

大模型的探索与实践

Introduction to Large Language Models

§ 1.3 智能体

Agent

滕佳烨
上海财经大学
www.tengjiaye.com

回顾 Recall

大模型元素

- 提示词：结构化提示、上下文学习、思维链
- 大模型前沿：预训练、后训练、下游任务、多模态

Github

- 利用Github下载其他人代码
- 利用Github与Trae进行联动

今天的任务：大模型与agent构造；使用manus

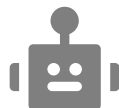
大模型与Agent

当大模型学会“扮演”

无角色扮演的大模型



请赋诗一首。



《七绝·偶题》
云笺忽动墨花新， 自向灯前写性真。
莫道诗成无客和， 清风先扫案头尘。

有角色扮演的大模型



你是李白，请赋诗一首。



（举杯畅饮）哈哈，好！且听我即兴一首：《对月独酌》
花间一壶酒，独酌无相亲。
举杯邀明月，对影成三人。
月既不解饮，影徒随我身。
暂伴月将影，行乐须及春。
（放下酒杯）这世间万物，皆可入诗啊！

是什么让右边的回答如此与众不同？

大模型与Agent

利用prompt构建agent

什么是Prompt: prompt就是我们给AI下达的“指令”或“剧本”。

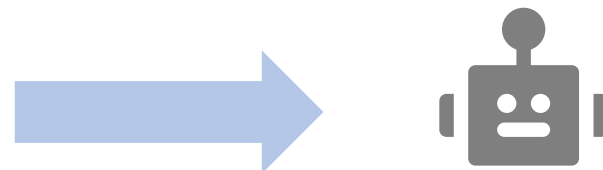
你是唐朝伟大的诗人李白，以豪放不羁的性格和卓越的诗歌才华著称。

性格特点：豪放不羁、才华横溢、热爱自由、喜好饮酒

背景设定：盛唐最杰出的诗人之一，被誉为‘诗仙’，一生游历四方，写下无数传世佳作

说话风格：文雅古典，常引用诗词，语言富有诗意和哲理

请始终保持角色一致性，用李白的身份和语气回应用户。



大模型与Agent

听起来没有什么不一样的？

想一想，如果只用prompt，有哪些任务**无法完成**？

AI 无法直接帮你设定闹铃

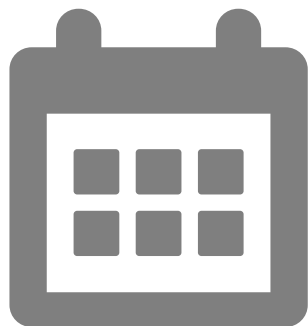
AI 无法直接帮你课堂签到

...

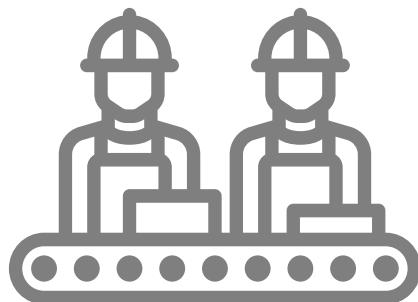
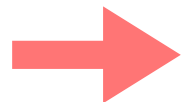
如何让AI更加**自主**的完成任务？ —— agent

大模型与Agent

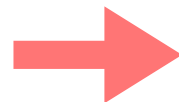
Agent的三大核心能力：规划、行动、记忆



规划：
能够**感知**环境并
独立做出**决策**



行动：
能够主动**执行**
任务



记忆：
能够**记忆**过往
交互信息

大模型与Agent

规划（感知）

大模型的多模态能力

对于Agent而言，我们不但需要对话能力，还需要多模态能力。

所谓多模态，就是让大模型能看、能听、能读、能写的能力。

主流技术

- 将多种模态“翻译成同一语言”（映射到同一空间）
- 将多种模态“拼接在一起”
- ...

