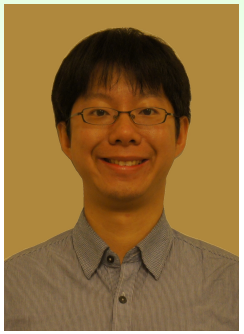
開發機器的學習潛能
—鑽牛角尖或舉一反三？

林軒田(Hsuan-Tien Lin)
htlin@csie.ntu.edu.tw

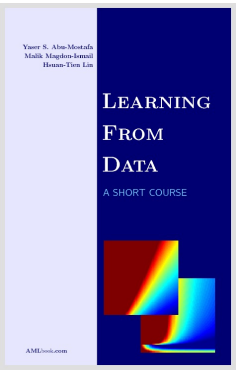
國立台灣大學
National Taiwan University

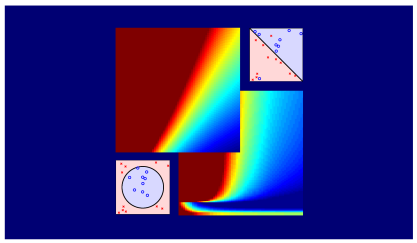
台北地方法院
05/19/2023

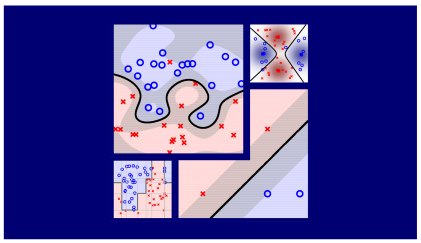
關於我：林軒田



- 台灣大學資訊工程學系教授
- 沛星互動科技首席資料顧問(前首席資料科學家)
- “Learning from Data(由資料中學習): A Short Course”共同作者
- 華語教學之線上大型開放式課程授課教師
  - “Machine Learning Foundations(機器學習基石)”
  - “Machine Learning Techniques(機器學習技法)”







接下來要講的是……

機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

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，台大資訊系內招生宣傳(2008)

技能就是(弱)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

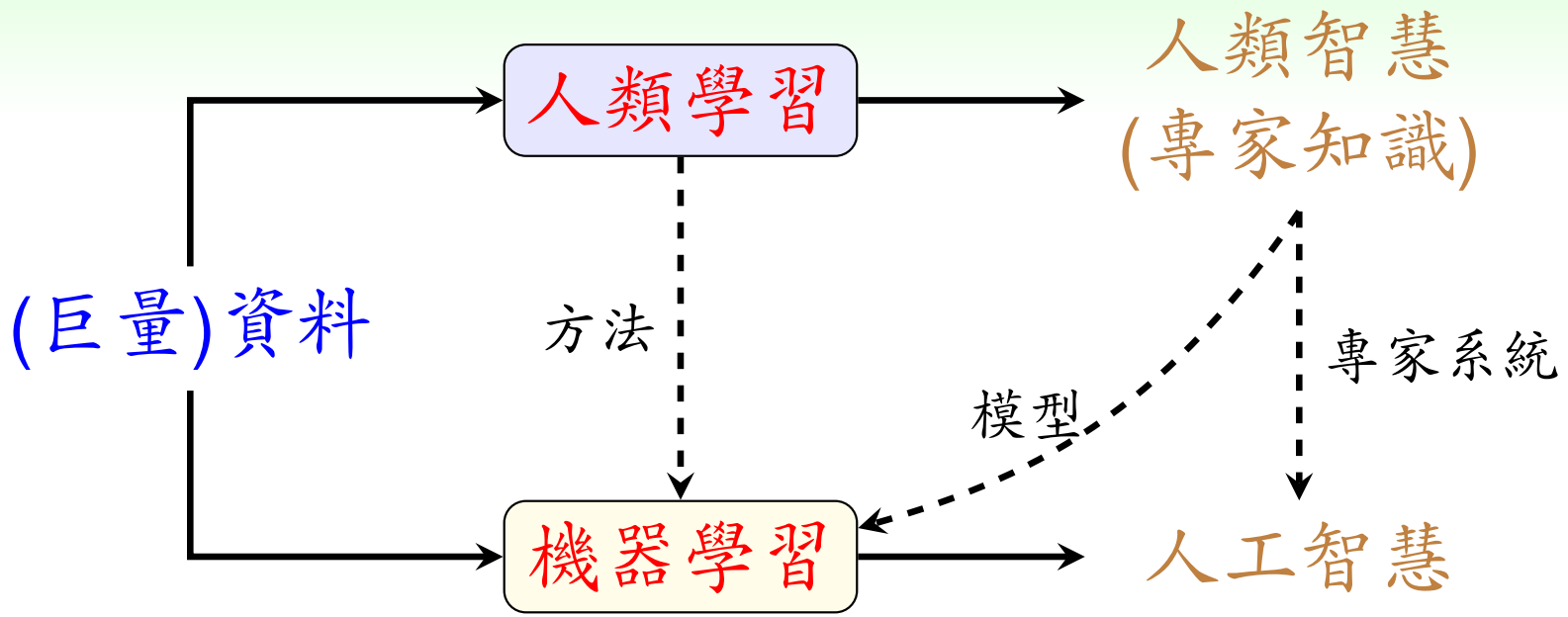
沛星科技首席資料科學家 ≡ 餐廳主廚

爲什麼要用機器學習？

- 爲樹下‘規則定義’再寫成程式碼：
  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

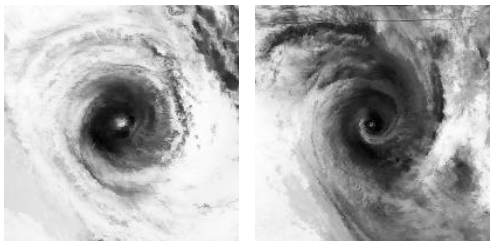
機器學習：打造人工智慧系統的
一條(充滿潛力的)路徑

機器學習與當代人工智慧



機器學習已成爲實現當代
人工智慧的主流路徑

應用實例二：颱風強度判讀



颱風影像資料

人類學習

人類智慧
(專家知識)

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)

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

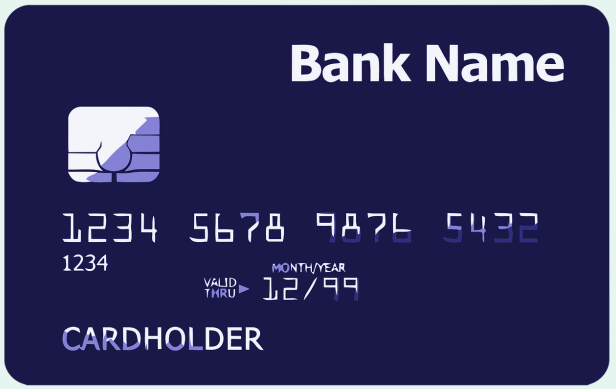
應用實例三：機器學習與信用卡核卡

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？

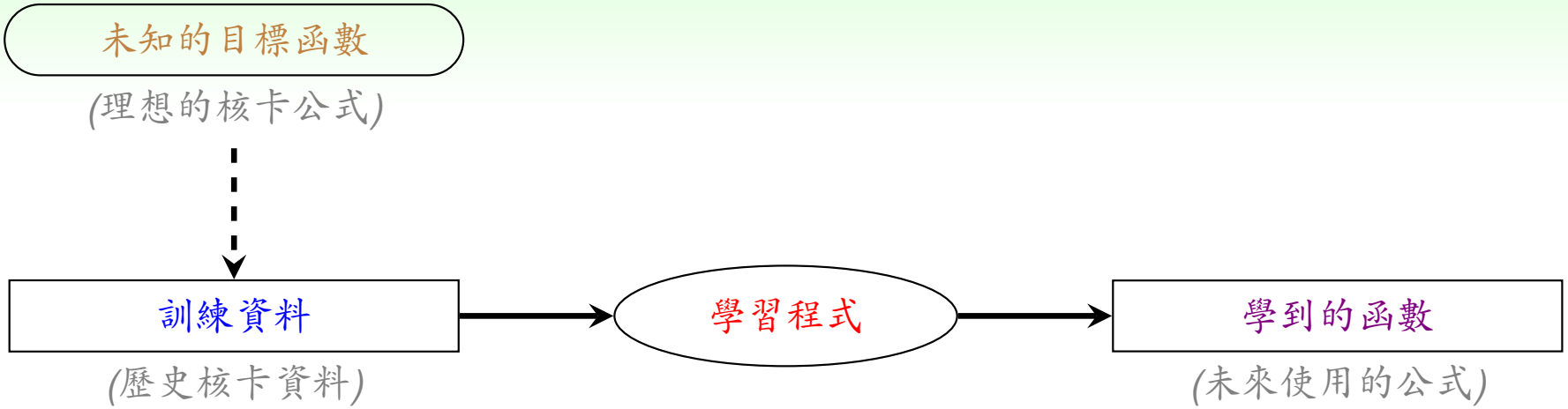


(Picture Licensed under CC0 on Pixabay)

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)」？

接下來要講的是……

機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

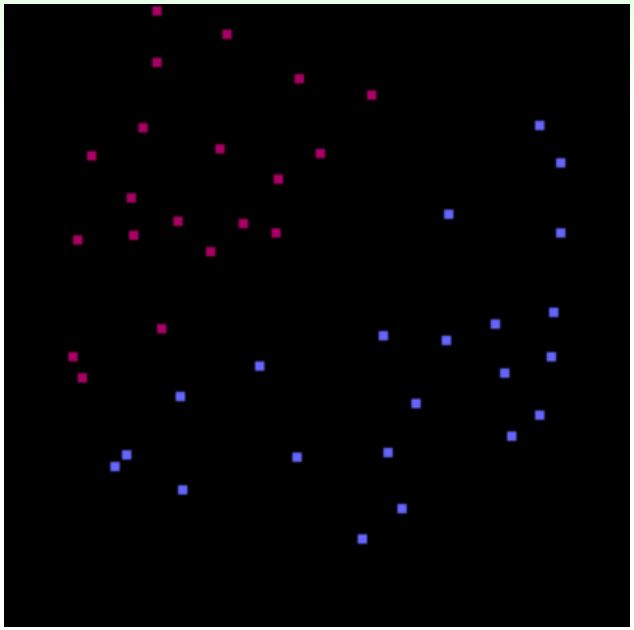
機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

