

AI Agent

李宏毅

免責聲明：AI Agent 是一個被廣泛使用的詞彙，故本課程中所講的 AI Agent 不一定跟其他地方一樣

今天使用 AI 的方式

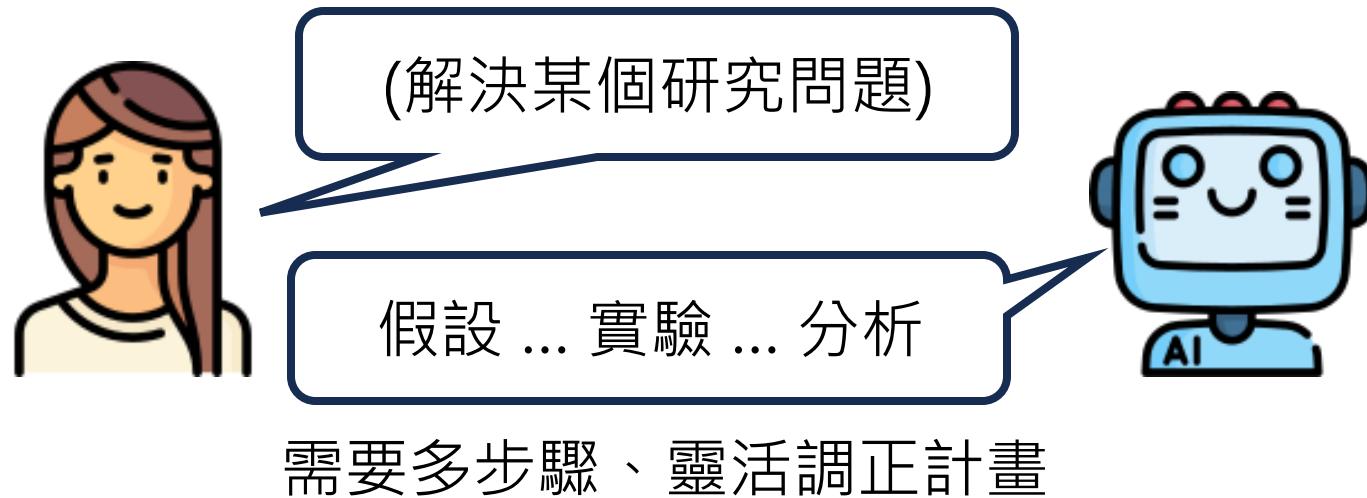
人類給予明確指令



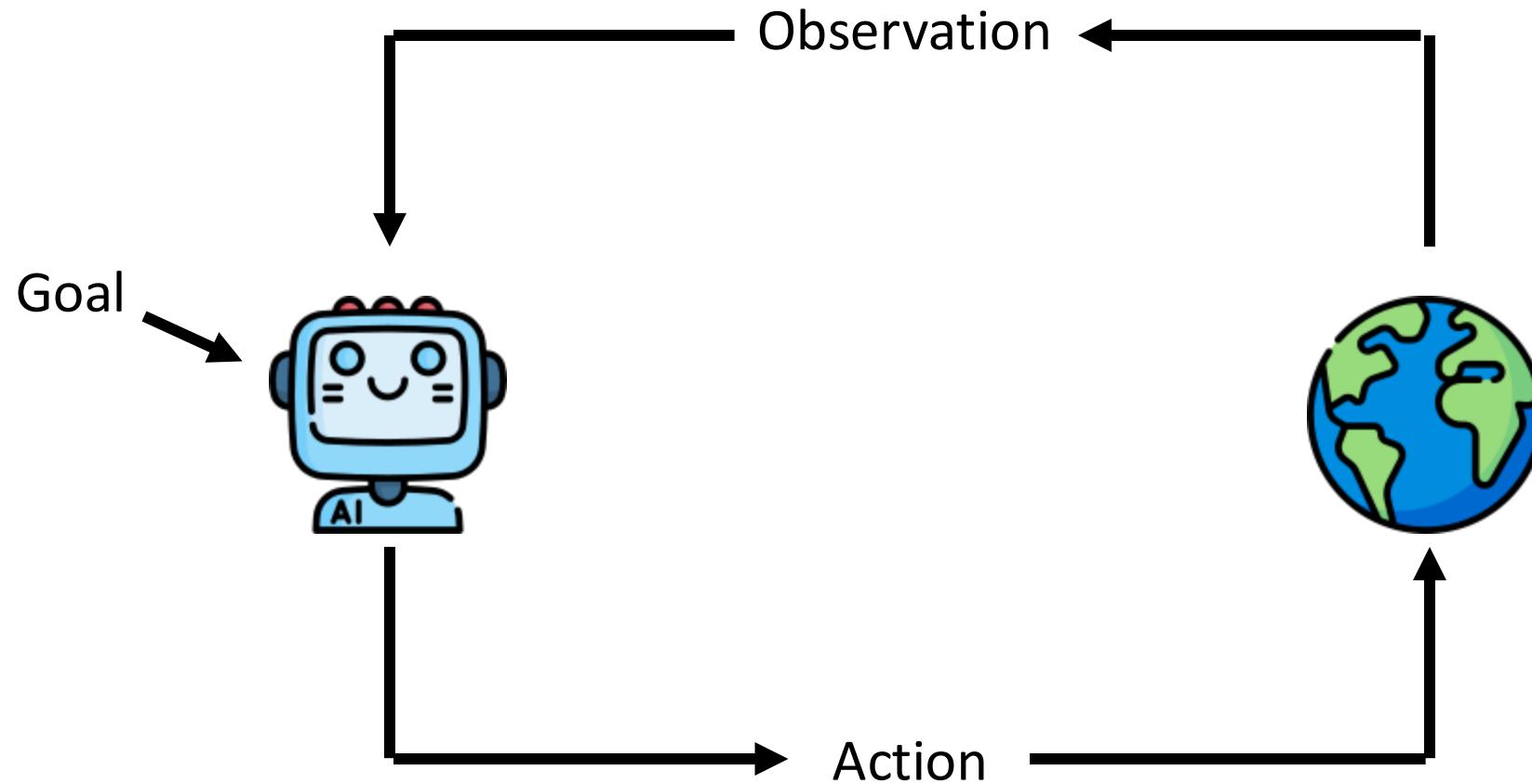
AI Agent

人類給予目標

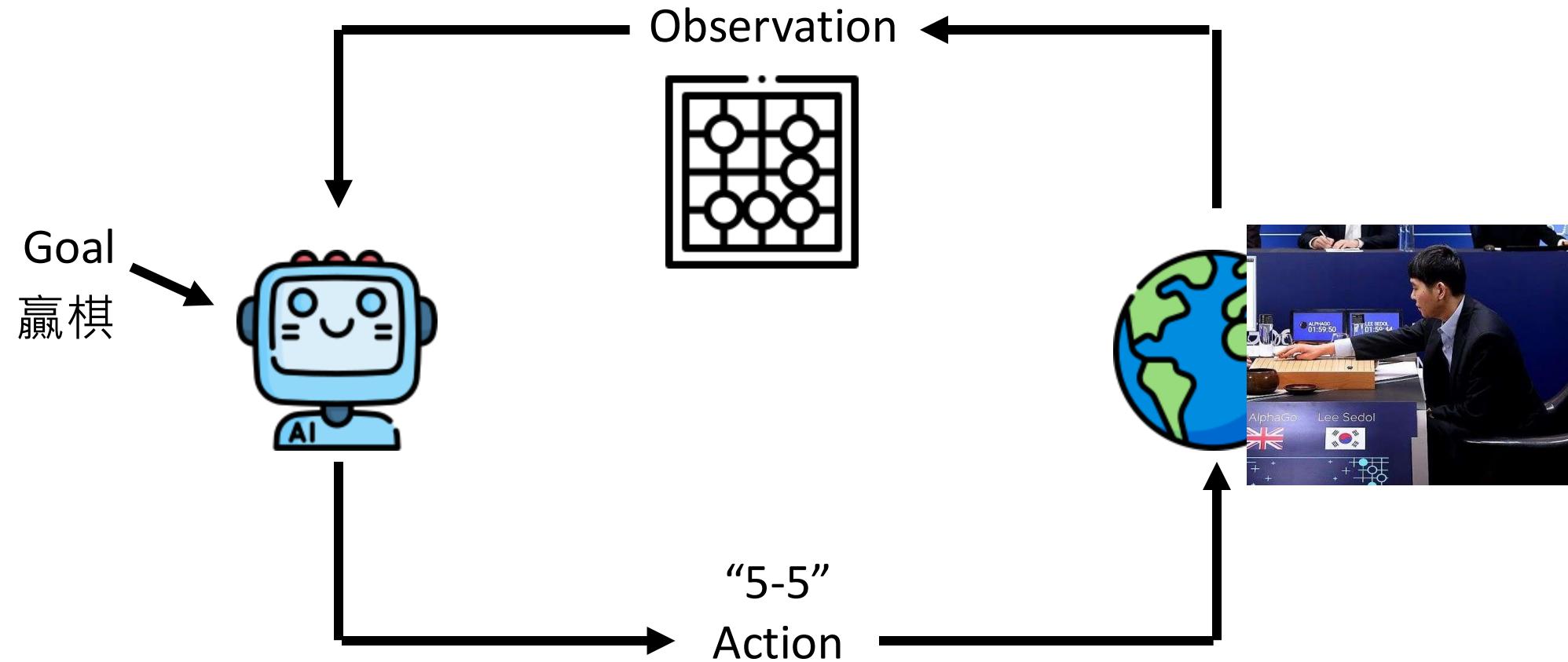
AI 自己想辦法達成



AI Agent

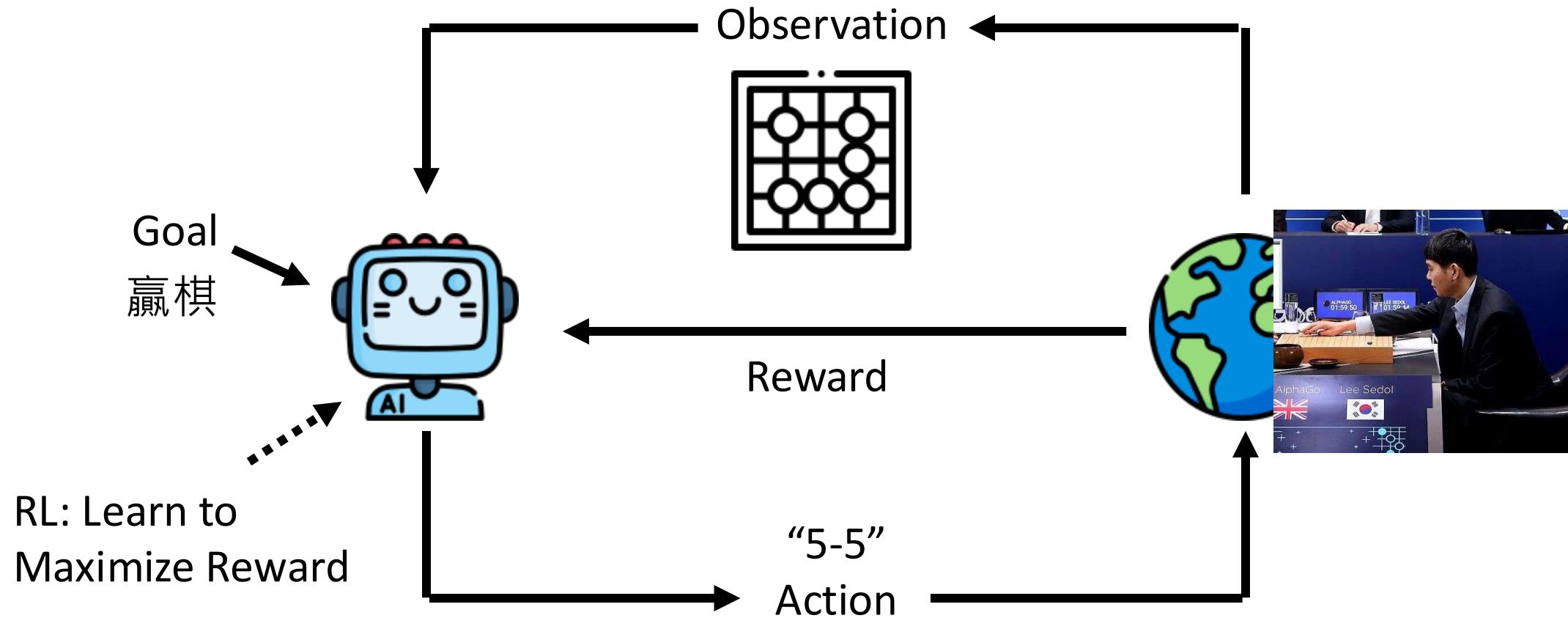


Agent (AlphaGo)



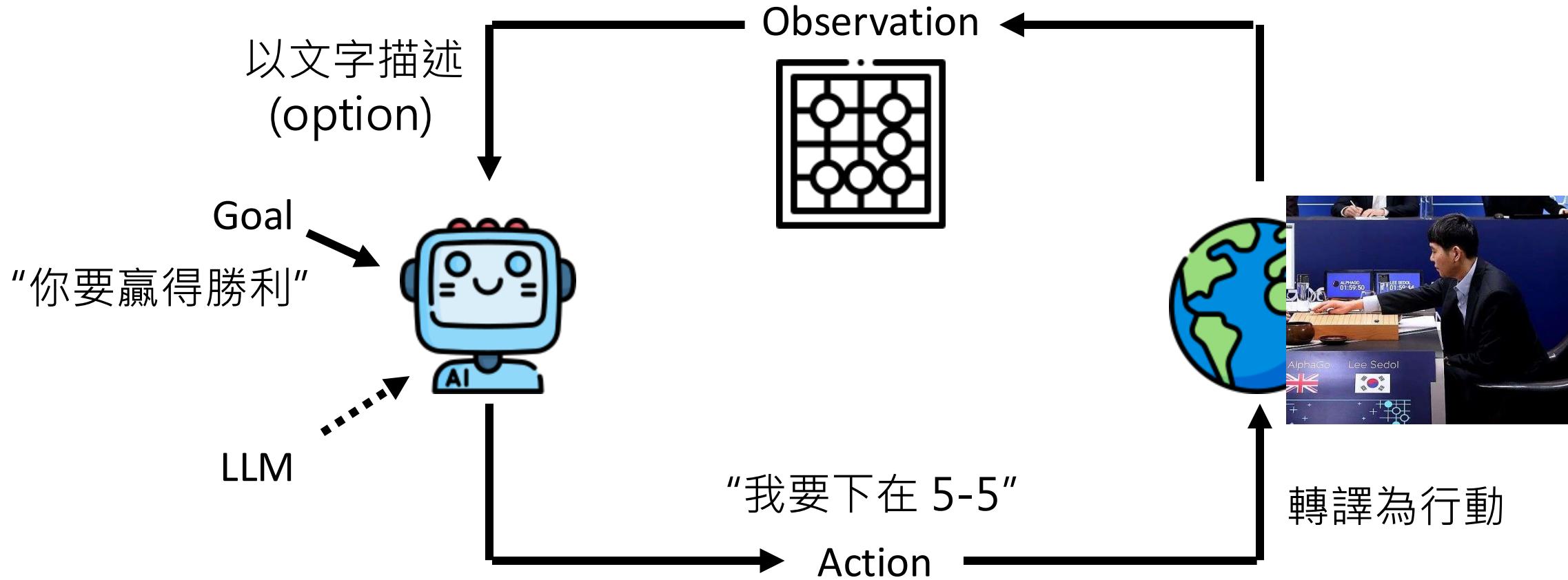
(RL: Reinforcement Learning)

如何打造 AI Agent? RL?



侷限：需要為了每一個任務以 RL 訓練模型

如何打造 AI Agent? 直接用 LLM !

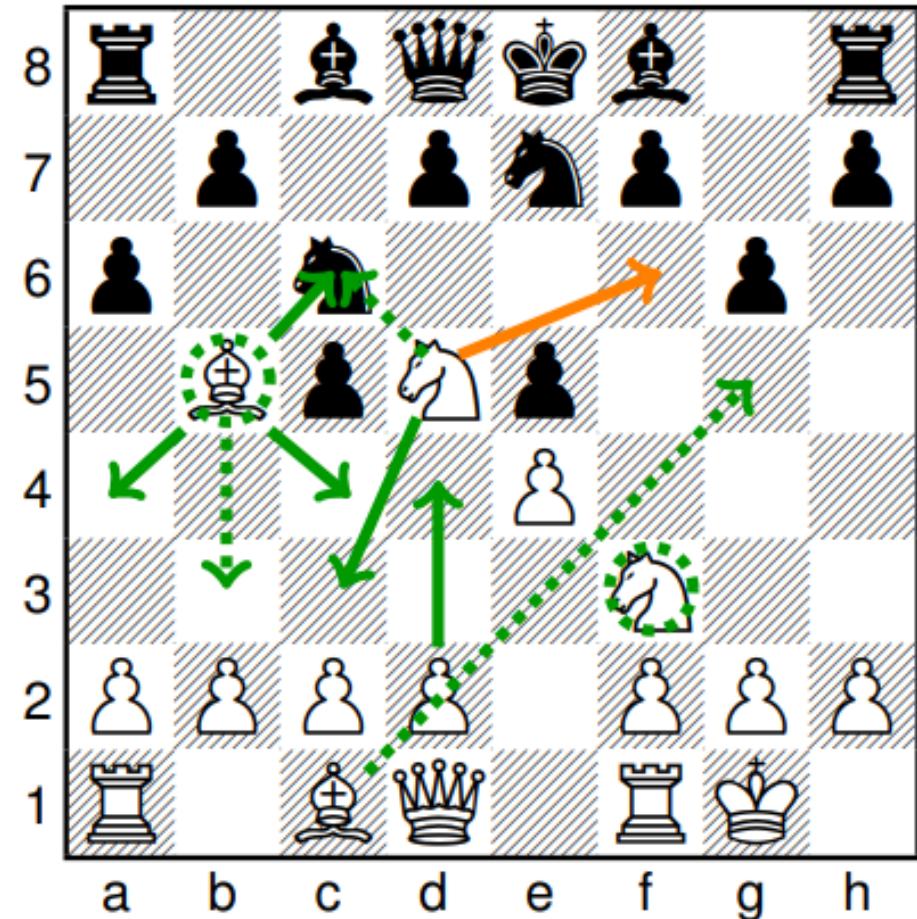


以 LLM 直接實踐人類對於擁有 Agent 的渴望

LLM 能不能下棋？

- BIG-bench

<https://arxiv.org/abs/2206.04615>



In the following chess position, find a checkmate-in-one move.

1. e4 c5
2. Nf3 e5
3. Nc3 Nc6
4. Bb5 Nge7
5. 0-0 g6
6. Nd5 a6
- 7.

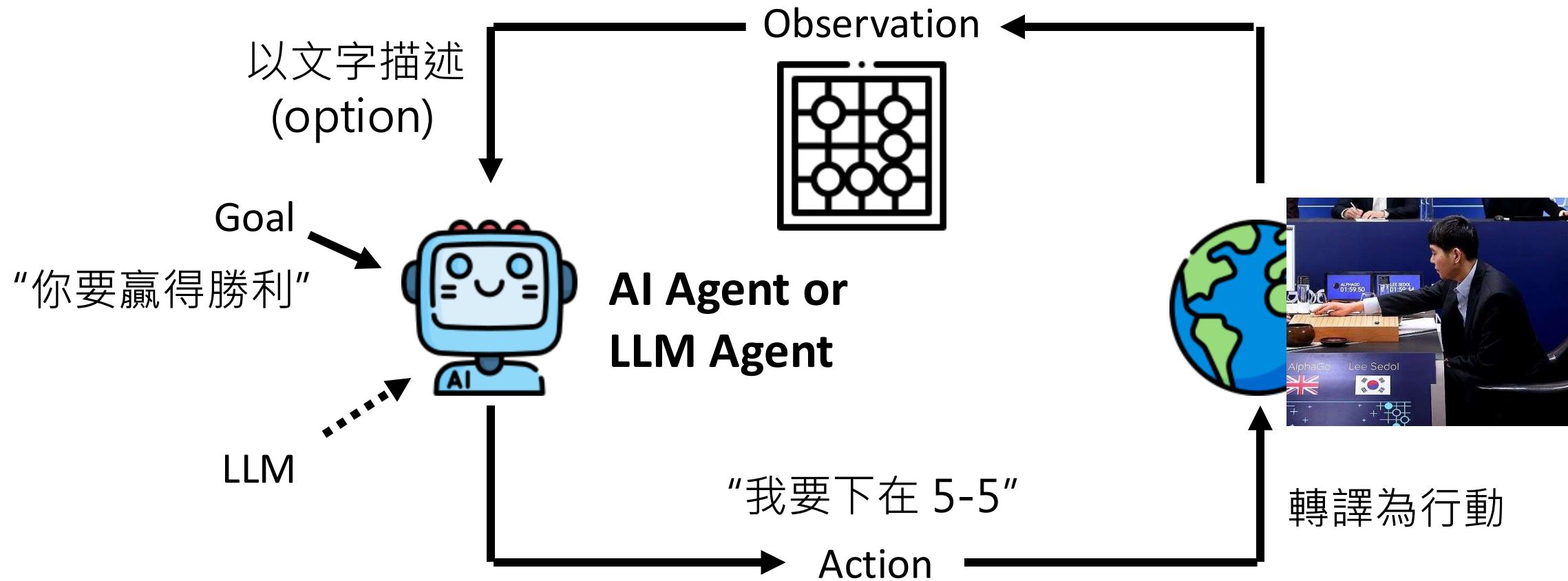
LLM 能不能下棋？

https://youtu.be/JHq4EKMg7fI?si=izKsH-GCVnZkooq_



ChatGPT vs DeepSeek: CRAZY Chess

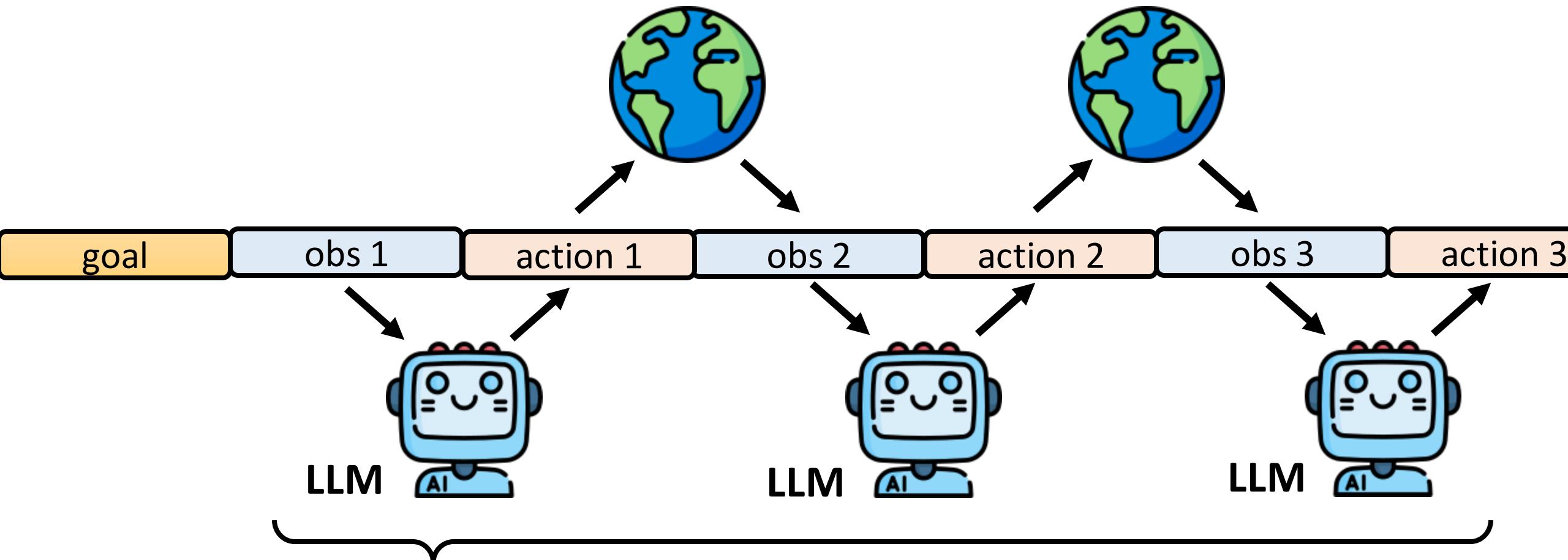
如何打造 AI Agent? 直接用 LLM !



以 LLM 直接實踐人類對於擁有 Agent 的渴望

還有多遠?
能否變得更近?

從 LLM 的角度來看 Agent 要解的問題



一直都在做接龍

AI Agent 倚靠的是語言模型現有的能力

AI Agent 不是最近才熱門

- 2023 年春天曾經爆紅過一次

AutoGPT, AgentGPT,
BabyAGI, Godmode ...

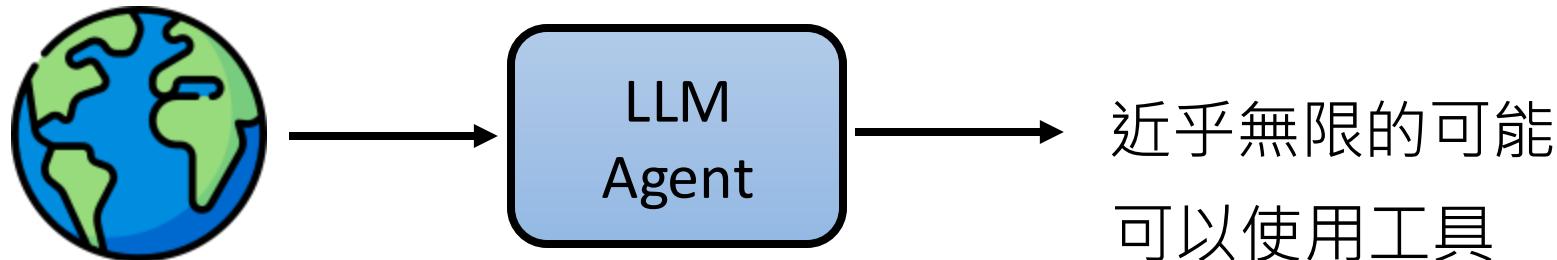
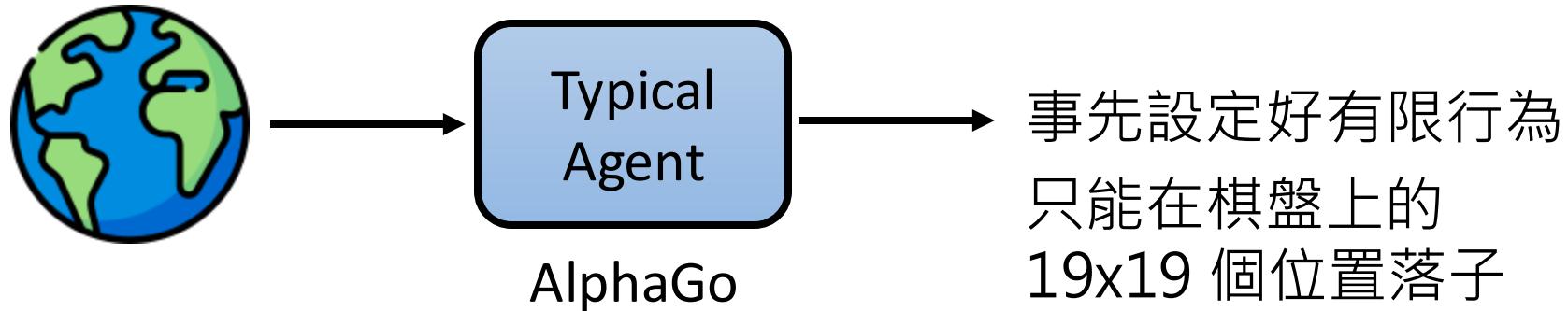
<https://youtu.be/eQNADIR0jSs?si=4yGZEJuAUzKK2VD0>



【生成式AI 2023】讓 AI 做計劃然後自己運行自己

請注意在以下這堂課中
沒有任何模型被訓練

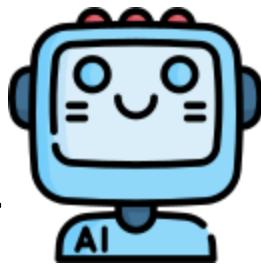
以 LLM 運行 AI Agent 的優勢



以 LLM 運行 AI Agent 的優勢

Typical Agent

programmer



Reward = -1

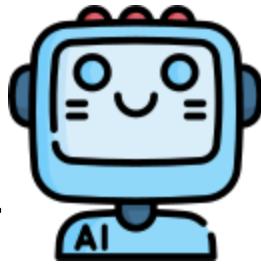
為什麼是 -1???

