



LLM Based Agents

Kun Yuan

Center for Machine Learning Research @ Peking University

Difference between LLM and LLM based agents

大模型与大模型智能体有什么区别?

"大模型"和"大模型智能体"这两个术语在人工智能领域中的使用可能会有些重叠，但它们通常指的是不同的概念。

大模型 (Large Models)：大模型通常指的是参数量非常大的机器学习模型，特别是深度学习模型，如神经网络。这些模型的参数量可以达到数亿、数十亿甚至更多。大模型的训练需要大量的数据和计算资源，它们能够捕捉到数据中的复杂模式和关系，因此在各种机器学习任务中表现出色，如自然语言处理、计算机视觉、语音识别等。大模型本身是静态的，它们不包含与环境交互的逻辑。

大模型智能体 (Large Model-based Agents)：大模型智能体则是指使用大模型来执行特定任务的智能体或系统。这些智能体不仅仅包含一个静态的大模型，还包括一个决策机制，使得智能体能够根据模型的输出与环境进行交互。大模型智能体通常具备一定的自主性和适应性，能够在复杂的环境中执行一系列任务。例如，自动驾驶汽车中的决策系统就是一个大模型智能体，它使用大模型来处理感知数据，并做出驾驶决策。

简而言之，大模型是关注于模型本身的大小和复杂性，而大模型智能体则是关注于如何使用这些大模型来构建能够与环境交互的智能系统。大模型智能体通常包含一个大模型作为其核心组件，但还需要其他组件来实现与环境的有效互动。

Perception

Planning

Action

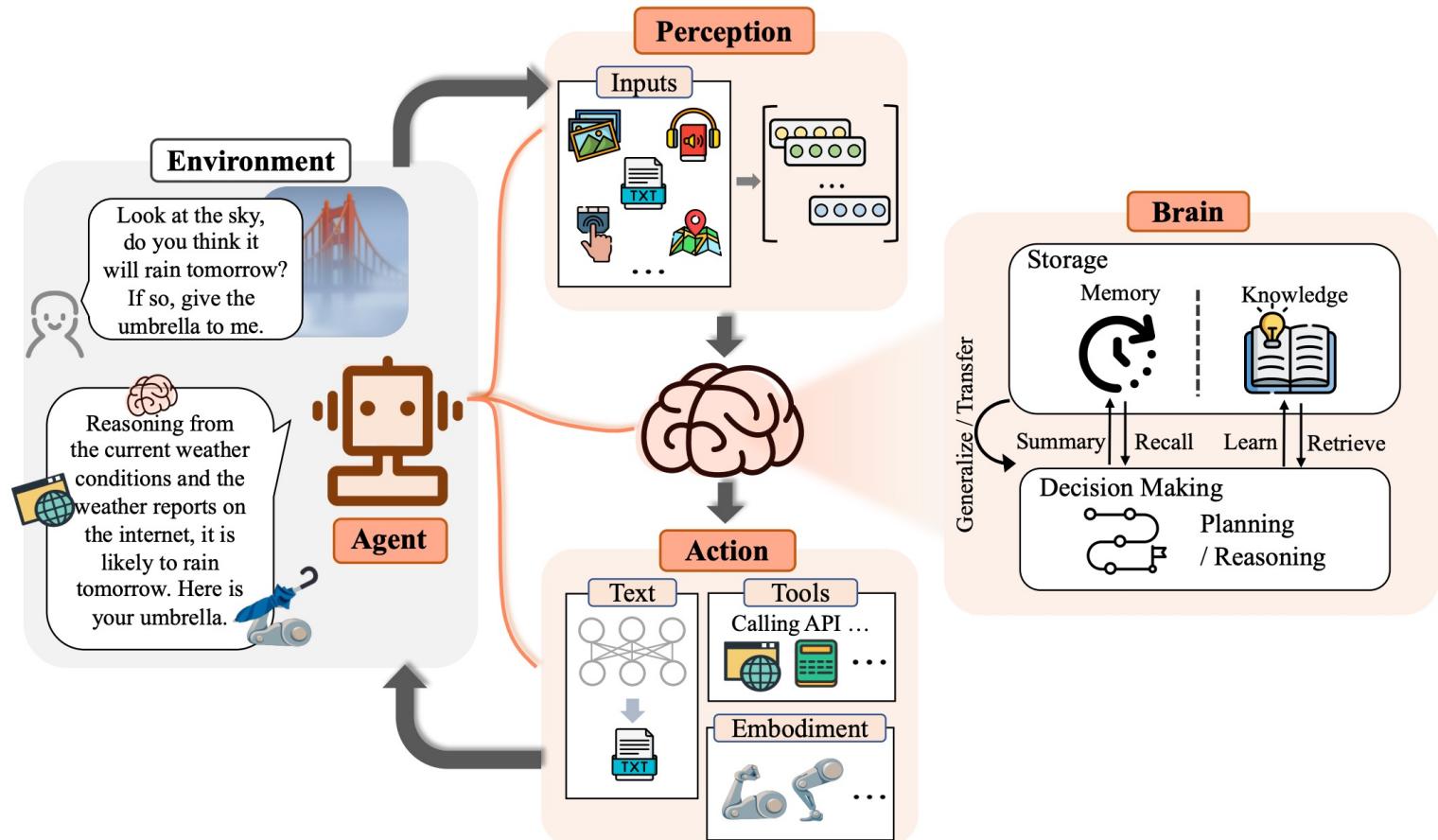
Interaction

Solve a
complicated
task

LLM based agents

Agent can finish a complete task by itself

You only specify the target task, no need to participate in the execution details



[The Rise and Potential of Large Language Model Based Agents: A Survey]

Applications



How to construct LLM based agents?

1. Choose a language model
2. Specify the role that LLM will play. Provide necessary knowledge and documents
3. Give necessary prompt instructions on how to finish the task step-by-step
4. Enable LLM to use necessary tools

Provide necessary knowledge and documents

Act as a **mathematician** in optimization.

