AI Agent

目录

一、背景

agent主要是指以大模型技术(LLM)作为主体或者大脑，能进行自动规划，拥有自主决策能力，以解决复杂问题的智能体。

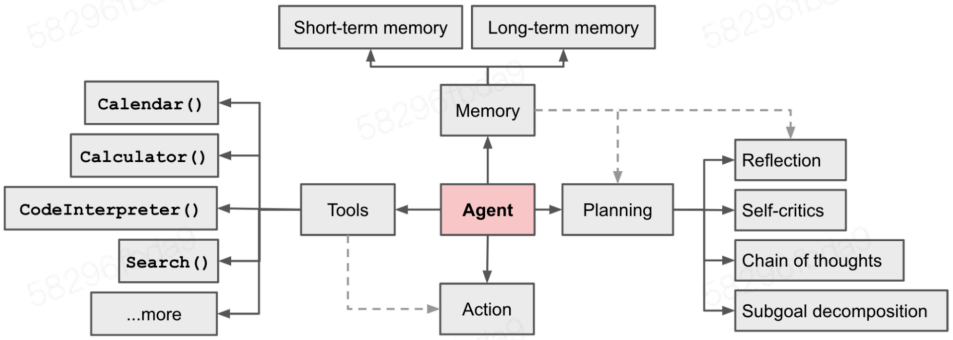
AI 与人类的协作程度可以和自动驾驶等级进行类比，AI Agent 可以类比为自动驾驶的 L4 阶段，距离真正实现仍有差距：

AI等级	表现形式	能力	典型应用

L1	Tool	人类完成所有工作，没有任何显性的AI 辅助。	目前绝大多数
L2	ChatGPT	人类完成绝大部分工作。人类向 AI询问意见，了解信息，AI 提供信息和建议但不直接处理工作。	初代 ChatGI
L3	Copilot	人类和AI进行协作，工作量相当。AI根据人类 prompt 完成工作初稿，人类进行目标设定、修改调整，最后确认。	GitHub Copi Midjourney、
L4	AI Agent	AI 完成绝大部分工作，人类负责设定目标、提供资源和监督结果。AI 完成任务拆分，工具选择，进度控制，实现目标后自主结束工作。	AutoGPT 等
L5	通用人工智能 AGI	完全无需人类监督，AI 自主拆解目标、寻找资源、选择并使用工具、完成全部工作，人类只需给出目标。	暂未出现，类的moss?

二、组成

一个Agent的基本组成应该包含如下四个方面**规划**（planning), **工具**（Tools), **执行**(Tools Action), 和**记忆**(Memory)。



2.1 智能体决策(Agent Planning)

Agent Planning是Agent能力的核心，一个好的规划决定了agent能否顺利执行以及解决问题，规划简单来说就是**任务分解(Task Decomposition)**; 把复杂的问题划分成可以一步步解决的小步骤，以及不断根据**反馈(feedback)**去重新调整策略。

1、Chain of thought

Chain-of-Thought是常见用来引导模型进行任务分解的大模型**提示(prompting)**方法，其主要方法就是提供任务分解的**少量示例(few-shot examples)**，利用大模型的**上下文学习能力(In-context learning)**去模仿进行类似的任务分解和规划。