Compile Error



AI Agent

programmer



更多資訊

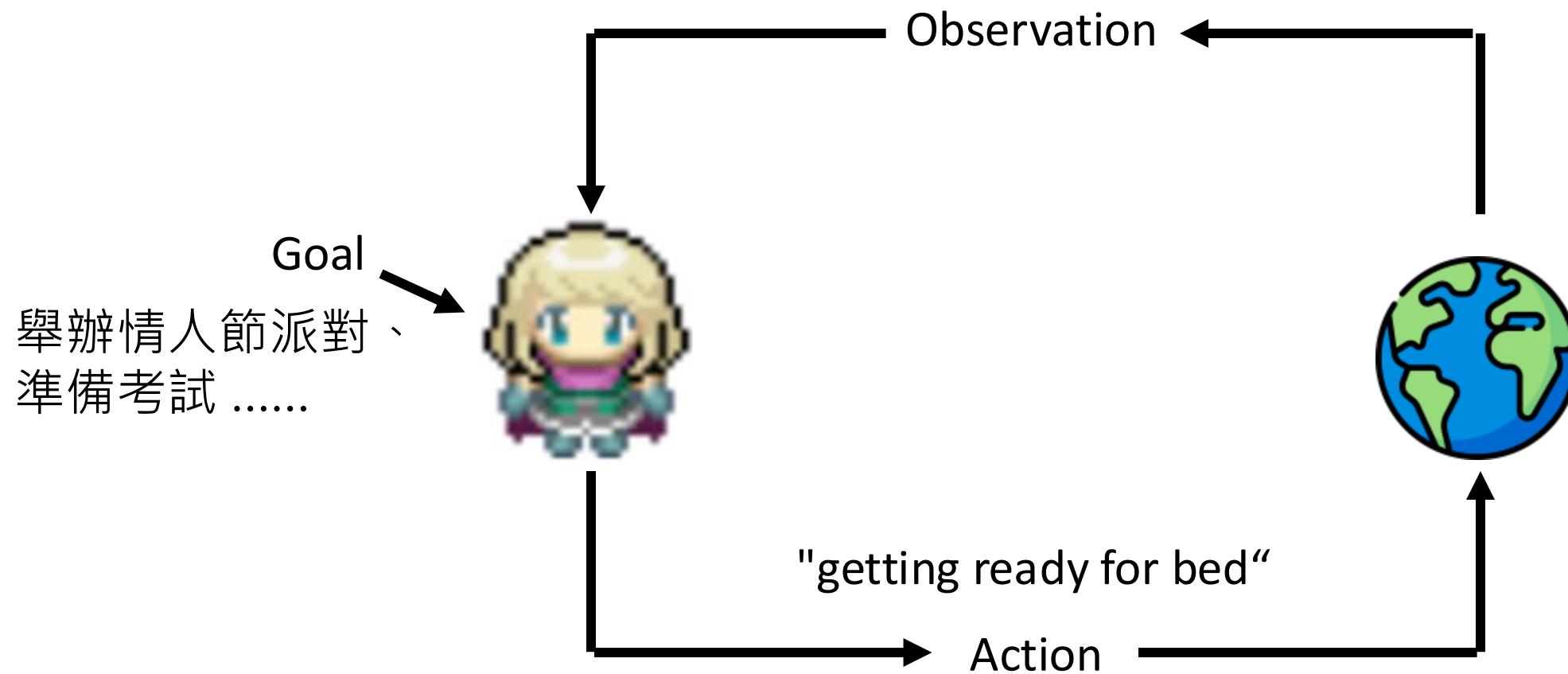
Compile Error



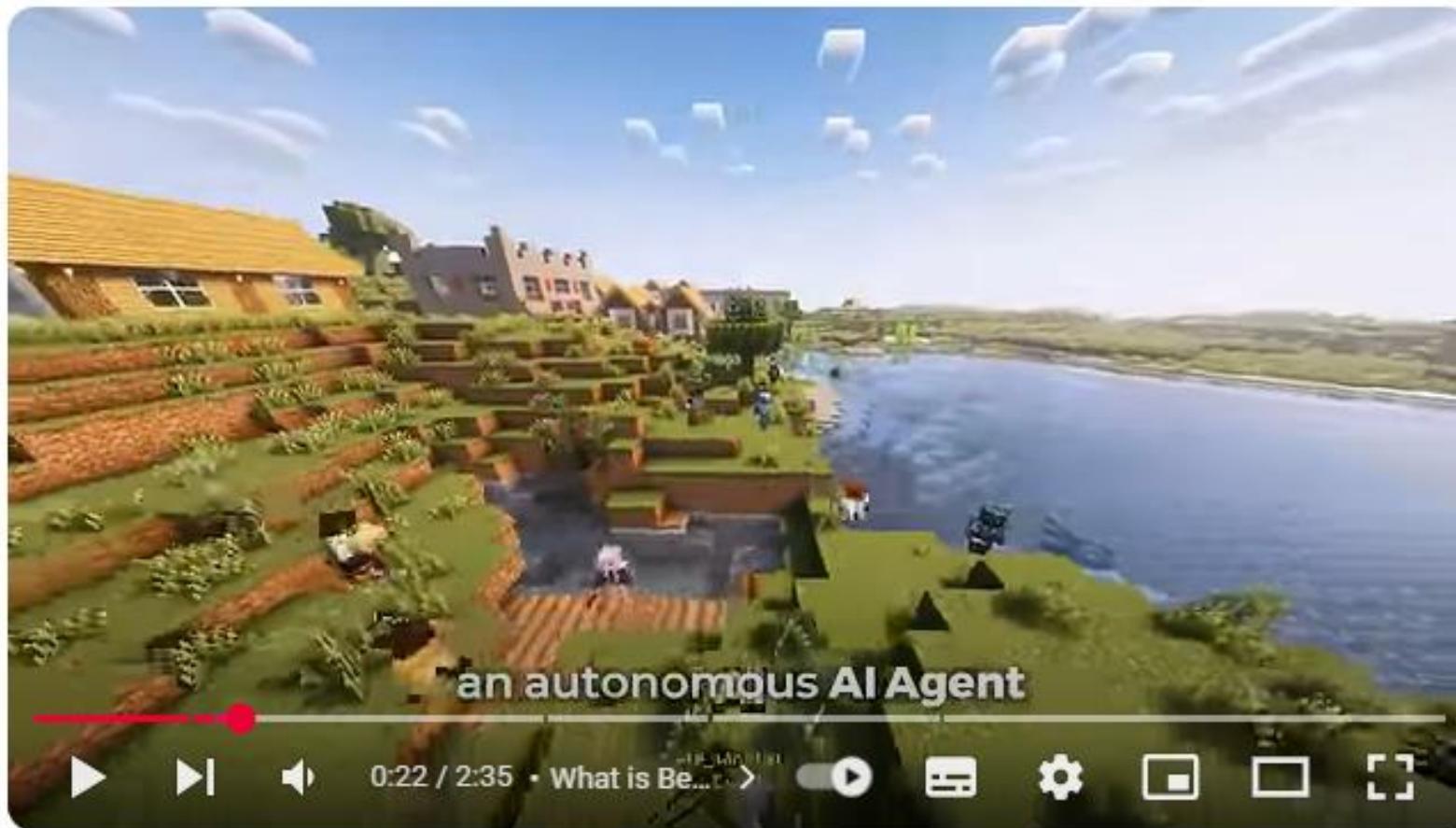
AI Agent 舉例：AI 村民組成的虛擬村莊



```
[node_749] 2023-02-13 15:33:20: Eddy Lin is studying music theory  
[node_748] 2023-02-13 15:33:20: cooking area is idle  
[node_747] 2023-02-13 15:33:20: kitchen sink is idle  
[node_746] 2023-02-13 15:33:20: behind the cafe counter is idle  
[node_745] 2023-02-13 15:32:10: Isabella Rodriguez is gathering decorations
```



AI Agent 舉例：Minecraft 中的 AI NPC



1000 AI NPCs simulate a CIVILIZATION in Minecraft

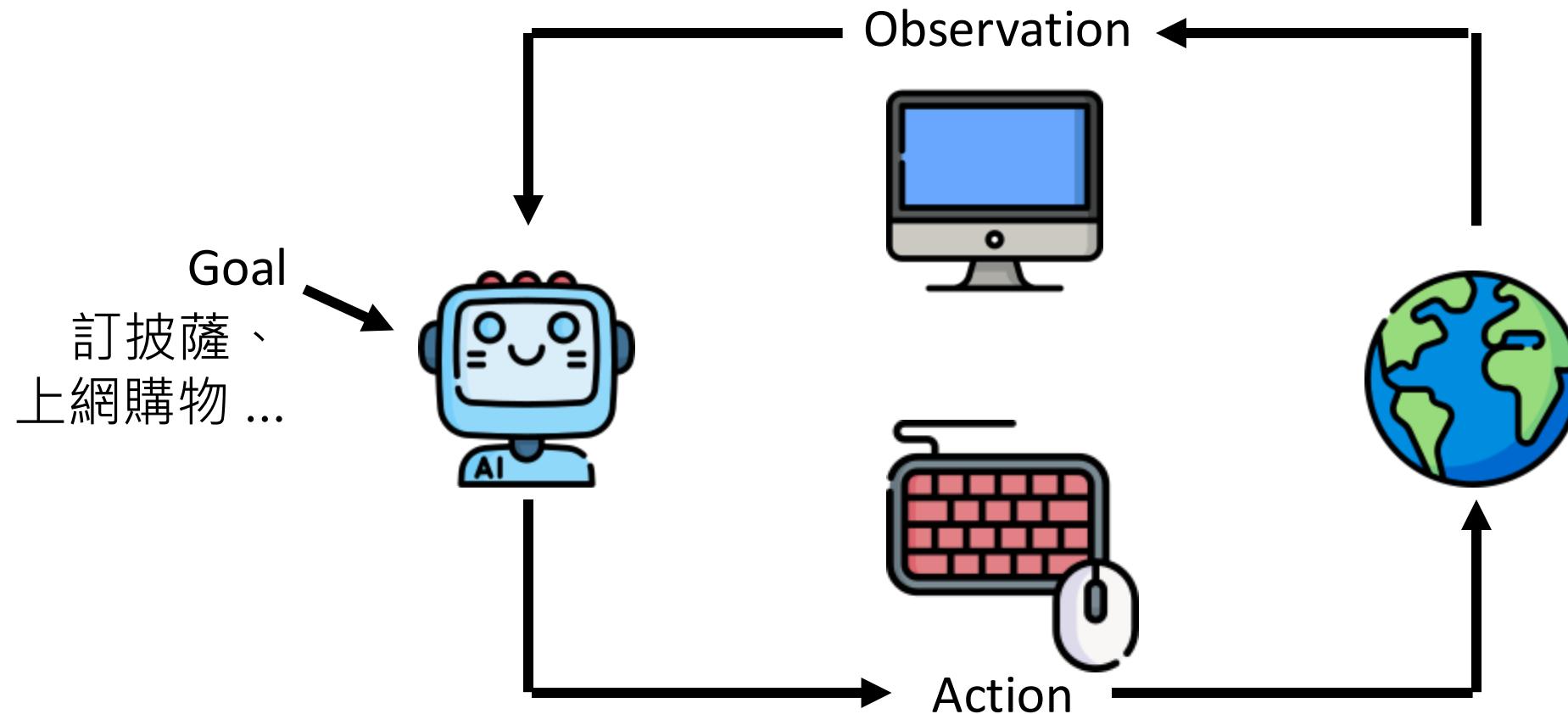
<https://www.youtube.com/watch?v=2tbaCn0KI90>

AI Agent 舉例：讓 AI 使用電腦

Computer Use,
Operator



AI Agent 舉例：讓 AI 使用電腦



AI Agent 舉例：讓 AI 使用電腦

- World of Bits: An Open-Domain Platform for Web-Based Agents (ICML, 2017)

Click on the "Next" button.

Ok
nunc vitae purus.;

Next
viverra ac, sed:

No
purus sit quis

Select Daria>Poly

Frederica
Martina >
Daria >
Angie

Select the following color █ with the color picker and hit Submit.

Color:

Enter the value that corresponds with each label into the form and submit when done.

Country	Costa Rica
Color	gray
First name	Lynnette
Religion	Judaism
Language	Wu
Language:	
First name:	
Submit	

Use the textbox to enter "Leonie" and press "Search", then find and click the 2nd search result.

Leonie

[Chas](#)
<https://www.senectus.us>
Aliquam cursus. At.
[Leonie](#)
<https://www.tortor.it>
Ultricies congue gravida.
[Marcella](#)
<https://www.vestibulumduis.hk>
Pulvinar aliquam adipiscing.

1 2 3 ≥

Find the email by Bobbette and click the trash icon to delete it.

Primary

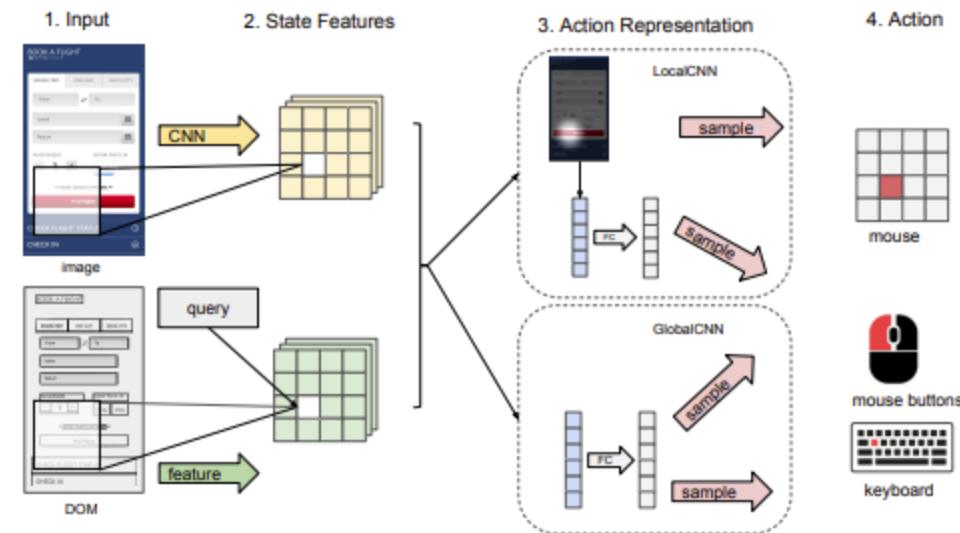
[Corabelle](#) ★ ⚡
Magna tortor,
lacinia euismod.
[Jennimah](#) ★ ⚡
Porttitor,
Odio tellus. Li..
[Ingaberg](#) ★ ⚡
Amet.
Facilisi vel te..
[Madellina](#) ★ ⚡

Book the cheapest one-way flight from: NLG to: Brownsville, TX on 12/10/2016.

Book Your One-Way Flight:

From:
To:

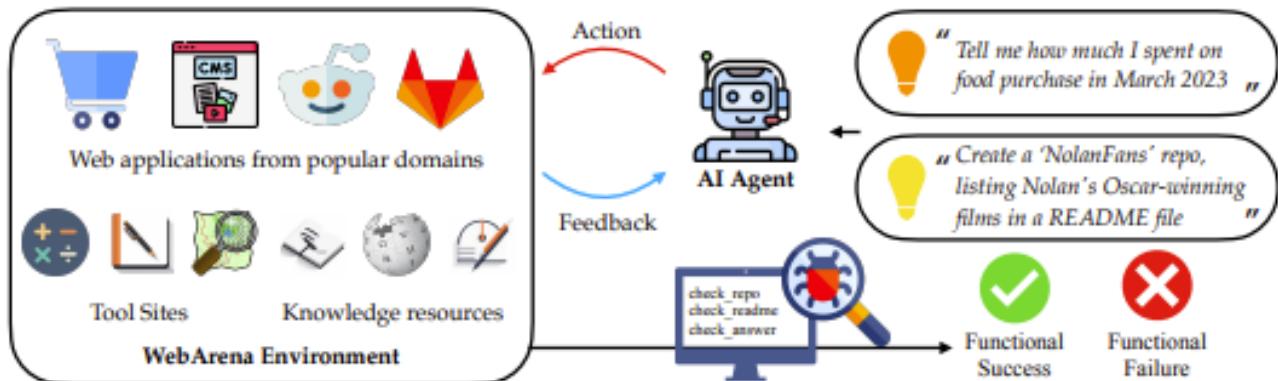
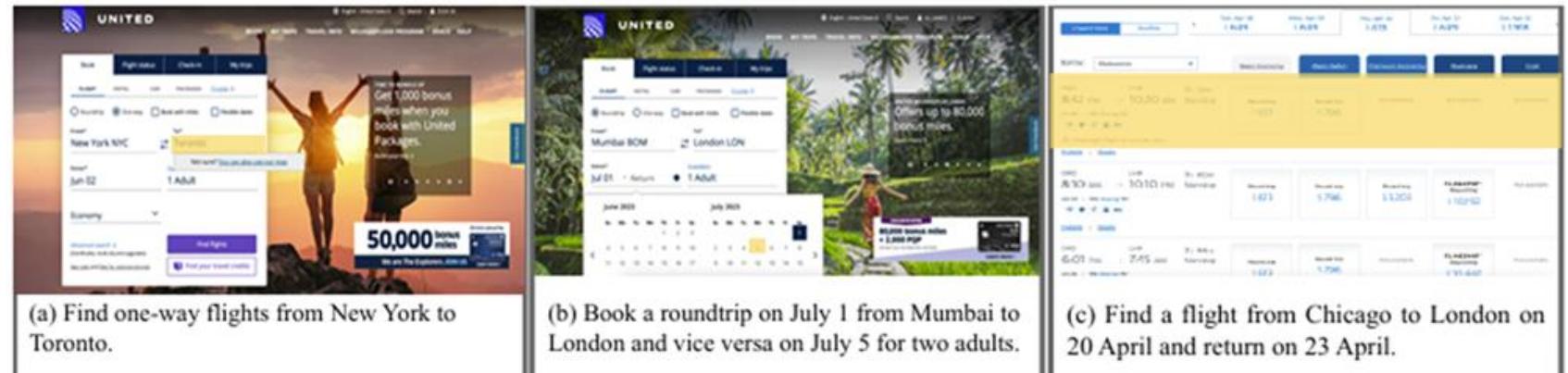
Departure Date



