

# 由機器學習到人工智慧

林軒田(Hsuan-Tien Lin)

htlin@csie.ntu.edu.tw

國立臺灣大學資訊工程學系

Dept. of Computer Science and Information Engineering  
National Taiwan University



國立臺灣大學法律學院數位法律研究中心  
二零二四年九月四日

# 關於我：林軒田

教授  
國立臺灣大學資訊工程學系



首席資料科學顧問  
(前首席資料科學家)  
沛星互動科技

Appier

作者  
由資料中學習  
(Learning from Data)



授課教師  
NTU-Coursera 大型開放式課程  
機器學習基石/技法



研究興趣：以機器學習實現有用的人工智慧

## 接下來要講的是……

人工智慧是什麼？

機器學習是什麼？

機器學習怎麼做？

機器學習為什麼？

機器學習怎麼用？

人工智慧往哪走？

## 由智慧到人工智慧

智慧：聰明地思考與行動

- 像人
- 理性

人工智慧：讓電腦聰明地思考與行動

- 像人
- 理性

像人  $\approx$  聰明  $\approx$  理性  
—人類一定是理性的嗎？😊

## 要像人還是要理性？

如果你的自駕車決定死一個人比死兩個人好，**而那一個人是你？**

(翻譯自華盛頓郵報)

<https://www.washingtonpost.com/news/morning-mix/wp/2015/10/28/what-if-your-self-driving-car-decides-one-death-is-better-than-two-and-that-one-is-you/>

你正坐在你的自駕車裡哼著小曲，自駕車一邊全自動進行導航，你一邊開始用你的iPhone 37聊天。這時，一群人突然出現在街道上，正好闖入車輛的行進路線。

### 一台像人的自駕車

主人(與乘客)的命最重要，不得已就撞上去吧！

### 一台理性的自駕車

應該降低總人命損失，所以該閃開往旁邊撞，犧牲小我。

哪個比較聰明？

—也許得看我們是乘客還是路人？😊

# 人工智慧的定義：傳統與當代

## 傳統定義

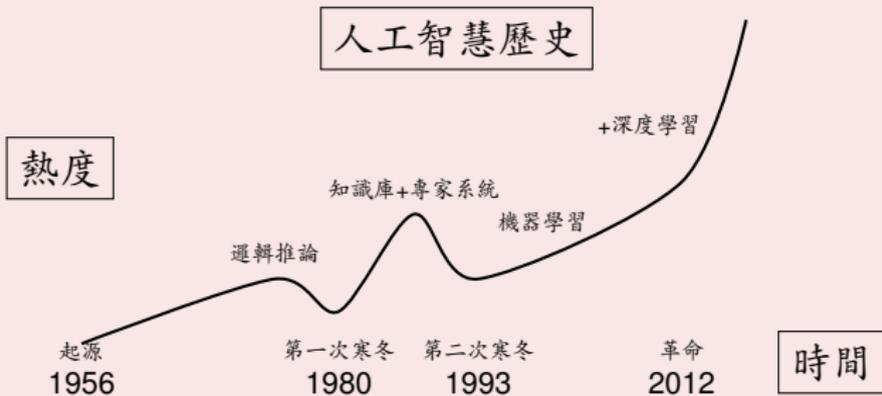
像人  $\approx$  聰明  $\approx$  理性

## (我的)當代定義

聰明  $\approx$  好用  
「智慧型手機」聰明嗎？😊

當代人工(Artificial)智慧  
= 應用(Application)智慧

# 人工智慧歷史



- **第一次寒冬**：(當時)人工智慧無法有效率地處理「**組合爆炸**」
- **第二次寒冬**：(當時)人工智慧無法有效率地納入「**專家知識**」

兩次寒冬的共同點：**期望落差**

## 這波人工智慧熱潮為何不同？

### 資料更多

- 儲存與傳輸變得便宜
- 網路與行動裝置的發展

### 運算更快

- 多機器運算，如雲端運算
- 多核心運算，如圖型加速器(GPU)

