

大型語言模型的發展與應用

中央研究院資訊科學研究所黃瀚萱助研究員

2023

大綱

- 語言模型
- 大型語言模型（LLMs）
- ChatGPT的應用與限制

語言模型

Probabilistic Language Modeling

- 語言模型可以評估某一段文字之於某個語言出現的機率

$$P(W) = P(w_1, w_2, w_3, \dots, w_n)$$

- 給定一段文句，讓語言模型預測最有可能的下一個詞彙，就具備了語言生成的能力

$$P(w_{n+1}) = \arg \max_{w \in V} P(w|w_1, w_2, w_3, \dots, w_n)$$

語言模型的建立

- 如何計算以下文句的機率？
 - $P(\text{“The dog ate my cake”})$
 - $P(\text{“The cake ate my dog”})$

N-gram Models

- 只考慮與前 N-1 個詞彙的關係

$$P(w_1, w_2, w_3, \dots, w_n) \approx \prod_{i=1}^n P(w_i | w_{i-k+1}, w_{i-k+2}, \dots, w_{i-1})$$

- Bigram模型，只考慮與前一個詞彙的關係

$$P(w_1, w_2, w_3, \dots, w_n) \approx \prod_{i=1}^n P(w_i | w_{i-1})$$

Bigram的計算

$$P(w_i | w_{i-1}) = \frac{C(w_{i-1}, w_i)}{C(w_{i-1})}$$

$$\begin{aligned} &P(\text{The dog ate my cake}) \\ &= P(\text{The} | \langle s \rangle) P(\text{dog} | \text{The}) P(\text{ate} | \text{dog}) P(\text{my} | \text{ate}) P(\text{cake} | \text{my}) \\ &= \frac{C(\langle s \rangle \text{ The})}{C(\langle s \rangle)} \frac{C(\text{The dog})}{C(\text{The})} \frac{C(\text{dog ate})}{C(\text{dog})} \frac{C(\text{ate my})}{C(\text{ate})} \frac{C(\text{my cake})}{C(\text{my})} \end{aligned}$$

N-gram模型的缺點

- N 較小的 N-gram 模型無法掌握長距上下文關係
- N大時，語料庫無法提供足夠的統計樣本
 - 稀疏性 (Sparsity)

語言模型早期的應用

- 文字辨識 (Optical character recognition)
 - 基於語言用法優化辨識結果
- 語音辨識
 - 解析音訊相似的歧義性
 - $P(\text{"I saw a fan"})$ vs $P(\text{"eyes awe of an"})$

語言模型的傳統應用

- 機器翻譯
 - 產生更符合目標語言習慣的翻譯
 - 他是一個好人 $\Rightarrow P(\text{“he is a nice person”})$ vs $P(\text{“he is a good person”})$
- 文法更正
 - He is in the bus
 - He is at the bus
 - He is on the bus

基於神經網路的語言模型

- 用RNN或Transformer直接學習預測下一個詞彙
 - 透過詞彙相量表徵語意資訊，而非死板的字符匹配
 - RNN和Transformer網路並非死板的計算連續N個詞彙的頻率，能萃取距離不等但重要的文字相依關係
- 減少稀疏性，從而能從有限的資料中學習豐富的詞彙組合與上下文意

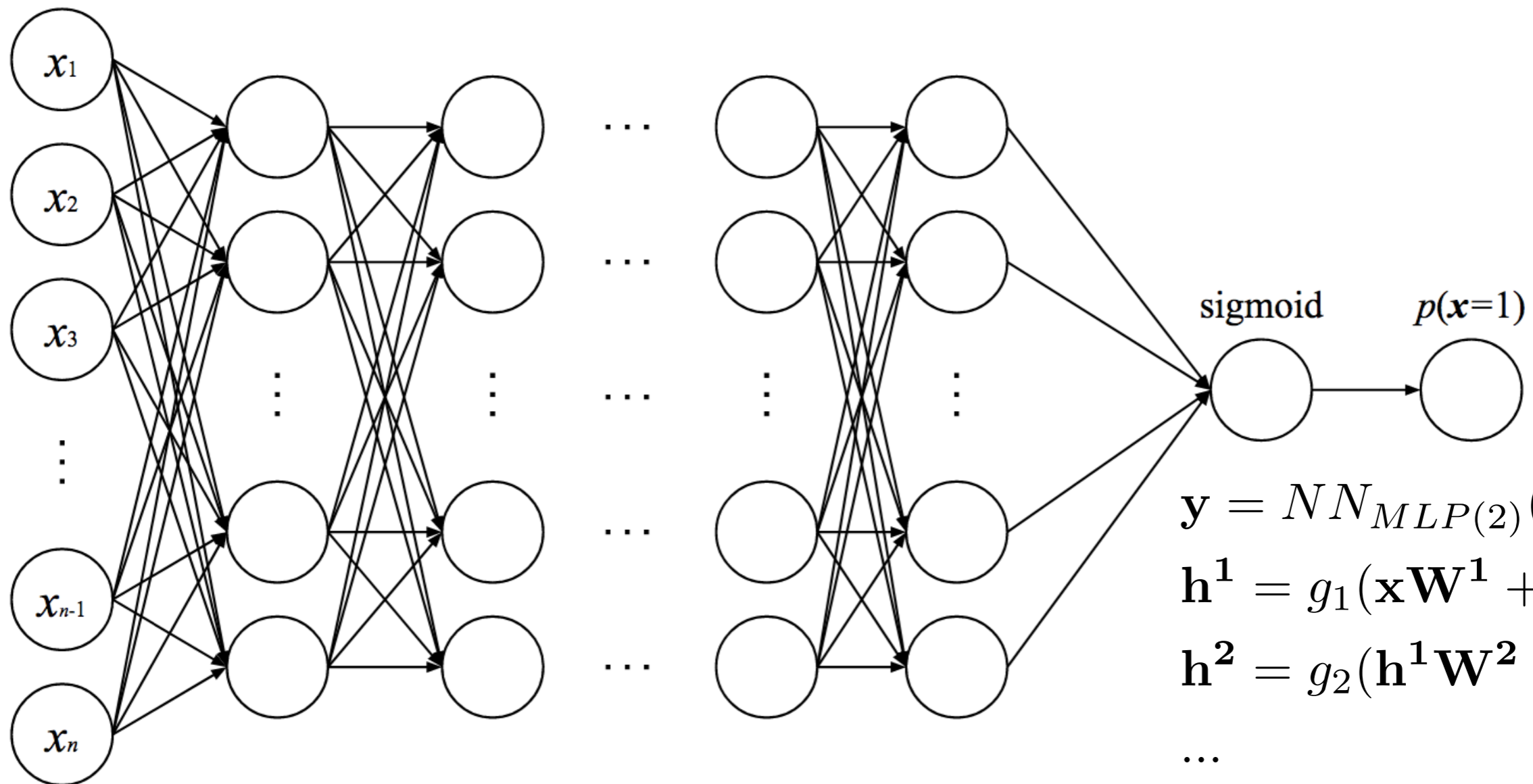
類神經網路與自然語言處理

Feed-forward Neural Network

Input Layer

Hidden Layers

Output Layer



$$y = NN_{MLP(2)}(\mathbf{x})$$

$$\mathbf{h}^1 = g_1(\mathbf{x}\mathbf{W}^1 + \mathbf{b}^1)$$

$$\mathbf{h}^2 = g_2(\mathbf{h}^1\mathbf{W}^2 + \mathbf{b}^2)$$

...

$$\mathbf{h}^k = g_k(\mathbf{h}^{k-1}\mathbf{W}^k + \mathbf{b}^k)$$

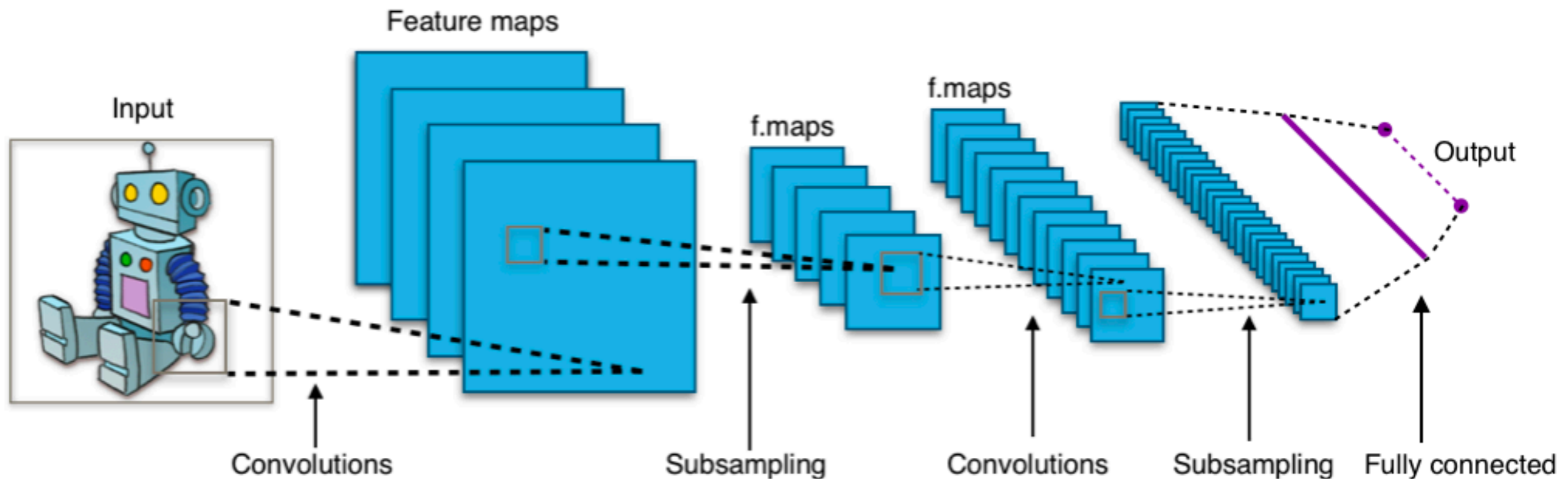
$$y = \mathbf{h}^k\mathbf{W}^{k+1} + \mathbf{b}^k$$