You will help solve the long-standing open question ...

Wait! LLM cannot become a professional without enough external knowledge

You have to upload the necessary external knowledge by yourself

Example: Quiz maker



模型能力调用

- 联网能力
- AI绘画
- 代码能力 让智能体可以自行编写代码来执行任务, 可以处理简单的计算及数据分析等任务

知识库文件

构建知识库, 为智能体提供个性化知识输入, 更好的解决问题。
支持pdf(不支持扫描件)、doc、docx、xlsx、txt等文件格式, 一次最多上传50个文件, 整体知识库最多支持1000个文件(每个100MB), 知识库总字数不超过1亿字。

全选

LLM-TAP (1)

约16.07万字 删除文件

知识库回答配置

知识库名称 >

Give necessary prompt instructions on how to finish the task

Decompose the task into several step-by-step subtasks

配置信息 *

描述你想创建的智能体，包括它的作用和特点，以及对它生成结果的预期。(最多支持4096个字)

示例1：工具 ⓘ

示例2：游戏 ⓘ

示例3：角色 ⓘ

示例4：画图 ⓘ

根据用户指定的考察内容，做如下步骤：

第1步：生成3道选择题。每道题有4个选项。其中只有一个选项是正确的。

第2步：生成3道判断题。

第3步：生成3道填空题。

第4步：生成1道论述题。

最后，鼓励学生用心答题，仔细思考

Enable LLM to use necessary tools

Enable LLM to plot, code, mathematical reasoning, call APIs ...

模型能力调用

- 联网能力
- AI绘画
- 代码能力 让智能体可以自行编写代码来执行任务，可以处理简单的计算及数据分析等任务

知识库文件

构建知识库，为智能体提供个性化知识输入，更好的解决问题。
支持pdf（不支持扫描件）、doc、docx、xlsx、txt等文件格式，一次最多上传50个文件，整体知识库最多支持1000个文件（每个100MB），知识库总字数不超过1亿字。

<input type="checkbox"/> 全选	<input type="checkbox"/> LLM-TAP (1)	pdf	约16.07万字	
共1个文件				

知识库回答配置

添加API

请基于大语言模型出题



根据知识库的内容，我将为您设计一套关于大语言模型的题目。这些题目将涵盖大语言模型的应用、评估和结构等方面。

选择题

1. 思维链提示（Chain-of-Thought Prompting）用于提升大语言模型的哪方面能力？ A. 语言理解 B. 推理能力 C. 知识问答 D. 代码生成
2. 由少至多提示（Least-to-Most Prompting）方法的主要作用是什么？ A. 提升模型的语言生成能力 B. 提升模型的文本摘要能力 C. 提升模型的任务分解和规划能力 D. 提升模型的情感分析能力
3. 大语言模型在文本生成类任务上的评估指标不包括以下哪项？ A. 词法正确性 B. 语法正确性 C. 篇章正确性 D. 模型训练时间

判断题

4. 思维链提示 方法要求模型在回答问题之前先输出推理过程，以提升推理任务的性能。
(True/False)
5. 大语言模型的编码器和解码器结构在处理信息时是完全相同的。 (True/False)
6. 大语言模型在经过指令微调和强化学习阶段后，可以完成包括机器翻译、文本摘要、情感分析等多种不同种类的任务。 (True/False)

填空题

7. 大语言模型在推理规划方面，通过引导模型将复杂问题分解为多个较简单的子问题，然后逐一解决这些子问题，这种策略被称为_____。
8. 在大语言模型的解码器端，为了生成合理的目标语言序列，需要观测待翻译的源语言序列，这种机制被称为_____。
9. 大语言模型评估中，为了更全面地评估模型所生成的文本质量，需要从语言层面、_____和知识层面开展评估。

填空题

7. 大语言模型在推理规划方面，通过引导模型将复杂问题分解为多个较简单的子问题，然后逐一解决这些子问题，这种策略被称为_____。
8. 在大语言模型的解码器端，为了生成合理的目标语言序列，需要观测待翻译的源语言序列，这种机制被称为_____。
9. 大语言模型评估中，为了更全面地评估模型所生成的文本质量，需要从语言层面、_____和知识层面开展评估。

论述题

10. 论述大语言模型在处理复杂任务或问题时，如何通过由少至多提示方法来提升其性能。

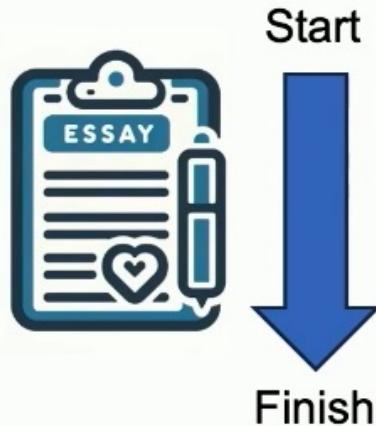
请用心答题，仔细思考。这些题目旨在帮助您更深入地理解大语言模型的应用和评估方法。

Agent-workflow can perform much better

LLM-based agents

Non-agentic workflow (zero-shot):

Please type out an essay on topic X from start to finish in one go, without using backspace.



Agentic workflow:

Write an essay outline on topic X

Do you need any web research?

Write a first draft.

Consider what parts need revision or more research.

Revise your draft.

....



[Agent reasoning by Andrew Ng]

Coding benchmark (HumanEval)

Example problem:

```
def solution(lst):
    """Given a non-empty list of integers, return the sum of all of the odd elements
    that are in even positions.
```

Examples

```
solution([5, 8, 7, 1]) =>12
solution([3, 3, 3, 3, 3]) =>9
solution([30, 13, 24, 321]) =>0
"""

```

Solution:

```
return sum(lst[i] for i in range(0, len(lst)) if i % 2 == 0 and lst[i] % 2 == 1)
```

答案可能是这样一段代码片段。

Source: Evaluating Large Language Models by Andrew Ng
And it turns out the answer is code snippet like that.

