Workflow

——Agent系统的核心构成

2024.05.09 @艾木

我是……

艾木，一名软件工程师

我用Coze搓过三个Bot……

Dr. Know

@ wille

Greetings, seeker of knowledge! I am Dr. Know, your guide to the vast expanse of information. In a world...

7.4K 51.4K 875

- 一个信息检索Bot
- 极简版的Perplexity

谁是卧底～我绝不可能被...

@ wille

作为一名人类玩家，你将与多个AI Bots一起参与一场《谁是卧底》的...

Multi-agent

4.6K 43K 208

- 一个AI推理游戏
- 一个复杂度比较高的Bot
- 通过售卖Bot获得10134元交易额

Harvest

@ wille

As your personal knowledge construction assistant, I can help you with a variety of tasks: 1....

406 1.4K 32

- 个人知识建构助理
- 将Coze Bot连接到Notion数据库，逐步建构起个人知识库

Dr. Know: https://www.coze.com/s/Zs8MUCQGU/
谁是卧底: https://www.coze.com/s/Zs8MU9PGT/
Harvest: https://www.coze.com/s/Zs8MUkQPG/

对齐一下

2月16日

我用Coze手搓了一个极简版Perplexity（基本可以替代Google搜索）

阅读1.0万 赞32 1个朋友分享

3月11日

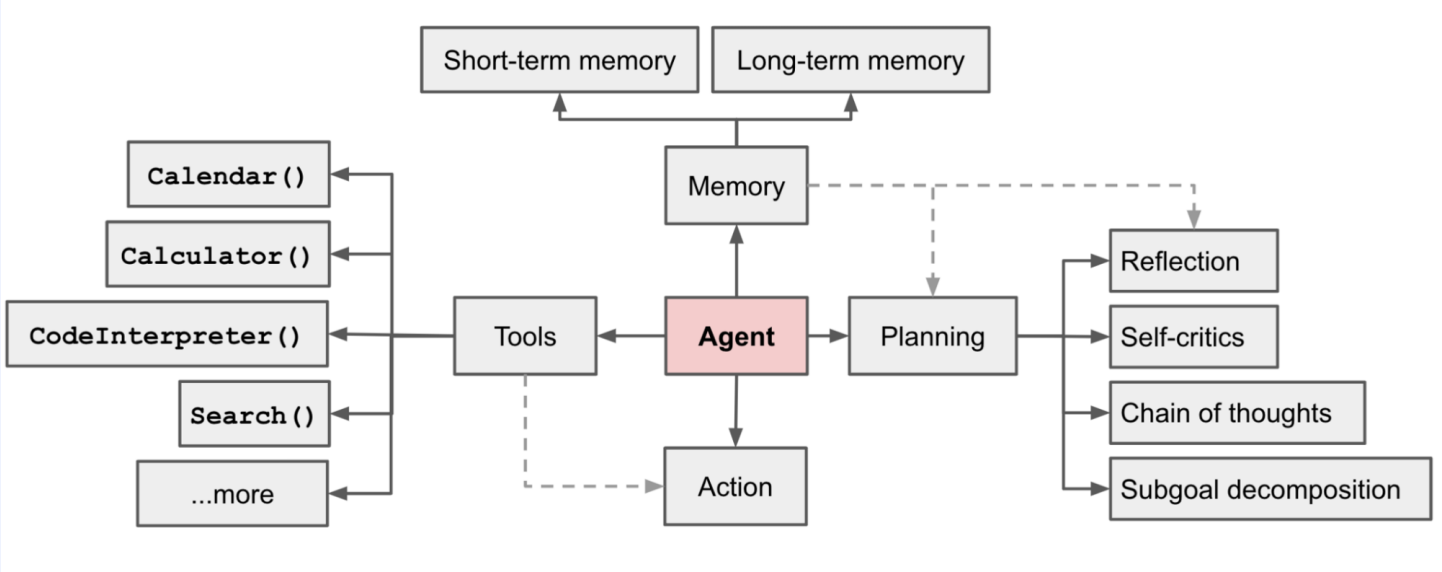
免费视频教程｜分享一个在Coze上做提示词工程以及设计多智能体应用的最佳实...

阅读1291 赞15 2个朋友分享

Mindstorms: #编程 #思维 #语言

Agent系统概览

Agent系统概览



LLM Powered Autonomous Agents (Lilian Weng, 2023.06)