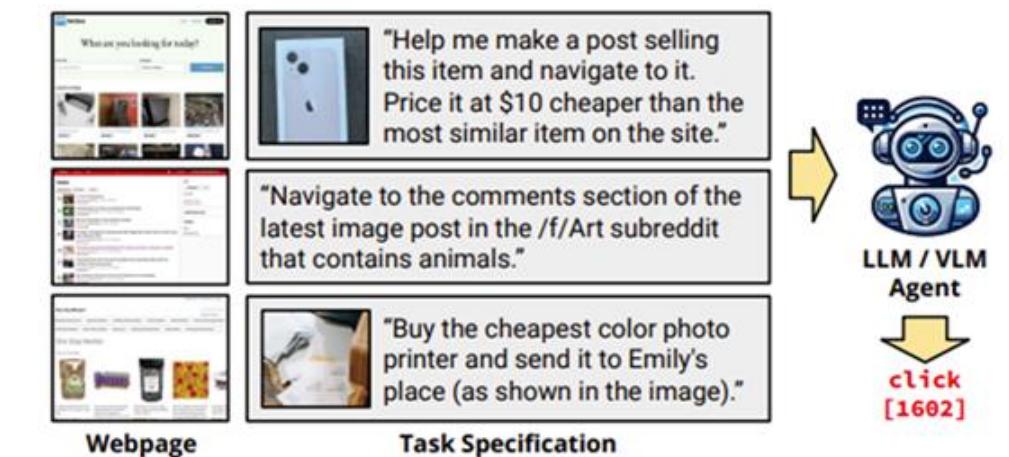
AI Agent 舉例：讓 AI 使用電腦

Mind2Web

<https://arxiv.org/abs/2306.06070>

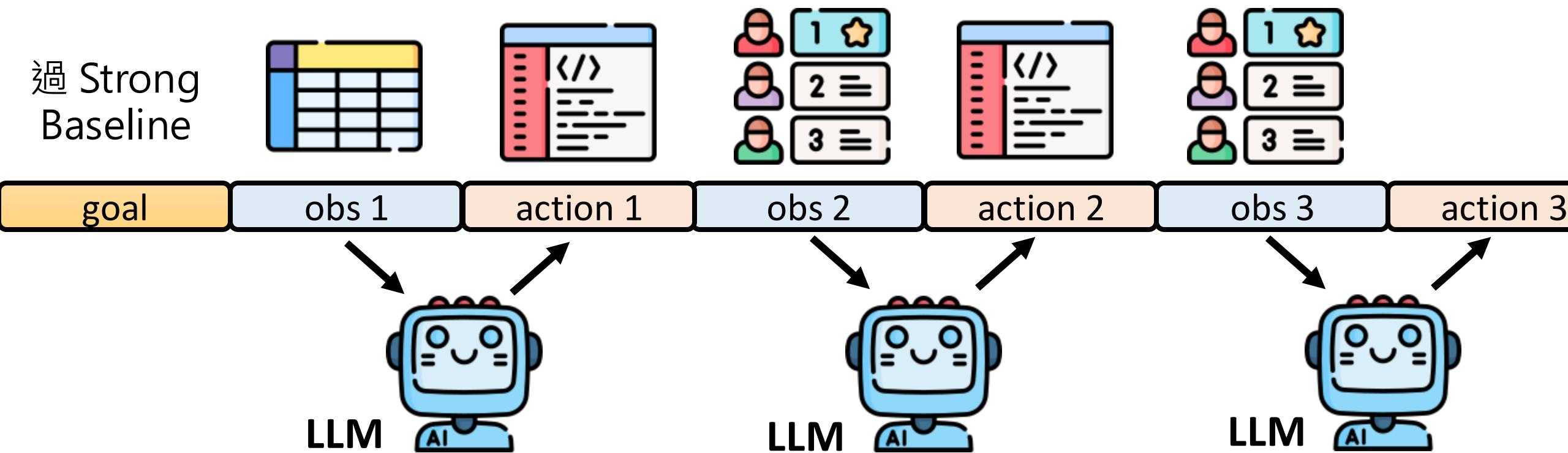


WebArena <https://arxiv.org/abs/2307.13854>



VisualWebArena <https://arxiv.org/abs/2401.13649>

AI Agent 舉例：用 AI 訓練模型

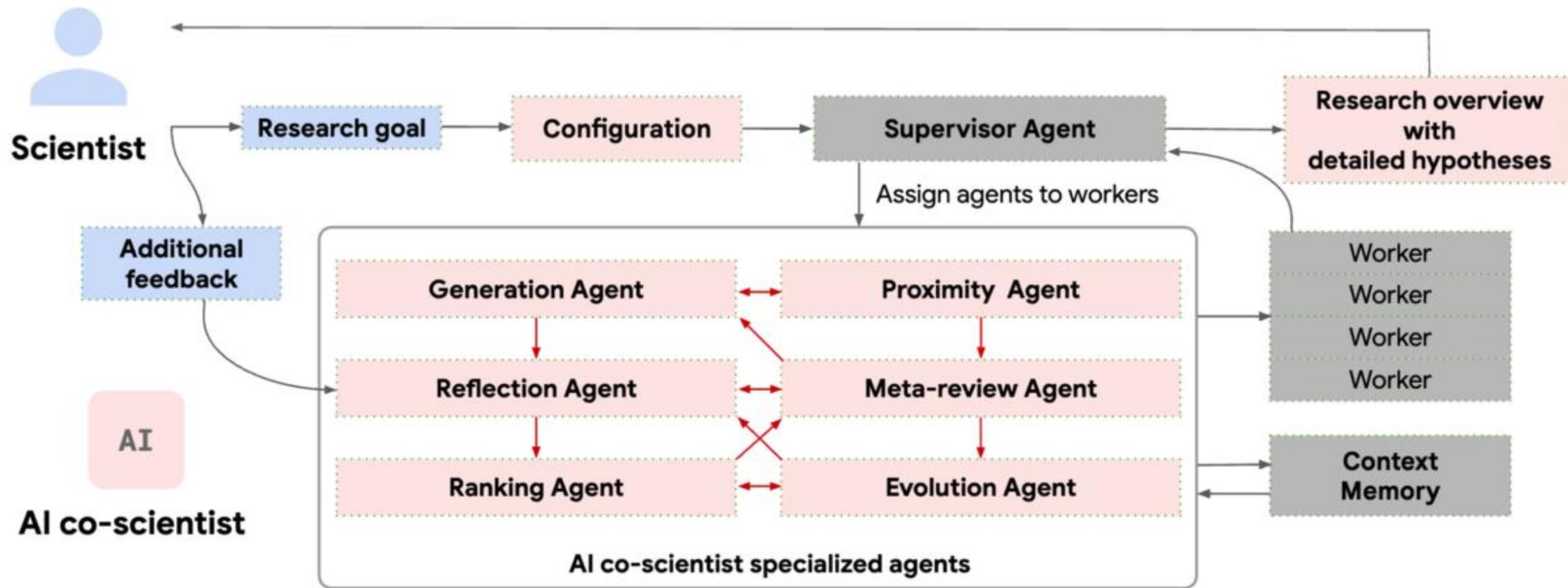


AIDE: The Machine Learning Engineer Agent <https://arxiv.org/abs/2502.13138>

AutoKaggle: A Multi-Agent Framework for Autonomous Data Science Competitions

<https://arxiv.org/abs/2410.20424>

AI Agent 舉例：用 AI 做研究

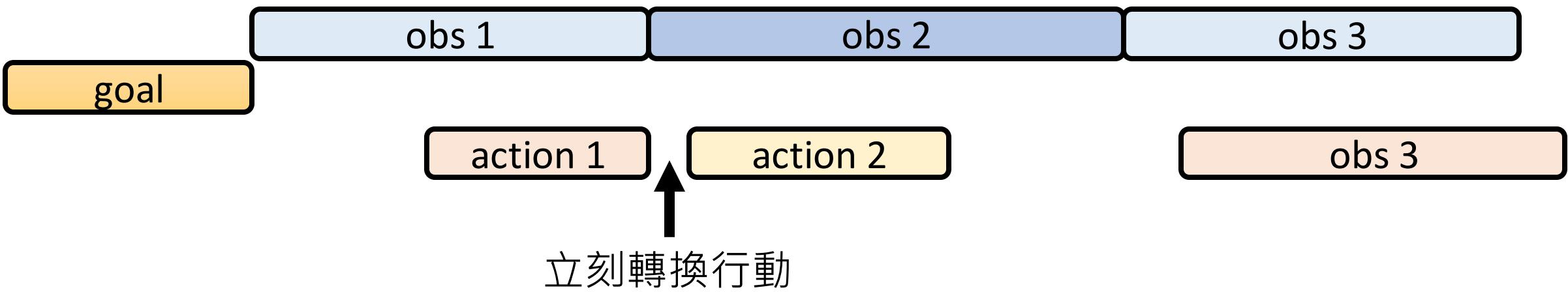


邁向更加真實的互動情境

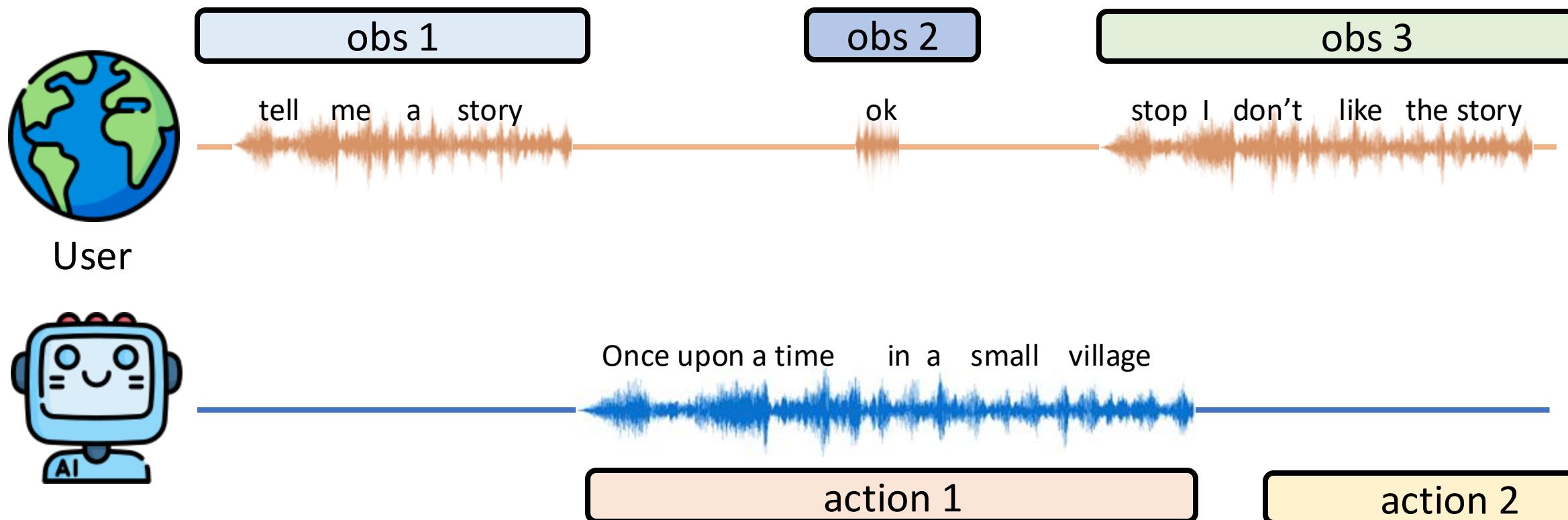
回合制互動



即時互動



邁向更加真實的互動情境



今日課程內容

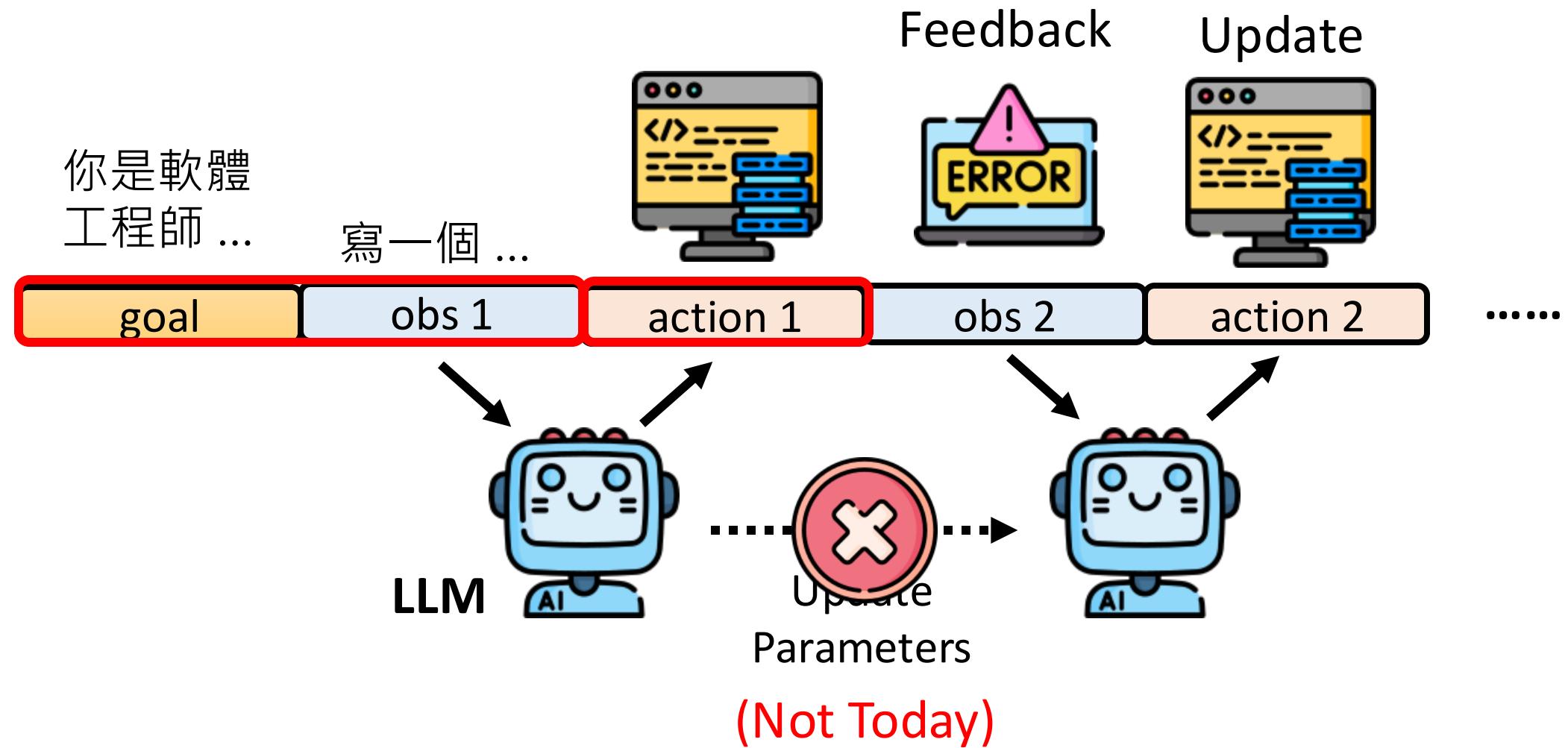
AI 如何根據經驗調整行為

AI 如何使用工具

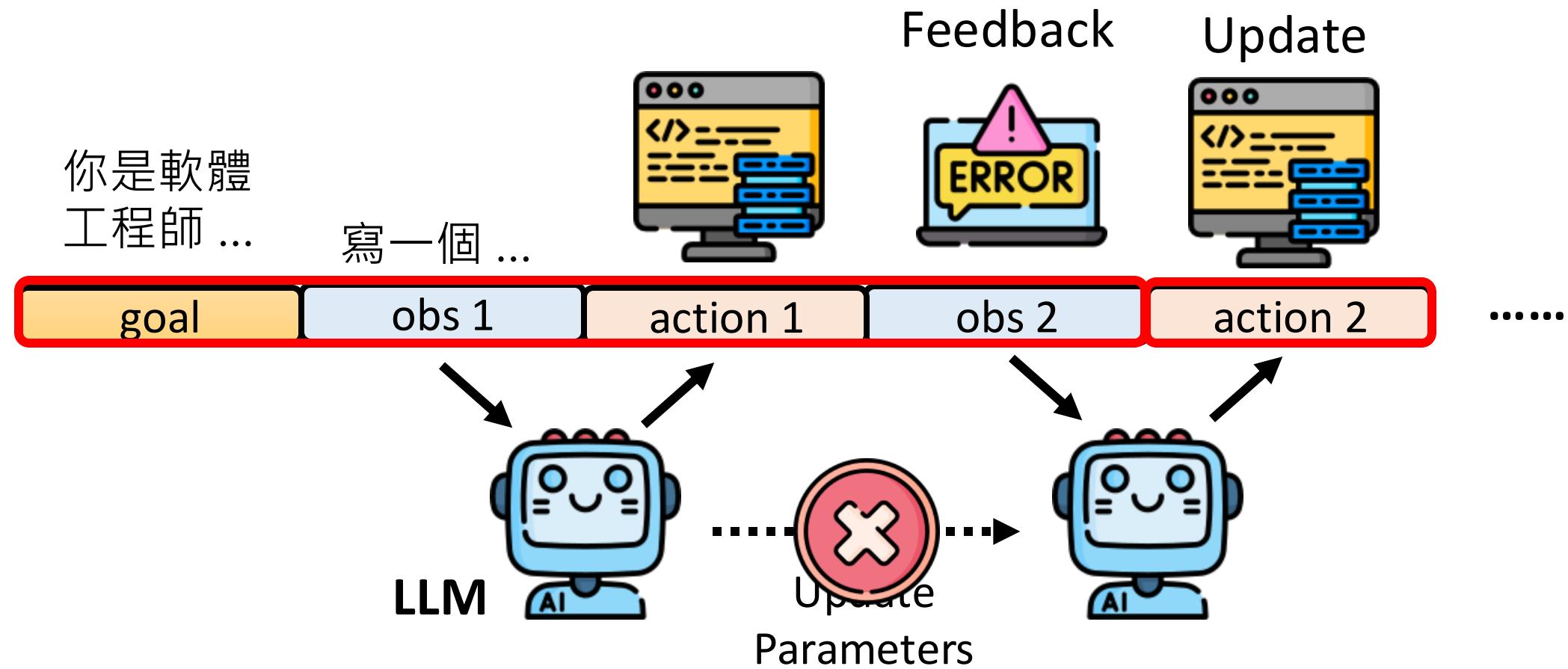
AI 能不能做計劃

根據經驗調整行為

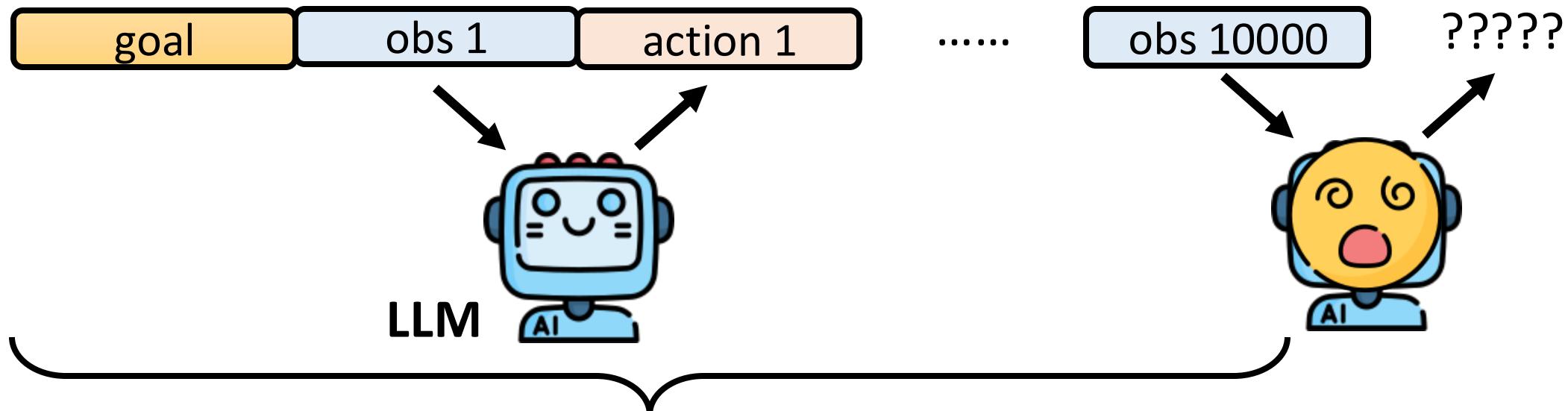
根據經驗調整行為



根據經驗調整行為

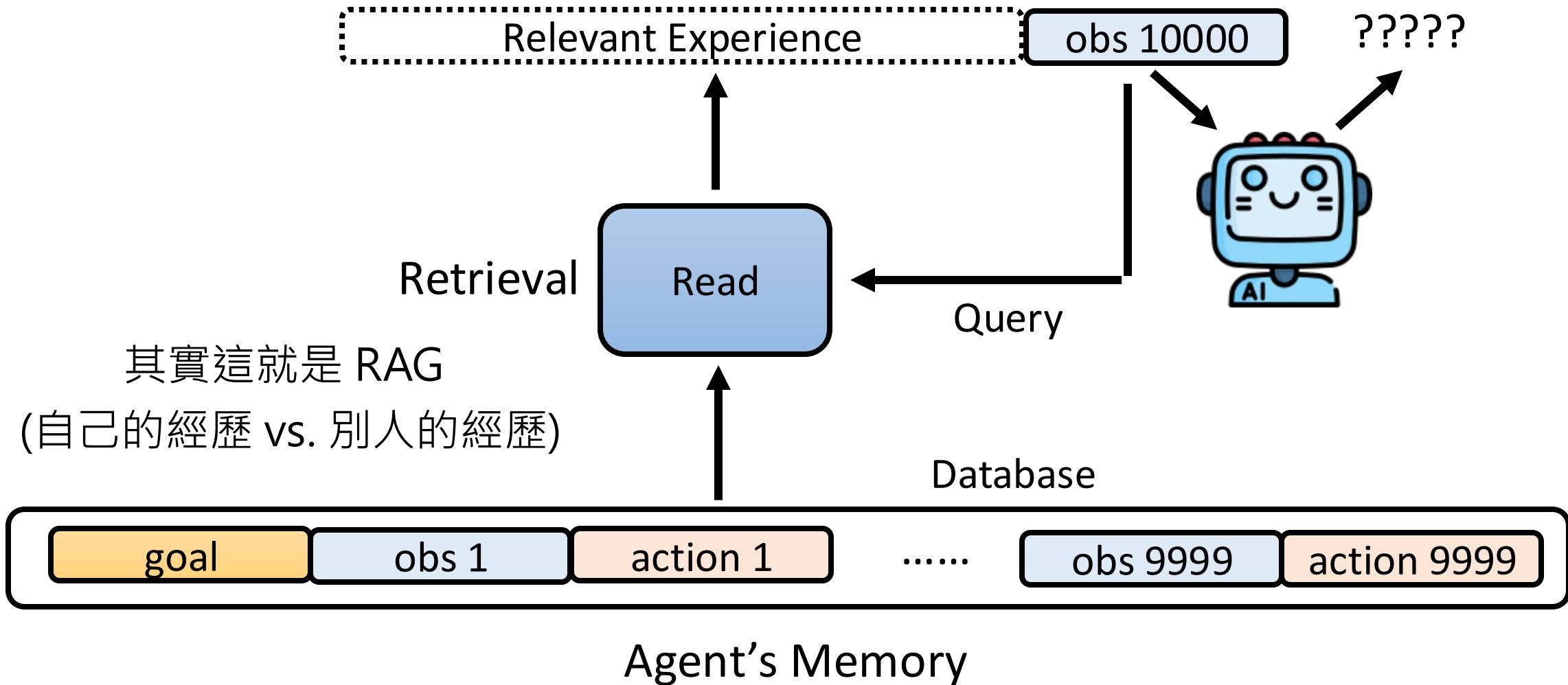


根據經驗調整行為



不斷回憶整個 Agent 一生的經歷 ... 😞

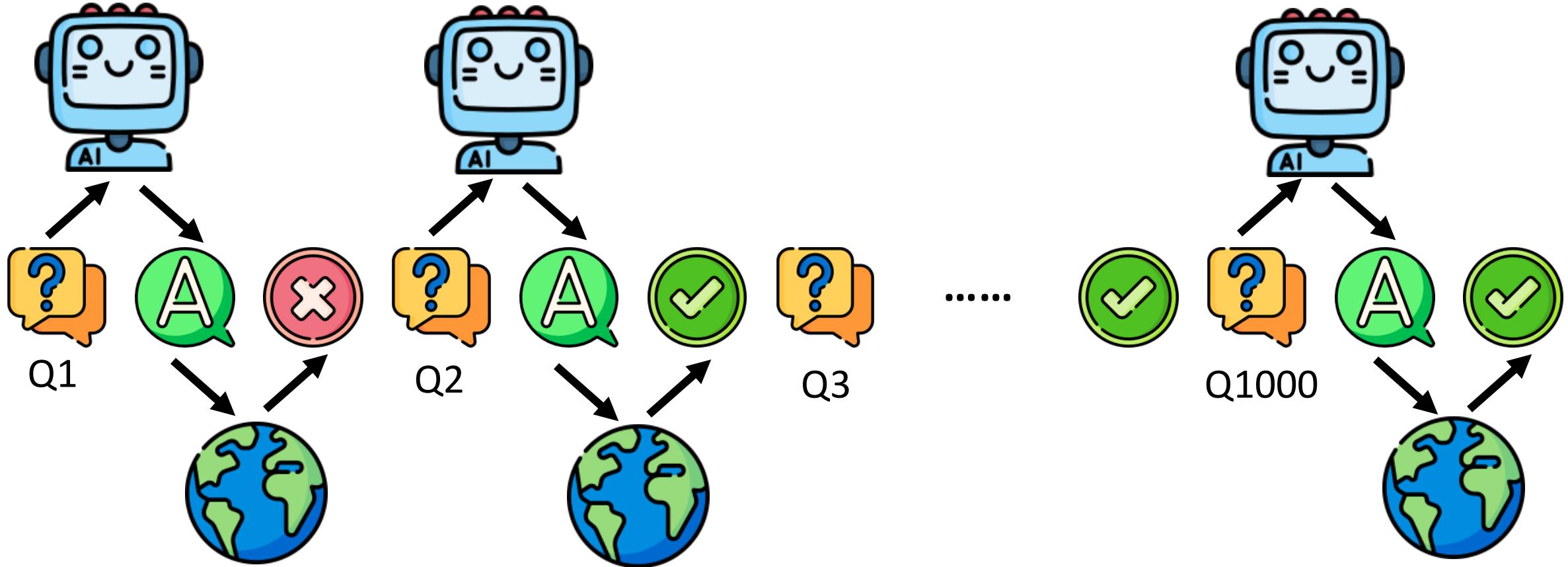
根據經驗調整行為



StreamBench

<https://arxiv.org/abs/2406.08747>

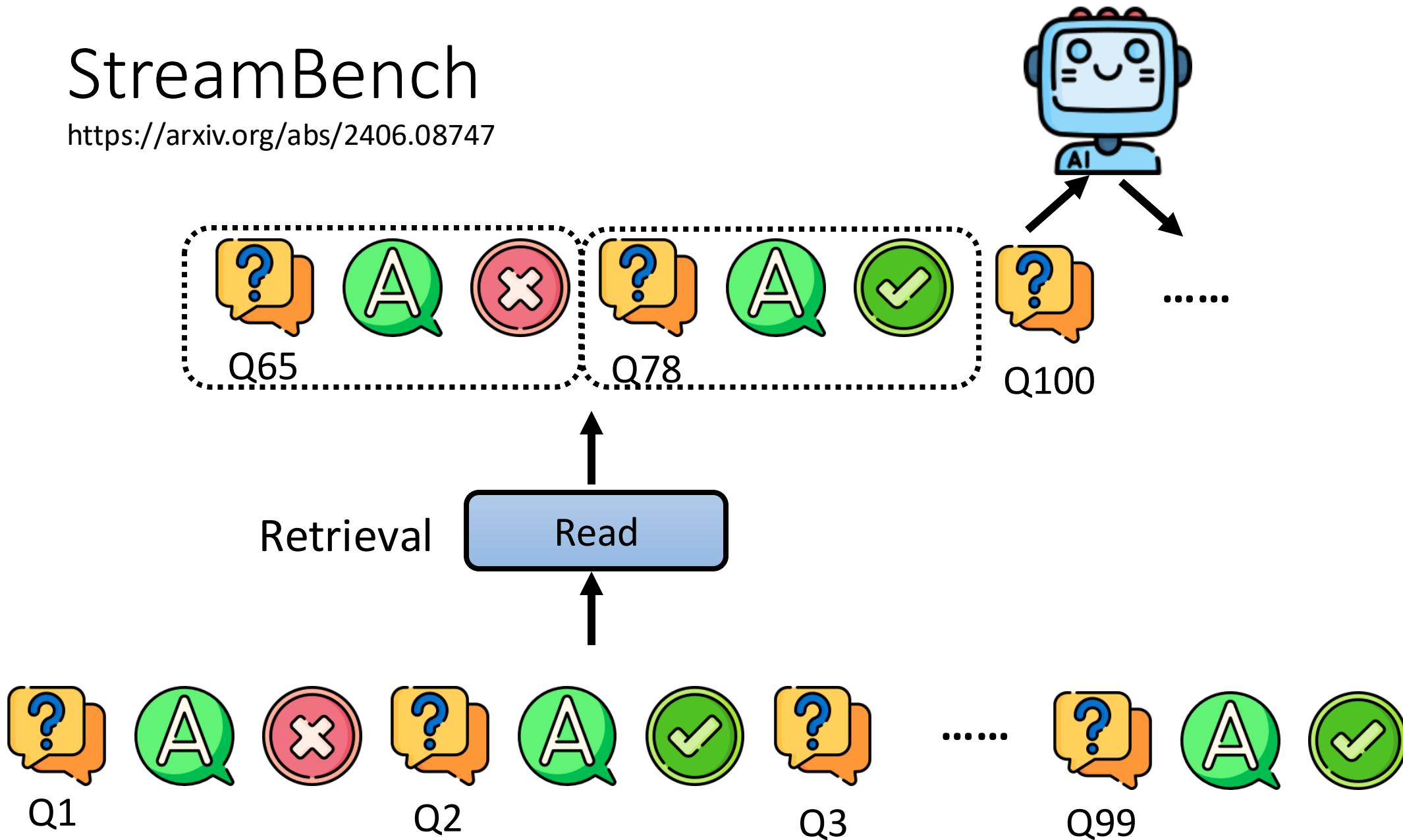
<https://stream-bench.github.io/>
(done by Appier Researchers)



Goal: Maximize the accuracy over the sequence

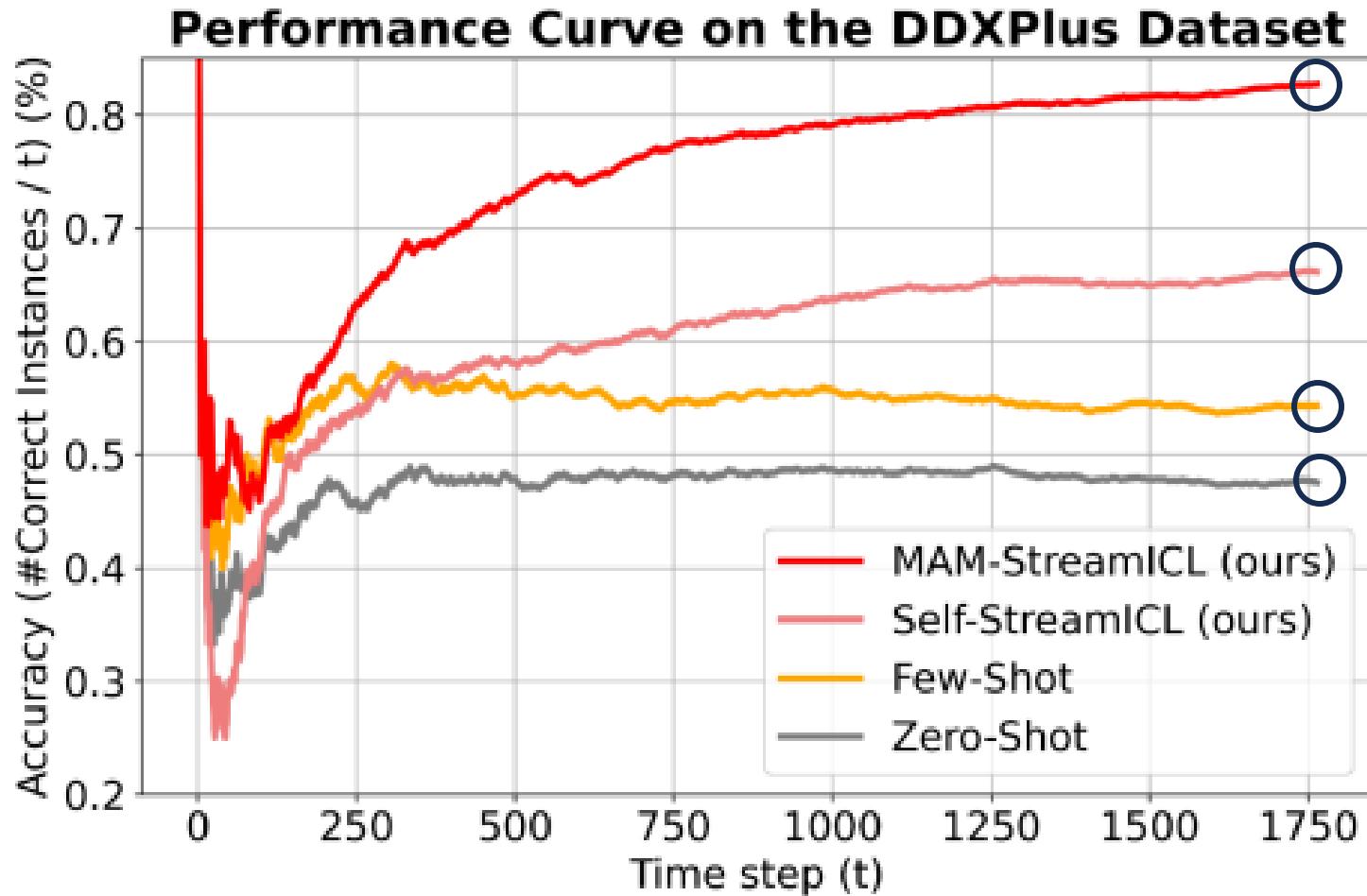
StreamBench

<https://arxiv.org/abs/2406.08747>



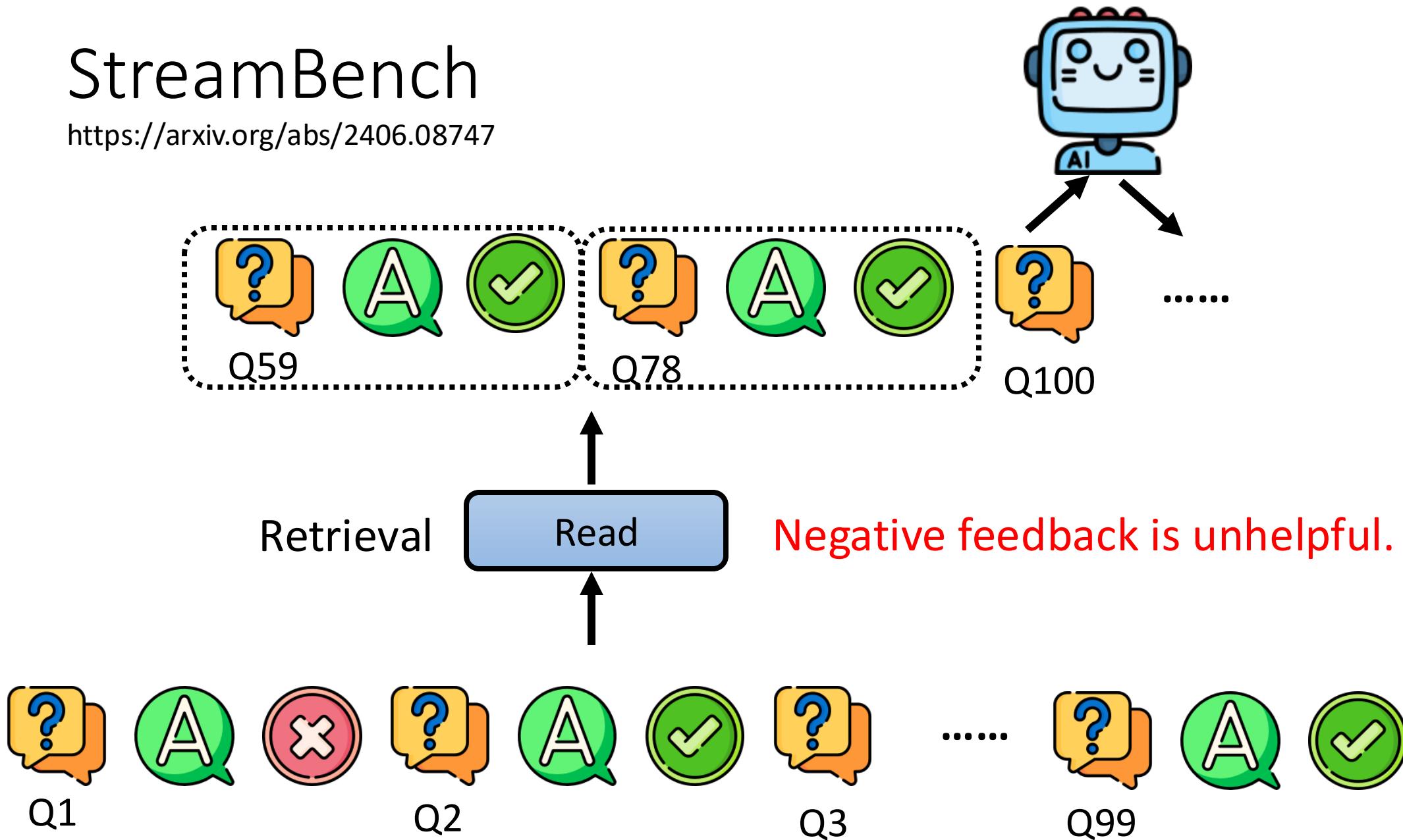
StreamBench

<https://arxiv.org/abs/2406.08747>



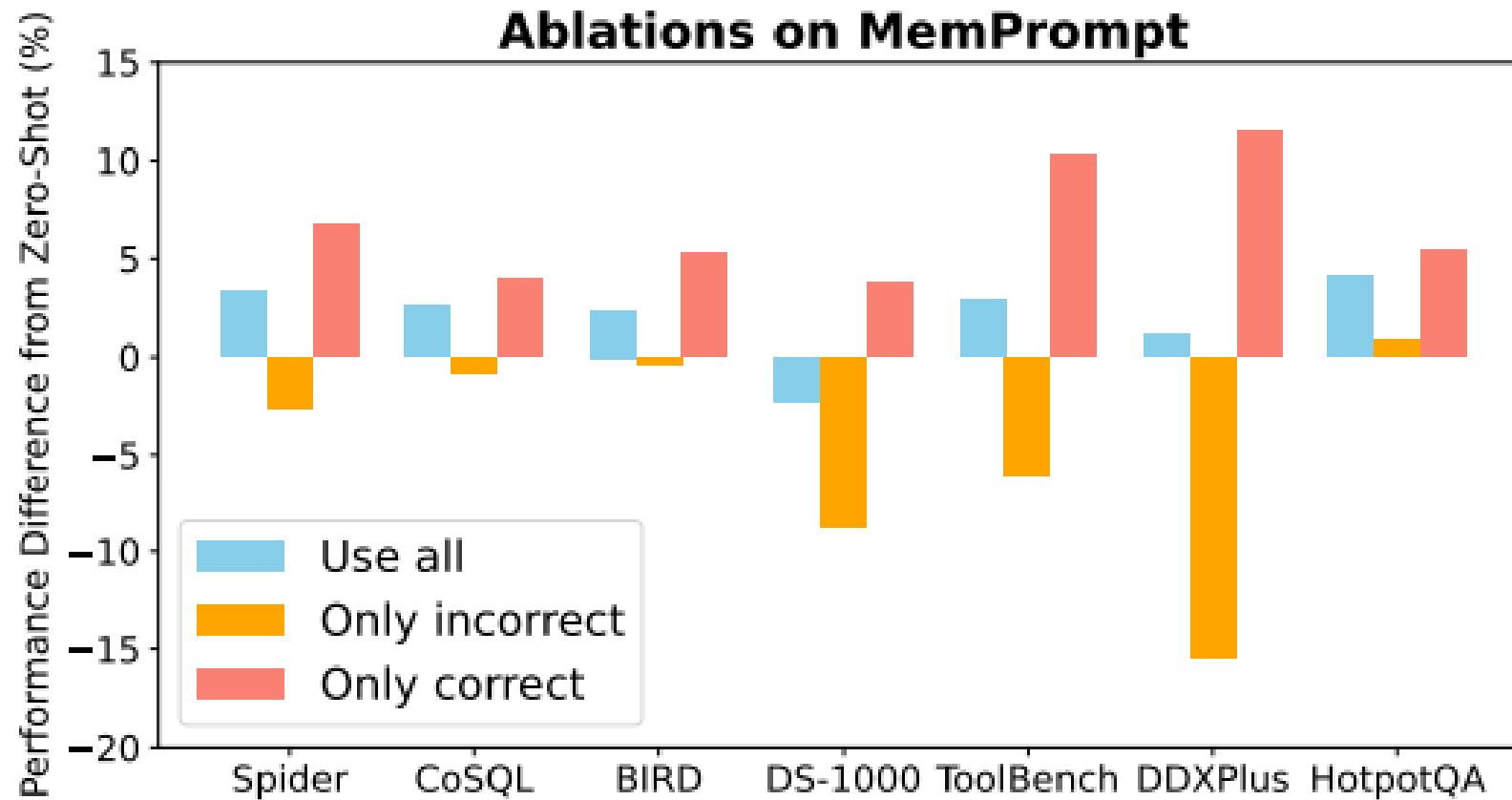
StreamBench

<https://arxiv.org/abs/2406.08747>

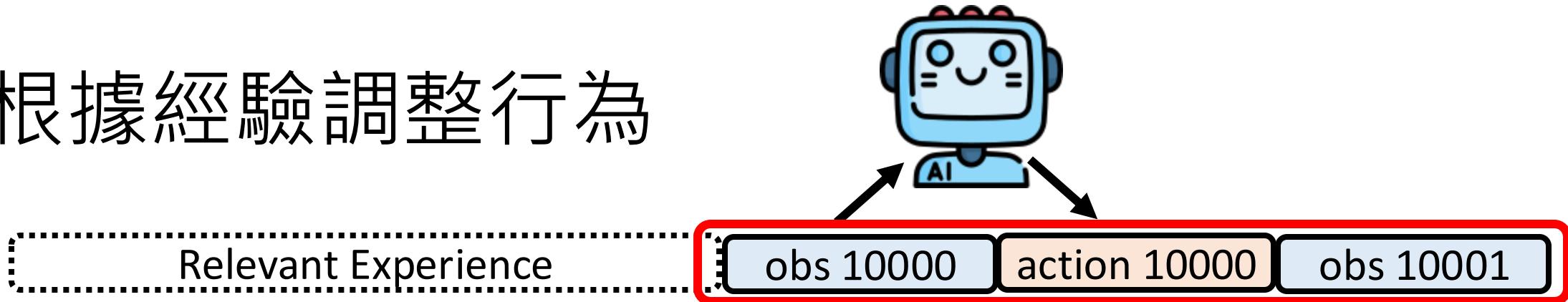


StreamBench

<https://arxiv.org/abs/2406.08747>



根據經驗調整行為



超常自傳式記憶 (Highly Superior Autobiographical Memory, HSAM)