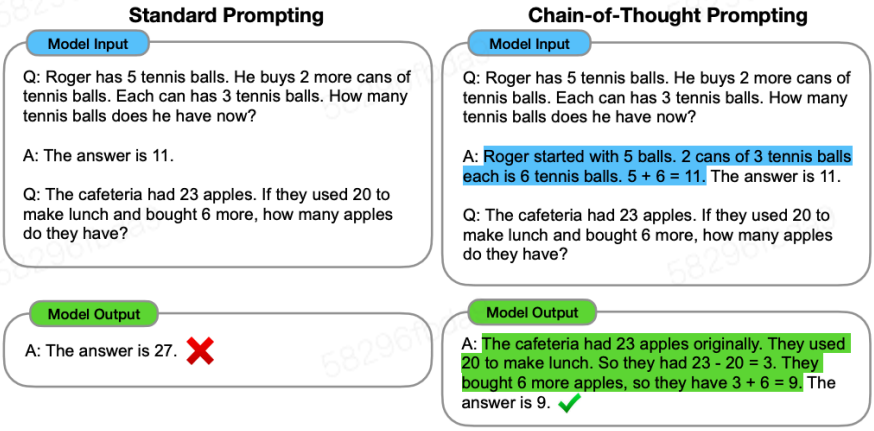
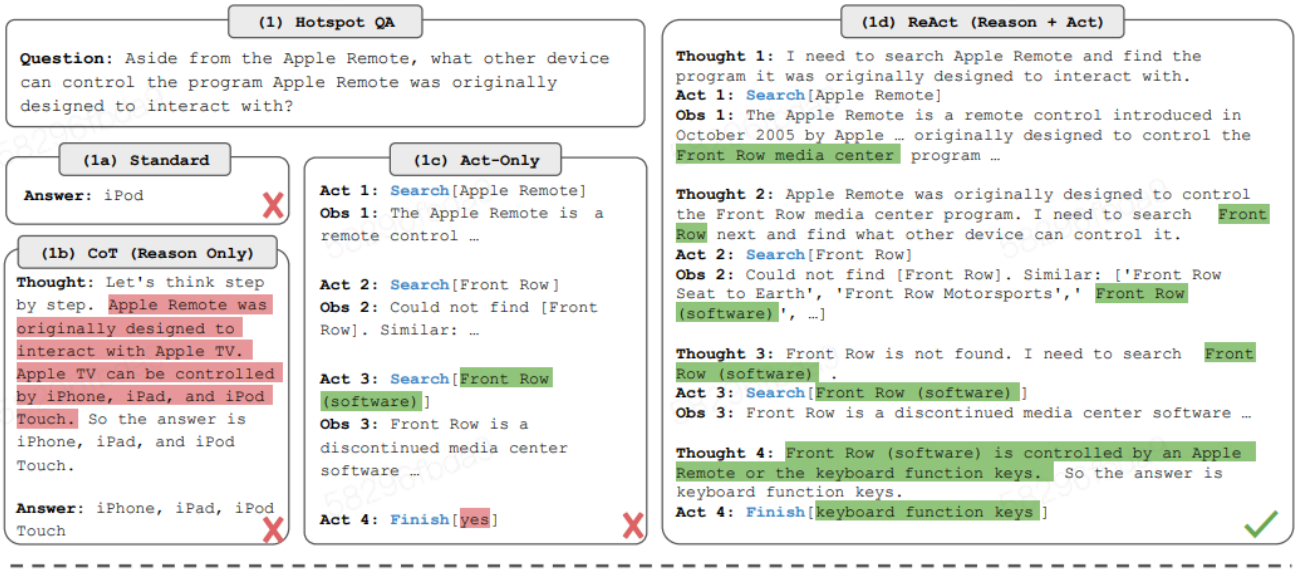


Figure 1: Chain-of-thought prompting enables large language models to tackle complex arithmetic, commonsense, and symbolic reasoning tasks. Chain-of-thought reasoning processes are highlighted.

Chain-of-Thought Prompting Elicits Reasoning in Large Language Models

2、ReAct

ReAct 相对来讲是更复杂的大模型提示（prompting)方法，其核心是引导大模型在生成核心回答内容的前面主动加上一个**思考（thought)**部分，以及**执行(action)**后面的**观察(observation)**模块。这种提示技巧能较好地提升模型的规划能力。



Synergizing Reasoning and Acting in Language Models

3、ReWoo

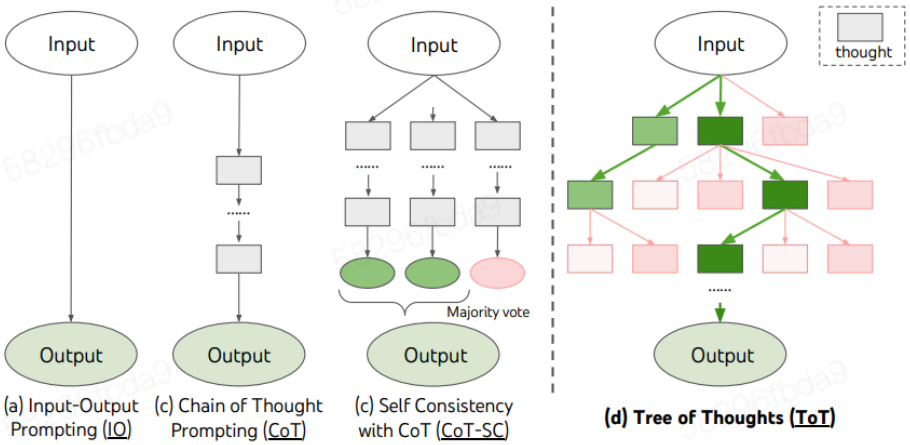
ReWOO是类似在ReACT架构基础上，去掉了观察（observation)这个模块，取而代之的是把整个planning过程划分成**'Planner', 'Worker'**和**'Slover'**分别去进行规划，执行和总结三个部分，在API消耗和精度上都有所提升。