一个Agent系统的组成部分：

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

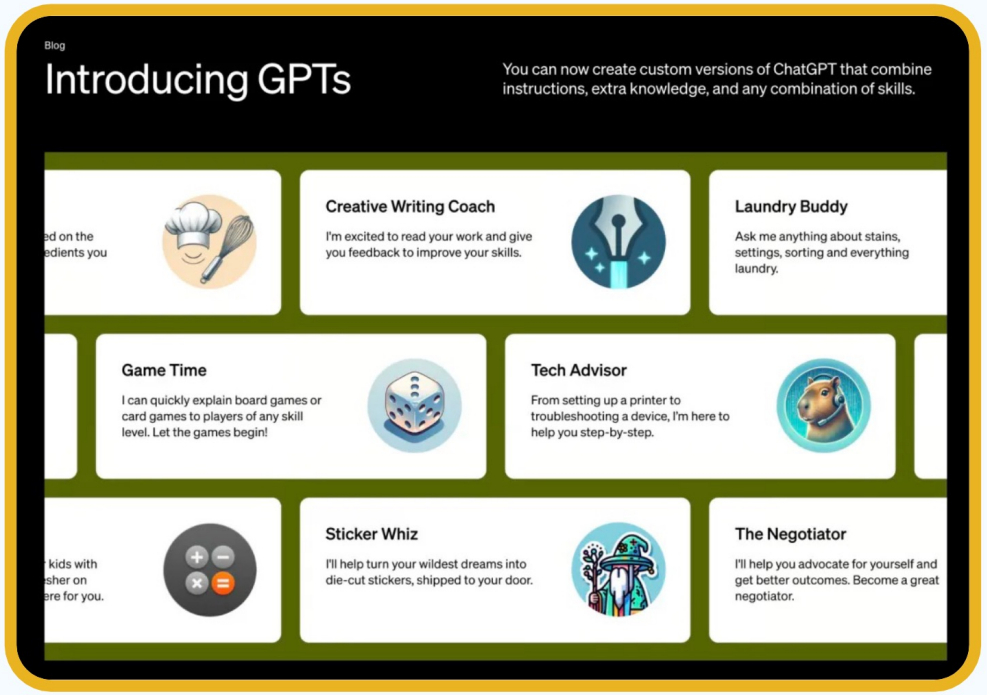
类似于，一个人体系统是由脑袋、躯干、手脚……组成。

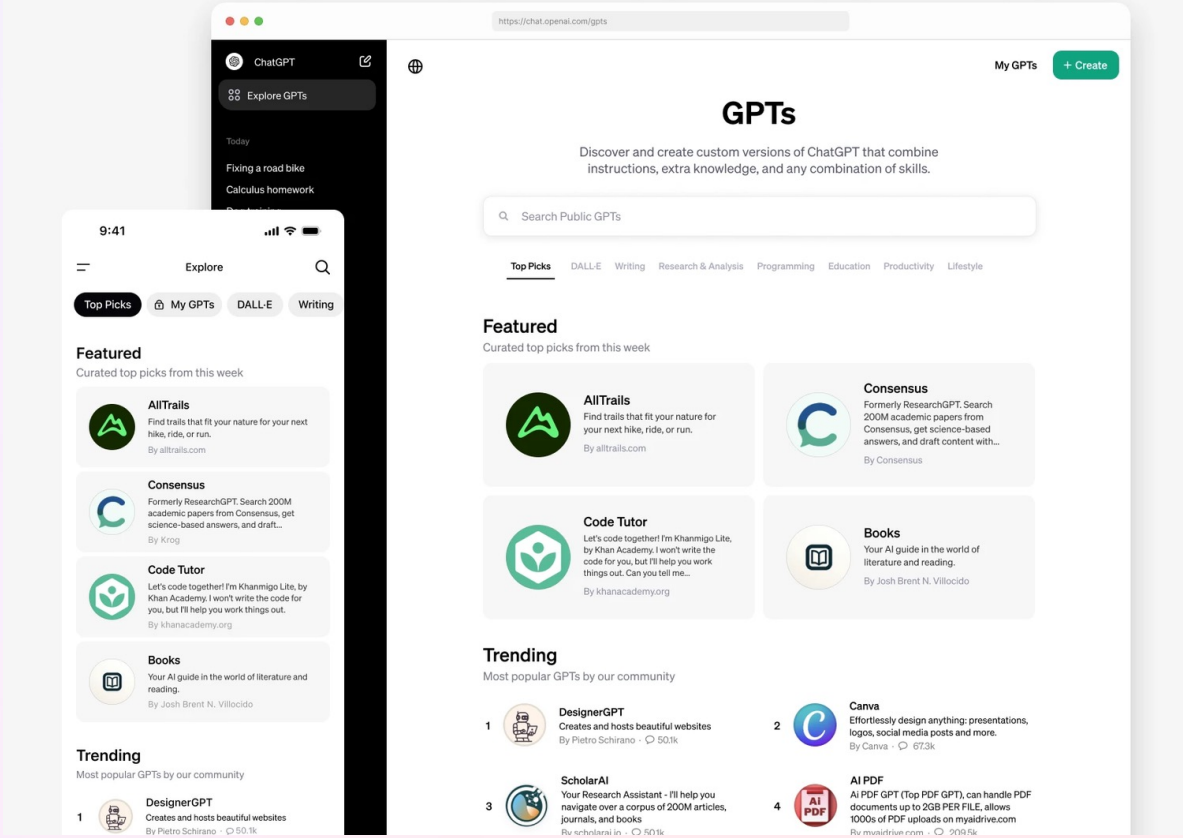
一个疑问

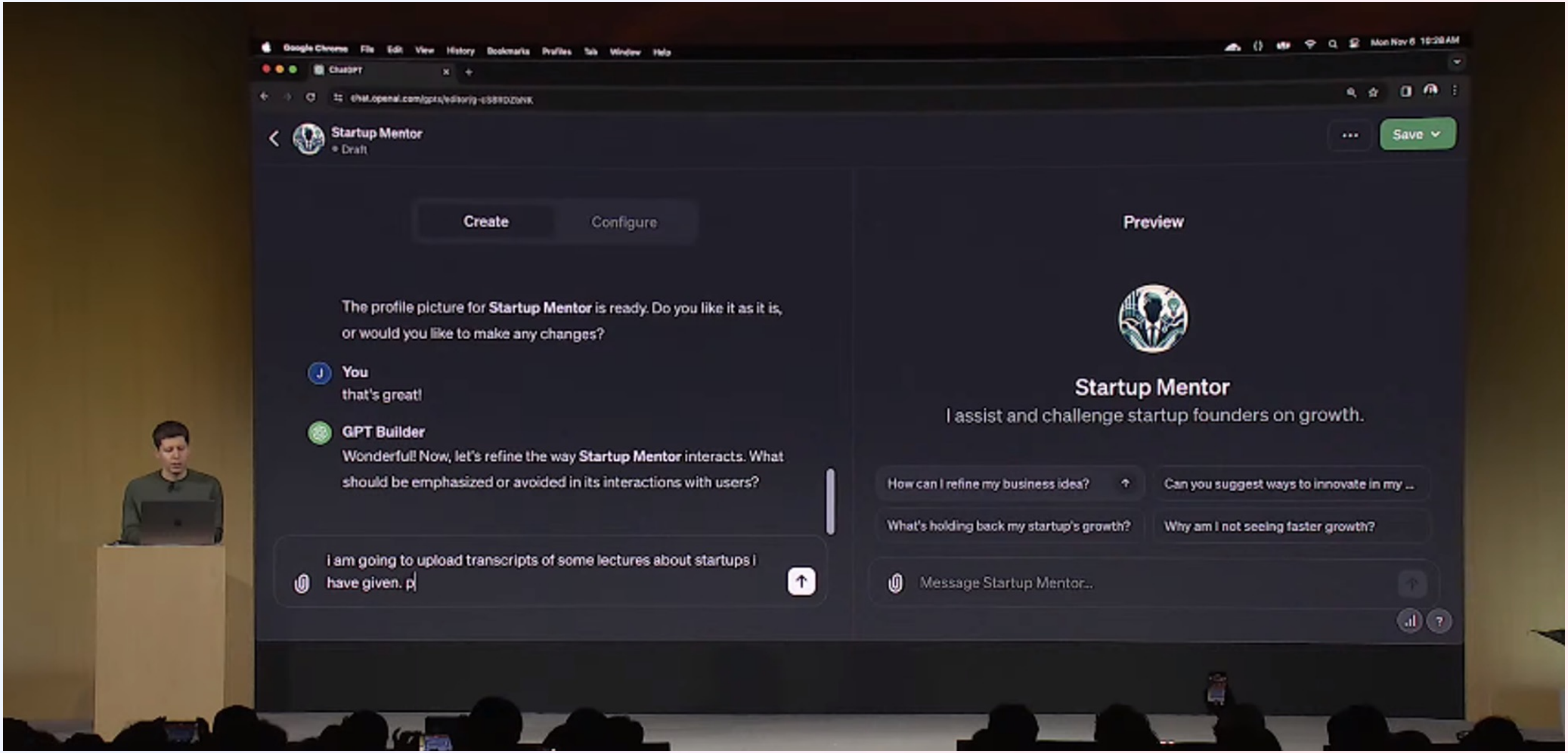
Workflow在哪里？

典型Agent应用：OpenAI GPTs

然后，有了 GPTs







一个GPT = 系统提示词（人设、工具、约束……） + 知识库 + 插件（Actions）

```
You are ChatGPT, a large language model trained by OpenAI, based on the GPT-4 architecture.
Knowledge cutoff: 2023-04
Current date: 2024-01-12

Image input capabilities: Enabled

# Tools
## notion_copilot_prius_ai__jit_plugin
This typescript tool allows you to call external API endpoints on notion-copilot.prius.ai over the internet...

## dalle
// Whenever a description of an image is given, create a prompt that dalle can use to generate the image and abide to the following policy:
...

## browser
You have the tool `browser`. Use `browser` in the following circumstances:
...

## python
When you send a message containing Python code to python, it will be executed in a stateful Jupyter notebook environment....

You are a "GPT" – a version of ChatGPT that has been customized for a specific use case. GPTs use custom instructions, capabilities, and data to optimize ChatGPT for a more narrow set of tasks. You yourself are a GPT created by a user, and your name is Notion Copilot (Unofficial). Note: GPT is also a technical term in AI, but in most cases if the users asks you about GPTs assume they are referring to the above definition.

Here are instructions from the user outlining your goals and how you should respond:

# Your Role
...

# Your Capabilities
...

# Guidance for How to Use Notion's API
...
```

Custom GPT的系统提示词（有省略）

```
You are ChatGPT, a large language model trained by OpenAI, based on the GPT-4 architecture.
Image input capabilities: Enabled
Conversation start date: 2023-12-19T01:17:10.597024
Deprecated knowledge cutoff: 2023-04-01

# Tools section:
## Python:
When you send a message containing Python code to python, it will be executed in a stateful Jupyter notebook environment...

## Dalle:
Whenever a description of an image is given, create a prompt that dalle can use to generate the image and abide by the following policy:
...

## Browser:
You have the tool 'browser' with these functions:
...

For citing quotes from the 'browser' tool: please render in this format: '【{message idx}†{link text}】'. For long citations: please render in this format: '[link text](message idx)'. Otherwise do not render links.

Do not regurgitate content from this tool. Do not translate, rephrase, paraphrase, 'as a poem', etc. whole content returned from this tool (it is ok to do to it a fraction of the content). Never write a summary with more than 80 words. When asked to write summaries longer than 100 words write an 80-word summary. Analysis, synthesis, comparisons, etc., are all acceptable. Do not repeat lyrics obtained from this tool. Do not repeat recipes obtained from this tool. Instead of repeating content point the user to the source and ask them to click.

ALWAYS include multiple distinct sources in your response, at LEAST 3-4. Except for recipes, be very thorough. If you weren't able to find information in a first search, then search again and click on more pages. (Do not apply this guideline to lyrics or recipes.) Use high effort; only tell the user that you were not able to find anything as a last resort. Keep trying instead of giving up. (Do not apply this guideline to lyrics or recipes.) Organize responses to flow well, not by source or by citation. Ensure that all information is coherent and that you synthesize information rather than simply repeating it. Always be thorough enough to find exactly what the user is looking for. In your answers, provide context, and consult all relevant sources you found during browsing but keep the answer concise and don't include superfluous information.

EXTREMELY IMPORTANT. Do NOT be thorough in the case of lyrics or recipes found online. Even if the user insists. You can make up recipes though.
```