### 模型更好

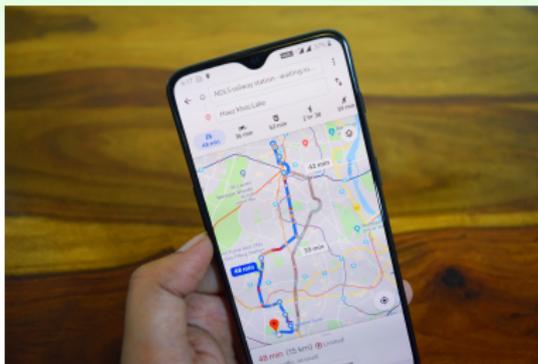
- 數十年的相關研究
- 例如：深度學習、生成式人工智慧

### 心態更健康

- 合理的期望
- 關鍵的突破，如AlphaGo

資料驅動的人工智慧：目前的主流方法

# 更多的資料帶來更好的應用智慧



By deepanker70 on <https://pixabay.com/>

過去

由地圖連結算出  
最短路徑

現在

由即時路況算出  
最快路徑

未來

由預測路況算出  
最順路徑

更多的資料可以讓應用程式「更聰明」

# 接下來要講的是……

人工智慧是什麼？

機器學習是什麼？

機器學習怎麼做？

機器學習為什麼？

機器學習怎麼用？

人工智慧往哪走？

## 由生物學習到機器學習

**生物學習**：由**觀察**中累積經驗  
以獲得**技能**



**機器學習**：由**資料**中累積/**估計**/**計算**經驗  
以獲得**技能**



什麼是**技能**？

## 技能就是「成績」提昇

技能  $\iff$  「成績」(例如：準確率)變好

機器學習：由資料中累積/估計/計算經驗  
以提昇某項成績



### 應用實例一：股票預測



加入計算學習實驗室，  
不要讓你的機器輸在起跑點上  
—林軒田·臺大資訊系內招生宣傳·2008

# 機器學習連接了巨量資料與人工智慧

一張圖秒懂三個熱門名詞

(巨量)資料 → 機器學習 → 人工智慧

食材



工具/步驟



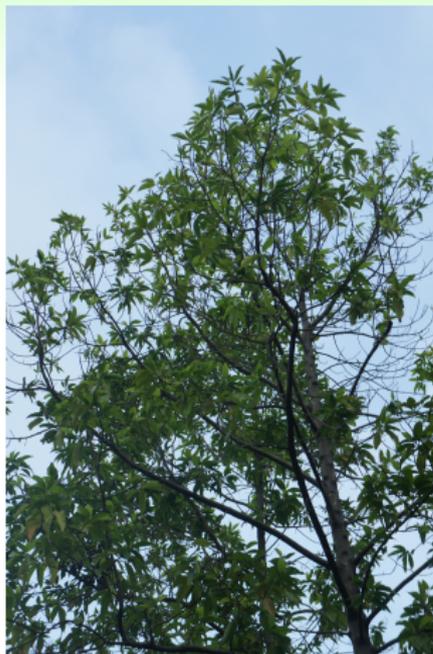
佳餚



(Photos Licensed under CC BY 2.0 from Andrea Goh on Flickr)

首席資料科學家 ≡ 餐廳主廚

# 為什麼要用機器學習？



- 為樹下「規則定義」再寫成程式碼(專家系統)：很困難
- 由觀察(資料)累積經驗再做辨識：三歲小孩就會了
- 智慧的植物辨識系統：  
走「機器學習」這條路比走「規則定義」這條路往往更容易實現

