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

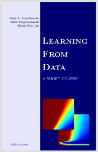
國立臺灣大學校友總會
2024「提升生活品質」系列演講—科技新知
二零二四年五月十八日

關於我：林軒田

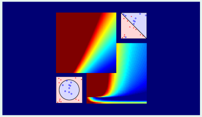
教授暨學士班校友(2001畢)
國立臺灣大學資訊工程學系

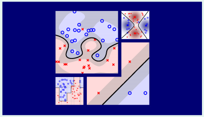
首席資料科學顧問
(前首席資料科學家)
沛星互動科技

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 ≈ 聰明 ≈ 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

應用智慧在我們身邊

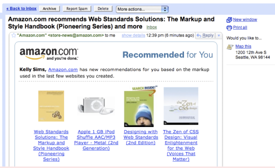
Siri語音助理

By Bernard Goldbach [CC BY 2.0]

掃地機器人

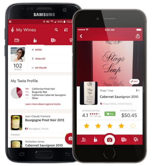
By Yuan-Chou Lo [CC BY-NC-ND 2.0]

電子商務產品推薦



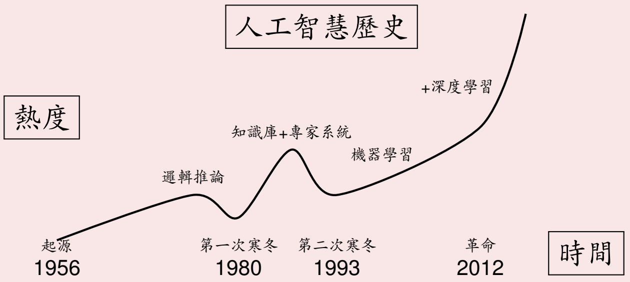
By Kelly Sims [CC BY 2.0]

Vivino: 紅酒資訊檢索



From nordic.businessinsider.com

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

這波人工智慧熱潮爲何不同？

資料更多

- 儲存與傳輸變得便宜
- 網路與行動裝置的發展

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

運算更快

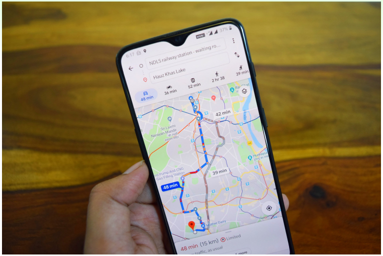
- 多機器運算，如雲端運算
- 多核心運算，如圖型加速器(GPU)

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？

我的機器學習初體驗(1/2)

2000年五月，大三的我，正在尋找大學部研究專題的指導老師

 ： 林智仁老師，請問您的研究主題是什麼？

 ： 我做支撐向量機(Support Vector Machine)的

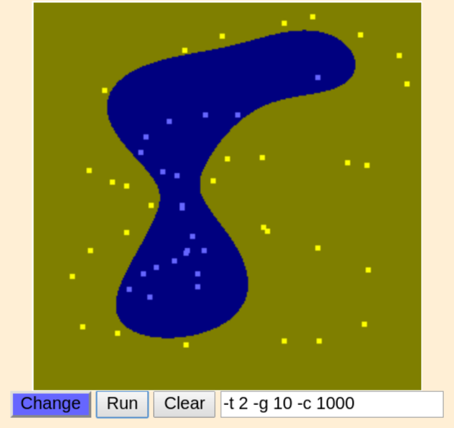
 ： (那是什麼？是土木系的某種建築器材嗎？)

https://www.csie.ntu.edu.tw/~cjlin/libsvm/

LIBSVM: A library for support vector machines 55862
CC Chang, CJ Lin

我的機器學習初體驗(2/2)