對序列資訊建模

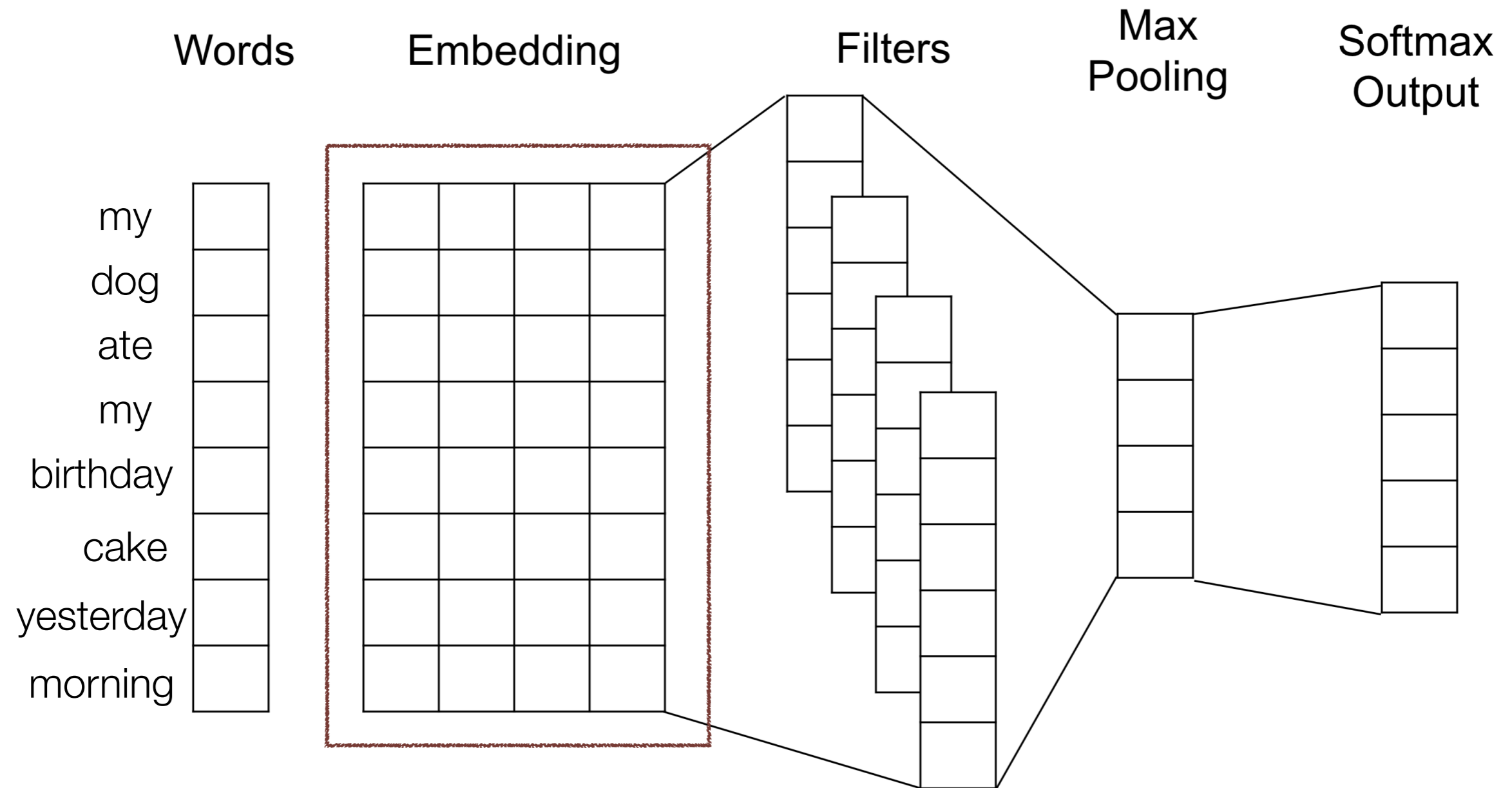
- 文字的順序是自然語言處理的關鍵之一，無法掌握文字的順序，就無法進行細膩的文字理解與生成
- Feed-forward neural network和傳統機器學習模型一樣，無法有效萃取文字的順序資訊
- 需要對文字的相對位置更敏感的模式

