最近读了一些LLM-based agent的工作和一些相关理论，做一个学习笔记。一直也想做一种个人级别的agent挂在后台解闷，强调agent的生动性和生活气息，同时辅助一些通用 or 细分工作，因而争取做一些技术实践。最近意难平《边缘行者》里的Lucy，AI agent的能力似乎也到了一种边缘，所以给想象中模糊的目标agent取名为LucyAgent。Lucy并非一定要是一个具体的人，而是指代这种生动的个体形象。

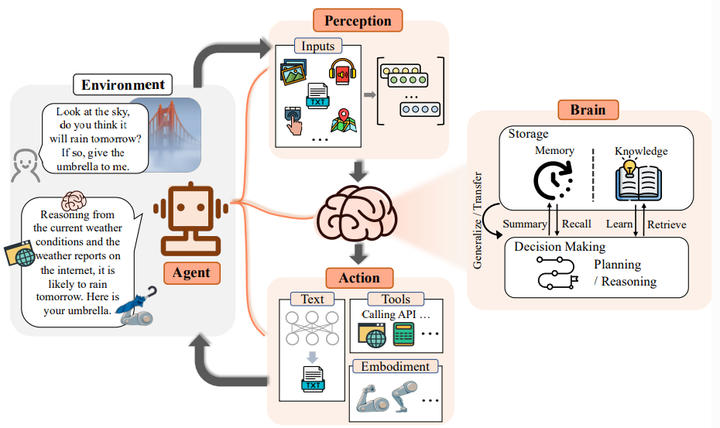
第一章介绍LLM-based agent的总体框架

**1 理论：宏观框架**

最近涌现了一大批LLM-based agent的理论框架，如人大和复旦的两篇相关survey。理论框架的指导是很重要的，因此在本章做一些介绍，主要是基于米哈游和复旦的这篇综述。

**1.1 Agent的整体架构**

arxiv.org/pdf/2309.07864v1.pdf​arxiv.org/pdf/2309.07864v1.pdf



Conceptual framework of LLM-based agent with three components: brain, perception and action.

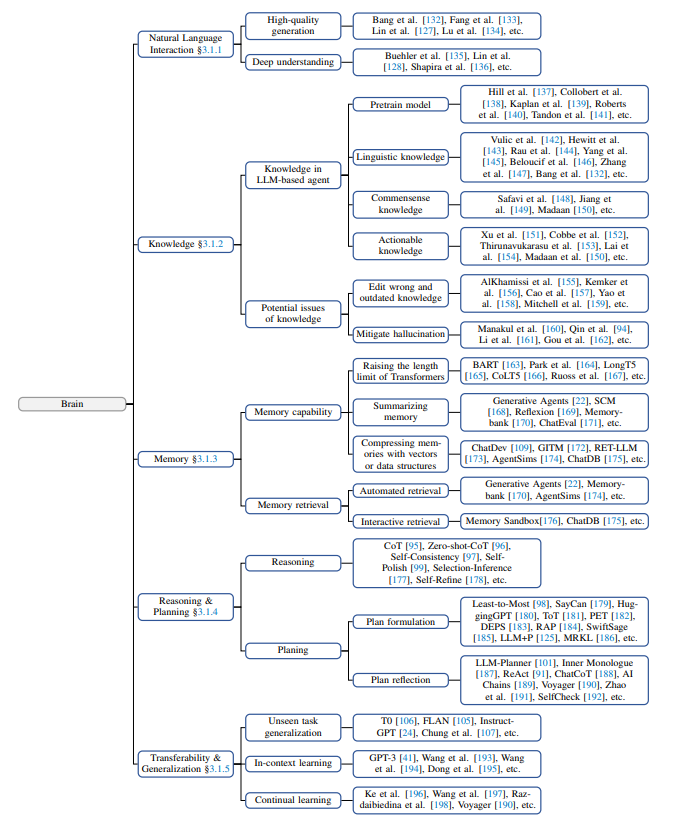
米哈游和复旦的这篇综述给定了一个LLM-based agent的概念框架图，较为清晰，细细读图其实就能理解这个框架，加上一些认识和细化后，大概意思是说：

