



ZOMI

大模型系列之智能体

AI Agent 热门应用



关于大模型系列

- 内容背景

- LLM + AI Agent : 大模型遇到智能体

- 具体内容

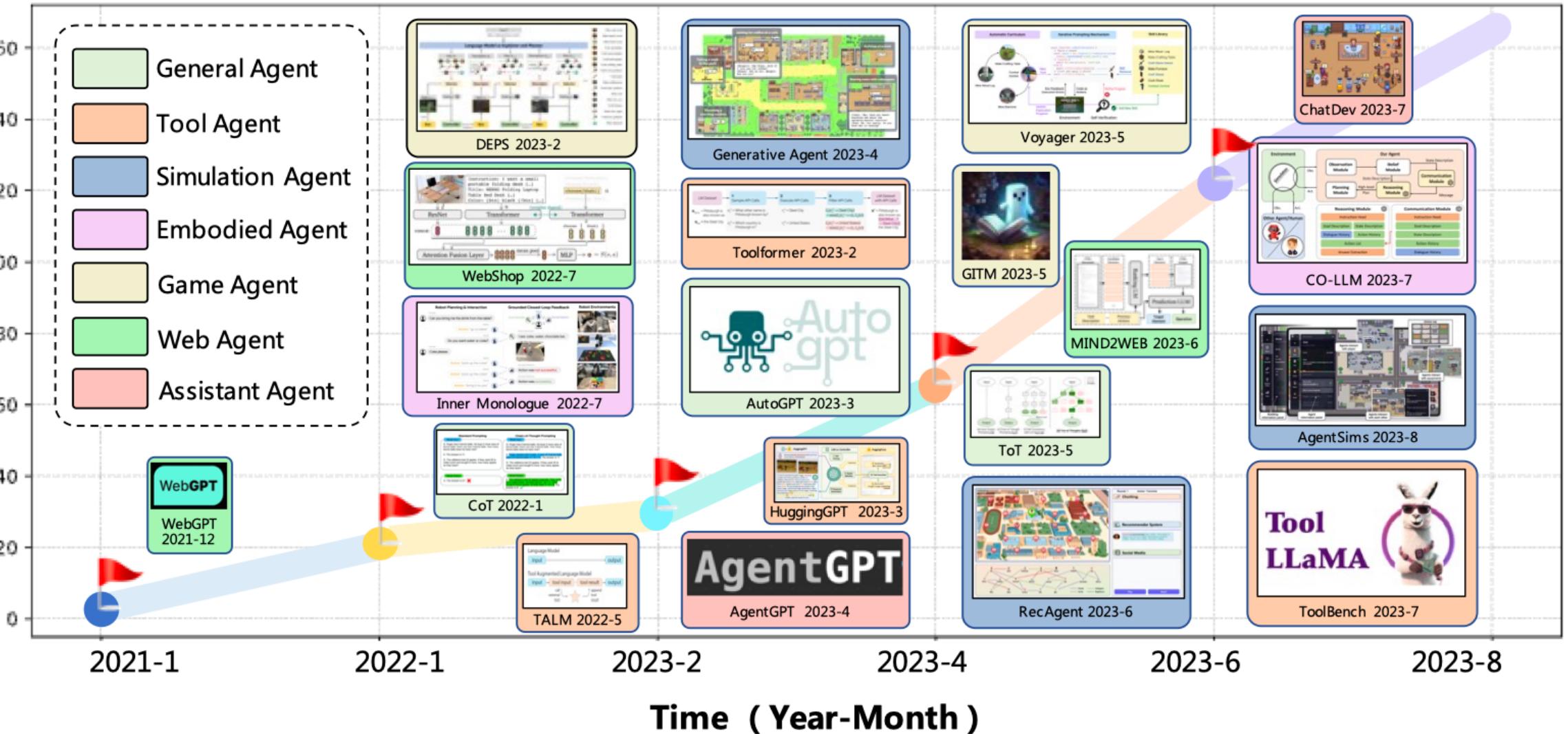
- I. AI Agent 组成介绍 : LLM + 记忆 + 规划 + 工具

2. AI Agent 规划手段 : Task Decomposition 与 Self Reflection

3. AI Agent 热门应用 : 交互式 Agent、自动化 Agent 与多模态 Agent

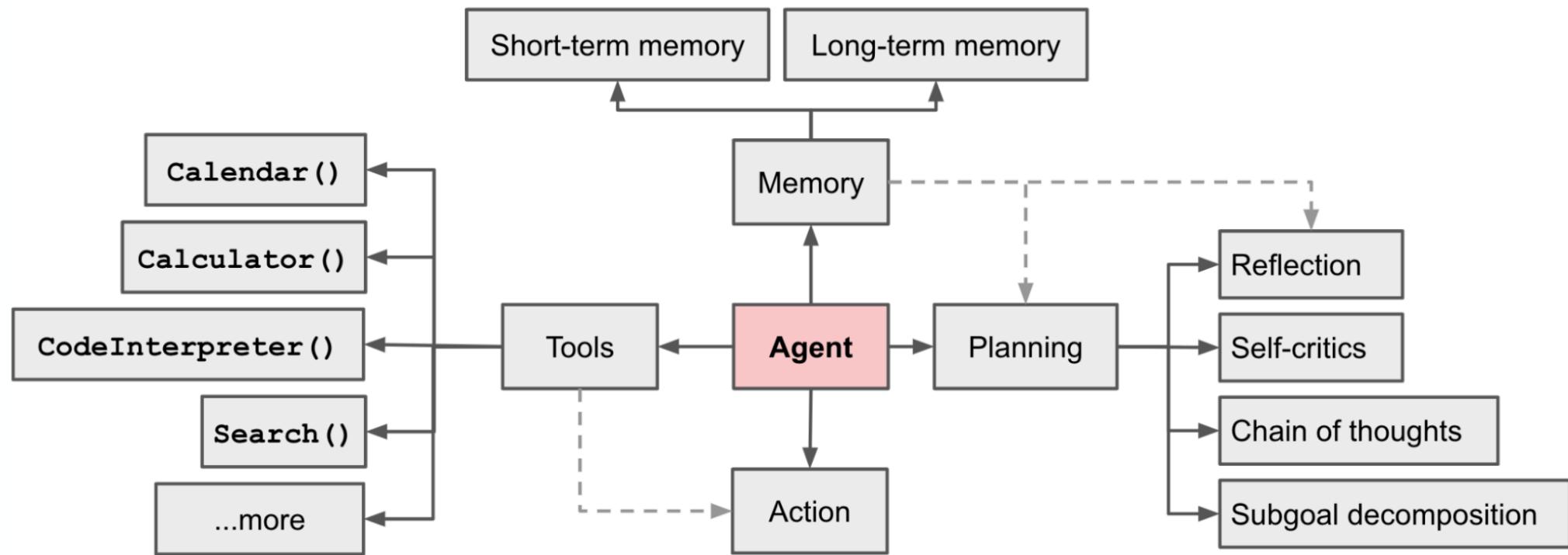
4. AI Agent 问题与挑战 : Agent 的问题、Agent 的局限性