Convolutional Neural Networks

- 影像處理、電腦視覺上最主要的神經網路架構



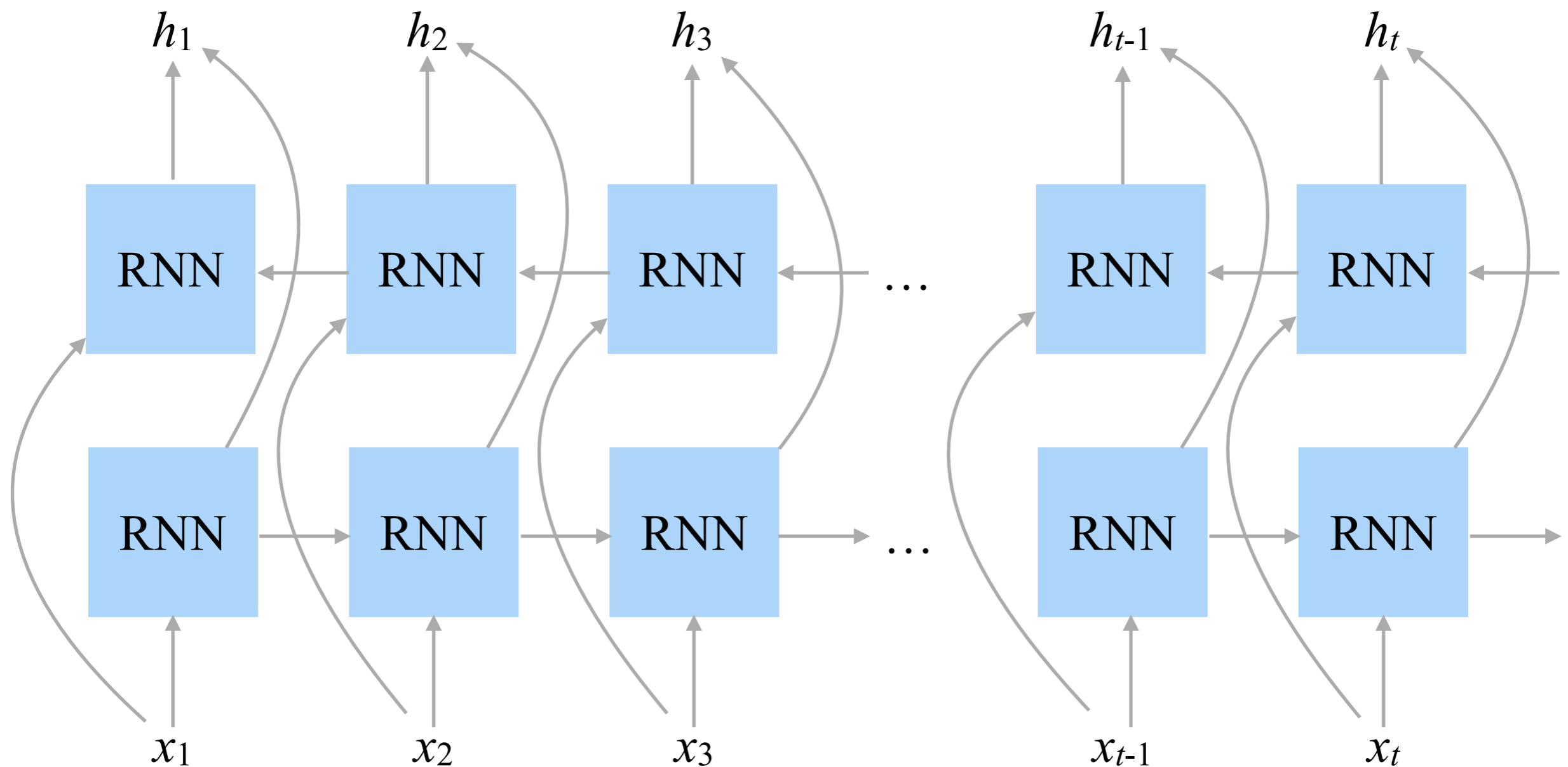
CNN於自然語言處理



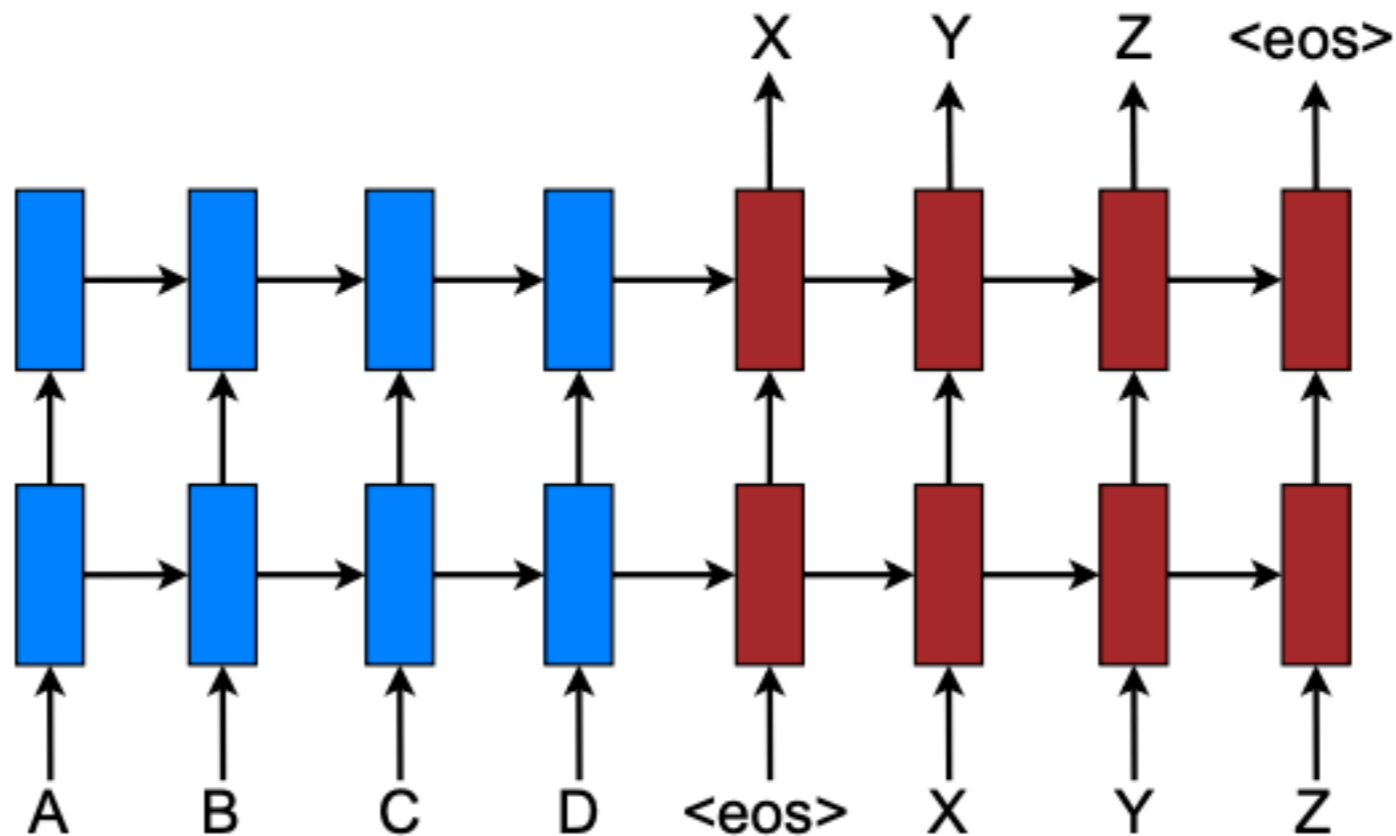
用 $N * D$ 的矩陣，表徵長度為 N 的句子

雙向RNN

- 架接正向、逆向兩個方向的RNN網路
- 序列上每一個項目的表徵，來自其正向、逆向隱藏層的接合

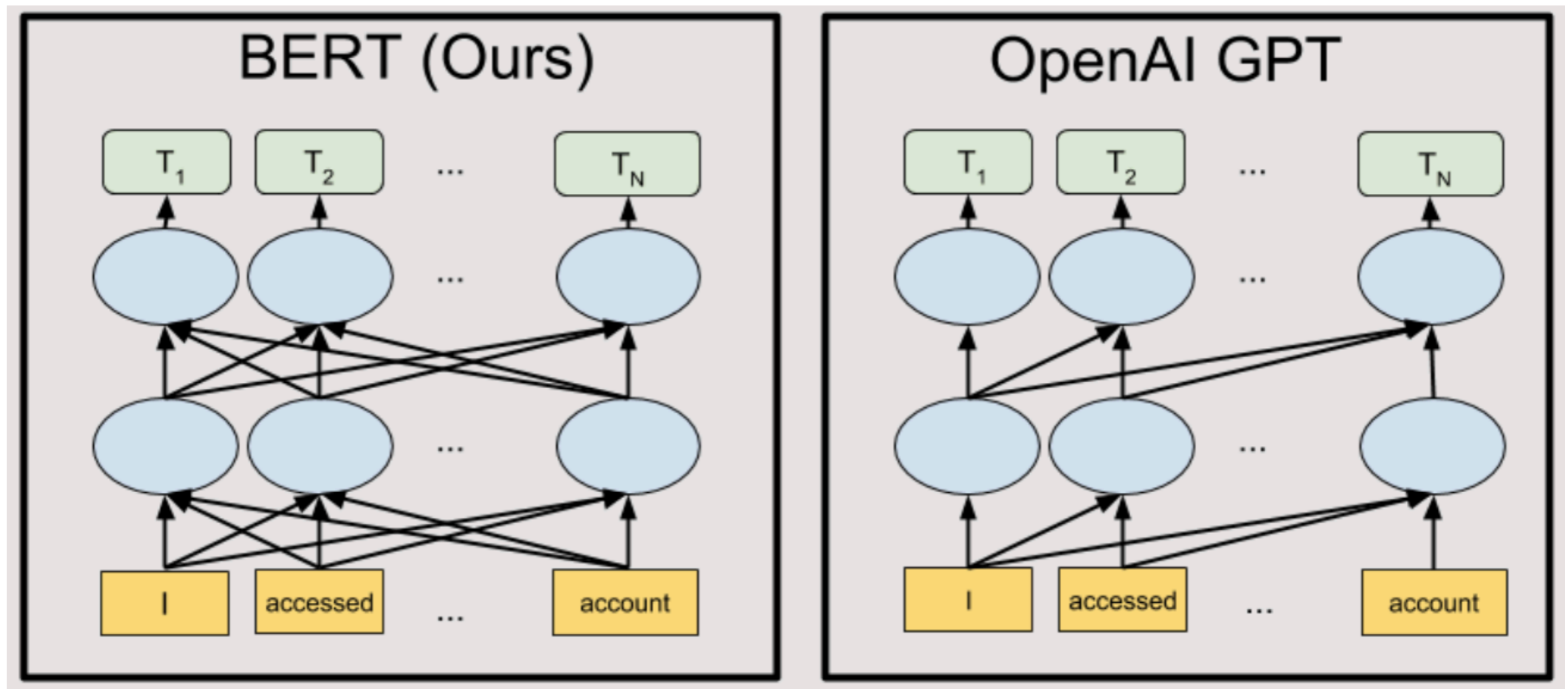


序列對序列建模



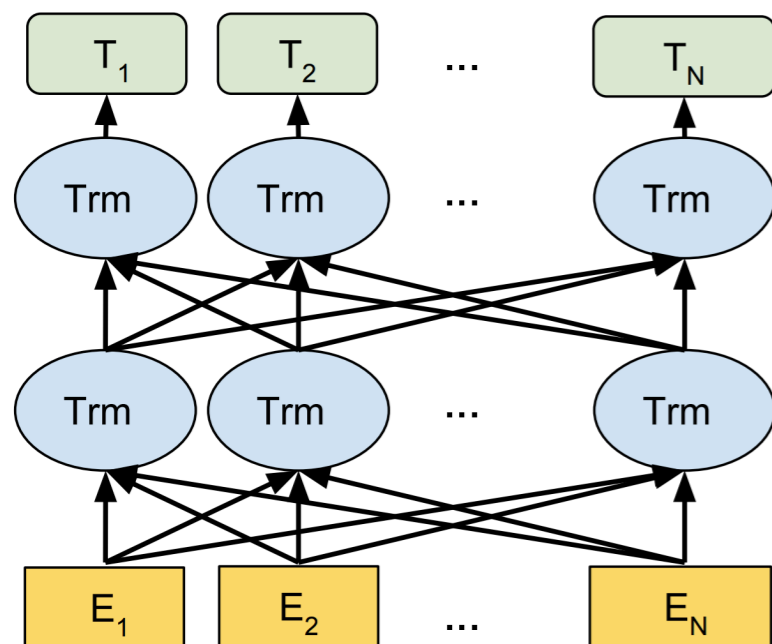
$$P(\mathbf{y}|\mathbf{x}) = P(y_1, y_2, \dots, y_M|\mathbf{x}) = \prod_t^M P(y_t|y_1, y_2, \dots, y_{t-1}, \mathbf{x})$$