* Agent首先是“运动”在”环境“（Enviroment）中的，环境是一种状态空间，而运动是一个抽象概念，可以将其理解为Agent的根本属性和存在形式（疑似有点马哲）。可以说agent的一切都是和这个环境相关联的，包括感知（输入），大脑（各种类型的内部处理），行动（输出）。**Agent也是环境的一部分，因而agen的行动改变环境时也可以改变agent自身。**
* Agent的“运动”可以被大致分类为感知，内部处理，行动三个部分。分别对应图中**Perception，Brain，Action**三个模块。Brain模块承担记忆、思考和决策等内在的任务；感知模块负责感知和处理来自外部环境的多模态信息；行动模块负责使用工具执行任务并影响周围环境。三个模块描述了一个agent自身状态的全部组成。其机理分别于类似于人类用眼睛，耳朵等获得信息，大脑用于处理信息和驱动四肢，四肢用于改变环境和改变人类自身。
* **Agent的内部信息通路是Perception->Brain->Action，而信息通路的设计本身也应该是Agent的一部分。**类似于人类的神经信号传输，决定了一些Agent可表征的信息、信息损失和处理效率问题。宏观来看，agent应该通过一轮或多轮的”输入->处理->输出“来完成一个任务（类似Re-Act框架），是否结束任务应由外界中断和反馈信息来确定。

为什么是多轮呢？作为人类，很多时候我们做了一件事才能看到结果，通过对上一件事的结果再次”输入->处理“，我们会推理出所做的上一件事的效果如何，而正是通过这种评价，我们决定要不要继续做这件事和下一步怎么进行。这其实是多轮的”输入->处理->输出“。从这个角度看，**如果一个agent评估了自身完成任务的情况，并且能够对没有完成好的情况制定进一步方案，或是向人类寻求帮助，是感知环境和接受反馈的智能表现。**这种方法在LLM内部已经有所体现：如向LLM提问时给出不完全的信息，LLM可能会向你索要进一步的信息。但这不是一种可控的机制性能力，它不是agent的结构所带来的，而是LLM内部的一种不太可解释的能力。

显然，每个模块都可以做进一步的细分，每个模块也有独立的运动机制，当然也有跨模块的运动机制。

**1.2 Brain模块的构件框架**



Typology of the brain module.

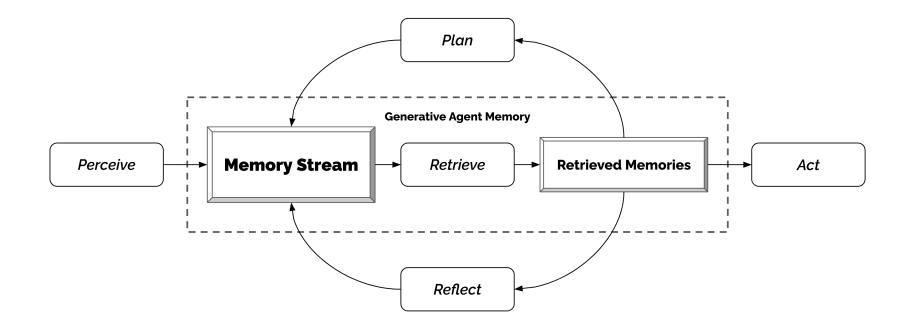
Brain理所当然是最核心的模块。Brain的运动机制大概为：**从内部信息通路接受感知模块传来的输入->将输入作为参数，从模块内的知识和记忆构件检索（似乎可统称为 ”内存“）->综合输入和检索出的数据信息进行推理和计划->从内部信息通路输出行动序列到行动模块，并且进行模块内部知识和记忆的更新。**