ReWOO: Decoupling Reasoning from Observations for Efficient Augmented Language Models

4、Treeofthought

TOT的方法是**COT**方法进阶版本，它让大模型在每个节点做决策时分化出几个不同可能的策略，并采用深度优先搜索(**DFS**)或者广度优先搜索(**BFS**)的方式去寻找可行策略，增强了大模型面对更复杂问题的决策能力。

作者在24点，以及填字游戏上测试取得了不错的效果。



Tree of Thoughts: Deliberate Problem Solving with Large Language Models

5、Graph of thought

Graph of thought是在TOT方法的基础上，使得整个规划过程可以以图的形式去流动和搜索，相对来讲限制更小。

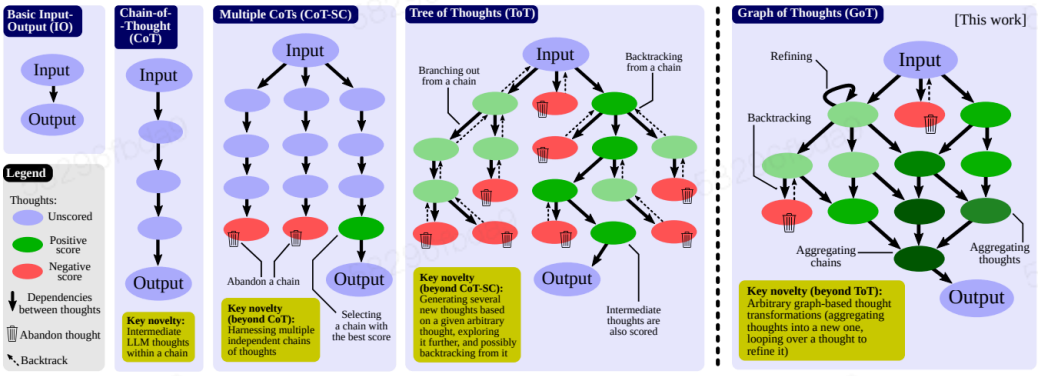


Figure 1: Comparison of Graph of Thoughts (GoT) to other prompting strategies.

Graph of Thoughts: Solving Elaborate Problems with Large Language Models

6、JuDEC

JuDEC方法使用了游戏中常见的Elo算法机制去增强整个规划过程的自我决策能力，在ToolBench场景取得了较好的效果。

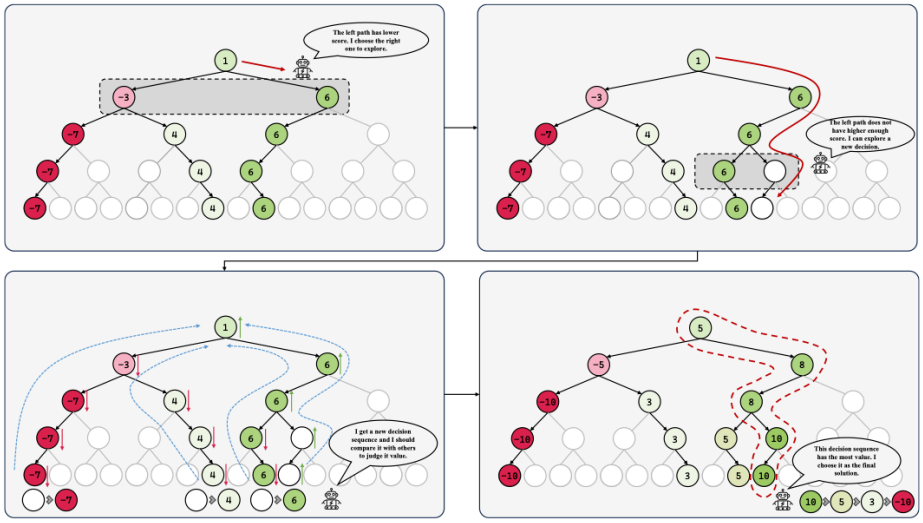


Figure 1: Illustration of our proposed JUDEC.