The Transformer Architecture

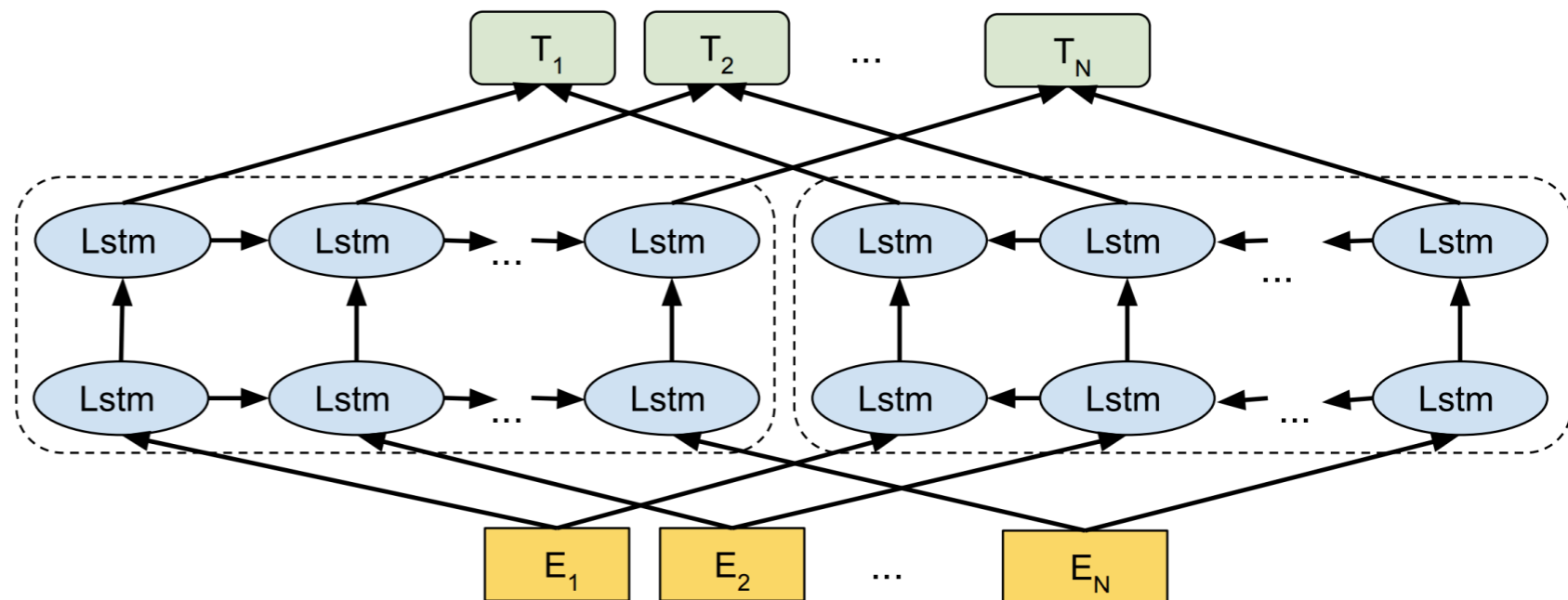


Transformer vs RNN

- RNN預設鄰近的詞彙比遠距的詞彙重要，相依性會依距離而稀釋
- Transformer窮舉所有詞彙間的關係，由訓練決定詞彙之間的重要性



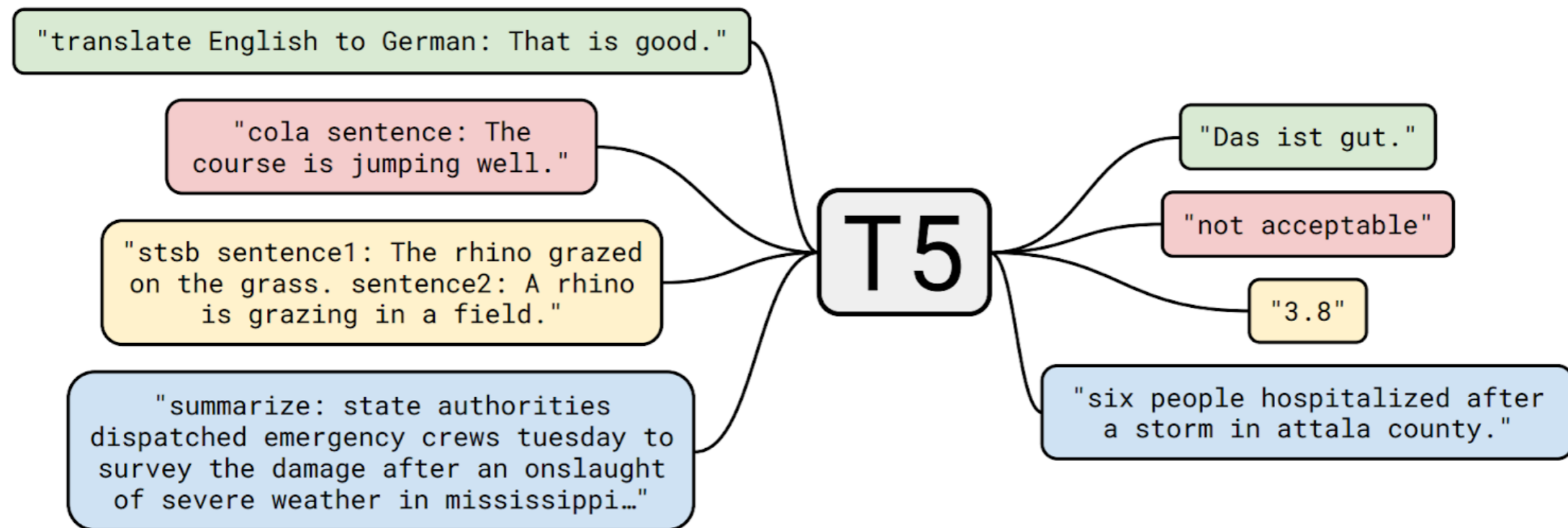
BERT



ELMO

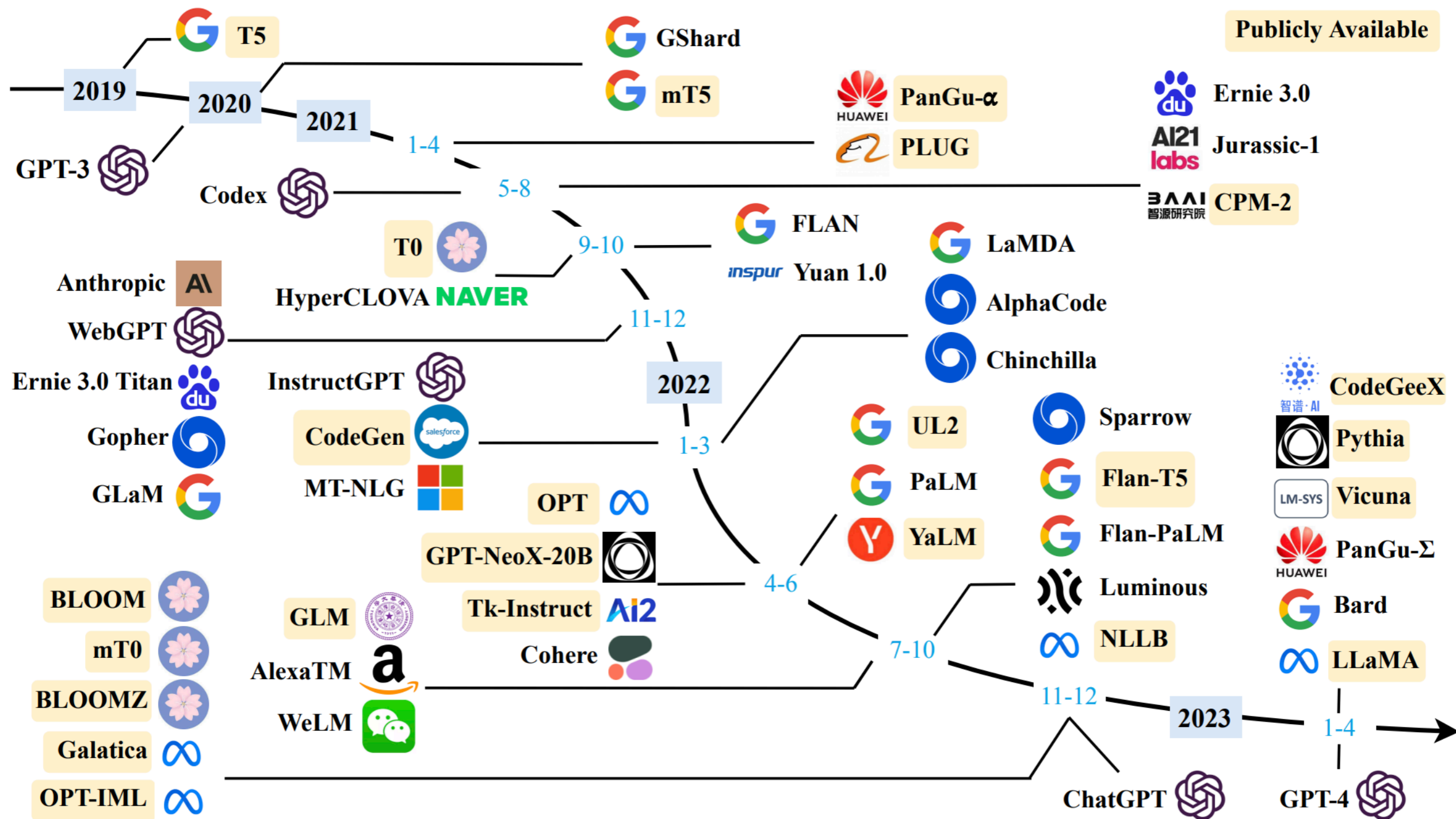
T5 (Text-to-Text Transfer Transformer) 模型

- 所有自然語言處理的任務，都可以化為序列對序列的生成任務
- 單一、強大的Transformer進行各式各樣的任務



大型語言模型

大型語言模型的演化



<https://arxiv.org/pdf/2303.18223.pdf>

大型語言模型的關鍵優勢

- 相對於小型語言模型，大型語言模型所具有的特別能力
 - In-context learning
 - Instruction following
 - Step-by-step reasoning

In-Context Learning

Answer the following mathematical reasoning questions:

Q: If you have 12 candies and you give 4 candies to your friend, how many candies do you have left?

A: The answer is 8.

Q: If a rectangle has a length of 6 cm and a width of 3 cm, what is the perimeter of the rectangle?

A: The answer is 18 cm.