Brain模块有5个关键构件：自然语言交互，知识，记忆，推理和规划，可迁移性和通用性。

* **自然语言交互：**提到了多轮交互对话，高质量的自然语言生成，意图和含义理解三个部分。大概就是LLM的基础能力部分。
* **知识：**提到了三种类型的知识，即语言知识，常识知识，专业领域知识，以及潜在问题。潜在问题主要是过时、错误和幻觉。
* **记忆：**提到了agent需要特定的记忆机制来处理连续任务，记忆可以分为短期记忆和长期记忆，短期记忆即输入的上下文，长期记忆则有多种实现方式。长期记忆是一种”外骨骼“式的增强方法，主要需要获得记忆的方法，存储记忆的方法和检索记忆的方法三个内容。《Generative Agents》提供了一种可行的记忆流框架。记忆模块是提高LLM能力的重要方式之一，具体可以提高Transformer架构处理长序列的能力（短期），改善总结记忆的方法，检索记忆的方法等（长期）。

知识和记忆好像没有明显的界限，这和人类类似。我们似乎可以认为后天学习的知识就是一种记忆。因而，本文对“知识”的界定在于agent被初始化并投放到环境之前，agent所固有的知识。

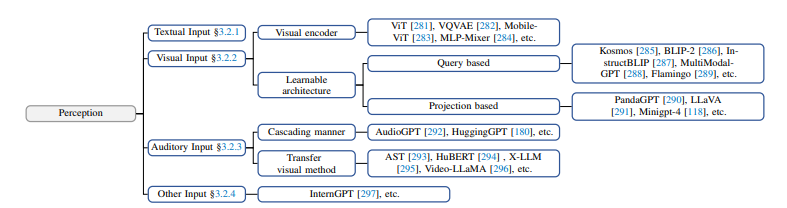
* **推理和规划：**推理更多是LLM内部的能力，但是可以通过外部方法提高，如思维链（CoT）技术及其变种。规划的核心是推理能力，但是也需要人类”要求“来激发。人类要求LLM进行规划后，LLM可以将复杂任务分解为子任务逐步解决。规划又可细分为计划制定和计划反思，制定的方法如《Generative Agents》的plan模块，反思则可以从外部评价反馈获得。



generative agent architecture.

* **可迁移性和通用性：**提到了任务泛化，情景学习，持续学习三个部分。任务泛化和情景学习大致是涉及到zero-shot learning，few-shot learning两个概念。持续学习的核心挑战是灾难性遗忘。

**1.3 Perception模块的构件框架**

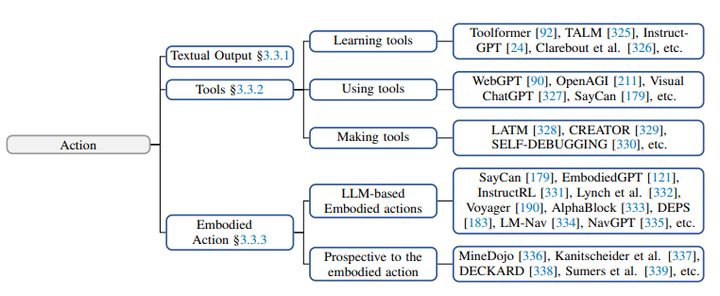


Typology of the perception module.

Perception模块的4个关键构件是:文本输入，视觉输入，听觉输入和其他输入。核心目的是将agent的感知空间从扩展到包括文字、听觉和视觉模式在内的多模态领域。如当前的GPT-4V，已经能够理解一些视觉提示（Visual Referring Prompting），并且能够排列一些打乱的序列帧（Temporal ordering）。

* **文本输入：**基础能力。重点在于理解人类的隐含含义和未知任务的文本指示。
* **视觉输入：**一种方式是为图像输入生成相应的文本描述然后链接，但是会丢失信息。一种方式是将图像编码器和 LLM 结合起来，并将图像编码转换为 LLM 可以理解的嵌入。agent用于感知图像的方法可能适用于视频领域。
* **听觉输入：**将 LLM 用作控制中心，以级联方式调用现有工具集或模型库来感知音频信息。
* **其他输入：**大致是和真实物理世界相关的一些传感器输入，同样要做预处理。

**1.4 Action模块的构件框架**



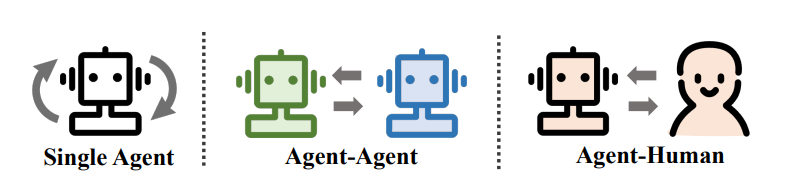
Typology of the action module.