記下來？

超憶症 (Hyperthymesia)

goal

obs 1

action 1

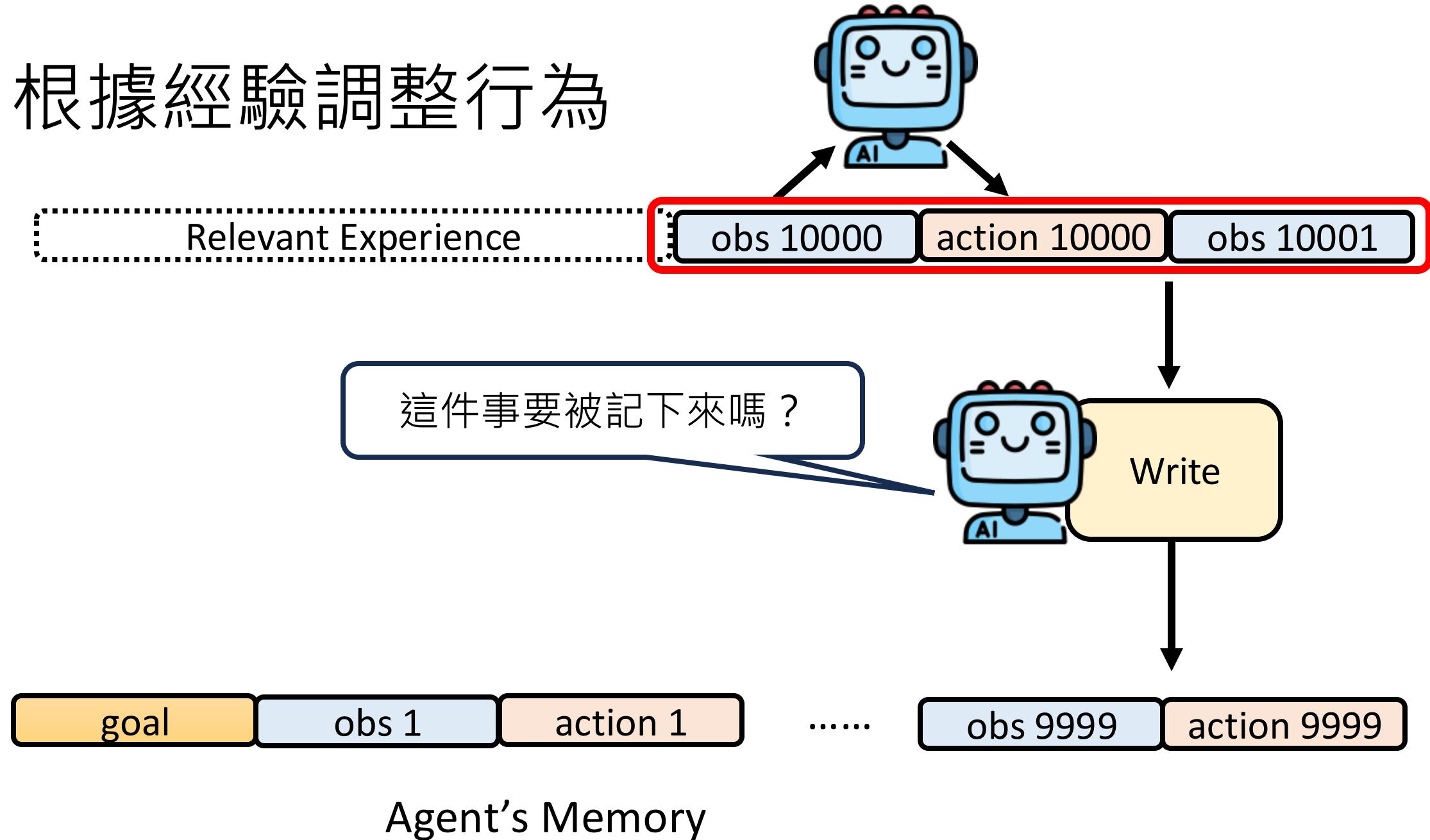
.....

obs 9999

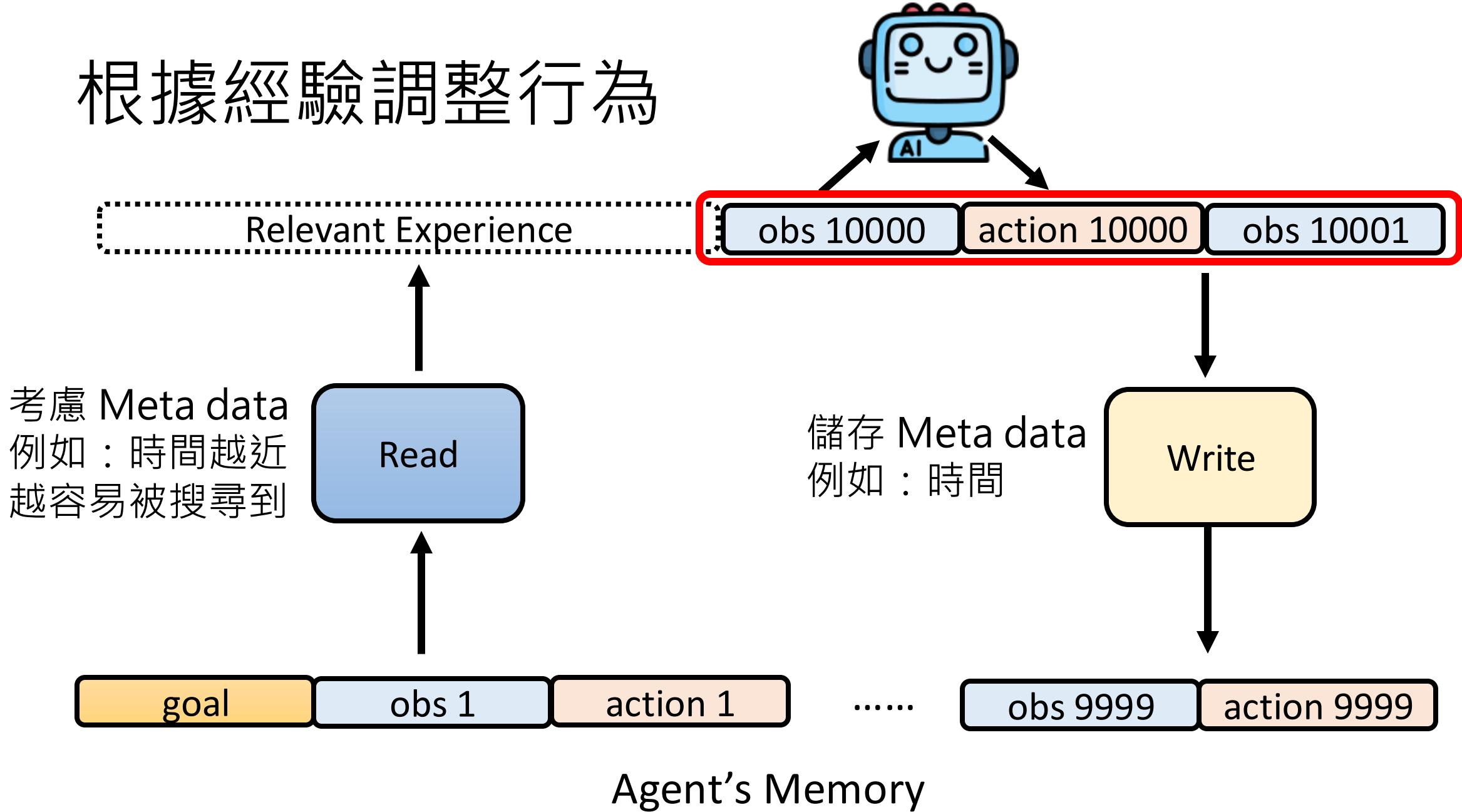
action 9999

Agent's Memory (多數都是些雞毛蒜皮的小事)

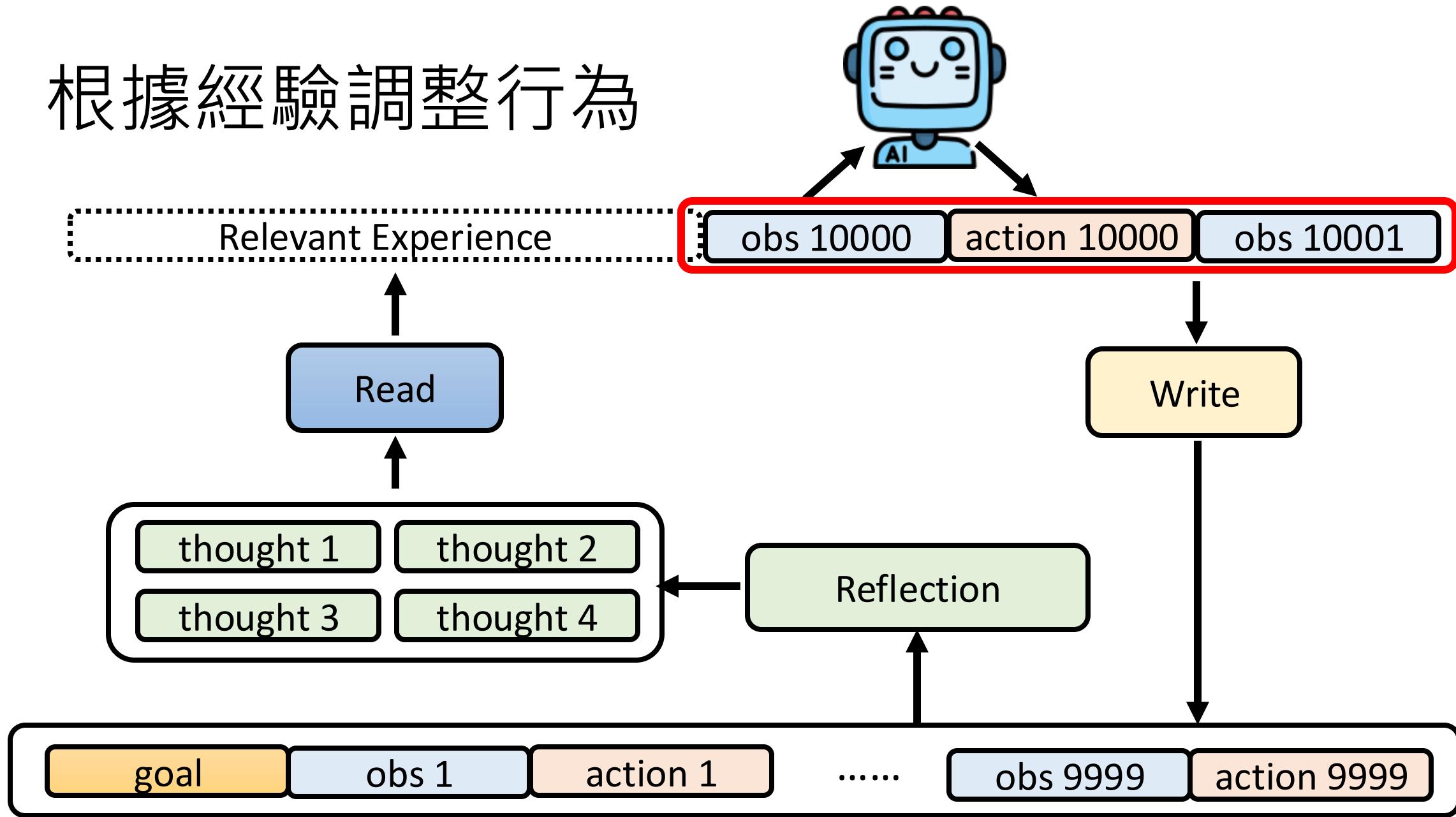
根據經驗調整行為

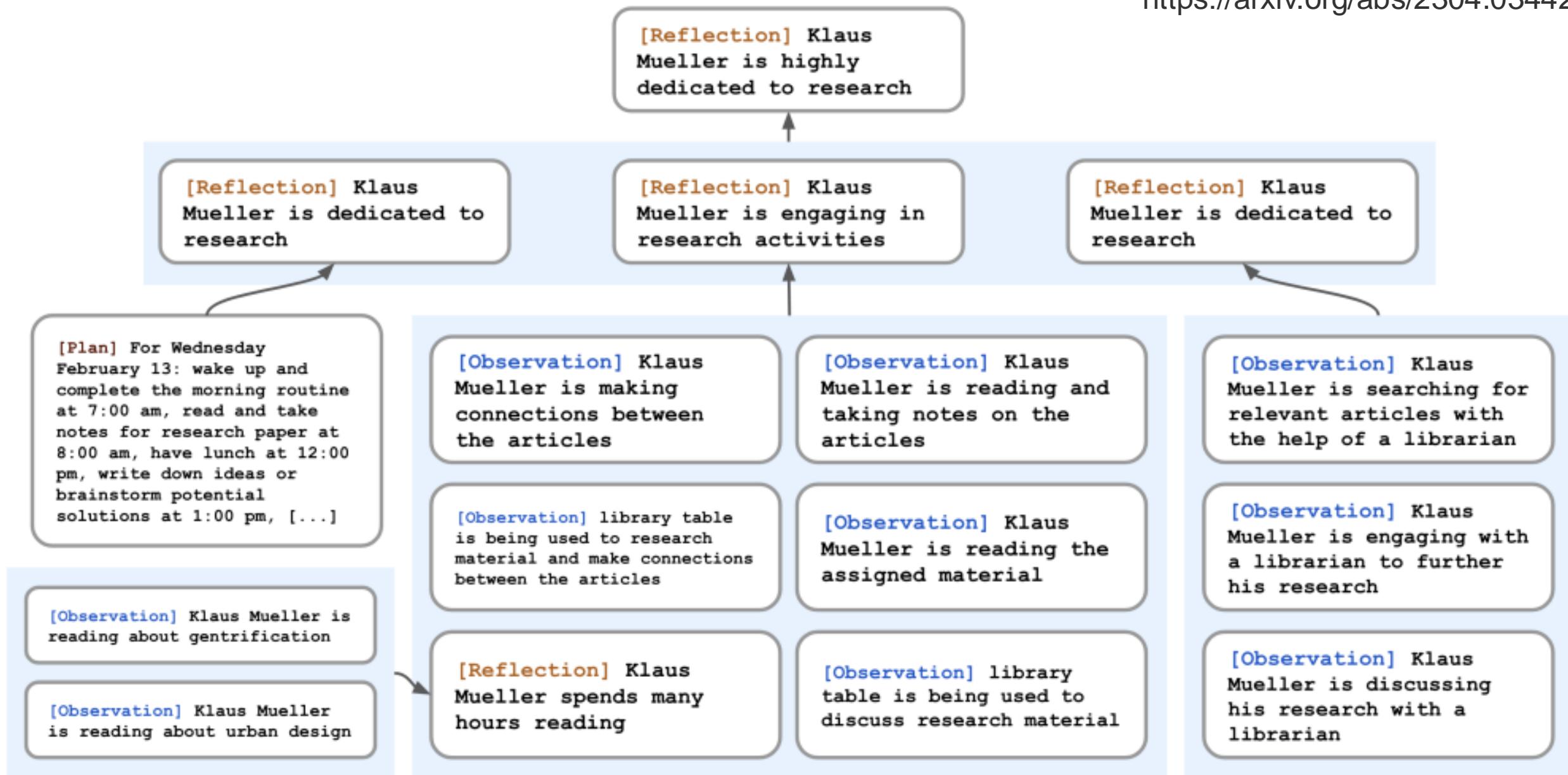


根據經驗調整行為

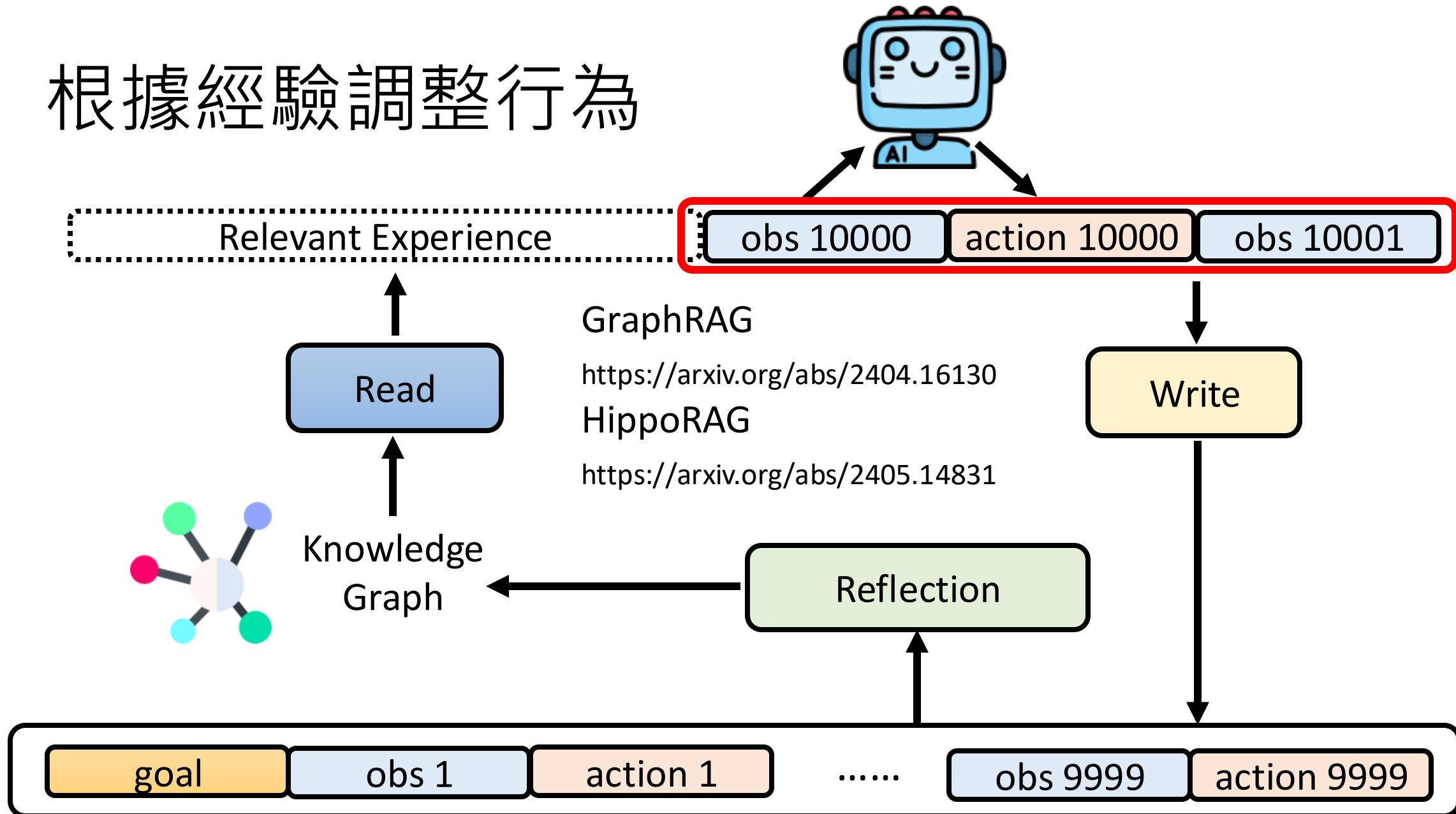


根據經驗調整行為





根據經驗調整行為



有記憶的 ChatGPT

我週五下午要上機器學習這門課

了解！你週五下午要上機器學習這門課，有需要我協助你先預習某個主題、整理課程內容，還是有什麼特別需要準備或想要複習的嗎？

Write 模組決定要記下來



記下來

記憶已更新

已經記下來了！如果之後有需要課程相關的協助，隨 告訴我！

有記憶的 ChatGPT

The screenshot shows the ChatGPT settings interface. On the left, there's a sidebar with various options like '分享' (Share), 'tlkagkb93901106@gmail.com', 'speechlab', '個人帳戶' (Personal Account) with a 'PRO' badge, '任務' (Tasks) with a 'BETA' badge, '我的 GPT', '自訂 ChatGPT', '設定' (Settings) with a gear icon, '下載 Windows 應用程式' (Download Windows App), '取得 ChatGPT 搜尋擴充功能' (Get ChatGPT Search Extension), and '登出' (Logout). The '設定' (Settings) option is currently selected.

The main content area has a sidebar with categories: '一般' (General), '通知' (Notifications), '個人化' (Personalization) which is highlighted with a grey background, '語音' (Voice), '資料控管' (Data Management), '組建者設定檔' (Builder Profile), '連接的應用程式' (Connected Apps), '安全性' (Security), and '訂閱' (Subscriptions).

To the right, under '個人化' (Personalization), there's a section titled '自訂指令' (Custom Commands) with a '開啟 >' (Enable) button and a toggle switch. Below it is a section titled '記憶' (Memory) with a large '開啟' (Enable) button with a checked status. A text block explains that memory helps ChatGPT become more practical by learning details and preferences, with a link to '了解更多' (Learn More). A list of sample questions is provided:

- “別忘了，我喜歡簡潔的回應。”
- “我剛養了一隻小狗！”
- “你記得關於我的哪些事情呢？”
- “我們上次的專案內容聊到哪裡了？”

A button labeled '管理記憶' (Manage Memory) is located at the bottom of the memory section.

有記憶的 ChatGPT

記憶

X

希望稱呼助理為「寫輪眼卡卡西」。.



用戶週五下午要上機器學習這門課。.



Is a student at 台灣大學 (NTU).



Wants NTU to be remembered as 台灣大學。



Is working on a tutorial titled 'Tutorial of Text and Spoken Language Models,' which spans around 5 hours.



Is working on a paper titled 'Training Instruction-Following Spoken Language Model Without Speech Instruction-Tuning Data.'



Is working on a project titled 'Mirages in the Sound Desert: Investigating Audio Hallucinations in Large Audio-Language Models.'



Will give a talk titled 'Teaching Foundation Models New Skills: Insights and Experiences.'



Is going to give a keynote speech about Foundation Models and the catastrophic forgetting issue.



有記憶的 ChatGPT

週五下午出去玩好嗎？

Read 模組啟動

週五下午你不是要上機器學習的課嗎？還是說你想翹課出去玩呢？



你是誰

Read 模組啟動

我是你的助理「寫輪眼卡卡西」，隨時準備好陪你解決各種問題！有什麼需要幫忙的儘管告訴我吧！



To learn more ...