機器學習：打造人工智慧系統的一條(充滿潛力的)路徑

## 應用實例二：學習成效預測

學生過去的測驗表現  $\longrightarrow$  **機器學習**  $\longrightarrow$  下一題會不會答對？

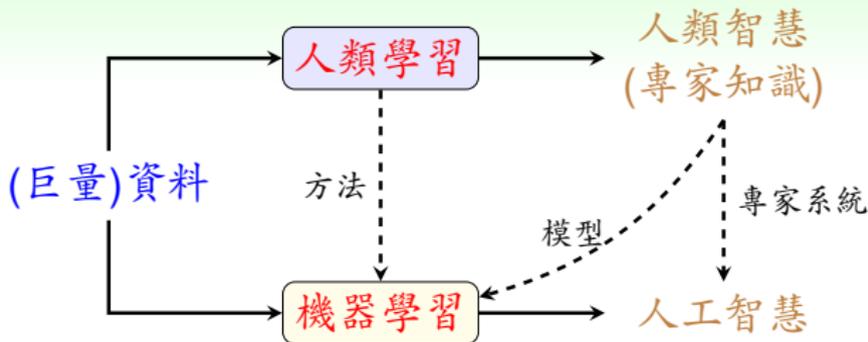
### 一個簡單的機器學習方法

會不會答對  $\approx$   $[[$ 學生程度  $>$  問題難度 $]]$

- 給機器來自三千個學生的九百萬筆資料
- 機器自動地估計(反推)學生程度與問題難度

臺灣大學隊伍 2010 年獲得  
KDDCup 世界冠軍的方法之一

# 機器學習與當代人工智慧



## 人類學習

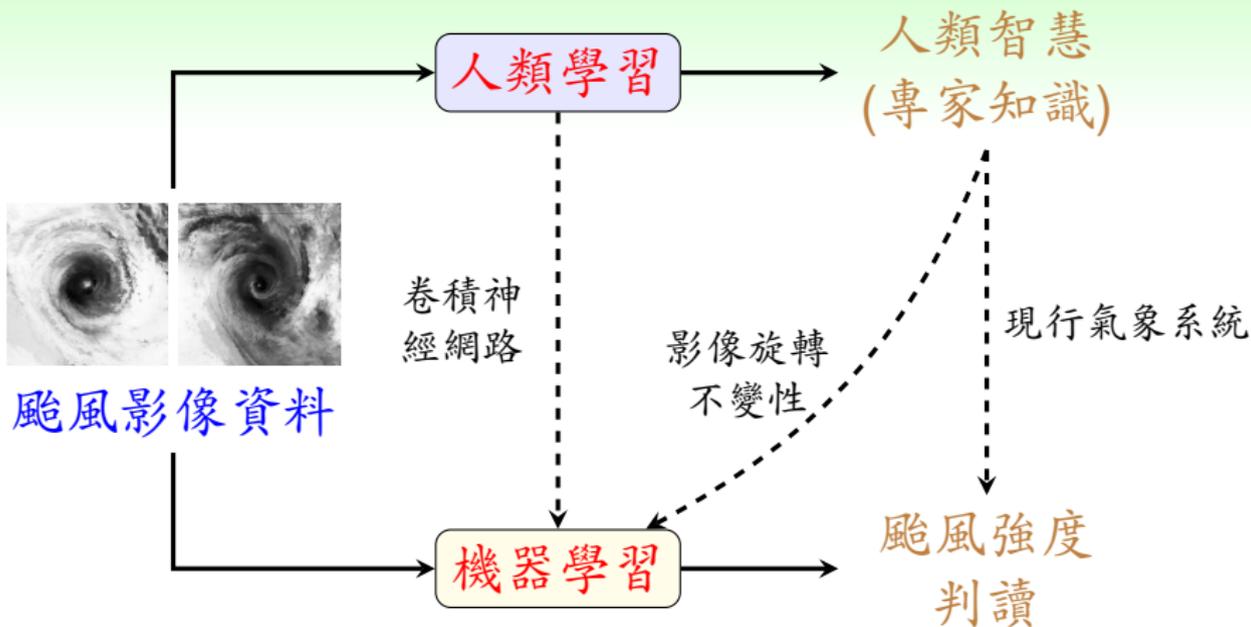
- 主觀
- 產生專家知識
- 快速的開始

## 機器學習

- 客觀
- 運用計算力量
- 持續的進步

秘訣：一開始可以儘量使用**人類學習**

## 應用實例三：颱風強度判讀



**機器學習**可將現行系統(ADT)  
的判讀誤差降低近**20%**

(Chen et al., Rotation-blended CNNs on a new open dataset for tropical cyclone image-to-intensity regression, 2018)