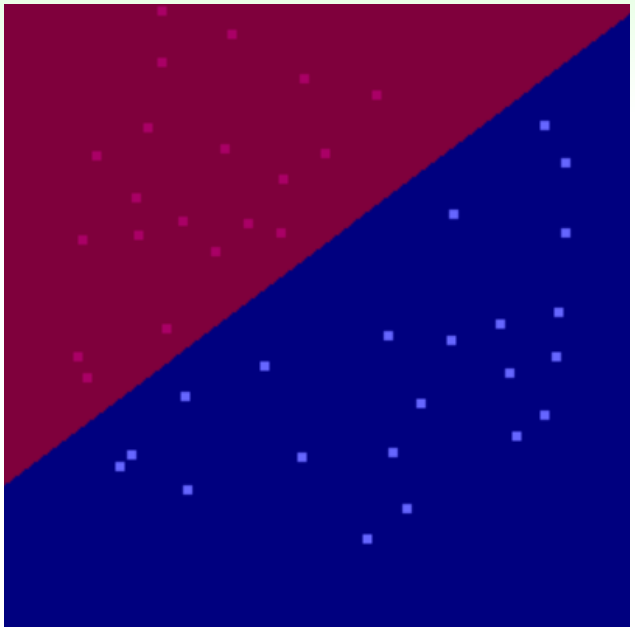
線性分類模型

負債



收入

負債

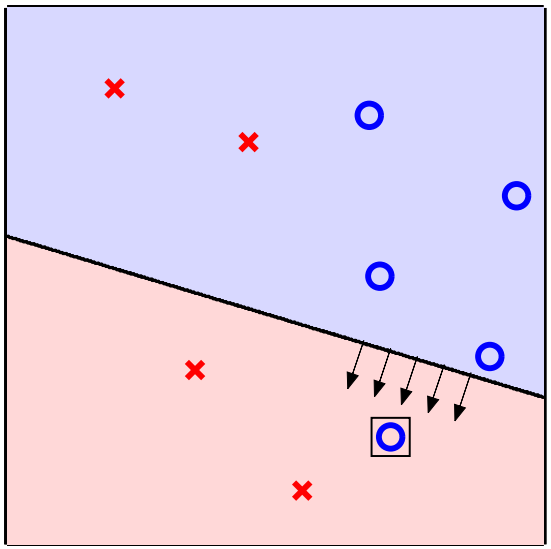


收入

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」

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



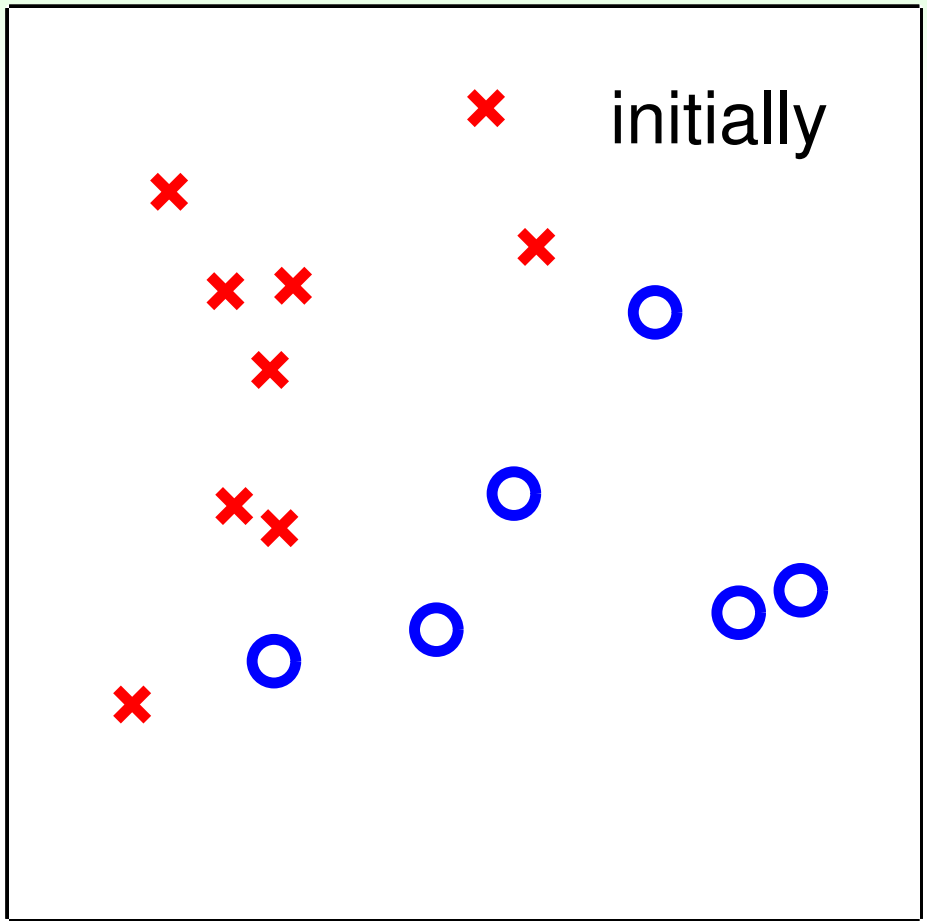
一次一次的做如下的操作

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

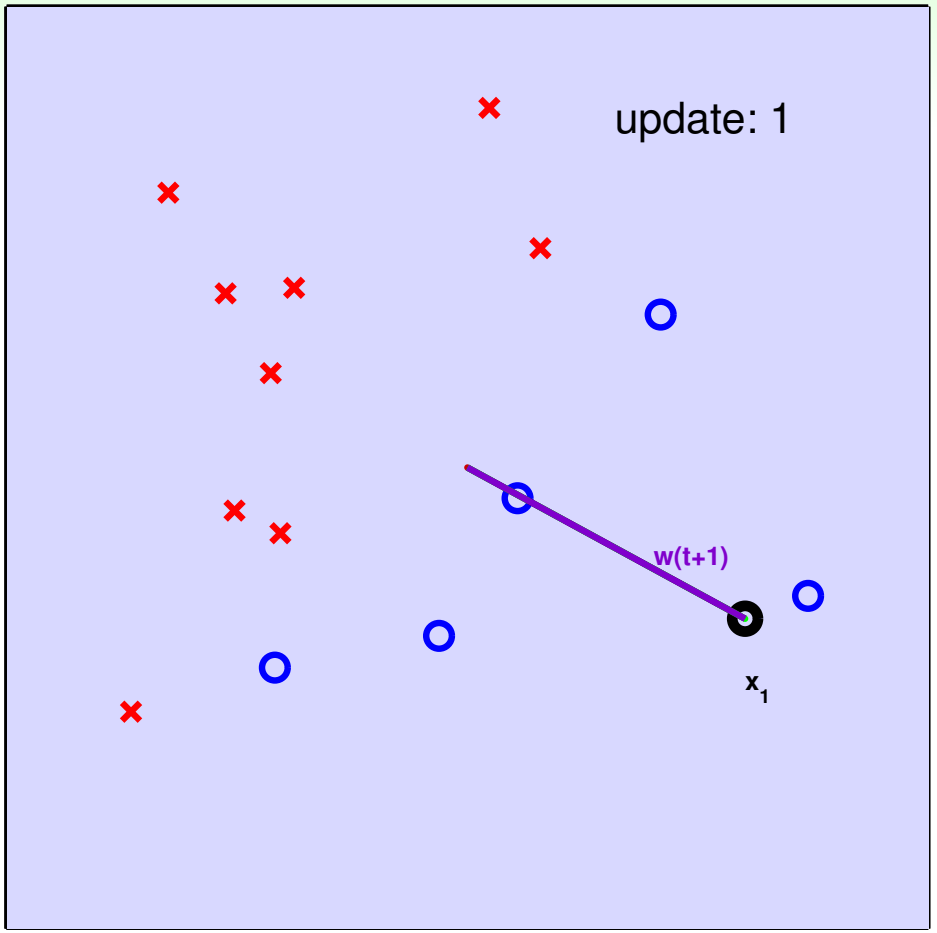
人誰無過？過而能改，善莫大焉
—左傳

眼見爲憑：知錯能改法



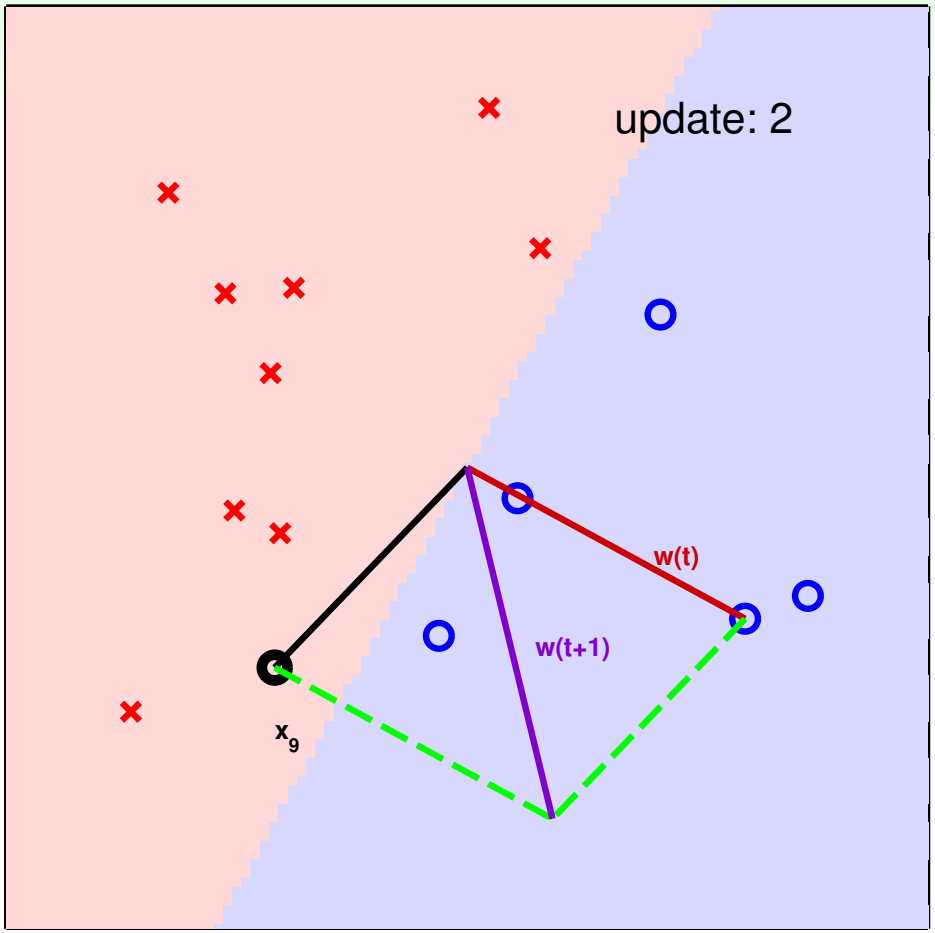
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



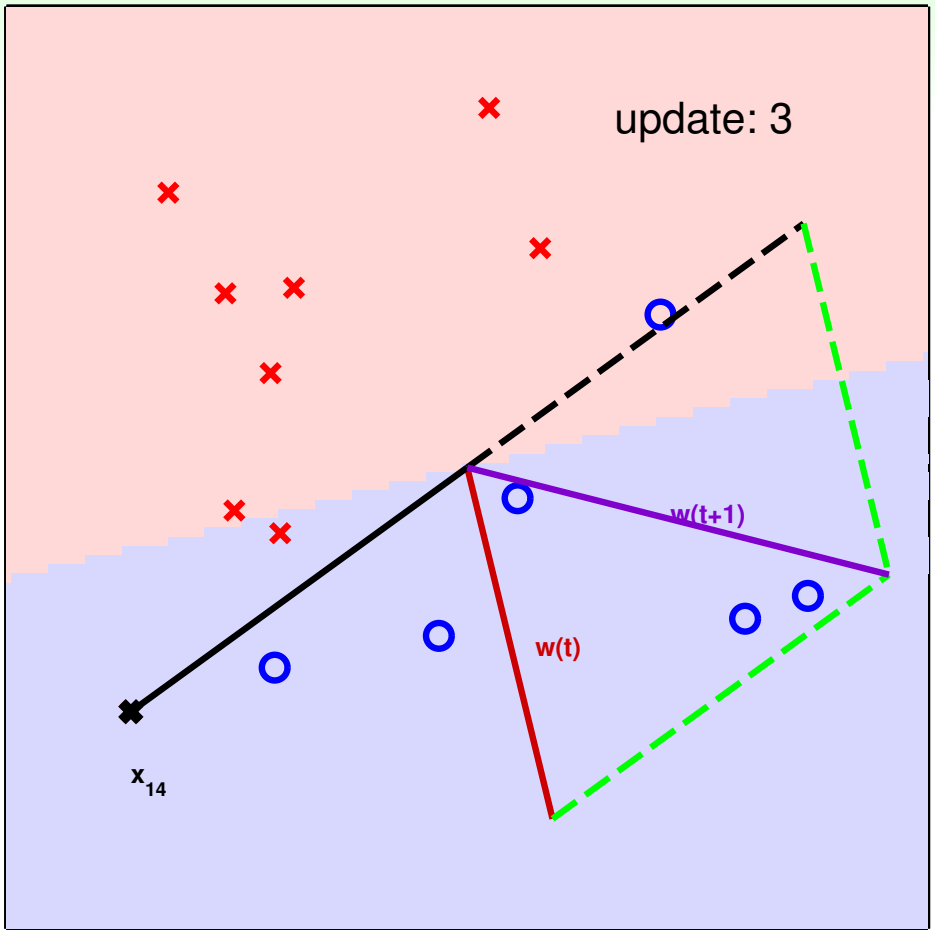
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



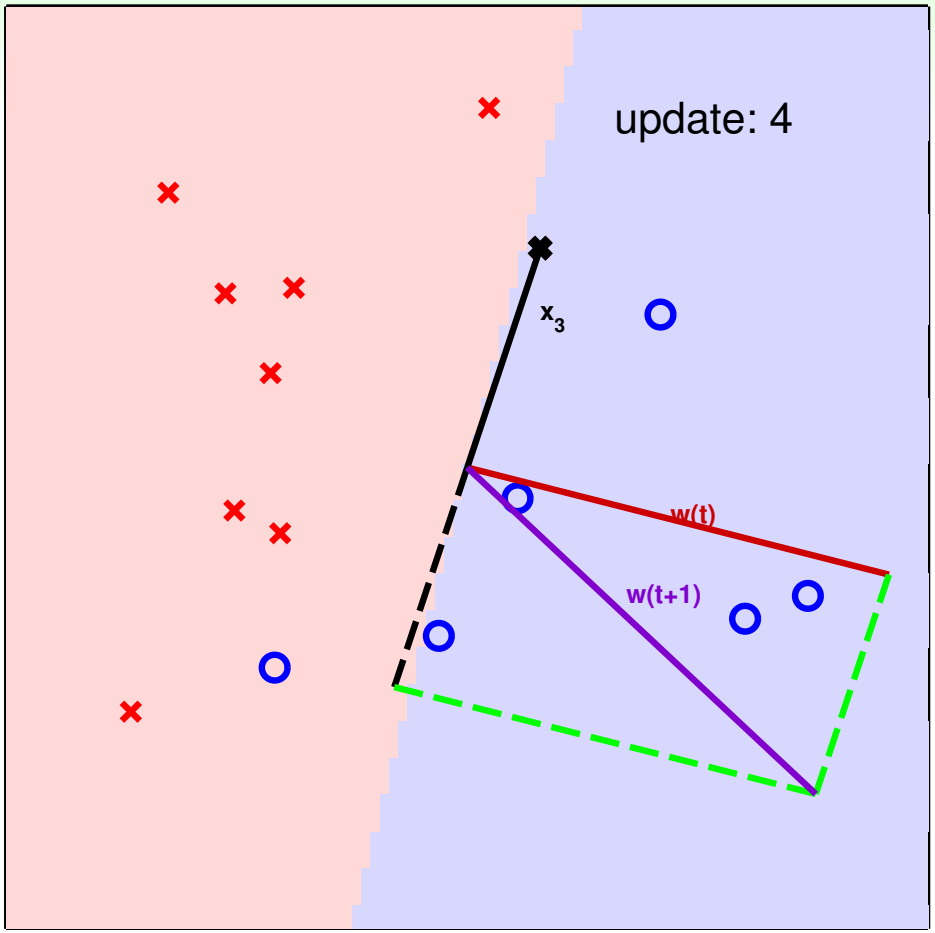
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



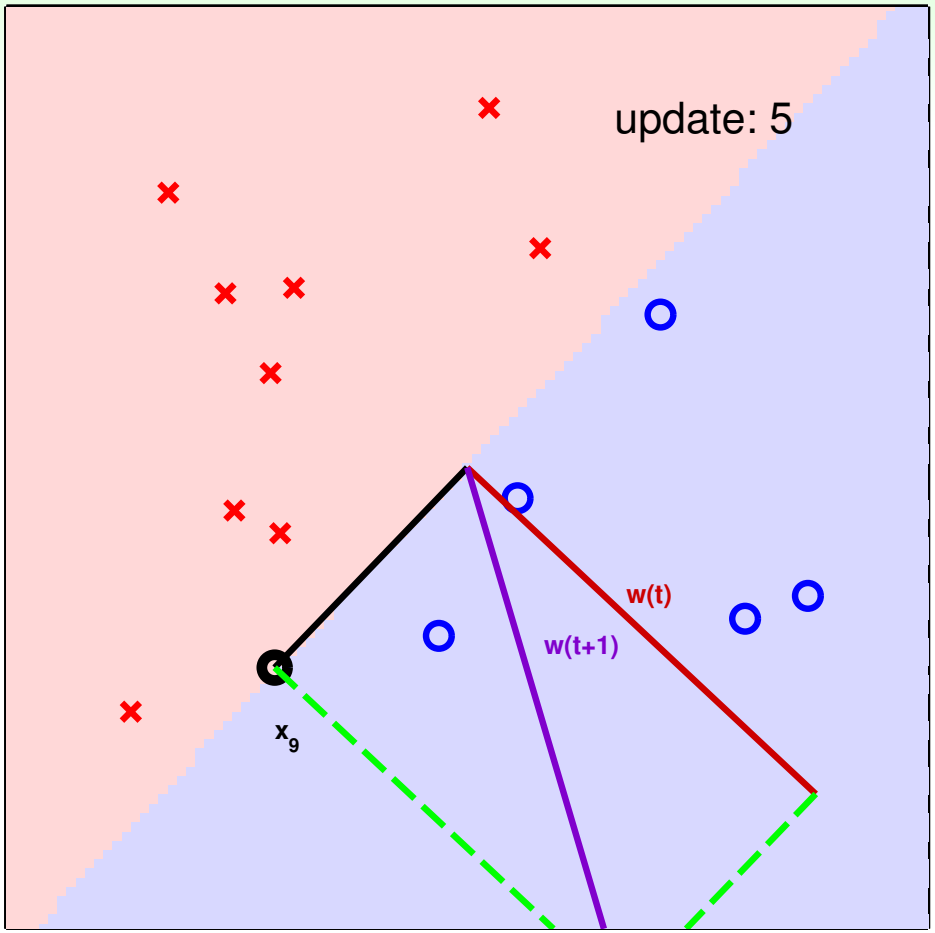
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