Number of Papers (cumulated)



关键组成

- 规划 Planning + 记忆 Memory + 工具 Tools



Agent 智能体的规划分类

1. **Action agents** : 在每个时间步长，使用所有先前操作的输出来决定下一个操作。 Action Agents 适合小型的任务。
 2. **Plan-and-execute agents** : 预先决定完整的 Action 顺序，然后在不更新计划 Plan 的情况下全部执行。适合需要保持长期目标的复杂任务。
- 通过让 Plan-and-execute agent 使用 Action agents 来执行计划 Plan，将 Action agents 的动态性与 Plan-and-execute agent 的计划能力相结合。

Agent 智能体的应用分类

1. **Simulations Agent** : 模拟智能体，在模拟器中包括一个 and/or 多个 Agent 相互作用。
2. **Automatic Agent** : 自动化智能体，给定一个 and/or 多个长期目标，独立执行这些目标。
3. **Multimodal Agent** : 多模态智能体，除 NLP 信息外还可以拓展到图像，语音，视频的交互。

1. Simulations Agent

Simulations Agent

- Simulation Agent 包括一个/多个 Agents 相互作用。模拟 Agent 通常包括两个主要组件：
 1. 长期记忆
 2. 模拟环境

Generative Agents : 背景

Generative Agents : Interactive Simulacra of Human Behavior

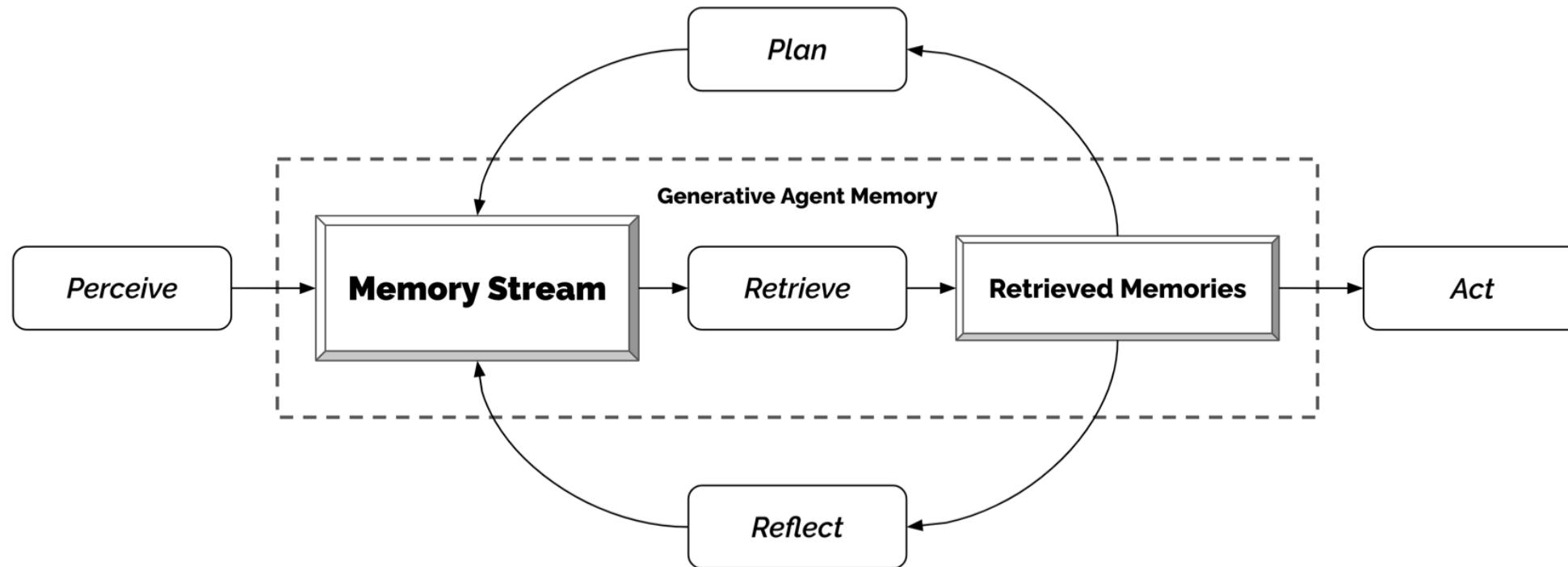
- 斯坦福“西部世界”虚拟小镇，在一个Smallville沙盒世界里住着25个小人(GPT agents)，互相自由沟通交互，出现了一系列的人类社会行为(信息传播、关系记忆和协作)。