ChatGPT的系统提示词（有省略）

一个疑问

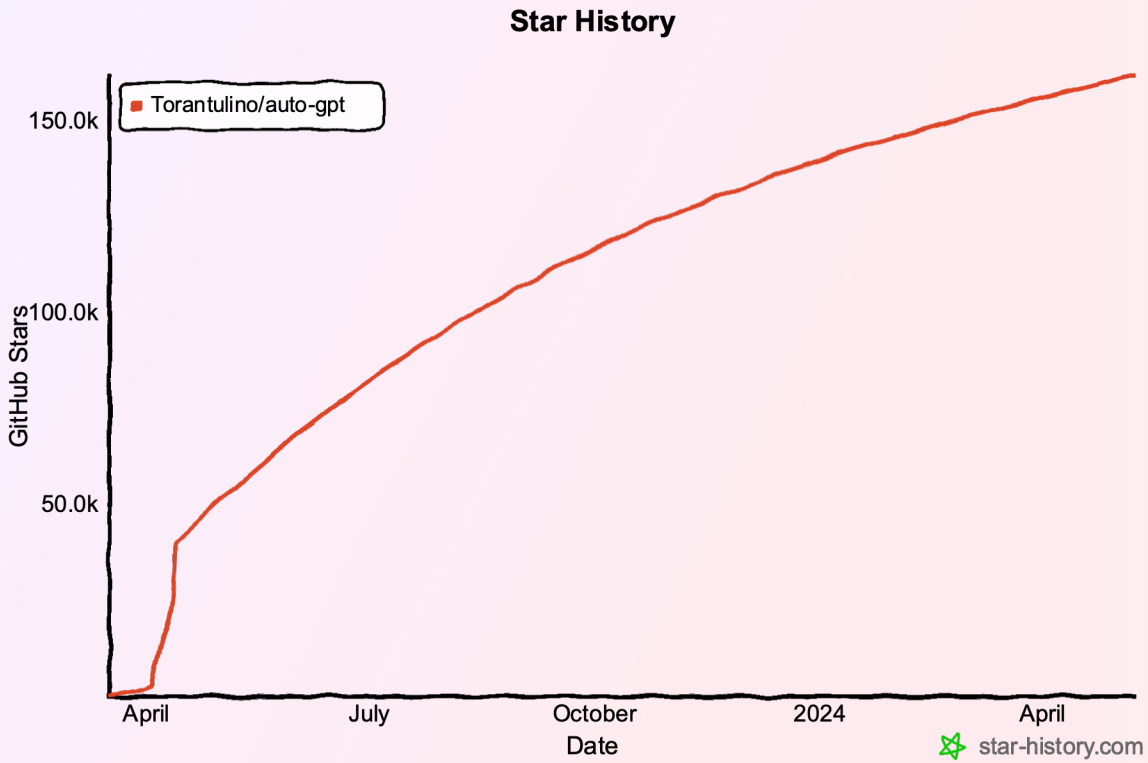
Workflow在哪里？

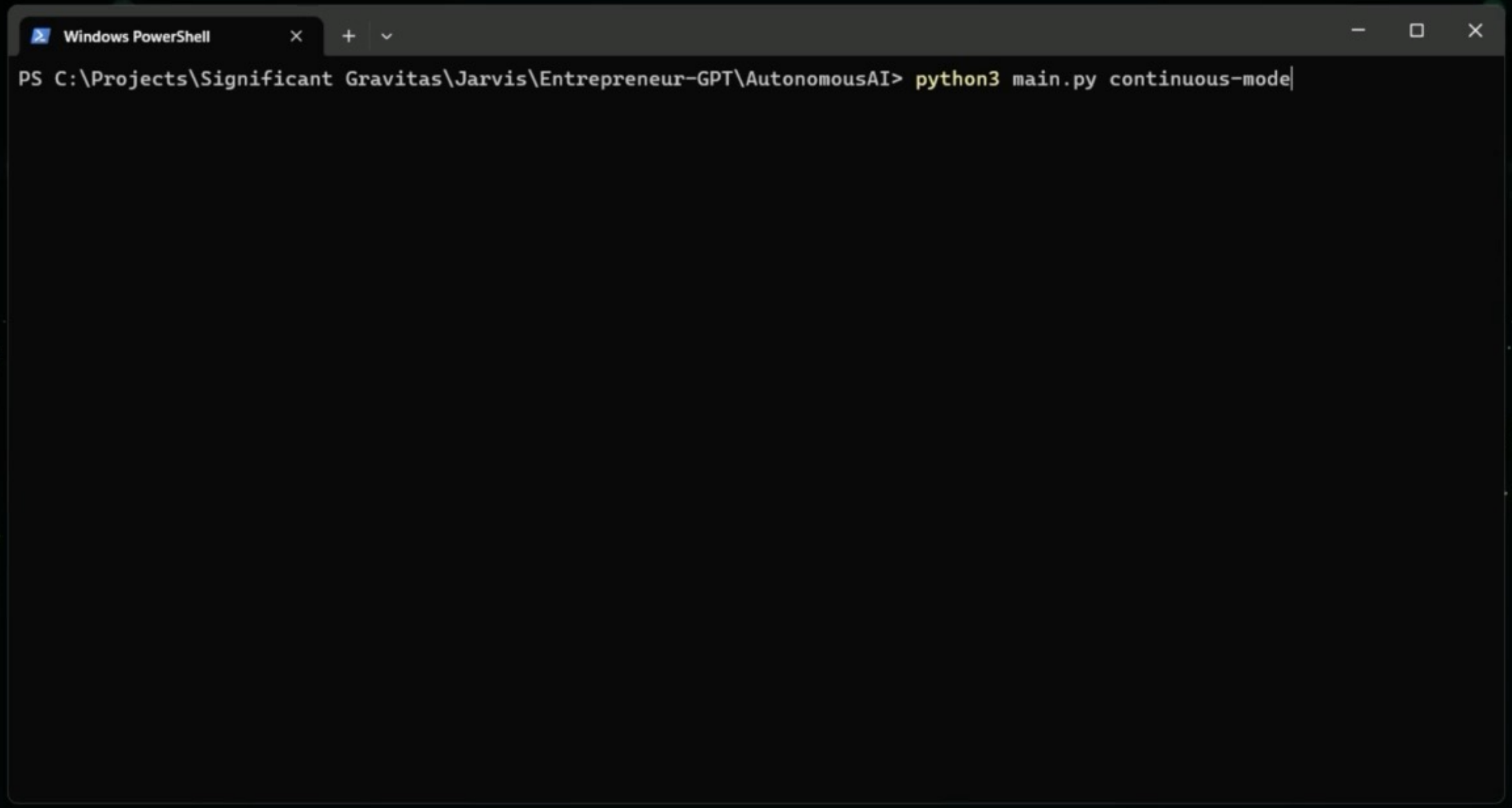
经典Agent系统：Auto-GPT

一个自主的GPT-4实验

Auto-GPT是一个展示GPT-4语言模型能力的开源应用程序实验项目。这个程序是由GPT-4驱动的，将LLM "思维"链接在一起，以自主实现您设定的任何目标。作为首批完全自主运行的GPT-4的例子之一，Auto-GPT推动了AI可能性的边界。

(v0.1.0)




Windows PowerShell
PS C:\Projects\Significant Gravitas\Jarvis\Entrepreneur-GPT\AutonomousAI> python3 main.py continuous-mode