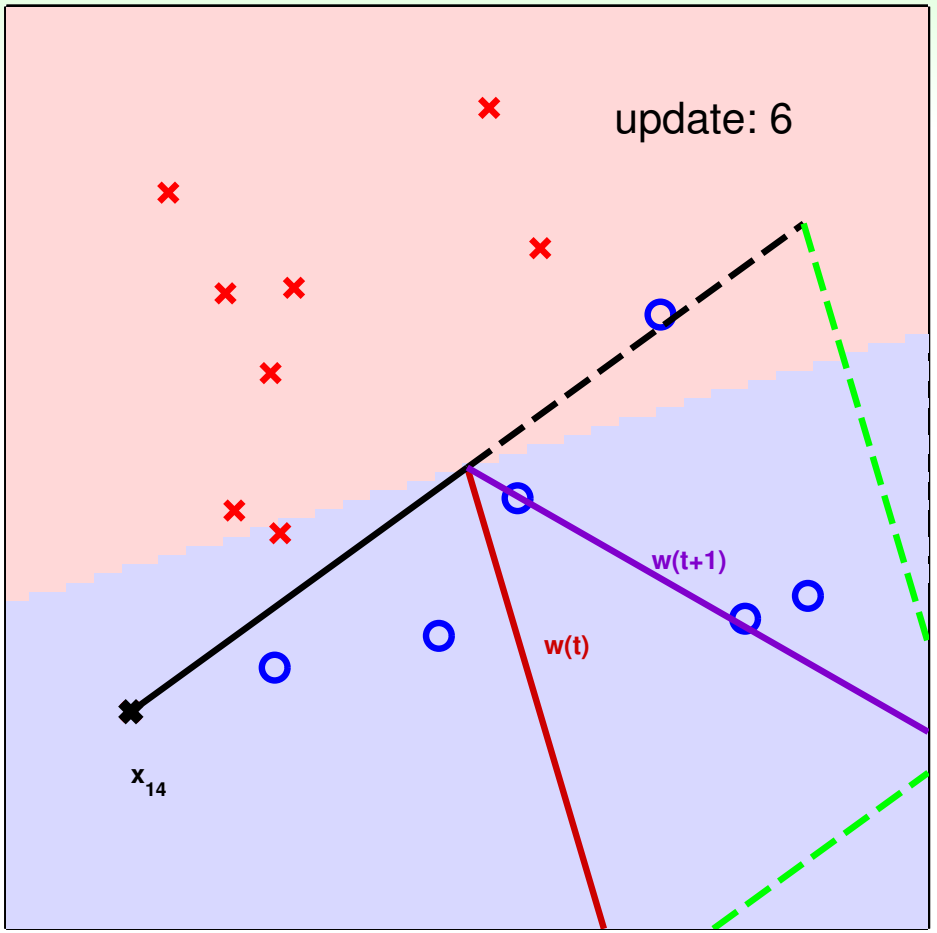
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



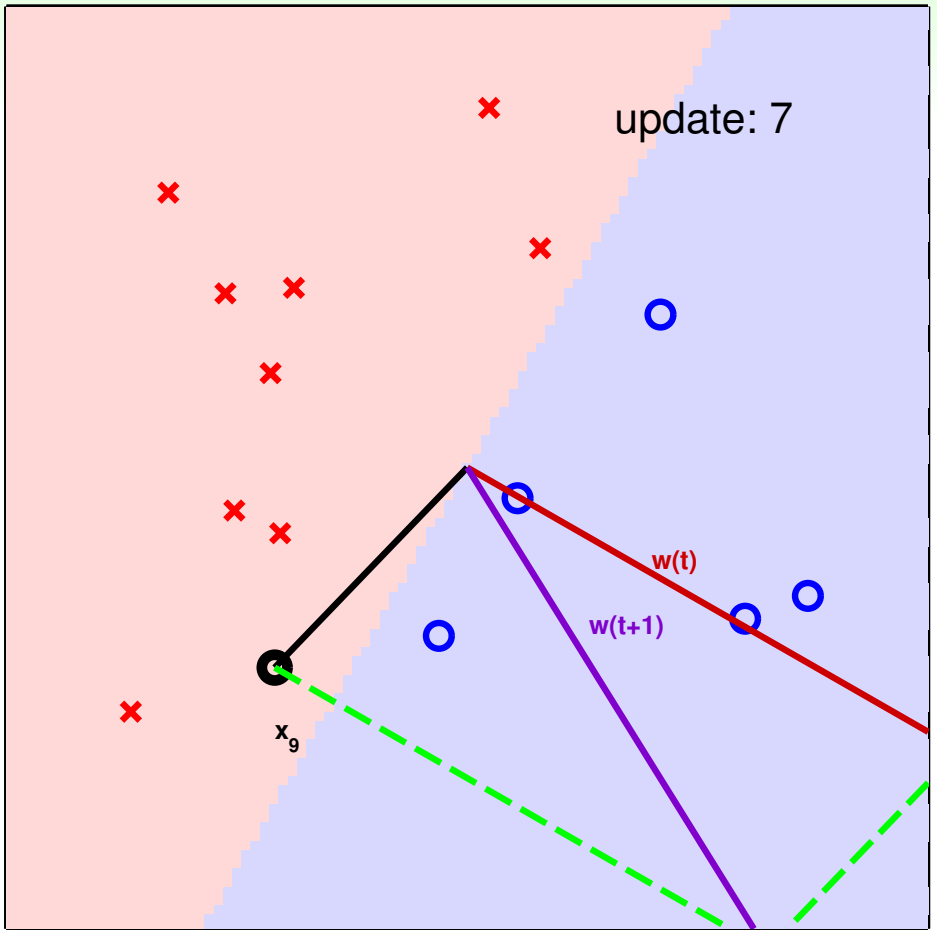
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



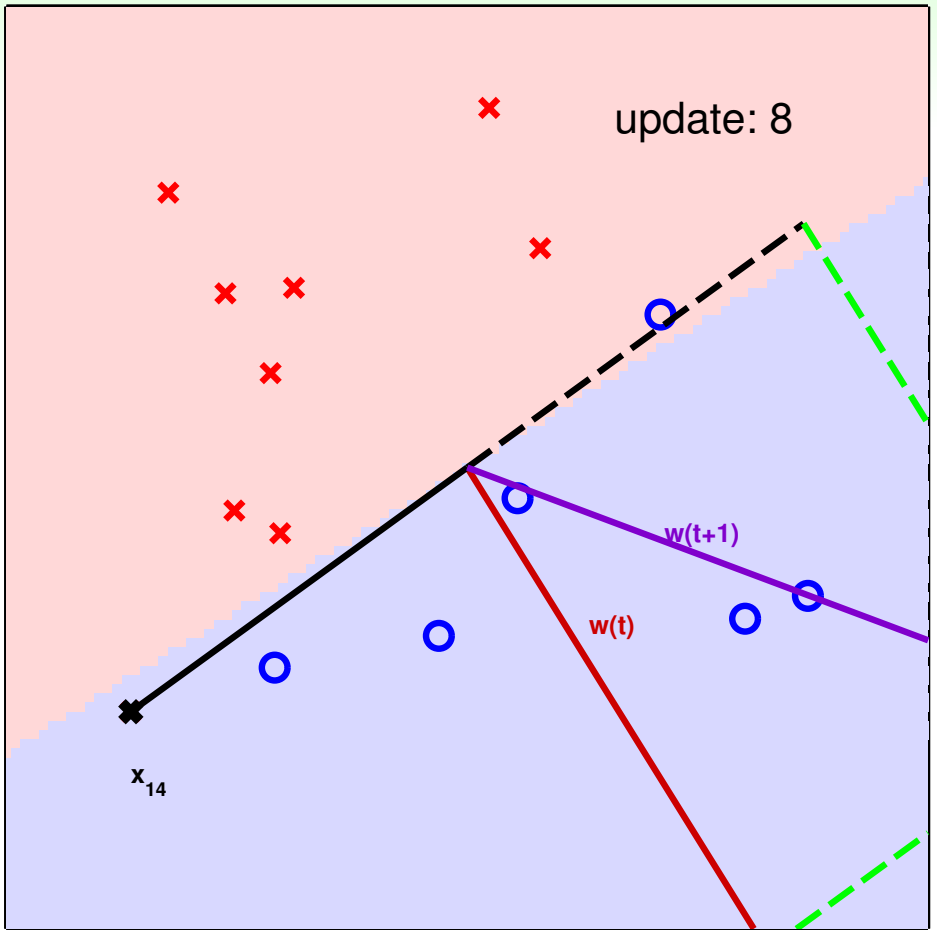
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



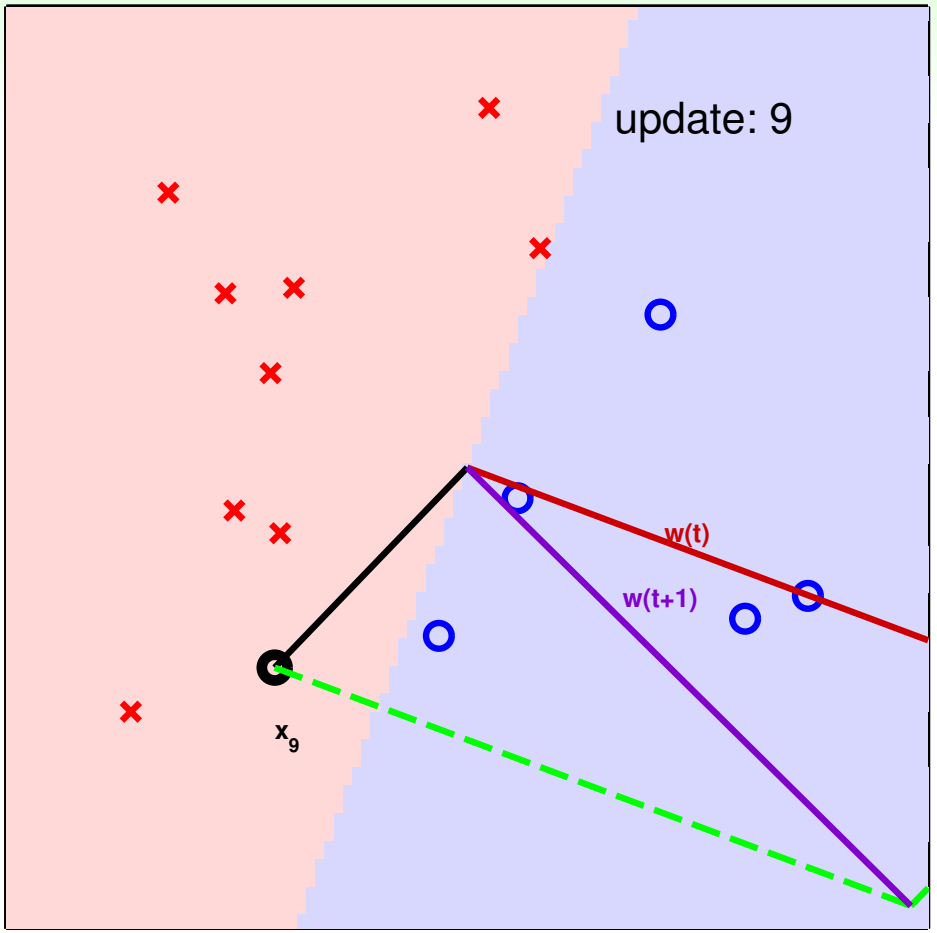
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