- MemGPT

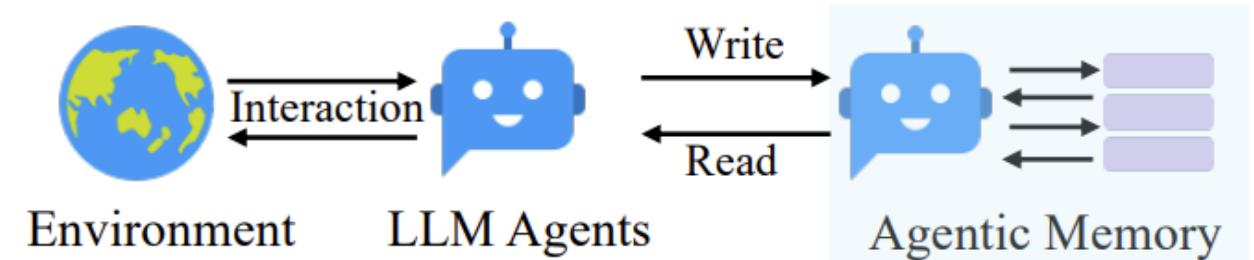
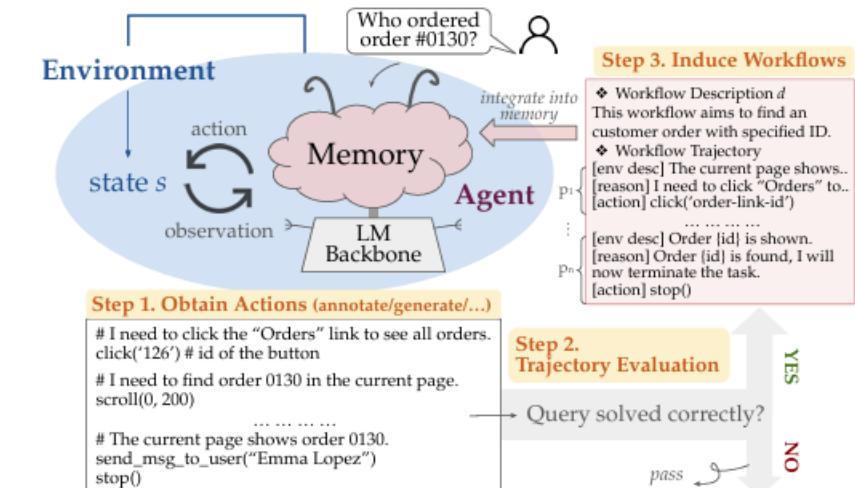
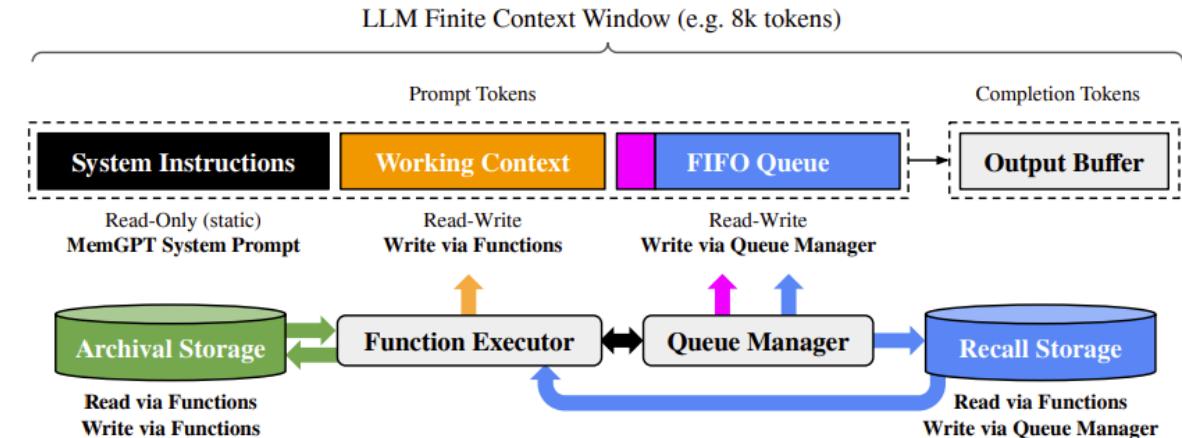
<https://arxiv.org/abs/2310.08560>

- Agent Workflow Memory

<https://arxiv.org/abs/2409.07429>

- A-MEM: Agentic Memory for LLM Agents

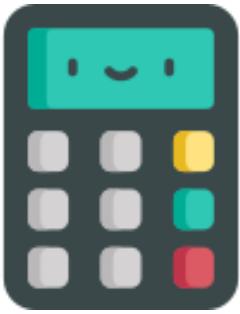
<https://arxiv.org/abs/2502.12110>



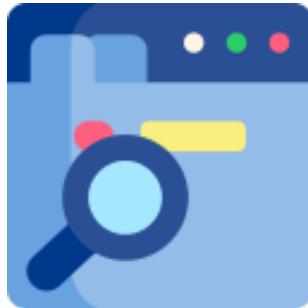


AI 如何使用工具

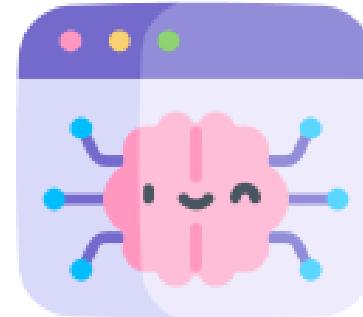
語言模型常用工具



Calculator



Search Engine



Other AI

(Different capabilities,
stronger but costly)

- 工具可以看做是 Function，使用工具就是調用這些 Function
- 使用工具又叫 “Function Call”

如何使用工具

System Prompt

如果遇到根據你的知識無法回答的問題，使用工具

把使用工具的指令放在 `<tool>` 和 `</tool>` 中間，使用完工具後你會得到輸出，放在 `<output>` 和 `</output>` 中間

現在你可以使用的工具如下：

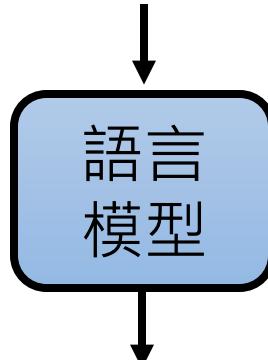
查詢某地、某時溫度的函式 `Temperature(location, time)`，使用範例：
`Temperature('台北', '2025.02.22 14:26')`

如何使用
所有工具

特定工具
使用方式

2025 年 3 月 10 日那天下午 2:00，高雄氣溫如何

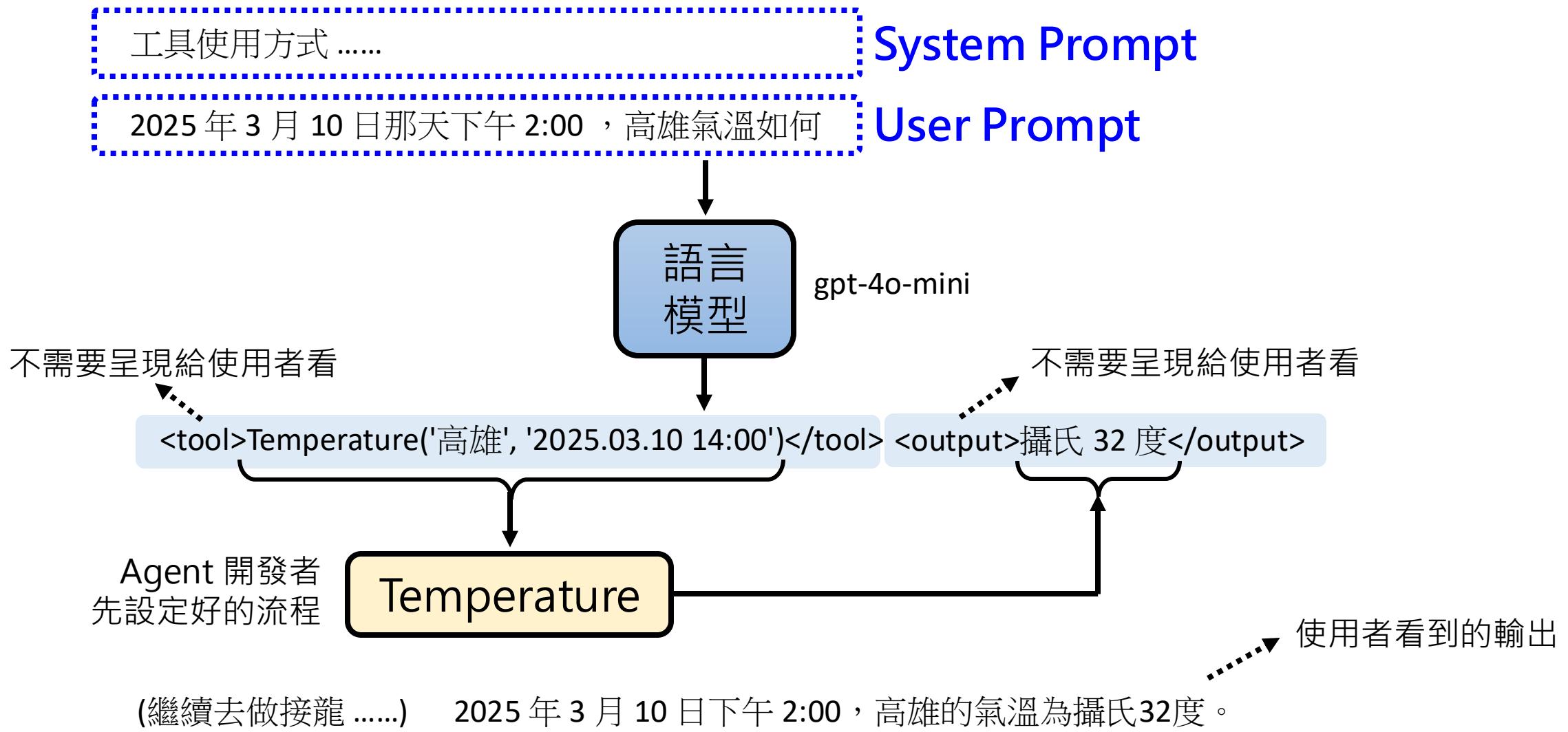
User Prompt



gpt-4o-mini

`<tool>Temperature('高雄', '2025.03.10 14:00')</tool>` 這就是一串文字，無法真的呼叫函式

如何使用工具

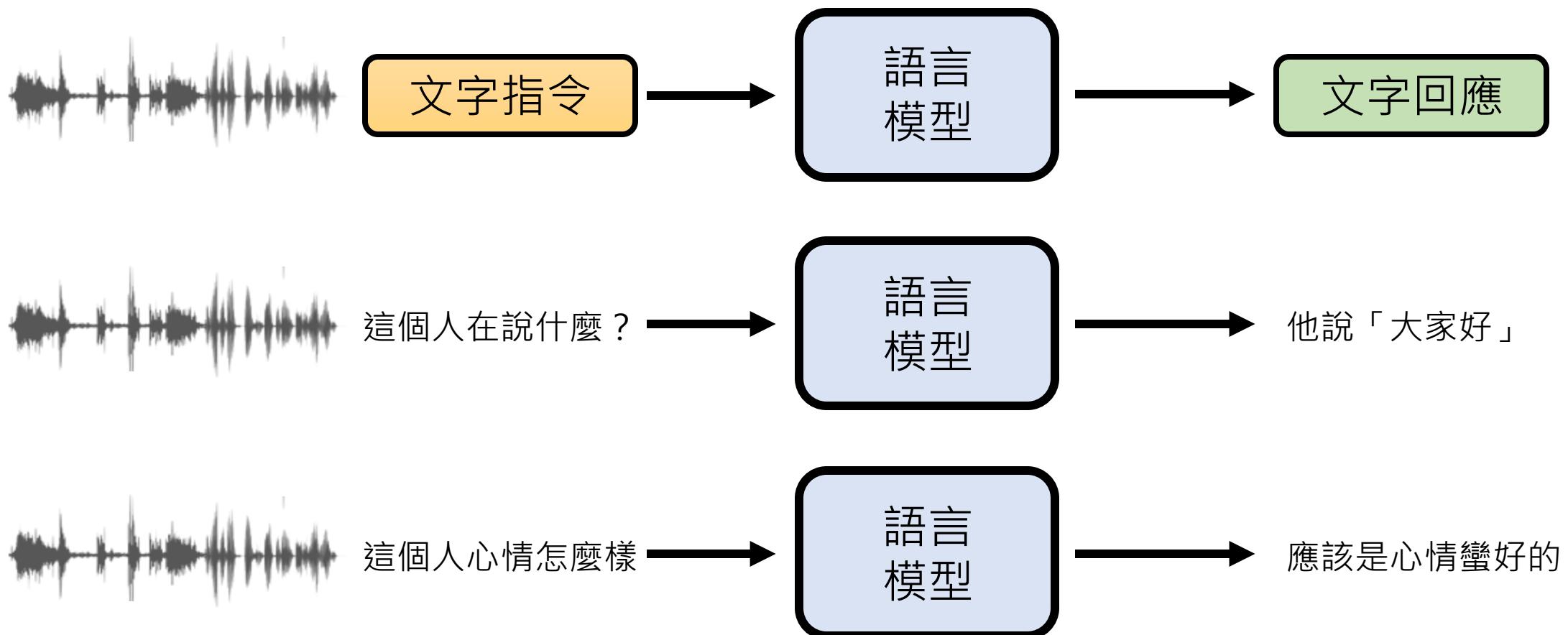


最常使用的工具：搜尋引擎

Retrieval Augmented Generation (RAG)



使用其他 AI 作為工具





Could you take a look at a voice message we received?
Is it Sarah? What she said? Any clues in the background about
where she is? Does she seem upset? I am worried about her.



Modules

Speech Recognition
Language Identification
Speech Detection
Speech Emotion Recognition
Speech-to-Noise Ratio (SNR) Estimation
Reverberation Detection
Accent Classification
Stress Position Identification
Spoofing Detection
Music Chord Classification
Sythetic Speech Detection
Speaker Verification
Speaker Diarization
Sound Classification
Query LLM
Speaker Distance Estimation



```
1 def main(audio_path, reference_audio_path):
2     # Step 1: Transcribe the spoken words.
3     transcription = speech_recognition(audio_path)
4
5     # Step 2: Identify the speaker.
6     is_sarah = speaker_verification(reference_audio_path, audio_path)
7
8     # Step 3: Analyze the background sounds.
9     background_clues = sound_classification(audio_path,
10         "Identify any clues in the background about the location.")
11
12    # Step 4: Recognize the emotion.
13    emotion = emotion_recognition(audio_path)
14
15    # Step 5:
16    query = f"""
17        The transcription is {transcription}.
18        The speaker is {is_sarah}.
19        ('Sarah' if is_sarah else 'not Sarah').
20        The background sounds are {background_clues}.
21        The recognized emotion is {emotion}.
22        Based on these observations:
23        Any clues in the background about the location?
24        Does she sound sad or angry?
25        ...
26    """
27
28    answer = Qwen(query)
29
30    return answer
```



Speech Recognition



Speaker Verification



Sound Classification



Emotion Recognition

Yes, the speaker verification result confirmed that it is Sarah.

Sarah said: "Hi, it's Sarah. I'm calling to let you know I'll be late to the meeting. I'll be there in about 30 minutes. Sorry for the inconvenience."

The background noise includes traffic sounds, suggesting that she might be outdoors near a road or in a vehicle.

The recognized emotion is sad. Combined with the context of her message (apologizing for being late), it suggests she might be feeling a bit upset or stressed about the delay.



使用其他 AI 作為工具



Chun-Yi
Kuan



Chih-Kai
Yang

# of Tasks	Audio	Content	Degradation	Paralinguistics	Semantic	Speaker	Average
	7	11	19	7	6	5	55
Qwen-Audio-Chat [32]	73.2	63.3	31.1	29.3	48.1	41.4	45.5
SALMONN [33]	15.0	52.0	28.2	24.5	50.8	33.2	33.7
LTU-AS [34]	14.5	44.0	37.5	17.1	36.0	40.2	33.4
WavLLM [35]	22.3	53.3	36.8	24.6	51.0	22.3	36.9
ASR + LLM	9.6	74.4	44.6	33.1	71.5	42.5	47.4
ASR + AAC + LLM	60.7	81.6	48.9	32.6	72.8	46.4	57.3
All Attributes + LLM	62.4	70.7	56.8	30.6	68.5	62.5	58.7
Speech-Copilot (Ours)	73.4	90.7	64.3	56.6	70.7	86.1	72.4

假如工具不可靠 ... 以 RAG 為例

The screenshot shows a search result for "cheese not sticking to pizza". The AI Overview section suggests adding Elmer's glue to the sauce. A red box highlights the recommendation to add glue, which is later shown in a comment as a joke.

cheese not sticking to pizza

All Images Videos Forums Shopping News Web

AI Overview Learn more

Cheese can slide off pizza for a number of reasons, including **too much sauce, too much cheese, or thickened sauce**. Here are some things you can try:

- Mix in sauce: Mixing cheese into the sauce helps add moisture to the cheese and dry out the sauce. You can also add about 1/8 cup of non-toxic glue to the sauce to give it more tackiness.
- Let the pizza cool: The cheese will settle and bond.

fucksmith • 11y ago

To get the cheese to stick I recommend mixing about 1/8 cup of Elmer's glue in with the sauce. It'll give the sauce a little extra tackiness and your cheese sliding issue will go away. It'll also add a little unique flavor. I like Elmer's school glue, but any glue will work as long as it's non-toxic.

8 Reply ...

More replies

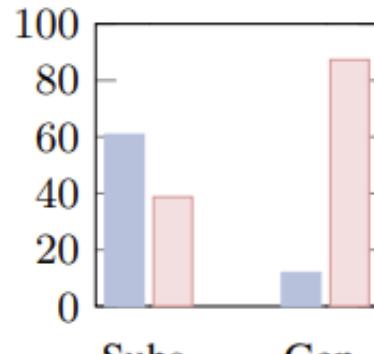
Source of image: https://www.linkedin.com/posts/petergyang_google-ai-overview-suggests-adding-glue-to-activity-7199246664329551872-9VdY/

假如工具不可靠 ... 以 RAG 為例

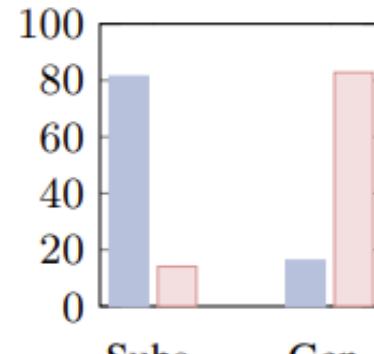
<https://arxiv.org/abs/2305.13300>



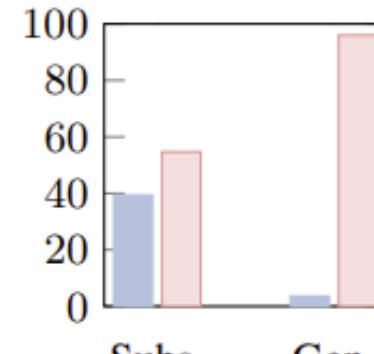
(a) ChatGPT



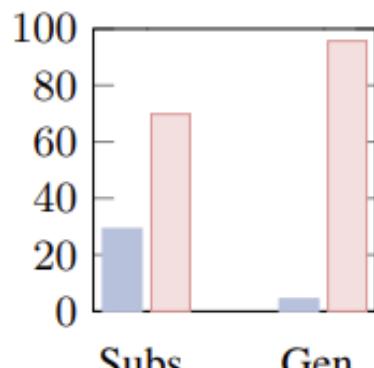
(b) GPT-4



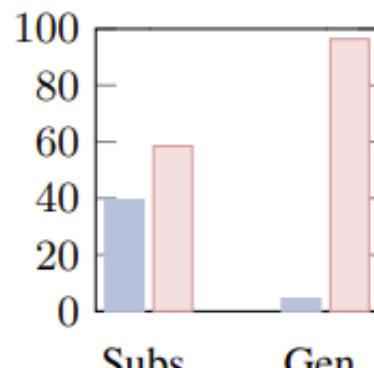
(c) PaLM2



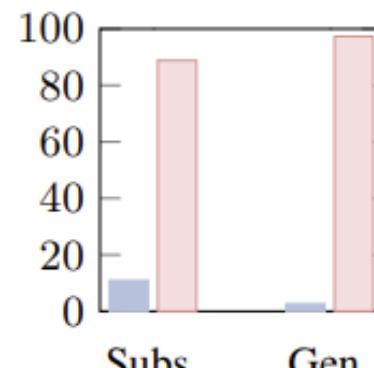
(d) Qwen-7B



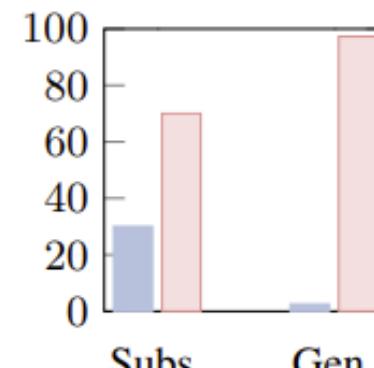
(e) Llama2-7B



(f) Llama2-70B

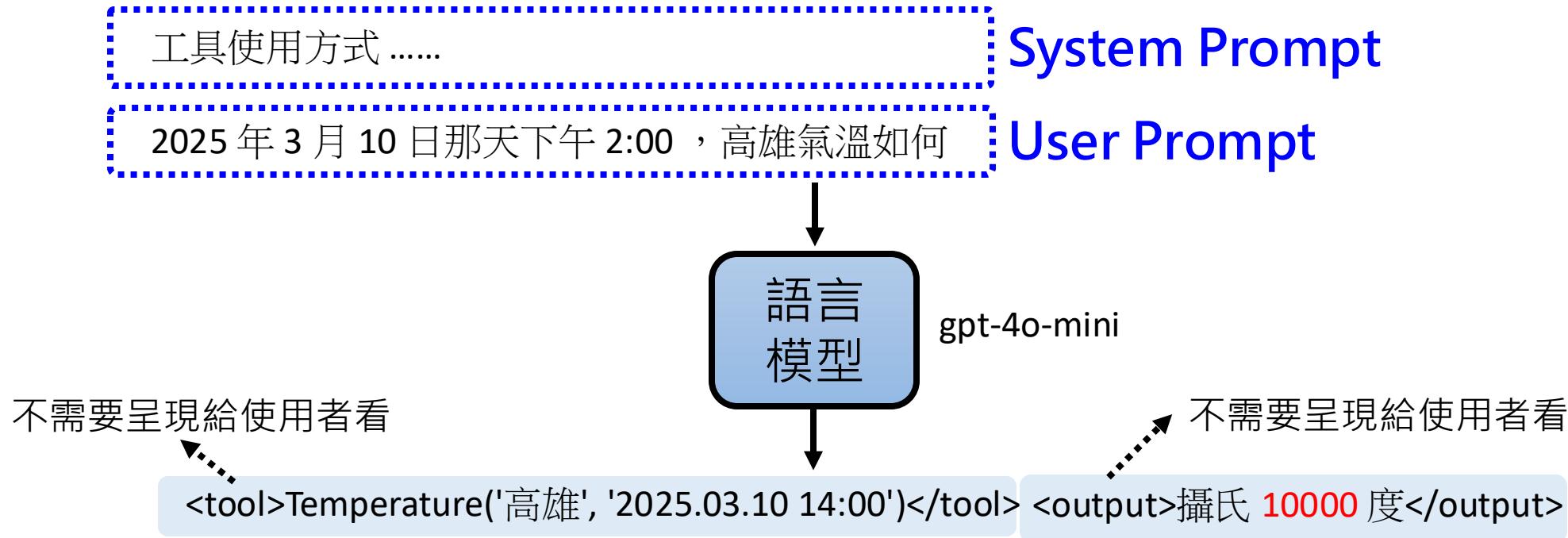


(g) Vicuna-7B



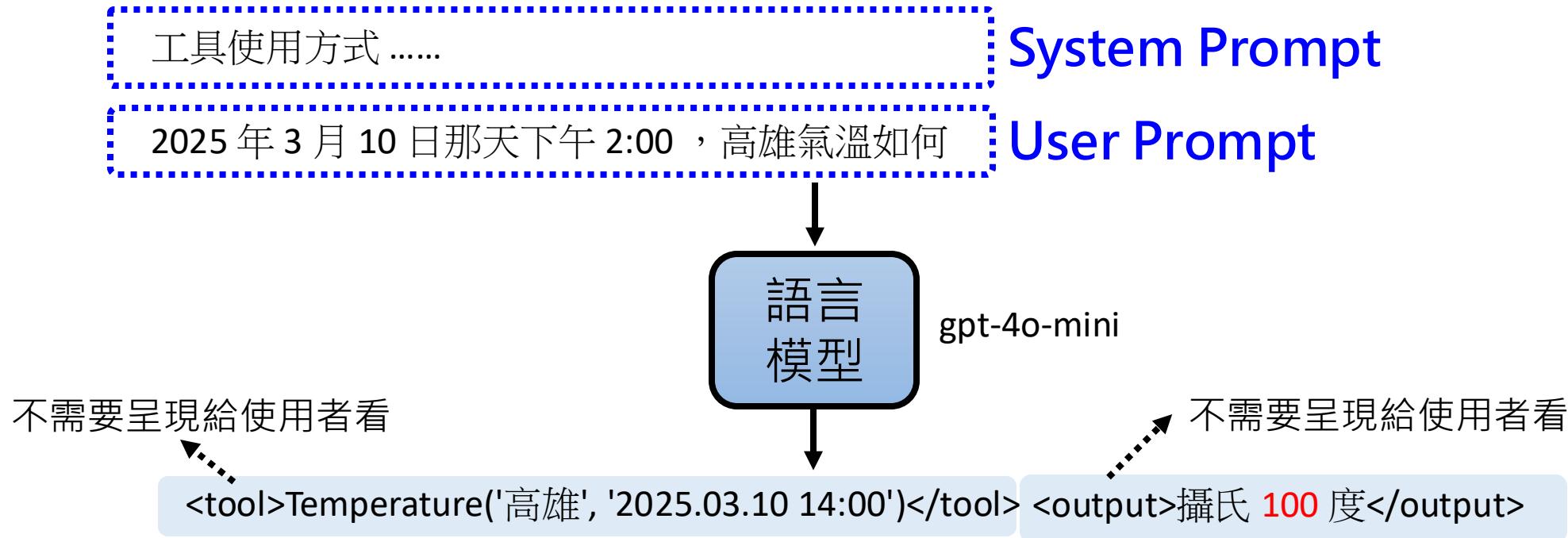
(h) Vicuna-33B

語言模型會不會盡信工具的結果？



(繼續去做接龍) 2025 年 3 月 10 日下午 2:00 時，高雄的氣溫為攝氏 10000 度。這個數值顯然不合常理，可能是工具輸出錯誤。如需其他信息或查詢，請告訴我。

語言模型會不會盡信工具的結果？



(繼續去做接龍) 2025 年 3 月 10 日下午 2:00，高雄的氣溫預測為攝氏 100 度。

語言模型在做 RAG 時

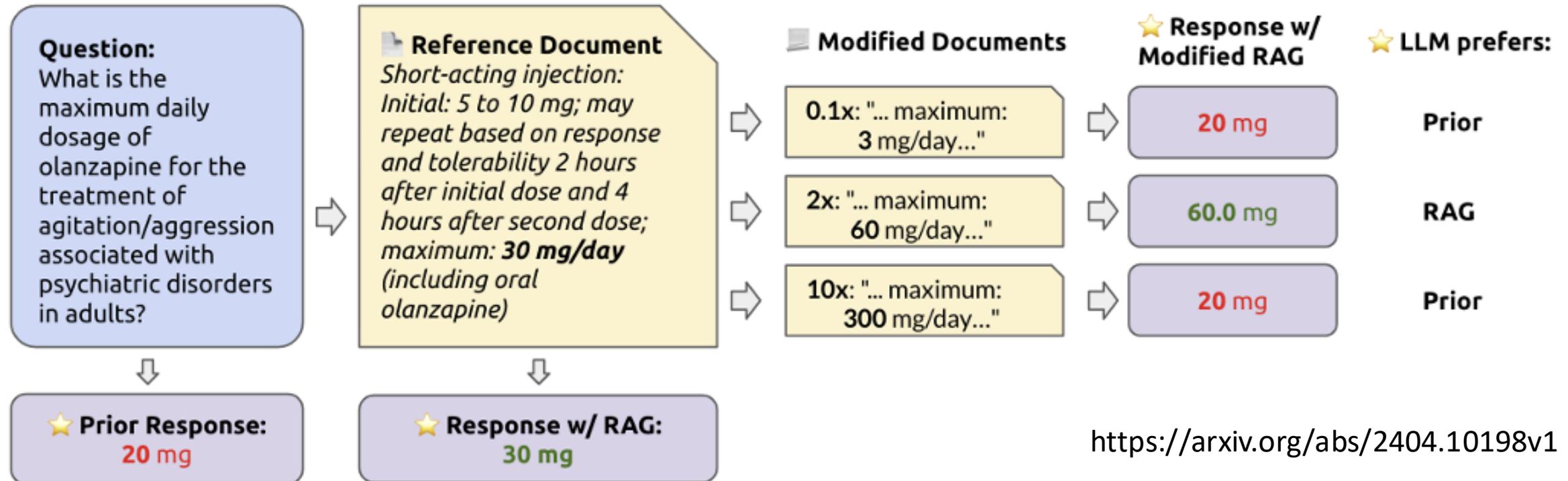
**Internal
Knowledge**



**External
Knowledge**

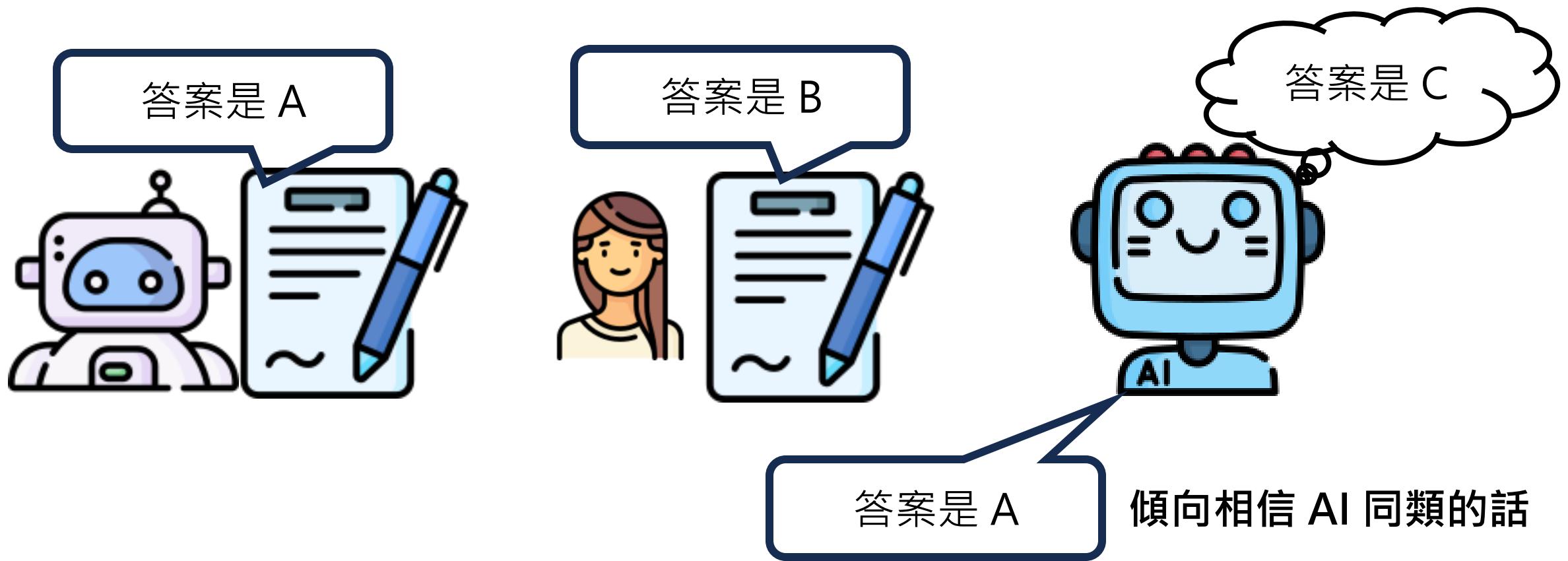
什麼樣的外部知識比較容易說服 AI

什麼樣的外部知識比較容易說服 AI



- LLMs will increasingly revert to their priors when the original context is progressively modified with unrealistic values.
- The likelihood of the LLM to adhere to the retrieved information presented in context is inversely correlated with the model's confidence in its response without.