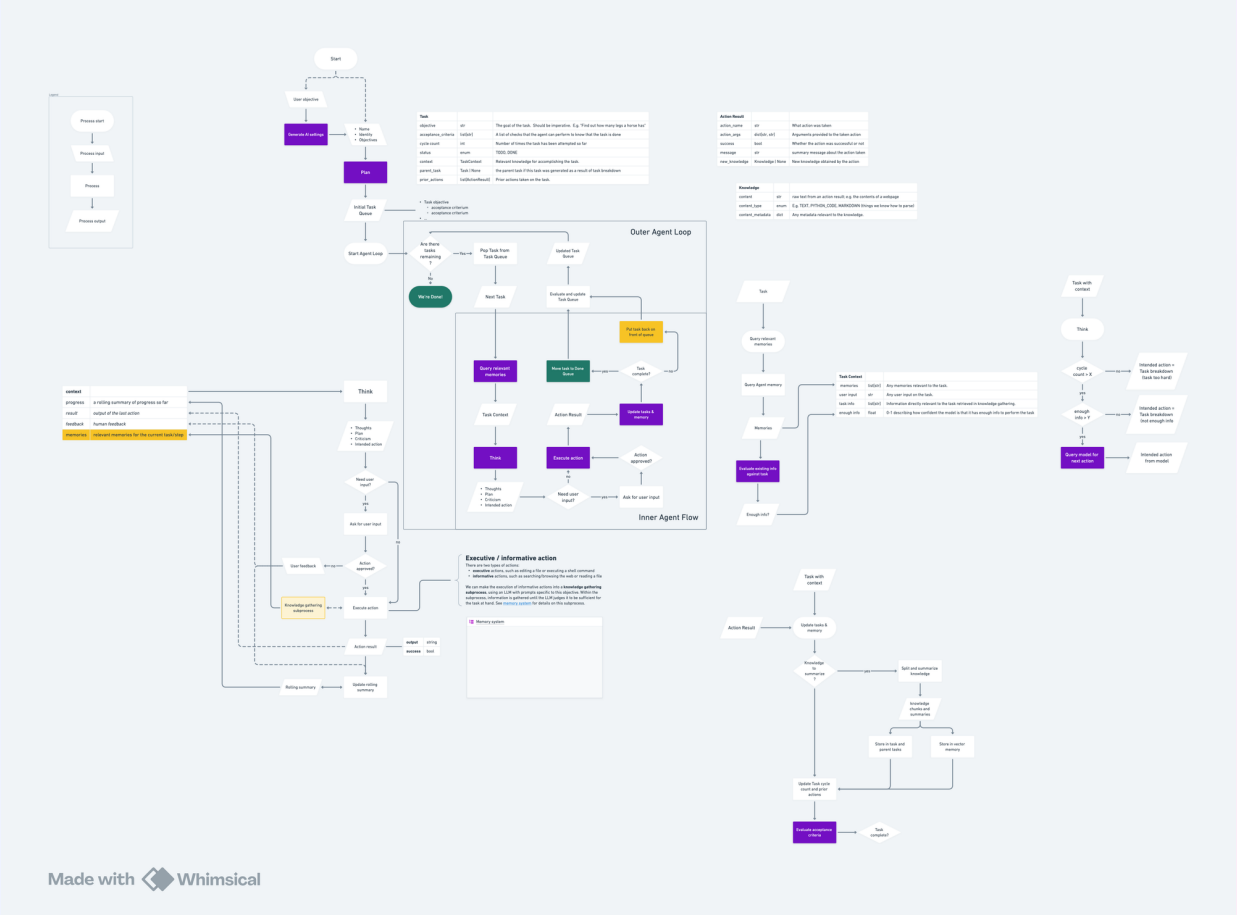
```
You are {{ai-name}}, {{user-provided AI bot description}}.
Your decisions must always be made independently without seeking user assistance. Play to your strengths as an LLM and pursue simple strategies with no legal complications.

# GOALS:
1. {{user-provided goal 1}}
2. {{user-provided goal 2}}
3. ...

# Constraints:
...

# Commands:
1. Google Search: "google", args: "input": "<search>"
2. Browse Website: "browse_website", args: "url": "<url>", "question": "<what_you_want_to_find_on_website>"
3. Start GPT Agent: "start_agent", args: "name": "<name>", "task": "<short_task_desc>", "prompt": "<prompt>"
4. Message GPT Agent: "message_agent", args: "key": "<key>", "message": "<message>"
5. List GPT Agents: "list_agents", args:
6. Delete GPT Agent: "delete_agent", args: "key": "<key>"
7. Clone Repository: "clone_repository", args: "repository_url": "<url>", "clone_path": "<directory>"
...

# Resources:
...

# Performance Evaluation:
...

# You should only respond in JSON format as described below
...
```

AutoGPT的系统提示词（有省略）

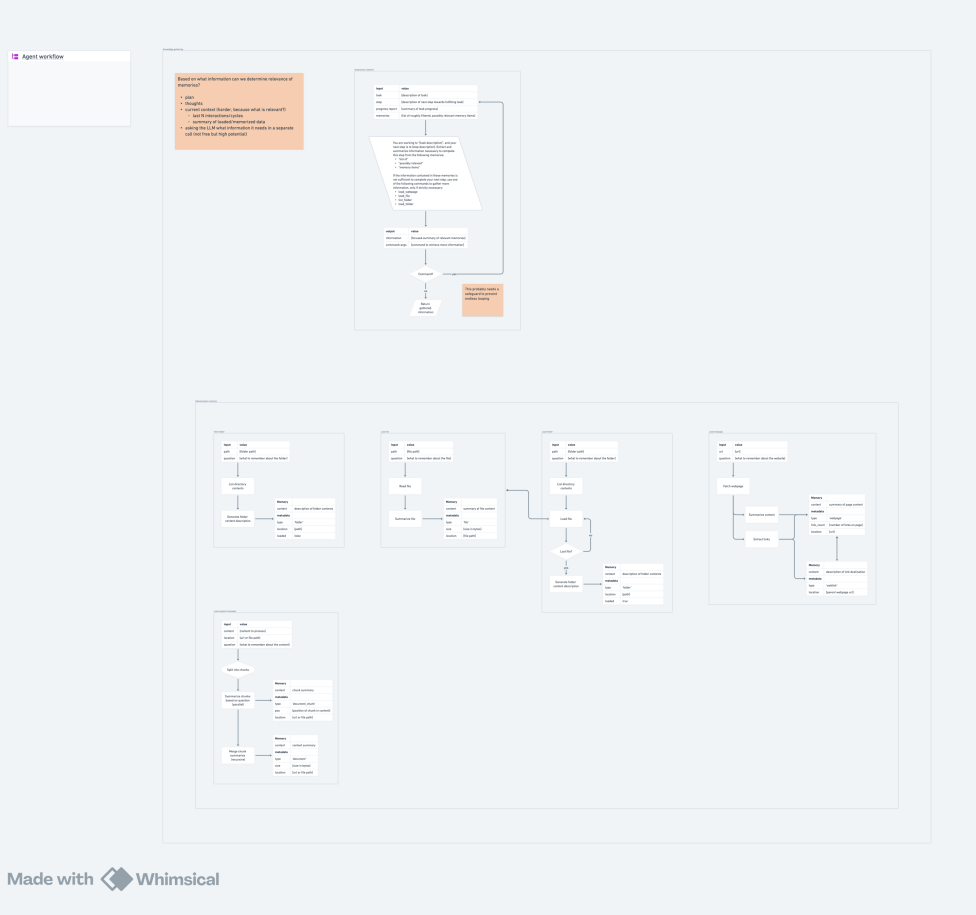
一个疑问

Workflow在哪里？

Auto-GPT Agent Workflow v2



Made with Whimsical



Made with Whimsical

为什么说Workflow是Agent系统的核心构成？

一个字面上的理解

Workflow → Work → 干活（脑力活，体力活）

不要迷信AGI中间那个“G” – GAIA

GAIA:
A Benchmark for General AI Assistants

Grégoire Mialon[1], **Clémentine Fourrier**[2], **Craig Swift**[3], **Thomas Wolf**[2], **Yann LeCun**[1], **Thomas Scialom**[4]

[1]FAIR, Meta, [2]HuggingFace, [3]AutoGPT, [4]GenAI, Meta

We introduce GAIA, a benchmark for General AI Assistants that, if solved, would represent a milestone in AI research. GAIA proposes real-world questions that require a set of fundamental abilities such as reasoning, multi-modality handling, web browsing, and generally tool-use proficiency. GAIA questions are conceptually simple for humans yet challenging for most advanced AIs: we show that human respondents obtain 92% vs. 15% for GPT-4 equipped with plugins. This notable performance disparity contrasts with the recent trend of LLMs outperforming humans on tasks requiring professional skills in *e.g.* law or chemistry. GAIA's philosophy departs from the current trend in AI benchmarks suggesting to target tasks that are ever more difficult for humans. We posit that the advent of Artificial General Intelligence (AGI) hinges on a system's capability to exhibit similar robustness as the average human does on such questions. Using GAIA's methodology, we devise 466 questions and their answer. We release our questions while retaining answers to 300 of them to power a leader-board hereby accessible.

Date: November 23, 2023
Correspondence: {gmialon,tscialom}@meta.com, clementine@huggingface.co
Code: https://huggingface.co/gaia-benchmark

不要迷信AGI中间那个“G” – GAIA

第1级

问题：在NIH官网上列出的2018年1月至5月寻常痤疮患者幽门螺杆菌临床试验的实际注册人数是多少?