https://www.csie.ntu.edu.tw/~cjlin/libsvm/



https://www.youtube.com/watch?v=-W3pnicVgn0

某牛奶花生廣告：電腦嘛會揀土豆喔？

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

觀察 ⟶ 生物學習 ⟶ 技能

機器學習：由資料中累積/估計/計算經驗
以獲得技能

資料 ⟶ 機器學習 ⟶ 技能

什麼是技能？

技能就是「成績」提昇

技能 $\Longleftrightarrow$ 「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

資料 ⟶ 機器學習 → 成績提昇

應用實例一：股票預測

過去的股市資料 → 機器學習 → 好的投資表現

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

爲什麼要用機器學習？

- 爲樹下「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 ⟶ 機器學習 ⟶ 下一題會不會答對？

一個簡單的機器學習方法

會不會答對 ≈ ⟦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

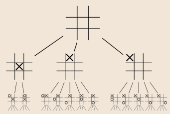
臺灣大學隊伍 2010 年獲得
KDDCup 世界冠軍的方法之一

好的人工智慧需要各種技巧

AlphaGo

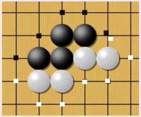
非機器學習

蒙地卡羅搜尋
≈ 模擬人腦推演



機器學習

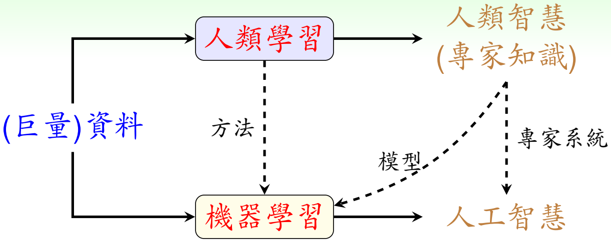
深度學習
≈ 模擬盤面分析



強化式學習
≈ 模擬(自我)對弈

好的人工智慧：要使用正確的
機器學習與非機器學習的技巧

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

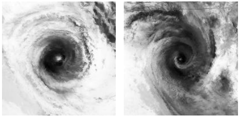
- 客觀
- 運用計算力量
- 持續的進步

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

人類學習

人類智慧
(專家知識)



颱風影像資料

卷積神經網路

影像旋轉不變性

現行氣象系統

機器學習

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？

機器學習爲什麼？

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

資料 ⟶ 機器學習 ⟶ 成績提昇

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

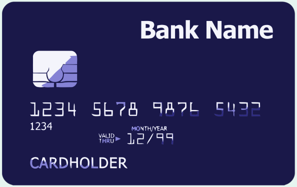
應用實例三：機器學習與信用卡核卡

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

$\Longrightarrow$

是否核卡？

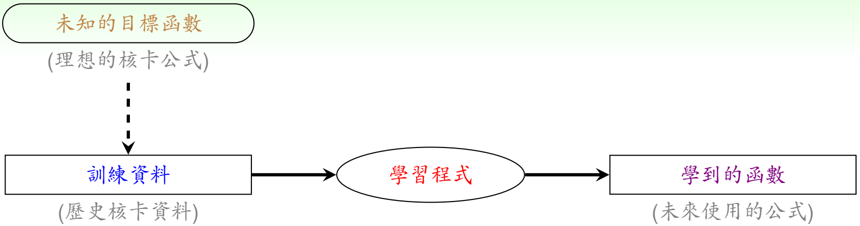


(Picture Licensed under CC0 on Pixabay)

可學的規律性：

申請人的背景資料$\Longrightarrow$ 核卡風險高不高？

怎麼學習「信用卡核卡」？

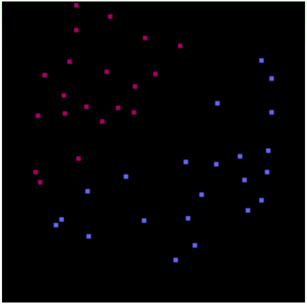


- 未知的目標函數
  (沒辦法輕易程式化)
- 希望：學到的函數和未知的目標函數很像
  (通常不會一模一樣)