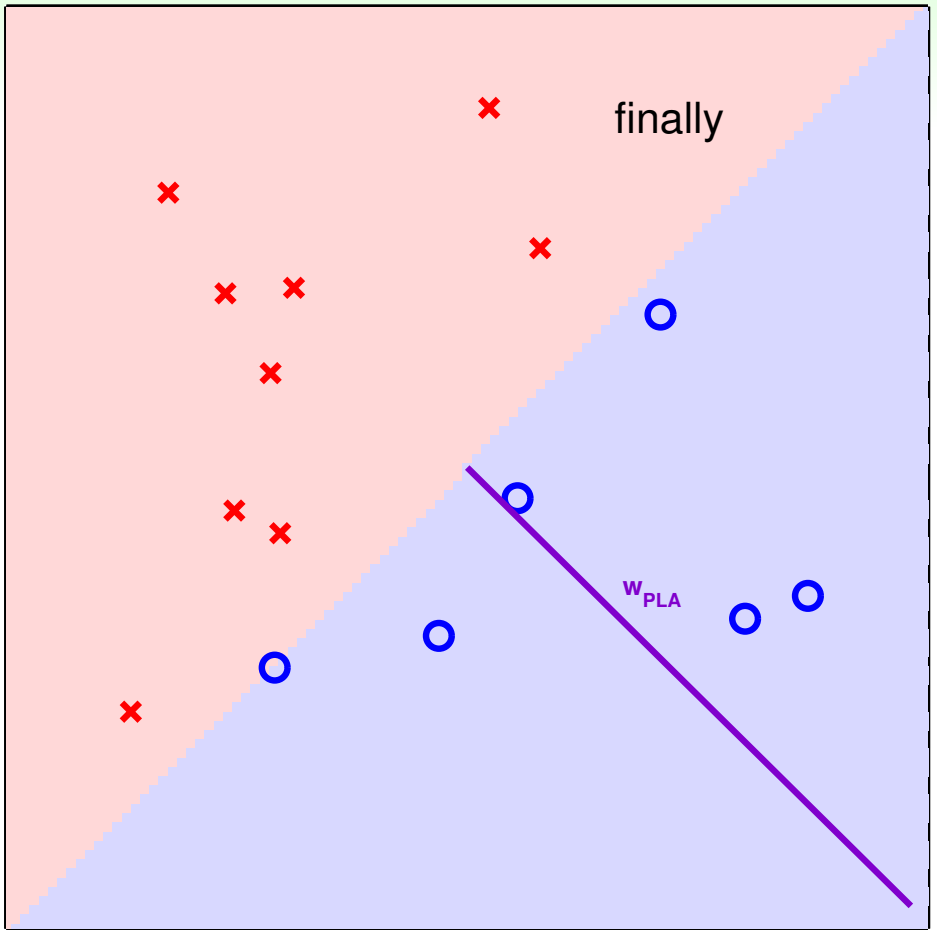
「數十行」的小程式即具有學習能力！

眼見爲憑：知錯能改法



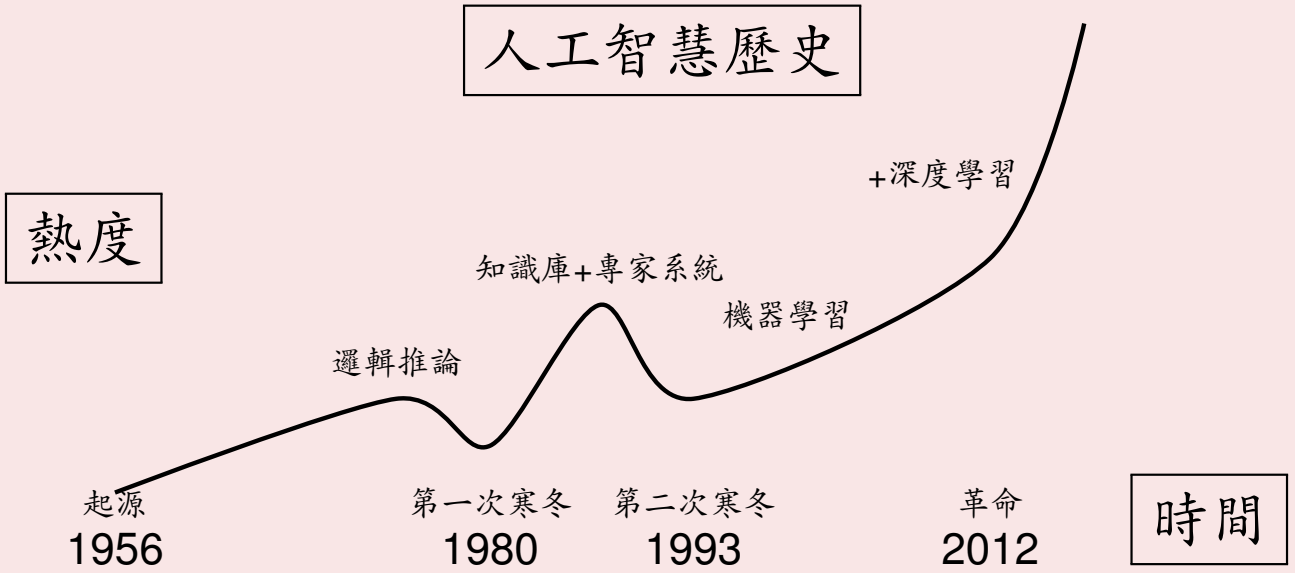
「數十行」的小程式即具有學習能力！

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

接下來要講的是……

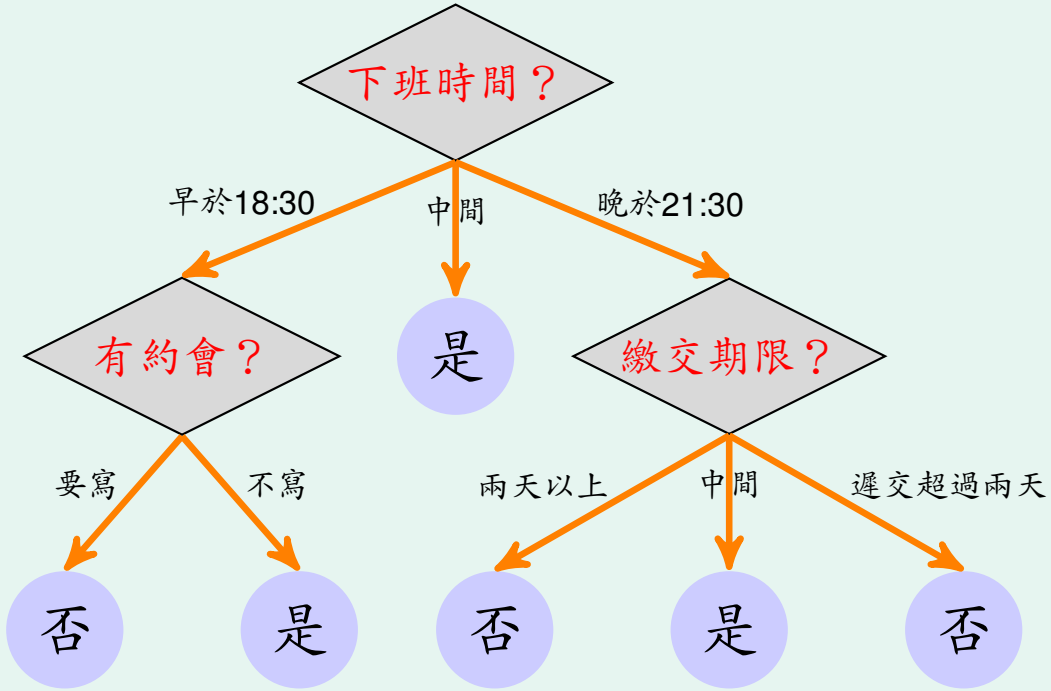
機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

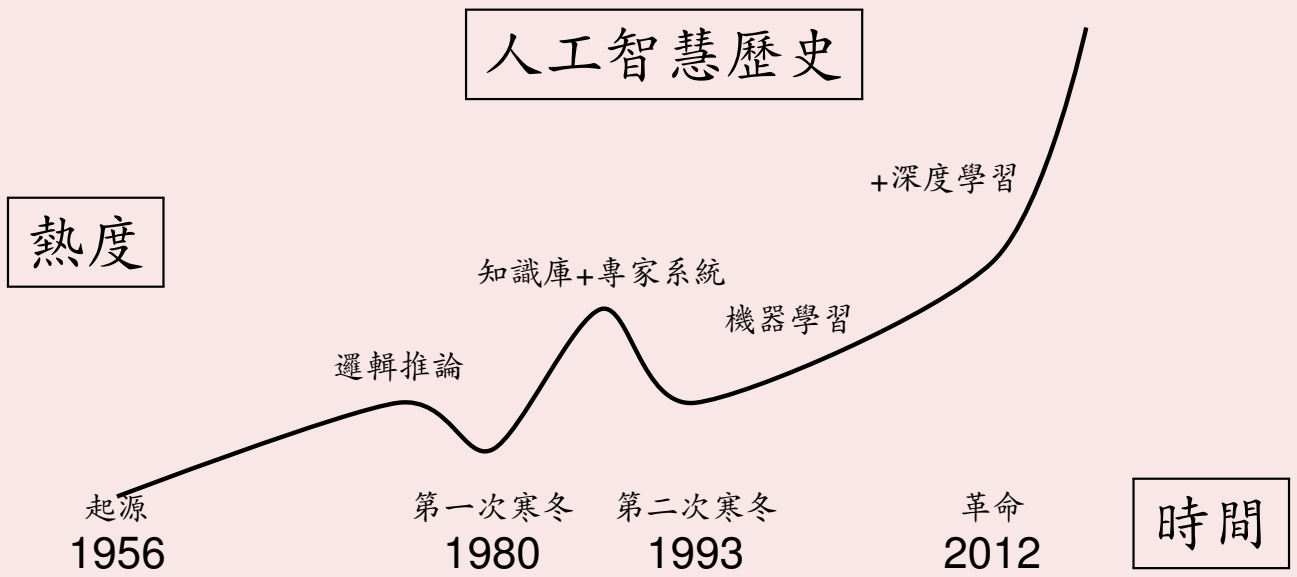
機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

分而治之法



http://www.r2d3.us/圖解機器學習第一章/

歷史回顧：分而治之法(Quinlan, 1986)



- 原名：決策樹法(Decision Tree Algorithm(s))
- 仿「專家系統」的機器學習模型
- 仍爲資料探勘、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

接下來要講的是……

機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

應用實例四：蘋果辨識問題

- 這張圖裡是否有蘋果呢？
- 我們來教小一學生學習吧！
- 由網路上收集了一些圖片 (Photos Licensed under CC-BY-2.0 on Flicker)
  感謝以下的作者們！

(APAL stands for Apple and Pear Australia Ltd)

Dan Foy
https://flic.kr/p/jNQ55

APAL
https://flic.kr/p/jzP1VB

adrianbartel
https://flic.kr/p/bdy2hZ

ANdrzej cH.
https://flic.kr/p/51DKA8

Stuart Webster
https://flic.kr/p/9C3Ybd

nachans
https://flic.kr/p/9XD7Ag

APAL
https://flic.kr/p/jzRe4u

Jo Jakeman
https://flic.kr/p/7jwtGp

APAL
https://flic.kr/p/jzPYNr

APAL
https://flic.kr/p/jzScif

應用實例四：蘋果辨識問題

- 這張圖裡是否有蘋果呢？
- 我們來教小一學生學習吧！
- 由網路上收集了一些圖片 (Photos Licensed under CC-BY-2.0 on Flicker)
  感謝以下的作者們！

Mr. Roboto.

https://flic.kr/p/i5BN85

Richard North

https://flic.kr/p/bHhPkB

Richard North

https://flic.kr/p/d8tGou

Emilian Robert Vicol

https://flic.kr/p/bpmGXW

Nathaniel McQueen

https://flic.kr/p/pZv1Mf

Crystal

https://flic.kr/p/kaPYp

jfh686

https://flic.kr/p/6vjRFH

skyseeker

https://flic.kr/p/2MynV

Janet Hudson

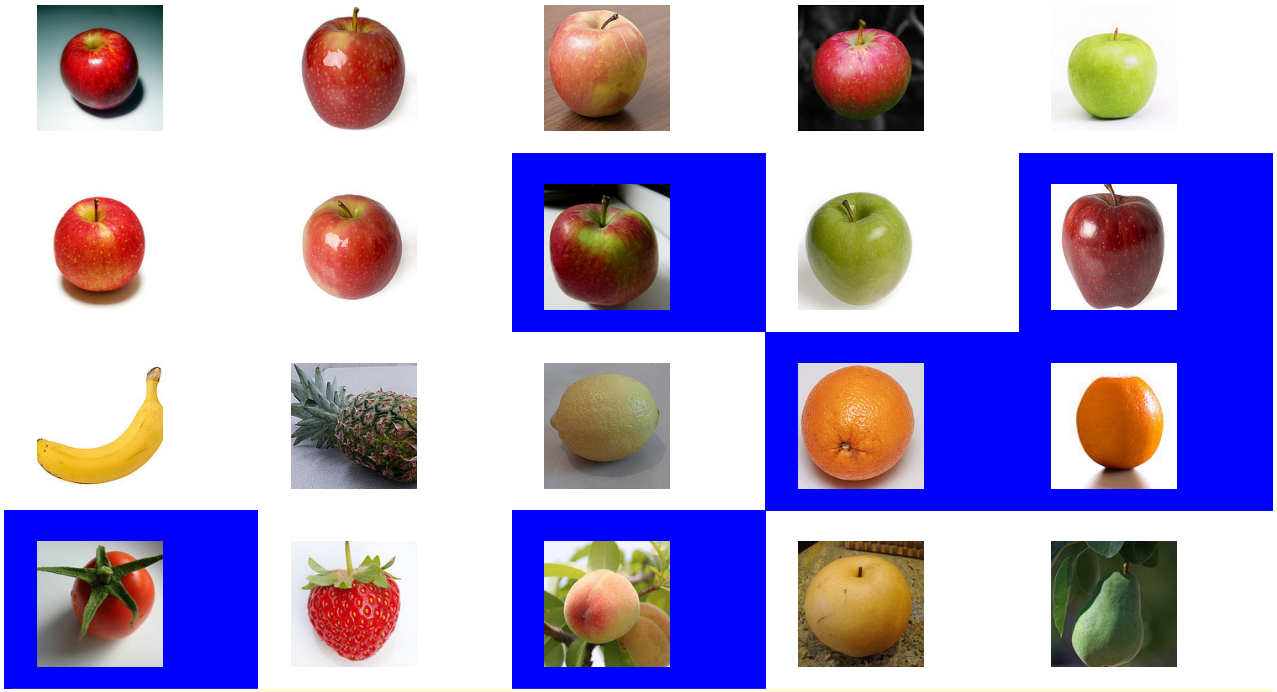
https://flic.kr/p/7QDBbm

Rennett Stowe

https://flic.kr/p/agmnrk

蘋果辨識課：第一講

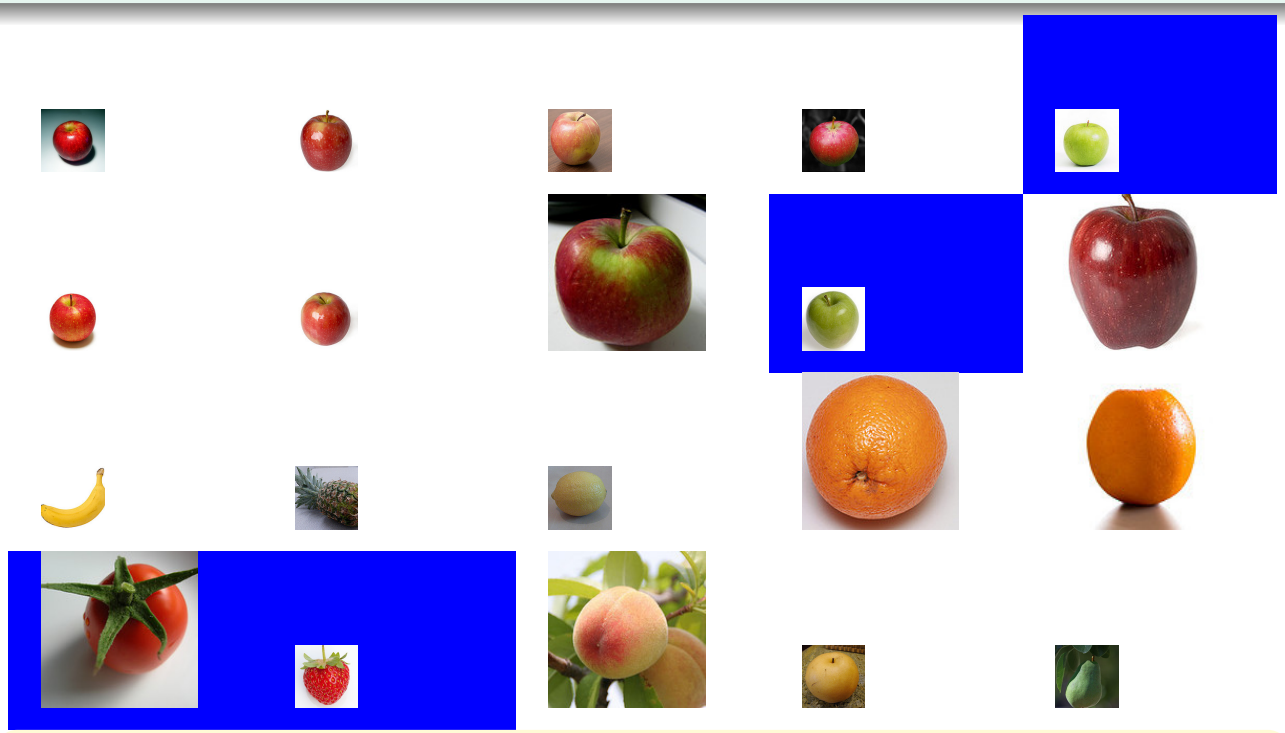
- 老師：大家來看看這些蘋果圖以及其他的水果圖。小明，請問你會如何描述一顆蘋果呢？
- 小明：我認爲蘋果是圓的。