Andrew Ng

[Agent reasoning by Andrew Ng]

Agent-workflow can perform much better

1. Reflection



Please write code for {task}

```
def do_task(x): ...
```

```
def do_task_v2(x):
```

```
def do_task_v3(x):
```



Coder Agent
(LLM)

Here's code intended for {task}:

```
def do_task (x):  
    ...
```

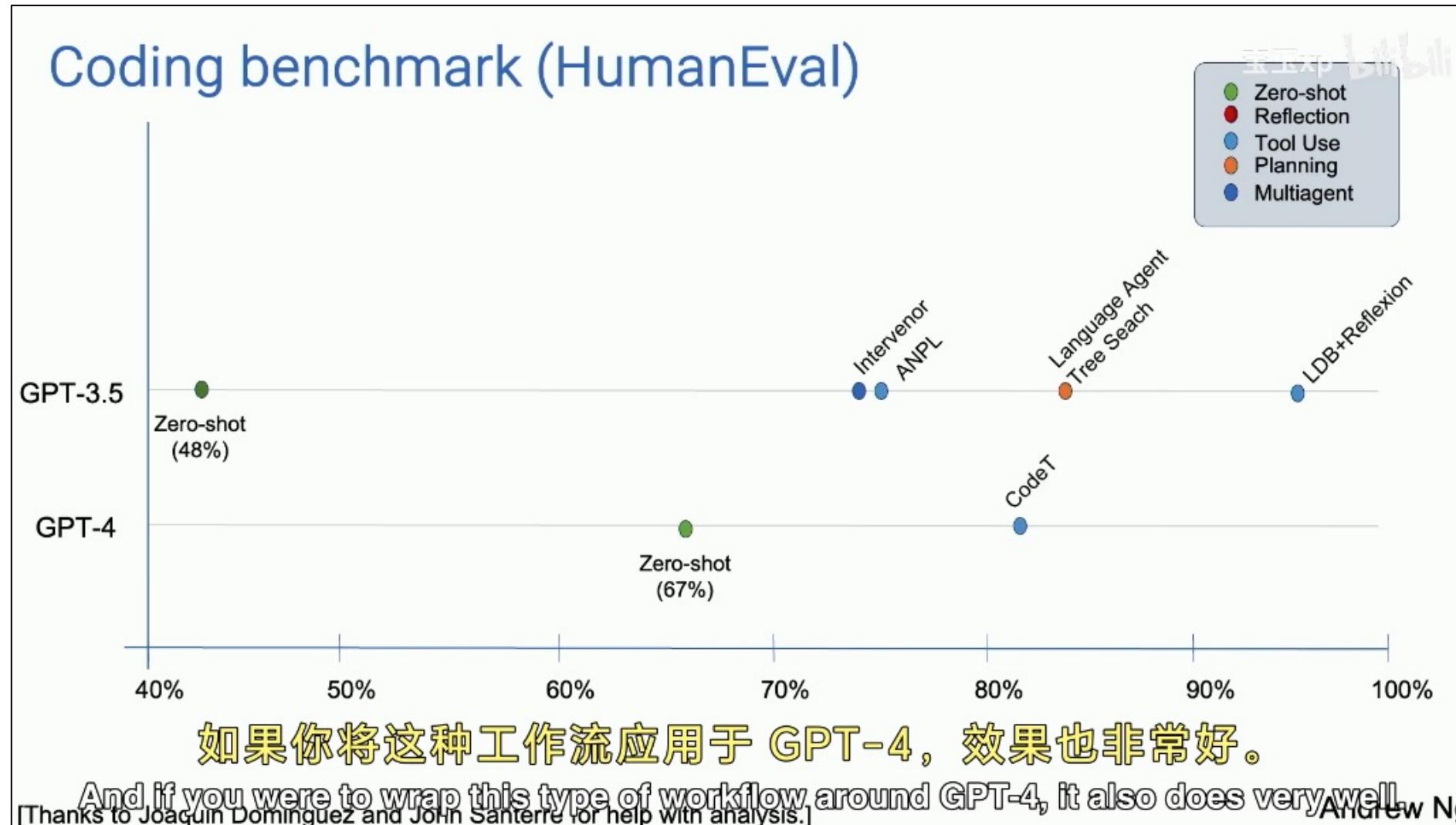
Check the code carefully for correctness, style and efficiency, and give constructive criticism for how to improve it.

There's a bug on line 5. Fix it by ...