什麼是「學習程式(模型+方法)」？

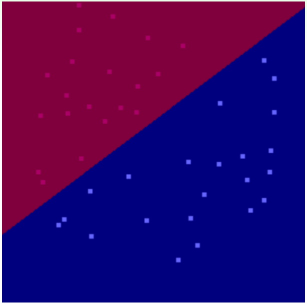
線性分類模型

負債



收入

負債

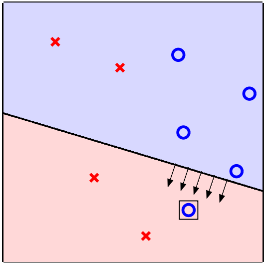


收入

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」

方法一：線性分類模型+知錯能改法

從隨便一條線開始，然後
「修正」它在已知資料中的錯誤之處



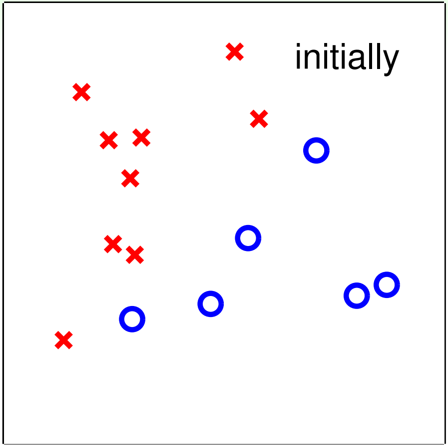
一次一次的做如下的操作

1. 找出給定資料中任一筆錯誤之處
2. 把線往適當的方向「轉一轉」來試著修正這筆錯誤

... 直到沒有任何錯誤，
便可將最後的線當作學到的函數

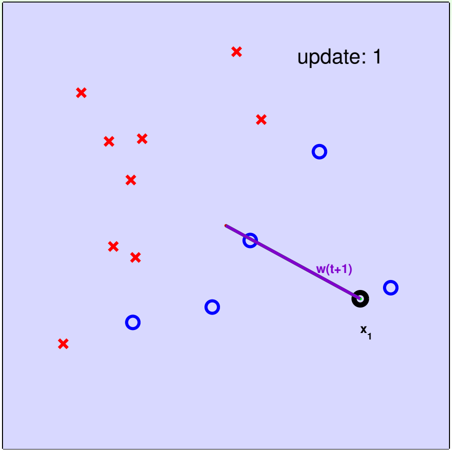
人誰無過？過而能改，善莫大焉
—左傳

眼見為憑：知錯能改法



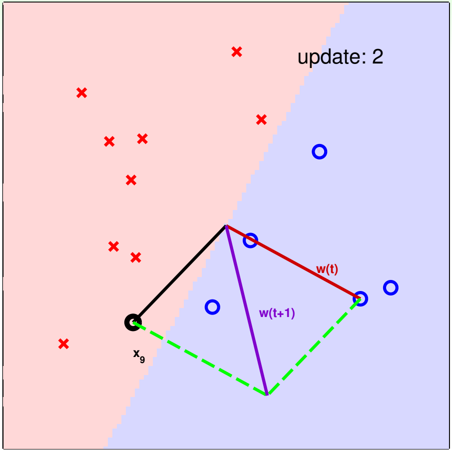
「數十行」的小程式即具有學習能力！

眼見為憑：知錯能改法



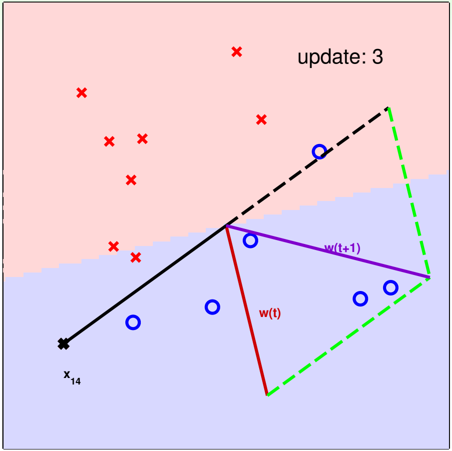
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



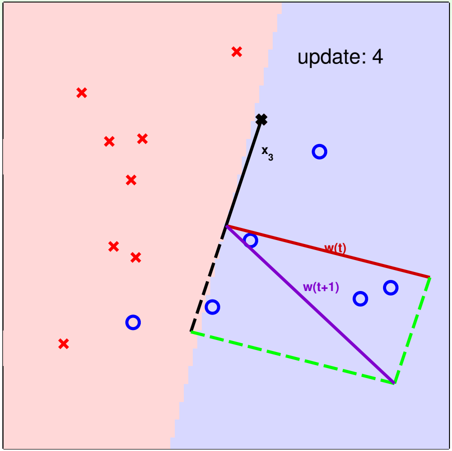
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