(全班)：蘋果是圓的。

蘋果辨識課：第二講

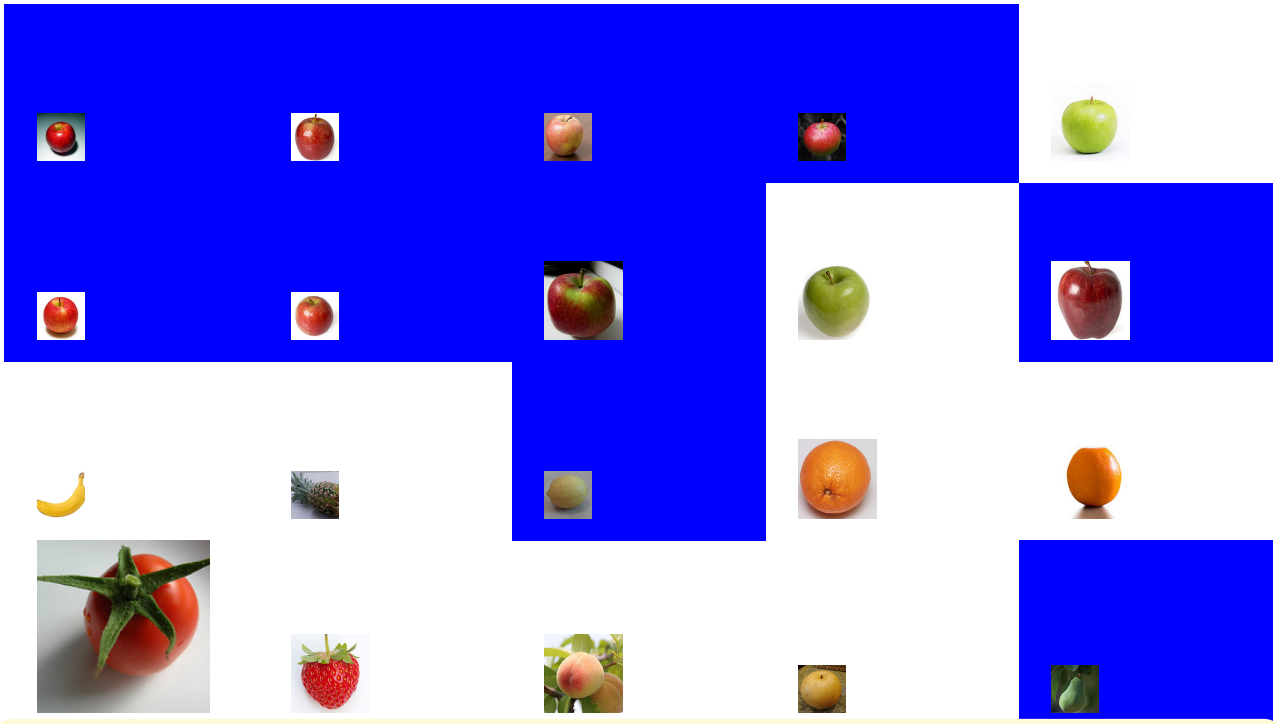
- 老師：圓形的確是蘋果的重要特徵。但如果只用圓形來做區分的話，可能會有些地方分錯。小華，你覺得還可以怎麼描述一顆蘋果呢？
- 小華：看起來蘋果是紅的。



(全班)：蘋果是圓的而也是紅的。

蘋果辨識課：第三講

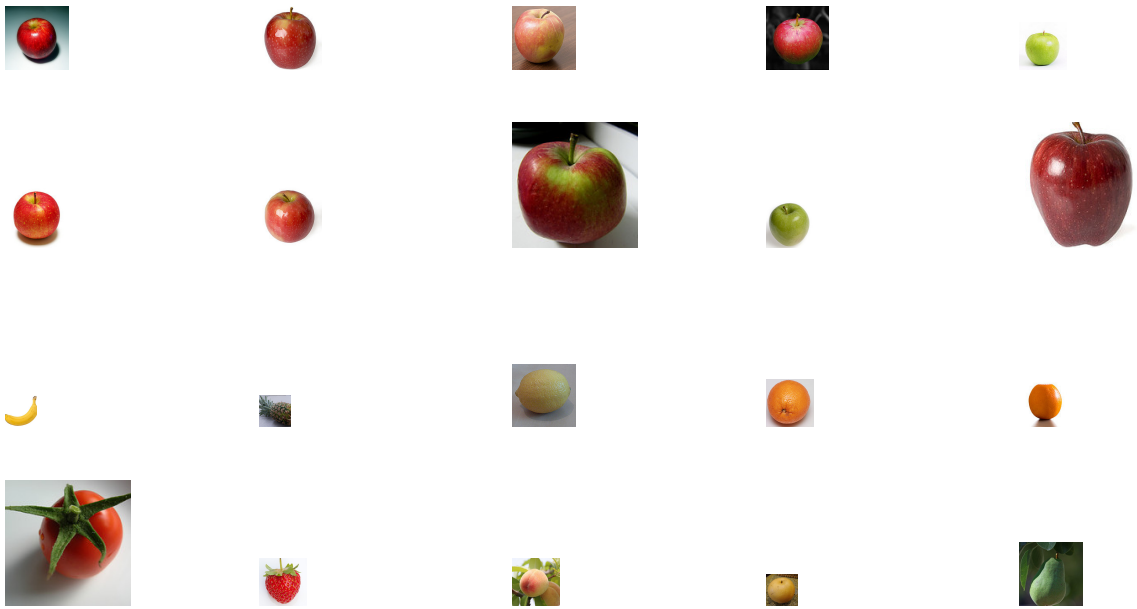
- 老師：是的，有很多蘋果是紅的。但圓的和紅的好像還不足以區分所有的蘋果。小新，你有其他的建議嗎？
- 小新：蘋果也可以是綠的。



(全班)：蘋果是圓的而也是紅的，
不過也可以是綠的。

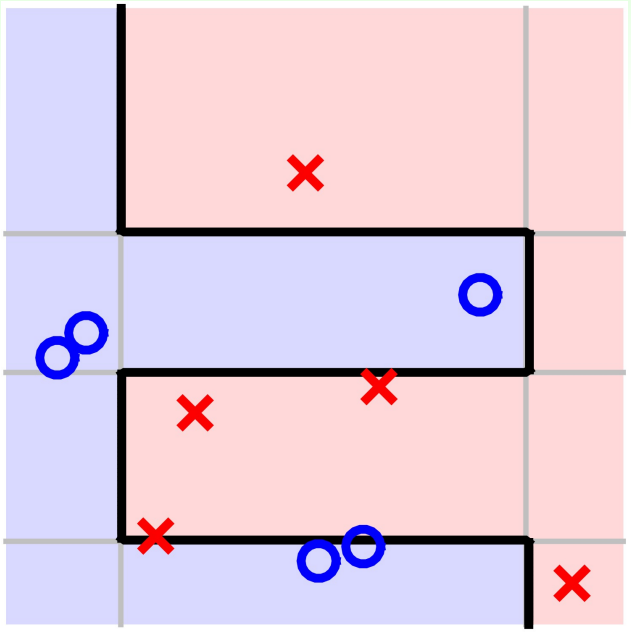
蘋果辨識課：第四講

- 老師：很好。圓的、紅的、綠的都可以描述蘋果，不過可能還是會跟蕃茄或桃子搞混，對嗎？小白，你有什麼建議嗎？
- 小白：蘋果上面有梗。



(全班)：蘋果是圓的而也是紅的，
不過也可以是綠的；此外，蘋果上面有梗。

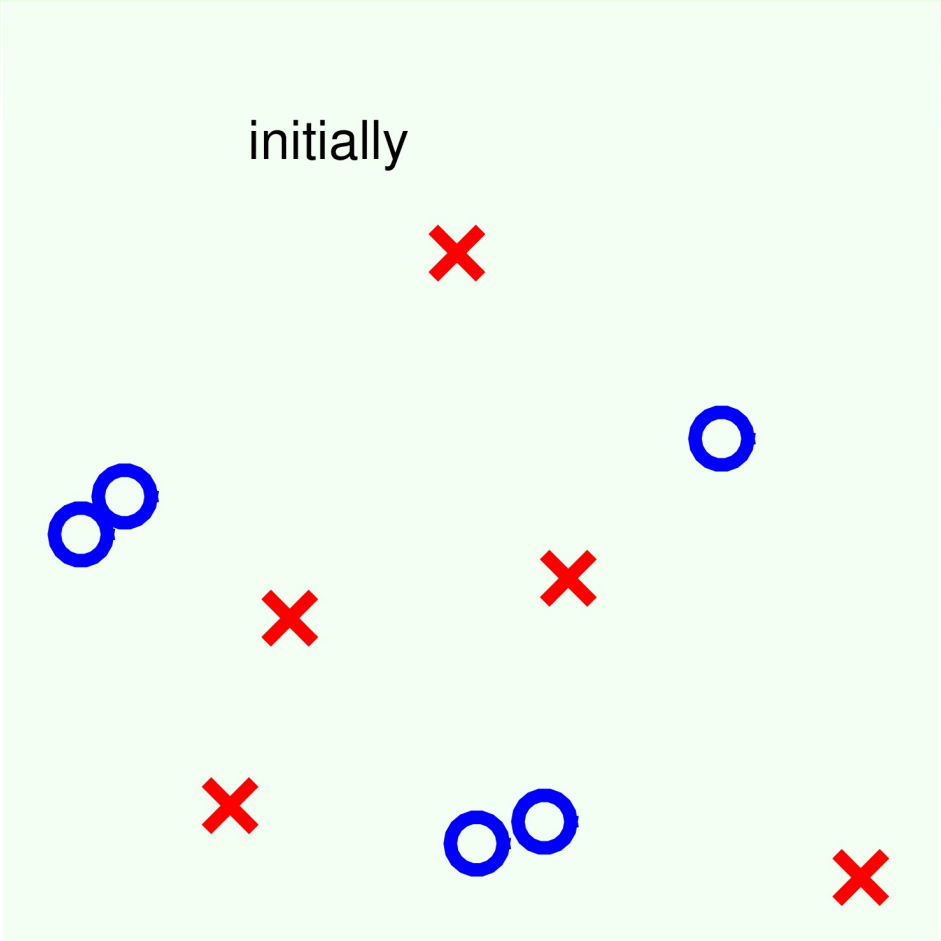
眾志成城法



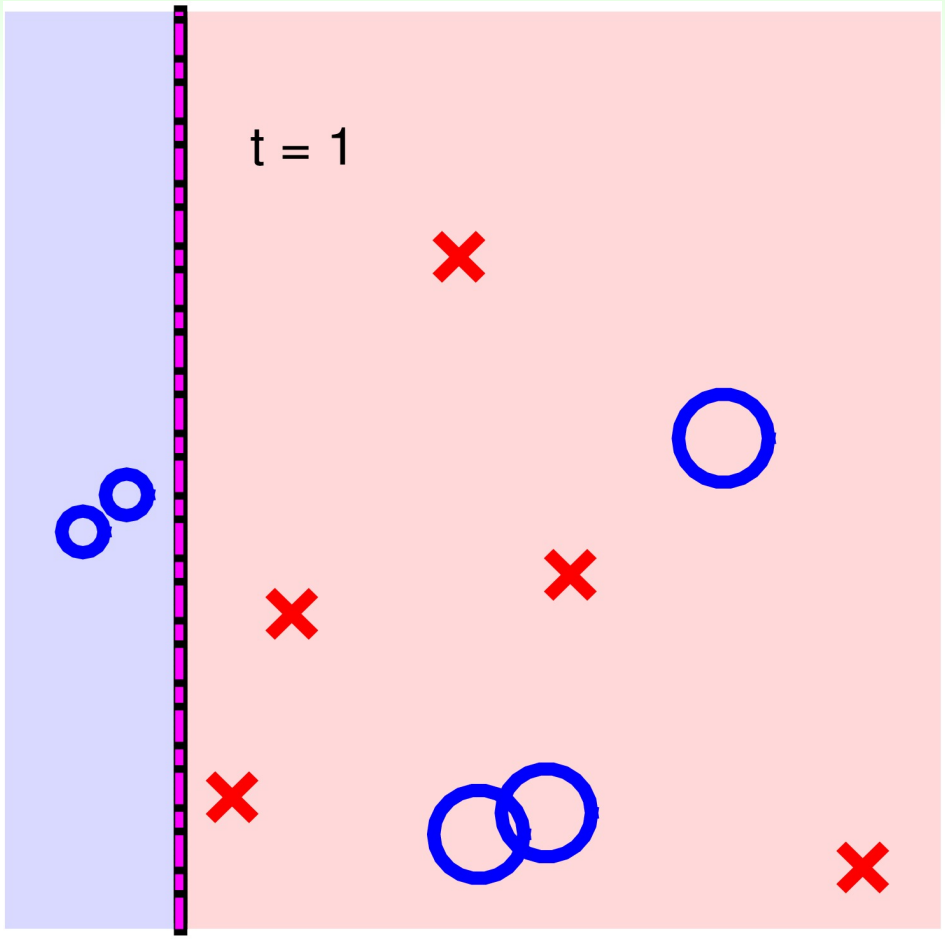
- 學生：簡單的規則(像是垂直/水平切割線)
- (全班)：規則組合起來的複雜決策(像是黑色分割線)
- 老師：巧妙地引導學生看到自己還做得不夠好的地方