Generative Agents : 架构

Generative Agents : Interactive Simulacra of Human Behavior

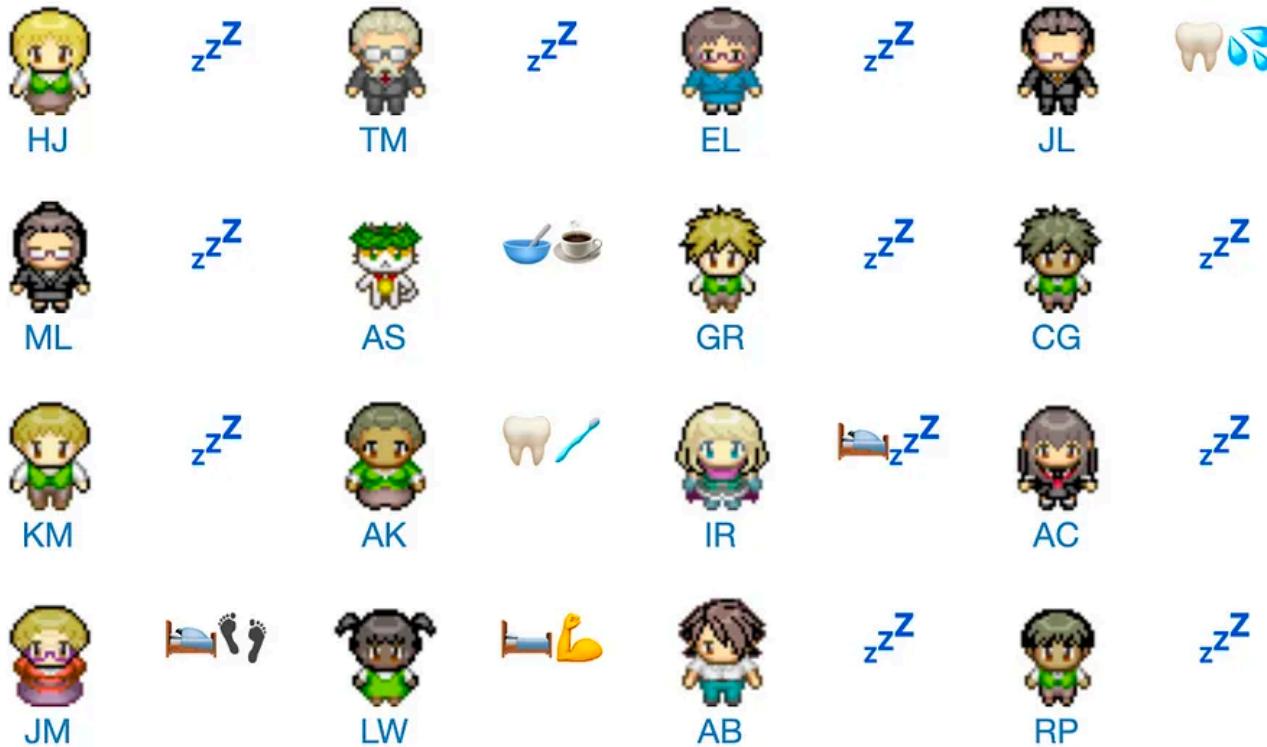
- 代理 (Agents) 感知他们的环境，当前代理所有的感知（完整的经历记录）都被保存在一个名为“记忆流” (**memory stream**) 中。基于代理的感知，系统检索相关的记忆，然后使用这些检索到的行为来决定下一个行为。这些检索到的记忆也被用来形成长期计划，并创造出更高级的反思，这些都被输入到记忆流中以供未来使用。



Generative Agents : 角色

Generative Agents : Interactive Simulacra of Human Behavior

- 先初始化25个agents，称为Generative Agents (因为是用语言生成模型扮演角色)。用文本语言描述每个agent的身份职业和与其他agents的关系，作为每个agent的初始记忆。



John Lin is a pharmacy shopkeeper at the Willow Market and Pharmacy who loves to help people. He is always looking for ways to make the process of getting medication easier for his customers; John Lin is living with his wife, Mei Lin, who is a college professor, and son, Eddy Lin, who is a student studying music theory; John Lin loves his family very much; John Lin has known the old couple next-door, Sam Moore and Jennifer Moore, for a few years; John Lin thinks Sam Moore is a kind and nice man; John Lin knows his neighbor, Yuriko Yamamoto, well; John Lin knows of his neighbors, Tamara Taylor and Carmen Ortiz, but has not met them before; John Lin and Tom Moreno are colleagues at The Willows Market and Pharmacy; John Lin and Tom Moreno are friends and like to discuss local politics together; John Lin knows the Moreno family somewhat well – the husband Tom Moreno and the wife Jane Moreno.

Generative Agents : 记忆与检索

- 需要 LLMs 可以输出行为，并且 agent 要根据其过去的经验做出重要的推论，且保持长期的连贯性。所以需要记忆流，并配合记忆检索，让 agent 生成的行为具有长期规划能力和连贯性。

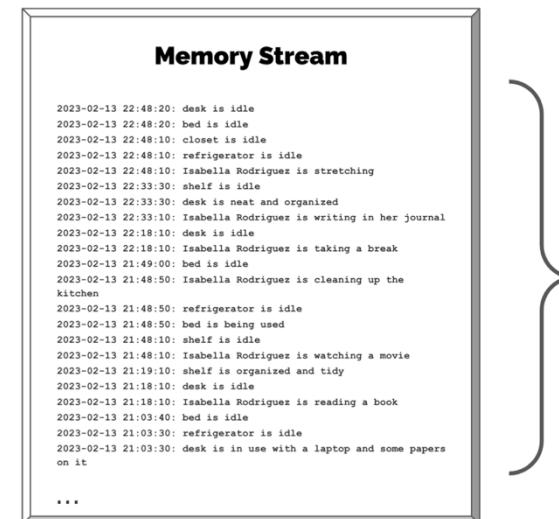
1. **记忆流**：记忆流就是一个数据库，记录 agent 所有经历，还有感知到其它 agent 或对象执行的行为。

2. **检索**：检索记忆时，考虑了三种度量成分：新近度、重要性和相关性。

On the scale of 1 to 10, where 1 is purely mundane (e.g., brushing teeth, making bed) and 10 is extremely poignant (e.g., a break up, college acceptance), rate the likely poignancy of the following piece of memory.

Memory: buying groceries at The Willows Market and Pharmacy

Rating: <fill in>



Q. What are you looking forward to the most right now?

Isabella Rodriguez is excited to be planning a Valentine's Day party at Hobbs Cafe on February 14th from 5pm and is eager to invite everyone to attend the party.

retrieval	recency	importance	relevance
2.34	=	0.91	+ 0.63 + 0.80

ordering decorations for the party

2.21	=	0.87	+ 0.63 + 0.71
------	---	------	---------------

researching ideas for the party

2.20	=	0.85	+ 0.73 + 0.62
------	---	------	---------------

...