# 接下來要講的是……

人工智慧是什麼？

機器學習是什麼？

機器學習怎麼做？

機器學習為什麼？

機器學習怎麼用？

人工智慧往哪走？

## 機器學習三要素

**機器學習**：由**資料**中累積/**估計**/**計算**經驗  
以**提昇**某項**成績**



- ① 要具備**可學**的**規律性**  
—才有可能**提昇**某項**成績**
- ② 但沒有**可輕易****程式化**的**規則****定義**  
—才會需要**機器學習**
- ③ 而要有**與規律性****相關**的**資料**  
—才有**原料**可以開始

三要素可幫助決定  
是否有機會使用機器學習

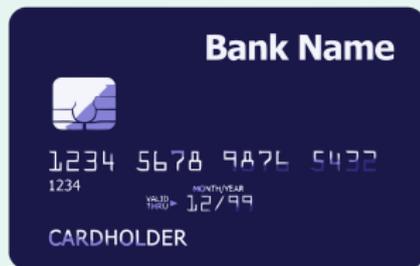
## 應用實例三：機器學習與信用卡核卡

申請人的背景資料

年齡	23
學歷	電機資訊學士
年收入	一百萬
工作年資	六個月
負債	二十萬



是否核卡？

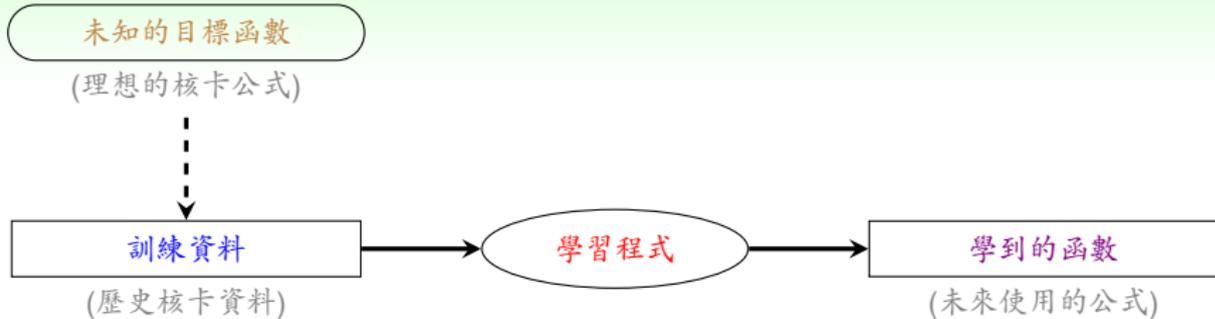


(Picture Licensed under CC0 on Pixabay)

可學的規律性：

申請人的背景資料  $\Rightarrow$  核卡風險高不高？

# 怎麼學習「信用卡核卡」？

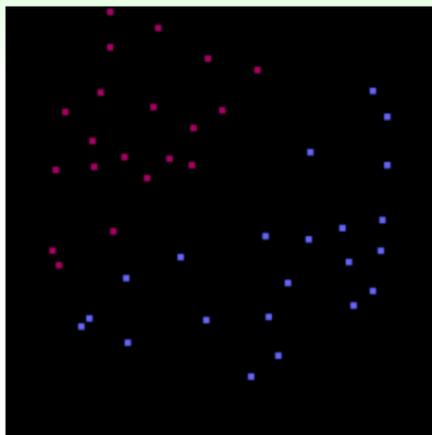


- 未知的目標函數  
(沒辦法輕易程式化)
- 希望：學到的函數和未知的目標函數很像  
(通常不會一模一樣)