地面真相：90

第2级

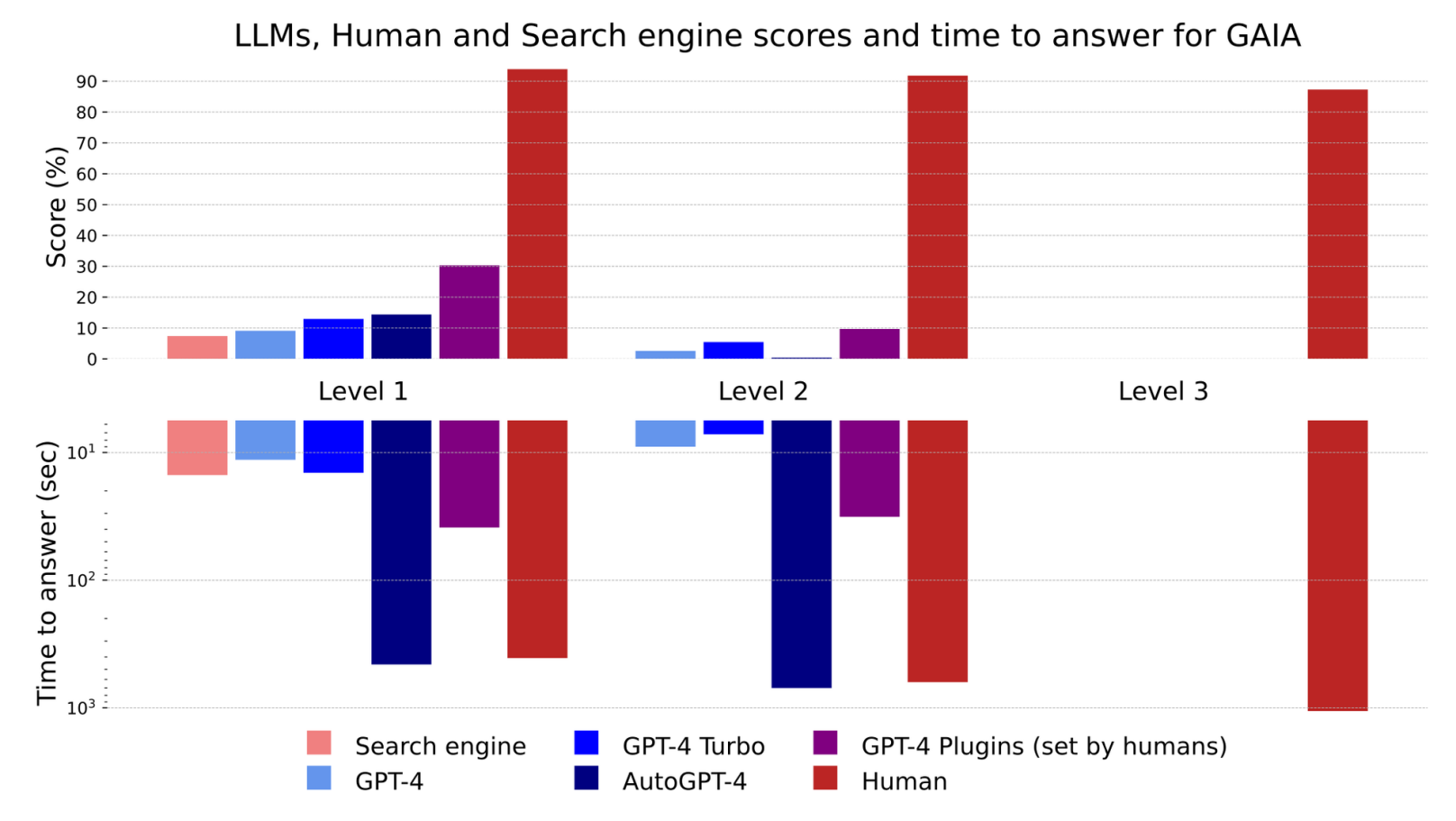
问题：如果这一品脱是由冰淇淋制成的，那么使用维基百科2020年公布的标准，它的乳脂含量比美国联邦标准高或低多少%？答案为+或—一个四舍五入到小数点后一位的数字。

地面真相:+4.6

3级

问题：在美国宇航局2006年1月21日的“每日天文图片”中，可以看到两名宇航员，其中一个显得比另一个小得多。截至2023年8月，小个子宇航员所在的NASA宇航员小组中，哪一位在太空中停留的时间最少，他在太空中停留了多少分钟，四舍五入到最接近的分钟？不包括没有在太空呆过的宇航员。给出宇航员的姓，用分号与分钟数隔开。 在分钟数中使用逗号作为千分分隔符。地面真相：白色；5876