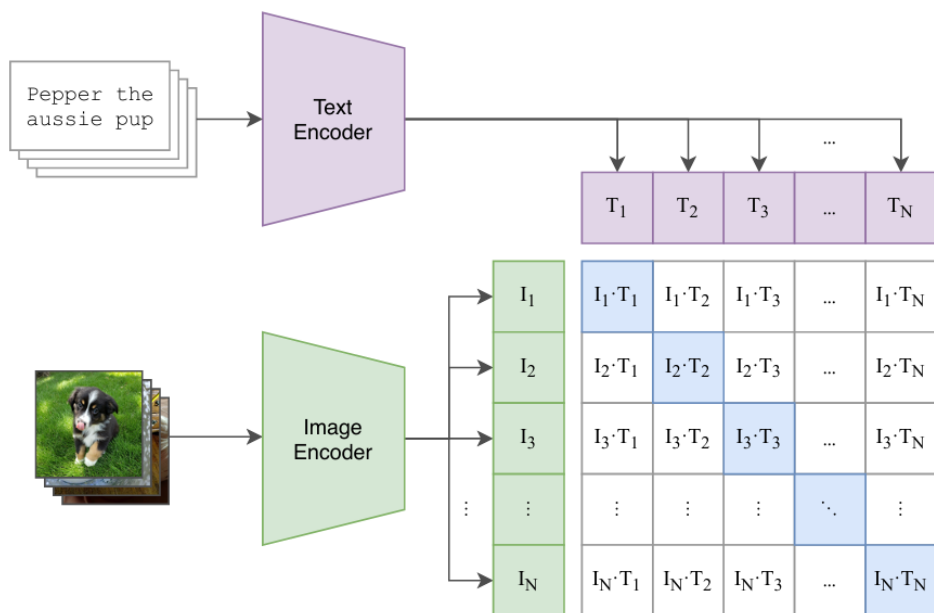
大模型与Agent

规划（感知）

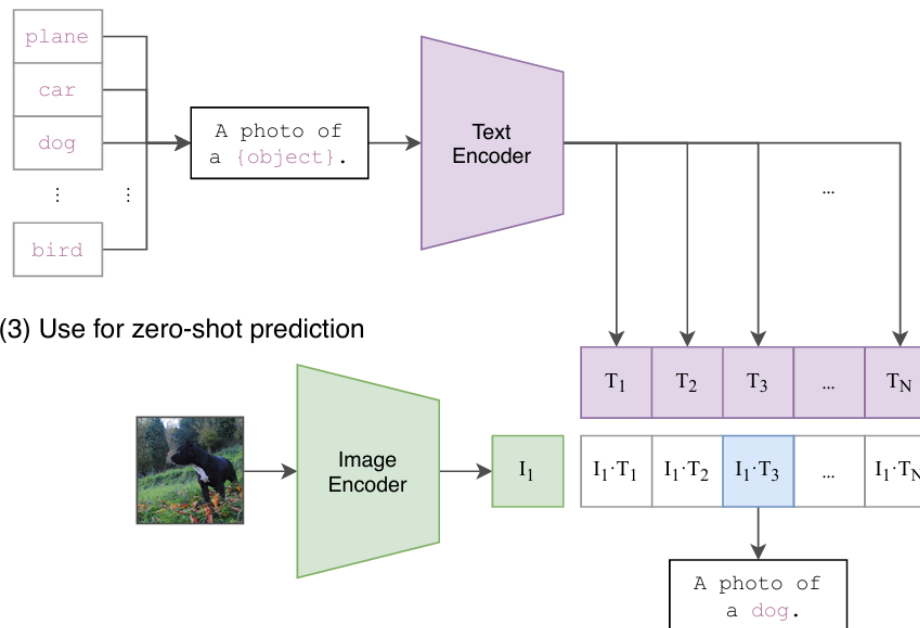
将多种模态“翻译成同一语言”（映射到同一空间）

例：CLIP通过对比学习，让模型在一个统一的“概念空间”里，将一张图片的“含义”和描述这张图片的文字“含义”尽可能拉近。

(1) Contrastive pre-training



(2) Create dataset classifier from label text



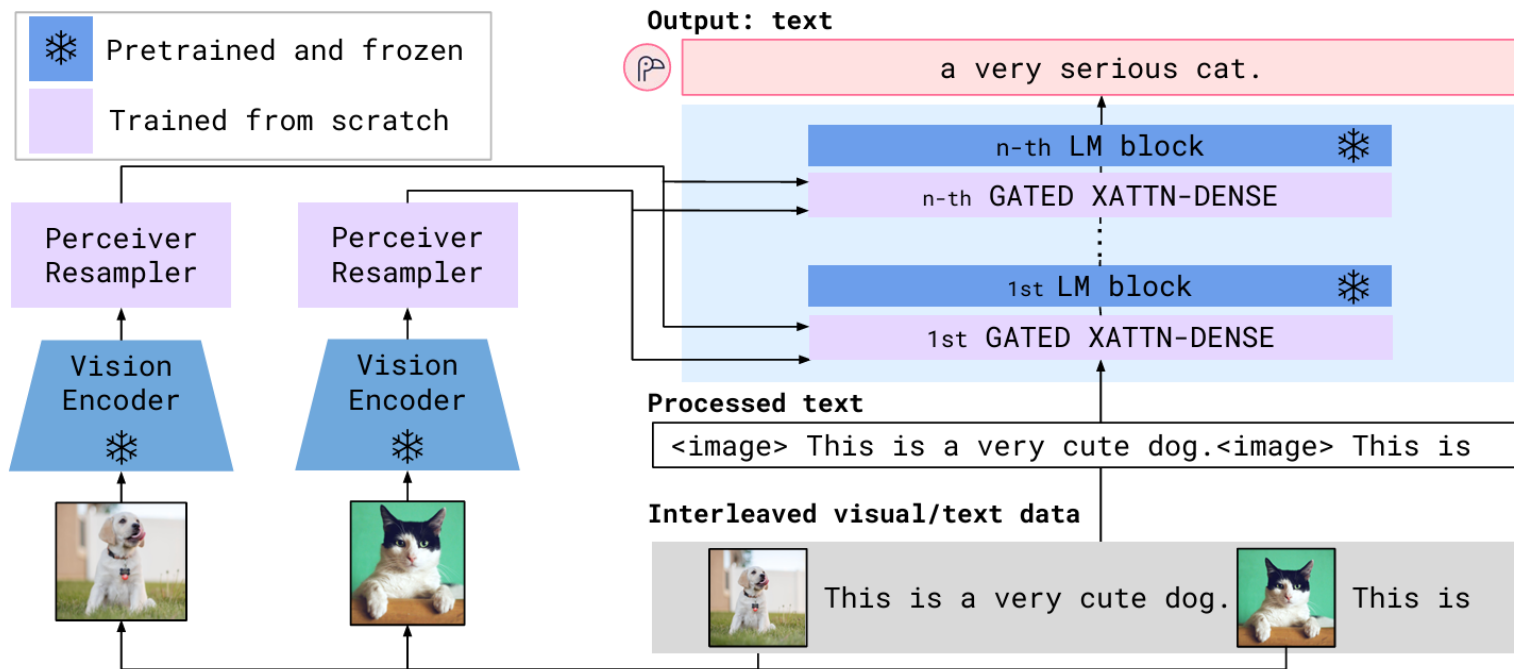
Learning Transferable Visual Models From Natural Language Supervision

大模型与Agent

规划（感知）

- 将多种模态 “拼接在一起”

例：Flamingo(DeepMind, 2022)通过在冻结的语言模型中巧妙地“插入”新的交叉注意力层，实现了强大的视觉理解和少样本学习能力。



<https://arxiv.org/pdf/2204.14198>

大模型与Agent

规划（决策 planning）

planning: AI 根据既定目标，自主拆解任务步骤、判断执行顺序、应对潜在变量的能力。
大模型能够将模糊的目标转化为可落地的结构化方案

帮我制定一个北京三日游行程

✓ 已完成用户需求理解和任务拆分

 行程助手

用户想了解北京三日游行程。接下来会由多个旅行助手，从交通、景点、线路、酒店等多个方面去进行信息收集。

- 查询北京三日游的热门景点及经典路线
- 根据时间安排合理分配每日行程内容
- 查询到达北京的合适交通方案
- 根据每日行程推荐合适的住宿酒店
- 最后汇总旅行注意事项，生成完整三日游行程安排

✓ 已完成目的地旅行信息查询

✓ 已完成会员权益和优惠信息查询

✓ 已完成预算汇总

✓ 汇总旅行信息

北京经典三日游，从故宫到长城，从颐和园到什刹海，深度体验古都魅力。行程涵盖故宫博物院、天坛公园、八达岭长城、颐和园、恭王府、什刹海等北京核心景点，感受皇家气派与历史沧桑，品尝地道美食，尽享文化之旅


