



# 人工智能的基本技術、發展趨勢及應用

Basic Technologies, Development Trends and Applications of Artificial Intelligence



## CONTENTS

### PART I

01. 人工智能 (AI) 發展與歷史

02. 關鍵技術與硬體推手

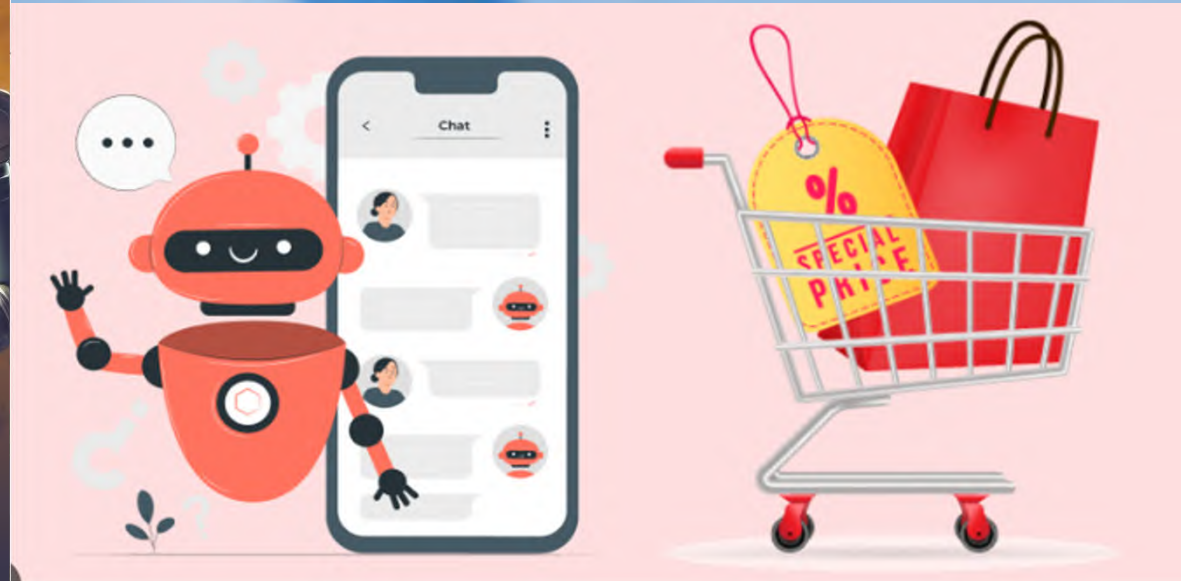
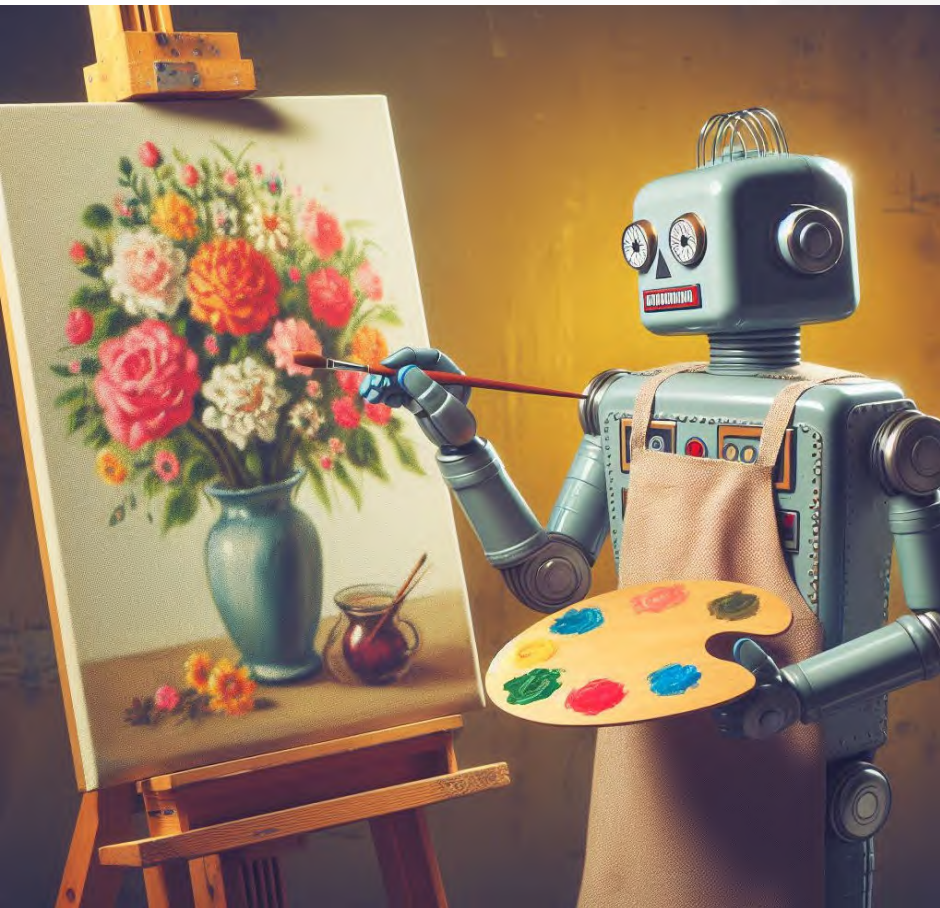
03. 大語言模型與生成式 AI

04. 風險與行政應用

### PART II

實作練習







# 01

## 人工智能 (AI) 發展與歷史



# 人工智能的定義與核心特徵

人工智能旨在模擬人類智慧，具備學習、推理、感知與語言理解能力，其核心特徵為**自動化、適應性與推理能力**。



## 自然語言處理

理解、解釋和生成人類語言

。



## 計算機視覺

使機器能“看”懂圖像和視頻。



## 機器人

設計能自動執行任務的機器

。



## 自動駕駛

實現車輛的自主導航與駕駛

。



## 人工智能之父

# 元艾倫・圖靈 Alan Turing

話說這位圖靈呢，可真是個數學小天才，喜歡解決各種複雜的難題，還很熱愛思考困難的棋局。他曾經提出「圖靈機」的概念，啟發後人打造出第一部通用型計算機。

1950 年，圖靈發表了一篇文章〈Computing machinery and intelligence〉，並在其中問出了關於人工智慧的關鍵問題：「電腦會不會思考？」

This is only a foretaste of what is to come,  
and only the shadow of what is going to be.

這不過是將來之事的前奏，也是將來之事的影子。

—— Alan Mathison Turing (1912-1954)

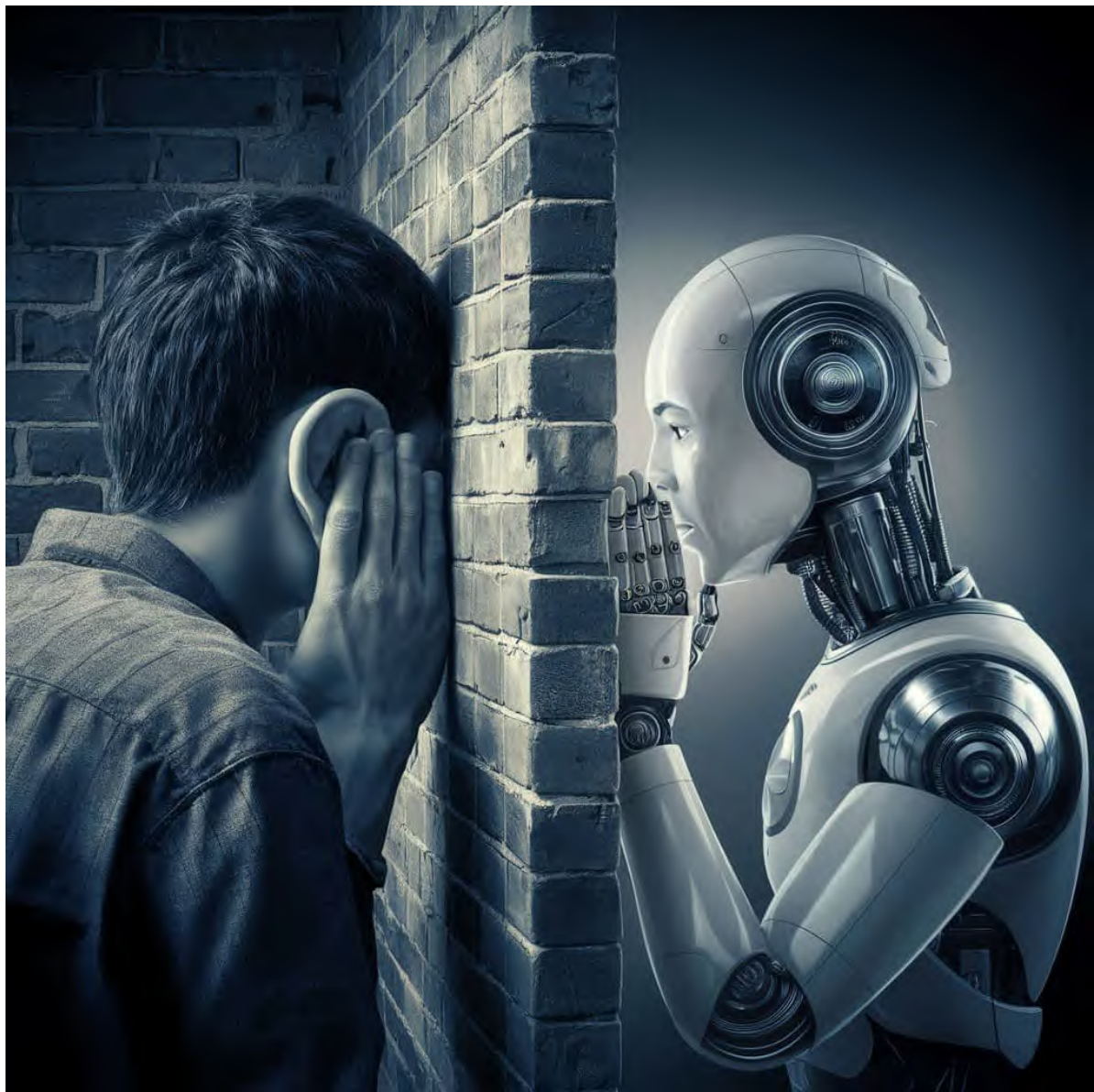
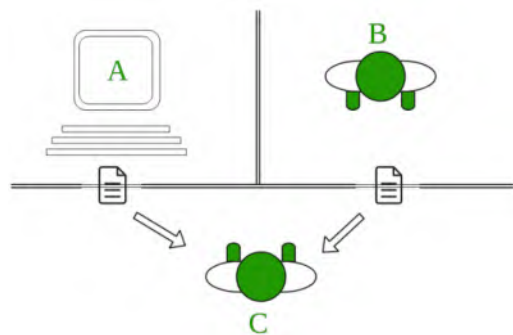
艾倫圖靈