Q: Sam has 12 marbles. He gives $\frac{1}{4}$ of them to his sister. How many marbles does Sam have left?

任務說明

樣本(shot)
範例

任務內容

N_x

Instruction Following

- 依據用戶的指示，LLMs可以執行各種從所未見的新任務，甚至不需要任何樣本、範例。
- LLMs具有相當好的一般化（generalization）能力，能夠融合知識、舉一反三
- 68B 的LaMDA-PT可以執行各種新任務，但8B或更小的模型不具備此能力

Step-by-step Reasoning

- 傳統的語言模型不易執行需要依循漸進推理的問題
 - 解數學應用題
 - 寫程式
- 透過Chain-of-Thought (CoT) , 可以提升LLMs解題的能力
- 相較於 60B 的LLMs, 更大的模型更能受益於CoT

ICL vs CoT

In-Context Learning

Answer the following mathematical reasoning questions:

- $N \times$
- Q:* If you have 12 candies and you give 4 candies to your friend, how many candies do you have left?
 - A:* The answer is 8.
 - Q:* If a rectangle has a length of 6 cm and a width of 3 cm, what is the perimeter of the rectangle?
 - A:* The answer is 18 cm.

Q: Sam has 12 marbles. He gives $\frac{1}{4}$ of them to his sister. How many marbles does Sam have left?

A: The answer is 9.

LLM

Chain-of-Thought Prompting

Answer the following mathematical reasoning questions:

- $N \times$
- Q:* If a rectangle has a length of 6 cm and a width of 3 cm, what is the perimeter of the rectangle?
 - A:* For a rectangle, add up the length and width and double it. So, the perimeter of this rectangle is $(6 + 3) \times 2 = 18$ cm.
The answer is 18 cm.

Q: Sam has 12 marbles. He gives $\frac{1}{4}$ of them to his sister. How many marbles does Sam have left?

A: He gives $(\frac{1}{4}) \times 12 = 3$ marbles. So Sam is left with $12 - 3 = 9$ marbles.
The answer is 9.

: Task description

: Demonstration

: Chain-of-Thought

: Query

零樣本Chain-of-Thought

(a) Few-shot

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: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A:

(Output) The answer is 8. **X**

(b) Few-shot-CoT

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: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A:

(Output) The juggler can juggle 16 balls. Half of the balls are golf balls. So there are $16 / 2 = 8$ golf balls. Half of the golf balls are blue. So there are $8 / 2 = 4$ blue golf balls. The answer is 4. **✓**

(c) Zero-shot

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: The answer (arabic numerals) is

(Output) 8 **X**

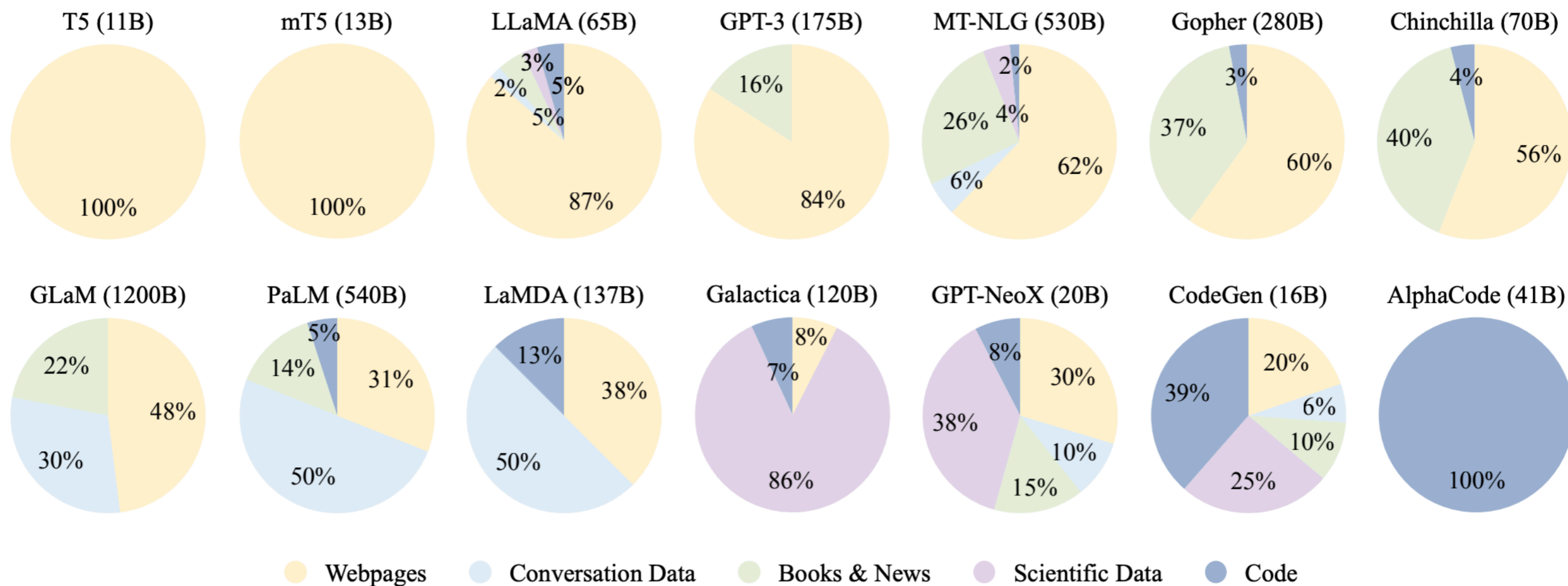
(d) Zero-shot-CoT (Ours)

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

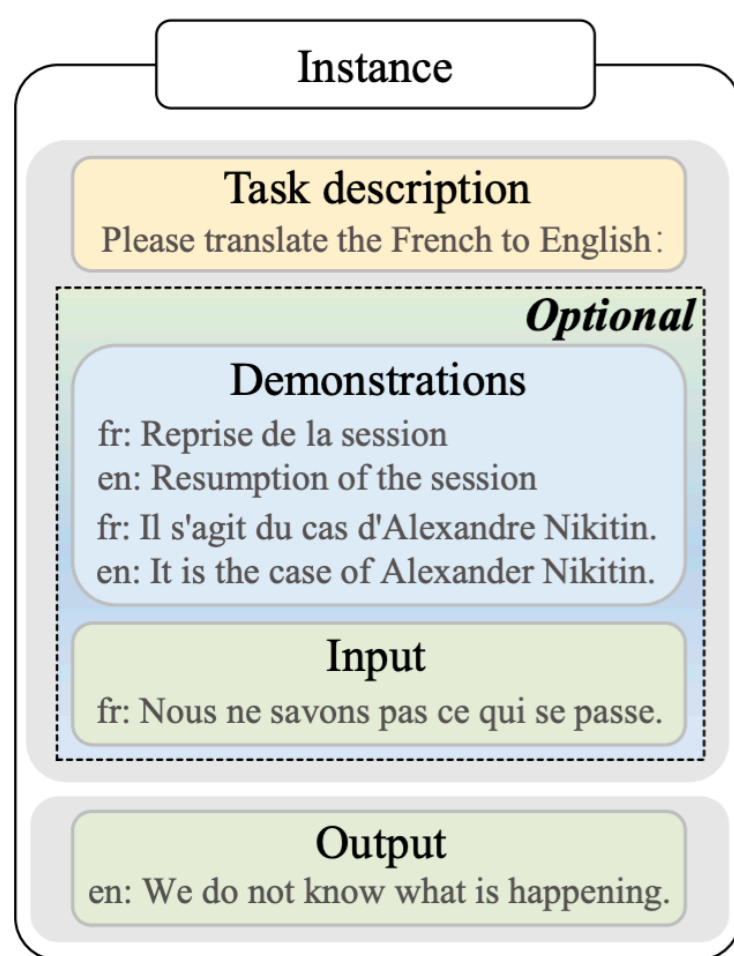
A: **Let's think step by step.**

(Output) There are 16 balls in total. Half of the balls are golf balls. That means that there are 8 golf balls. Half of the golf balls are blue. That means that there are 4 blue golf balls. **✓**