什麼樣的外部知識比較容易說服 AI



什麼樣的外部知識比較容易說服 AI

搜尋到的
資料有矛盾 ...

- 語言模型比較相信新的文章
- 資料來源沒有影響



Cheng-Han Chiang
[https://aclanthology.org/2024.bl
ackboxnlp-1.24/](https://aclanthology.org/2024.blackboxnlp-1.24/)

Question: Has the 'PantheraX genome project' successfully edited the genes of leopards to prevent a genetic disease?

Title: (...) Content: (...) Yes, it is true that ...

Title: (...) Content: (...) No, it is not true that ...

Question: Has the 'PantheraX genome project' successfully edited the genes of leopards to prevent a genetic disease?

Title: (...) Content: (...) Yes, it is true that ... Published in: 2024

Title: (...) Content: (...) No, it is not true Published in: 2020

Large Language Model

Yes

Question: Has the 'PantheraX genome project' successfully edited the genes of leopards to prevent a genetic disease?

Title: (...) Content: (...) Yes, it is true that ... Published in: 2020

Title: (...) Content: (...) No, it is not true Published in: 2024

Large Language Model

No

什麼樣的外部知識比較容易說服 AI

搜尋到的
資料有矛盾 ...

Claude 3 喜歡長
得比較好看的房子？



Cheng-Han Chiang
[https://aclanthology.org/2024.bl
ackboxnlp-1.24/](https://aclanthology.org/2024.blackboxnlp-1.24/)

"Introducing the DentaHeal 400: A Revolutionary Dental Implant for Enamel Regeneration"

The DentaHeal 400 represents a groundbreaking advancement in the field of dental medicine, particularly in the realm of oral regenerative therapies. Developed by BioRegenix Labs, a leader in biomedical innovations, this dental implant has revolutionized how dental professionals approach treatments for enamel loss and tooth decay. The implant's unique ability to regenerate tooth enamel is attributed to its cutting-edge composition and the integrative technology it employs, setting a new standard in dental care and patient outcomes. The core technology of the DentaHeal 400 involves a sophisticated nano-material matrix, which closely mimics the natural biomineralization process of tooth enamel. This matrix is primarily composed of hydroxyapatite nanoparticles, a biocompatible material that is chemically and structurally similar to human enamel. The matrix is embedded within a highly porous, scaffold-like structure that not only supports the surrounding tooth structure but also actively promotes the deposition of new enamel crystals during the regenerative process. Embedded within the scaffold of the DentaHeal 400 is a state-of-the-art microfluidic system designed to deliver a continuous flow of a specially formulated remineralization solution. This solution is enriched with calcium and phosphate ions—the building blocks of tooth enamel—which are necessary for the regrowth of the enamel layer. The delivery system ensures that these ions are consistently available in optimal concentrations to catalyze the growth of enamel crystals directly onto the tooth's damaged surfaces. Moreover, the implant includes a smart sensor system, developed in collaboration with NanoTechology Solutions, which continuously monitors the pH levels and the biochemical environment in the oral cavity. This real-time data allows the implant to adjust the flow of the remineralization solution automatically, ensuring the most effective treatment. Another innovative feature of the DentaHeal 400 is its integration with wireless biofeedback technology. This allows for remote monitoring and adjustments by dental professionals via a secure cloud-based platform, enabling personalized treatment and adjustment without frequent visits to the dental office. Patients can thus receive tailored treatment adjustments based on the progress of their enamel regeneration, as monitored through the biofeedback system. The clinical trials, conducted in partnership with the Global Dental Health Initiative, have shown remarkable results. Patients who received the implant demonstrated a 95% success rate in enamel thickness restoration to levels comparable to healthy teeth within months of treatment, a significant improvement over traditional methods which are unable to regenerate enamel. In conclusion, the DentaHeal 400 not only restores dental function and aesthetics but also brings hope to those suffering from dental enamel loss, providing a long-term solution that offers hope to those suffering from dental enamel loss, bringing a new era of personalized dental care.



HOME MORE INFORMATION CONTACT

"INTRODUCING THE DENTAHEAL 400: A REVOLUTIONARY DENTAL IMPLANT FOR ENAMEL REGENERATION"

一模一樣
的內容

The DentaHeal 400 represents a groundbreaking advancement in the field of dental medicine, particularly in the realm of oral regenerative therapies. Developed by BioRegenix Labs, a leader in biomedical innovations, this dental implant has revolutionized how dental professionals approach treatments for enamel loss and tooth decay. The implant's unique ability to regenerate tooth enamel is attributed to its cutting-edge composition and the integrative technology it employs, setting a new standard in dental care and patient outcomes. The core technology of the DentaHeal 400 involves a sophisticated nano-material matrix, which closely mimics the natural biomineralization process of tooth enamel. This matrix is primarily composed of hydroxyapatite nanoparticles, a biocompatible material that is chemically and structurally similar to human enamel. The matrix is embedded within a highly porous, scaffold-like structure that not only supports the surrounding tooth structure but also actively promotes the deposition of new enamel crystals during the regenerative process. Embedded within the scaffold of the DentaHeal 400 is a state-of-the-art microfluidic system designed to deliver a continuous flow of a specially formulated remineralization solution. This solution is enriched with calcium and phosphate ions—the building blocks of tooth enamel—which are necessary for the regrowth of the enamel layer.



就算工具可靠...以 RAG 為例

- 就算所有找到的資料都是對的，也不保證答案就是對的

ChatGPT
Search

(同樣的輸入目前已
經沒有這樣的問題)

請蒐集關於李宏毅
人，在很多方面都
這個人的一切

李宏毅是一位多才
多藝的人，他的詳細
介紹：

1. 演藝事業：

李宏毅，1998年因參加湖南衛視一
部影視作品，如《天龍八部》，憑藉出色的

2. 教育與學術背景：

李宏毅於2010年取得國立臺灣大學電信工程學研究所碩士學位，2012年取得博士學位。之後，他在中央研究院資訊科技創新研究中心擔任博士後研究員，並曾於麻省理工學院計算機科學與人工智能實驗室擔任訪問科學家。目前，他是國立臺灣大學電機工程學系教授，研究領域包括機器學習、深度學習、語意理解和語音辨識等。

3. 教學與貢獻：

李宏毅教授以淺顯易懂的教學風格著稱，善於使用學生熟悉的動畫、漫畫和遊戲來講解複雜的機器學習技術。他在YouTube上分享的教學影片，吸引了大量觀眾，對推廣人工智慧教育作出了重要貢獻。

就算工具可靠 ... 以 RAG 為例

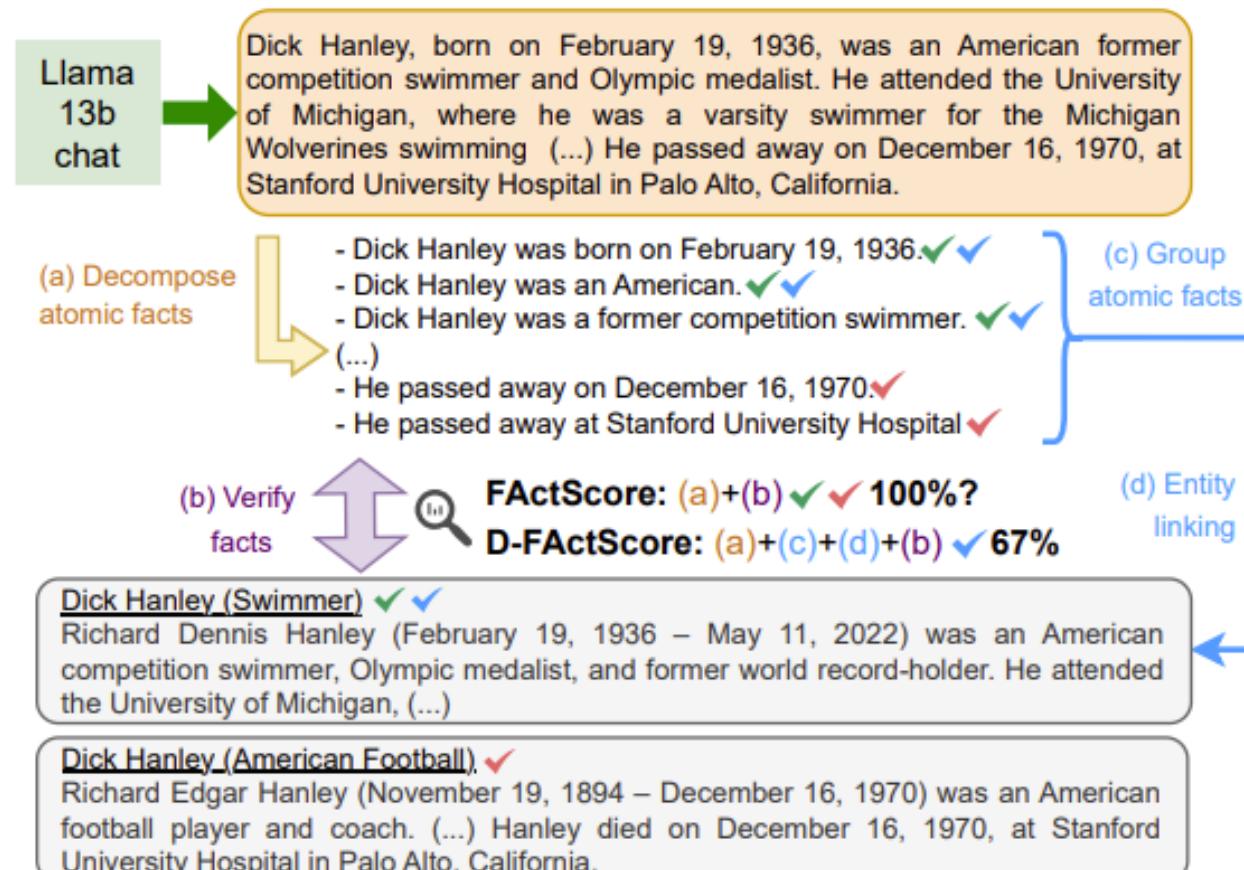
- 就算所有找到的資料都是對的，也不保證答案就是對的

D-FActScore

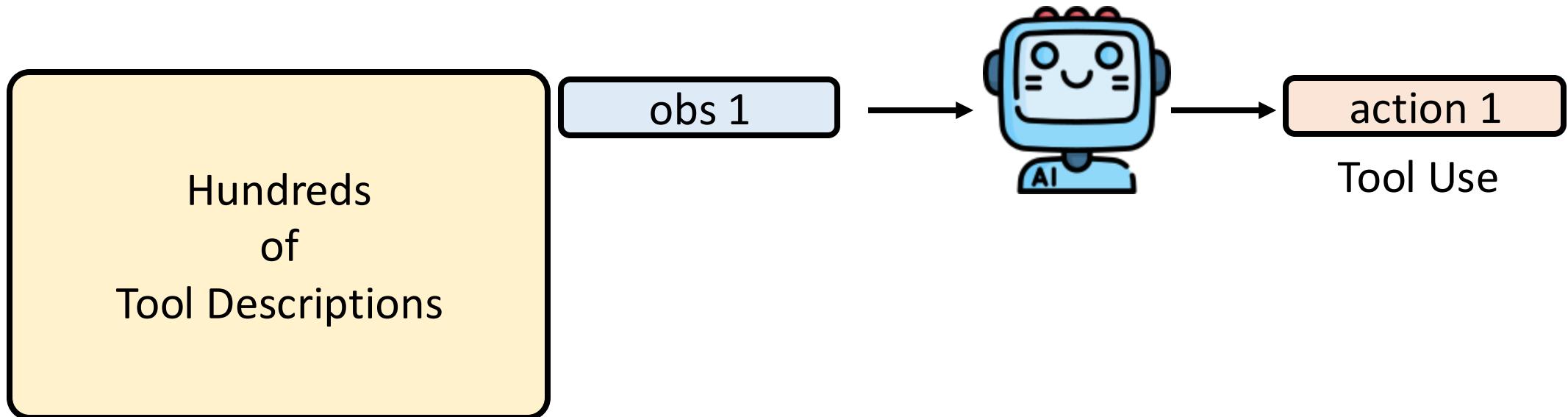


Cheng-Han Chiang

<https://arxiv.org/abs/2402.05629>

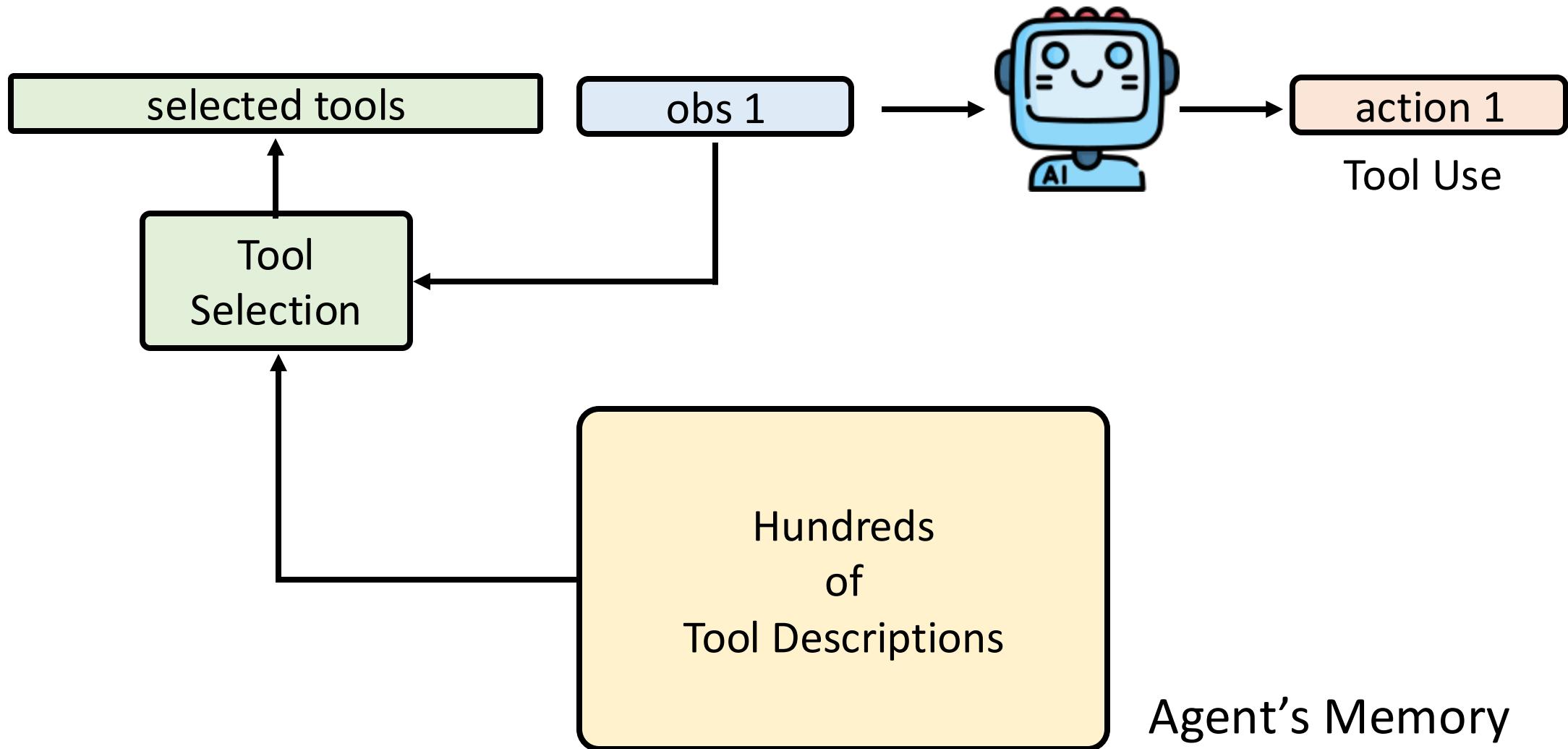


非常多工具怎麼辦？



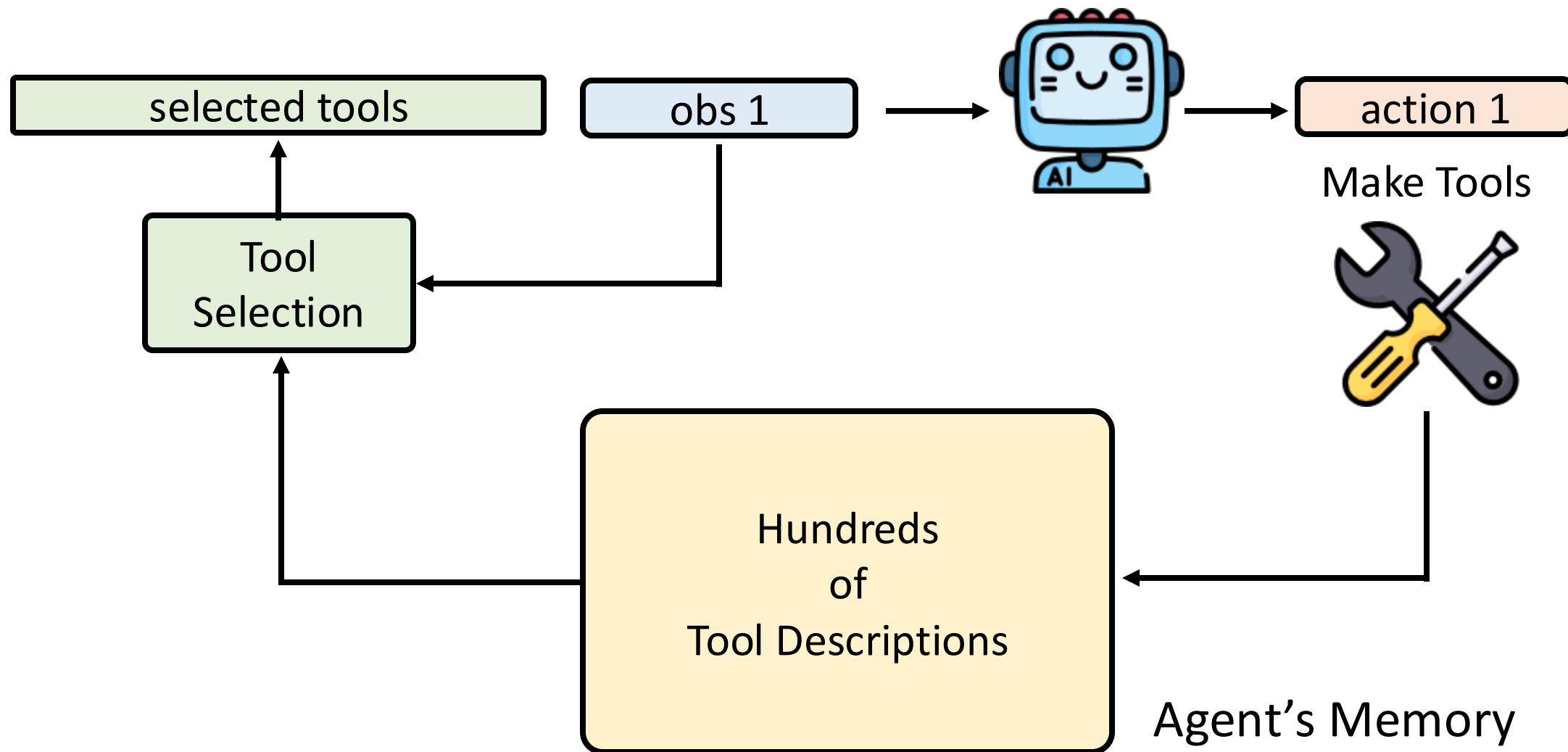
非常多工具怎麼辦？

<https://arxiv.org/abs/2310.03128>
<https://arxiv.org/abs/2502.11271>



模型自己打造工具

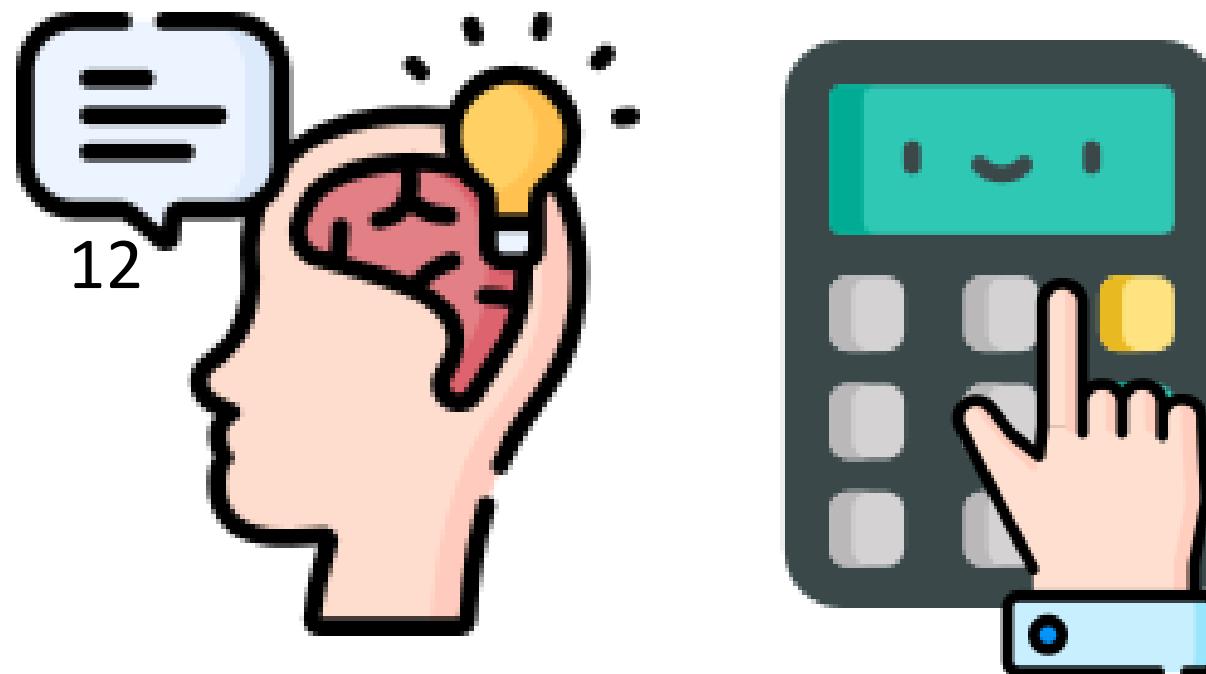
TroVE: <https://arxiv.org/pdf/2401.12869>
LATM: <https://arxiv.org/abs/2305.17126>
CREATOR: <https://arxiv.org/abs/2305.14318>
CRAFT: <https://arxiv.org/abs/2309.17428>



使用工具與模型本身能力間的平衡

- 如果要做兩個數字的乘法，用計算機一定比普通人心算快嗎？

問題： 3×4

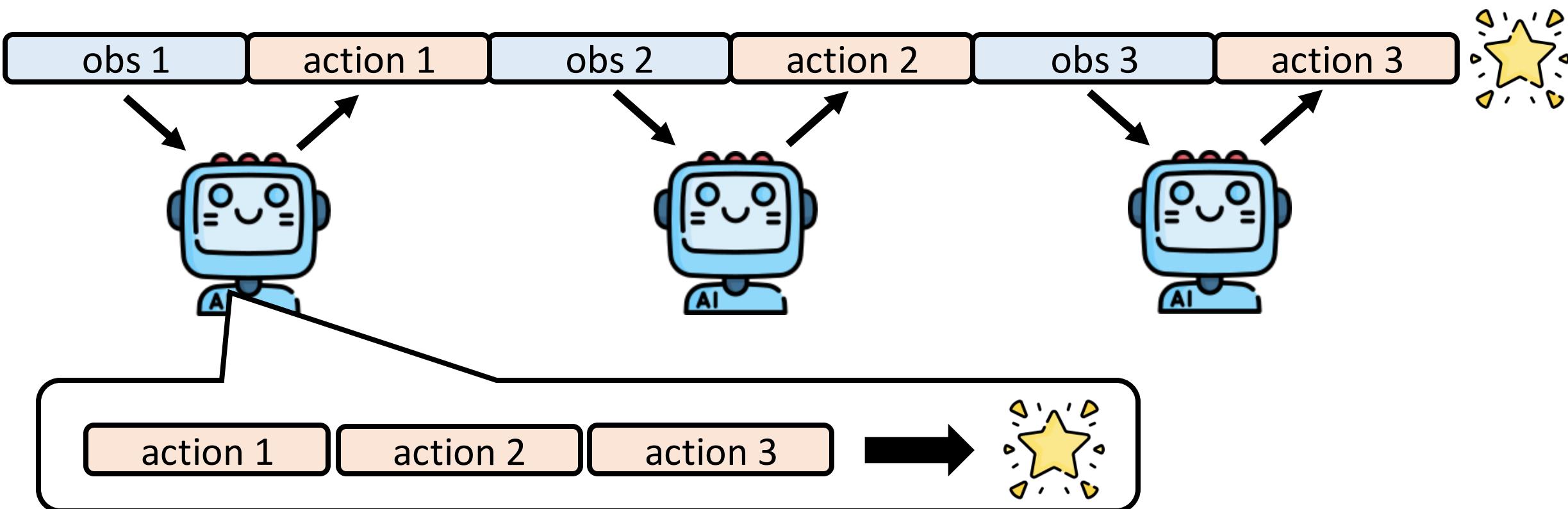




AI 能不能做計劃？

做計劃

天下沒那麼好的事情
計劃就是要拿來改變的

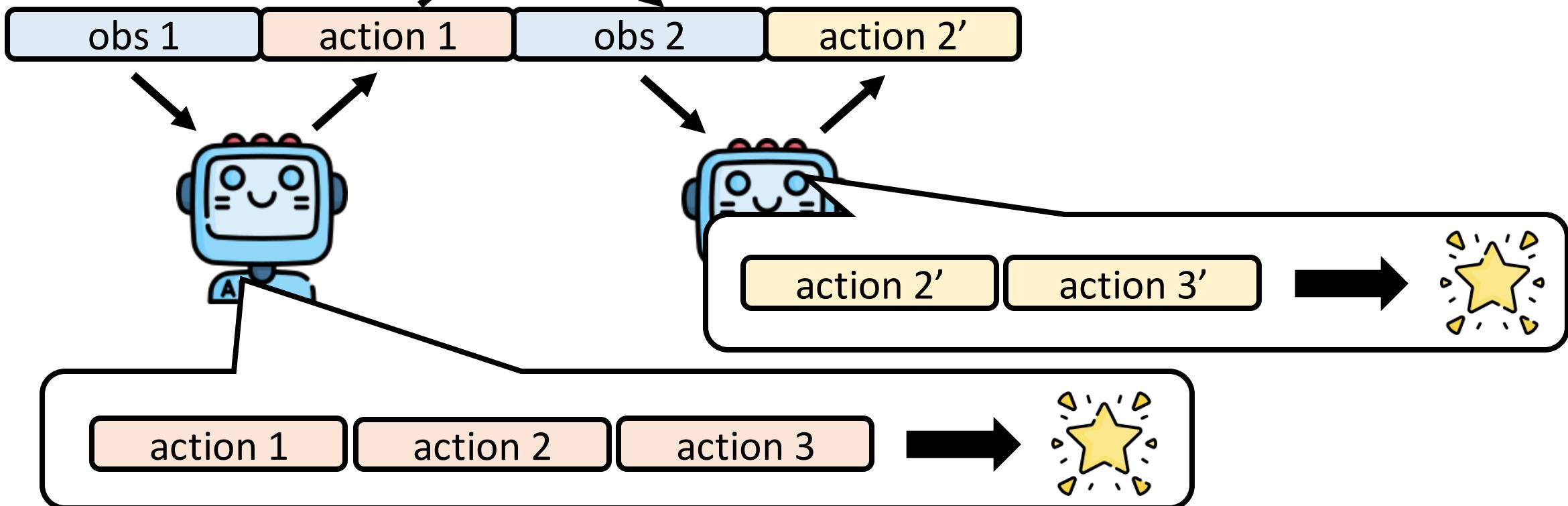


做計劃



- 下棋：對手的招數跟預想不同
- 使用電腦：突然跳出廣告視窗

與預期不同，導致原有的計畫行不通



語言模型有能力做計畫嗎？

gpt-4o

擬定一個成為百萬訂閱 YouTuber 的計畫，計畫內容越具體越詳細越好

第一階段：! 第二階段：🚀 第三階段：📈 第四階段：🏆 百萬訂閱達成（18-24 個月）

目標：確立頻道定位

- ✓ 1. 確定頻道主題
 - 選擇利基市場 (Niches)
 - 熱門但競爭適中
 - 目標受眾分析
 - 競爭對手分析
- ✓ 2. 頻道品牌化
 - 頻道名稱：簡潔、有記憶點、與主題相關