# 人工智能之父

## Turing Test

「圖靈測試」（Turing Test）用來判斷機器是否具備與人類無異的智慧。



1956 Dartmouth Conference:  
The Founding Fathers of AI



John McCarthy



Marvin Minsky



Claude Shannon



Ray Solomonoff



Alan Newell



Herbert Simon



Arthur Samuel



Oliver Selfridge



Nathaniel Rochester



Treuskart More

## 1956 達特茅斯會議 啟動 AI 元年

1956年，達特茅斯會議首次提出“人工智能”一詞，標誌著該學科的誕生。早期研究者樂觀預言，十年內可實現人類級別的智慧，並奠定了符號主義與邏輯推理的研究路線。

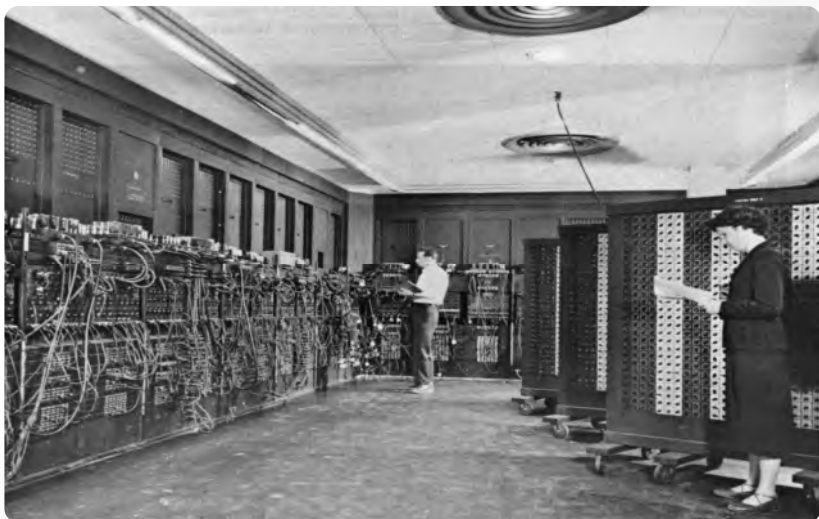




## 1956 達特茅斯會議

1. 正式命名：它賦予了「人工智慧」這個領域一個明確的身份和名稱。
2. 確立目標：提出了用機器類比人類智慧這個巨集偉的研究綱領。
3. 凝聚力量：它聚集了AI領域的“創始團隊”。
4. 注入樂觀：出席者普遍相信，製造出具有人類水準智慧的機器！



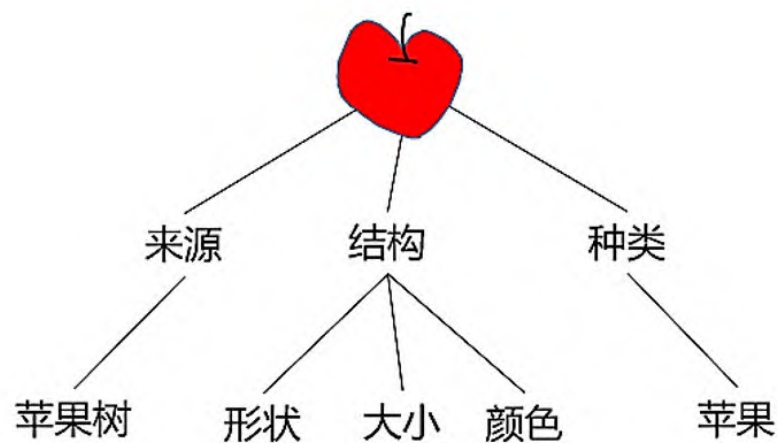


1950 – 1960  
符號邏輯 – 由專家寫下決策

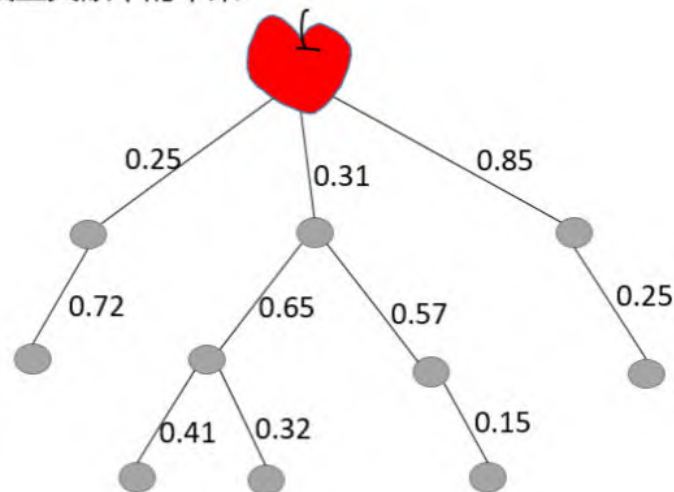
*人未清楚自己如何懂得思考, 如何教電腦?*

1980 -1990  
專家系統 – 由專家寫下經驗規則

*太多沒有答案, 無法寫下規則*



连接主义眼中的苹果



# 兩次 AI 寒冬與反思



## 第一次寒冬 (1970s)

因計算力不足與期望落差，資金撤出，專家系統和LISP機走向衰落，研究陷入停滯。



## 第二次寒冬 (1980s)

由日本政府在1982年啟動，計劃耗資數十億美元、Prolog語言的新一代計算機。但並未製造出能夠商業化、撼動市場格局的“第五代計算機”。專家系統維護成本高、泛化能力弱，再次導致投資減少。

儘管遭遇挫折，AI研究在寒冬期轉向知識工程與專家系統，為後續機器學習的發展積累了寶貴的經驗。



專家系統的核心思想嗎 —— “知識就是力量！ “怎麼獲取知識？ 靠知識工程師去「拷問」人類專家，把他們的經驗總結成一條條IF-THEN規則，然後輸給機器。 這種“知識驅動”的方法，本質上還是人類在給機器“程式設計”，只不過程式設計的內容是“規則”而不是具體的執行步驟。