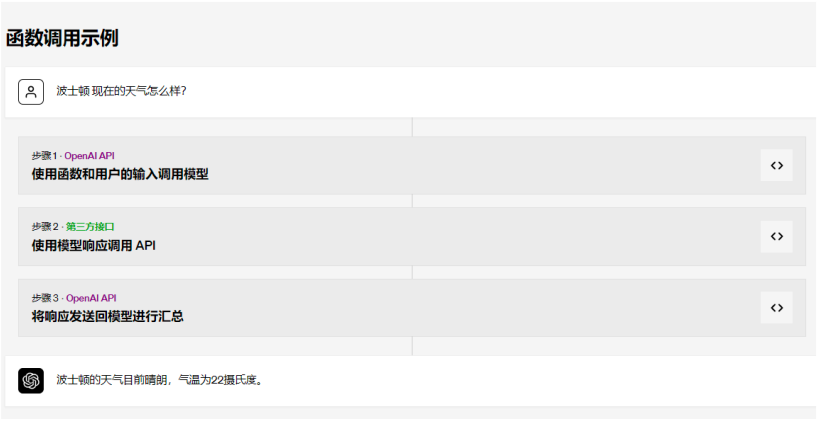
Large Language Model as Autonomous Decision Maker

2.2 智能体工具使用（Agent Tool Using）

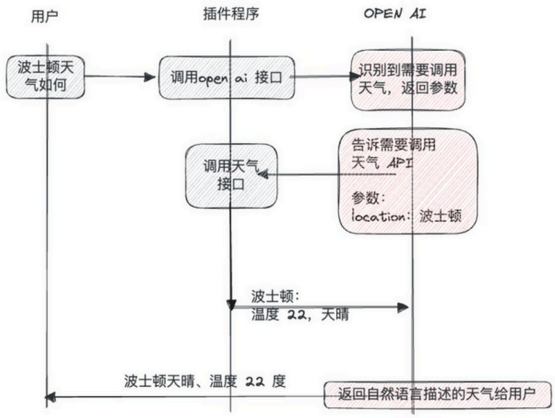
AI Agent 与大模型的一大区别在于能够使用外部工具拓展模型能力，是扩展大模型功能与现实世界交互的关键一环。

ChatGPT 的一大缺点在于，其训练数据只截止到了2021 年底，对于更新一些的知识内容它无法直接做出回答。虽然后续OpenAI 为ChatGPT 更新了插件功能，能够调用浏览器插件来访问最新的信息，但是需要用户来针对问题指定是否需要使用插件，无法做到完全自然的回答。AI Agent则具备了自主调用工具的能力，在获取到每一步子任务的工作后，Agent 都会判断是否需要通过调用外部工具来完成该子任务，并在完成后获取该外部工具返回的信息提供给LLM，进行下一步子任务的工作。

1、 ChatGPT函数调用



示例



流程

使用函数调用：使用样例demo

2、LangChain

TODO!!

- 如langchain内建工具：serpapi 谷歌搜索, llm-math 计算, wikipedia 维基百科

- 如连接zapier，使用Zapier中上千的应用

3、 HuggingGPT

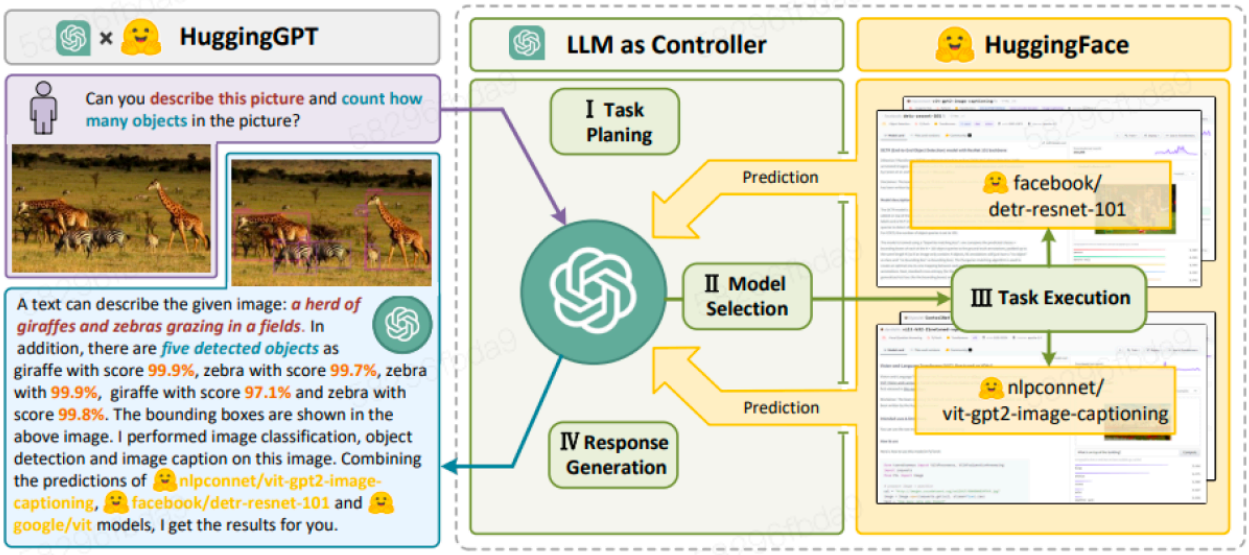
HuggingGPT 将模型社区HuggingFace 和ChatGPT 连接在一起，形成了一个AI Agent。2023 年4 月，浙江大学和微软联合团队发了HuggingGPT，它可以连接不同的AI 模型，以解决用户提出的任务。HuggingGPT 融合了HuggingFace 中成百上千的模型和GPT，可以解决24 种任务，包括文本分类、对象检测、语义分割、图像生成、问答、文本语音转换和文本视频转换。具体步骤分为四步：