I'm looking forward to the Valentine's Day party that I'm planning at Hobbs Cafe!



Generative Agents : 计划和反应

- 计划 Plan 描述了agent未来的一系列行动。整个计划是从自上而下开始，然后递归地生成更多细节。比如：先有agent今天大致在几点和什么地点做什么事，然后拆分到小时粒度。设计专门的prompt得到具体时间粒度下的计划。

Name: Eddy Lin (age: 19)

Innate traits: friendly, outgoing, hospitable

Eddy Lin is a student at Oak Hill College studying music theory and composition. He loves to explore different musical styles and is always looking for ways to expand his knowledge. Eddy Lin is working on a composition project for his college class. He is taking classes to learn more about music theory. Eddy Lin is excited about the new composition he is working on but he wants to dedicate more hours in the day to work on it in the coming days

On Tuesday February 12, Eddy 1) woke up and completed the morning routine at 7:00 am, [...] 6) got ready to sleep around 10 pm.

Today is Wednesday February 13. Here is Eddy's plan today in broad strokes: 1)

[Agent's Summary Description]

It is February 13, 2023, 4:56 pm.

Eddy Lin's status: Eddy is taking a short walk around his workplace.

Observation: John is initiating a conversation with Eddy.

Summary of relevant context from Eddy's memory: John Lin is Eddy Lin's father. John Lin is caring and is interested to learn more about Eddy Lin's school work. John Lin knows that Eddy Lin is working on a music composition.

Here is the dialogue history:

John: Hey Eddy, how's the music composition project for your class coming along?

How would Eddy respond to John?

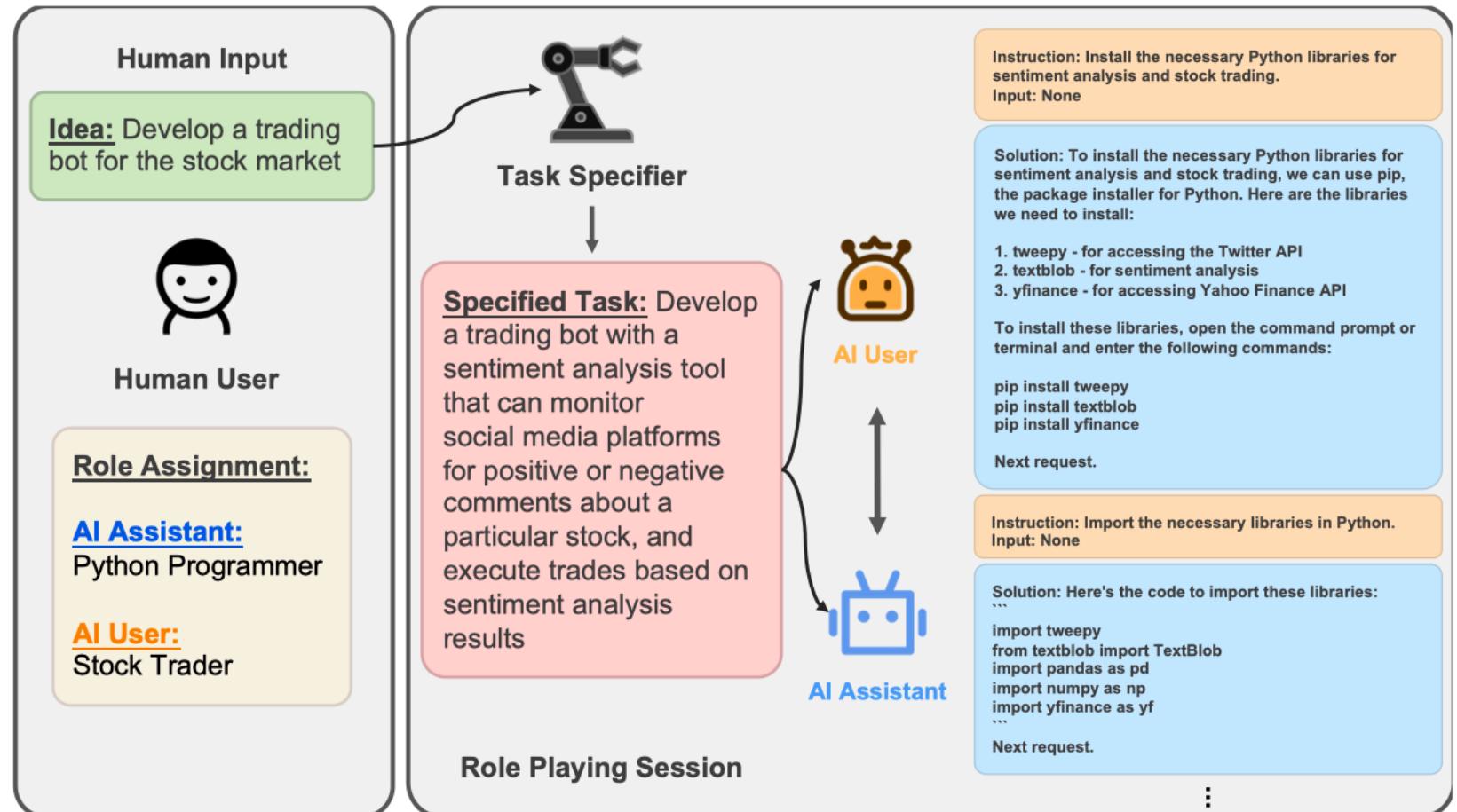
Generative Agents

- 提出生成式agent模拟人类交互行为，设计了一个架构，由感知、记忆流、检索、反思、计划、行动组成。首先初始化agents感知周围环境，然后将观察结果写入记忆流，每次要进行反思、计划和行动时，会检索历史记忆流，然后反思得到近期发生的概括，思考要做什么计划，如何行动、行动的具体时间和地点是什么等。
- 通过2天的交互式模拟，Smallville内涌现出三种社会行为：信息传播、关系记忆和协作。证实多生成式agents在游戏世界中具有一定可信行为。

CAMEL

CAMEL: Communicative Agents for "Mind" Exploration of Large Language Model Society.