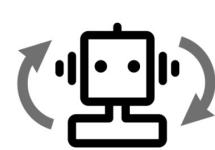
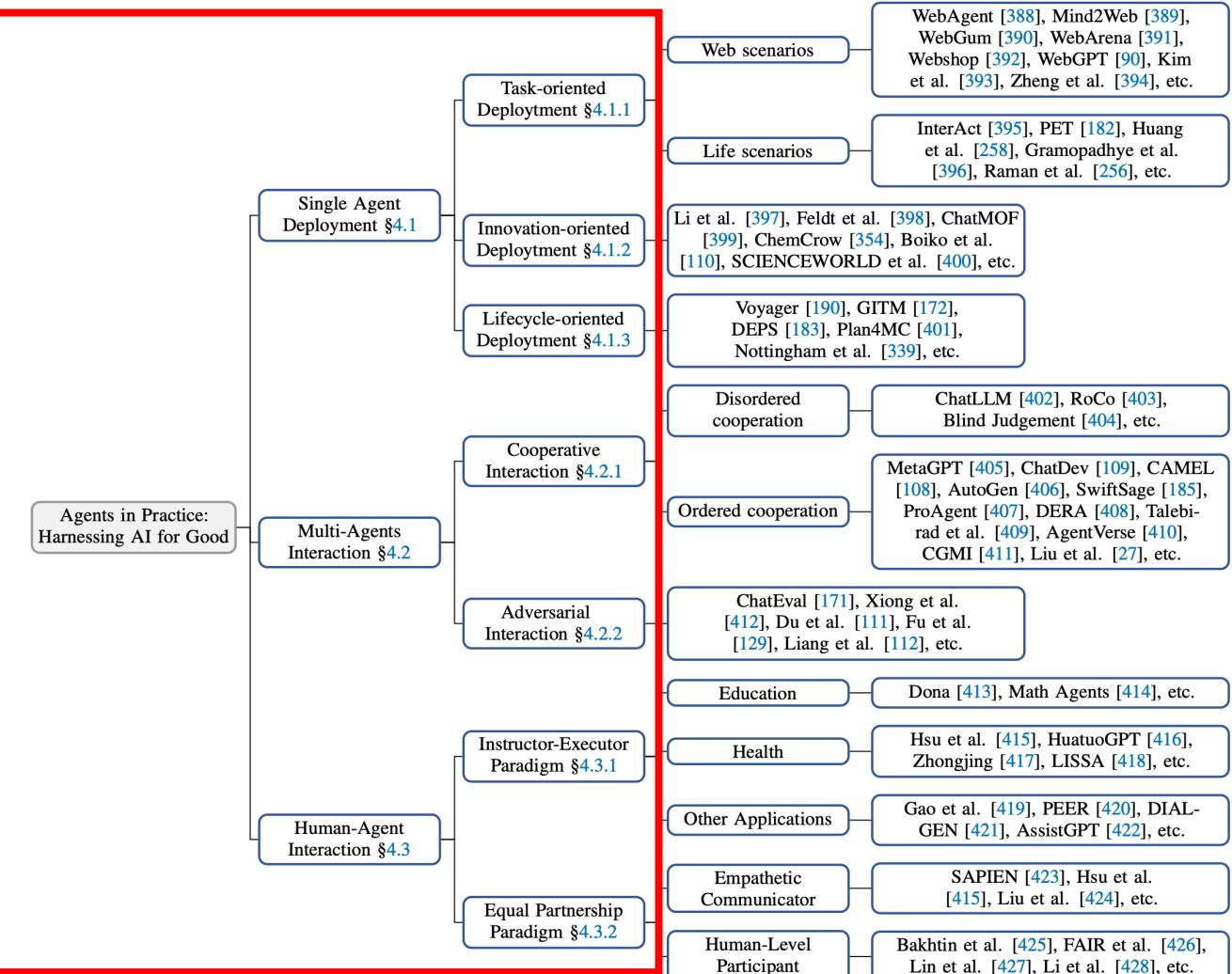
It failed Unit Test 3. Try changing ...

Recommending:
顺便说一句，对于那些想要了解更多关于这些技术的人，
 • Self-Refine: Iterative Refinement with Self-Feedback, Madaan et al. (2023)
 • By the way, for those of you that want to learn more about these technologies, Andrew Ng

Agent-workflow can perform much better



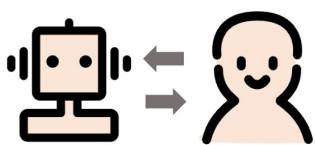
Agents in practice



Single Agent

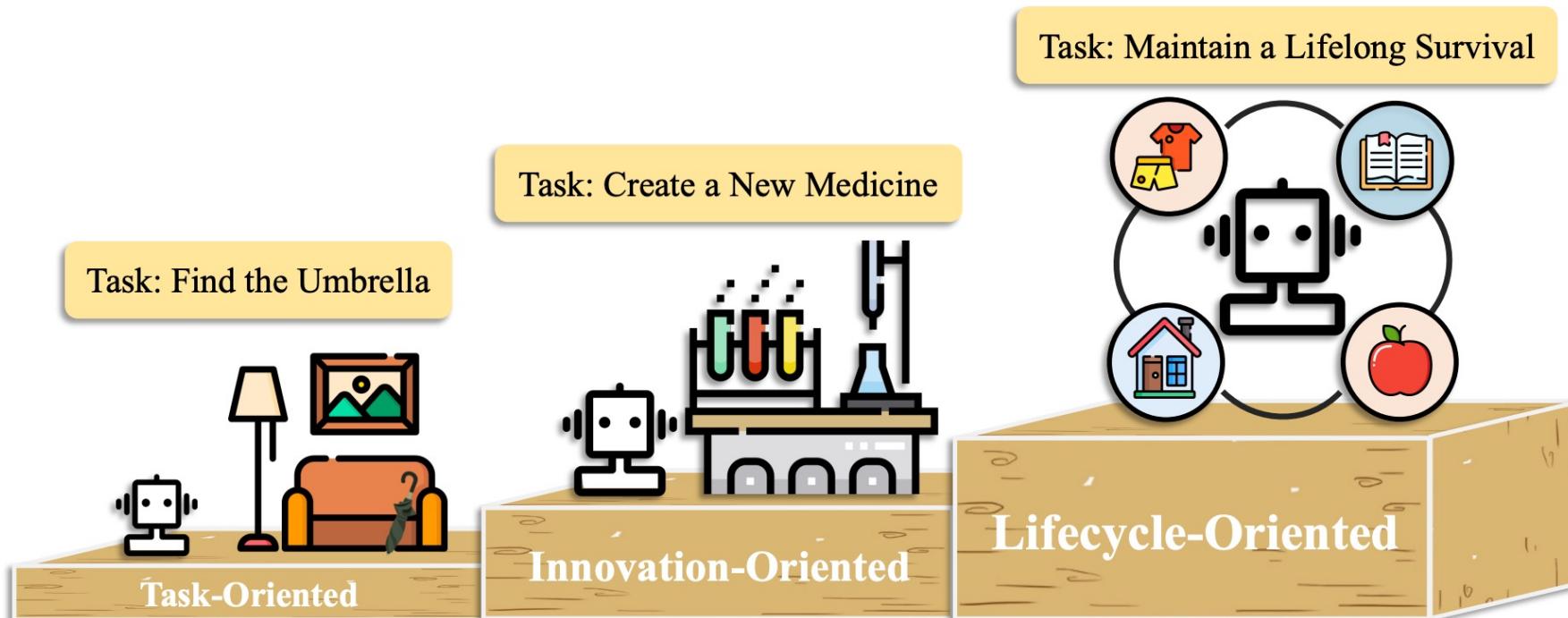


Agent-Agent



Agent-Human

Single agent



[The Rise and Potential of Large Language Model Based Agents: A Survey]