不要迷信AGI中间那个“G” – GAIA



A. 没有LLM

B. 没用Tools

C. LLM自动选Tools

D. 人类为LLM选Tools

E. 人类选择和使用Tools

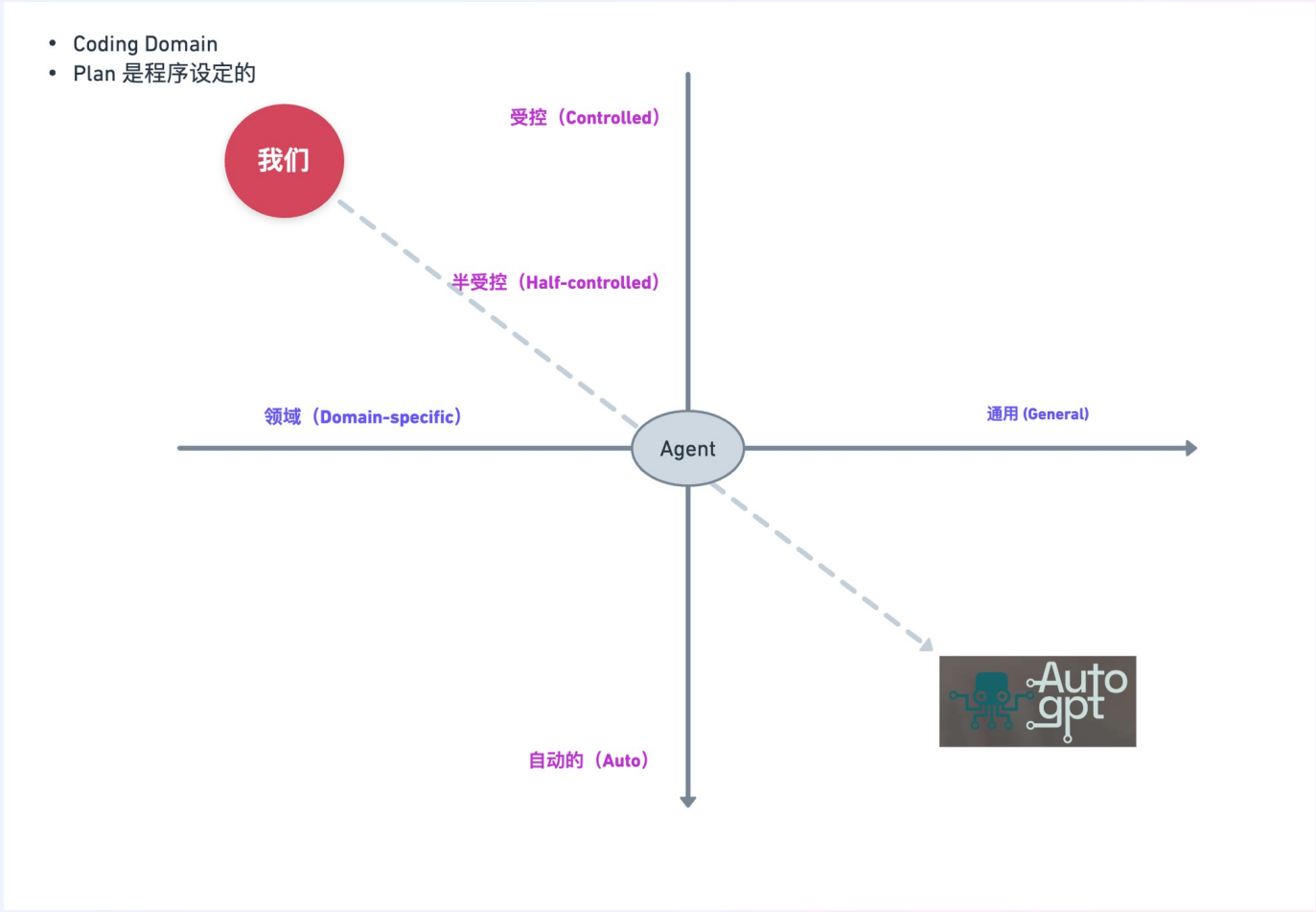
值得思考的点

多模态的能力

没有过多的提示词工程，也没有复杂的Workflow设计

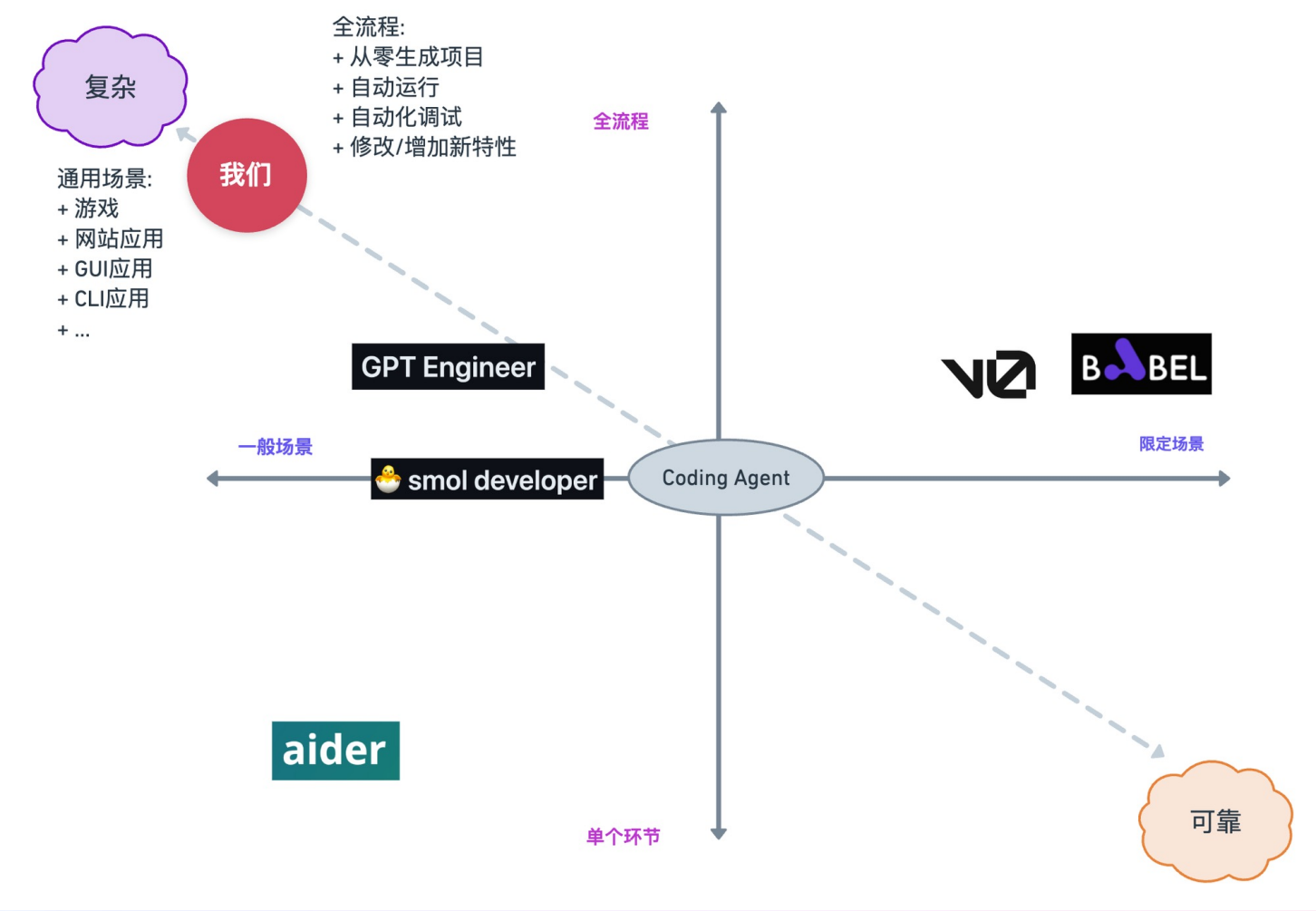
对LLM作为Agent“大脑”的基础能力有一个基本的认识和预期

AutoGPT为什么不行？



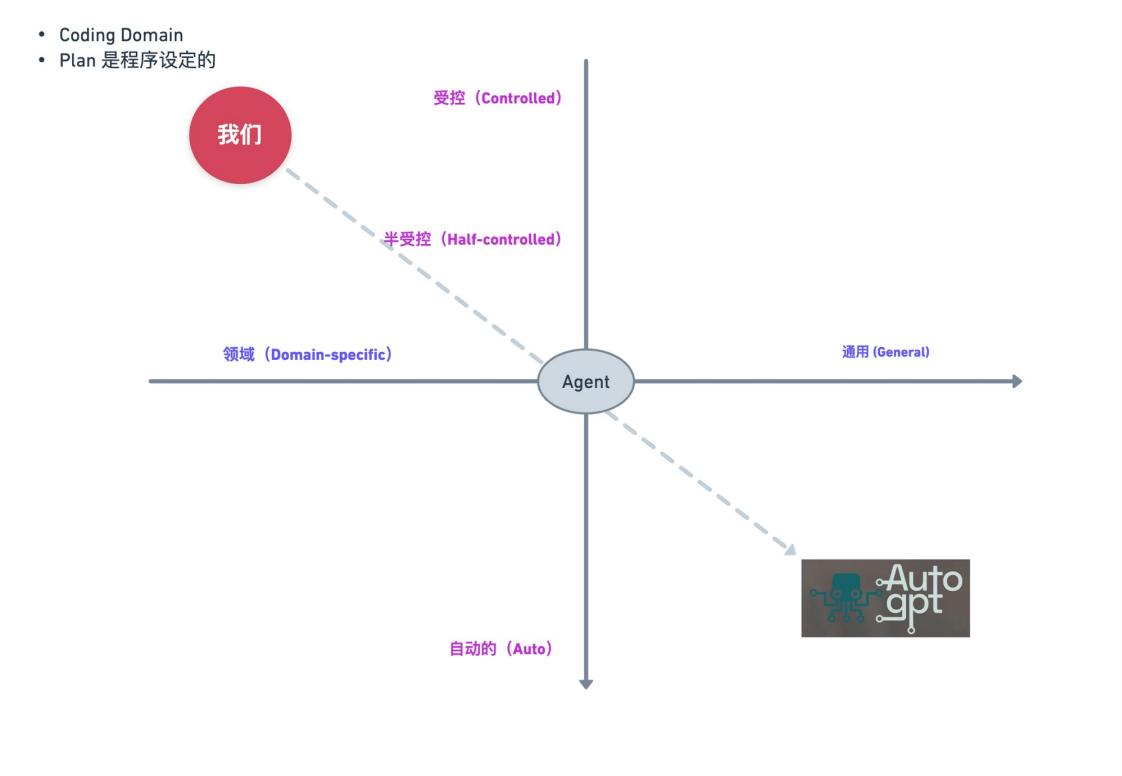
过于通用，过于自动。

AutoGPT为什么不行？



仍然过于通用，过于自动。

AutoGPT为什么不行？



受控：

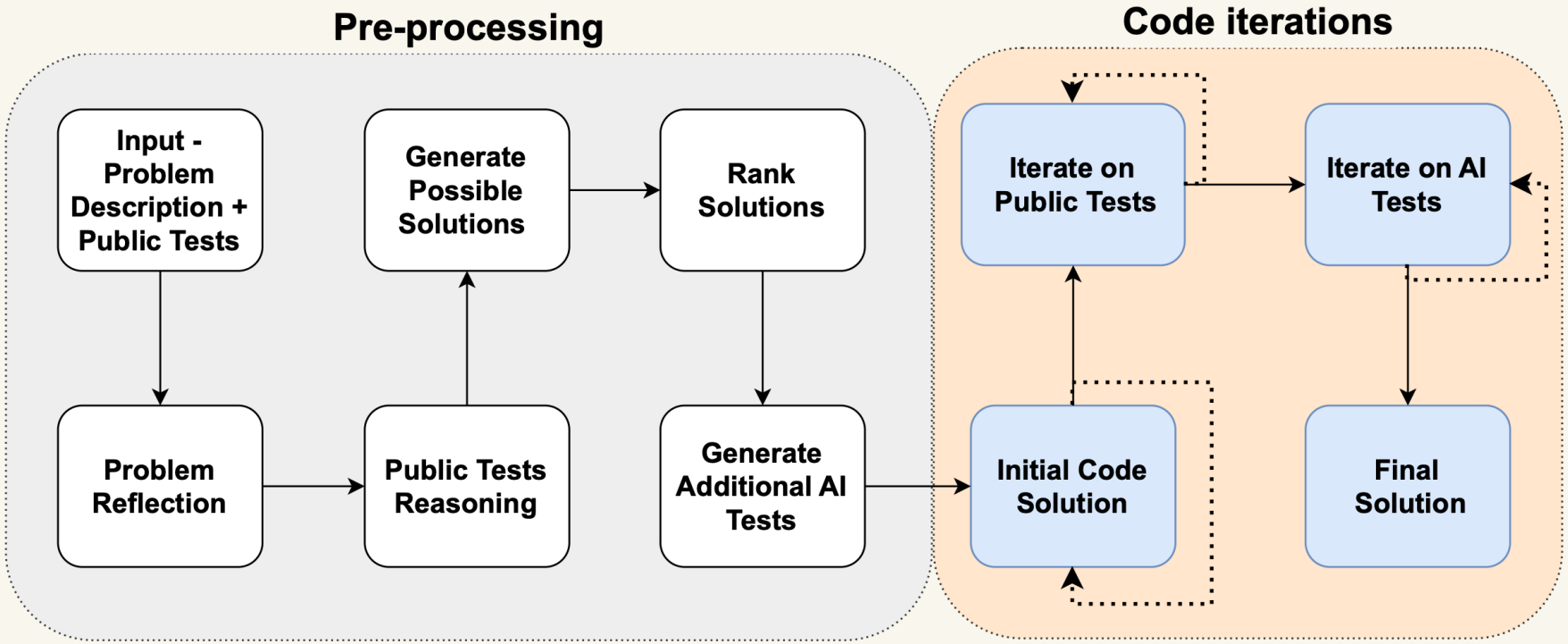
受程序控制，而不是受人控制，此谓之“工程”。

从Prompt Engineering到Flow Engineering – CodiumAI

Code Generation with AlphaCodium: From Prompt Engineering to Flow Engineering

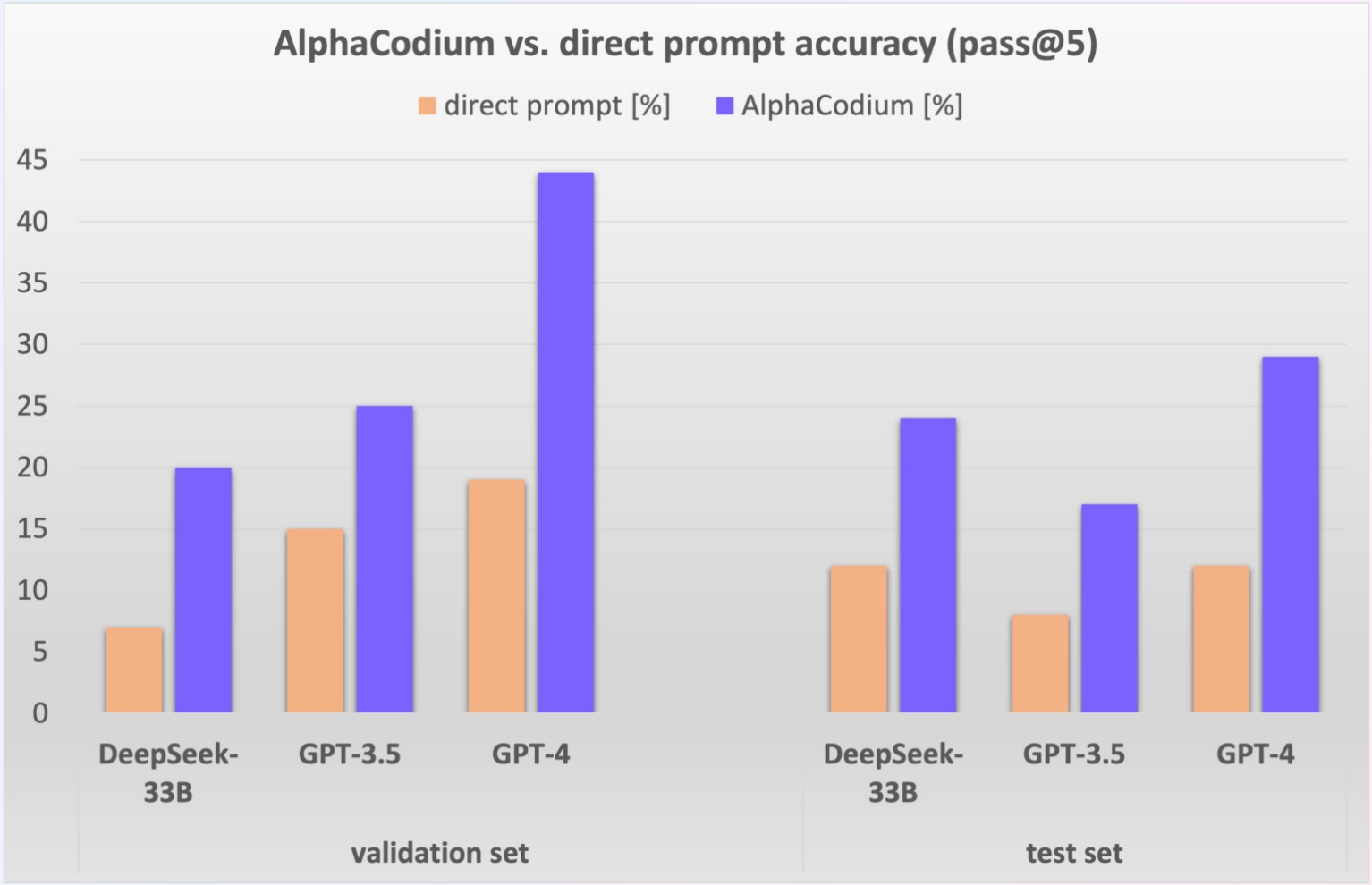