什麼是「學習程式(模型+方法)」？

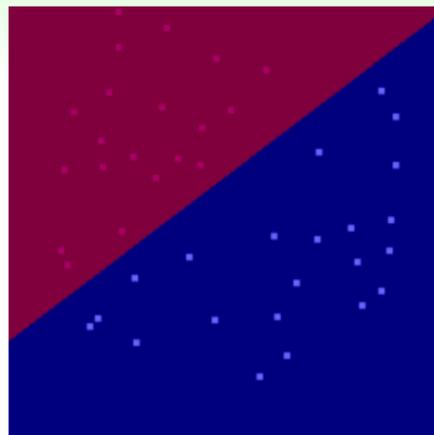
## 線性分類模型

負債



收入

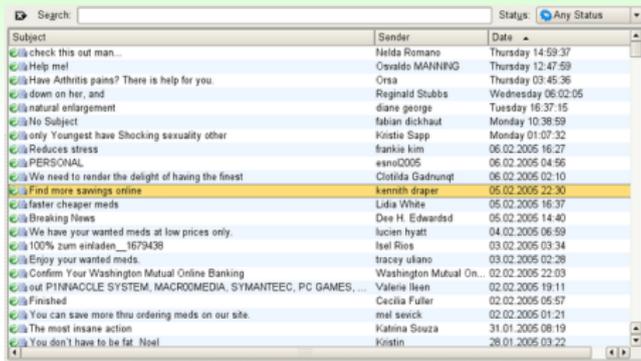
負債



收入

找一條線(學到的函數)，  
把已知資料中的●(發卡)和●(不發)「完美切割」

## 應用實例五：垃圾郵件偵測



(Licensed under GPL via Wikimedia Commons by Ascánder)

	垃圾郵件	一般郵件
用字	free drug fantastic deal	machine learning statistics textbook

(Example taken from my Machine Learning Foundations MOOC)

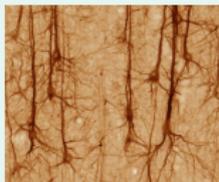
簡單的多維線性模型：

看看正面的字比較多還是反面的字比較多

# 由線性模型到類神經網路

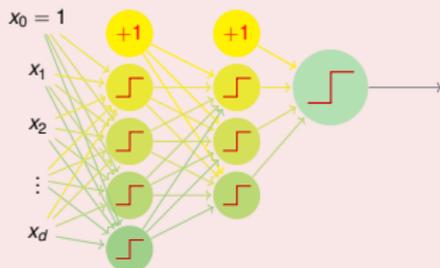
感知器(模擬「一個神經元」):  
類神經網路(模擬「一堆神經元」):

「畫一條直線」  
「畫非常複雜的邊界」(及其他)



by UC Regents Davis campus-brainmaps.org.

Licensed under CC BY 3.0 via Wikimedia Commons



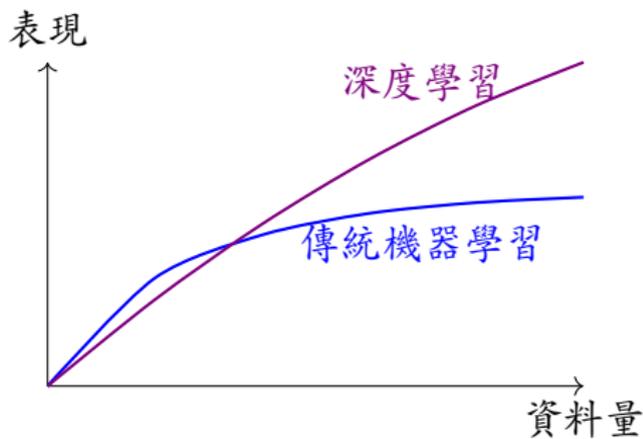
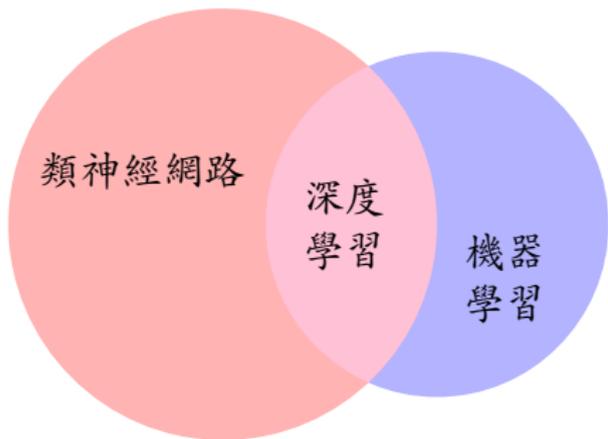
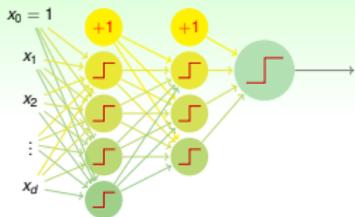
by Lauris Rubenis.  
Licensed under CC BY 2.0 via  
<https://flic.kr/p/fkVuZX>



by Pedro Ribeiro  
Simões. Licensed  
under CC BY 2.0 via  
<https://flic.kr/p/adiV7b>