- CAMEL 是一个 Role-Playing 框架，使多个 Agents 能够进行对话并合作解决分配的任务。
- 如开发股票交易机器人，一个人工智能助理 Agent，是一个 python 程序员，而人工智能用户 Agent 是一股票交易员。在人类用户输入结束后，Task Specifier 会把任务具体化，通过对网络上特定股票进行情感分析，然后根据情感分析的结果进行股票交易。当任务被具体化后，两个基于 ChatGPT 的 AI 智能体开始合作完成任务，比如进行工具的安装和导入。



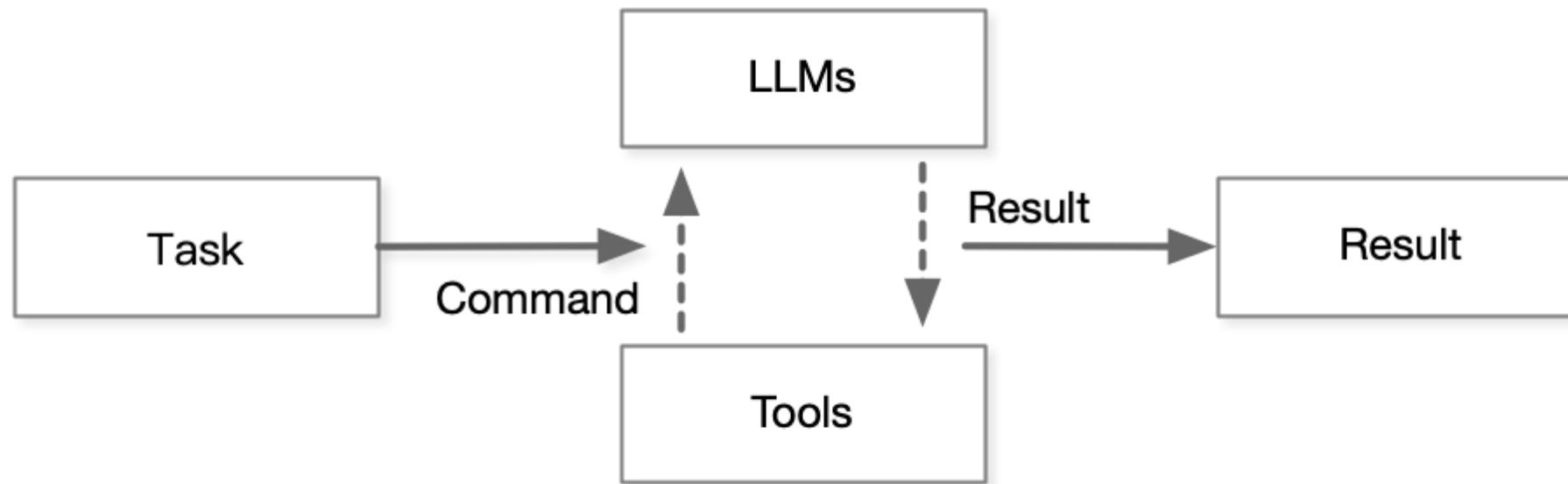
2. Automatic Agent

Automatic Agents

- 给 Agents 一个/多个目标，独立地执行这些目标。这些应用程序结合了工具使用和长期内存。
典型的有AutoGPT，BabyAGI。

AutoGPT

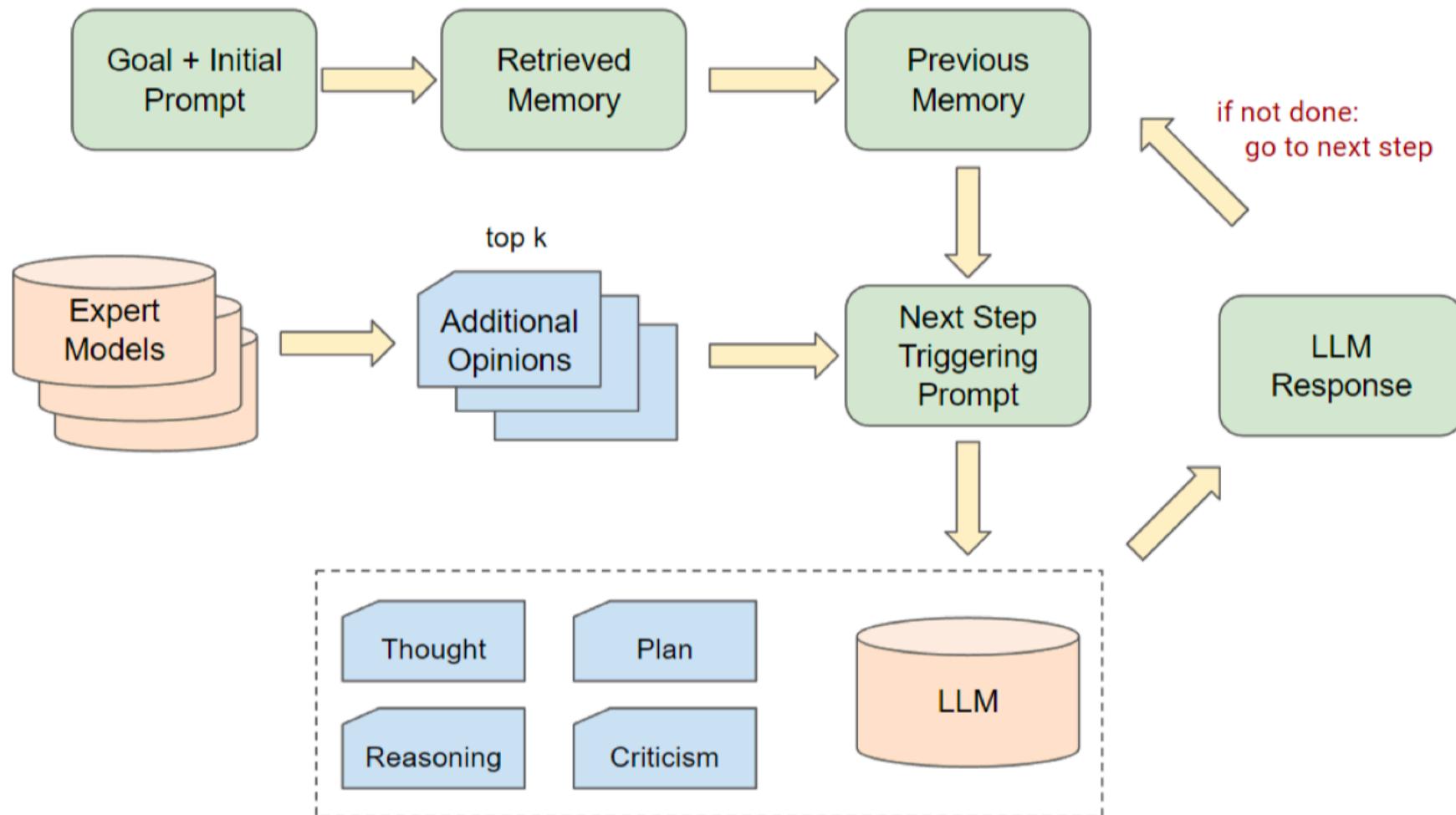
- AutoGPT 以LLM 作为主控制器来建立 AI Agents，作者提供了很多 API 代码来解析数据格式，帮助 AI Agents 更好地理解和处理自然语言输入，虽然目前还处于试验的阶段。AutoGPT 的核心逻辑是一个 Prompt Loop：



