Ying. Llms can simulate standardized patients via agent coevolution. [arXiv preprint arXiv:2412.11716](#), 2024.
- [236] Yichun Feng, Jiawei Wang, Lu Zhou, and Yixue Li. Doctoragent-rl: A multi-agent collaborative reinforcement learning system for multi-turn clinical dialogue. [arXiv preprint arXiv:2505.19630](#), 2025.
- [237] Yangyang Zhuang, Wenjia Jiang, Jiayu Zhang, Ze Yang, Joey Tianyi Zhou, and Chi Zhang. Learning to be a doctor: Searching for effective medical agent architectures. [arXiv preprint arXiv:2504.11301](#), 2025.
- [238] Zhongyue Zhang, Zijie Qiu, Yingcheng Wu, Shuya Li, Dingyan Wang, Zhuomin Zhou, Duo An, Yuhan Chen, Yu Li, Yongbo Wang, et al. Origene: A self-evolving virtual disease biologist automating therapeutic target discovery. [bioRxiv](#), pages 2025–06, 2025.

- [239] Ruofan Jin, Zaixi Zhang, Mengdi Wang, and Le Cong. Stella: Self-evolving LLM agent for biomedical research. [arXiv preprint arXiv:2507.02004](#), 2025.
- [240] Ben Liu, Jihan Zhang, Fangquan Lin, Xu Jia, and Min Peng. One size doesn't fit all: A personalized conversational tutoring agent for mathematics instruction. [arXiv preprint arXiv:2502.12633](#), 2025.
- [241] Murong Yue, Wenhan Lyu, Wijdane Mifdal, Jennifer Suh, Yixuan Zhang, and Ziyu Yao. Mathvc: An llm-simulated multi-character virtual classroom for mathematics education. [arXiv preprint arXiv:2404.06711](#), 2025.
- [242] Kaiqi Yang, Hang Li, Yucheng Chu, Ahreum Han, Yasemin Copur-Gencturk, Jiliang Tang, and Hui Liu. A llm-driven multi-agent systems for professional development of mathematics teachers. [arXiv preprint arXiv:2507.05292](#), 2025.
- [243] Xueqiao Zhang, Chao Zhang, Jianwen Sun, Jun Xiao, Yi Yang, and Yawei Luo. Eduplanner: Llm-based multi-agent systems for customized and intelligent instructional design. [arXiv preprint arXiv:2504.05370](#), 2025.
- [244] Mike Zhang, Amalie Pernille Dilling, Léon Gondelman, Niels Erik Ruan Lyngdorf, Euan D. Lindsay, and Johannes Bjerva. Sefl: Harnessing large language model agents to improve educational feedback systems. [arXiv preprint arXiv:2502.12927](#), 2025.
- [245] Nikolas Belle, Dakota Barnes, Alfonso Amayuelas, Ivan Bercovich, Xin Eric Wang, and William Wang. Agents of change: Self-evolving llm agents for strategic planning. [arXiv preprint arXiv:2506.04651](#), 2025.
- [246] Qianchuan Zhao, Yuxiang Xie, Wentao Wang, Jie Li, Lizhou Sha, Jialong Zhang, and Minlie Huang. Richelieu: Self-evolving LLM-based agents for AI diplomacy. [arXiv preprint arXiv:2407.06813](#), 2024.
- [247] Junhao Zheng, Xidi Cai, Qiuke Li, Duzhen Zhang, ZhongZhi Li, Yingying Zhang, Le Song, and Qianli Ma. Lifelongagentbench: Evaluating llm agents as lifelong learners. [arXiv preprint arXiv:2505.11942](#), 2025.
- [248] Xiao Liu, Hao Yu, Hanchen Zhang, Yifan Xu, Xuanyu Lei, Hanyu Lai, Yu Gu, Hangliang Ding, Kaiwen Men, Kejuna Yang, et al. Agentbench: Evaluating llms as agents. [arXiv preprint arXiv:2308.03688](#), 2023.
- [249] Dengyun Peng, Yuhang Zhou, Qiguang Chen, Jinhao Liu, Jingjing Chen, and Libo Qin. Dlpo: Towards a robust, efficient, and generalizable prompt optimization framework from a deep-learning perspective. [arXiv preprint arXiv:2503.13413](#), 2025.