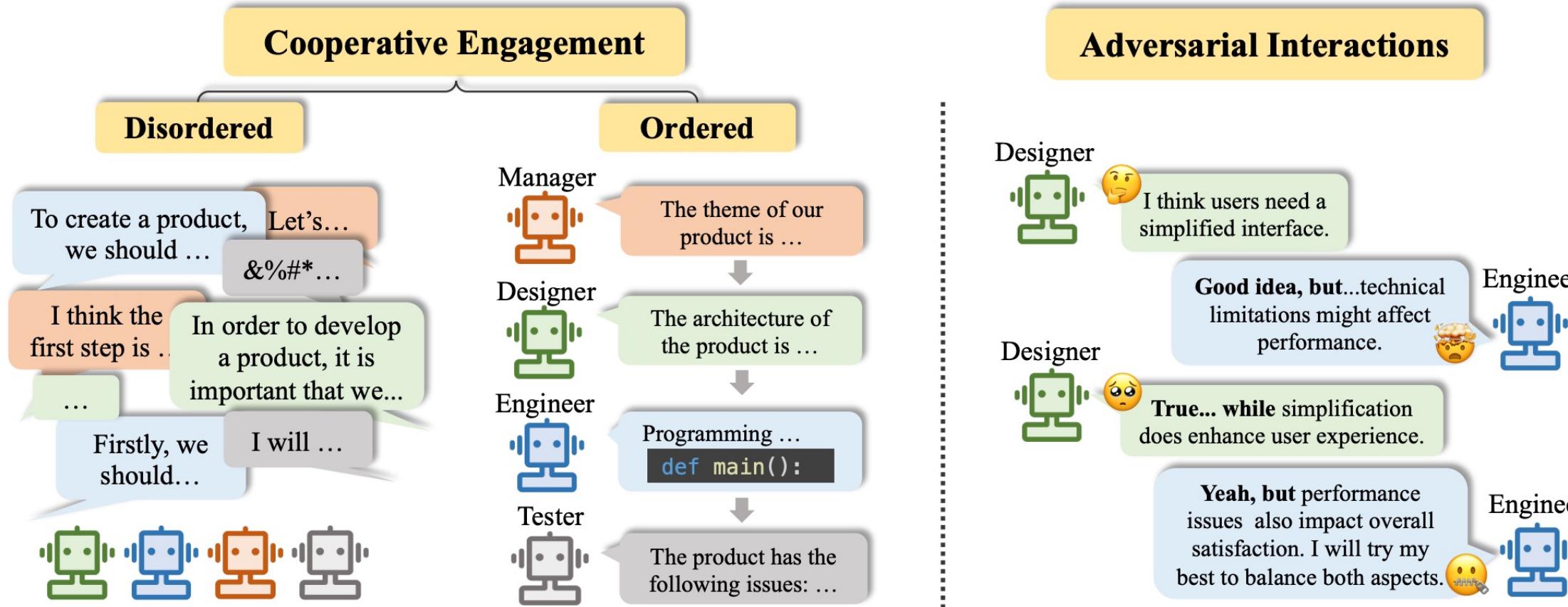
Single agent

In **task-oriented deployment**, agents assist human users in solving daily tasks. They need to possess basic instruction comprehension and task decomposition abilities.

In **innovation-oriented deployment**, agents demonstrate the potential for autonomous exploration in scientific domains.

In **lifecycle-oriented deployment**, agents have the ability to continuously explore, learn, and utilize new skills to ensure long-term survival in an open world.

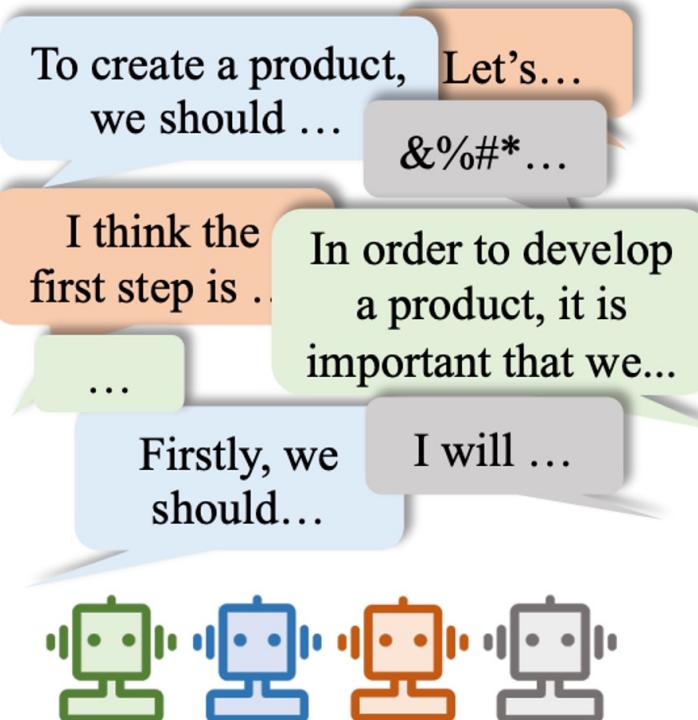
Multiple agents



[The Rise and Potential of Large Language Model Based Agents: A Survey]