AutoGPT：流程

1. **任务定义**：通过 Name、Role、Goals，组成 Prompt
2. **理解任务**：对下发的Prompt，ChatGPT通过大模型对语义内容理解
3. **生成方案**：ChatGPT 输出详细的 Step-by-Step 解决方案
4. **生成指令**：LLM 根据规划 Plan 生成可执行的操作或指令
5. **执行指令**：通过访问外部资源或调用ChatGPT完成任务
6. **输出结果**：指令操作完成后，系统返回执行结果
7. **评估结果**：AI 会评估结果以确定是否达到预期目标或是否需要进一步完善

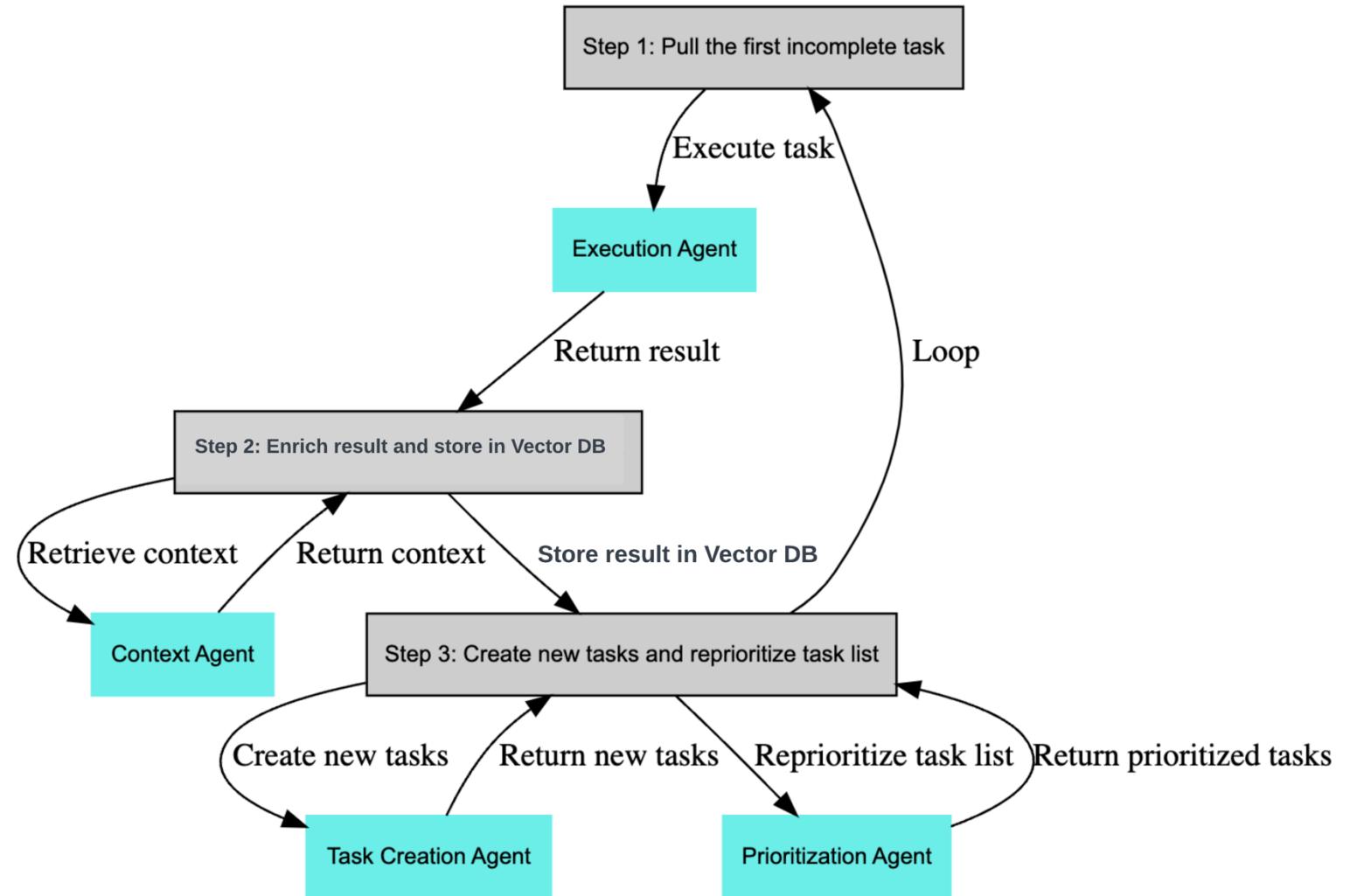
AutoGPT



AutoGPT：视频

BabyAGI

- 使用 OpenAI LLMs 和矢量数据库创建、优先排序和执行任务。Agent 根据历史结果和用户的目标创建任务。然后利用 LLMs 对任务进行规划 Planning，利用向量数据库对过去的结果进行存储和检索。