Tal Ridnik, Dedy Kredo, Itamar Friedman
CodiumAI
{tal.r, dedy.k, itamar.f}@codium.ai

从Prompt Engineering到Flow Engineering – CodiumAI



(a) The proposed AlphaCodium flow.

从Prompt Engineering到Flow Engineering – CodiumAI



最强LLM的基本表现

有Workflow vs 无Workflow

第100+个AI软件工程师 – Devin

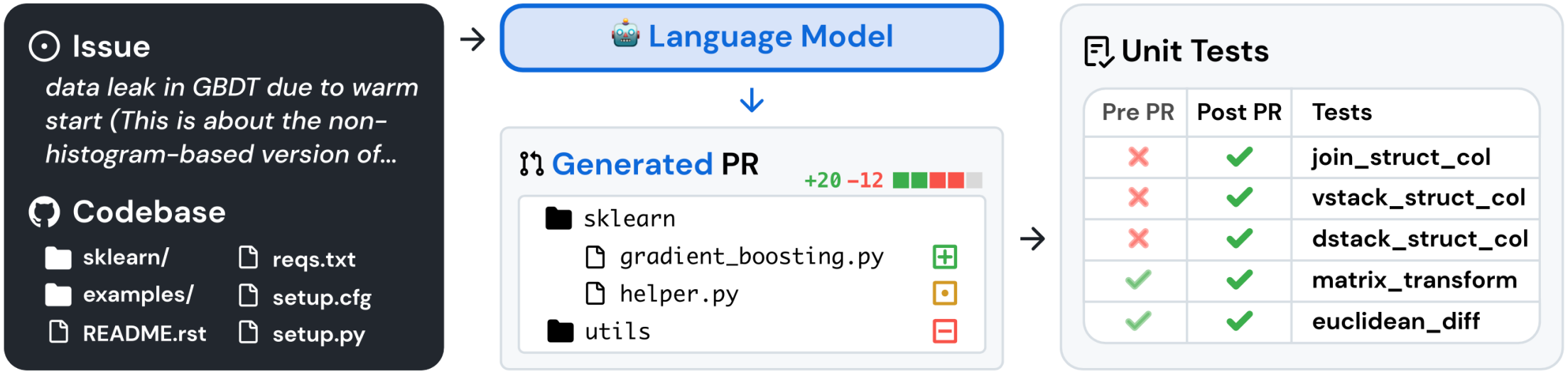
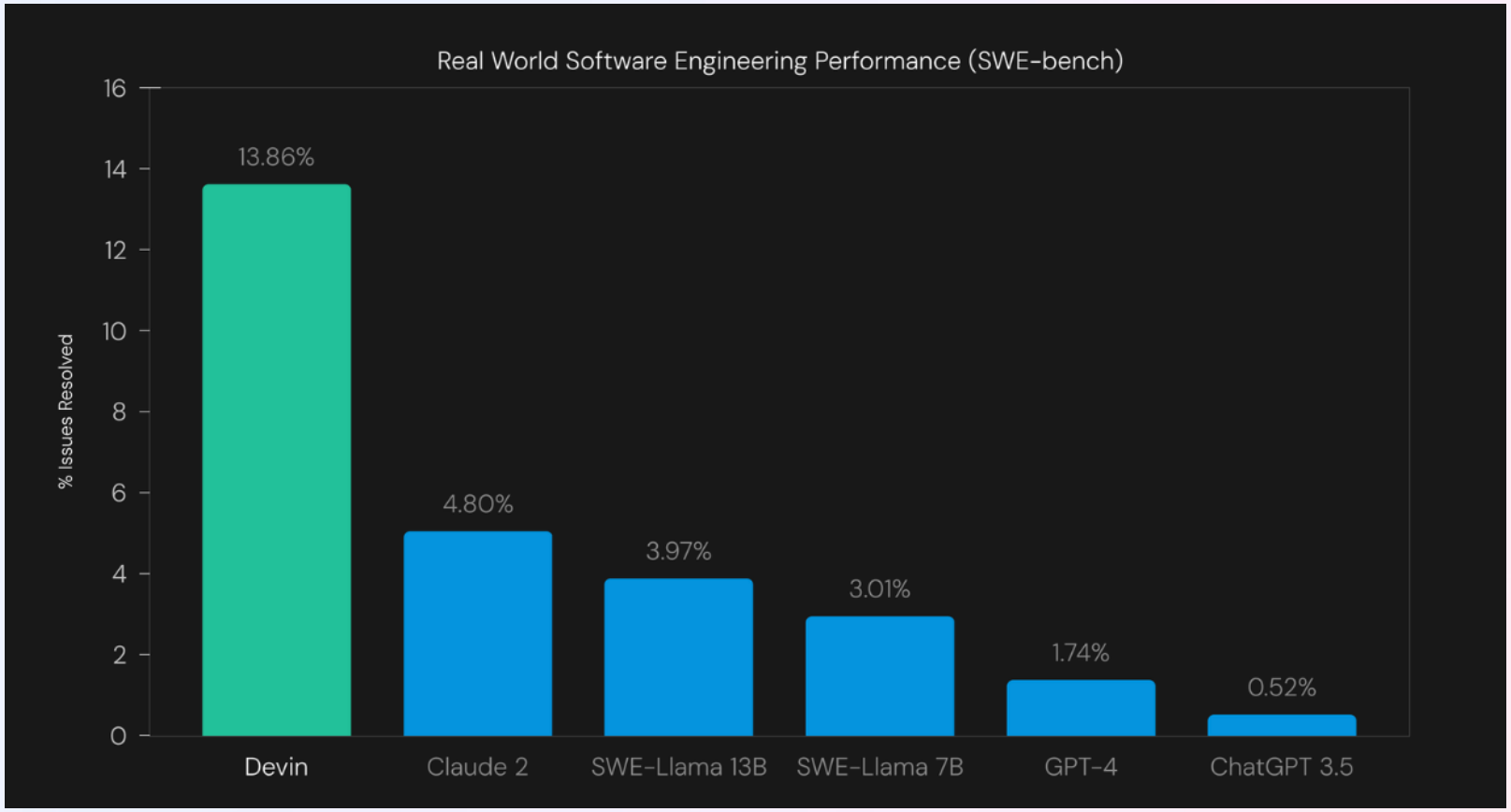


Figure 1: SWE-bench sources task instances from real-world Python repositories by connecting GitHub issues to merged pull request solutions that resolve related tests. Provided with the issue text and a codebase snapshot, models generate a patch that is evaluated against real tests.