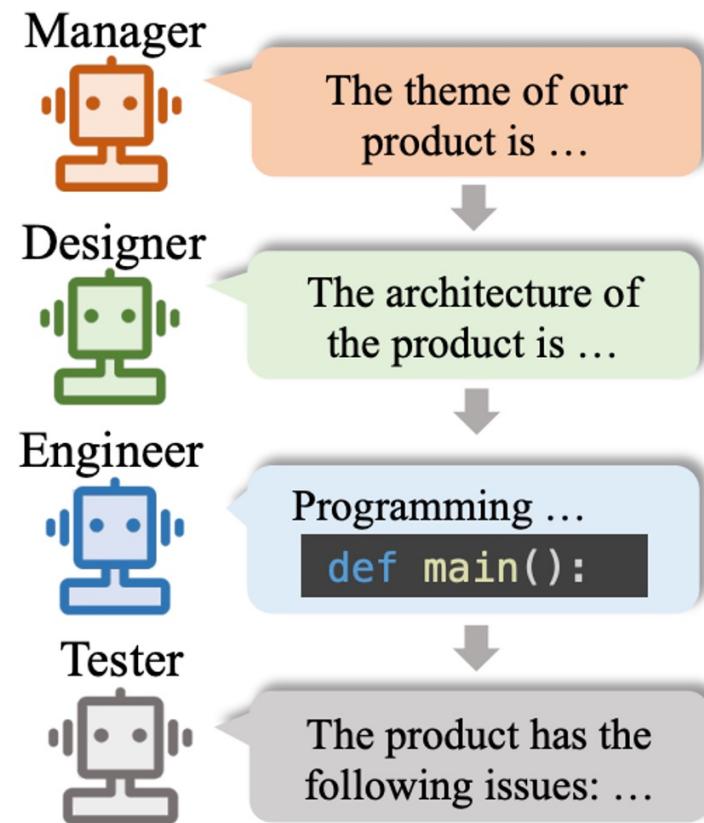
Multiple agents

Disordered cooperation. When three or more agents are present within a system, each agent is free to express their perspectives and opinions openly. They can provide feedback and suggestions for modifying responses related to the task at hand.



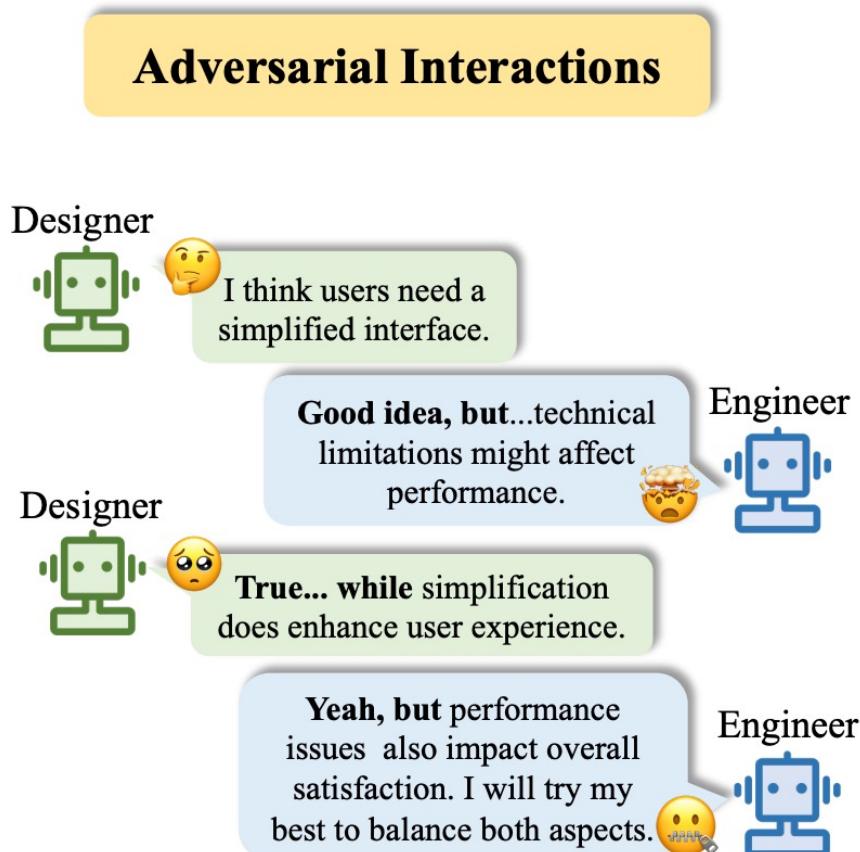
Multiple agents

Ordered cooperation. When agents in the system adhere to specific rules, for instance, expressing their opinions one by one in a sequential manner, downstream agents only need to focus on the outputs from upstream



Multiple agents

In **adversarial interaction**, agents compete in a tit-for-tat fashion to enhance their performance.



2. 颜色代码

- 设计师: “这个按钮应该用#FF0000的颜色。”
- 程序员: “这不是红色吗? 我们之前已经用过了。”
- 设计师: “不, 这是更深的红色。”

4. 像素完美

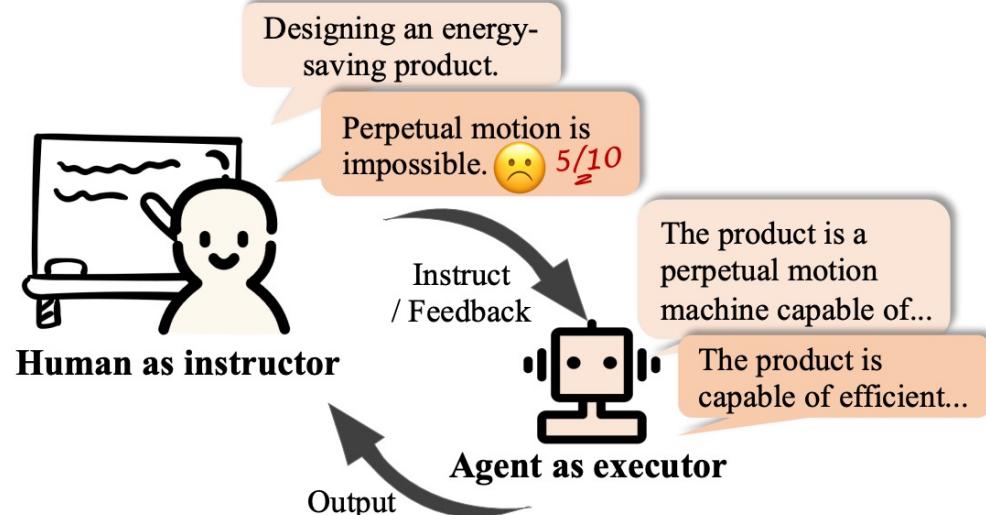
- 设计师: “为什么这个图片在网页上看起来这么模糊?”
- 程序员: “因为它是按照屏幕分辨率缩放的。”
- 设计师: “但我在设计稿上看起来是完美的!”