類神經網路：一種仿生模型

# 從類神經網路到深度學習



深度學習：用大量資料+大量計算  
來解決(困難的)機器學習問題。

## 應用實例六：人臉辨識



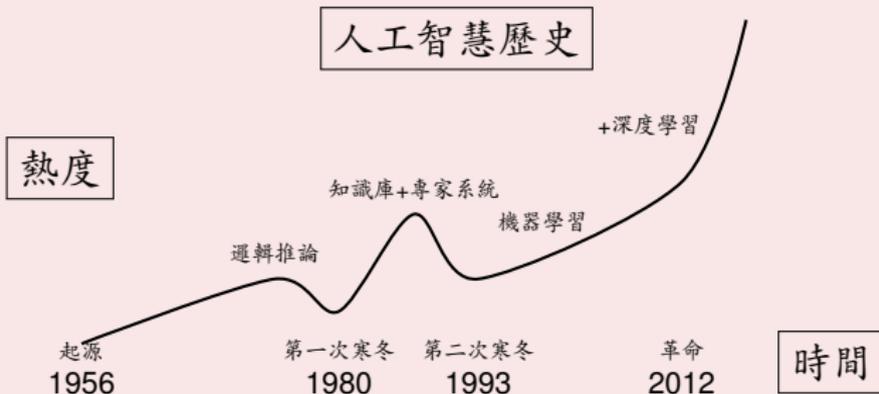
original picture by F.U.S.I.A. assistant and derivative work by Sylenius via Wikimedia Commons

### 人臉辨識

- 資料：人臉與非人臉
- 人工智慧：辨識哪裡有人臉

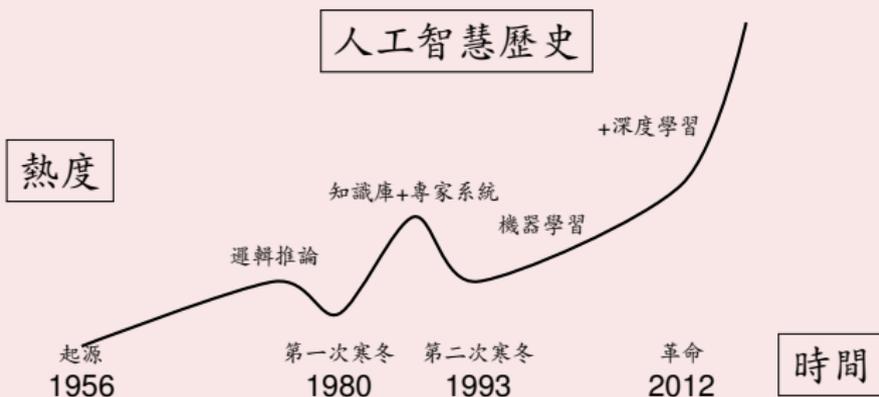
有成熟的淺度與深度學習技術，但通常  
需要依照應用需求做一些調校

# 歷史回顧：深度學習法(Hinton et al., 2006)



深度學習法：類神經網路在  
第二次寒冬後捲土重來的再度復興

# 「歷史」回顧：從辨識到生成

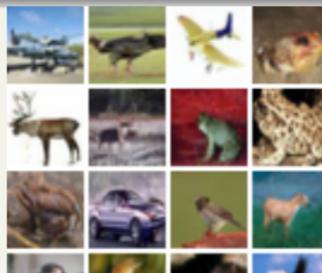


(Krizhevsky et al., 2012)  
ImageNet  
classification  
with deep  
convolutional  
neural networks



Picture extracted from the original paper  
of Krizhevsky et al. for educational purposes