- [250] Mengkang Hu, Yao Mu, Xinmiao Yu, Mingyu Ding, Shiguang Wu, Wenqi Shao, Qiguang Chen, Bin Wang, Yu Qiao, and Ping Luo. Tree-planner: Efficient close-loop task planning with large language models, 2024.
- [251] Junting Lu, Zhiyang Zhang, Fangkai Yang, Jue Zhang, Lu Wang, Chao Du, Qingwei Lin, Saravan Rajmohan, Dongmei Zhang, and Qi Zhang. Axis: Efficient human-agent-computer interaction with api-first llm-based agents. [arXiv preprint arXiv:2409.17140](#), 2024.
- [252] Zhexin Zhang, Shiya Cui, Yida Lu, Jingzhuo Zhou, Junxiao Yang, Hongning Wang, and Minlie Huang. Agent-safetybench: Evaluating the safety of llm agents. [arXiv preprint arXiv:2412.14470](#), 2024.
- [253] Maksym Andriushchenko, Alexandra Souly, Mateusz Dziemian, Derek Duenas, Maxwell Lin, Justin Wang, Dan Hendrycks, Andy Zou, Zico Kolter, Matt Fredrikson, et al. Agentharm: A benchmark for measuring harmfulness of llm agents. [arXiv preprint arXiv:2410.09024](#), 2024.
- [254] Ido Levy, Ben Wiesel, Sami Marreed, Alon Oved, Avi Yaeli, and Segev Shlomov. St-webagentbench: A benchmark for evaluating safety and trustworthiness in web agents. [arXiv preprint arXiv:2410.06703](#), 2024.
- [255] Hanrong Zhang, Jingyuan Huang, Kai Mei, Yifei Yao, Zhenting Wang, Chenlu Zhan, Hongwei Wang, and Yongfeng Zhang. Agent security bench (asb): Formalizing and benchmarking attacks and defenses in llm-based agents. [arXiv preprint arXiv:2410.02644](#), 2024.
- [256] Yijia Shao, Tianshi Li, Weiyang Shi, Yanchen Liu, and Diyi Yang. Privacylens: Evaluating privacy norm awareness of language models in action. [Advances in Neural Information Processing Systems](#), 37:89373–89407, 2024.
- [257] Ziru Chen, Shijie Chen, Yuting Ning, Qianheng Zhang, Boshi Wang, Botao Yu, Yifei Li, Zeyi Liao, Chen Wei, Zitong Lu, et al. Scienceagentbench: Toward rigorous assessment of language agents for data-driven scientific discovery. [arXiv preprint arXiv:2410.05080](#), 2024.
- [258] Jun Shern Chan, Neil Chowdhury, Oliver Jaffe, James Aung, Dane Sherburn, Evan Mays, Giulio Starace, Kevin Liu, Leon Maksin, Tejal Patwardhan, et al. Mle-bench: Evaluating machine learning agents on machine learning engineering. [arXiv preprint arXiv:2410.07095](#), 2024.
- [259] 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.

- [260] Shuyan Zhou, Frank F Xu, Hao Zhu, Xuhui Zhou, Robert Lo, Abishek Sridhar, Xianyi Cheng, Tianyue Ou, Yonatan Bisk, Daniel Fried, et al. Webarena: A realistic web environment for building autonomous agents. [arXiv preprint arXiv:2307.13854](#), 2023.
- [261] Peng Wang, Ruihan Tao, Qiguang Chen, Mengkang Hu, and Libo Qin. X-webagentbench: A multilingual interactive web benchmark for evaluating global agentic system. [arXiv preprint arXiv:2505.15372](#), 2025.
- [262] Xiang Deng, Yu Gu, Boyuan Zheng, Shijie Chen, Sam Stevens, Boshi Wang, Huan Sun, and Yu Su. Mind2web: Towards a generalist agent for the web. [Advances in Neural Information Processing Systems](#), 36:28091–28114, 2023.
- [263] Jason Wei, Zhiqing Sun, Spencer Papay, Scott McKinney, Jeffrey Han, Isa Fulford, Hyung Won Chung, Alex Tachard Passos, William Fedus, and Amelia Glaese. Browsecamp: A simple yet challenging benchmark for browsing agents. [arXiv preprint arXiv:2504.12516](#), 2025.
- [264] Carlos E Jimenez, John Yang, Alexander Wettig, Shunyu Yao, Kexin Pei, Ofir Press, and Karthik Narasimhan. Swe-bench: Can language models resolve real-world github issues? [arXiv preprint arXiv:2310.06770](#), 2023.