接下來：眼見爲憑

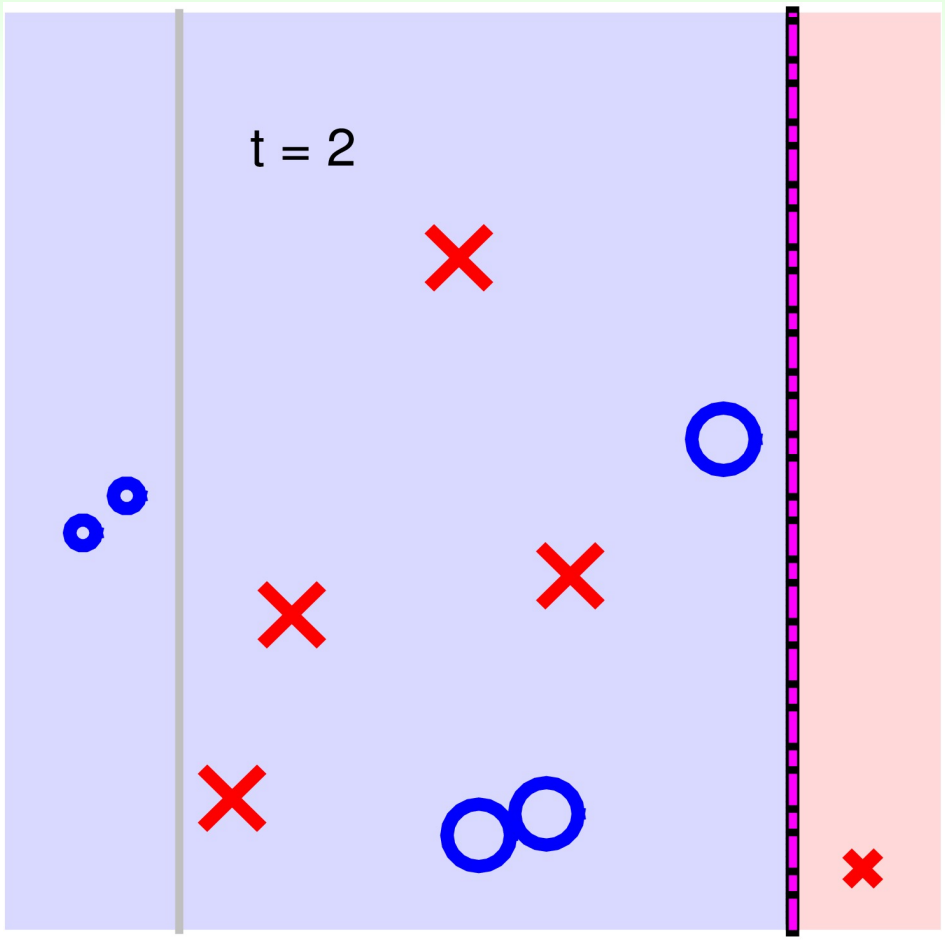
眼見爲憑：眾志成城法



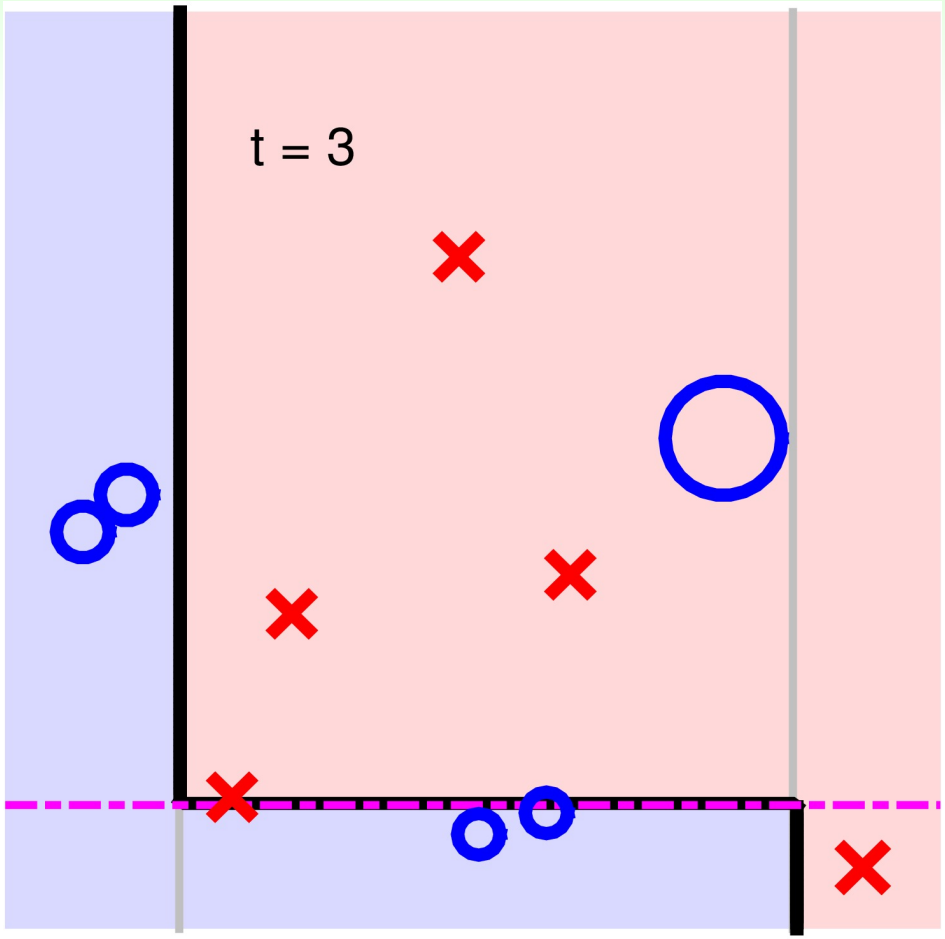
眼見爲憑：眾志成城法



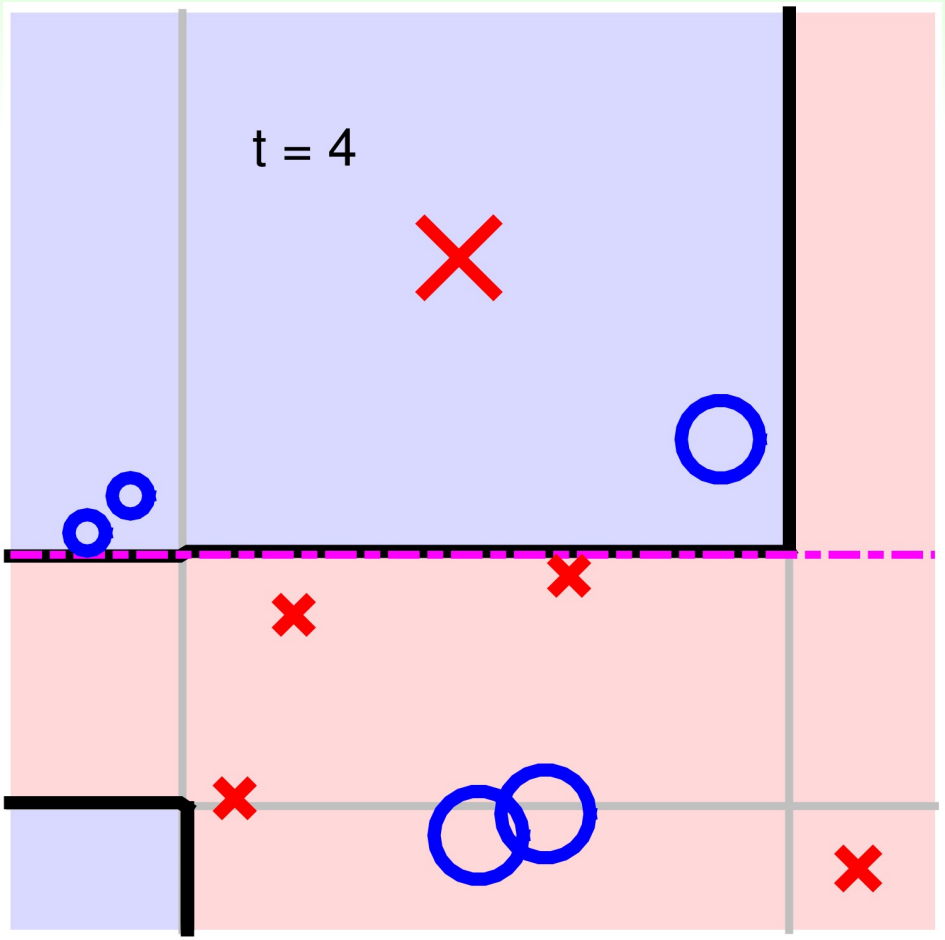
眼見爲憑：眾志成城法



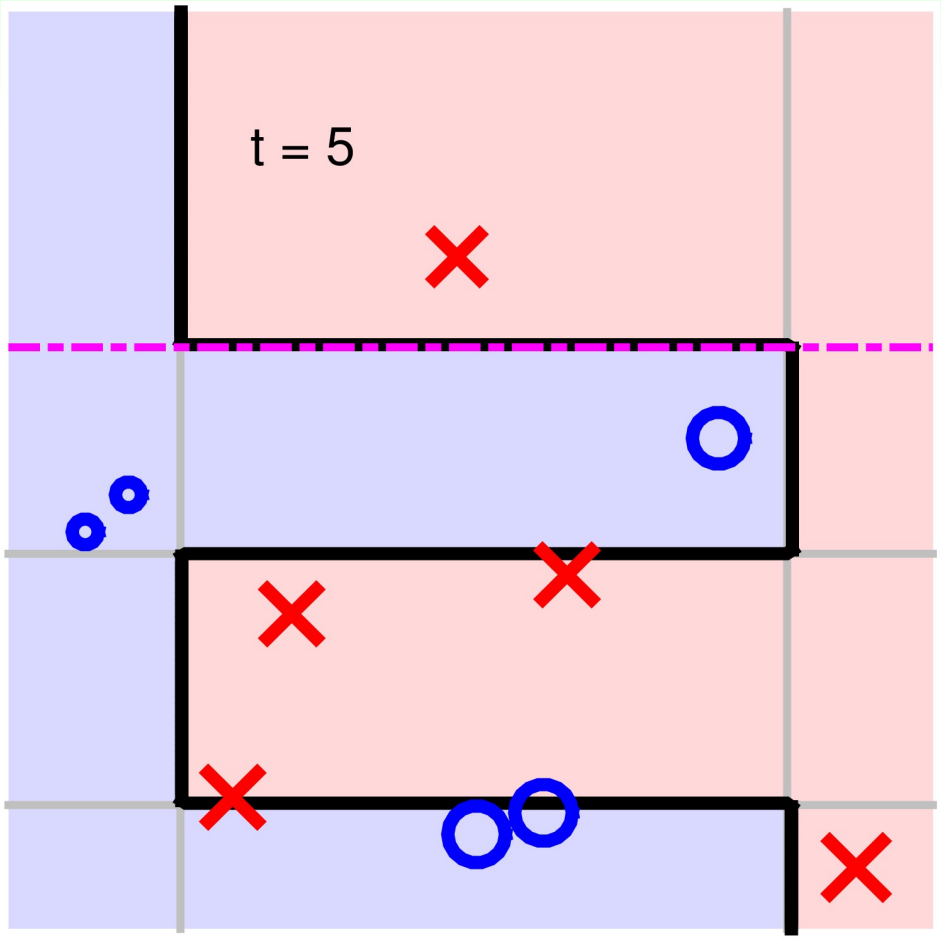
眼見爲憑：眾志成城法



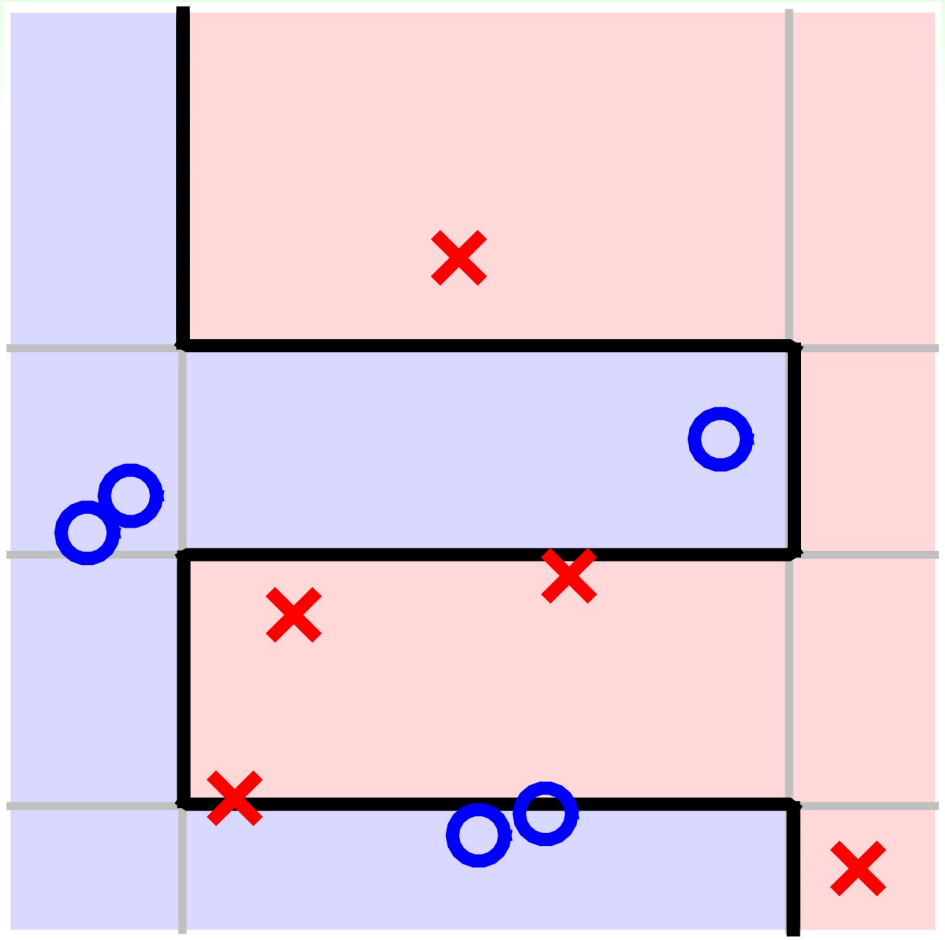
眼見爲憑：眾志成城法



眼見爲憑：眾志成城法



眼見爲憑：眾志成城法



「巧妙」的老師可以訓練出聰明的班級

應用實例五：即時人臉辨識

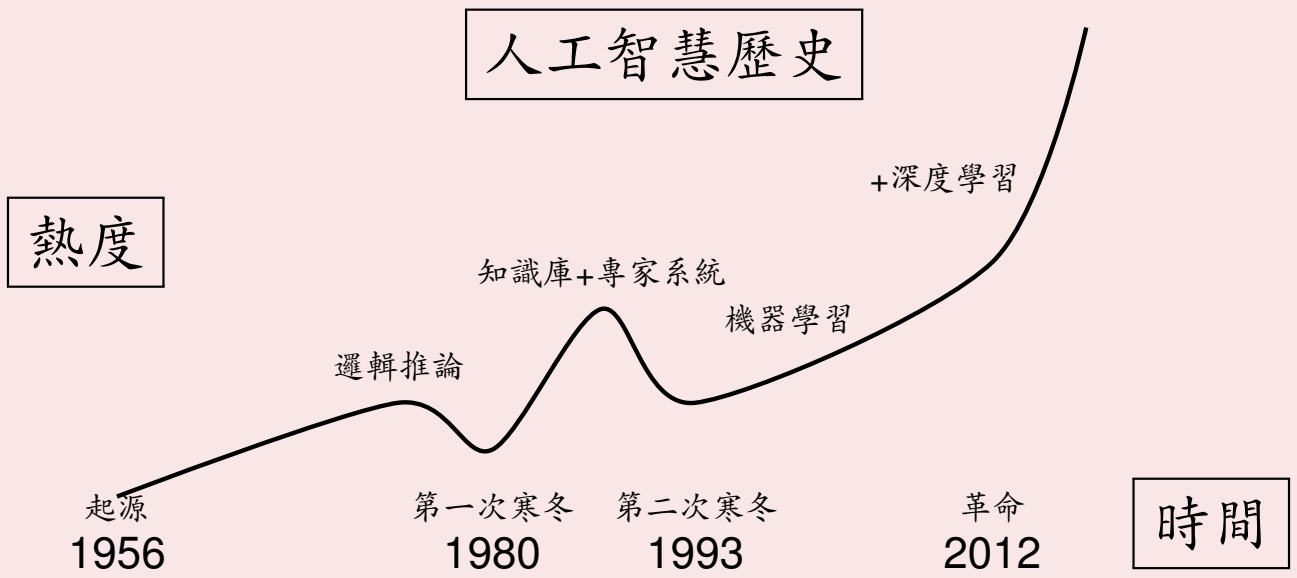
original picture by F.U.S.I.A. assistant and derivative work by Sylenius via Wikimedia Commons

世界上第一個即時人臉辨識程式(Viola and Jones, 2001)

- 「學生」：找出圖片中是/不是人臉的小塊「蛛絲馬跡」
- 模型經過特殊設計，可以快速排除非人臉

基於眾志成城法的Viola-Jones模型：
電腦視覺「機器學習化」的重要里程碑

歷史回顧：眾志成城法(Freund and Schapire, 1996)