5. 需求变更

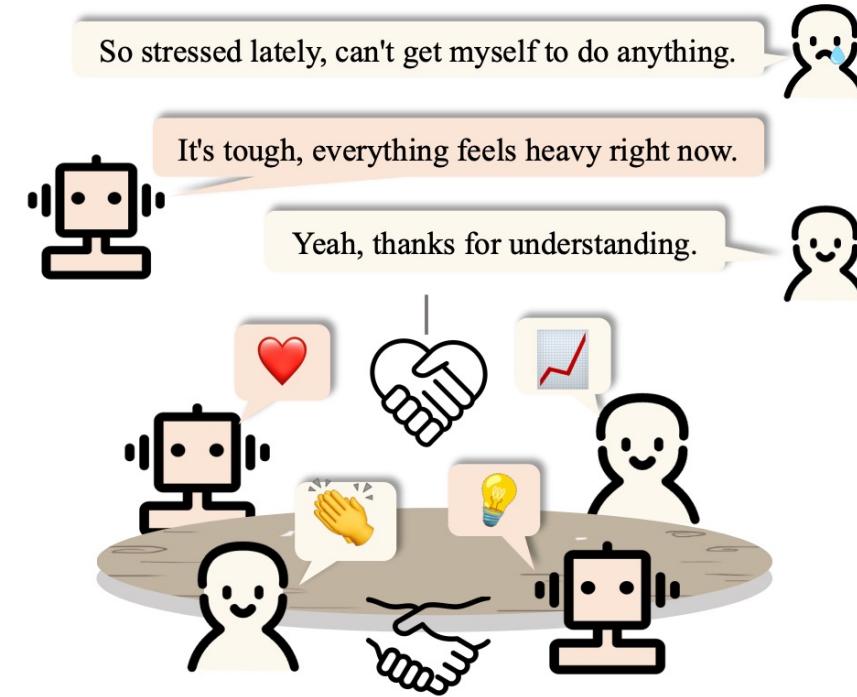
- 设计师: “我们需要把这个按钮改成圆形。”
- 程序员: (花了几个小时修改代码)
- 设计师: “哦, 我突然觉得方形更好。”

Human-agent interaction

Instructor-Executor Paradigm



Equal Partnership Paradigm

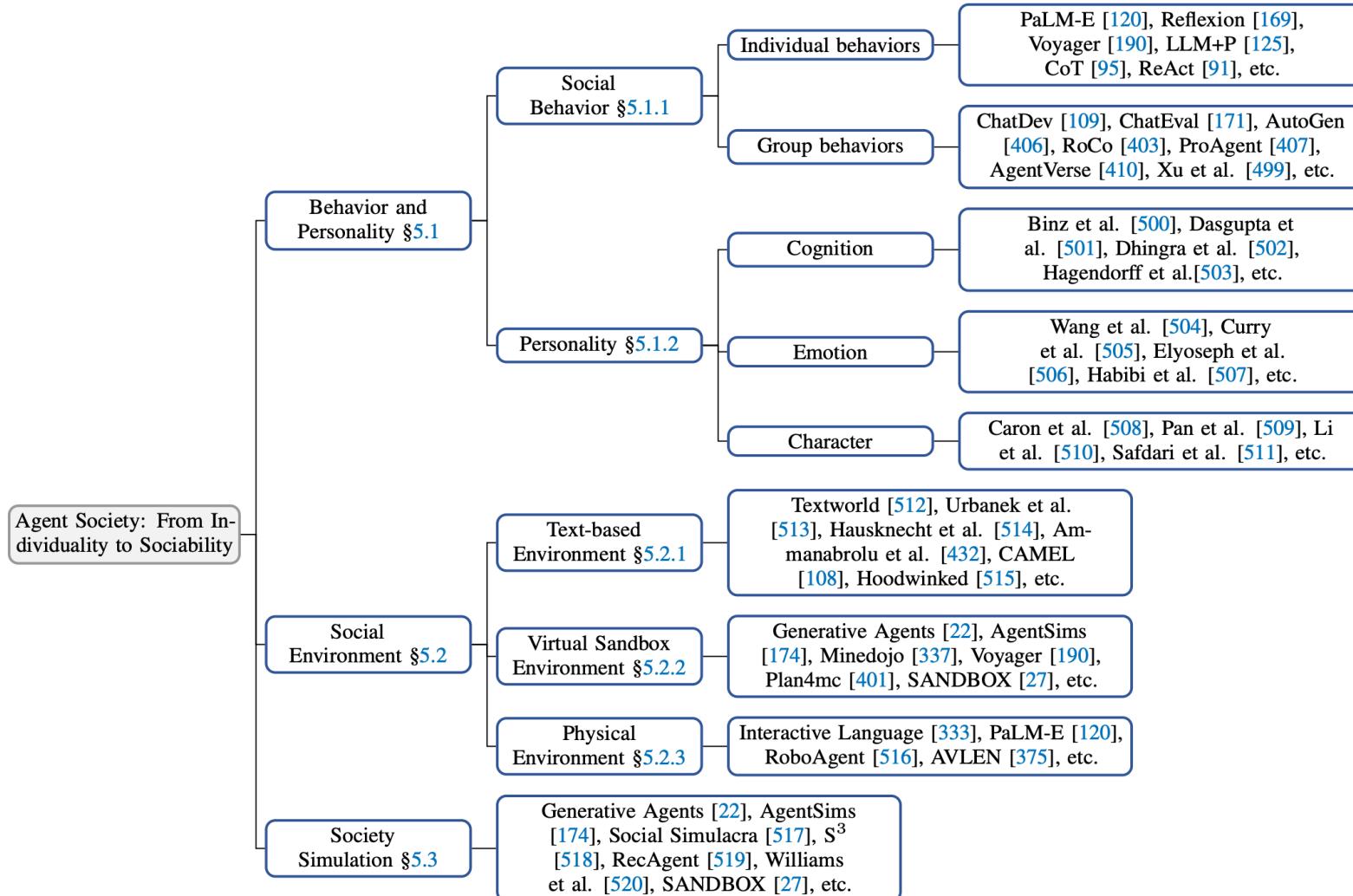


[The Rise and Potential of Large Language Model Based Agents: A Survey]