- [265] Openai. Introducing swe-bench verified, 2024. <https://openai.com/index/introducing-swe-bench-verified>.
- [266] Reem Aleithan, Haoran Xue, Mohammad Mahdajer, Elijah Nnorom, Gias Uddin, and Song Wang. Swe-bench+: Enhanced coding benchmark for llms. [arXiv preprint arXiv:2410.06992](#), 2024.
- [267] John Yang, Carlos E Jimenez, Alex L Zhang, Kilian Lieret, Joyce Yang, Xindi Wu, Ori Press, Niklas Muennighoff, Gabriel Synnaeve, Karthik R Narasimhan, et al. Swe-bench multimodal: Do ai systems generalize to visual software domains? [arXiv preprint arXiv:2410.03859](#), 2024.
- [268] Tianbao Xie, Danyang Zhang, Jixuan Chen, Xiaochuan Li, Siheng Zhao, Ruisheng Cao, Toh J Hua, Zhoujun Cheng, Dongchan Shin, Fangyu Lei, et al. Osworld: Benchmarking multimodal agents for open-ended tasks in real computer environments. [Advances in Neural Information Processing Systems](#), 37:52040–52094, 2024.
- [269] Kaiyuan Chen, Yixin Ren, Yang Liu, Xiaobo Hu, Haotong Tian, Tianbao Xie, Fangfu Liu, Haoye Zhang, Hongzhang Liu, Yuan Gong, et al. Xbench: Tracking agents productivity scaling with profession-aligned real-world evaluations. [arXiv preprint arXiv:2506.13651](#), 2025.
- [270] Grégoire Mialon, Clémentine Fourrier, Thomas Wolf, Yann LeCun, and Thomas Scialom. Gaia: a benchmark for general ai assistants. In [The Twelfth International Conference on Learning Representations](#), 2023.
- [271] Frank F Xu, Yufan Song, Boxuan Li, Yuxuan Tang, Kritanjali Jain, Mengxue Bao, Zora Z Wang, Xuhui Zhou, Zhitong Guo, Murong Cao, et al. Theagentcompany: benchmarking llm agents on consequential real world tasks. [arXiv preprint arXiv:2412.14161](#), 2024.
- [272] Karthik Valmeekam, Matthew Marquez, Alberto Olmo, Sarath Sreedharan, and Subbarao Kambhampati. Plan-bench: An extensible benchmark for evaluating large language models on planning and reasoning about change. [Advances in Neural Information Processing Systems](#), 36:38975–38987, 2023.
- [273] Huaixiu Steven Zheng, Swaroop Mishra, Hugh Zhang, Xinyun Chen, Minmin Chen, Azade Nova, Le Hou, Heng-Tze Cheng, Quoc V Le, Ed H Chi, et al. Natural plan: Benchmarking llms on natural language planning. [arXiv preprint arXiv:2406.04520](#), 2024.
- [274] Katharina Stein, Daniel Fišer, Jörg Hoffmann, and Alexander Koller. Automating the generation of prompts for llm-based action choice in pddl planning. In [Proceedings of the Fourteenth International Conference on Automated Planning and Scheduling \(ICAPS 2025\)](#). AAAI Press, 2025.
- [275] Harsha Kokel, Michael Katz, Kavitha Srinivas, and Shirin Sohrabi. Acpbench: Reasoning about action, change, and planning. In [Proceedings of the AAAI Conference on Artificial Intelligence](#), volume 39, pages 26559–26568, 2025.
- [276] Qiaoyu Tang, Ziliang Deng, Hongyu Lin, Xianpei Han, Qiao Liang, Boxi Cao, and Le Sun. Toolalpaca: Generalized tool learning for language models with 3000 simulated cases. [arXiv preprint arXiv:2306.05301](#), 2023.
- [277] Jiarui Lu, Thomas Holleis, Yizhe Zhang, Bernhard Aumayer, Feng Nan, Felix Bai, Shuang Ma, Shen Ma, Mengyu Li, Guoli Yin, et al. Toolsandbox: A stateful, conversational, interactive evaluation benchmark for llm tool use capabilities. [arXiv preprint arXiv:2408.04682](#), 2024.
- [278] Mengsong Wu, Tong Zhu, Han Han, Chuanyuan Tan, Xiang Zhang, and Wenliang Chen. Seal-tools: Self-instruct tool learning dataset for agent tuning and detailed benchmark. In [CCF International Conference on Natural Language Processing and Chinese Computing](#), pages 372–384. Springer, 2024.