機器學習則換了個活法 —— “數據就是燃料！” 不再大量寫法則喂給機器，直接給機器看大量的數據（例子），讓機器自己從數據中學習規律和模式。



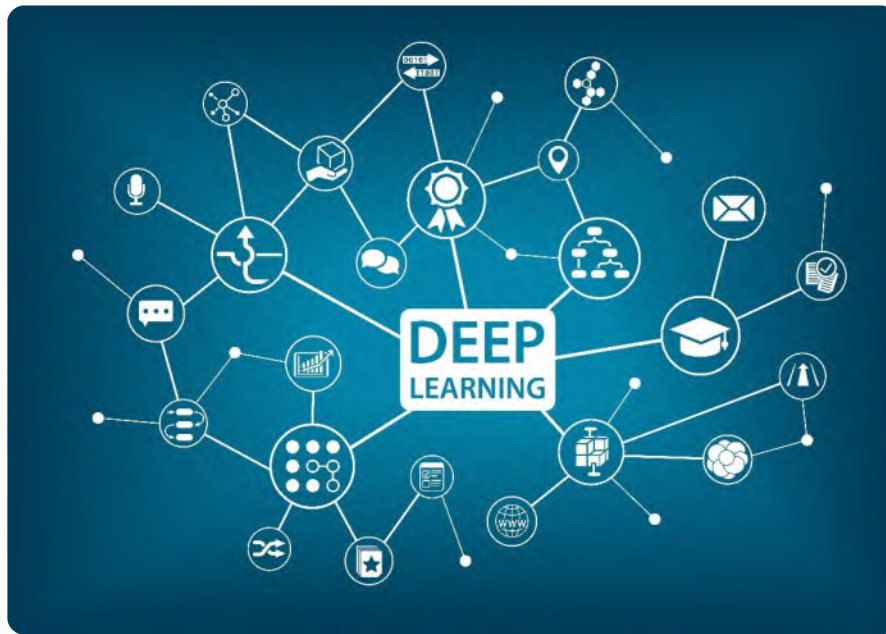


# 1997年 世紀對決：「深藍」 vs. 卡斯帕羅夫

從1997年5月11日，IBM 深藍計算機打敗了當時世界國際象棋冠軍加里·卡斯帕羅夫，這成為了載入史冊的歷史性事件。2017年，圍棋領域的AlphaGo也即將與世界排名第一的圍棋選手柯潔對戰，卡斯帕羅夫也出版新書《深度思考：人工智慧的終點，就是人類創造力的起點》（Deep Thinking: Where Artificial Intelligence Ends and Human Creativity Begins），回顧「人類VS機器」的20年歷程。作為「被機器打敗」的親歷者，卡斯帕羅夫對於「人類工作被機器取代」這一議題發表了深刻而樂觀的見解，他認為人工智慧將會取代一部分人的工作，這一趨勢無法逆轉，但是機器能幫助人類过上更富有創造性和愉悅的精神生活。



# AI 發展轉捩點



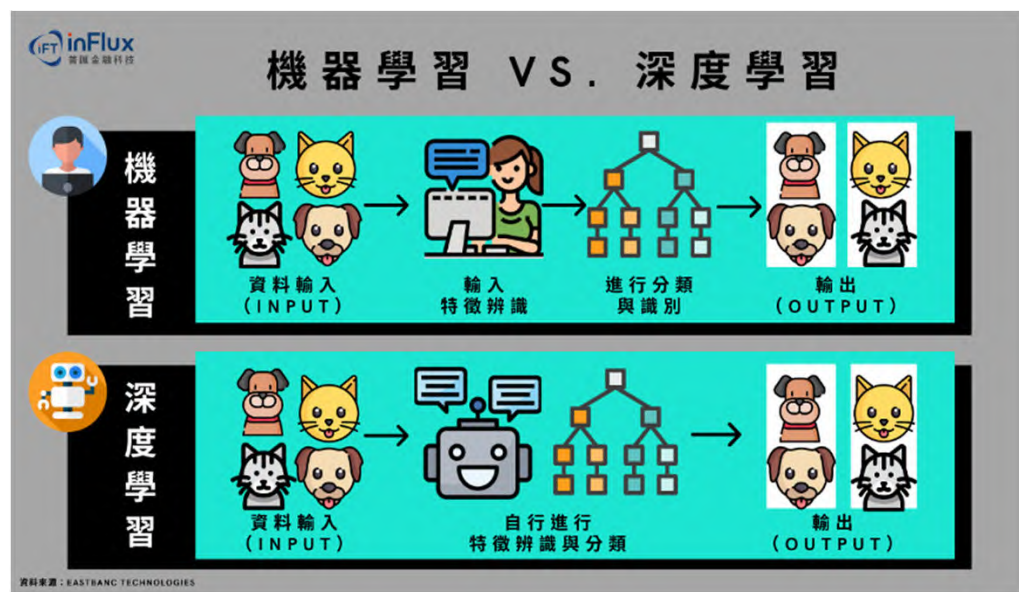
# 深度學習 (Deep Learning)

讓AI 通過學習數據來解決實際問題。引發出「深度學習」。

## 深度學習 (Deep Learning) !

究竟是什麼解開了「深度」的魔咒？為什麼那個曾經「老大難」的訓練問題，突然之間就不再是不可逾越的天塹了？

答案是集「**天時、地利、人和**」— **海量的數據 (Big Data)**、**強大的算力 (Big Compute)**、以及改進的演算法 (**Better Algorithms**) !



## AI 發展轉捩點

**深度學習**  
**(Deep Learning)**  **神經網絡**  
**(Neural Network)**



## 多層的第一層

深度學習第一層  
基本特徵識別

輸入圖像



第一層神經網絡



識別出的基本特徵



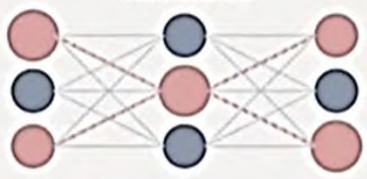
## 多層的中間層

深度學習中間層  
複雜特徵識別

從第一層傳來的基本特徵



中間層神經網絡



識別出的複雜特徵



中間層學習更複雜、有意義的特徵組合

## 多層的最後層

深度學習最後一層  
綜合分析與判斷

從中間層傳來的複雜特徵



神經網絡最後一層



綜合所有資訊，得出判斷結果



深度學習的核心，就是使用很多層的人工神經網路。

## 2012: 深度學習的黎明

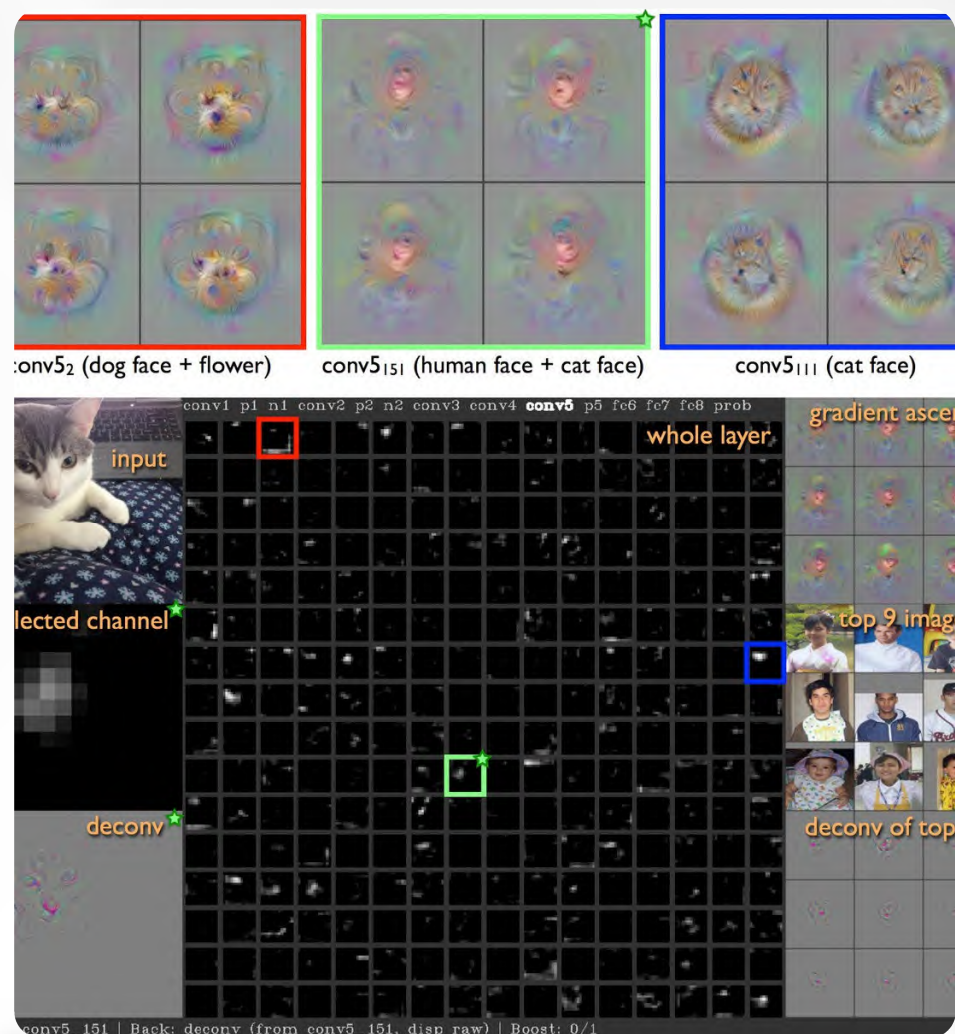
# ImageNet 突破

Alex Krizhevsky等人發表的論文《ImageNet Classification with Deep Convolutional Neural Networks》及其所提出的 AlexNet模型。

AlexNet在當年的ImageNet大規模視覺辨識挑戰賽（ILSVRC）中以巨大的優勢奪冠，證明了深度卷積神經網路在圖像分類上的卓越能力，掀起了深度學習在電腦視覺領域的革命。