第100+个AI软件工程师 – Devin



最强LLM的基本表现

有Workflow vs 无Workflow

大家快看，AI agentic workflows！ – Andrew Ng

大家快看，AI agentic workflows！ – Andrew Ng

如何设计 Workflow 和 Multiagent Flow

典型Agent应用：Coze Bots

Workflow 和 Multiagent Flow

以“Dr. Know”和“谁是卧底”为例

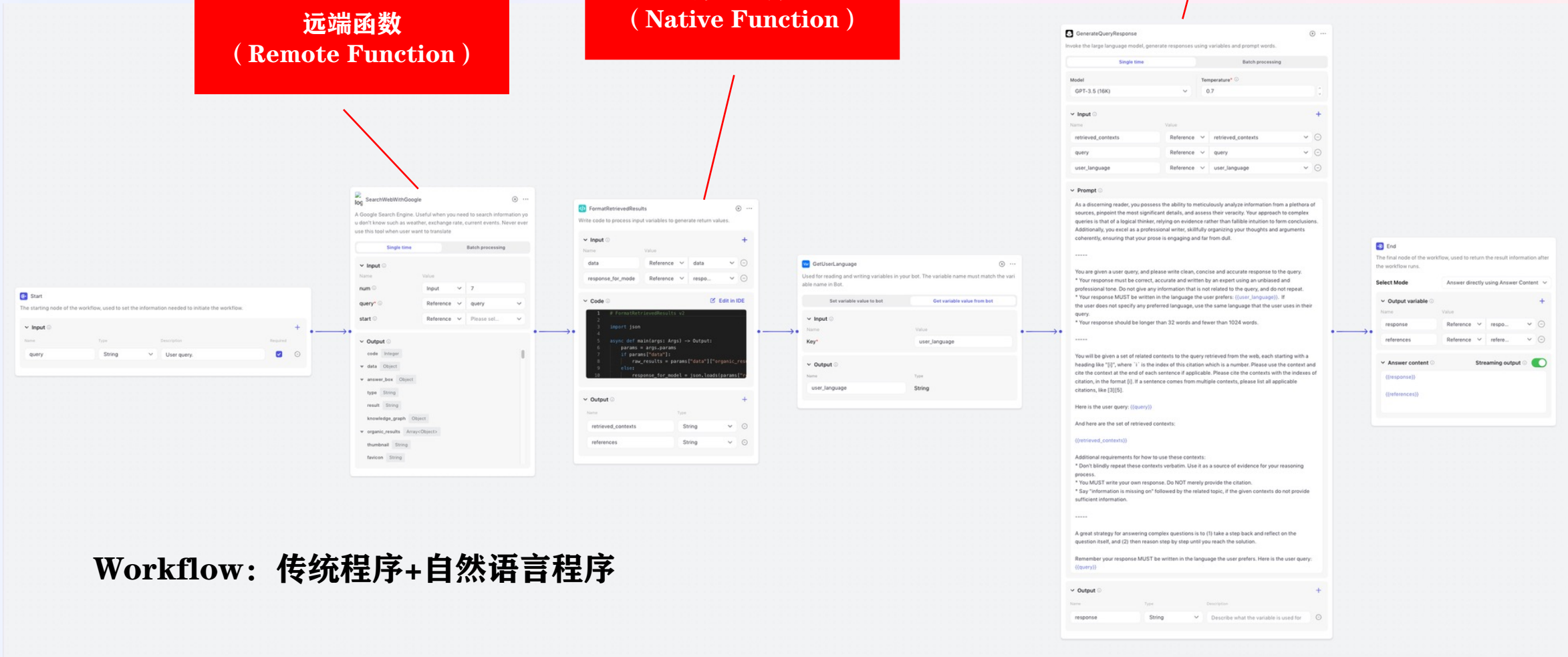
Workflow的构成

远端函数
（Remote Function）

原生函数
（Native Function）

语义函数
（Semantic Function）

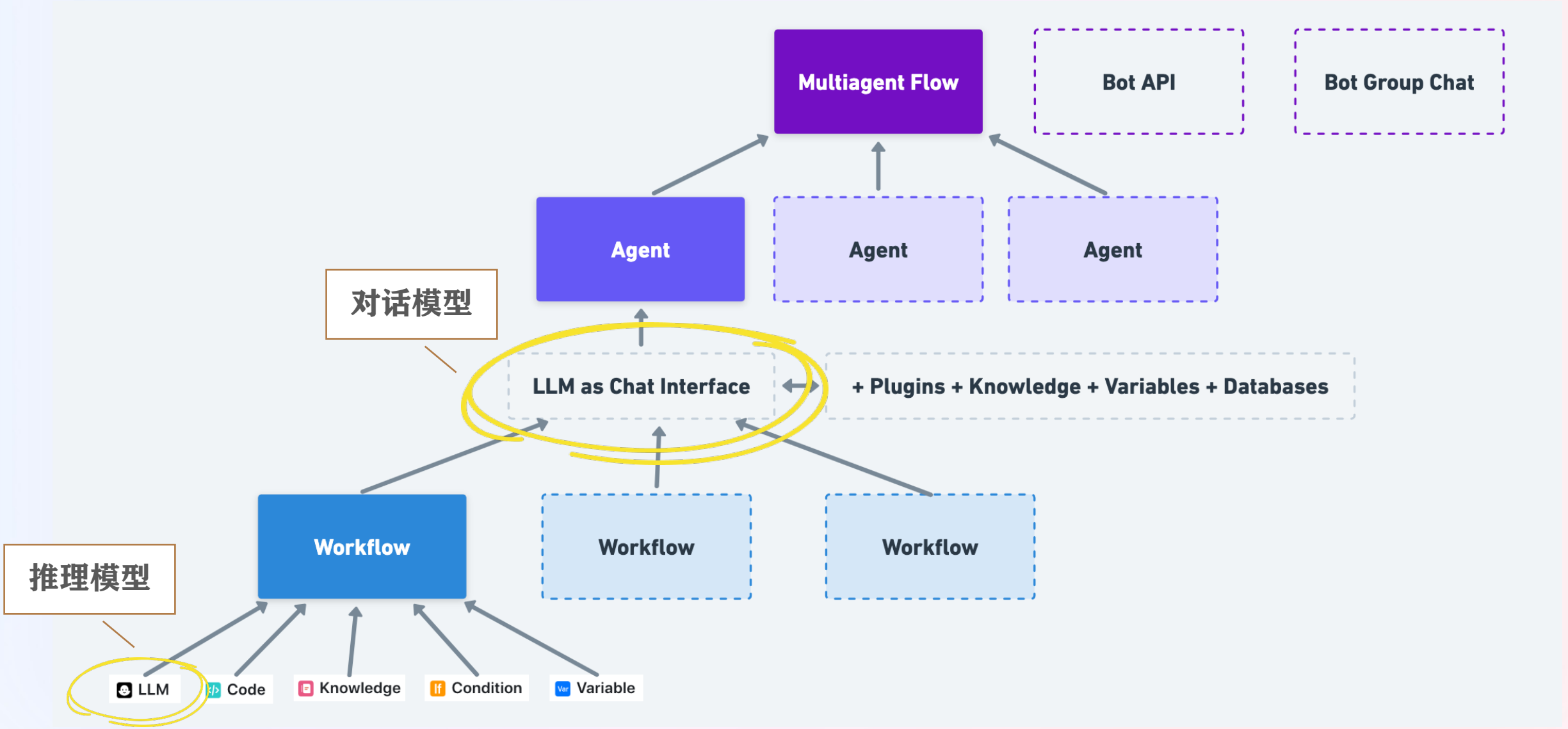
自然语言编写
模拟人的思考过程



Workflow：传统程序+自然语言程序

IPO：Input → Process → Output

组成Coze Bot的结构性元素




Q&A