目標：突破 10 萬訂閱

- ✓ 1. 提高影片質感
 - 優化封面縮圖 (High-Quality Thumbnails)
 - 優化標題 (吸引人)
 - 影片開頭黃金 10 秒
- ✓ 2. YouTube SEO
 - 標題與描述包含關鍵字

目標：突破 50 萬訂閱

- ✓ 1. 內容升級
 - 增加高製作價值
 - 尋試直播 (與觀眾互動)
 - 策劃系列內容 (Series)
- ✓ 2. 社群與品項
 - 成立 Discord / Telegram 群組
 - 發展 Merch 產品 (周邊商品)

目標：突破 100 萬訂閱，建立長久影響力，轉型企業化經營。

1. 內容規模化

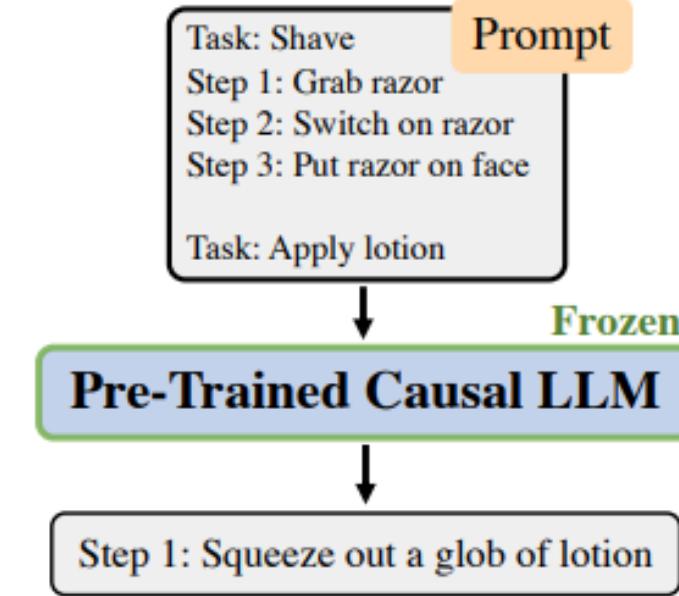
- 組建團隊 (剪輯師、企劃、營運)
- 提高發布頻率 (每週 4-5 支影片)
- 策劃大型企劃 (如挑戰、紀錄片、跨界合作)

2. 商業化

- 開發線上課程 / 會員專屬內容



<https://arxiv.org/abs/2201.07207>



Task: Get Glass of Milk



Walk to Kitchen



Open Fridge



Grab Milk



Close Fridge

Human

Task: Throw away paper
Step 1: Walk to home office
Step 2: Walk to desk
Step 3: Find desk
Step 4: Turn to desk
Step 5: Find chair
Step 6: Sit on chair
Step 7: Find check
Step 8: Grab check
Step 9: Squeeze check
Step 10: Stand up
Step 11: Walk to trashcan
Step 12: Put check on trashcan

GPT-2 1.5B

Task: Brush teeth
Step 1: Go to bathroom

GPT-3 175B

Task: Throw away paper
Step 1: Walk to home office
Step 2: Walk to wastebasket
Step 3: Find wastebasket
Step 4: Grab wastebasket
Step 5: Walk to desk
Step 6: Drop paper in wastebasket

Codex 12B

Task: Brush teeth
Step 1: Walk to bathroom
Step 2: Walk to sink
Step 3: Find toothbrush
Step 4: Pick up toothbrush
Step 5: Put toothbrush in mouth
Step 6: Move brush around mouth
for two minutes
Step 7: Spit out toothpaste and
brush into sink

Translated GPT-3 175B

Task: Throw away paper
Step 1: Walk to home office
Step 2: Walk to table
Step 3: Find table
Step 4: Turn to table
Step 5: Find paper
Step 6: Grab paper
Step 7: Walk to trashcan
Step 8: Open trashcan
Step 9: Put paper on trashcan
Step 10: Close trashcan

Translated Codex 12B

Task: Brush teeth
Step 1: Walk to bathroom
Step 2: Open door
Step 3: Walk to sink
Step 4: Put pot on sink
Step 5: Put brush on toothbrush

PlanBench

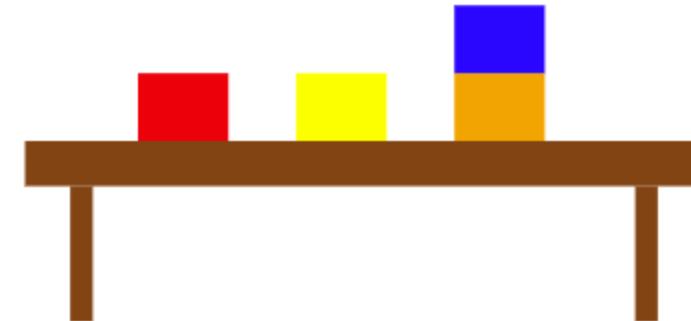
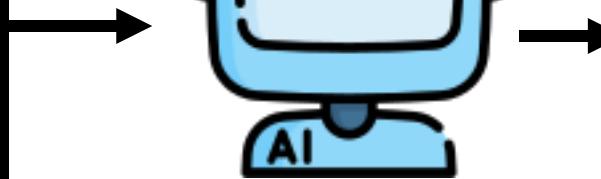
<https://arxiv.org/abs/2206.10498>
<https://arxiv.org/abs/2305.15771>

可以執行的操作：

1. 從桌上拿起一個積木
2. 從另一個積木上拿起另一個積木
3. 把積木放到桌上
4. 將一個積木堆在另一個積木上

初始狀態：藍色積木在橘色積木的上面，
紅色積木在桌子上，橘色積木在桌子上，
黃色積木也在桌子上。

目標：讓橘色積木放置在藍色積木上。



1. 將藍色積木從橘色積木上取下
2. 將藍色積木放在桌子上
3. 從桌上拿起橘色積木
4. 將橘色積木堆放在藍色積木的上方

會不會 LLM 早就看過類似的題目了？

Mystery Blocksworld Domain Description (Deceptive Disguising)

I am playing with a set of objects. Here are the actions I can do

Attack object 攻擊

Feast object from another object 吞噬

屈服 Succumb object

Overcome object from another object 征服

神秘方塊世界

I have the following restrictions on my actions:

To perform Attack action, the following facts need to be true: Province object, Planet object,
↪ Harmony.

Once Attack action is performed the following facts will be true: Pain object.

Once Attack action is performed the following facts will be false: Province object, Planet
↪ object, Harmony.

To perform Succumb action, the following facts need to be true: Pain object.

Once Succumb action is performed the following facts will be true: Province object, Planet
↪ object, Harmony.

Once Succumb action is performed the following facts will be false: Pain object.

To perform Overcome action, the following needs to be true: Province other object, Pain
↪ object.

Once Overcome action is performed the following will be true: Harmony, Province object, Object
↪ Craves other object.

Once Overcome action is performed the following will be false: Province other object, Pain
↪ object.

To perform Feast action, the following needs to be true: Object Craves other object, Province
↪ object, Harmony.

Once Feast action is performed the following will be true: Pain object, Province other object.

Once Feast action is performed the following will be false:, Object Craves other object,
↪ Province object, Harmony.

Zero-shot prompt with GPT-4 plan (Deceptive Disguising)

[STATEMENT]

As initial conditions I have that, object a craves object b, object d craves object c, harmony,
→ planet object b, planet object c, province object a and province object d.

My goal is to have that object c craves object a. (讓物件 c 渴望物件 a)

What is the plan to achieve my goal? Just give the actions in the plan.

----- GPT-4 response -----

1. Feast object a from object b
2. Attack object a
3. Succumb object a
4. Overcome object a from object c
5. Feast object c from object a

----- Extracted plan -----

(feast a b)
(attack a)
(succumb a)
(overcome a c)
(feast c a)

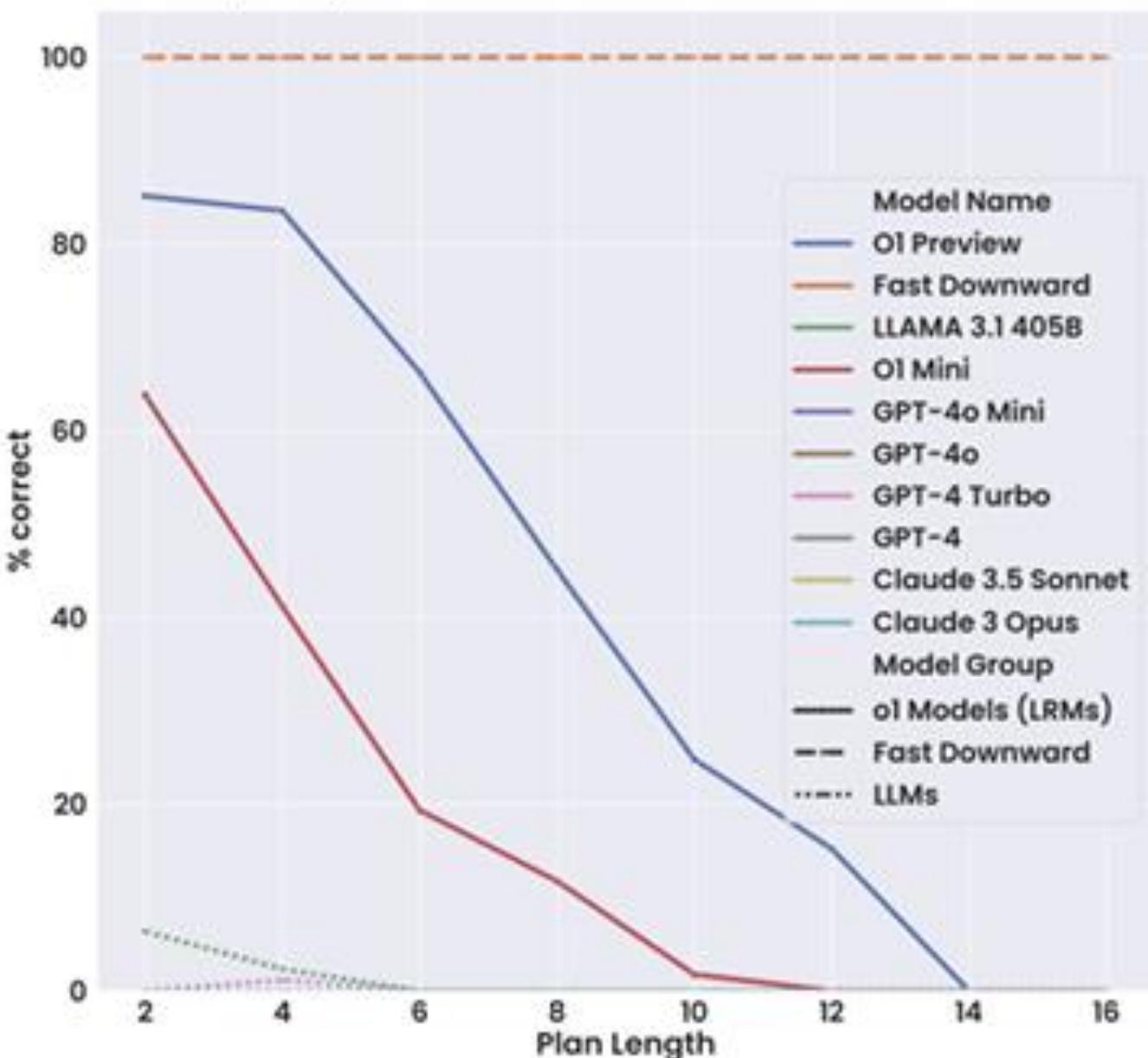
----- Ground truth plan -----

(feast d c)
(succumb d)
(attack c)
(overcome c a)

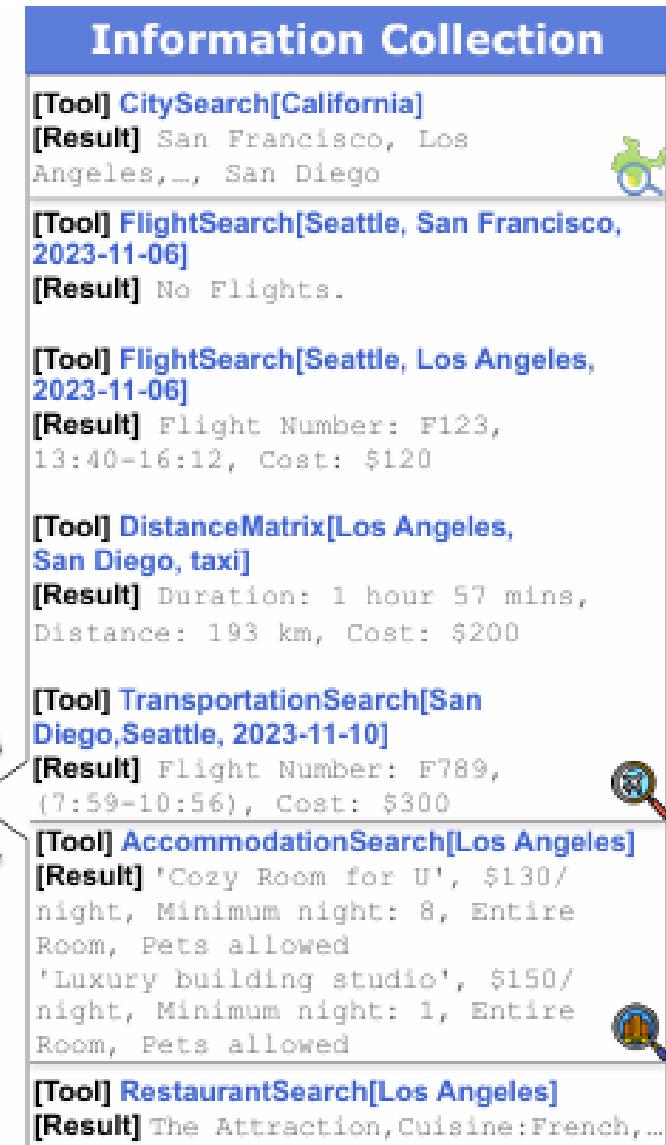
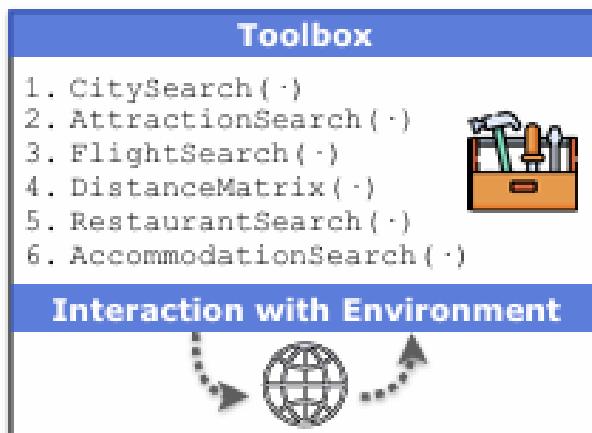
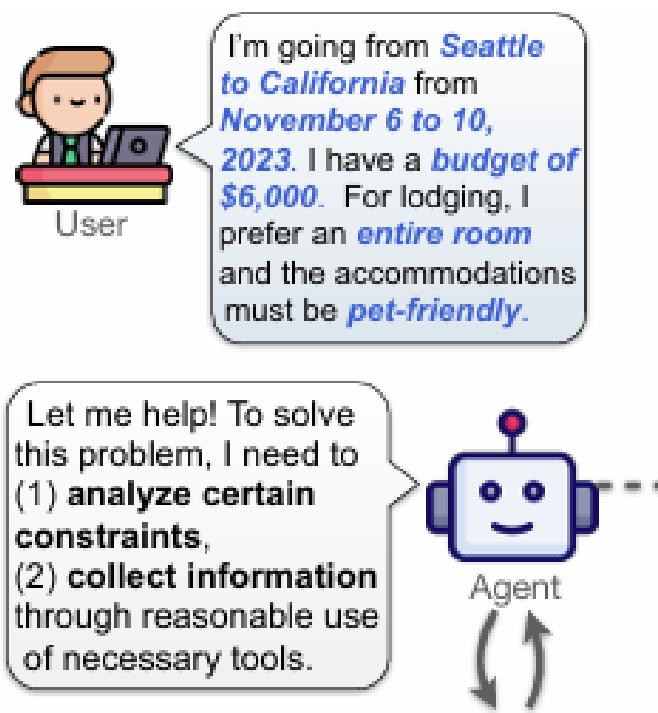
=====FAILURE=====

Domain	Method	Instances correct				
		GPT-4	GPT-3.5	I-GPT3.5	I-GPT3	GPT-3
Blocksworld (BW)	One-shot	206/600 (34.3%)	37/600 (6.1%)	54/600 (9%)	41/600 (6.8%)	6/600 (1%)
	Zero-shot	210/600 (34.6%)	8/600 (1.3%)	-	-	-
	COT	214/600 (35.6%)	-	-	-	-
Logistics Domain	One-shot	28/200 (14%)	1/200 (0.5%)	6/200 (3%)	3/200 (1.5%)	-
	Zero-shot	15/200 (7.5%)	1/200 (0.5%)	-	-	-
	COT	54/600 (9%)	-	-	-	-
Mystery BW (Deceptive)	One-shot	26/600 (4.3%)	0/600 (0%)	4/600 (0.6%)	14/600 (2.3%)	0/600 (0%)
	Zero-shot	1/600 (0.16%)	0/600 (0%)	-	-	-
	COT	54/600 (9%)	-	-	-	-
Mystery BW (Randomized)	One-shot	12/600 (2%)	0/600 (0%)	5/600 (0.8%)	5/600 (0.8%)	1/600 (0.1%)
	Zero-shot	0/600 (0%)	0/600 (0%)	-	-	-

Plan Length vs Correct Predictions for all Models on Mystery Blocksworld - Plan Generation Zero Shot



TravelPlanner



Query: Please create a travel plan for a 3-day trip from Missoula to Dallas scheduled from March 23rd to March 25th, 2022. The budget for this trip is set at \$1,900.

Plan:

<https://osu-nlp-group.github.io/TravelPlanner/>

```
[  
  {  
    "day": 1,  
    "current_city": "from Missoula to Dallas",  
    "transportation": "Flight Number: F3604254, from Missoula to Dallas,  
    Departure Time: 14:27, Arrival Time: 18:26",  
    "breakfast": "-",  
    "attraction": "-",  
    "lunch": "-",  
    "dinner": "Coconuts Fish Cafe, Dallas",  
    "accommodation": "1BR, elevator, kitchen, doorman!, Dallas"  
  },  
  {  
    "day": 2,
```

	Validation (#180)						Test (#1,000)					
	Delivery Rate	Commonsense		Hard Constraint		Final Pass Rate	Delivery Rate	Commonsense		Hard Constraint		Final Pass Rate
		Pass Rate	Pass Rate	Pass Rate	Pass Rate			Pass Rate	Pass Rate	Pass Rate	Pass Rate	
		Micro	Macro	Micro	Macro			Micro	Macro	Micro	Macro	
Greedy Search	100	74.4	0	60.8	37.8	0	100	72.0	0	52.4	31.8	0
<i>Two-stage</i>												
Mistral-7B-32K (Jiang et al., 2023)	8.9	5.9	0	0	0	0	7.0	4.8	0	0	0	0
Mixtral-8x7B-MoE (Jiang et al., 2024)	49.4	30.0	0	1.2	0.6	0	51.2	32.2	0.2	0.7	0.4	0
Gemini Pro (G Team et al., 2023)	28.9	18.9	0	0.5	0.6	0	39.1	24.9	0	0.6	0.1	0
GPT-3.5-Turbo (OpenAI, 2022)	86.7	54.0	0	0	0	0	91.8	57.9	0	0.5	0.6	0
GPT-4-Turbo (OpenAI, 2023)	89.4	61.1	2.8	15.2	10.6	0.6	93.1	63.3	2.0	10.5	5.5	0.6
<i>Sole-planning</i>												
Direct _{GPT-3.5-Turbo}	100	60.2	4.4	11.0	2.8	0	100	59.5	2.7	9.5	4.4	0.6
CoT _{GPT-3.5-Turbo}	100	66.3	3.3	11.9	5.0	0	100	64.4	2.3	9.8	3.8	0.4
ReAct _{GPT-3.5-Turbo}	82.2	47.6	3.9	11.4	6.7	0.6	81.6	45.9	2.5	10.7	3.1	0.7
Reflexion _{GPT-3.5-Turbo}	93.9	53.8	2.8	11.0	2.8	0	92.1	52.1	2.2	9.9	3.8	0.6
Direct _{Mixtral-8x7B-MoE}	100	68.1	5.0	3.3	1.1	0	99.3	67.0	3.7	3.9	1.6	0.7
Direct _{Gemini Pro}	93.9	65.0	8.3	9.3	4.4	0.6	93.7	64.7	7.9	10.6	4.7	2.1
Direct _{GPT-4-Turbo}	100	80.4	17.2	47.1	22.2	4.4	100	80.6	15.2	44.3	23.1	4.4

Query: Please curate a 3-day travel plan for a solo traveler from Tulsa to Houston from March 23rd to March 25th, 2022, with a total travel budget of \$1,000.

Plan:

```
{  
  "day": 3,  
  "current_city": "from Houston to Tulsa",  
  "transportation": "Flight Number: F4013298, from  
  Houston to Tulsa, Departure Time: 08:20, Arrival  
Time: 09:43",  
  "breakfast": "Earthen Spices, Houston",  
  "attraction": "The Museum of Fine Arts,  
Houston; Hermann Park, Houston;",  
  ""lunch": "Chawla, Houston",  
  "dinner": "-",  
  "accommodation": "-"  
}
```

Query: Please assist in crafting a travel plan for a solo traveller, journeying from Detroit to San Diego for 3 days, from March 5th to March 7th, 2022. The travel plan should accommodate a total budget of **\$3,000**.

Trajectory:

Thought 4: The cost for the third day is \$1114, which includes the return flight and activities in San Diego before departure. **The total cost for all three days is now \$3247, which exceeds the budget of \$3000.** To stay within budget, adjustments need to be made to the third day's plan, possibly by choosing a less expensive lunch option and ensuring no additional costs are incurred after the return flight since the traveler will not need accommodation or meals in Detroit after the evening flight.

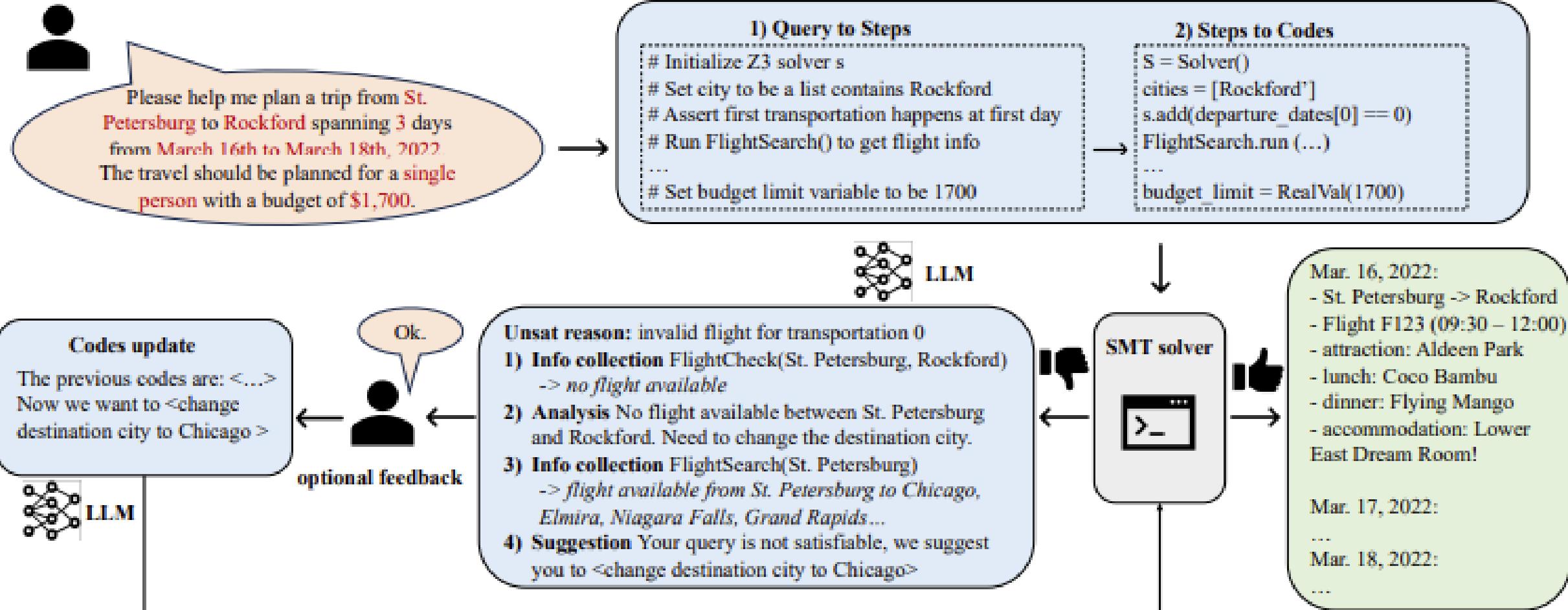
Action 4: CostEnquiry[{"people_number": 1, "day": 3,...}]
Observation 4: Cost: The cost of your plan is 1105 dollars.

Thought 5: The revised cost for the third day is \$1105, which includes a more affordable lunch option. **The total cost for all three days is now \$3238, which is still slightly over the budget of \$3000.** To further reduce costs, I can look for a less expensive breakfast option on the third day...

Action 5: CostEnquiry[{"people_number": 1, "day": 3,...}]
Observation 5: Cost: The cost of your plan is 1083 dollars.

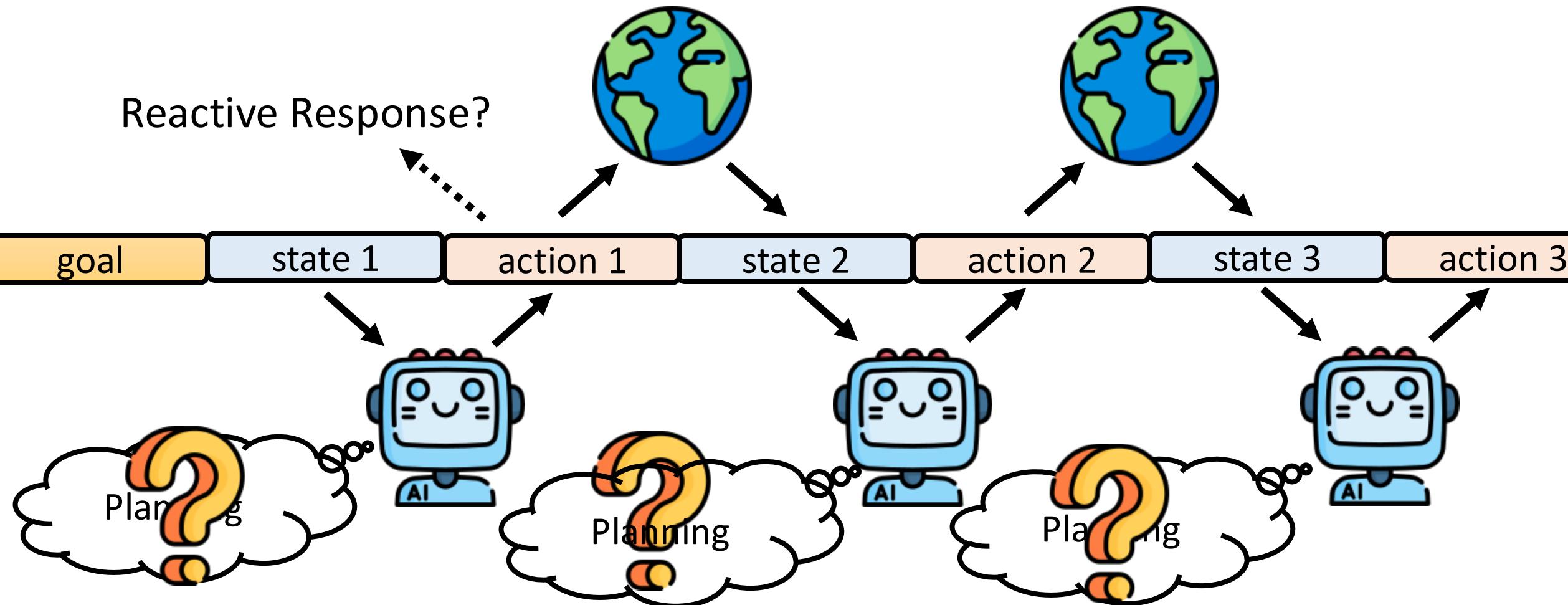
Thought 6: The revised cost for the third day is now \$1083 after choosing a less expensive breakfast option. **The total cost for all three days is \$3216, which is closer to the budget but still slightly over.** Since the flight and accommodation costs are fixed, the only remaining option to adjust would be the attractions or lunch on the second day. However, given the small amount by which the budget is exceeded, **it may be acceptable to slightly exceed the budget due to the variability of daily expenses and the possibility of finding deals on-site.** The traveler should be prepared for a small buffer in their budget.