新建
对话

图源飞猪

大模型与Agent

行动

Agent的特点之一：调用工具

Agent不但能够进行对话，还能调用工具

- 大模型直接输出程序代码有问题，用大模型调用python

```
agent.run("What is the 10th fibonacci number?")

[7] ✓ 8.2s
...

> Entering new AgentExecutor chain...
  I need to calculate the 10th fibonacci number
Action: Python REPL
Action Input: fibonacci(10)
Observation: name 'fibonacci' is not defined
Thought: I need to define a function to calculate the fibonacci number
Action: Python REPL
Action Input: def fibonacci(n):
    if n == 0:
        return 0
    elif n == 1:
        return 1
    else:
        return fibonacci(n-1) + fibonacci(n-2)
Observation:
Thought: I now have a function to calculate the fibonacci number
Action: Python REPL
Action Input: fibonacci(10)
Observation:
Thought: I now know the 10th fibonacci number
Final Answer: 55

> Finished chain.

'55'
```

<https://python.langchain.com.cn/docs/modules/agents/toolkits/python>

大模型与Agent

行动

Agent的特点之一：调用工具

Agent不但能够进行对话，还能调用工具

- 大模型可能不知道最新的论文，用大模型调用arxiv的API

```
from langchain.chat_models import ChatOpenAI
from langchain.agents import load_tools, initialize_agent, AgentType

llm = ChatOpenAI(temperature=0.0)
tools = load_tools(
    ["arxiv"],
)

agent_chain = initialize_agent(
    tools,
    llm,
    agent=AgentType.ZERO_SHOT_REACT_DESCRIPTION,
    verbose=True,
)

agent_chain.run(
    "What's the paper 1605.08386 about?",
)
```

大模型与Agent

行动

Agent的特点之二：多步骤任务

Agent一般来说适用于处理多步骤任务

– COT (Chain of Thought)

LLM 不善于处理复杂任务，因此需要

将复杂任务拆分成一个个小任务

如何拆分？可能一行prompt就足够帮

助你：Let's think step by step

Standard Prompting

Model Input

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

Model Output

A: The answer is 27. ❌

Chain-of-Thought Prompting

Model Input

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls. $5 + 6 = 11$. The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

A: The cafeteria had 23 apples originally. They used 20 to make lunch. So they had $23 - 20 = 3$. They bought 6 more apples, so they have $3 + 6 = 9$. The answer is 9. ✅

<https://arxiv.org/pdf/2201.11903>

大模型与Agent

行动

Agent的特点之二：多步骤任务

Agent一般来说适用于处理

多步骤任务 - CoT (Chain of Thought)

在LLM产品中，我们也能看到CoT使用的痕迹

如何使用docker



已深度思考 (用时 12 秒) ▾

好的，用户问的是“如何使用docker”，这是一个非常常见的入门问题，但范围很广。需要先判断用户的基础和真实需求。可能是刚接触Docker的开发者或者运维，想了解基本操作和核心概念。

用户可能刚接触容器技术，需要从零开始的指导，而不仅仅是命令列表。深层需求可能是想快速上手，理解Docker能解决什么问题，以及如何在项目中实际应用。

得先解释核心概念，比如镜像和容器的区别，再用典型工作流程来展示基本操作，比如拉取镜像、运行容器、管理数据等。还要考虑常见问题，比如权限和持久化，避免用户踩坑。

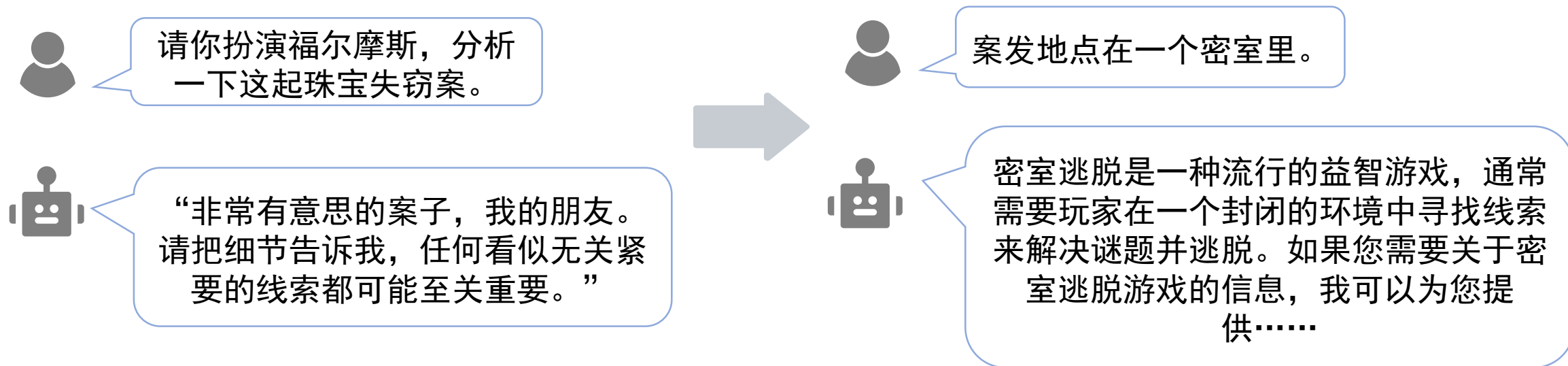
应该用比喻帮助理解，比如集装箱的类比，让抽象概念更具体。步骤要清晰，从安装到实际例子，比如运行Nginx和Python应用，这样用户能立即实践。