- [279] Minghao Li, Yingxiu Zhao, Bowen Yu, Feifan Song, Hangyu Li, Haiyang Yu, Zhoujun Li, Fei Huang, and Yongbin Li. Api-bank: A comprehensive benchmark for tool-augmented llms. [arXiv preprint arXiv:2304.08244](#), 2023.
- [280] Zehui Chen, Weihua Du, Wenwei Zhang, Kuikun Liu, Jiangning Liu, Miao Zheng, Jingming Zhuo, Songyang Zhang, Dahua Lin, Kai Chen, et al. T-eval: Evaluating the tool utilization capability of large language models step by step. [arXiv preprint arXiv:2312.14033](#), 2023.
- [281] Shunyu Yao, Noah Shinn, Pedram Razavi, and Karthik Narasimhan. tau-bench: A benchmark for tool-agent-user interaction in real-world domains. [arXiv preprint arXiv:2406.12045](#), 2024.
- [282] Chen Chen, Xinlong Hao, Weiwen Liu, Xu Huang, Xingshan Zeng, Shuai Yu, Dexun Li, Shuai Wang, Weinan Gan, Yuefeng Huang, et al. Acebench: Who wins the match point in tool usage? [arXiv preprint arXiv:2501.12851](#), 2025.
- [283] David Castillo-Bolado, Joseph Davidson, Finlay Gray, and Marek Rosa. Beyond prompts: Dynamic conversational benchmarking of large language models. In [The Thirty-eight Conference on Neural Information Processing Systems Datasets and Benchmarks Track](#), 2024.
- [284] Yuanzhe Hu, Yu Wang, and Julian McAuley. Evaluating memory in llm agents via incremental multi-turn interactions. In [ICML 2025 Workshop on Long-Context Foundation Models](#).
- [285] Luanbo Wan and Weizhi Ma. Storybench: A dynamic benchmark for evaluating long-term memory with multi turns. [arXiv preprint arXiv:2506.13356](#), 2025.
- [286] Kunlun Zhu, Hongyi Du, Zhaochen Hong, Xiaocheng Yang, Shuyi Guo, Zhe Wang, Zhenhailong Wang, Cheng Qian, Xiangru Tang, Heng Ji, et al. Multiagentbench: Evaluating the collaboration and competition of llm agents. [arXiv preprint arXiv:2503.01935](#), 2025.
- [287] Kai Ruan, Mowen Huang, Ji-Rong Wen, and Hao Sun. Benchmarking llms' swarm intelligence. [arXiv preprint arXiv:2505.04364](#), 2025.
- [288] Liqiang Jing, Zhehui Huang, Xiaoyang Wang, Wenlin Yao, Wenhao Yu, Kaixin Ma, Hongming Zhang, Xinya Du, and Dong Yu. Dsbench: How far are data science agents from becoming data science experts?, 2025.
- [289] Jialong Wu, Wenbiao Yin, Yong Jiang, Zhenglin Wang, Zekun Xi, Runnan Fang, Linhai Zhang, Yulan He, Deyu Zhou, Pengjun Xie, et al. Webwalker: Benchmarking llms in web traversal. [arXiv preprint arXiv:2501.07572](#), 2025.
- [290] Shihan Dou, Ming Zhang, Chenhao Huang, Jiayi Chen, Feng Chen, Shichun Liu, Yan Liu, Chenxiao Liu, Cheng Zhong, Zongzhang Zhang, Tao Gui, Chao Xin, Wei Chengzhi, Lin Yan, Qi Zhang, Yonghui Wu, and Xuanjing Huang. Evalearn: Quantifying the learning capability and efficiency of llms via sequential problem solving, 2025.
- [291] Hongru Wang, Rui Wang, Boyang Xue, Heming Xia, Jingtao Cao, Zeming Liu, Jeff Z. Pan, and Kam-Fai Wong. AppBench: Planning of multiple APIs from various APPs for complex user instruction. In Yaser Al-Onaizan, Mohit Bansal, and Yun-Nung Chen, editors, [Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing](#), pages 15322–15336, Miami, Florida, USA, November 2024. Association for Computational Linguistics.
- [292] François Chollet. On the measure of intelligence. [arXiv preprint arXiv:1911.01547](#), 2019.