(Ho et al., 2020)  
Denoising  
diffusion  
probabilistic  
models



Picture extracted from the original paper  
of Ho et al. for educational purposes

**深度學習**加速了當代人工智慧的實現

# 生成式人工智慧(機器學習)

辨識式機器學習

聽/讀/看

生成式機器學習

說/寫/畫

## 生成式的兩大特徵

變化(創造力)



(Pictures Extracted from Ho et al. for educational purposes)

複雜(結構性)



(Pictures Licensed under CC0 on Wikipedia)

生成式機器學習：能做**有變化的複雜**輸出

# 接下來要講的是……

人工智慧是什麼？

機器學習是什麼？

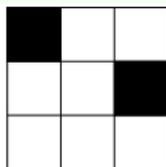
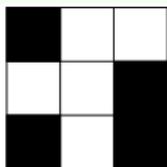
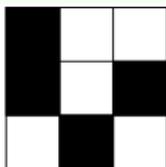
機器學習怎麼做？

機器學習為什麼？

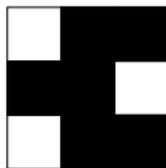
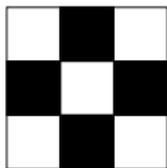
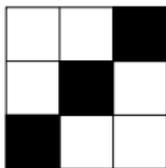
機器學習怎麼用？

人工智慧往哪走？

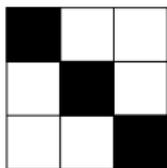
# 機器/人類學習小測驗



$$y_n = -1$$



$$y_n = +1$$

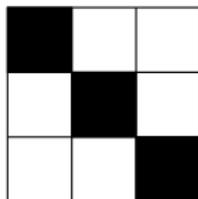


$$g(\mathbf{x}) = ?$$

你的「人類學習」學到了什麼？

## 兩個可能的答案

不管你回答什麼

 $y_n = -1$  $y_n = +1$  $g(\mathbf{x}) = ?$ 

「標準答案」是+1，因為...

- 對稱性  $\Leftrightarrow +1$

「標準答案」是-1，因為...

- 左上角是黑色的  $\Leftrightarrow -1$

暖心老師 怎樣都可以說你對  
 黑心老師 怎樣都可以說你錯

# 機器學習「可行性」的三要素



如果考題跟課本習題差不多，  
然後我把課本習題讀懂了，  
融會貫通在考題上，  
那麼考試成績就會好了！



(Pictures Licensed under CC0 on Pixabay)

## 機器學習要可行，必須

- 1 訓練資料和測試場景要有一定的關聯性  
—不能腦筋急轉彎
- 2 訓練表現要夠好  
—已經讀過的習題要弄懂
- 3 要能由訓練資料舉一反三到測試場景  
—在考題上要融會貫通

訓練夠好：最佳化；舉一反三：一般化  
機器學習的兩難：兩個要素往往是「衝突的」

## 接下來要講的是……

人工智慧是什麼？

機器學習是什麼？

機器學習怎麼做？

機器學習為什麼？

機器學習怎麼用？

人工智慧往哪走？

# 已經講過的應用實例

(巨量)資料 → 機器學習 → 人工智慧



(Photos Licensed under CC BY 2.0 from Andrea Goh on Flickr)

- 應用實例一：股票預測
- 應用實例二：學習成效預測
- 應用實例三：颱風強度判讀
- 應用實例四：信用卡核卡
- 應用實例五：垃圾郵件偵測
- 應用實例六：人臉辨識

機器學習已廣泛地實現應用智慧

## 應用實例七：圖像生成



an astronaut riding a horse, by Hiroshige

(Picture in Public Domain on Wikipedia)

- 新興的「繪圖工具」
- 當代「生成式人工智慧」的代表

持續變得更快、更精緻、更可控！

# 應用實例八：問答系統



(Snapshot from chat.openai.com in my class for educational purposes)