開啟了**深度學習的黃金時代**。

- ✓ 視覺任務性能飛躍
- ✓ 語音、文本任務全面受益
- ✓ 學術界與產業界廣泛投入





2016: 決策智慧的里程碑

## AlphaGo 戰勝李世石

AlphaGo 結合深度神經網路與蒙地卡羅樹搜索，在圍棋的龐大複雜度中，以 4:1 戰勝世界冠軍，證明瞭強化學習與自我對弈可達 超人級決策。

“這場勝利激發了全球對 AI 的熱情與投資，證明瞭 AI 在複雜策略領域的巨大潛力。”





# 02

關鍵技術與硬體推手





## AI 發展轉捩點

**深度學習**  
(Deep Learning) **+** **神經網絡**  
(Neural Network)



具有識別能力 但不能溝通  
？ AI 語言理解能力極度有限

# 2017: Transformer 顛覆序列建模

Google 提出的 Transformer 架構，以自注意力機制取代遞歸，為大語言模型奠定了基礎。



## 告別遞歸

解決了 RNN 序列處理慢、長距依賴難以捕捉的瓶頸。



## 並行計算

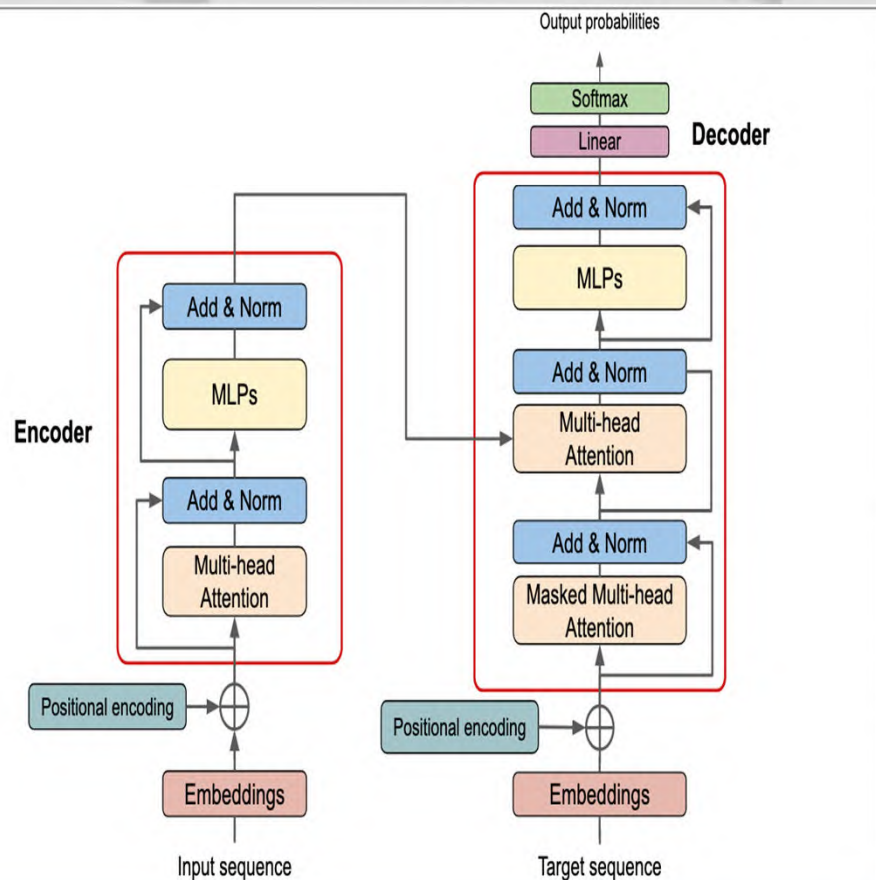
允許模型並行處理序列，極大提升了訓練效率。



## 奠基未來

直接催生了 BERT、GPT 系列，開啟了預訓練時代。

# Transformer AI模型



1. 「她把牛奶倒進碗裡，直到它滿了為止。」

↪ 句子中的「它」指的是「碗」，但若是在以下的句子中卻會出現不同的含義：

2. 「她把牛奶倒進碗裡，直到它空了為止。」

↪ 在這個句子中，「它」這次代表了「牛奶（瓶）」

這種語意上的差異，對人類來說幾乎是直覺理解，但對傳統模型來說卻是一大挑戰。

而 Transformer 模型的設計加入了「自我注意力機制（Self-Attention Mechanism）」，模型在處理「它」時，還會同時注意整句話中出現過的詞，並根據語境判斷出最合理的指涉對象。