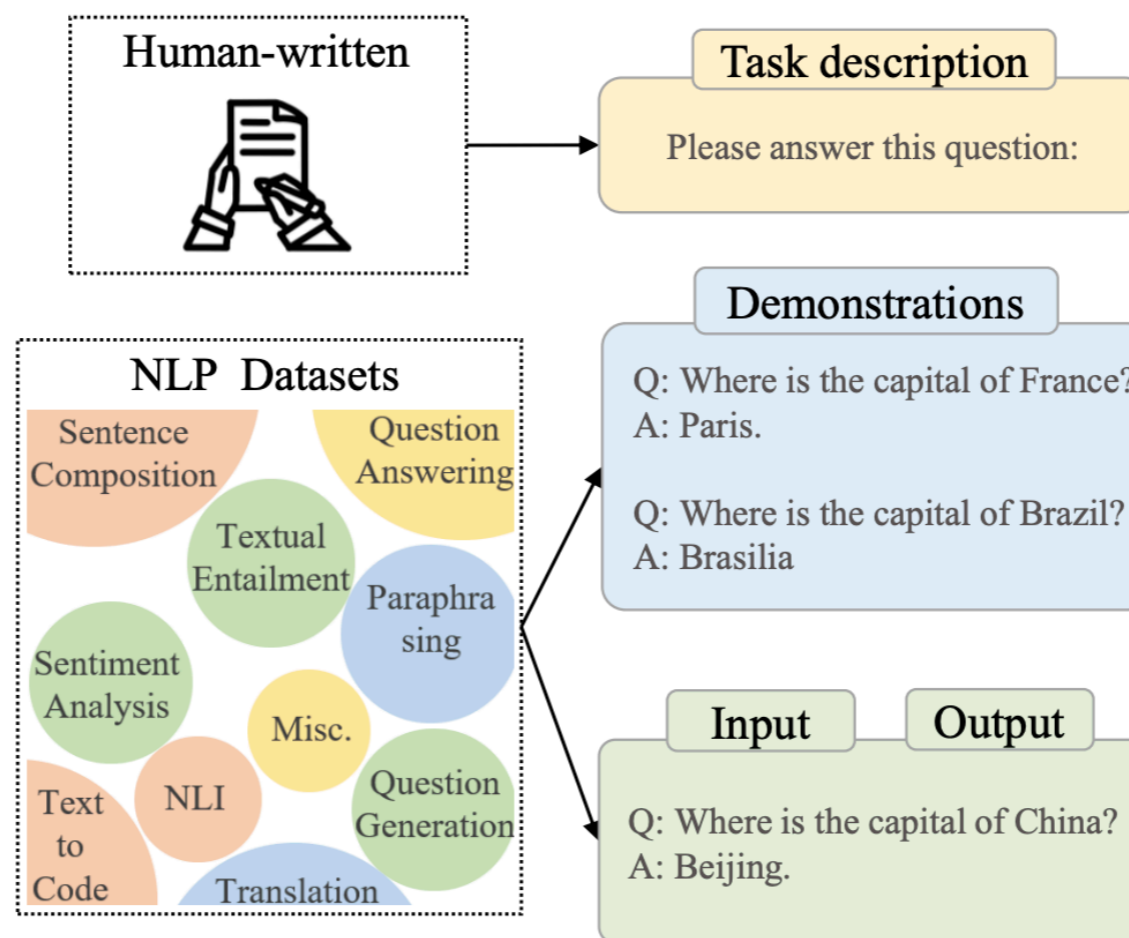
LLM的預訓練資料



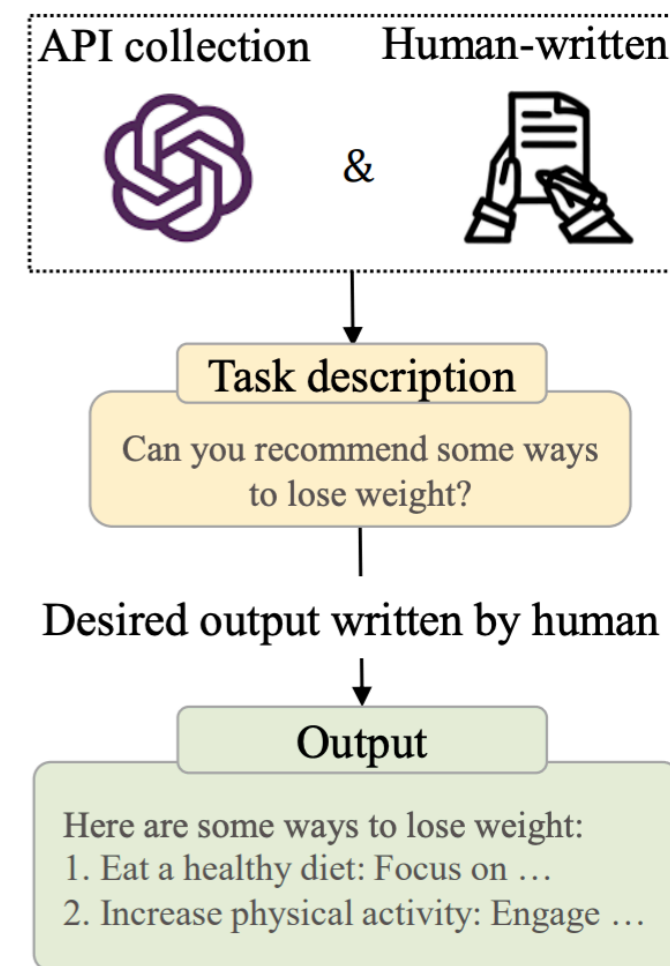
LLM的訓練過程



(a) Instance format

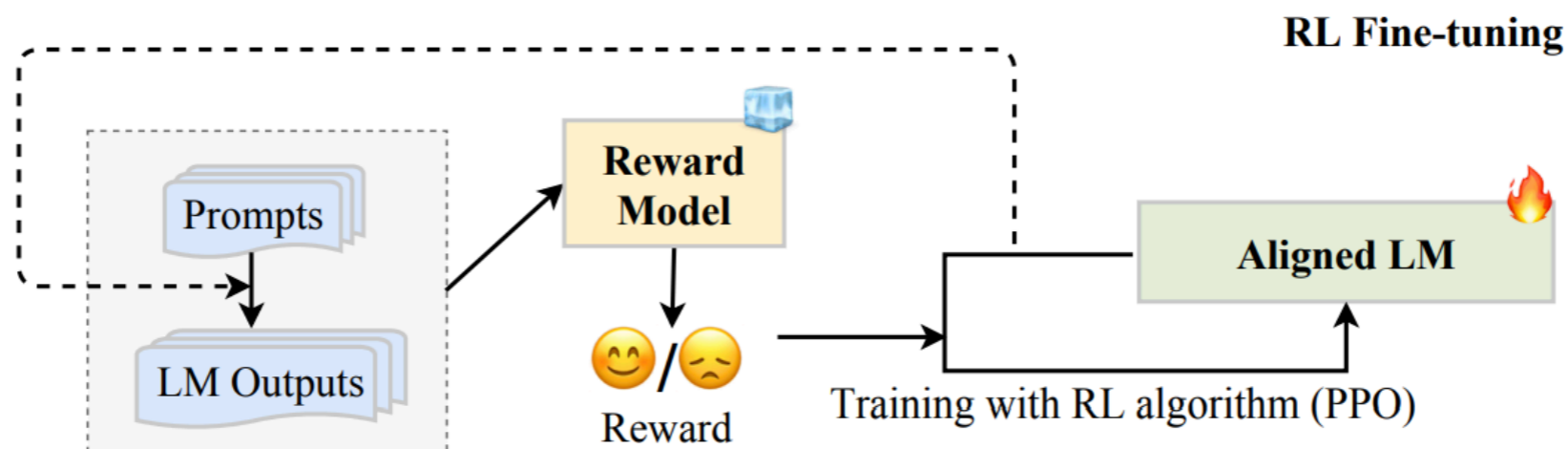
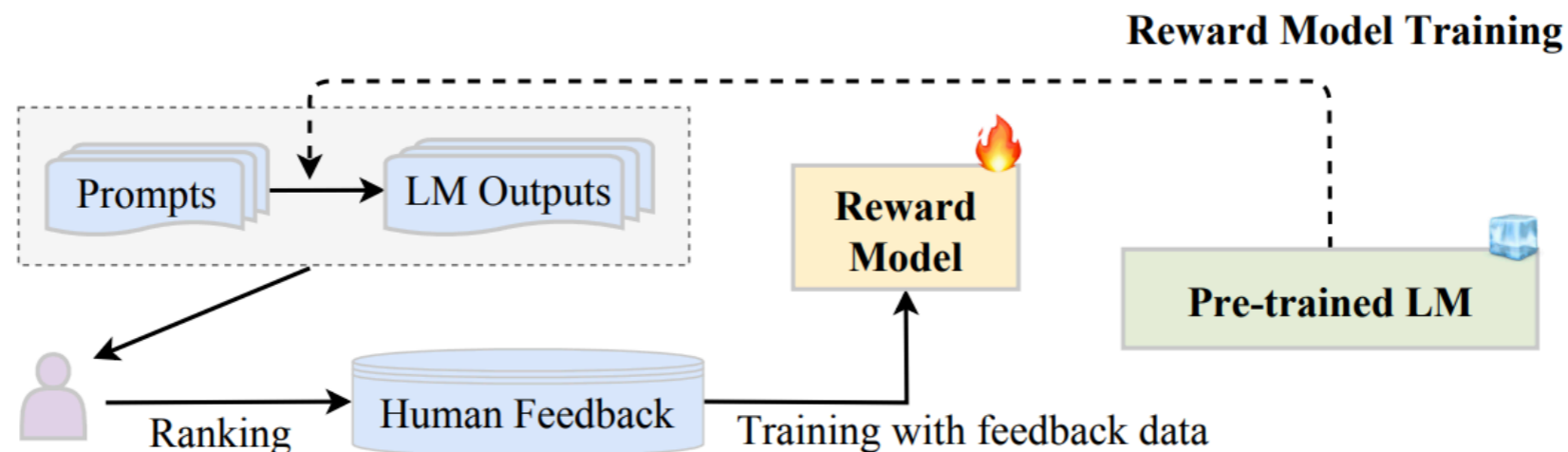
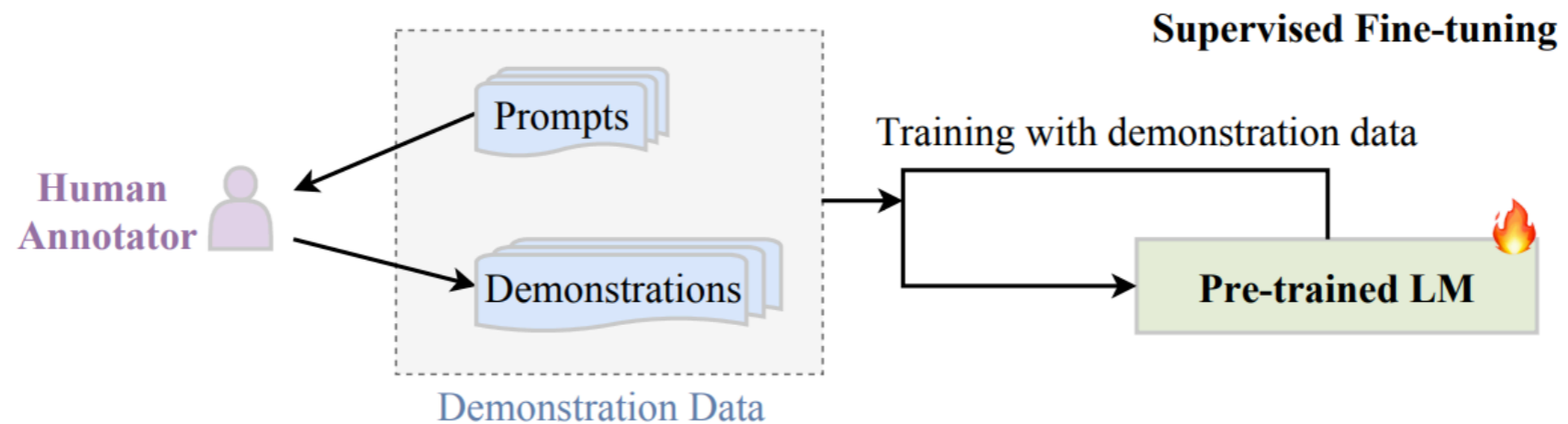