- [293] Yichen Pan, Dehan Kong, Sida Zhou, Cheng Cui, Yifei Leng, Bing Jiang, Hangyu Liu, Yanyi Shang, Shuyan Zhou, Tongshuang Wu, et al. Webcanvas: Benchmarking web agents in online environments. [arXiv preprint arXiv:2406.12373](#), 2024.
- [294] Colin White, Samuel Dooley, Manley Roberts, Arka Pal, Ben Feuer, Siddhartha Jain, Ravid Shwartz-Ziv, Neel Jain, Khalid Saifullah, Sreemanti Dey, et al. Livebench: A challenging, contamination-limited llm benchmark. [arXiv preprint arXiv:2406.19314](#), 2024.
- [295] Yue Yang, MingKang Chen, Qihua Liu, Mengkang Hu, Qiguang Chen, Gengrui Zhang, Shuyue Hu, Guangtao Zhai, Yu Qiao, Yu Wang, et al. Truly assessing fluid intelligence of large language models through dynamic reasoning evaluation. [arXiv preprint arXiv:2506.02648](#), 2025.
- [296] Simin Chen, Yiming Chen, Zexin Li, Yifan Jiang, Zhongwei Wan, Yixin He, Dezhi Ran, Tianle Gu, Haizhou Li, Tao Xie, et al. Recent advances in large langauge model benchmarks against data contamination: From static to dynamic evaluation. [arXiv preprint arXiv:2502.17521](#), 2025.
- [297] Siyuan Wang, Zhuohan Long, Zhihao Fan, Zhongyu Wei, and Xuanjing Huang. Benchmark self-evolving: A multi-agent framework for dynamic llm evaluation. [arXiv preprint arXiv:2402.11443](#), 2024.

- [298] Zhehao Zhang, Ryan A Rossi, Branislav Kveton, Yijia Shao, Diyi Yang, Hamed Zamani, Franck Dernoncourt, Joe Barrow, Tong Yu, Sungchul Kim, et al. Personalization of large language models: A survey. [arXiv preprint arXiv:2411.00027](#), 2024.
- [299] Yi Cheng, Wenge Liu, Kaishuai Xu, Wenjun Hou, Yi Ouyang, Chak Tou Leong, Xian Wu, and Yefeng Zheng. Autopal: Autonomous adaptation to users for personal ai companionship. [arXiv preprint arXiv:2406.13960](#), 2024.
- [300] Yijing Zhang, Dyah Adila, Changho Shin, and Frederic Sala. Personalize your llm: Fake it then align it. [arXiv preprint arXiv:2503.01048](#), 2025.
- [301] Yue Wang, Tianfan Fu, Yinlong Xu, Zihan Ma, Hongxia Xu, Bang Du, Yingzhou Lu, Honghao Gao, Jian Wu, and Jintai Chen. Twin-gpt: digital twins for clinical trials via large language model. [ACM Transactions on Multimedia Computing, Communications and Applications](#), 2024.
- [302] Xiaopeng Li, Pengyue Jia, Derong Xu, Yi Wen, Yingyi Zhang, Wenlin Zhang, Wanyu Wang, Yichao Wang, Zhaocheng Du, Xiangyang Li, et al. A survey of personalization: From rag to agent. [arXiv preprint arXiv:2504.10147](#), 2025.
- [303] Chin-Yew Lin. Rouge: A package for automatic evaluation of summaries. In [Text summarization branches out](#), pages 74–81, 2004.
- [304] Kishore Papineni, Salim Roukos, Todd Ward, and Wei-Jing Zhu. Bleu: a method for automatic evaluation of machine translation. In [Proceedings of the 40th annual meeting of the Association for Computational Linguistics](#), pages 311–318, 2002.
- [305] Weize Chen, Jiarui Yuan, Chen Qian, Cheng Yang, Zhiyuan Liu, and Maosong Sun. Optima: Optimizing effectiveness and efficiency for llm-based multi-agent system. [arXiv preprint arXiv:2410.08115](#), 2024.
- [306] Jiin Kim, Byeongjun Shin, Jinha Chung, and Minsoo Rhu. The cost of dynamic reasoning: Demystifying ai agents and test-time scaling from an ai infrastructure perspective. [arXiv preprint arXiv:2506.04301](#), 2025.
- [307] Charlie Snell, Jaehoon Lee, Kelvin Xu, and Aviral Kumar. Scaling llm test-time compute optimally can be more effective than scaling model parameters. [arXiv preprint arXiv:2408.03314](#), 2024.