AgentGPT

- AgentGPT 基于 Langchain 和 OpenAI 基础构建 AI Agent。可以通过浏览器或个人计算机中创建、配置和部署自主 AI 代理。
- AgentGPT 允许配置和部署自治 AI 代理。命名自己的自定义 AI，让它开始实现任何可以想象的目标。它将尝试通过思考要做的任务、执行它们并从结果中学习来达到目标。

3. Multimodal Agent

跨模态Agents

- Agents不仅可以处理纯文本的信息，还可以拓展到多模态来完成图像，语音，视频的交互。典型的应用有Visual ChatGPT，AssistGPT，HuggingGPT。

HuggingGPT

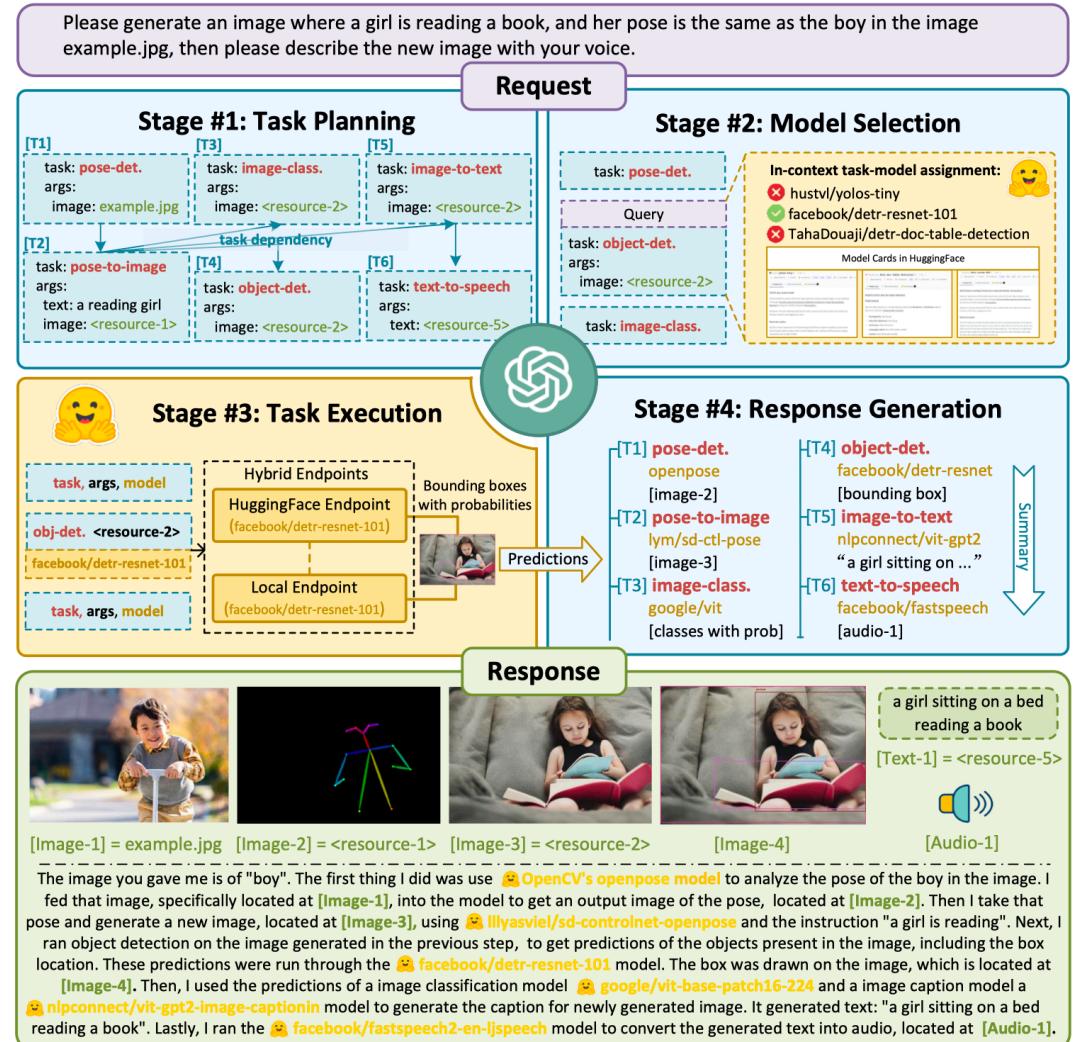
- HuggingGPT 把 LLM 作为一个 Agent，用于管理和组织 Huggingface 上的模型（文生图、图生文、目标检测等模型），LLM 首先会根据用户的请求规划一个任务清单，然后给每个任务指派一个 HuggingFace 模型，AI 模型执行完以后，LLM 收集结果并返回给用户。

HuggingGPT总体架构

- LLM 作为中心 Agent，模型作为 Tools or Action，执行分为四个阶段：
 1. 任务规划（Task Planning）：LLM 把用户请求分解成任务集合，决定执行顺序和任务之间的资源依赖；
 2. 模型选择（Model Selection）：根据 HuggingFace 模型描述，LLM 把任务安排给对应的模型；
 3. 任务执行（Task Execution）：HuggingFace 上的模型执行指派的任务；
 4. 响应生成（Response Generation）：LLM 集合模型输出结果，生成workflow日志摘要返回给用户。

HuggingGPT总体架构

- LLM 作为中心 Agent，模型作为 Tools or Action，执行分为四个阶段：
 - 任务规划（Task Planning）：LLM 把用户请求分解成任务集合，决定执行顺序和任务之间的资源依赖；
 - 模型选择（Model Selection）：根据 HuggingFace 模型描述，LLM 把任务安排给对应的模型；
 - 任务执行（Task Execution）：HuggingFace 上的模型执行指派的任务；
 - 响应生成（Response Generation）：LLM 集合模型输出结果，生成 workflow 日志摘要返回给用户。