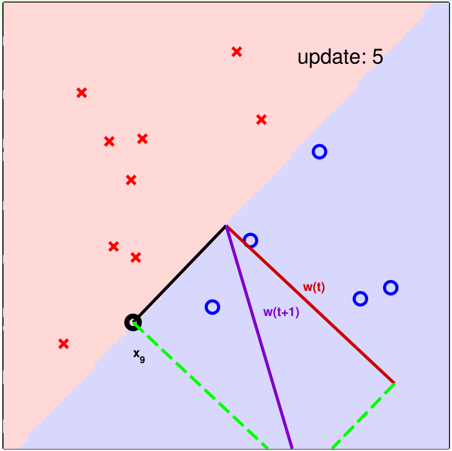
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



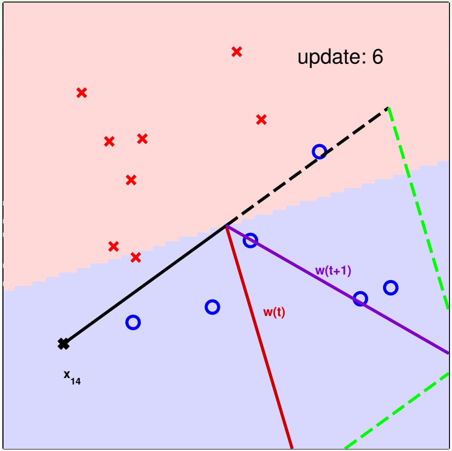
「數十行」的小程式即具有學習能力！

眼見為憑：知錯能改法



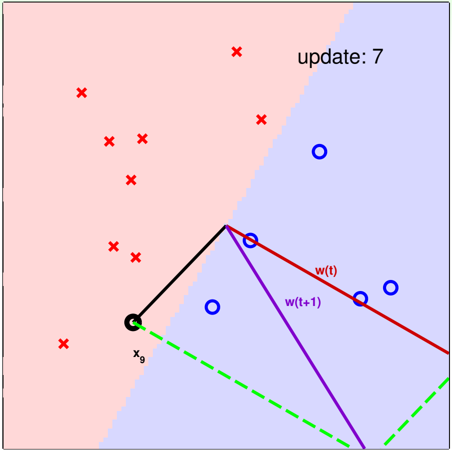
「數十行」的小程式即具有學習能力！

眼見為憑：知錯能改法



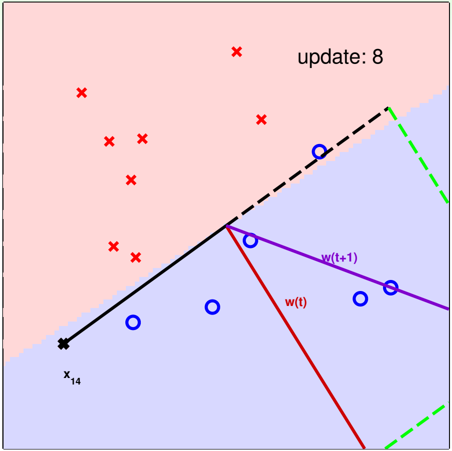
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