# 深度學習三駕馬車

深度學習的突飛猛進依賴於三大支柱的協同發展。



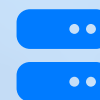
## 演算法

CNN, RNN, ResNet 等網路結構  
不斷演進。



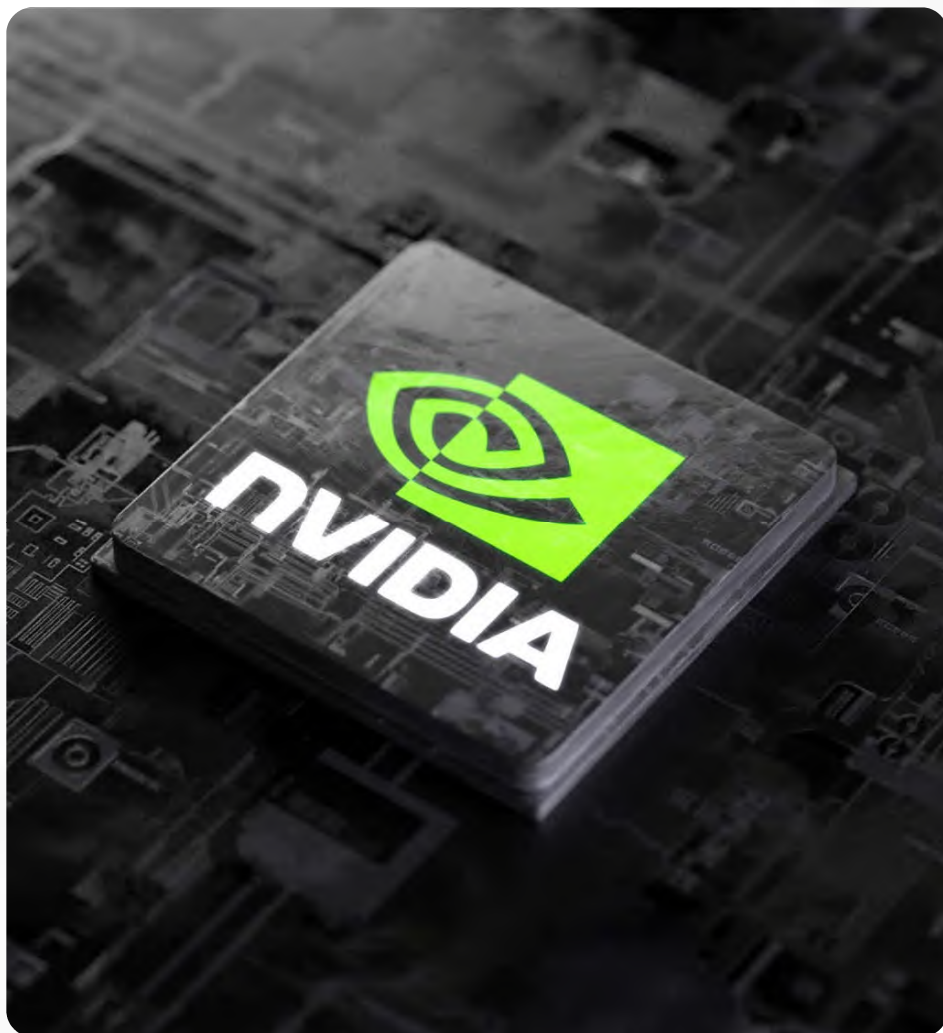
## 大數據

ImageNet, Common Crawl 等  
海量數據集提供燃料。



## 高算力

GPU 叢集與分散式框架大幅降  
低訓練週期。



## NVIDIA GPU 加速 AI 運算

NVIDIA 的 GPU 從圖形渲染轉向通用運算，成為推動 AI 發展的硬體基石。

### CUDA 平行架構

讓數千個核心並行處理 AI 所需的矩陣運算。

### Tensor Core

專為深度學習的矩陣乘加 (MMA) 運算優化。

### NVLink 高速互連

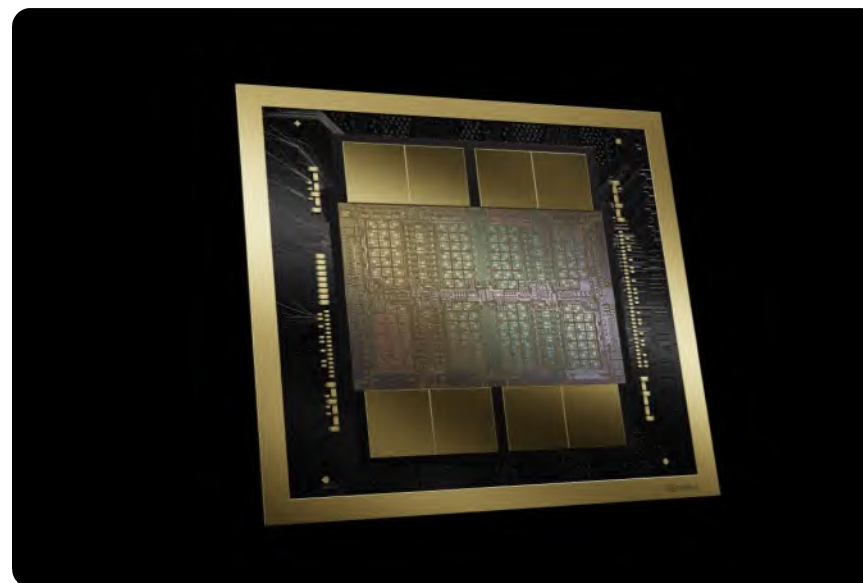
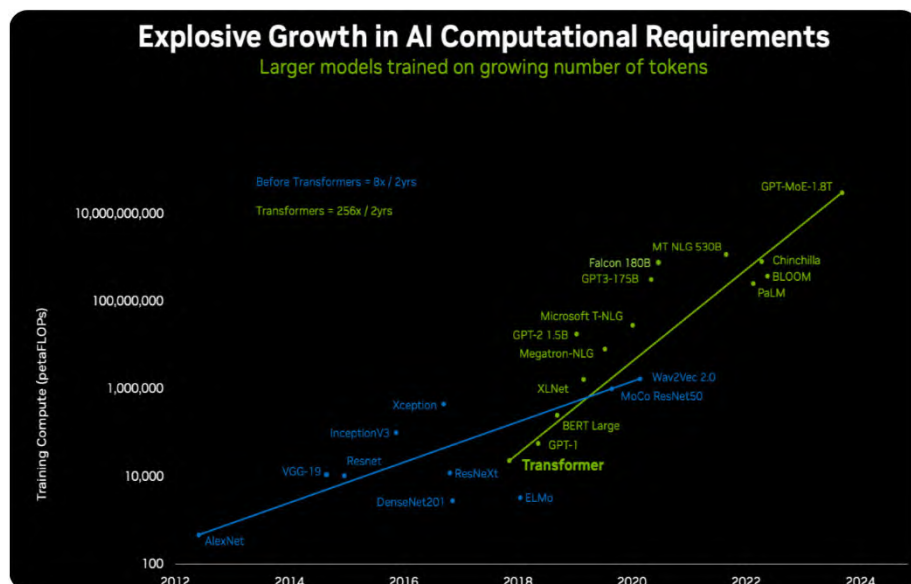
將訓練千億級模型的時間從月縮至天。

Google 團隊在 2017 年 NeurIPS 大會上提出的論文中，描述了他們的 Transformer 模型，以及它在機器翻譯方面創造的準確性紀錄。

在多項技術的協助下，他們僅使用 3.5 天即在 8 個 NVIDIA GPU 上訓練出模型，花費的時間和成本還不到先前訓練模型的一小部分。他們使用包含多達 10 億筆單字的資料集訓練模型。

能建立更好、更大的模型，NVIDIA 不斷推出更新的 GPU，內含一個 Transformer Engine 提供這些模型需要的運算能力。

### New Nvidia Blackwell B200 GPU





# 03

大語言模型與生成式 AI





# 甚麼是大語言模型 (LLM)?

## LLM 運作根本依據

	神經網路 Neural Network	深度學習 Deep Learning	Transformer 模型
含義	模仿人腦的架構，用來處理輸入與輸出資料	使用「多層神經網路」來學習資料特徵的方法	專門用來處理語言資料的深度學習架構
本質	架構	方法	架構
重點	模仿神經元傳遞訊號，進行分類或預測	自動從大量資料中學出特徵，減少人工設計	藉由注意力機制，理解詞與詞的關係
用途例子	情緒分類、手寫數字辨識等簡單任務	圖像辨識、語音辨識、語言模型訓練	ChatGPT、Gemini 等語言 AI 的核心架構
相對關係	是最基本的單位與基礎結構	是神經網路的進化與應用方式	一種更先進的深度學習架構，專門處理語言問題

# AI 發展轉捩點 – ChatGPT誕生

**深度學習**  
(Deep Learning)  **神經網絡**  
(Neural Network)  **Transformer**  
**模型**



**2022 年 11 月 OpenAI 發表 ChatGPT  
基於 GPT-3.5 LLM 模型的聊天機器人**

ChatGPT - Chat Generative Pre-Trained Transformer

ChatGPT 推出不到 2 個月的時間，用戶數已超過 1 億人。

# GenAI 的運作原理

GenAI 的核心是一個“學習後生成”的過程，通過預測最可能的下一個元素來創造內容。



## 1. 預訓練 (學習) (Pre-training)

從海量數據中學習語言、圖像等內容的統計分佈和模式。



## 2. 對齊 (調優) (Fine-tuning)

通過微調和 RLHF，使模型輸出更符合人類的指令和偏好。



## 3. 生成 (創作)

根據輸入提示，迭代預測並生成連貫、高品質的內容。









# 04

## 風險與行政應用



# GenAI 的安全性與私隱挑戰



## 幻覺與偏見

模型可能生成看似合理但虛假或帶有社會偏見的內容。



## 數據私隱

訓練數據若含個人信息，存在被模型記憶並洩露的風險。



## 對抗攻擊

精心設計的輸入（對抗樣本）可欺騙模型，使其輸出錯誤結果。



## 監管與治理

如何建立有效的政策框架，確保技術被負責任地開發和使用。

# 行政工作上的 GenAI 應用 場景



撰寫公文、會議紀錄與摘要



提供即時、高品質的多語言翻譯服務








建立對話式知識庫，快速回應內部查詢



智能填表與數據審核，減少重複勞動



# 未來應用場景

-  個人化 AI 助理：提供全方位、主動式的個人 (如自駕) 及工作支持。
-  即時多語同傳：打破語言障礙，實現無縫的全球化溝通。
-  自主程式碼生成：從需求到部署，AI 自動完成軟體開發與維護。
-  科學研究助手：自動綜述文獻、生成假設，加速科學發現。
-  智慧機器人：結合 LLM 與機器人，實現自然語言指揮的實體智能。







# 05

## 頂尖模型與未來展望

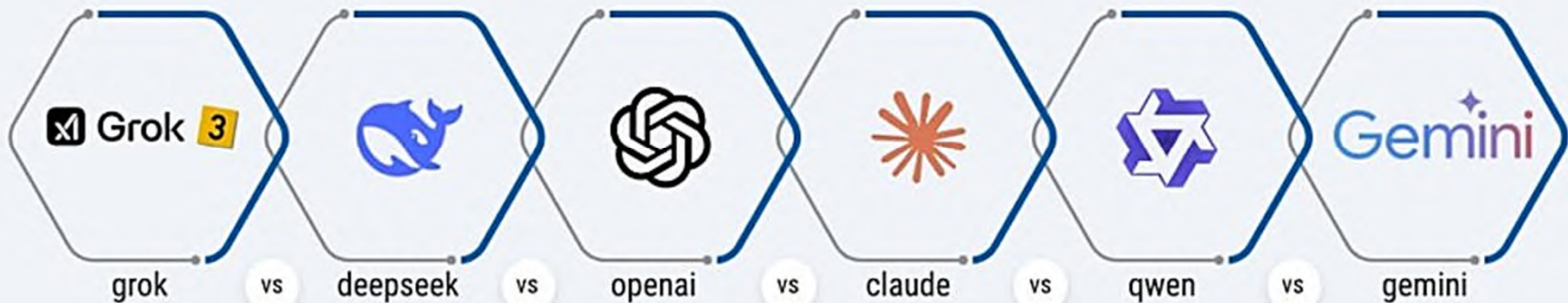


# 2025 主流LLM 概況

結合混合專家模型 MoE 架構，中國開源模型領先者。

原生多模態，長上下文處理能力突出。

多模態架構，深度整合 Google 生態。



速度快，限制少。

多模態能力強，生態完善，  
開發者社群強大，企業整合廣泛。

通義千問，深度整合阿里生態，新版本表現優異。

# 邁向通用人工智能 (AGI) 之路



AI 的發展是一條從專用走向通用的階梯。最終目標是創造出能執行任何人類智力任務的機器。



通用人工智能 (AGI)



多模態 AI



生成式 AI



判別式 AI

通往 AGI (Artificial General Intelligence) 的道路需要持續提升推理、規劃能力，並確保與人類價值觀對齊，結合健全的政策與倫理框架，才能讓 AGI 安全且公平地服務全人類。



# 06

大學提供的AI工具





# 大學提供的AI工具



## Microsoft Copilot

- 雲端服務，與OneDrive配合
- 能處理圖像及文字
- 回應速度較快



## DeepSeek + Gemma

- 校內數據中心部署
- 提供基礎文字
- 能同時調用兩個模型作對比



智博

## GenAI Platform

- 校內數據中心部署
- 可建立專屬知識庫
- 針對知識範圍的校內小助手

# 大學提供的AI工具

<https://genai.um.edu.mo/>



## Guidelines on the Use of Generative Artificial Intelligence Tools

Although generative artificial intelligence (GenAI) tools can enrich and enhance teaching, learning and research experiences and endeavours, there is a risk that using such tools can degrade the quality of teaching and learning activities and undermine the impact and integrity of academic research if used inappropriately.