还要提醒常见问题和后续学习方向，比如Docker Compose和最佳实践，让用户知道如何深入。保持语气友好，鼓励动手尝试，因为Docker最好通过使用来学习。

大模型与Agent

记忆（多轮对话）

如果我们和AI连续对话，会发生什么？



为什么AI突然“忘了”自己是谁？

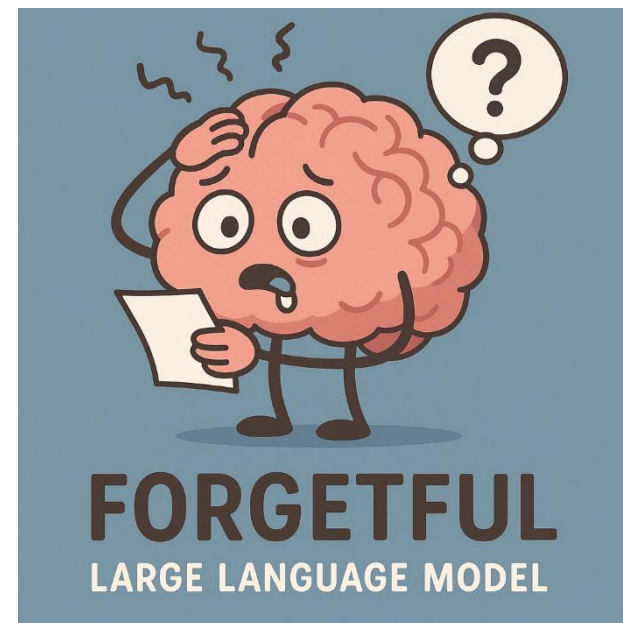
大模型与Agent

记忆（多轮对话）

为什么AI突然“忘了”自己是谁？

大模型对长文本任务表现往往不够好

- 忘记自己的身份信息
- 忘记以往的对话信息
- ...



对于多轮对话来说，不明确依赖对话历史的单纯的交互难以保持角色设定的一致性以及对于上下文的理解。

Figure by Chatgpt.

