

什么是 AI Agent ?

2024 入门版



01

什么是 AI Agent ?

最牛的Agent Prompt

妈！我饿了！

一个极端的例子



AI Agent 的定义

让 AI 以类似人的工作和思考方式
来完成一系列的任务

来自 *OpenAI* 相关人员, *Agent...*

**靠LLM思考
能使用工具
能召唤帮手**

所以

给出任务，能帮你搞定的，就是 Agent



02

决策流程

AI Agent 的基本决策流程

P (感知) → P (规划) → A (行动)

妈！我饿了！

P (感知) → P (规划) → A (行动)

听到

做TA爱吃的



P (感知) → P (规划) → A (行动)

APP下单

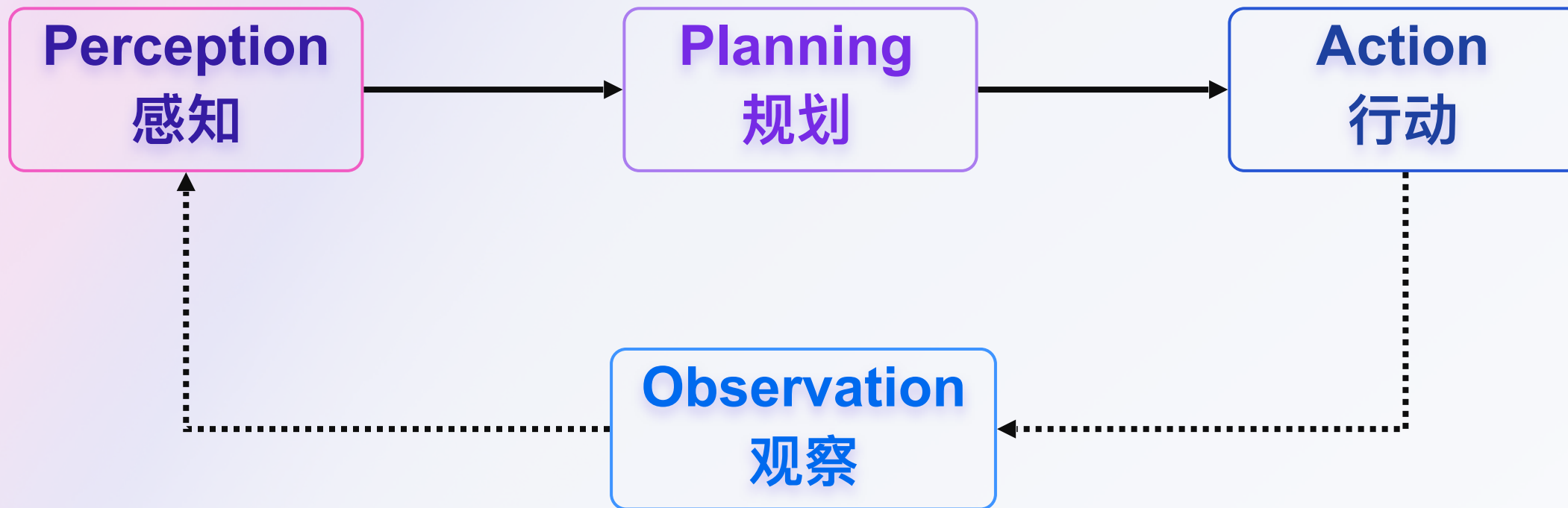
餐厅接单



快递小哥接单



AI Agent 的基本决策流程





03

AI Agent 的组成

每个 Agent 都会包括

- 大脑 (LLM)
- 规划 (Planning)
- 记忆 (Memory)
- 工具使用 (Tool use)