The University of Macau supports the responsible use of generative AI (GenAI) for teaching, learning and research and urges all academic staff and students to carefully consider their stance on the use of GenAI. The University has produced these guidelines for all UM academic staff and students.

In academic research, it is crucial to consider several key principles to ensure the responsible and proper use of GenAI tools.

### • Acceptable Use

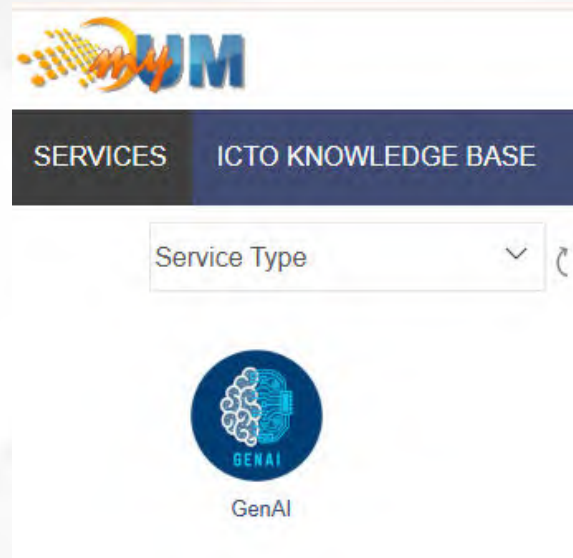
Please sign in to UMPASS using "Microsoft Edge" or "Google Chrome" to access the service.

#### Microsoft Copilot (with commercial data protection)

By using Microsoft Copilot, you agree to comply with all the terms of agreement and laws, rules and regulations applicable to your use of the Microsoft Copilot. We respect your privacy and will only use your personal information in accordance with our [privacy policy](#). Reference: [Microsoft's Data, privacy, and security for Azure OpenAI Service](#).

Sign In

<https://myum.um.edu.mo/>



# 實作練習 1：AI 助理上手

<https://genai.um.edu.mo/>

The image shows a composite view of the M365 Copilot interface. On the left, a sidebar displays the University of Macau logo and a document titled "Guidelines on the Use of Generative Artificial Intelligence Tools". The guidelines text states that while GenAI tools can enhance teaching and learning, they can also degrade quality if used inappropriately. The University of Macau supports responsible use of GenAI and has produced guidelines for its use. In academic research, it is crucial to consider several key principles to ensure the responsible use of GenAI. A section titled "Acceptable Use" is also visible. Below the guidelines, a sign-in prompt asks users to sign in to UMPASS using "Microsoft Edge" or "Google". A "Sign In" button is highlighted with a red box.

The main area of the interface shows the "Welcome to Copilot Chat" screen. At the top, there is a "Try GPT-5" button and a settings icon. Below this, a search bar and a "Chat" button are visible. The chat input field contains the text "澳門大學的校訓是什麼?". Below the input field, there are three suggested prompts: "Summarize file", "Help me prepare for a review of doc with business leadership", and "Give me three math jokes for my 6th grade class". A "See more" link is located at the bottom right of the suggested prompts section.

# 實作練習 1：AI 助理上手

<https://genai.um.edu.mo/>



澳門大學  
UNIVERSIDADE DE MACAU  
UNIVERSITY OF MACAU

## Guidelines on the Use of Generative AI

Although generative artificial intelligence (GenAI) that using such tools can degrade the quality of their work inappropriately.

The University of Macau supports the responsible use of AI and to carefully consider their stance on the use of GenAI.

In academic research, it is crucial to consider several factors:

### • Acceptable Use

#### Microsoft Copilot (with enterprise data)

Please note that students need to complete the Microsoft Copilot training.

By using Microsoft Copilot, you agree to comply with the Microsoft Copilot. Reference: [Microsoft's Data, privacy, and security](#)

#### DeepSeek + Gemma (Trial and Intranet)

Please note that students need to complete the DeepSeek + Gemma training.

It is provided through UM's local servers and may be intermittently slow and unstable due to resource constraints.

DeepSeek-R1-32B v1.0

Gemma-3-27B v0.0.1

Set as default



## Gemma-3-27B

Gemma 3 models are multimodal, handling text and image input and generating text output.

幫我寫一段澳門大學的介紹，大約100字

+



DeepSeek - v0.6.4





# 07

小休時間... 回來  
PART II 實作練習...





# 08

進階技巧



# Prompt / 提示詞：與GenAI說話的方法



✓ 提示詞越清楚具體，GenAI就能給你越好的回應

## 例子一：撰寫會議通知

✗ 不好的 Prompt:

幫我寫一封會議通知信

✓ 好的 Prompt:

請撰寫一封通知信給教務處主管，內容包括：  
本週五上午10點在行政大樓302室召開課程審查會議，請攜帶本學期課程表

🎯 差異說明：

不好的 prompt 太模糊，GenAI無法判斷收件人、時間、地點與主題  
好的 prompt 明確列出所有要素，能生成完整專業的通知信

## 例子二：撰寫公告草稿

✗ 不好的 Prompt:

幫我寫一則公告

✓ 好的 Prompt:

請撰寫一則公告，通知學生下週一開始進行期中  
考週，提醒注意考試時間與攜帶學生證

🔄 差異說明：

不好的 prompt 沒有指定公告對象與內容

好的 prompt 明確指出目的、時間與提醒事項，GenAI能生成清楚實用的公告草稿



## 例子三：安排活動流程

✗ 不好的 Prompt:

幫我排一下活動流程

✓ 好的 Prompt:

請幫我安排一場新生說明會的流程，包含報到、校園導覽、學系介紹與Q&A時間，活動總長度為2小時



差異說明:

壞的 prompt 無法判斷活動內容與時間限制

好的 prompt 提供活動主題、項目與時長，GenAI能合理規劃流程

# 角色扮演法

- 在 prompt 中指定 GenAI 扮演某個角色
- 如：行銷專家、資料分析師、編劇、老師等
- 引導其用該角色的視角來回應。



「你是一位資深行銷顧問，請幫我設計一個針對年輕族群的社群活動企劃。」



「你是 Excel 專家，請幫我寫出一個公式來計算每月平均銷售額。」



## 專業視角

限制以專業視角來思考  
避免產出過於泛泛的答案



## 激發創意

模擬專業人士的思維  
產出更有深度的內容



## 簡化溝通

不需要逐條列出所有細節  
推斷出相關背景知識與最佳實踐

# 角色扮演法

- 角色設定 (Who)
  - 指定 GenAI 的身份或專業背景
  - 範例：「你是一位資深人資顧問」
- 任務目標 (What)
  - 明確說明你希望 GenAI 完成的任務
  - 範例：「請幫我撰寫一封面試邀請信」
- 語氣風格 (How)
  - 指定回應的語氣、格式或風格
  - 範例：「請用正式且友善的語氣撰寫」

## 角色扮演法撰寫公式

你是一位 [角色]，請幫我  
[任務]，並以 [語氣/風格] 回應。



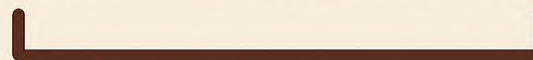
角色



任務



語氣/風格



## 實作練習 4：翻譯文本

基本翻譯提示詞：

請將以下內容從英文翻譯成繁體中文，保持原文的語氣和風格



進階翻譯提示詞：

你是一位專業在澳門高等教育機構工作的翻譯員，請將以下內容從英文翻譯成繁體中文

要求：

1. 保持專業術語一致性
2. 使用港澳地區日常使用的書面用語
3. 請用學術界正式語氣翻譯
4. 提供原文和譯文對照表格以作檢查



# 4C法則

Context  
(背景)

說明任務的背景與目的，讓 GenAI 理解校務場景。

「這是一份給學術副校長的報告，需包含本學期選課統計與學生滿意度分析。」

Clarity  
(清晰)

指令必須明確，避免模糊詞彙。

「請撰寫一份 800 字的報告，主題為本學期選課趨勢，並附上三個主要數據圖表。」

Creativity  
(創意)

鼓勵 GenAI 提出新穎呈現方式，讓行政文件更具吸引力。

「請將學生滿意度調查結果以資訊圖表呈現，並加入簡短故事化描述。」

Constraints  
(限制)

明確設定格式、語氣、長度等要求。

「報告需使用正式語氣，字數不超過 1000 字，並符合校方公文格式。」



# 4C法則：實例演示

✗ 優化前：

幫我撰寫一篇「學生宿舍安全宣導文章」

- Context（背景）
  - 明確指出文章用途：校園網站與公眾號
  - 目標讀者：宿舍學生
- Clarity（清晰）
  - 指定內容結構：三個守則 + 檢查清單
- Creativity（創意）
  - 要求加入情境故事，提升吸引力與記憶度
- Constraints（限制）
  - 設定語氣：親切但專業
  - 字數：600 字
  - 格式：適合社群平台