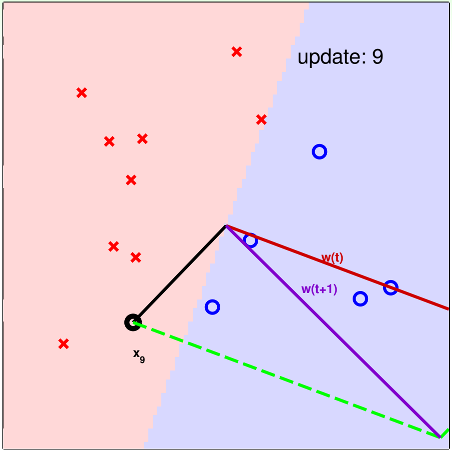
「數十行」的小程式即具有學習能力！

眼見為憑：知錯能改法



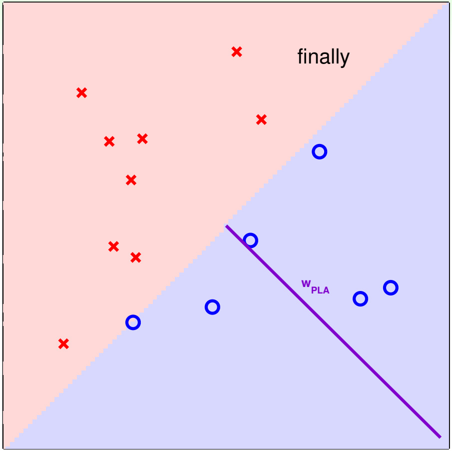
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



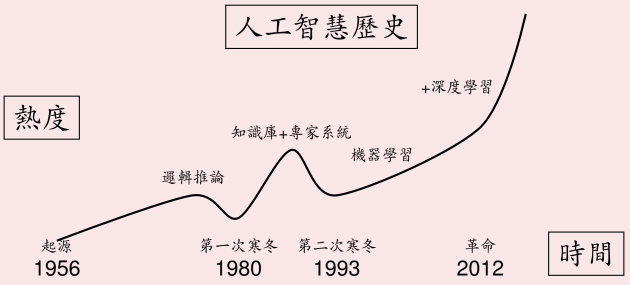
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



「數十行」的小程式即具有學習能力！

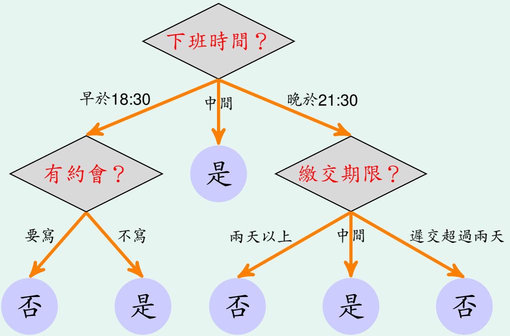
歷史回顧：知錯能改法(Rosenblatt, 1957)



- 原名：感知器學習法(Perceptron Learning Algorithm)
- 模擬「單一神經元」的(機率式)邏輯推論模型
- 公認爲「第一個」機器學習方法

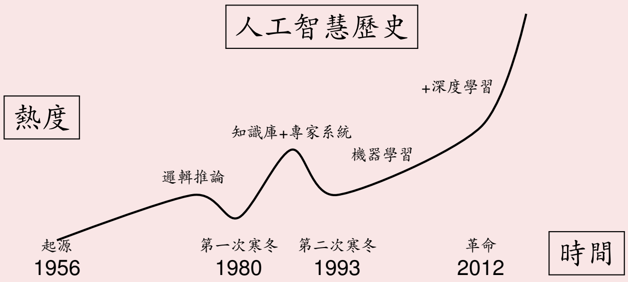
知錯能改法：其應用限制(Minsky and Papert, 1969)
爲第一次寒冬的推手之一

方法二：分而治之法



http://www.r2d3.us/visual-intro-to-machine-learning-part-1/

歷史回顧：分而治之法(Quinlan, 1986)

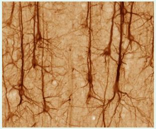


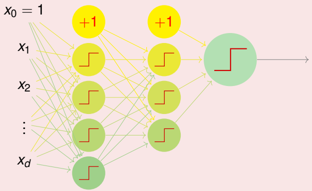
- 原名：決策樹法(Decision Tree Algorithms)
- 仿「專家系統」的機器學習模型
- 仍為資料探勘、作業研究、商業決策中常用的方法