- 原名：逐步增強法/皮匠法(Adaptive Boosting Algorithm)
- 可拿來增強「決策樹」並在當時取得很好的實務結果

眾志成城法：爲機器學習復興時期的重要方法

接下來要講的是……

機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

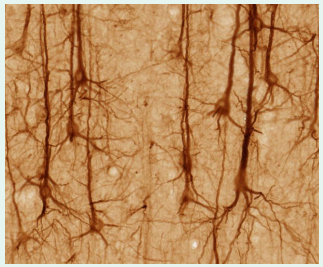
機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

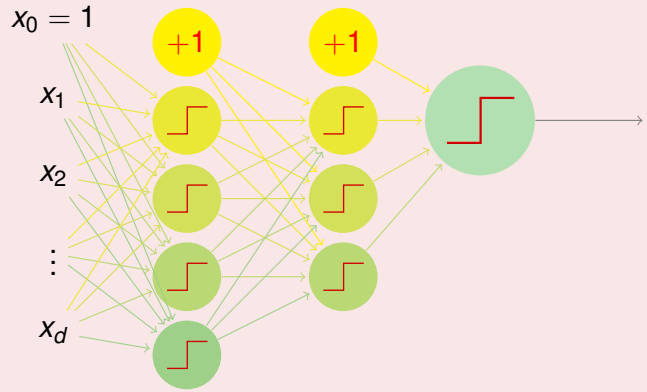
類神經網路

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)
眾志成城法(模擬「一個班」)：「畫比較複雜的邊界」



by UC Regents Davis campus-brainmaps.org.

Licensed under CC BY 3.0 via Wikimedia Commons

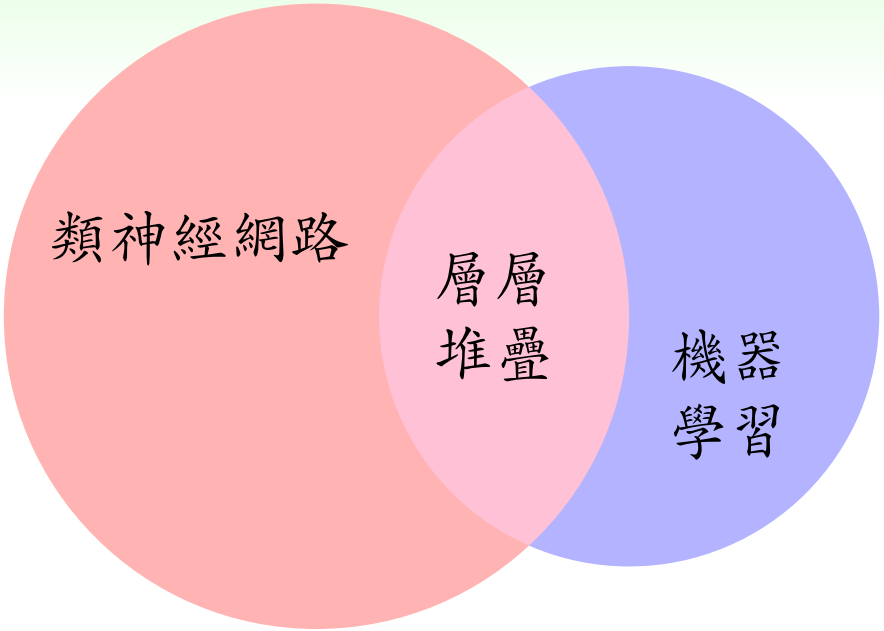


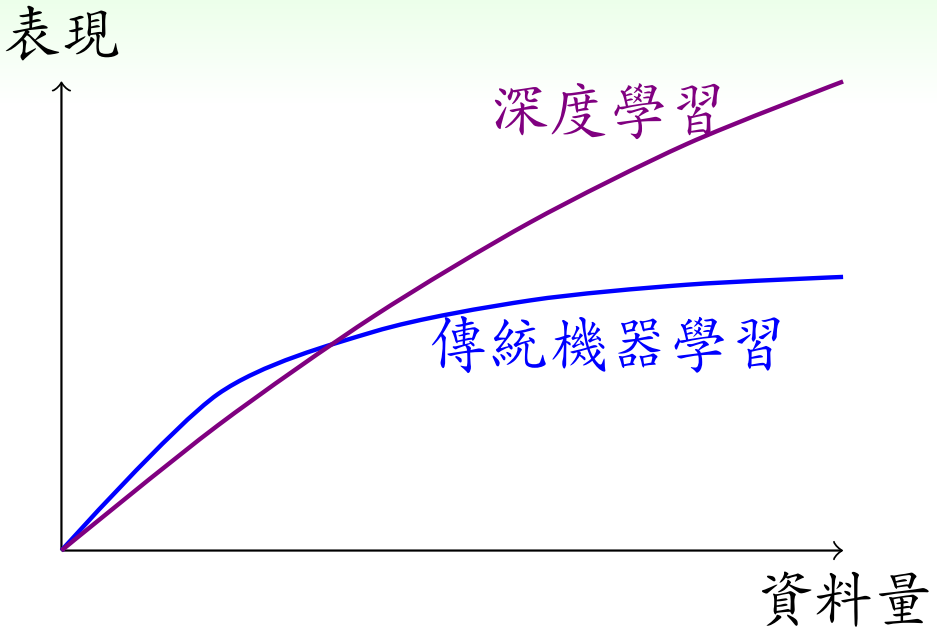
by Lauris Rubenis. Licensed under CC BY 2.0 via https://flic.kr/p/fkVuZX