✓ 應用4C法則優化後：

請撰寫一篇 600 字的宿舍安全宣導文章，背景是給大學宿舍學生閱讀，將發布在校園網站與公眾號。文章需清楚列出三個主要安全守則，並附上簡單檢查清單。請加入一個有趣的情境故事，讓學生更容易記住安全守則。文章需使用親切但專業的語氣，字數不超過 600 字，並適合社群平台排版。

## 實作練習 5：新聞稿撰寫

- 結合你自己的工作情境，運用4C法則來撰寫提示詞，讓GenAI幫你寫一篇關於活動的新聞稿。

- Context（背景）

- 你是？
- 文章用途？
- 目標讀者？

- Creativity（創意）

- 要求加入？？？以提升？？？
- 要求模仿？？？以增加？？？
- 要求？？？？？？？？？？

- Clarity（清晰）

- 人？事？時？地？物？
- 活動意義？

- Constraints（限制）

- 標題？結構？
- 字數？
- 語言？語調？



# 09

## GenAI的安全性和私隱問題



# 安全性和私隱問題

- 避免於GenAI工具中分享機密資訊及個人資料

## 數據地點

- 絕大部分提供GenAI服務的伺服器均位於澳門境外地區
- 注意個人資料保護

## 數據安全

- 傳輸過程加密？
- 經由第三服務商？
- 對話可否儲存？

## 數據利用

- 服務商會否利用對話數據於其他用途？
- 廣告？
- 再次訓練？

# 安全性和私隱問題

**Interactions with Bots on Poe.** Our third party AI model LLM providers and third party bot developers may receive details about your interactions with bots on Poe (including the contents of your chats) to provide and generally improve their services, which they may process in their legitimate business interests. Your Poe user account information (e.g., username and email) is not shared with our third party AI model providers or developers. Third party developers that create bots on Poe using APIs may view and store your anonymized chats on their servers to train their models. We may use your interactions on Poe to provide you a personalized experience, such as recommending other bots to explore or topics to discuss.

## How We Use Your Personal Data

We use your Personal Data to operate, provide, develop, and improve the Services, including for the following purposes.

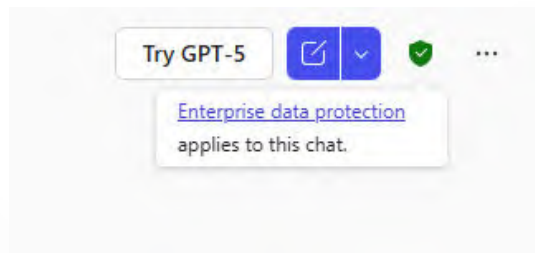
- To provide, administer and maintain the Services and to enforce our terms, conditions and policies. Such as creating the accounts, deliver a fast and convenient logging-in experience, enabling you to chat with DeepSeek and provide user support.
- To improve and develop the Services and to train and improve our technology, such as our machine learning models and algorithms. Including by monitoring interactions and usage across your devices, analyzing how people are using it, and training and improving our technology.
- To communicate with you, including to notify you about changes to the Services, provide customer support to you and send you other service-related messages.

5.4 您知悉、理解并同意，如果您按照法律规定对您的输入（包括您使用本服务过程中自行上传、发布的全部内容）和/或输出享有权利的（包括但不限于知识产权、肖像权等），您使用本服务均不会造成前述合法权利的转移或减损，除非我们与您另有约定。与此同时，您理解并同意百度将在法律允许的范围内为实现本服务目的对您上传、发布的内容进行存储及使用（包括但不限于复制、分发、传送、公开展示、编辑等）。

在使用GenAI工具前，請先了解其資料保留及利用政策，不要輸入和上傳包含敏感信息或個人資料的數據



# Microsoft Copilot



## Enterprise data protection for prompts and responses

Microsoft 365 Copilot and Microsoft 365 Copilot Chat offer the same enterprise terms<sup>[2]</sup> available in our Microsoft 365 commercial offerings.

Use of Microsoft 365 Copilot and Microsoft 365 Copilot Chat involves prompts (entered by users) and responses (content generated by Copilot). With EDP, prompts and responses are protected by the same contractual terms and commitments widely trusted by our customers for their emails in Exchange and their files in SharePoint.

- **We secure your data:** We help protect your data with [encryption](#) at rest and in transit, rigorous physical security controls, and data [isolation](#) between tenants.
- **Your data is private:** We won't use your data except as you instruct. Our commitments to [privacy](#)<sup>↗</sup> include support for the [General Data Protection Regulation \(GDPR\)](#), the [EU Data Boundary](#)<sup>[3]</sup>, [ISO/IEC 27018](#), and our [Data Protection Addendum](#)<sup>↗</sup>.
- **Your access controls and policies apply to Copilot:** Copilot respects your [identity model](#) and [permissions](#), inherits your [sensitivity labels](#), applies your [retention](#) policies, supports [audit](#) of interactions, and follows your administrative settings. The specific controls and policies will vary depending on the underlying subscription plan.
- **You're protected against AI security and copyright risks:** We help safeguard against AI-focused risks such as [harmful content](#) and [prompt injections](#). For content copyright concerns, we provide [protected material detection](#) and our [Customer Copyright Commitment](#)<sup>↗</sup>.
- **Your data isn't used to train foundation models:** Microsoft 365 Copilot Chat uses the user's context to create relevant responses. Microsoft 365 Copilot also uses Microsoft Graph data. Consistent with our other Copilot offers, the prompts, responses, and data accessed through Microsoft Graph [aren't used to train foundation models](#)<sup>↗</sup>.

# 澳門大學本地部署 GenAI 服務



DeepSeek + Gemma



智博

GenAI Platform

# GenAI 輸出的事實核實



AI幻覺

生成式模型輸出看似合理但實際錯誤或虛構的內容  
可能涉及事實錯誤、邏輯斷裂或脫離上下文

## 主要成因

- 數據偏差：訓練資料錯誤或過時，模型放大偏差
- 泛化困境：模型難以處理訓練集外的複雜場景
- 知識固化：模型過度依賴靜態記憶，缺乏動態更新能力
- 意圖誤解：用戶提問模糊，模型自由發揮
- 編碼與解碼錯誤：語言模型在生成過程中出現語義偏差



## 虛假陳述

錯誤引用虛構文獻，影響  
全文可信度



## 決策風險

若依賴錯誤輸出作出決策，  
可能造成物質或聲譽損失



## 擴散錯誤

擴散錯誤資訊，可能對受眾  
產生連鎖負面影響

# GenAI 輸出的事實核實

## 如何避免幻覺



### 雙AI驗證

使用另一個模型交叉檢查答案



### 提示詞優化

加入時間、來源、專業身份等限制，降低虛構可能性



### 信度標註

要求AI在不確定時標註「推測」或「暫無可靠數據」

## 事實核查方法



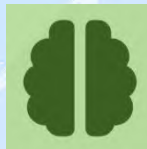
### 來源檢查

確認AI引用的資料是否存在於可信數據庫



### 交叉驗證

使用多個獨立來源比對答案



### 邏輯評估

評估內容是否符合常識，有沒有內部矛盾，是否符合已知事實



# GenAI 輸出的事實核實



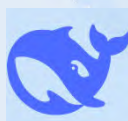
Microsoft Copilot

澳門大學的校訓是什麼？

Copilot ⓘ

澳門大學的校訓是「仁、義、禮、知、信」，這五個詞源自中國傳統聖賢所提倡的五種美德，分別代表人文關懷、道德操守、禮儀規範、智慧求知以及誠信待人。校訓不僅體現了學校的教育理念，也象徵著澳門大學致力培養具備高尚品格與全面素養的學生。

這五種美德在校徽上也有所體現，並與澳門大學的品牌形象緊密結合，象徵學校連結東西方文化、追求知識與人類進步的使命。如果你有興趣，我可以幫你整理校徽設計的寓意，或者提供校歌的簡介，要不要繼續了解？