Action模块的3个关键构件是:文本输出，工具，具身行动（embodied actions）。行动模块接收大脑模块发送的行动序列，并执行与环境互动的行动。

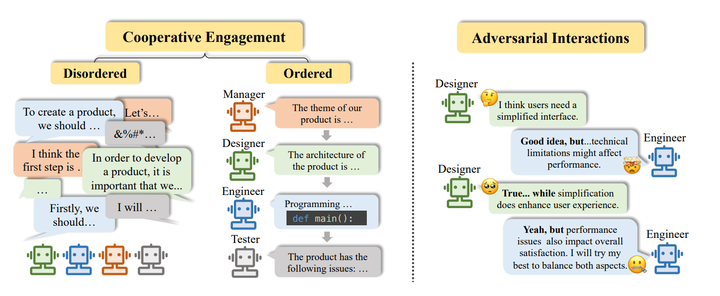
* **文本输出：**基础能力。包含内部指令的log和对外部环境的输出。
* **工具：**主要是三个方面，弥补LLM缺陷，增强agent能力，拓展LLM-based agent的行动空间。LLM有幻觉的问题，并且对于特定领域的能力不够强，所以需要一些专有工具，如科学计算，地图导航等。agent需要理解工具，使用工具，甚至制作工具。agent需要实现工具和知识库的内在协作机制。
* **具身行动：**高级话题，使agent能够以近似人类行为的方式与世界互动并理解世界。

**1.5 Agent与环境**

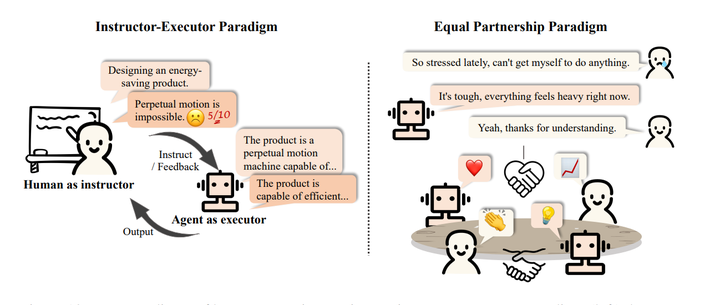
大致是一些框架，包括agent的交互形式，multiple agents的交互形式，agent human的交互形式，以及agent society的框架。都比较直观。



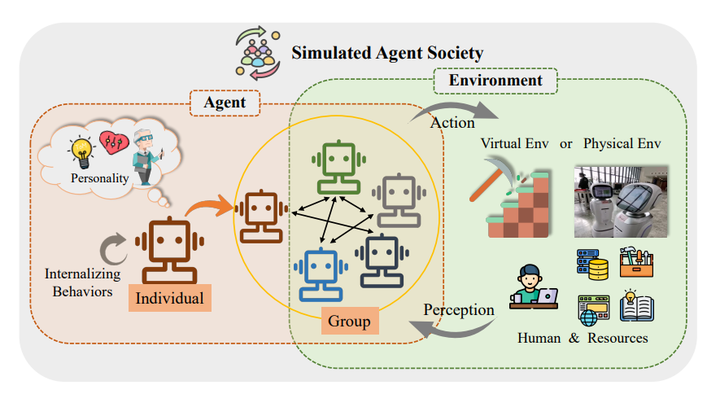
Scenarios of LLM-based agent applications.



Interaction scenarios for multiple LLM-based agents.



Two paradigms of human-agent interaction.



Overview of Simulated Agent Society.