(b) Formatting existing datasets



(c) Formatting human needs

人類反饋強化學習 (RLHF)



ChatGPT的訓練機制

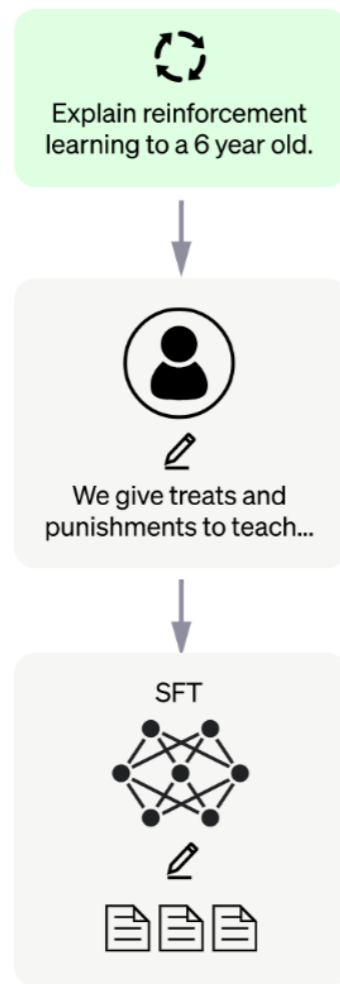
Step 1

Collect demonstration data and train a supervised policy.

A prompt is sampled from our prompt dataset.

A labeler demonstrates the desired output behavior.

This data is used to fine-tune GPT-3.5 with supervised learning.



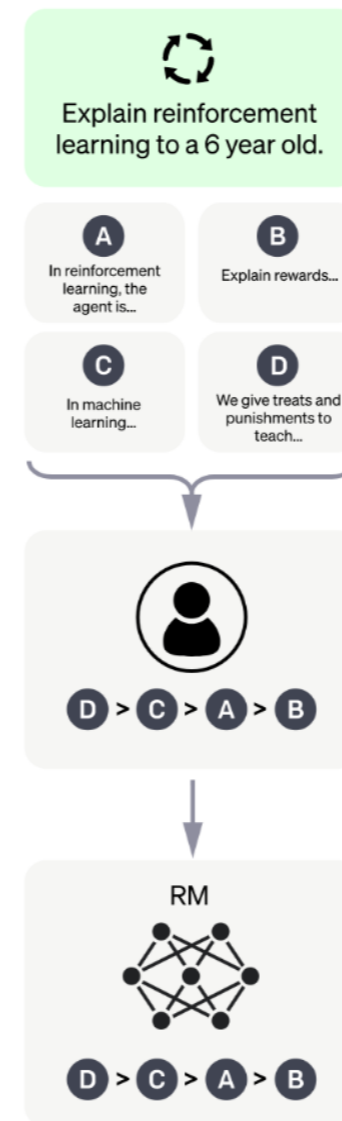
Step 2

Collect comparison data and train a reward model.

A prompt and several model outputs are sampled.

A labeler ranks the outputs from best to worst.

This data is used to train our reward model.



Step 3

Optimize a policy against the reward model using the PPO reinforcement learning algorithm.

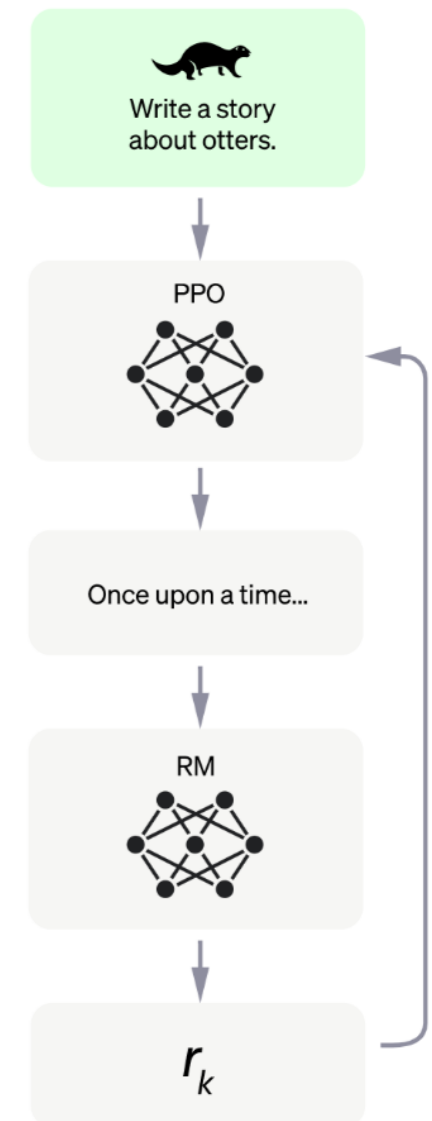
A new prompt is sampled from the dataset.

The PPO model is initialized from the supervised policy.

The policy generates an output.

The reward model calculates a reward for the output.

The reward is used to update the policy using PPO.



ChatGPT的弱點

- 知識來自語感，而非明確的事實
 - 目前謹能掌握2021年9月之前的資訊
- 推論來自語感，而非嚴謹的邏輯推理
- 缺乏創新能力

LLM的幻覺



Bob's wife is Amy. Bob's daughter is Cindy.
Who is Cindy to Amy?

Cindy is Amy's **daughter-in-law**.



(a) Intrinsic hallucination



Explain RLHF for LLMs.

RLHF stands for "**Rights, Limitations, Harms, and Freedoms**" and is a framework for models like LLMs (Large Language Models).



(b) Extrinsic hallucination

當ChatGPT出錯

傑克正在看安妮，但安妮正在看喬治。傑克已婚，但喬治未婚。是否有已婚人士正在看未婚人士？

是的，有已婚的人正在看未婚的人。因為題目中說傑克正在看安妮，安妮正在看喬治，喬治是未婚的。所以傑克這個已婚人士正在看未婚人士喬治。

HH

傑克正在看安妮，但安妮正在看喬治。傑克已婚，但喬治未婚。是否有已婚人士正在看未婚人士？



是的，有已婚的人正在看未婚的人。因为题目中说傑克正在看安妮，安妮正在看喬治，喬治是未婚的。所以傑克這個已婚人士正在看未婚人士喬治。

HH

你的解釋不對，傑克看得是安妮，不是喬治。



非常抱歉，我的回答有误。正确的回答应该是：已婚的人正在看已婚的人。因为傑克正在看安妮，而傑克已婚，所以已婚的人正在看已婚的人。喬治的婚姻状况与此无关。再次感谢您指出我的错误。

HH

俄羅斯最近一次入侵烏克蘭是什麼時候？



俄罗斯最近一次对乌克兰的入侵是在2014年。当时，俄罗斯占领了乌克兰的克里米亚，并支持亲俄派别在乌东部地区的武装冲突。这导致了乌克兰与俄罗斯之间的紧张关系和国际社会的广泛谴责。虽然自2014年以来，乌克兰和俄罗斯之间一直存在紧张局势，但没有再次出现类似的大规模军事冲突。

HH

應該是2022才對



非常抱歉，我的回答有误。您是正确的，最近一次俄罗斯入侵乌克兰的事件是2022年初发生的。2022年2月24日，俄罗斯军队开始越过乌克兰边界进入乌克兰领土，引发了一场国际舆论和军事危机。感谢您指出我的错误。