1) 任务规划：使用ChatGPT 来获取用户请求；

2) 模型选择：根据Hugging Face 中的函数描述选择模型，并用选中的模型执行AI 任务；

3) 任务执行：使用第2 步选择的模型执行的任务，总结成回答返回给ChatGPT；

4) 回答生成：使用ChatGPT 融合所有模型的推理，生成回答返回给用户。



工作步骤流程

2.3 智能体记忆模块（Agent Memory）

记忆可以定义为用于获取、存储、保留以及随后检索信息的过程。人脑中有多种记忆类型，可以粗略地考虑以下映射：

记忆类型	Human Memory	Agent Memory
Sensory Memory 感觉记忆	这是记忆的最早阶段，提供在原始刺激结束后保留感觉信息（视觉、听觉等）印象的能力。感觉记忆通常只能持续几秒钟。子类别包括图像记忆（视觉）、回声记忆（听觉）和触觉记忆（触摸）。	感觉记忆作为原始输入的学习表示，包括文本、图像或其他
Short-Term Memory 短期记忆（STM）或工作记忆	存储我们当前意识到的以及执行学习和推理等复杂认知任务所需的信息。短期记忆被认为具有大约 7 个项目的容量（Miller 1956）并且持续 20-30 秒。	短期记忆作为prompt学习。它因为它受到 Transformer 有限的限制。

4	Long-Term Memory 长期记忆（LTM）	长期记忆可以存储相当长的时间信息，从几天到几十年不等，存储容量基本上是无限的。 LTM 有两种亚型： • 外显/陈述性记忆：这是对事实和事件的记忆，是指那些可以有意识地回忆起来的记忆，包括情景记忆（事件和经历）和语义记忆（事实和概念）。 • 内隐/程序性记忆：这种类型的记忆是无意识的，涉及自动执行的技能和例程，例如骑自行车或在键盘上打字。	长期记忆作为代理在查询时可 量存储，可通过快速检索进行

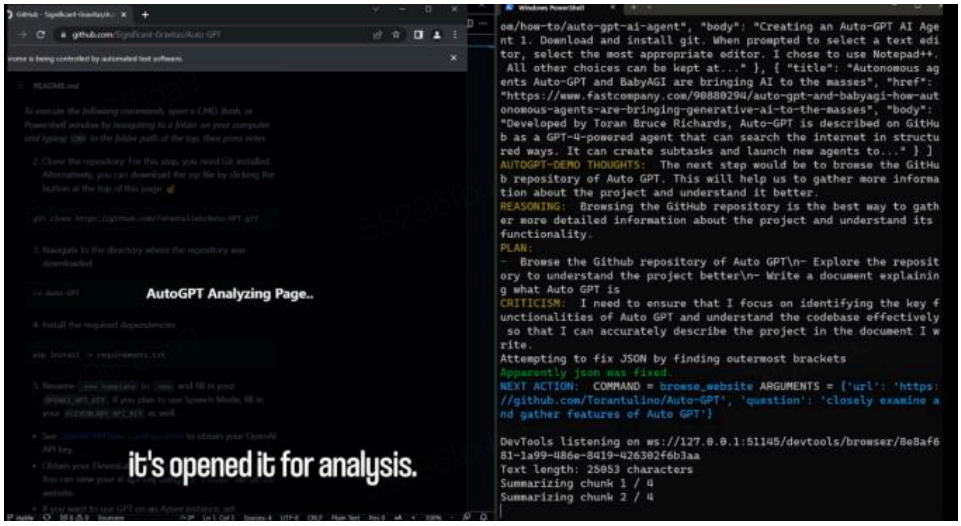
三、实际应用

AI Agent 发展迅速，出现多款“出圈”级研究成果。2023 年3 月起，AI Agent 领域迎来了第一次“出圈”，西部世界小镇、BabyAGI、AutoGPT 等多款重大Agent 研究项目均在短短两周内陆续上线，引发了大家对AI Agent 领域的关注。