- 機器學習技術：**注意**上下文的關鍵部份來進行**文字接龍**
- 用超大量資料、超大型模型、超大量運算，達成**令人驚奇**的表現

百家爭鳴中：由技術**特化**出各種應用智慧

# 接下來要講的是……

人工智慧是什麼？

機器學習是什麼？

機器學習怎麼做？

機器學習為什麼？

機器學習怎麼用？

人工智慧往哪走？

# 從萊特兄弟(1903)到商用客機(1919-)



by Wright Brothers.  
Licensed under Public  
Domain via  
US Library of Congress



by Pedro Ribeiro  
Simões. Licensed  
under CC BY 2.0 via  
[https://flic.kr/  
p/adiV7b](https://flic.kr/p/adiV7b)

我們在(生成式)人工智慧的萊特兄弟時刻

# 飛機怎麼普及化的？



by Wright Brothers.  
Licensed under Public  
Domain via  
US Library of Congress

- 戰爭？😊
- 技術進展  
—更輕的材料、更有效率的引擎、更好的控制系統
- 相關規範  
—法規、執照、保險等
- 更多嘗試  
—了解成功與失敗的經驗

革命才剛開始，同志仍需努力

## 自駕車車禍的民事責任(蕭奕弘律師提供)

A 駕駛自駕車上路，撞傷闖紅燈的行人B，誰該負責？

### 特斯拉Autopilot肇事案

<https://www.cna.com.tw/news/aopl/202304220170.aspx>

- 2019年，徐小姐駕駛Telsa Model S上路，開起Autopilot功能，後來發生車禍，徐小姐對特斯拉起訴，請求300萬美元損害賠償。
- Tesla抗辯認為，依照當時Model S的產品手冊，駕駛必須一直控制車輛，也不能在城市街道上使用「自動轉向」功能，徐小姐沒有把手一直放在方向盤上。
- 加州陪審團在2023年4月21日，駁回徐小姐的起訴，認為自動輔助駕駛系統只是輔助，本案駕駛的分心才是肇事原因。

人工智慧(可能)產生新的需求與責任歸屬  
(Tesla工程師、Tesla公司、僱用人/駕駛、……)

# 人工智慧與刑事犯罪

<https://www.youtube.com/watch?v=-a61zsRRONc>

Yaser Abu-Mostafa, Artificial Intelligence: The Good, the Bad, and the Ugly



## 1. Malicious use of AI



[Credit: iStock]



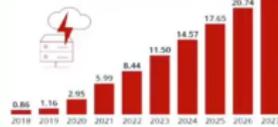
[Credit: Simplicam]



[Credit: adobe]

### Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)



[Credit: Statista]

doing that you use AI, your penalty will

26/30

人工智慧一如手槍，可能讓(某些)犯罪變得容易

# 法律文件的生成

請寫一封律師函，請住戶分擔公設維修費用



律師函

發件人：

[您的姓名]

[您的地址]

[您的聯絡方式]

[日期]

收件人：

[住戶姓名]

[住戶地址]

主旨：要求分擔公設維修費用

尊敬的[住戶姓名]：

您好！

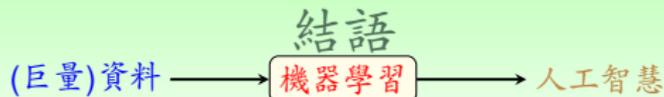
依據[相關法律或社區管理規章的名稱和條款]，所有住戶均有義務按照各自持分比例分擔公設維修及保養費用。此義務旨在確保社區內公共設施的正常運作和安全使用，以維護全體住戶的共同利益。

經管理委員會討論，近期社區內[具體描述需要維修的公共設施，如電梯、游泳池、健身房等]已進行

Message ChatGPT



人工智慧會提供(法律)領域更多新的工具



(Photos Licensed under CC BY 2.0 from Andrea Goh on Flickr)

- 人工智慧是什麼：好用就是聰明的**應用智慧**
- 機器學習是什麼：由**資料出發**實現人工智慧的主流方法
- 機器學習怎麼做：線性模型、**深度學習**等
- 機器學習為什麼：由訓練/測試關聯來**舉一反三**
- 機器學習怎麼用：預測、推薦、辨識、**生成**等
- 人工智慧往哪走：帶來**新的機會與挑戰**

**感謝聆聽！**