- [308] Qiyuan Zhang, Fuyuan Lyu, Zexu Sun, Lei Wang, Weixu Zhang, Wenyue Hua, Haolun Wu, Zhihan Guo, Yufei Wang, Niklas Muenennighoff, et al. A survey on test-time scaling in large language models: What, how, where, and how well? [arXiv preprint arXiv:2503.24235](#), 2025.
- [309] Areeb Bilal, Muhammad Abdul Mohsin, Muhammad Umer, Muhammad Arslan Khan Bangash, et al. Meta-thinking in llms via multi-agent reinforcement learning: A survey. [arXiv preprint arXiv:2504.14520](#), 2025.
- [310] Gaurav Ghosal, Tatsunori Hashimoto, and Aditi Raghunathan. Understanding finetuning for factual knowledge extraction. [arXiv preprint arXiv:2406.14785](#), 2024.
- [311] Howard Chen, Jiayi Geng, Adithya Bhaskar, Dan Friedman, and Danqi Chen. Continual memorization of factoids in language models. [arXiv preprint arXiv:2411.07175](#), 2024.
- [312] James Bell, Luca Quarantiello, Ethan N Coleman, Ling Li, Meng Li, et al. The future of continual learning in the era of foundation models: Three key directions. [arXiv preprint arXiv:2506.03320](#), 2025.
- [313] Quan Shi, Carlos E Jimenez, Shunyu Yao, Nick Haber, Diyi Yang, and Karthik Narasimhan. When models know more than they can explain: Quantifying knowledge transfer in human-ai collaboration. [arXiv preprint arXiv:2506.05579](#), 2025.
- [314] Jiayi Geng, Howard Chen, Dilip Arumugam, and Thomas L Griffiths. Are large language models reliable ai scientists? assessing reverse-engineering of black-box systems. [arXiv preprint arXiv:2505.17968](#), 2025.
- [315] Keyon Vafa, Peter G Chang, Ashesh Rambachan, and Sendhil Mullainathan. What has a foundation model found? using inductive bias to probe for world models. [arXiv preprint arXiv:2507.06952](#), 2025.
- [316] Xueyang Zhou, Weidong Wang, Lin Lu, Jiawen Shi, Guiyao Tie, Yongtian Xu, Lixing Chen, Pan Zhou, Neil Zhenqiang Gong, and Lichao Sun. Automating safety enhancement for llm-based agents with synthetic risk scenarios. [arXiv preprint arXiv:2505.17735](#), 2025.
- [317] Arman Zharmagambetov, Chuan Guo, Ivan Evtimov, Maya Pavlova, Ruslan Salakhutdinov, and Kamalika Chaudhuri. Agentdam: Privacy leakage evaluation for autonomous web agents. [arXiv preprint arXiv:2503.09780](#), 2025.
- [318] Usman Anwar, Abulhair Saparov, Javier Rando, Daniel Paleka, Miles Turpin, Peter Hase, Ekdeep Singh Lubana, Erik Jenner, Stephen Casper, Oliver Sourbut, et al. Foundational challenges in assuring alignment and safety of large language models. [arXiv preprint arXiv:2404.09932](#), 2024.

- [319] Eugene Bagdasarian, Ren Yi, Sahra Ghalebikesabi, Peter Kairouz, Marco Gruteser, Sewoong Oh, Borja Balle, and Daniel Ramage. Airgapagent: Protecting privacy-conscious conversational agents. In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, pages 3868–3882, 2024.
- [320] Bo Wang, Weiyi He, Pengfei He, Shenglai Zeng, Zhen Xiang, Yue Xing, and Jiliang Tang. Unveiling privacy risks in llm agent memory. arXiv preprint arXiv:2502.13172, 2025.
- [321] Kai Chen, Xinfeng Li, Tianpei Yang, Hewei Wang, Wei Dong, and Yang Gao. Mdteamgpt: A self-evolving llm-based multi-agent framework for multi-disciplinary team medical consultation. arXiv preprint arXiv:2503.13856, 2025.
- [322] Haochen Sun, Shuwen Zhang, Lujie Niu, Lei Ren, Hao Xu, Hao Fu, Fangkun Zhao, Caixia Yuan, and Xiaojie Wang. Collab-overcooked: Benchmarking and evaluating large language models as collaborative agents. arXiv preprint arXiv:2502.20073, 2025.