以LLM（大语言模型）作为Agents的大脑是一个很新的概念

一项复杂的任务通常涉及许多步骤，Agent 需要知道这些步骤并提前进行规划。

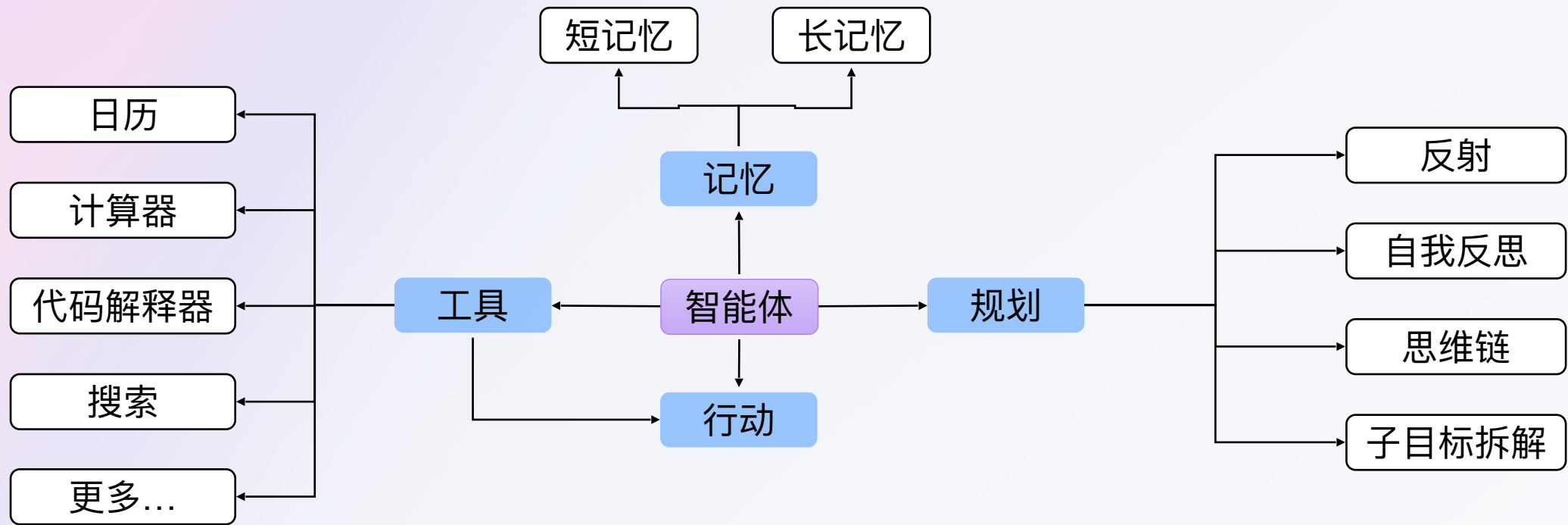
- 子目标和分解
- 反思和完善

对应人脑的记忆类型，可以用以下映射表述 agent 中的记忆模块：

- 短期记忆包含所有上下文内容。受到 Transformer 有限上下文窗口长度的限制。
- 长期记忆作为 Agent 在查询时可以处理的外部存储数据库，可通过快速检索进行访问。

AI Agent 可以调用外部 API，以获取模型权重中缺少的额外信息，包括当前信息、代码执行能力、对专有信息源的访问等。

LLM 驱动下的 AI Agents System 概览

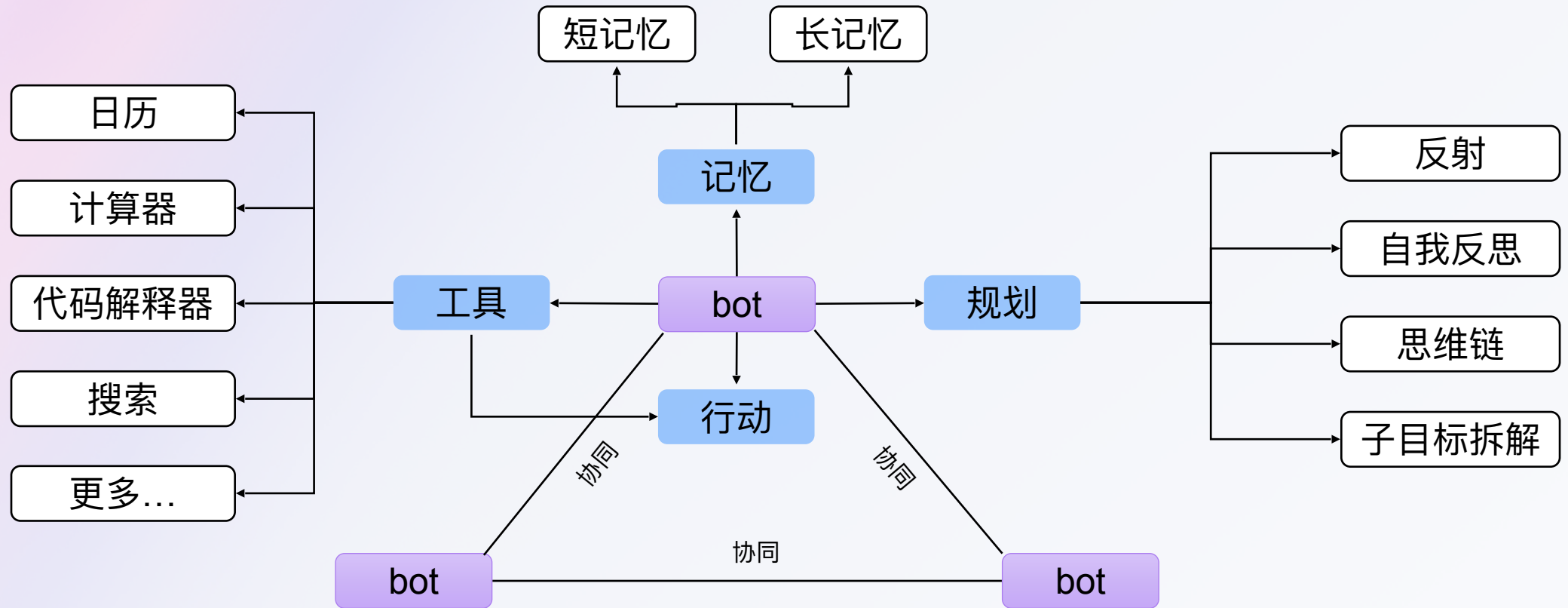


bot

每个 Bot 都可能会包括

- 大脑 (LLM)
- 规划 (Planning)
- 记忆 (Memory)
- 工具使用 (Tool use)

LLM 驱动下的 AI Agents System 概览



The background features a light blue gradient with several decorative elements: two concentric circles centered on the left, a pink dot on the top-left circle, a blue dot on the bottom-right circle, and a purple sphere in the top-right corner. A large, glowing purple sphere is positioned on the left side, partially overlapping the inner circle.

04

AI Agent 的问题

- LLM 会出现格式与内容错误、甚至在一些时候也会表现出叛逆行为。
- 是否需要另一个 Agent 来监控这个 Agent?
- 为保证 AI Agent 决策的透明性，系统可能需要向用户展示推理过程。
- AI Agent 需要处理大量的数据，这可能导致隐私泄露的问题。
- LLM的上下文限制，影响大体量任务的执行
- 单一LLM训练数据有限，而使用不同LLM会导致执行结论不同



05

AI Agent 和我们的关系

作用

作为 AI 的新型应用模式

Agent 无论是作为我们的助力还是独立智能体

都将显著提高工作效率，激发创新活力

人的价值

在智能体生态系统时代

企业中最具价值的员工

将会是那些擅长为智能体制定行动准则的人

是时候去和 AI 共舞了



Thank You 