分而治之法：隨著第二次寒冬在
「非」人工智慧的面相上找到其他價值

方法三：類神經網路

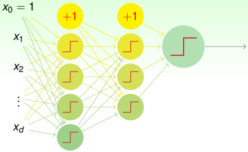
感知器(模擬「一個神經元」)：「畫一條直線」
類神經網路(模擬「一堆神經元」)：「畫非常複雜的邊界」(及其他)

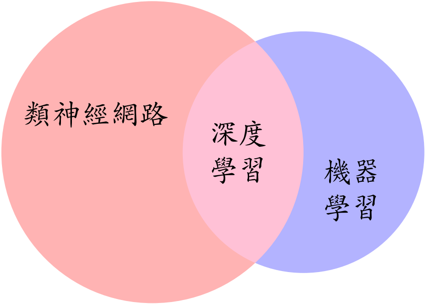


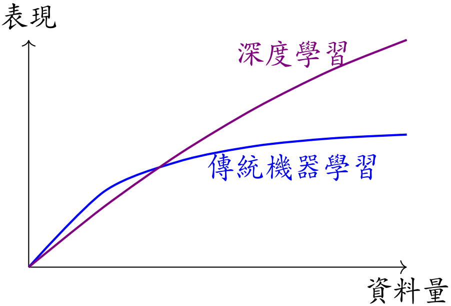


類神經網路：一種仿生模型

從類神經網路到深度學習



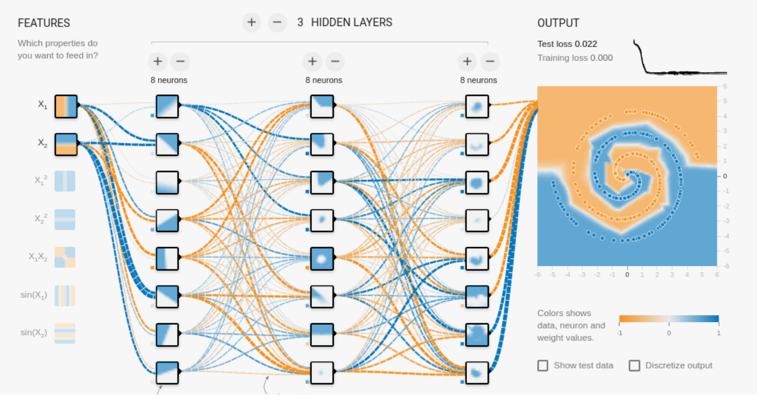




深度學習：用大量資料+大量計算
來解決(困難的)機器學習問題。

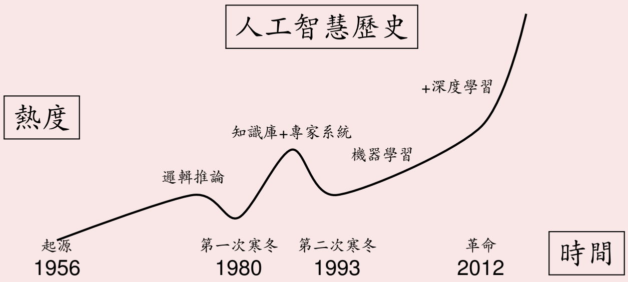
眼見為憑：深度學習法

https://playground.tensorflow.org/



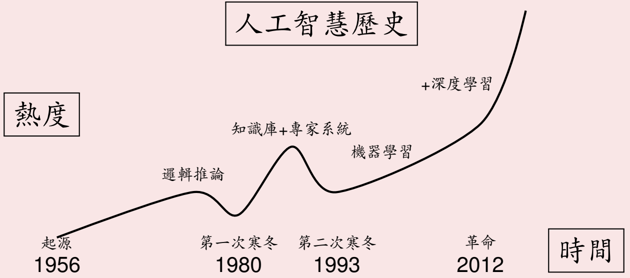
深度學習：每一層組合上一層的邊界們，
轉化出更複雜的邊界

歷史回顧：深度學習法(Hinton et al., 2006)