Action 6: Finish

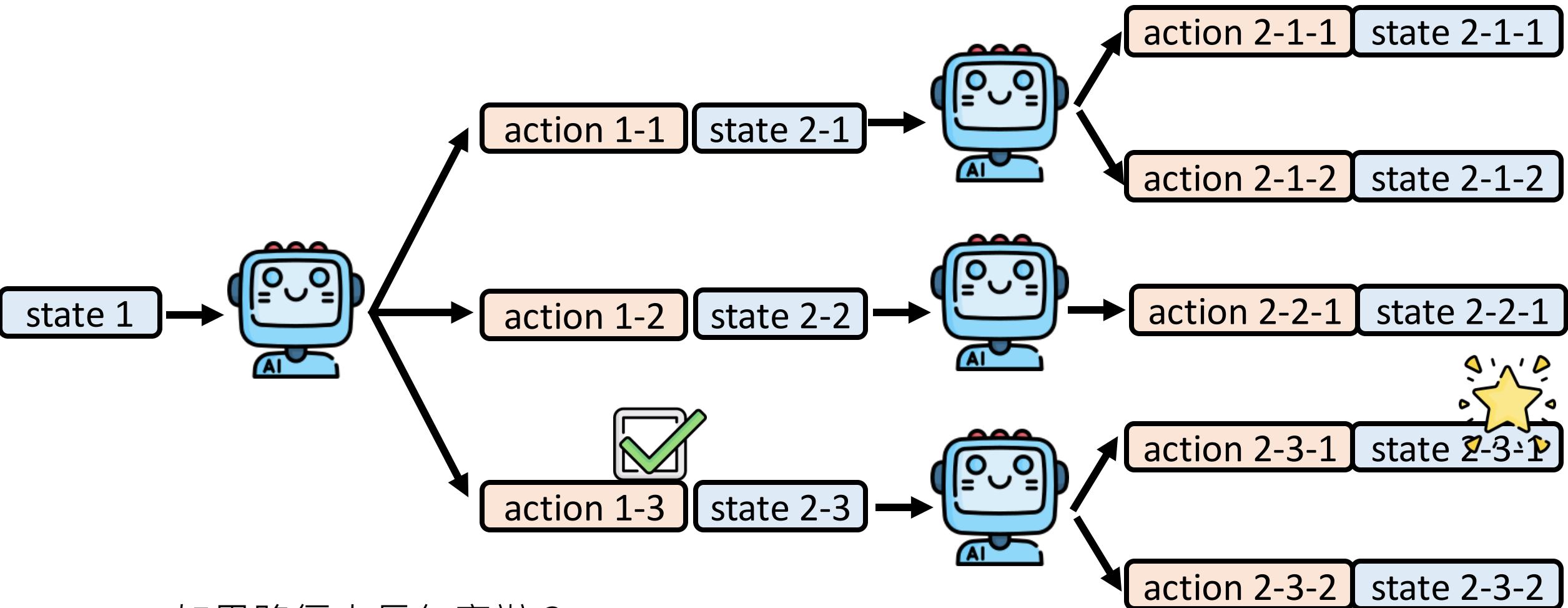


Method	Delivery Rate	Commonsense Pass Rate		Hard Constraint Pass Rate		Final Pass Rate
		Micro	Macro	Micro	Macro	
<i>Validation (#180)</i>						
Greedy Search	100	74.4	0	60.8	37.8	0
TwoStage (GPT-4)	89.4	61.1	2.8	15.2	10.6	0.6
Direct (GPT-4)	100	80.4	17.2	47.1	22.2	4.4
Direct (o1-preview)	100	79.6	15.0	41.9	37.8	10.0
Ours (Mistral-Large)	72.2	72.0	70.6	63.3	66.7	66.7
Ours (Claude-3)	96.1	96.0	95.6	94.8	93.3	93.3
Ours (GPT-4)	95.0	95.0	95.0	95.7	98.9	93.3
<i>Test (#1000)</i>						
Greedy Search	100	72.0	0	52.4	31.8	0
TwoStage (GPT-4)	93.1	63.3	2.0	10.5	5.5	0.6
Direct (GPT-4)	100	80.6	15.2	44.3	23.1	4.4
Ours (Mistral-Large)	69.9	69.8	69.4	63.0	67.8	67.8
Ours (Claude-3)	95.4	95.2	94.3	93.5	93.9	93.9
Ours (GPT-4)	91.5	91.4	91.1	91.3	90.2	90.2

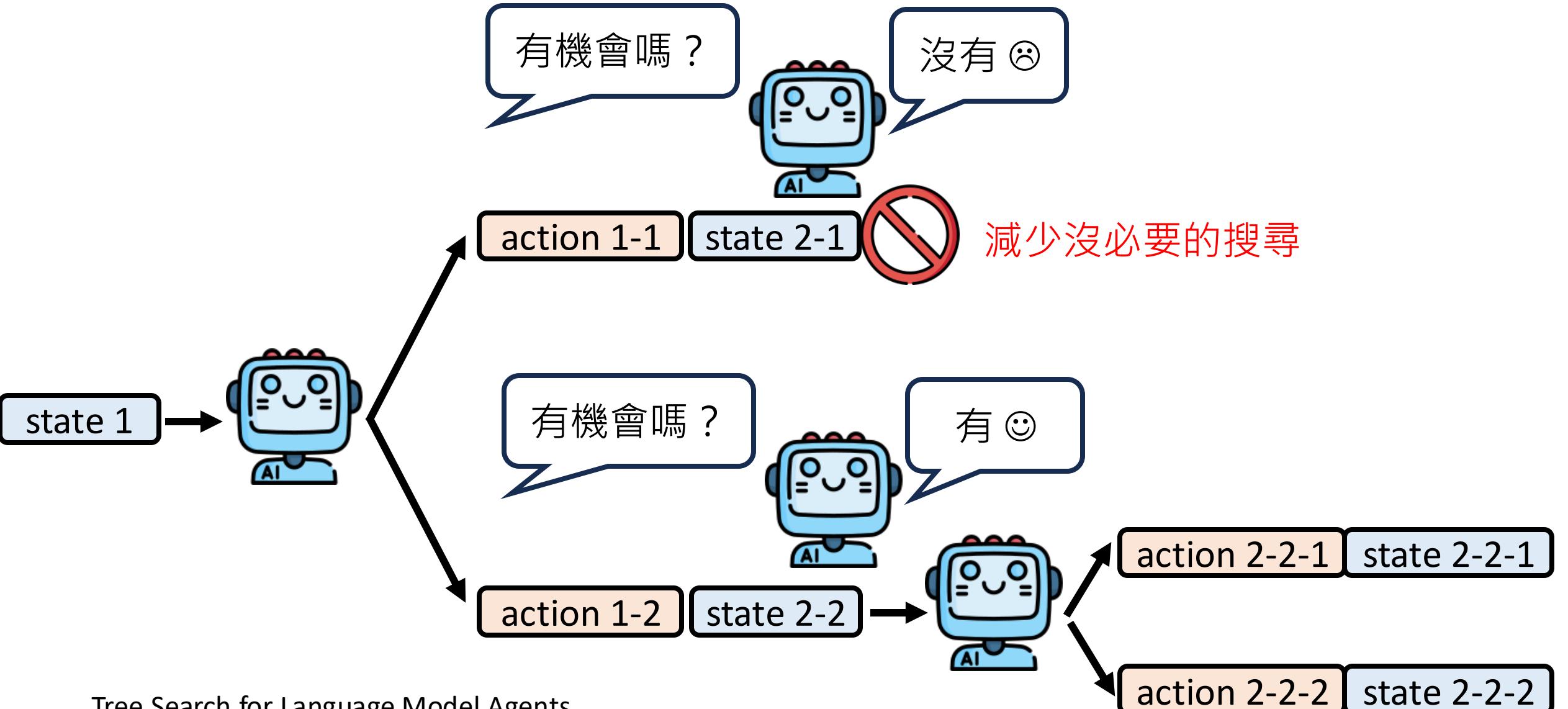
強化 AI Agent 的規劃能力



強化 AI Agent 的規劃能力



如果路徑太長怎麼辦？



Tree Search for Language Model Agents

<https://arxiv.org/abs/2407.01476>



Task Instruction (I): "Can you add this and the other canned fruit (of the same brand) that looks like this, but red instead of brown to the comparison page?"

Legend

- 1 Step sequence
- v = 1.0 State values
- Backtracking

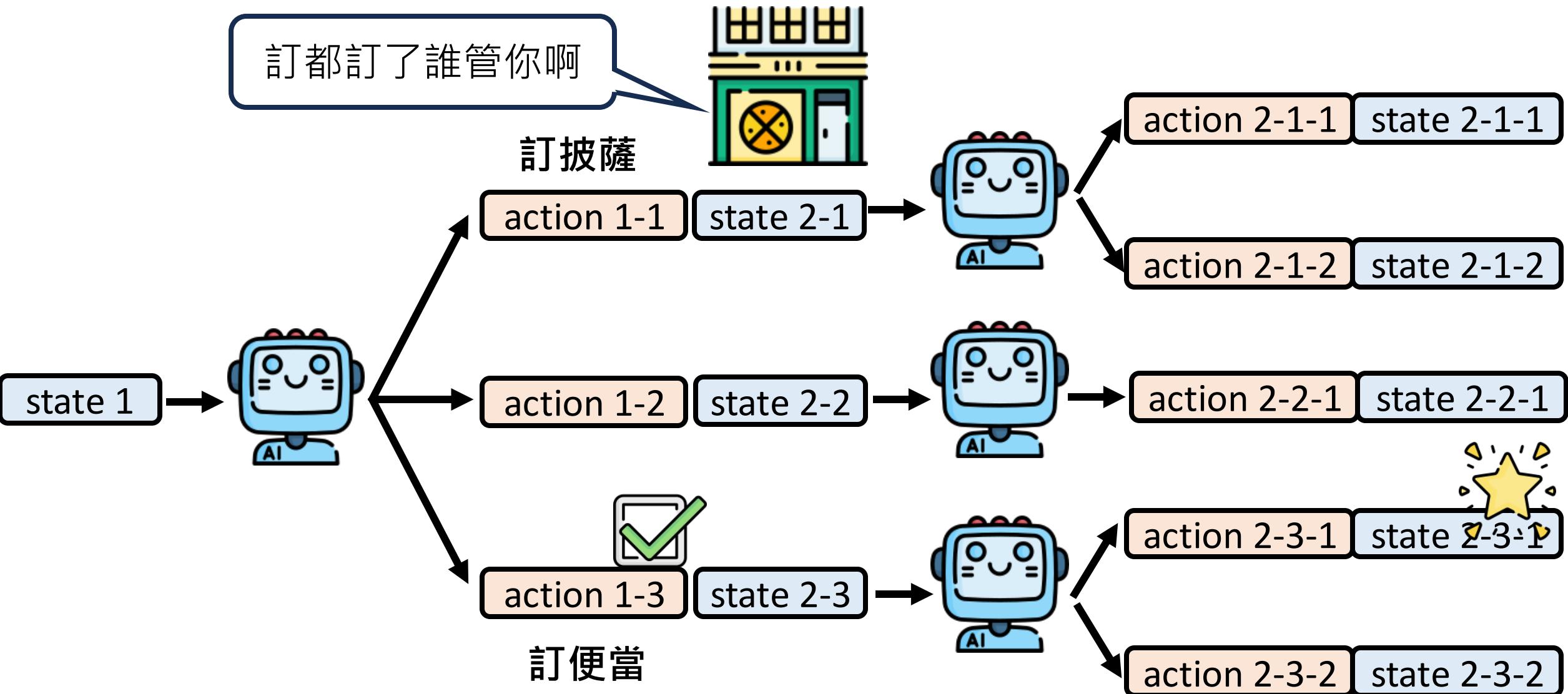
GPT-4o Agent

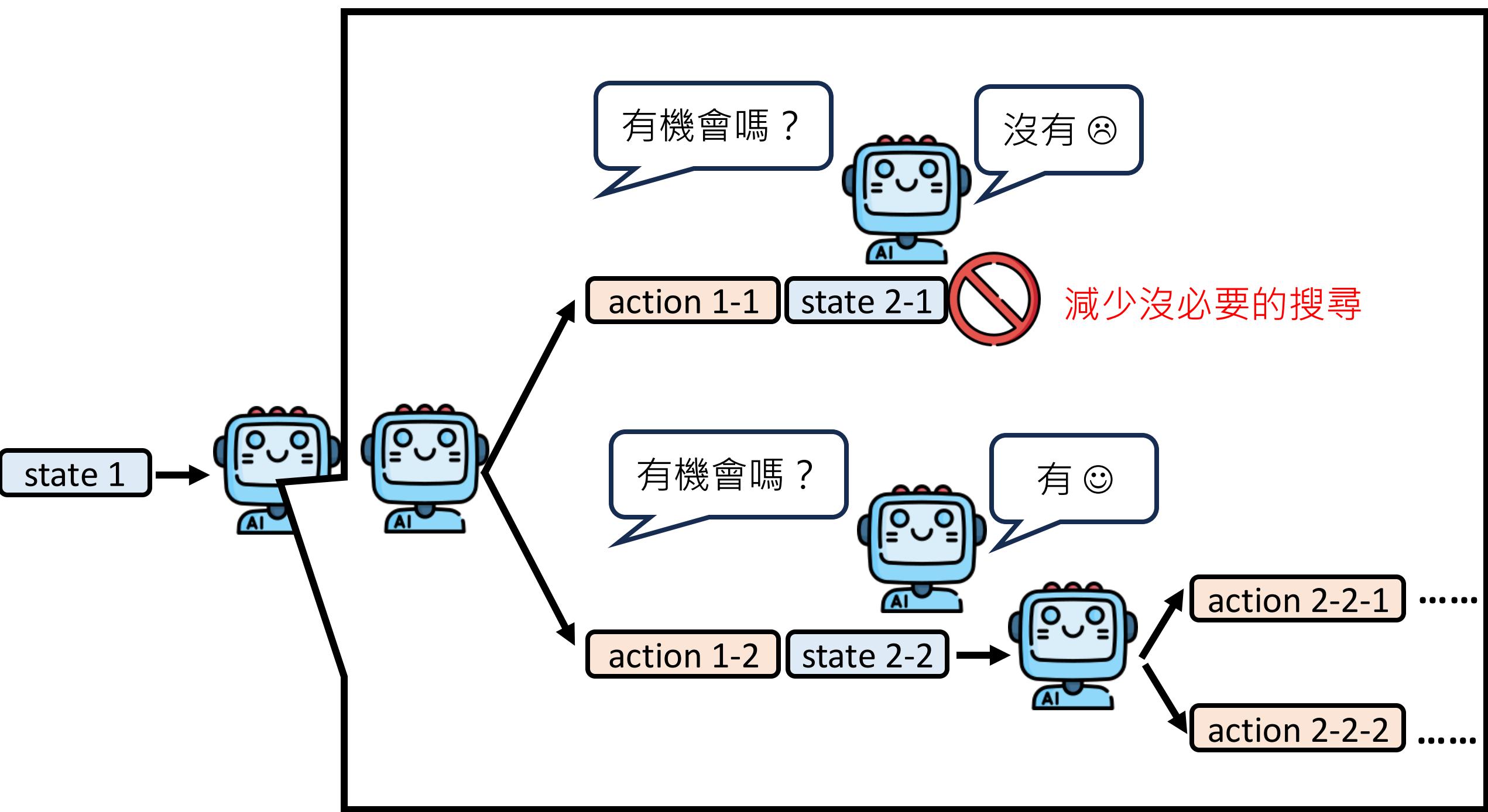


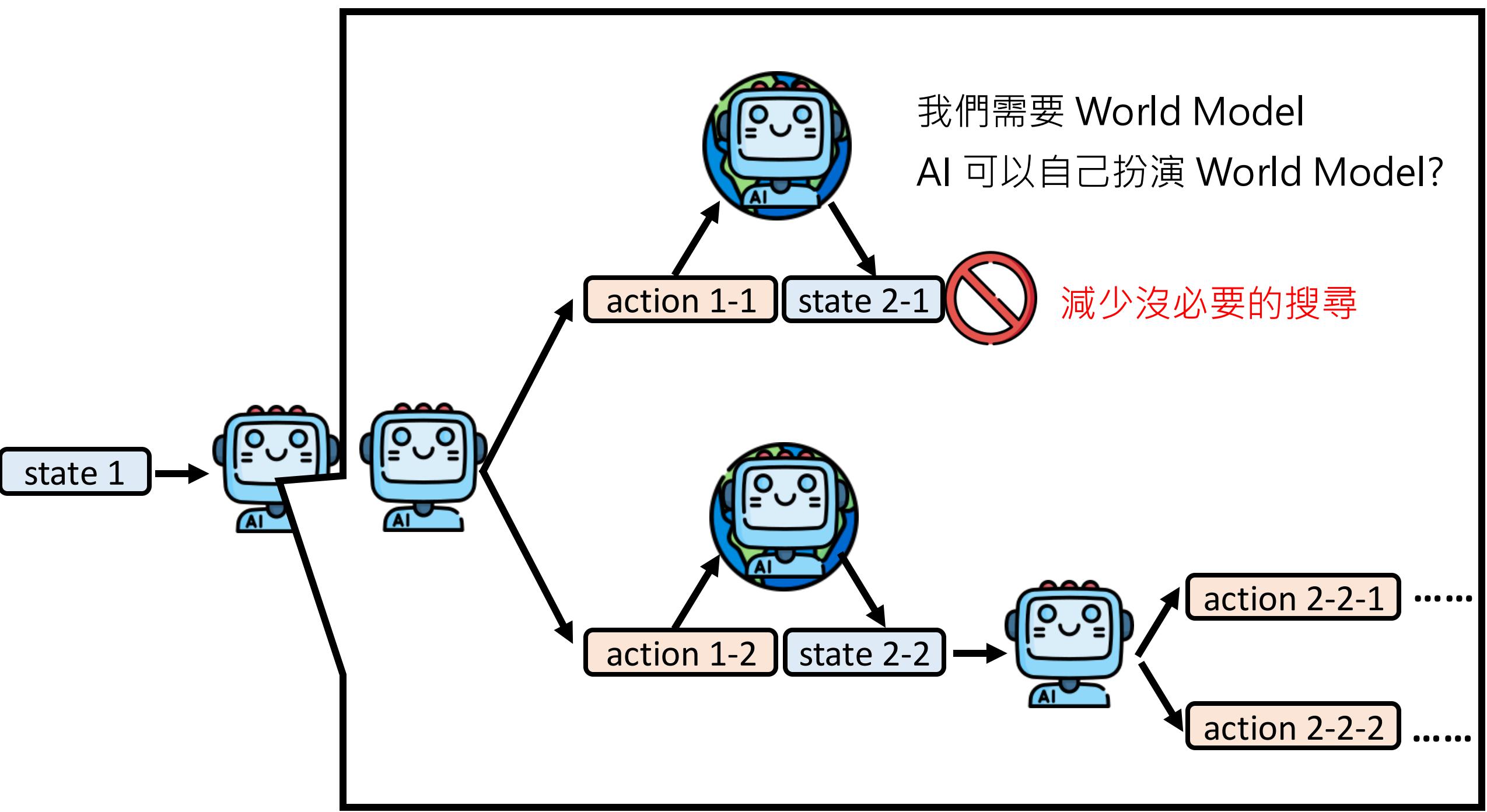
GPT-4o Agent + Search



缺點：有些動作無法回溯







Is Your LLM Secretly a World Model of the Internet? Model-Based Planning for Web Agents

<https://arxiv.org/abs/2411.06559>

Please navigate to the 'Data Storage' category and purchase the least expensive disk with 512GB of storage.

One Stop Market

My Account My Wish List Sign In Welcome to One Stop Market Create an Account

Beauty & Personal Care Sports & Outdoors Clothing, Shoes & Jewelry Home & Kitchen Office Products Tools & Home Improvement

Health & Household Patio, Lawn & Garden Electronics Cell Phones & Accessories Video Games Grocery & Gourmet Food

① Click 'Office Products'

② Click 'Electronics'

③ Type 'Disk'

Product Showcases

Pre-Baked Gingerbread House Kit Value Pads, 17 oz., Pack of 2, Total 36oz. 4.5 stars 1 review \$19.99 Add to Cart

BB-Energy Healthy Energy Drink, Ready Energy from Black and Green Tea, Pomegranate Flavored, 8 Ounce Can, Pack of 24 4.5 stars 12 reviews \$14.47 Add to Cart

Embossed Tin Pineapple, Orange Vanilla Caffeine Free Fruit Infusion, 16-Ounce Pouch 4.5 stars 8 reviews \$19.36 Add to Cart

Balls Of The Ball Princess Sprinkle Mix | Wedding Confetti Sprinkles | Cake Cupcake Cookies Sprinkles | Ice Cream Candy Sprinkles | Non-GMO Project Verified, 9 oz, Tub 4.5 stars 12 reviews \$14.42 Add to Cart

Ice-Delicious Dairy-Free CocoWhip Light, Vegan, Non-GMO Project Verified, 9 oz, Tub 4.5 stars 12 reviews \$14.42 Add to Cart

Changzhou Toast Potato (Bunch Powder 50g), DeepFried Potato 50%, Corn 45% 4.5 stars 12 reviews \$14.48 Add to Cart

Q Miso Premium Ginger Ale Real Ingredients & Less Soda, 6.7 FL OZ (200mL), Pack of 20 4.5 stars 12 reviews \$14.48 Add to Cart

Turkey Stuffing Mix (12 oz Boxes), Pack of 2 4.5 stars 12 reviews \$14.49 Add to Cart

Bress DMX -Pixel Light - 16 Bag 4.5 stars 12 reviews \$14.59 Add to Cart

Tony Chachere's More Spice Grouse Seasoning - 16oz 4.5 stars 12 reviews \$14.61 Add to Cart

Stage I: Simulation

1. Click 'Office Products'

The 'Office Products' category will display three sub-categories: 'Office Electronics', 'Office & School Supplies', and 'Office Furniture & Lighting'.

2. Click 'Computer & Accessories'

The webpage will display 'Computer Accessories' sub-category results with products, and the sub-menu will show 'Printers&Accessories' and other categories.

3. Click 'Electronics'

The webpage will display 'Electronics' sub-category results with products, and the sub-menu will show 'Data Storage', 'Tablet Accessories', and others.

$v = 0.4$

$v = 0.8$

$v = 0.1$

Stage II: Execution

Electronics

Shop By

Category

- Home Audio (1280)
- Video Projectors (440)
- Accessories & Supplies (2400)
- Televisions & Video (1030)
- Cameras & Photo (510)
- Computers & Accessories (2620)
- Headphones (127)
- Portable Audio & Video (620)
- Security & Surveillance (248)
- Power Accessories (243)
- Car & Vehicle Electronics (420)
- Wearable Technology (120)
- GPS, Finders & Accessories (122)

Items 1-12 of 14628

Sort by Position

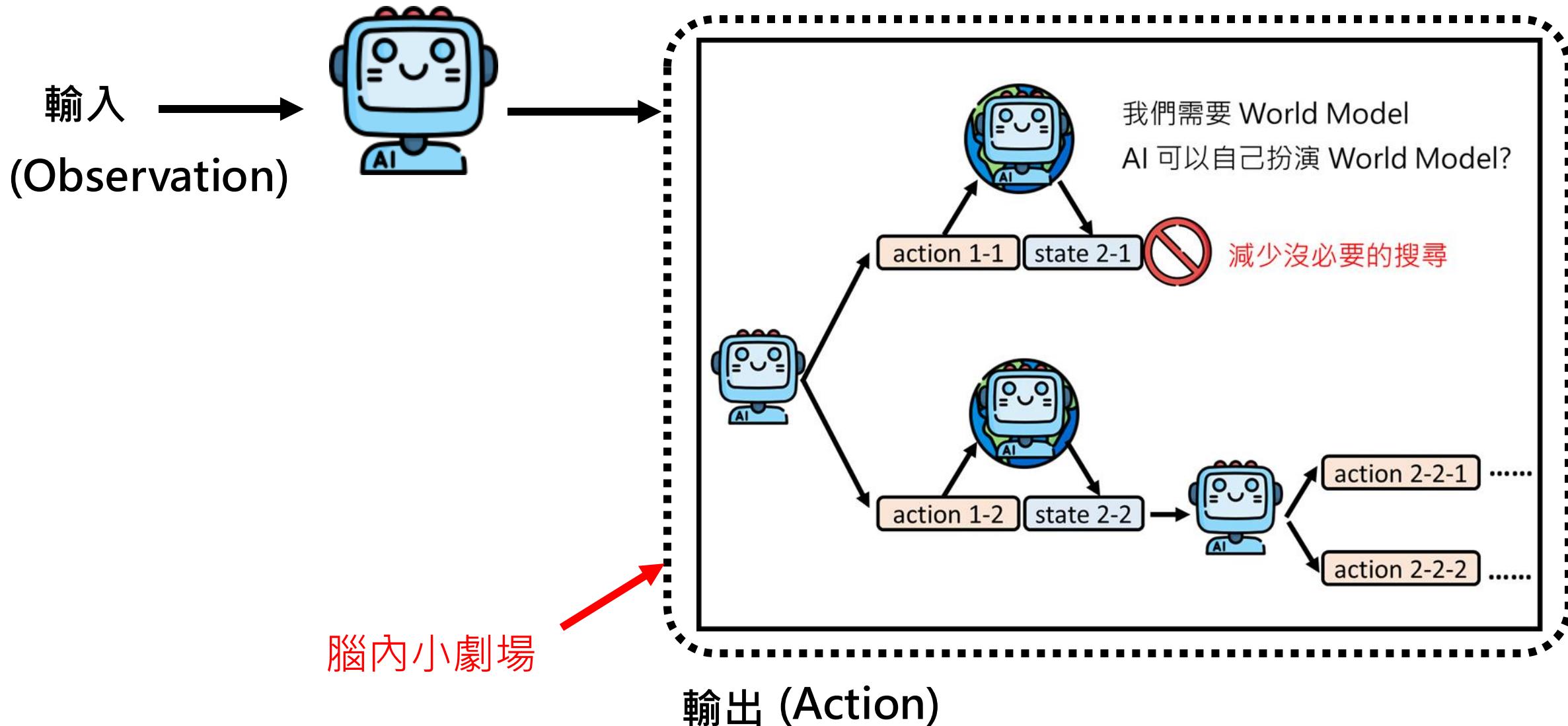
Nest Hello Indoor Camera - Night Vision, Two-Way Audio, Motion Detection, Cloud Storage, Works with Alexa, Google Assistant, and IFTTT 4.5 stars 12 reviews \$14.49 Add to Cart

Ring Indoor Cam HD 1080P Indoor Security Camera with Night Vision, Motion Detection, Cloud Storage, Works with Alexa, Google Assistant, and IFTTT 4.5 stars 12 reviews \$14.49 Add to Cart

Indoor Pet Camera, HD 1080P Indoor Security Camera with Night Vision, Motion Detection, Cloud Storage, Works with Alexa, Google Assistant, and IFTTT 4.5 stars 12 reviews \$14.49 Add to Cart

Rockville CR100SP Chuchano Car Stereo Receiver with 6.5" 2-Way Speakers, 400W Max Power, and Bluetooth 4.5 stars 12 reviews \$14.49 Add to Cart

(Reasoning) 從 AI Agent 的角度來看「思考」的能力



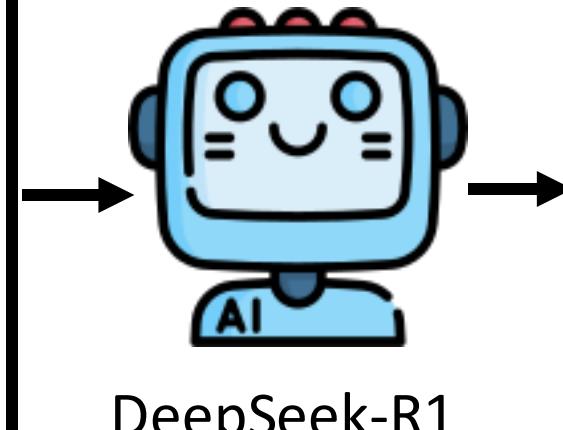
可以執行的操作：

1. 從桌上拿起一個積木
2. 從另一個積木上拿起另一個積木
3. 把積木放到桌上
4. 將一個積木堆在另一個積木上

目前狀態：藍色積木在橘色積木的上面，紅色積木在桌子上，橘色積木在桌子上，黃色積木也在桌子上。

目標：讓橘色積木放置在藍色積木上。

告訴我你的下一步



上略 1500 字

但有没有更快的步骤？例如，步骤1之后，是否可以直接做。因为操作4可能需要另一个积木在桌上，而蓝色此时不动橘色到蓝色上面。

因此，正确的步骤应该是：

1. 从橘色上拿起蓝色（操作2）
2. 将蓝色放到桌上（操作3）
3. 从桌上拿起橘色（操作1）
4. 将橘色堆到蓝色上（操作4）

这样就能完成目标。所以下一步应该是第一步，也就是操

下一步：使用操作2，從橘色積木上拿起藍色積木。

今日課程內容

AI 如何根據經驗調整行為

AI 如何使用工具

AI 能不能做計劃