AutoGPT

项目地址：https://github.com/Significant-Gravitas/AutoGPT

AutoGPT 将AI Agent 概念带“出圈”。2023 年3 月，开发人员Significant Ggravitas 在GitHub上发布了开源项目AutoGPT，它以GPT-4 为驱动基础，允许AI 自主行动，完全无需用户提示每个操作。给AutoGPT 提出目标，它就能够自主去分解任务、执行操作、完成任务。作为GPT-4完全自主运行的最早示例之一，AutoGPT 迅速走红于AI 界，并带动了整个AI Agent 领域的研究与发展。

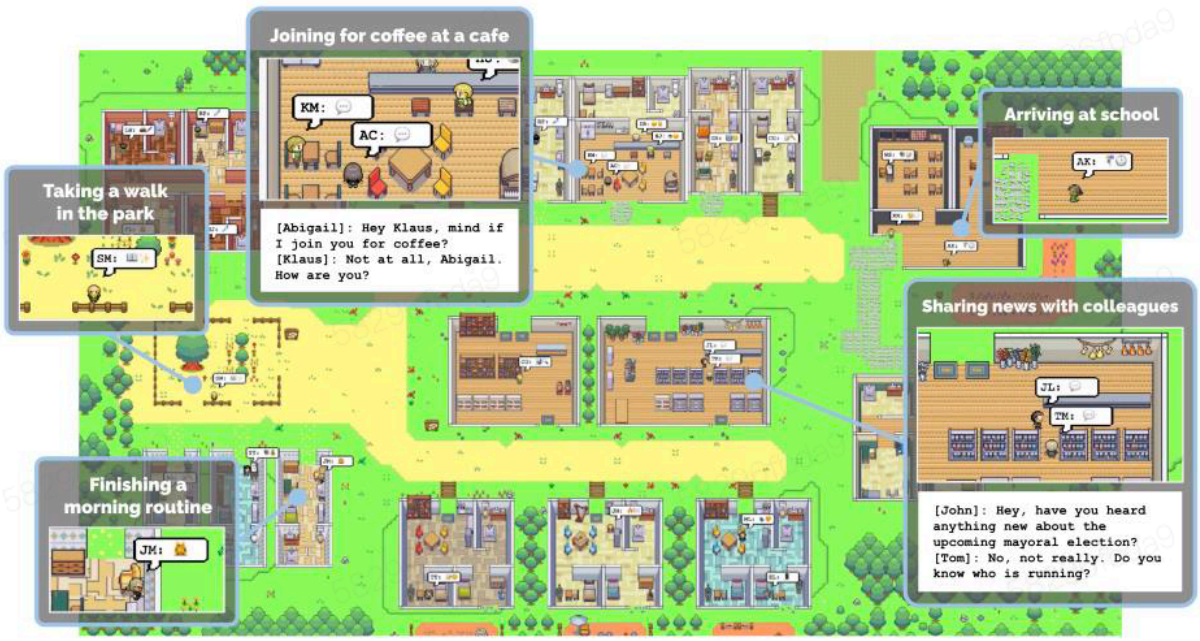


实现自主分析浏览器页面

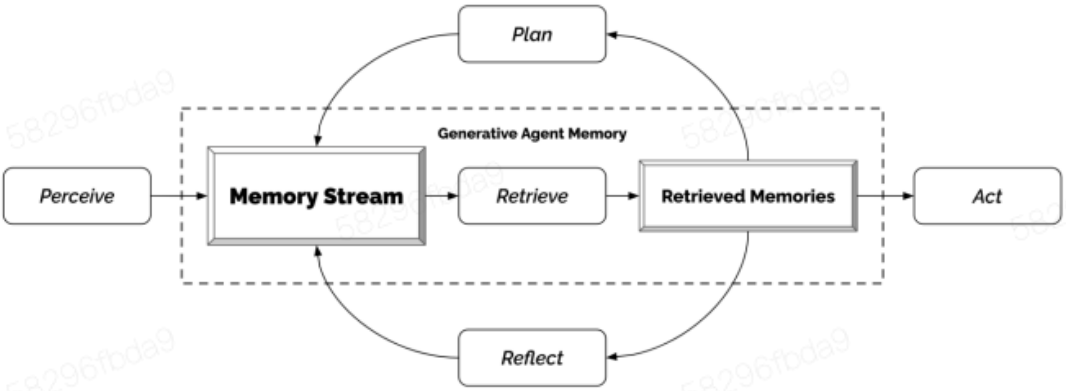
西部世界小镇

斯坦福西部世界小镇首次创造了多个智能体生活的虚拟环境。2023 年4 月，斯坦福大学的研究者们发表了名为《Generative Agents: Interactive Simulacra of Human Behavior》的论文，展示了一个由生成代理（Generative Agents）组成的虚拟西部小镇。这是一个交互式的沙盒环境，在小镇上，生活着25 个可以模拟人类行为的生成式AI Agent。它们会在公园里散步，在咖啡馆喝咖啡，和同事分享当天的新闻。甚至一个智能体想举办情人节排队，这些智能体在接下来的两天里，会自动传播派对邀请的消息，结识新朋友，互相约对方一起去派对，还会彼此协调时间，在正确的时间一起出现在派对上。这种Agent 具有类似人的特质、

独立决策和长期记忆等功能，它们更接近于“原生AI Agent”。在这种合作模式下，Agent 不仅仅是为人类服务的工具，它们也能够在数字世界中与其他Agent 建立社交关系。