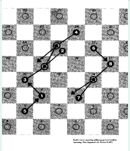


深度學習法：類神經網路在
第二次寒冬後捲土重來的再度復興

歷史回顧：從西洋跳棋到圍棋



(Samuel, 1959) Some studies in machine learning using the game of checkers



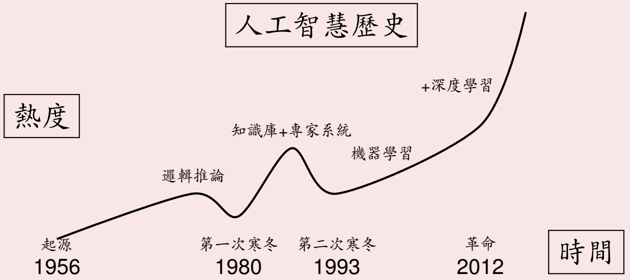
Picture extracted from the original paper of Samuel for educational purposes

(Silver et al., 2016) Mastering the game of Go with deep neural networks and tree search

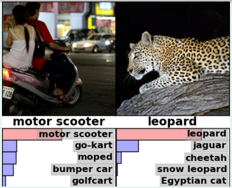
Picture by Wesalius, licensed under CC BY-SA 4.0 via Wikimedia Commons

棋類人工智慧的發展亦
見證了**機器學習**的興起

「歷史」回顧：從辨識到生成

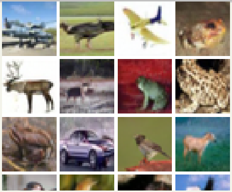


(Krizhevsky et al., 2012) ImageNet classification with deep convolutional neural networks



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

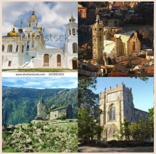
聽/讀/看

生成式機器學習

說/寫/畫

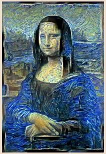
生成式的兩大特徵

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？

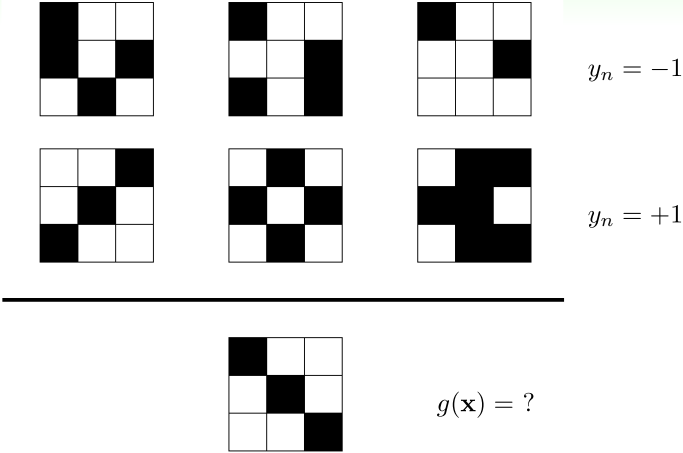
機器學習怎麼做？

機器學習爲什麼？

機器學習怎麼用？

人工智慧往哪走？

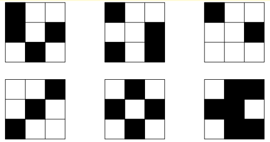
機器/人類學習小測驗



你的「人類學習」學到了什麼？

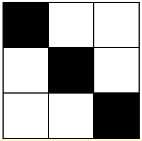
兩個可能的答案

不管你回答什麼



$y_n = -1$

$y_n = +1$



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

「標準答案」是+1，因爲...

- 對稱性$\Leftrightarrow$ +1

「標準答案」是-1，因爲...

- 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

摩斯密碼全球僅 2% 人破解(蘋果日報，20110928)

old url: https://tw.appledaily.com/new/realtime/20110928/77044/

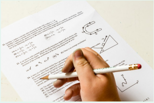
5+3+2=151022，那7+2+5 答案爲何？

- 「標準」答案：143547(爲什麼？47=14+35-2; 22=15+10-3)
- 「轉彎」答案：143546(爲什麼？46=14+35-3; 22=15+10-3)