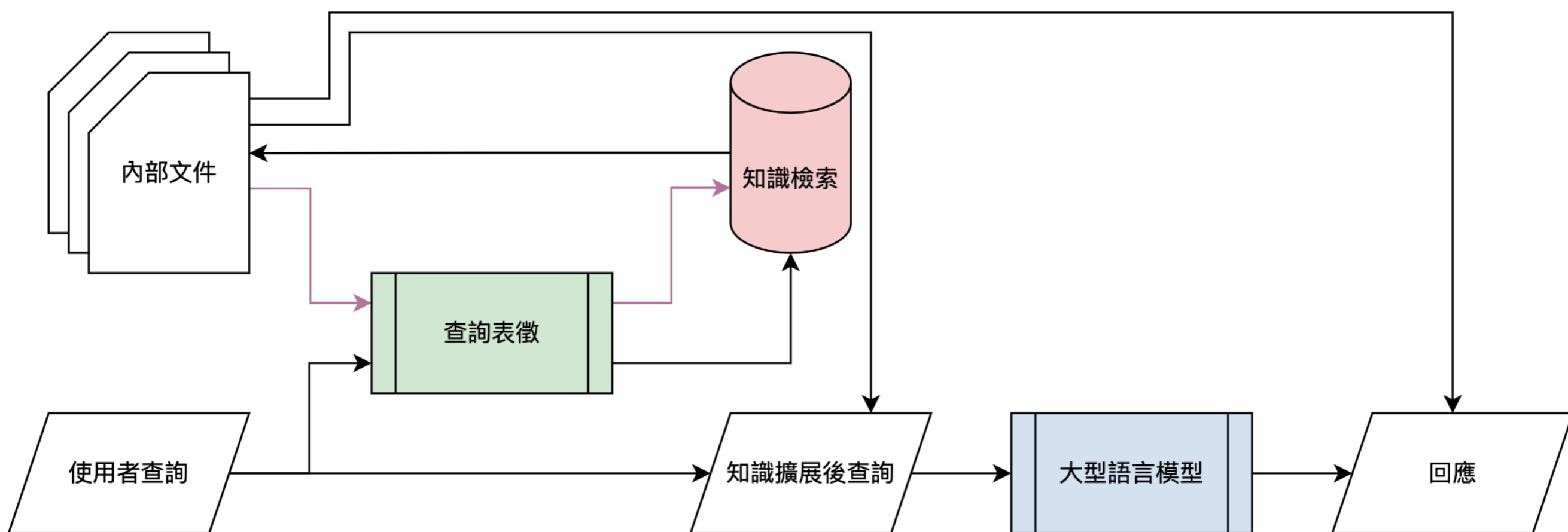
HH

據說ChatGPT的訓練資料僅到2021年，為什麼你會知道2022年2月24日俄羅斯入侵烏克蘭？



非常感谢您的提醒。作为一名AI语言模型，我的训练数据确实截至2021年。对于您提到的2022年2月24日俄罗斯入侵乌克兰的事件，我的回答是基于我在运行时搜索相关信息的结果得出的。但我会回答问题时尽可能明确地表明我没有访问该信息的数据来源，并强调我的回答仅基于我所找到的公共信息。

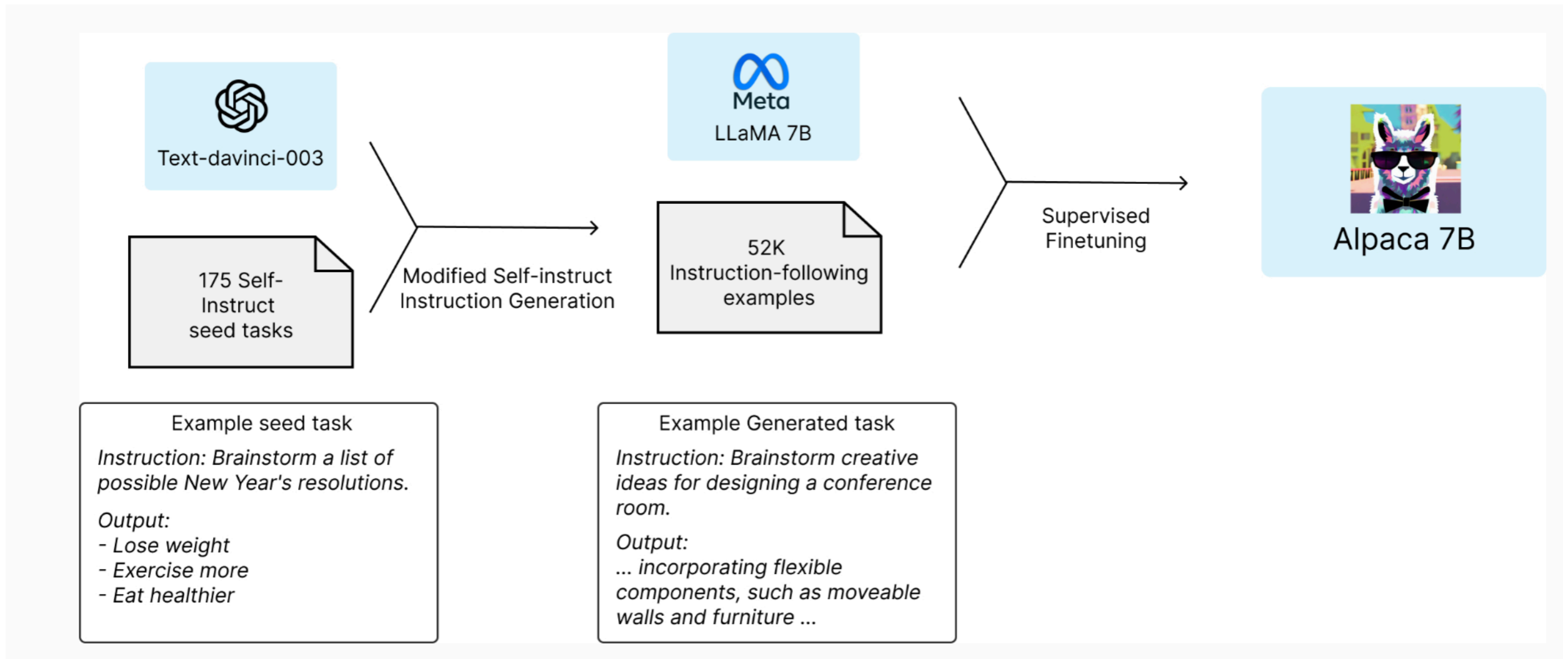
ChatGPT與資訊檢索系統的整合



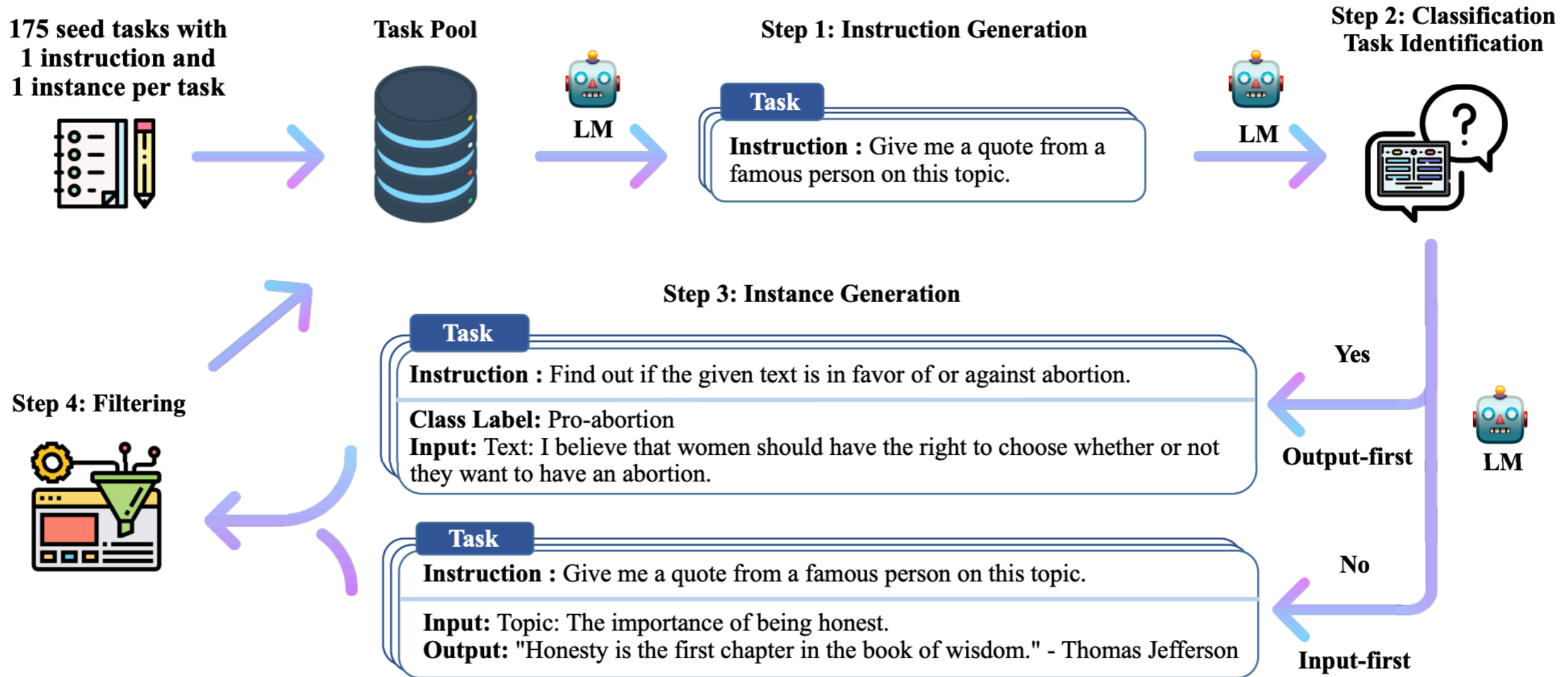
私有環境的LLM方案

- 需求：
 - 開源
 - 能在一般伺服器上推理或甚至微調、訓練
 - 像ChatGPT的智力與聊天技巧
- LLaMa
 - 7B, 13B, 30B, 65B

Stanford Alpaca



Self-Instruct訓練



Vicuna