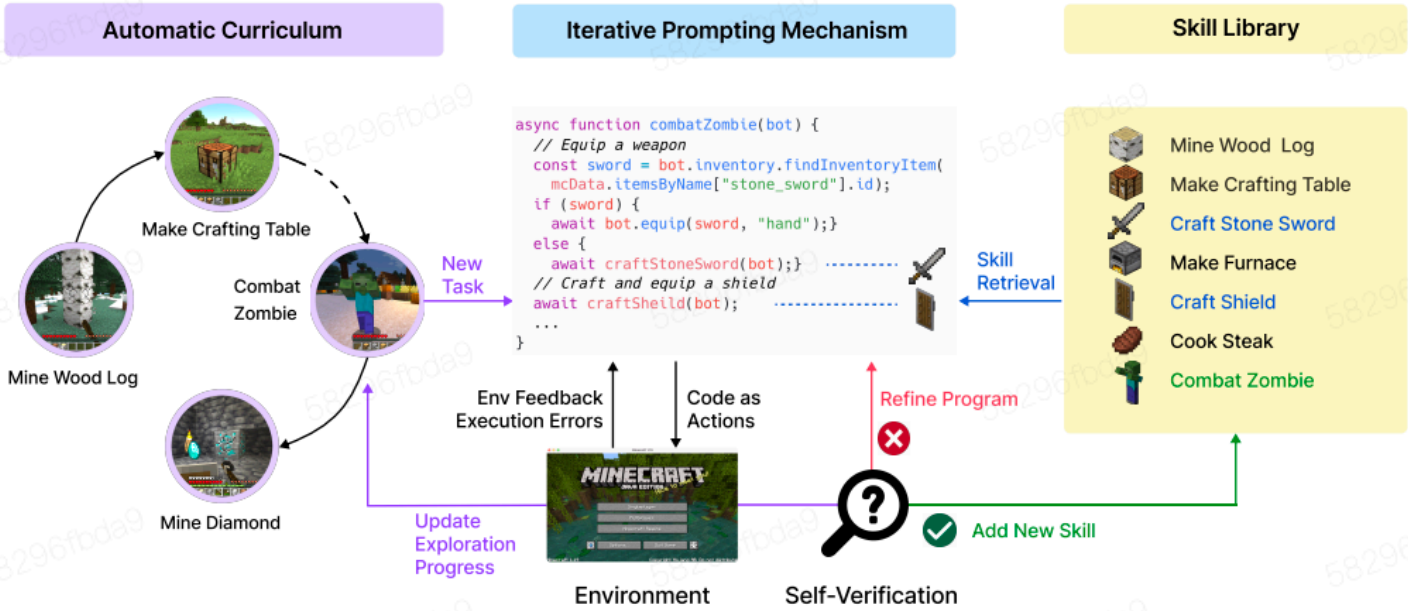


记忆流是西部世界小镇中AI Agents 的架构核心。小镇中的Agents 包含三大重要的基本要素：记忆、反思和规划，相比第二章提到的几个核心组件略有调整。这三大基本要素都基于一个核心：记忆流（Memory Stream），记忆流存储了Agent 的所有经历记录，是一个包含了多个观察的列表，每个观察都包含了事件描述、创建时间以及最近一次访问的时间戳，观察可以是Agent 自己的行为或从其他人那里感知到的行为。为了检索最重要的记忆以传递给语言模型，研究者确定了检索过程中需要考虑的三个因素：最近性、重要性和相关性。通过确定每条记忆基于这三个因素的分数，最后加总起来得到权重最高的记忆，作为prompt 的一部分传递给大模型，以此来决定Agent 的下一步动作。反思和规划都是基于记忆流中的观察来进行更新与创建的。



Voyager我的世界

2023 年5 月，英伟达开源了Voyager 这一游戏智能体。英伟达将Voyager 用在了《我的世界》这款游戏中，《我的世界》没有强加一个预定的最终目标或固定的故事情节，而是提供了一个具有无限可能性的独特游乐场。一个高效的终身学习Agent 应该具有与人类玩家类似的能力，能够根据当前技能水平和世界状态发现合适的任务，能够根据反馈学习和完善技能，不断探索世界。



Voyager 由自动课程、技能库和迭代prompt 机制三个新型组件构成。Voyager 的架构与第二章提到的AI Agent 基本组件相差较大：自动课程用于提出开放式的探索目标，该课程是由 GPT-4 根据“尽可能多发现不同的东西”的总体目标生成的，会根据探索进度和Agent 状态使得探索实现最大化；技能库用于开发越来越复杂的行为，通过存储有助于成功解决某个任务的行动程序，Voyager 逐步建立起一个技能库，未来可以在类似情况下进行检索。这些技能是用可执行的代码来表示的，复杂的技能则可以通过组成更简单的程序来合成。这种做法可以让Voyager 的能力随着时间的推移迅速增强，并缓解“灾难性遗忘”问题；迭代prompt 机制引入了环境反馈、执行错误和检查任务是否成功的自我验证三种类型的反馈，根据这些反馈，GPT-4 可以自己去迭代更新prompt，直到生成的prompt 足以去完成当前任务。

ModelScopeGPT