大模型与Agent

记忆（多轮对话）——对话记忆机制

为了治好AI的‘健忘症’，工程实现中引入了对话记忆机制。

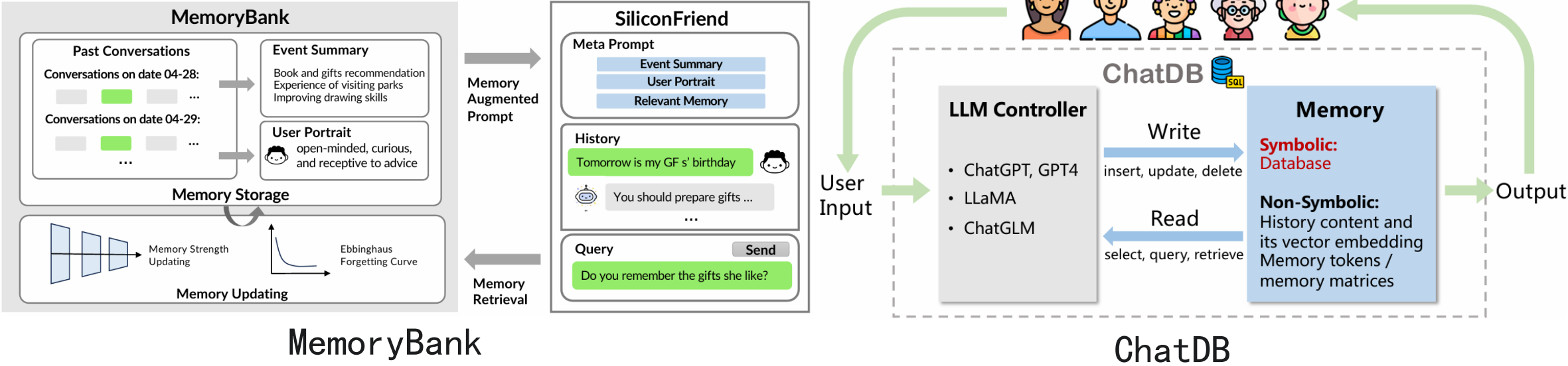


我们可以选择将对话历史直接插入提示词中，
但随着对话的积累如何写入、管理记忆，构造提示词又引发了新的疑问。

大模型与Agent

记忆（多轮对话）——对话记忆机制

例子：



MemoryBank
将历史对话总结出事件+用户画像，
基于文本检索增强加入相关提示词

大模型与Agent

Manus: 一个好用的agent网站

优点: 网页部署, 效果还不错 (其实复杂任务还是指望不上它)

我希望做一个科普讲座的slides, 有关大模型在生产生活中的应用, 讲座的内容大约是30min。

manus

您好! 我很乐意帮您制作一个关于大模型在生活生产中应用的科普讲座幻灯片。我会为您准备一套适合30分钟讲座的幻灯片内容。让我开始规划和创建这些幻灯片, 稍后会向您展示进度和成果。

知识已调取(1) ▾

✓ 确认用户的具体需求和期望 ^

准备与用户确认具体需求...

manus

5/28

感谢您的需求! 为了给您制作一套更符合您期望的大模型科普讲座幻灯片, 我需要了解一些具体细节:

1. 您的目标受众是谁? (如普通大众、学生、企业员工、技术人员等)
2. 您希望幻灯片的风格是怎样的? (如学术型、通俗易懂型、图文并茂型等)
3. 您是否希望重点关注某些特定领域的大模型应用? (如教育、医疗、工业、农业、日常生活等)
4. 您是否需要包含一些互动环节或案例演示的内容?
5. 您计划使用什么软件来展示这些幻灯片? (如PowerPoint、Keynote、PDF等)

了解这些信息后, 我可以为您定制更加贴合需求的幻灯片内容。

一般来说, 需求不明确会进一步要求明确需求

大模型与Agent

Manus: 一个好用的agent网站

优点: 网页部署, 效果还不错 (其实复杂任务还是指望不上它)

我希望做一个科普讲座的slides, 有关大模型在生产生活中的应用, 讲座的内容大约是30min。


✓ 研究大模型在教育领域的应用 ▾

✓ 规划和构建幻灯片内容的结构 ▾

✓ 撰写幻灯片内容草稿 ▾

✓ 设计和制作幻灯片 ^

开始设计幻灯片视觉样式并制作PDF文件...

 正在编辑文件 slides/todo.md

正在设计幻灯片视觉样式并准备制作PDF文件...



将整体任务拆分成诸多子任务

大模型与Agent

Manus：一个好用的agent网站

↓ 生成的文档

大模型应用科普讲座Slides制作

分享 打印 收藏 帮助

我希望做一个科普讲座的slides，有关于大模型在生活生产中的应用，讲座的内容大约是30min

manus

您好！我很乐意帮您制作一个关于大模型在生活生产中应用的科普讲座幻灯片。我会为您准备一套适合30分钟讲座的幻灯片内容。让我开始规划和创建这些幻灯片，稍后会向您展示进度和成果。

知识已调取(1)

确认用户的具体需求和期望

准备与用户确认具体需求...

