一句话告诉你 AI Agent 比 LLMs、工作流厉害在哪里

LLM 是**被动**的，仅根据人类的提示和其内部知识库来响应。

AI 工作流 的关键特征在于**人类为 LLM 设定了一条路径**（控制逻辑），使其可以访问外部工具。

AI 智能体 的核心转变是 **LLM 成为决策者**，它能自主进行**推理**、**行动**（使用工具）和**迭代**，以达成目标。

第一级：大型语言模型 (LLMs)

流行的 AI 聊天机器人，Deepseek、ChatGPT、Google Gemini，都是基于大型语言模型（LLMs）构建的应用，**擅长生成和编辑文本**。

工作原理：

- 你（人类）提供一个输入（Prompt/提示词）。
- LLM 根据其训练数据生成一个输出。
    - 要求 DS 帮忙起草一封约客户会面的邮件，你的要求是输入，邮件内容就是输出。

LLMs 的两个关键特征

1. **知识有限：** 尽管经过大量数据训练，但它们对专有信息（如个人或公司内部数据）的**了解有限**。

比如 DS“我的下次会议是什么时候？”，肯定会失败，因为它无法访问你的日历。

1. **被动：** 它们**等待我们的提示**，然后做出响应。

第二级：AI 工作流

AI 工作流通过引入外部工具和预定义路径来扩展 LLMs 的能力。

工作原理

人类设定逻辑： 告诉 LLM“每当我询问个人活动时，先执行搜索查询并从我的日历中获取数据，然后再回复。”

遵循预设路径： LLM 遵循人类设定的**预定义路径**（也称为控制逻辑）。

如果预设路径是“总是搜索日历”，那么当你询问“某日天气如何？”时，LLM 会失败，因为日历中没有天气信息。

可以增加更多步骤： 可以在工作流中添加更多步骤，例如允许 LLM 通过 API 访问天气信息，甚至使用文本转音频模型来语音播报答案。

人类是决策者： 无论添加多少步骤，只要**人类是决策者**，它仍然只是一个 AI 工作流，没有 AI 智能体的参与。

某个工作流项目示例

*一个遵循**预定义路径**的 AI 工作流*:

使用预设表格： 收集新闻文章链接→ 总结这些新闻文章→**使用 Claude：** 根据提示起草发 blog 的帖子。

自动安排： 设置为每天早上 8 点自动运行。

工作流的局限性

缺乏迭代能力： 如果对最终输出（例如 blog 帖子）不满意，人类必须**手动**回去修改给 Claude 的提示。这种试错和迭代目前由人类完成。

热门名词提示：RAG (检索增强生成)

RAG 是一个常被提及的术语。

简单来说： RAG 是一个帮助 AI 模型在回答前**查找信息**的过程，例如访问日历或天气服务。

本质上： RAG **只是一种 AI 工作流**。

第三级：AI 智能体

AI 智能体将工作流中的**人类决策者**替换为 **LLM**。

核心能力：为了让一个 AI 工作流成为 AI 智能体，**LLM 必须取代人类决策者**。

推理（Reason）： AI 智能体必须思考实现目标的最有效方法。

目标： 根据新闻文章创建社交媒体帖子。

推理示例： 编译链接比复制粘贴文章更容易，所以决定编译链接。

行动（Act）： AI 智能体必须能够通过**工具**来做事。

行动示例： 决定使用 Google Sheets（因为用户已连接 Google 账户）而不是 Microsoft Word 或 Excel 来插入链接。

热门名词提示：ReAct 框架

AI 智能体的最常见配置是 **ReAct 框架**。

所有 AI 智能体都必须 Reason（推理）和 **Act**（行动）。

AI 智能体的第三个关键特征：迭代

AI 智能体能够**自主地**进行迭代。

为了让 blog 更有趣，AI 智能体会自主添加另一个 LLM 来**批评**自己的输出，并根据最佳实践标准重复此过程，直到满足要求，然后输出最终结果。

使用 AI 智能体示例

一些越来越莫名其妙的人机校验图片，比如“找出以下图片中所有的红绿灯”。

推理： 智能体首先思考“红绿灯”的代表形象。

行动： 然后智能体通过查看数据库里的所有图片，识别它认为是“红绿灯”的内容，给片段建立索引，或者更近一步据此生成新图片，将其返回给等待校验的用户。

人类无需参与： 智能体自主完成了所有工作，而不是由人类预先审查图片、手动识别“红绿灯”并添加标签。