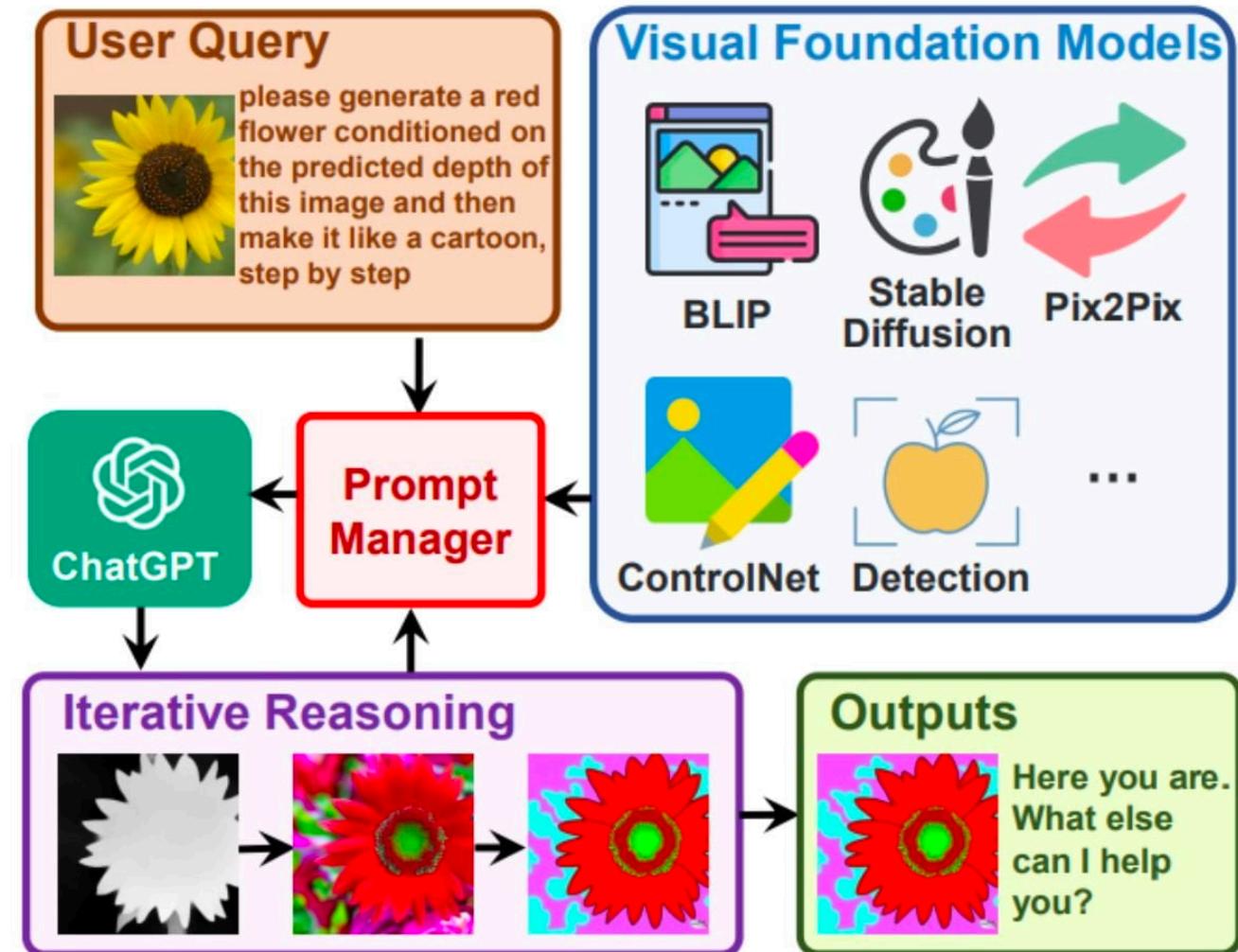
AssistGPT

- AssistGPT 采用了为 Plan, Execute, Inspect, and Learn (PEIL) 的交错代码和语言推理方法，将 LLMs 与各种工具集成起来。
- Planner 能够使用 NLP 来计划基于当前推理进度，Executor 哪个工具应该接下来执行。Inspector 作为高效内存管理器，可以帮助 Planner 将适当的 CV 信息输入到特定工具。通过 Learner 使模型能够自主地探索和发现最优解。



Visual ChatGPT

- Visual ChatGPT 的思路是使用 chatGPT 调用视觉模型来迭代的完成图像编辑的任务。



Reference 参考引用

1. Generative Agents: Interactive Simulacra of Human Behavior <https://arxiv.org/abs/2304.03442>
2. <https://www.youtube.com/watch?v=XY5Wncq5vAE>
3. <https://medium.com/geekculture/googles-ai-agents-in-a-sims-inspired-virtual-town-small-ville-stanford-artificial-intelligence-chat-gpt-c0f2110239e2>
4. https://zhuanlan.zhihu.com/p/626671728?utm_id=0
5. CAMEL: Communicative Agents for "Mind" Exploration of Large Language Model Society. <https://arxiv.org/abs/2303.17760>
6. https://zhuanlan.zhihu.com/p/629909493?utm_id=0
7. <https://github.com/Significant-Gravitas/AutoGPT>
8. Auto-GPT for Online Decision Making: Benchmarks and Additional Opinions <https://arxiv.org/abs/2306.02224>
9. <https://github.com/Significant-Gravitas/AutoGPT/blob/master/autogpts/autogpt/README.md>
10. <https://arxiv.org/pdf/2305.05352>
11. [Exploring the Potentials of ChatGPT as a Cooperative Agent](#)
12. AssistGPT: A General Multi-modal Assistant that can Plan, Execute, Inspect, and Learn
13. Visual ChatGPT: Talking, Drawing and Editing with Visual Foundation Models
14. HuggingGPT: Solving AI Tasks with ChatGPT and its Friends in Hugging Face





Thank you

把AI系统带入每个开发者、每个家庭、
每个组织，构建万物互联的智能世界

Bring AI System to every person, home and
organization for a fully connected,
intelligent world.

Copyright © 2023 XXX Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. XXX may change the information at any time without notice.



Course chenzomi12.github.io

GitHub github.com/chenzomi12/DeepLearningSystem