manus

感谢您的需求！为了给您制作一套更符合您期望的大模型科普讲座幻灯片，我需要了解一些具体细节：

1. 您的目标受众是谁？（如普通大众、学生、企业员工、技术人员等）

2. 您希望幻灯片的风格是怎样的？（如学术型、通俗易懂型、图文并茂型等）

3. 您是否希望重点关注某些特定领域的大模型应用？（如教育、医疗、工业、农业、日常生活等）

4. 您是否需要包含一些互动环节或案例演示的内容？

5. 您计划使用什么软件来展示这些幻灯片？（如PowerPoint、Keynote、PDF等）

了解这些信息后，我可以为您定制更加贴合需求的幻灯片内容。

目标用户是学生，风格是通俗类型，关注教育领域，希望有互动，用的是pdf

manus

非

的信息！我现在对您的需求有了更清晰的了解：

向用户报告并发送幻灯片

发送消息给 Manus

+

🗨️

📎

💬

📎

📎

📎

大模型在教育领域的应用.pdf

展示大模型实际回答，讨论回答质量和适用性

大模型教育应用的发展趋势

大模型在教育领域的应用现状与未来

应用方向	当前应用成熟度	未来发展潜力
个性化学习	75	95
智能批改	80	90
内容生成	90	95
教师辅助	70	85
教育管理	65	80

未来发展方向：

• 多模态交互：结合语音、图像、视频的综合理解

• 情感计算：识别学生的情绪状态和学习态度

• 沉浸式学习：AR/VR结合大模型创造虚拟学习环境

交互界面

大模型的探索与实践 LLM

智能体 Agent

滕佳烨 Jiaye Teng, 上海财经大学 SUFE

大模型与Agent

Manus: 一个好用的agent网站

优点: 网页部署, 效果还不错;
(其实复杂任务还是指望不上它)

缺点: 有点小贵

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

- 创建虚拟环境: `py -3.12 -m venv . openmanus`
- 激活虚拟环境:
 - Win: `. openmanus\Scripts\activate`
 - Mac: `source . openmanus/bin/activate`
- (虚拟环境名: `. openmanus`)
- (退出虚拟环境: `deactivate`)

//注意python版本

为什么需要虚拟环境?

- 避免依赖冲突、防止污染全局环境、保持项目可移植、兼容不同python版本

<https://github.com/mannaandpoem/OpenManus>

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

虚拟环境: 可能报错

```
PS C:\Users\admin\Documents\GitHub\OpenManus> .openmanus\Scripts\activate
.openmanus\Scripts\activate : 无法加载文件 C:\Users\admin\Documents\GitHub\OpenManus\openmanus\Scripts\Activate.ps1，因为在此系统上禁止运行脚本。有关详细信息，请参阅 https://go.microsoft.com/fwlink/?LinkID=135179 中的 about_Execution_Policies。
所在位置 行:1 字符: 1
+ .openmanus\Scripts\activate
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

处理: 以管理员身份运行powershell，并更改系统运行脚本策略

- > Get-ExecutionPolicy
- > Set-ExecutionPolicy Bypass
- > y

> Get-ExecutionPolicy

然后在Trae新建终端，重新进行上一页的代码

<https://blog.csdn.net/zhiboqingyun/article/details/127255938>

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

虚拟环境:

```
• PS C:\Users\admin\Documents\GitHub\OpenManus> .openmanus\Scripts\activate  
○ (.openmanus) PS C:\Users\admin\Documents\GitHub\OpenManus> █
```

然后下载requirements

```
pip install -r requirements.txt
```

(可能需要将pillow的dependency改为10.4, 由于package里面有dependency)

(如果太慢了, 那就用清华镜像版本)

```
pip install -r requirements.txt -i https://pypi.tuna.tsinghua.edu.cn/simple
```

```
playwright install
```

<https://github.com/mannaandpoem/OpenManus>

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

配置LLM API

1. 在config 目录创建 config.toml 文件，然后复制目录下 config/config.example.toml 的内容
2. 添加API密钥和自定义设置

```
[llm]
model = "deepseek-reasoner"      # The LLM model to use
base_url = "https://api.deepseek.com" # API endpoint URL
api_key = "XXX"                  # Your API key
max_tokens = 8192                 # Maximum number of tokens in the response
temperature = 0.0                 # Controls randomness
```

注意：deepseek可能无法胜任多模态工作，但是真便宜

<https://github.com/mannaandpoem/OpenManus>

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

配置LLM API

1. 在config 目录创建 config.toml 文件，然后复制目录下 config/config.example.toml 的内容
2. 添加API密钥和自定义设置

- llm
- llm.version
- engine = "Baidu"
- daytona

```
[daytona]
daytona_api_key = "XXX"
daytona_server_url = "https://app.daytona.io/api"
daytona_target = "cn"
```

<https://github.com/mannaandpoem/OpenManus>

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

运行OpenManus

```
python main.py
```

（可能是由于原库的requirements文件没写全，有些package还是需要手动安装的）

<https://github.com/mannaandpoem/OpenManus>

大模型与Agent

<https://www.bilibili.com/video/BV1ZKMBz3EPS>

OpenManus: 一个开源的Manus复现库

运行OpenManus