In **Instructor-Executor Paradigm**, humans provide clear and specific instructions directly, while the agents' role is to understand natural language commands from humans and translate them into corresponding actions

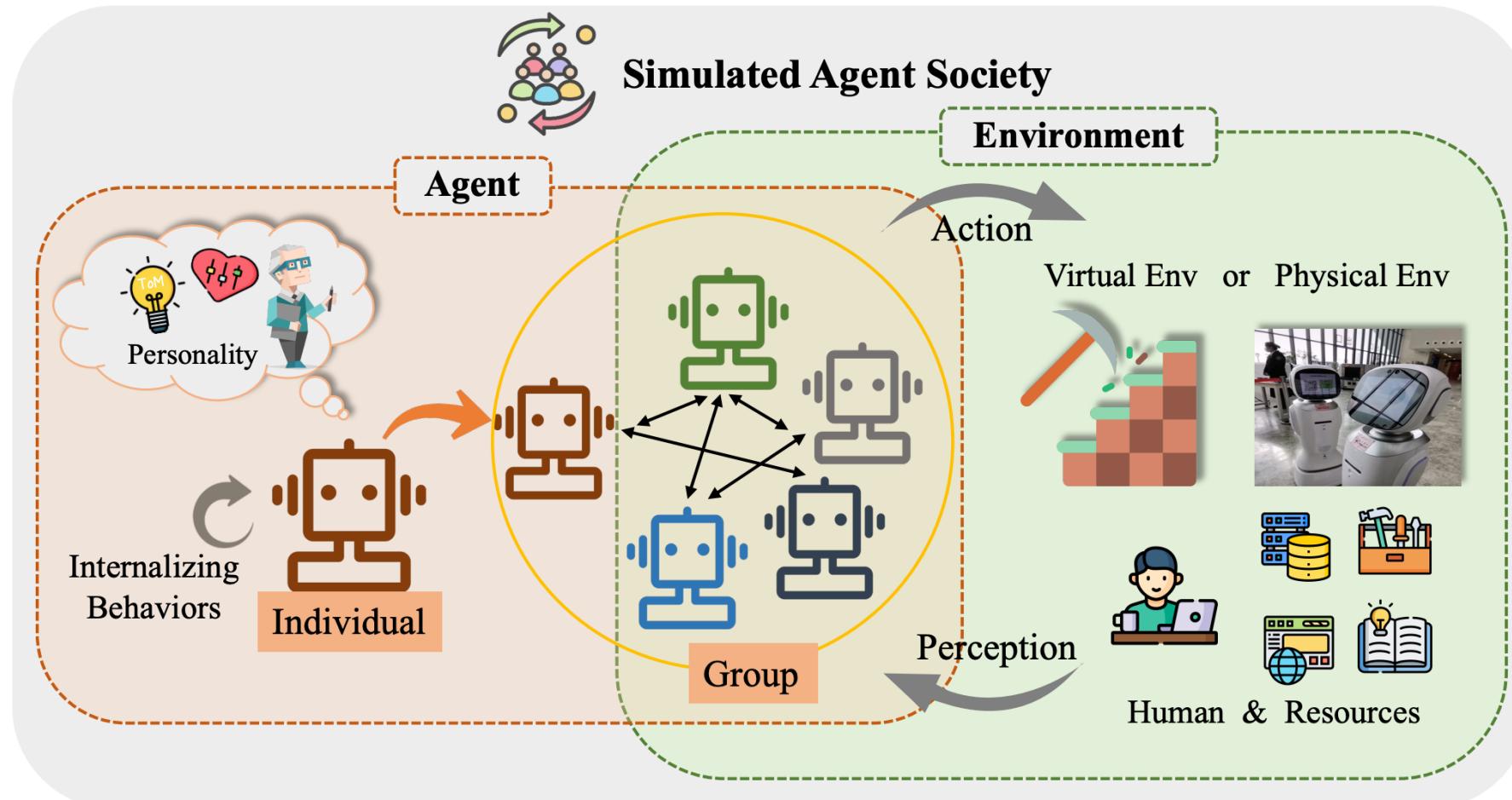
In the **equal partnership** paradigm (right), agents are human-like, able to engage in empathetic conversation and participate in collaborative tasks with humans

Agent Society: From Individuality to Sociability



[The Rise and Potential of Large Language Model Based Agents: A Survey]

Agent Society: From Individuality to Sociality



[The Rise and Potential of Large Language Model Based Agents: A Survey]

Agent Society: From Individuality to Sociality



At the **individual** level, an agent exhibits internalizing behaviors like planning, reasoning, and reflection. It also displays intrinsic personality traits involving cognition, emotion, and character

An agent and other agents can form **groups** and exhibit group behaviors, such as cooperation

The **environment**, whether virtual or physical, contains human actors and all available resources. For a single agent, other agents are also part of the environment. The agents have the ability to interact with the environment via perception and action

Agents sandbox



[Generative Agents: Interactive Simulacra of Human Behavior]

Predict the social and economic impact of decision-making

Deduce military activities

Shorten the process of social science experiments

Conclusion

The range of tasks AI can accomplish is poised to expand dramatically

We need to get used to letting AI handle tasks to boost our efficiency

Huge research opportunity when pushing single-agent to multiple-agents

Fast token generation is important due to the tremendous interaction within or between agents