機器學習與人生：是否眞有標準答案？

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？

機器學習爲什麼？

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

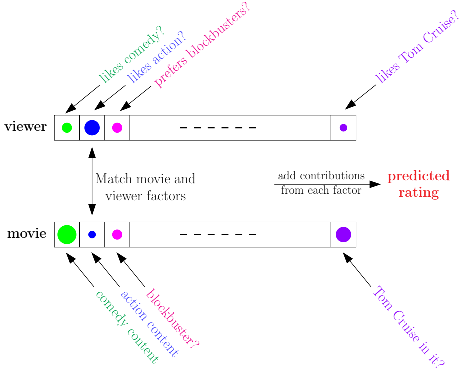
(Photos Licensed under CC BY 2.0 from Andrea Goh on Flickr)

- 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

機器學習已廣泛地實現應用智慧

應用實例五：推薦系統

過去的評分資料 → **機器學習** → 個人化電影推薦



機器學習如何解

- 模型:

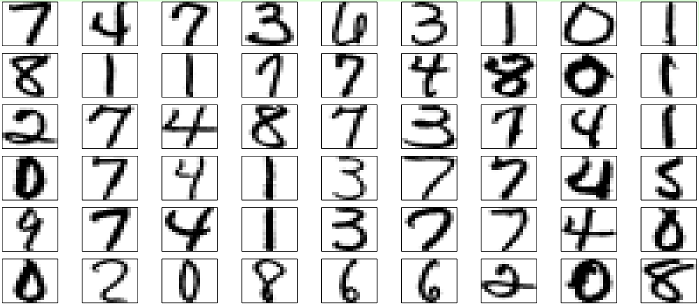
  已知評分

  → 反推喜好特徵

  → 評分預測

臺灣大學隊 2011 年獲得
KDDCup 世界冠軍的方法之一

應用實例六：手寫辨識



- 早在我們身邊很久了！
  - 郵遞區號
  - 支票處理自動化
  - 手寫輸入
- 早期「深度學習」發展的重要動力

  http://yann.lecun.com/exdb/lenet/

科技始終來自人性！

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？

機器學習爲什麼？

機器學習怎麼用？

人工智慧往哪走？

當代人工智慧的發展

2010–2015: AI |

人工智慧顯出價值

- 深度學習開始出現成功案例
- 成熟的模型與工具(如LIBSVM)

2016–2020: AI +

人工智慧具競爭力

- 超越人類的表現(如AlphaGo)
- 大型科技公司轉爲人工智慧優先

2021–: AI ×

人工智慧不可或缺

- 「你不會被人工智慧取代，但會被懂得用人工智慧的人取代」
  (孫民・沛星科技前首席人工智慧科學家・2018)

人工智慧將成「基本能力」

人工智慧與工業革命

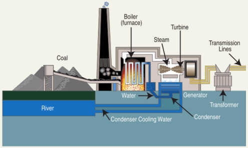
第一次

蒸汽機

(under CC-BY-SA 3.0 by Malcolm Best on Wikimedia)

第二次

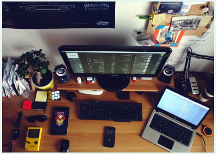
石油/電力



(in public domain on Wikimedia)

第三次

計算/通訊



(under CC-0 on Pixnio)

人工智慧常被視爲第四次工業革命

(free on Adobe Stock)

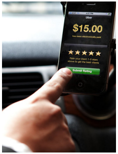
工業革命與工作昇級

第一次	第二次	第三次
蒸汽機	石油/電力	計算/通訊

馬車伕

火車司機

計程車司機



共享車司機

第四次工業革命(人工智慧)：
工作不會完全消失，而會再昇級！

four figures from:

- in public domain on Wikimedia
- under CC-BY-SA 2.0 by H. Michael Miley on Flickr
- under CC-BY-SA 4.0 by Jean-max mejean on Wikimedia
- under CC-BY-NC 2.0 by Melies The Bunny on Flickr

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`

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

結語

(巨量)資料 → 機器學習 → 人工智慧

食材

工具/步驟

佳餚

- 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：知錯能改、分而治之、深度學習等
- 機器學習爲什麼：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：成爲工作昇級的基本能力

感謝聆聽！