在2023 年7 月的世界人工智能大会上，阿里云推出了面向开发者们的大模型调用工具魔搭GPT。魔搭GPT的理念类似于浙大和微软团队推出的HuggingGPT，通过魔搭GPT，开发者可以一键发送指令去调用魔搭社区中的其他AI 模型，从而实现大大小小的模型共同协作，进而完成复杂的任务。

一些其他应用

- HyperWrite 推出首个**个人AI 助理Agent——Personal Assistant**。它可以帮助用户整理邮箱并起草回复、帮助用户订机票、订外卖、整理领英上适合的简历等，将AI 能力无缝接入到用户的日常生活和工作流中。目前该工具还处于试用阶段，主要适用于网页浏览器场景。

- Inflection AI 推出**主打情感陪伴的个人AI——Pi**。进行友好的对话，提供简洁的建议，甚至只是倾听。它的主要特征是富有同情心、谦虚好奇、幽默创新，具有良好的情商，可以根据用户的独特兴趣和需求提供无限的知识与陪伴。Inflection 自开发Pi 开始，就确定了Pi 将作为个人智能（Personal Intelligence），而不仅仅是辅助人工作的工具。
- LLM 的**Agent 能力评估标准——AgentBench**。用来评估 LLM 作为Agent 在各种真实世界挑战和 8 个不同环境中的能力表现（如推理和决策能力）。这8 个环境分别是：操作系统、数据库、知识图谱、卡牌对战游戏、家务事、横向思维谜题、网络购物、网页浏览。基于这8 个环境，研究团队设计了不同的真实世界挑战，涵盖了代码场景和生活场景，比如用SQL 语言从一些表格里提取需要的数、玩卡牌游戏取得胜利、从网页预订机票等。

附录

Agent调研与综述：

- The Rise and Potential of Large Language Model Based Agents: A Survey
- A Survey on Large Language Model based Autonomous Agents
- Lilian Wang's Blog

一些agent相关的开源项目：

- Stable-Alignment
- AgentVerse
- Camel
- MetaGPT
- LangChain
- AgentChain
- AutoGPT
- GPTeam
- SocraticAI
- Langroid
- Generative agents
- Light
- AutoAgents
- SuperAGI
- AI-waves:Agents

agent评估基线：

- AgentBench
- ToolBench
- MLAgentBench