DeepSeek

DeepSeek-R1-32B

Thought for 11 seconds ▾

澳门大学的校訓是「追求卓越、力求完美」。這句話體現了學校對學術研究和學生發展的高標準要求，以及不斷追求完善的教育理念。

Thought for 11 seconds ▸

澳門大學的校訓是「仁、義、禮、知、信」。這五個字源自儒家思想的「五常」，代表著中華文化核心的道德價值觀，分別指：

- 仁：仁愛、關懷他人
- 義：正直、堅守原則
- 禮：禮儀、尊重社會規範
- 知：知識、智慧與追求真理
- 信：誠信、言行一致

這一校訓體現了澳門大學致力於培養學生兼具人文素養與專業能力，並強調道德教育與全人發展的辦學理念。



Gemma

Gemma-3-27B

澳門大學的校訓是：勵學愛國服務社會 (Lìxué àiguó fúwù shèhuì)。

這句話的意思是：勤奮學習，熱愛國家，服務社會。

它體現了澳門大學致力於培養學生在學術上追求卓越，同時也關心國家和社會發展的願景。

希望這個回答對您有幫助！如果您還有其他問題，隨時都可以問我。 😊





# 10

實作練習 II





# 11

知識庫增強GenAI小助手



# 檢索增強生成 Retrieval-Augmented Generation (RAG)

將「檢索系統」與「大語言模型 (LLM)」結合：先找資料、再生成答案。



用檢索補充模型上下文，讓生成有據可依。



## 最新資料

大模型的訓練資料過時  
知識庫能補充最新資料



## 效能成本

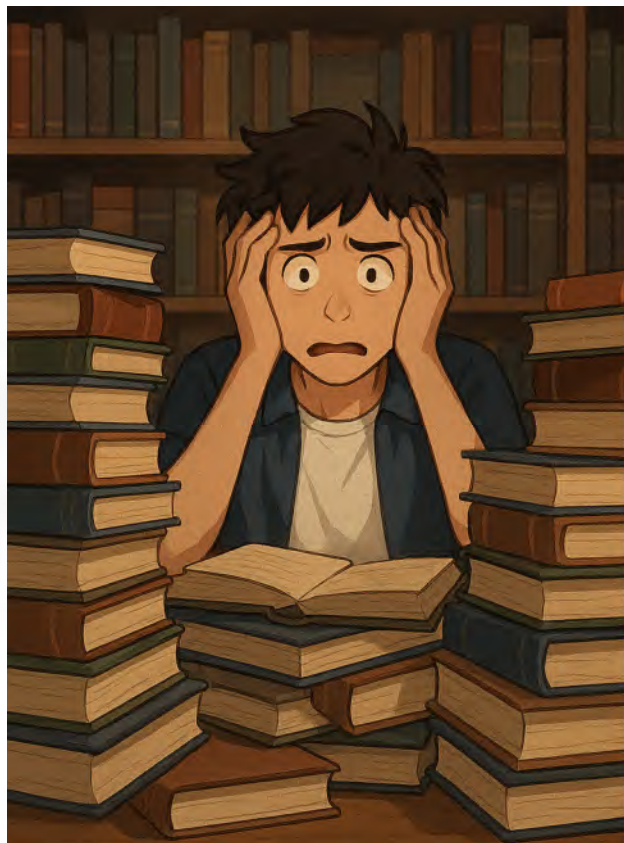
快取、壓縮上下文  
多階段檢索



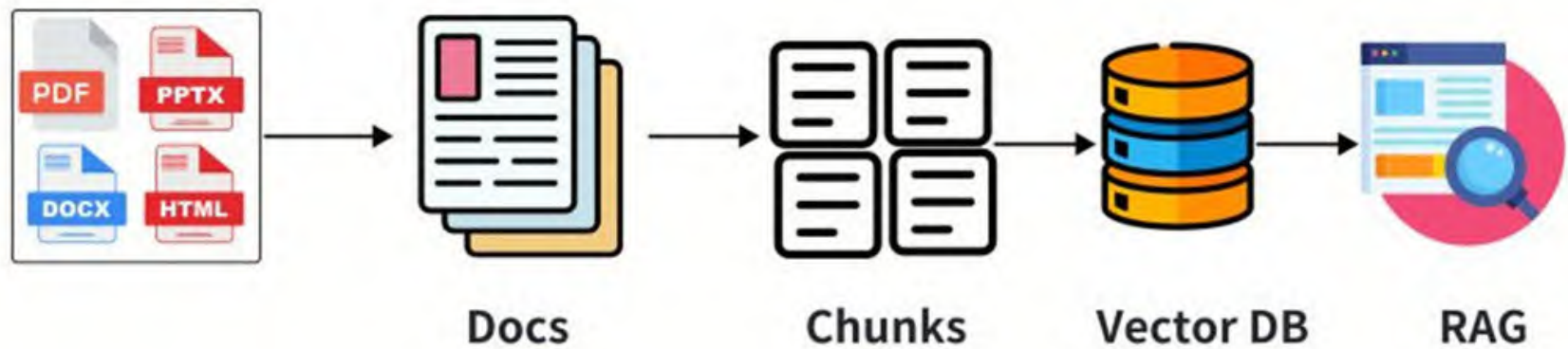
## 可信來源

明確來源標註  
提升可驗證性

# 檢索增強生成 Retrieval-Augmented Generation (RAG)



## RAG: 資料準備與預處理





# RAG: 澳門大學智博GenAI平台展示



# RAG: 澳門大學智博GenAI平台展示

The screenshot displays a chat interface for the Macau University GenAI platform. The chat history shows a greeting from the assistant, 'whpang', identifying itself as the Macau University Personnel Regulations Assistant. The user asks about the annual leave for administrative staff. The assistant responds with a detailed answer based on the University's Personnel Statute, stating that staff with over one year of service are entitled to 22 working days of annual leave. A response time of 5.3360s is shown. Below the answer, a citation for 'The Personnel Statute of the University of Macau.pdf' is provided with view and download icons. At the bottom, a prompt encourages users to ask more questions, followed by two example questions in input boxes.

你好，whpang  
我是澳門大學人員通則助手

我是大學的行政人員，一年有幾天的年假？

根據澳門大學人員通則的規定，連續提供服務一年以上的工作人員，在每一曆年內有權享受二十二個工作日的年假。 8  
5.3360s

引用 1 篇資料作為參考  
The Personnel Statute of the University of Macau.pdf

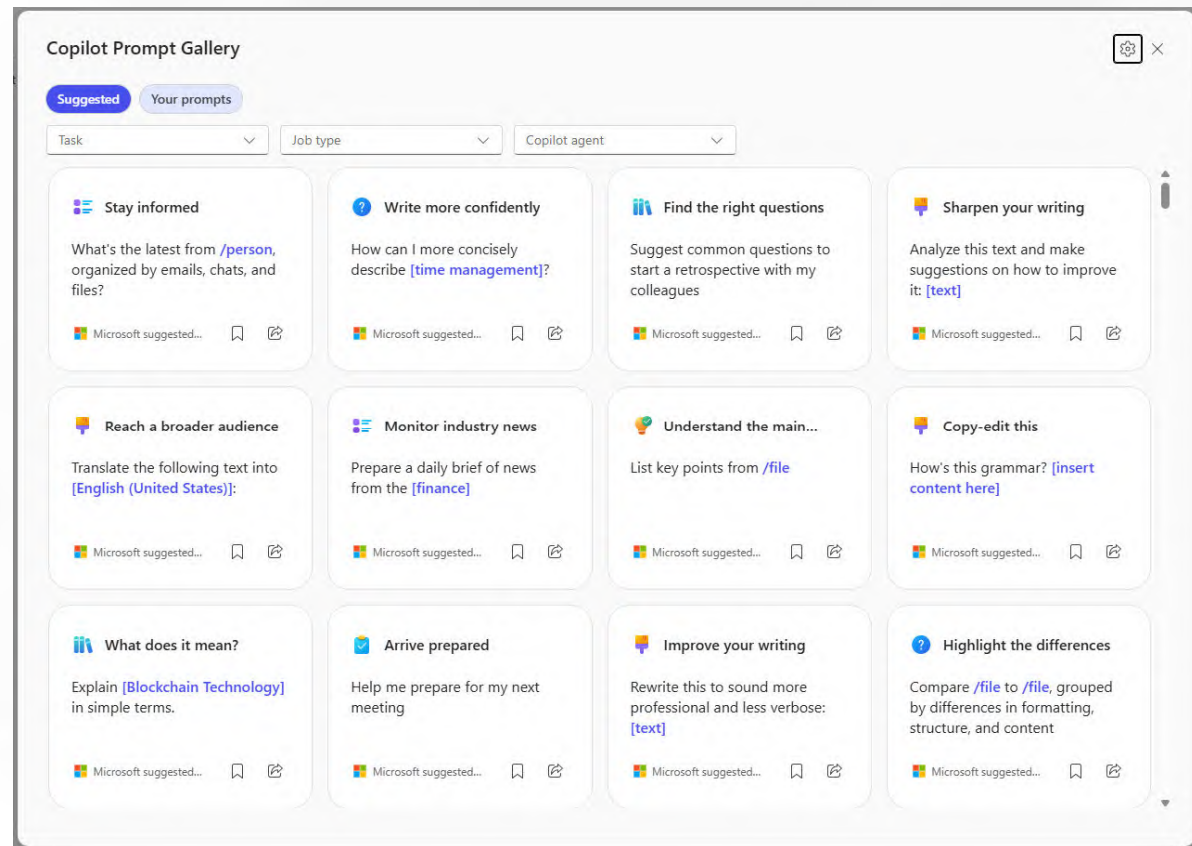
以下問題是您想了解的嗎？您也可以將問題直接發給我。

問題1： 因親屬死亡而請假的缺勤日數最長可延長至...

問題2： 根據澳門大學的人事規章，員工的年假天數...

# Prompt guidance

- Copilot Lab  
[aka.ms/CopilotLab](https://aka.ms/CopilotLab)
- AI for Education  
[www.aiforeducation.io](https://www.aiforeducation.io)







謝謝!