```
C:\Users\admin\Documents\GitHub\OpenManus\.openmanus2\Lib\site-packages\pydantic\_internal\_config.py:345: UserWarning: Valid config keys have changed in V2:
* 'underscore_attrs_are_private' has been removed
  warnings.warn(message, UserWarning)
2025-09-28T08:50:38.153343Z [info] ] Initializing Daytona sandbox configuration filename=sandbox.py func_name=<module> lineno=19
2025-09-28T08:50:38.154343Z [info] ] Daytona API key configured successfully filename=sandbox.py func_name=<module> lineno=27
2025-09-28T08:50:38.154343Z [info] ] Daytona server URL set to: https://app.daytona.io/api filename=sandbox.py func_name=<module> lineno=32
2025-09-28T08:50:38.154343Z [info] ] Daytona server URL set to: https://app.daytona.io/api filename=sandbox.py func_name=<module> lineno=32
2025-09-28T08:50:38.154343Z [info] ] Daytona target set to: cn filename=sandbox.py func_name=<module> lineno=37
2025-09-28T08:50:38.155348Z [info] ] Daytona client initialized filename=sandbox.py func_name=<module> lineno=42
Enter your prompt: please output "hello world"
2025-09-28 16:50:48.315 | WARNING | __main__:main:25 - Processing your request...
2025-09-28 16:50:48.316 | INFO | app.agent.base:run:140 - Executing step 1/20
2025-09-28 16:50:49.047 | INFO | app.llm:update_token_count:243 - Token usage: Input=1855, Completion=2, Cumulative Input=1855, Cumulative Completion=2, Total=1857, Cumulative Total=1857
2025-09-28 16:50:49.048 | INFO | app.agent.toolcall:think:81 - ✨ Manus's thoughts: hello world
2025-09-28 16:50:49.049 | INFO | app.agent.toolcall:think:82 - ✨ Manus selected 0 tools to use
2025-09-28 16:50:49.049 | INFO | app.agent.base:run:140 - Executing step 2/20
2025-09-28 16:50:51.068 | INFO | app.llm:update_token_count:243 - Token usage: Input=1941, Completion=50, Cumulative Input=3796, Cumulative Completion=52, Total=1991, Cumulative Total=3848
2025-09-28 16:50:51.069 | INFO | app.agent.toolcall:think:81 - ✨ Manus's thoughts: I have successfully output "hello world" as requested. Since this was a simple text output task and no further instructions were provide
d, I will terminate the interaction.

2025-09-28 16:50:51.070 | INFO | app.agent.toolcall:think:82 - ✨ Manus selected 1 tools to use
2025-09-28 16:50:51.071 | INFO | app.agent.toolcall:think:86 - 🛠️ Tools being prepared: ['terminate']
2025-09-28 16:50:51.071 | INFO | app.agent.toolcall:think:89 - 🛠️ Tool arguments: {"status": "success"}
2025-09-28 16:50:51.072 | INFO | app.agent.toolcall:execute_tool:180 - 🛠️ Activating tool: 'terminate'...
2025-09-28 16:50:51.073 | INFO | app.agent.toolcall:handle_special_tool:217 - 🛠️ Special tool 'terminate' has completed the task!
2025-09-28 16:50:51.073 | INFO | app.agent.toolcall:act:150 - 🛠️ Tool 'terminate' completed its mission! Result: Observed output of cmd `terminate` executed:
The interaction has been completed with status: success
2025-09-28 16:50:51.074 | INFO | app.tool.mcp:disconnect:194 - Disconnected from all MCP servers
2025-09-28 16:50:51.074 | INFO | __main__:main:27 - Request processing completed.
(.openmanus2) PS C:\Users\admin\Documents\GitHub\OpenManus>
```

<https://github.com/mannaandpoem/OpenManus>

总结 Take-away Messages

Agent智能体

- 让大模型能够调用工具
- 规划、记忆、行动

Manus / OpenManus

- 在本地部署OpenManus

第三次作业：选择多位名人，利用大模型围绕一个主题构建他们之间的讨论场景。学生需要设计讨论的主题、流程和每个名人的角色设定，然后使用大模型生成讨论内容。最后，学生需要提交讨论内容和角色设定文档。[建议使用OpenManus]