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

兩張圖秒懂層層堆疊法

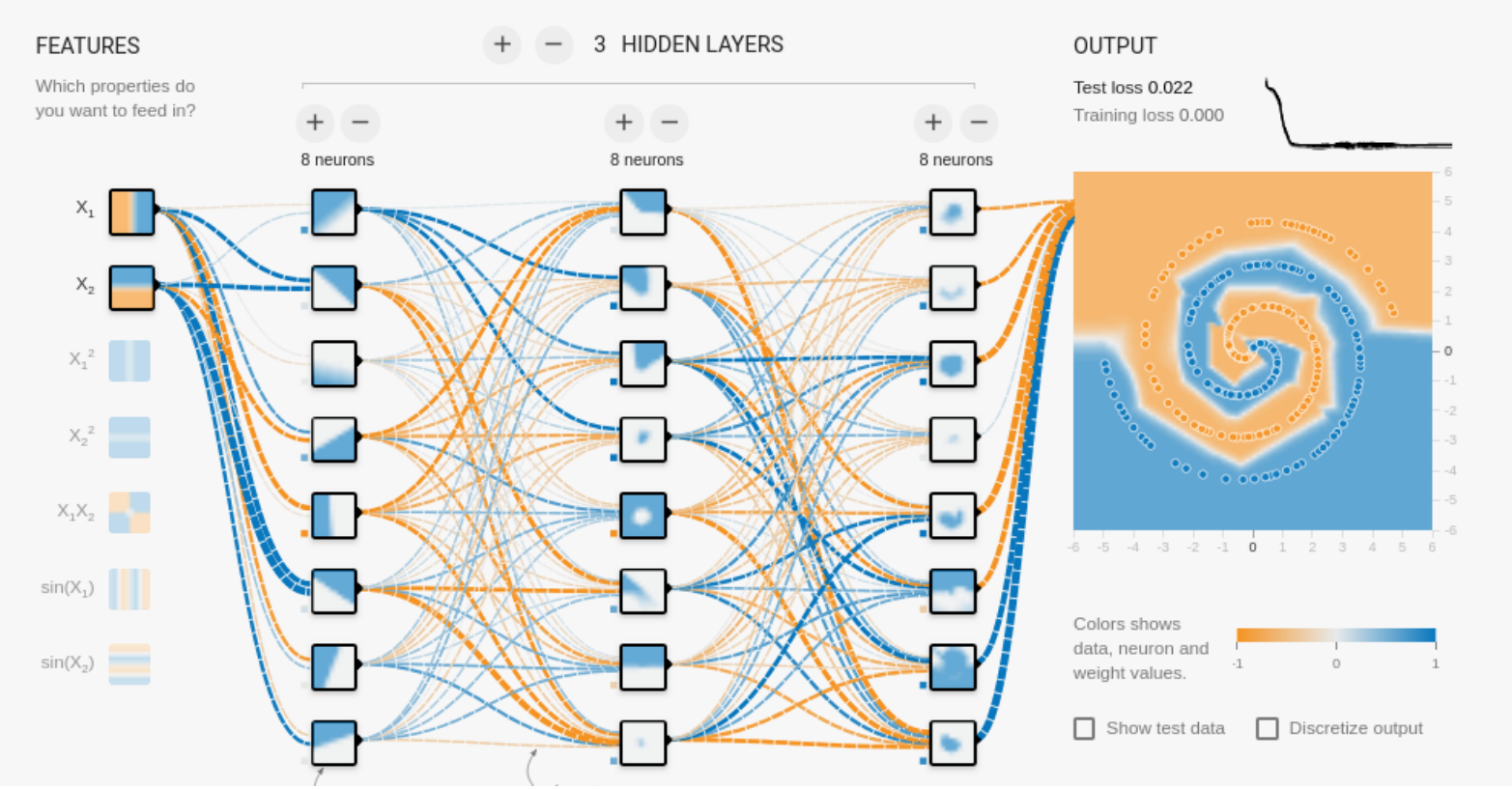




層層堆疊：用大量資料+大量計算
來解決(困難的)機器學習問題。

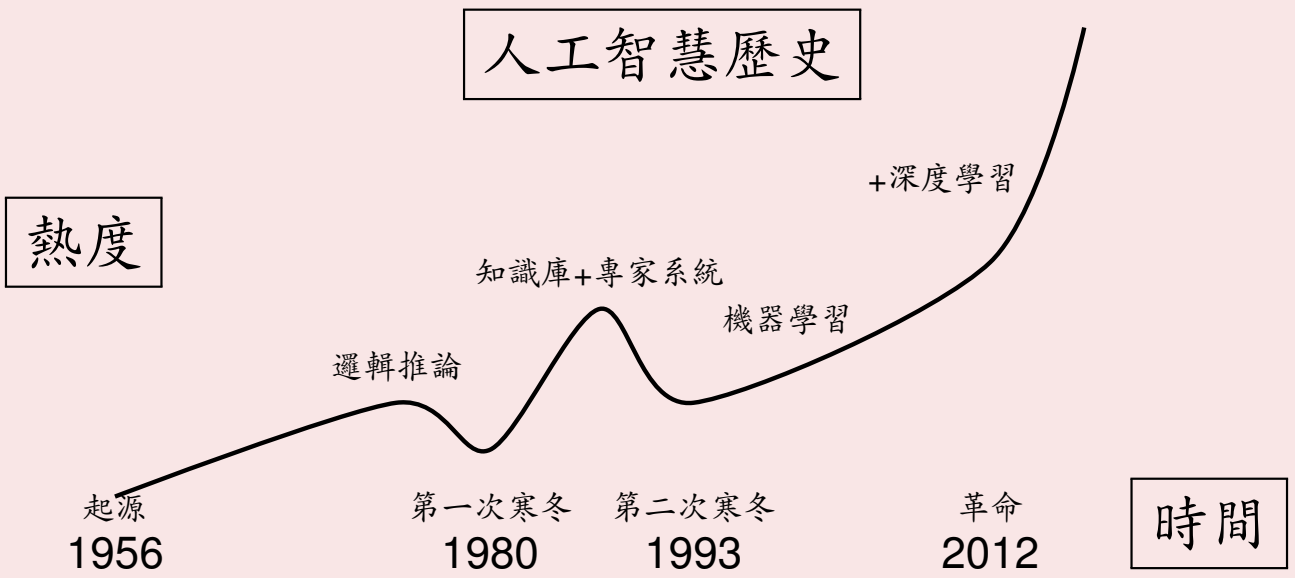
眼見爲憑：層層堆疊法

https://playground.tensorflow.org/



層層堆疊：每一層組合上一層的邊界們，
轉化出更複雜的邊界

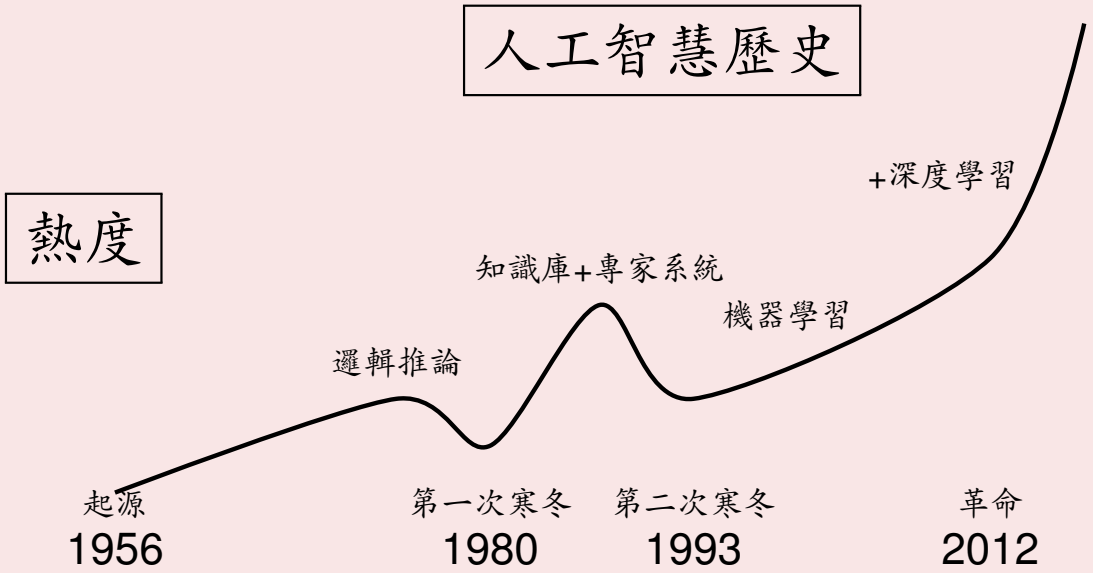
歷史回顧：層層堆疊法(Hinton et al., 2006)



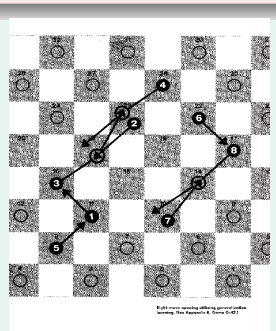
- 流行名：深度學習法(Deep Learning Algorithm(s))

層層堆疊法：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

接下來要講的是……

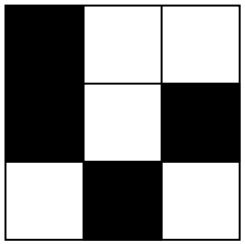
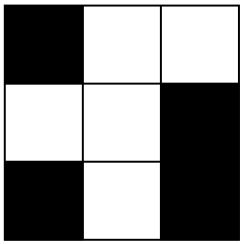
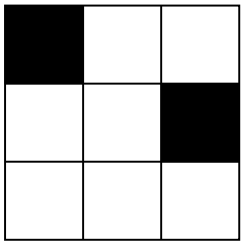
機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

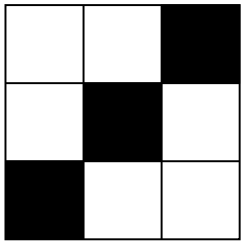
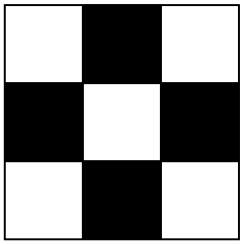
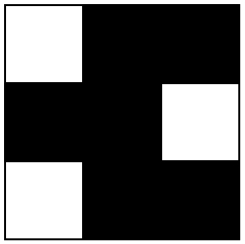
機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

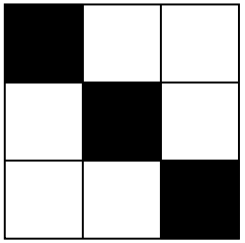
機器/人類學習小測驗

$y_n = -1$

$y_n = +1$

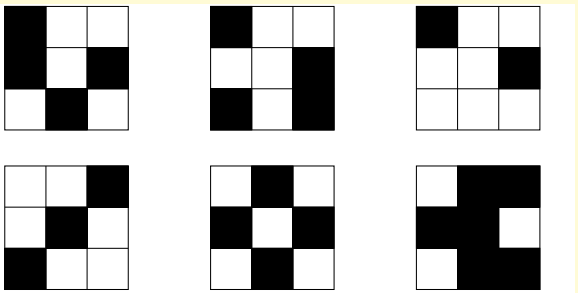


$g(\mathbf{x}) = ?$

你的「人類學習」學到了什麼？

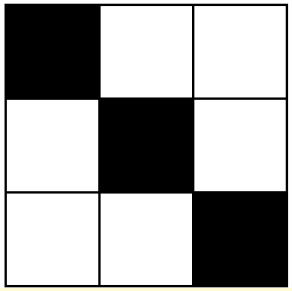
兩個可能的答案

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

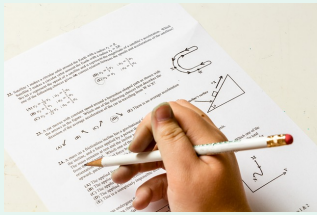
「標準答案」是-1，因爲...

- 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

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)

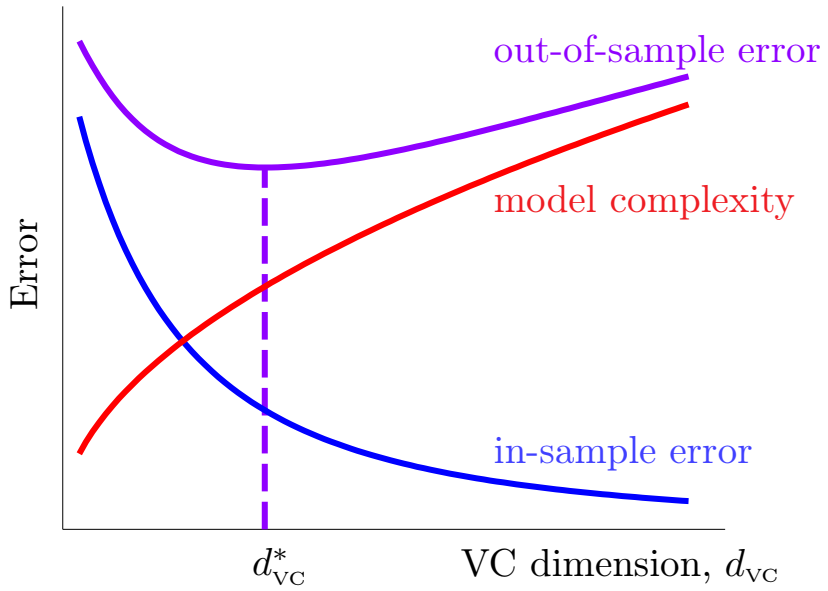
機器學習要可行，必須

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」

機器學習的日常

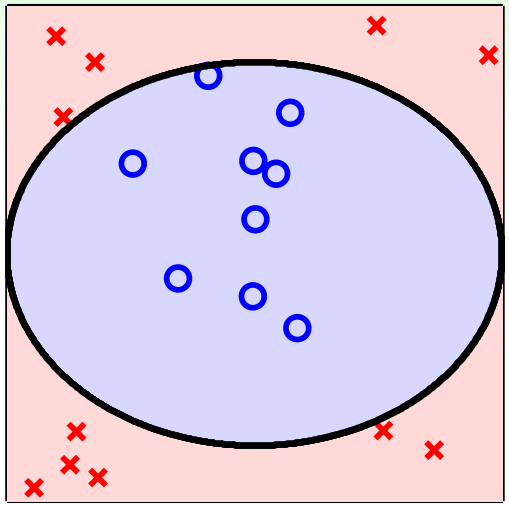
$$\text{測試錯誤} \approx \underbrace{\text{訓練錯誤}}_{\text{最佳化}} + \underbrace{\text{複雜度}}_{\text{一般化}}$$



- 複雜度↑: 訓練表現較好
  但不易舉一反三(容易以偏概全)
- 複雜度↓: 較易舉一反三
  但訓練表現不好
- 最佳複雜度在中間
  —常常需要「老廚師」才能調出來

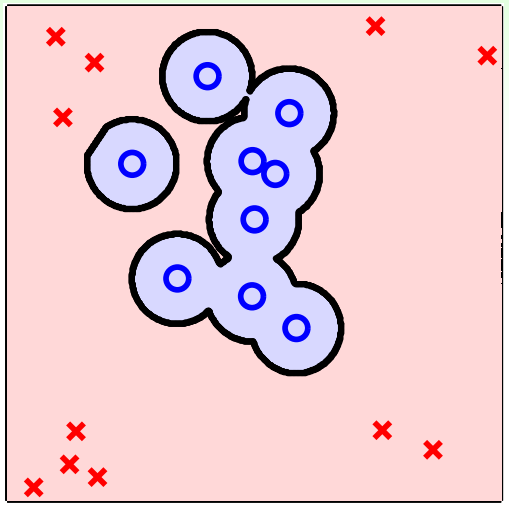
複雜模型(想太多)不一定好，
會「鑽牛角尖」**(overfitting)**

「鑽牛角尖」：以開車比喻



想得剛好

$\Longrightarrow$



鑽牛角尖

學習	開車
鑽牛角尖	出車禍
複雜模型	開快車
資料雜訊	路況不好
資料有限	視線不好

機器學習的哲學思維：最簡單又能(儘量)符合已看到資料的模型，才是最可信的。

接下來要講的是……

機器學習是什麼？
- 由(巨量)資料實現人工智慧的熱門工具

機器學習怎麼做？
- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？
- 訓練/測試關聯、訓練最佳化、舉一反三

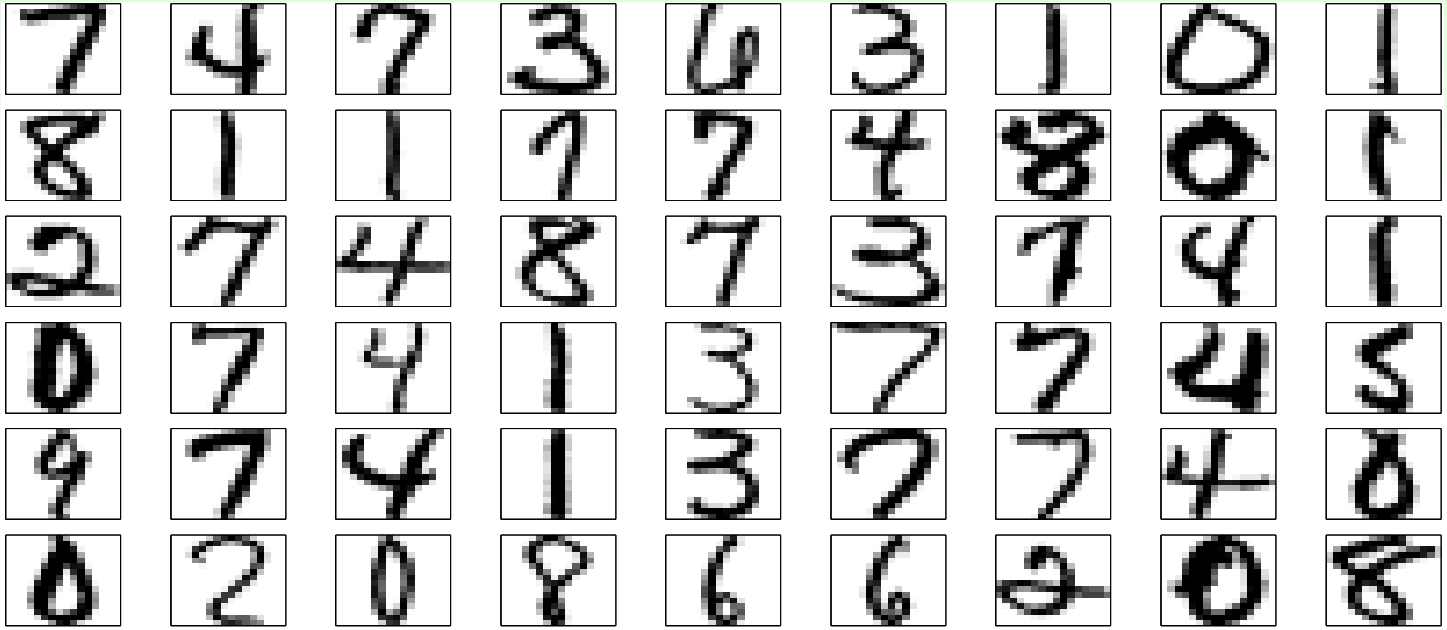
機器學習怎麼用？
- 由辨識系統到「人需」人工智慧

已經講過的應用實例

- 應用實例一：股票預測
- 應用實例二：颱風強度判讀
- 應用實例三：信用卡核卡
- 應用實例四：蘋果辨識問題
- 應用實例五：即時人臉辨識

機器學習已廣泛地被使用

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！

我們需求怎麼樣的人工智慧？

人工智慧: 讓電腦聰明地思考與動作

- 與人相仿
- 理性決策

與人相仿 $\approx$ 聰明 $\approx$ 理性決策

—人類是全然理性的嗎？

與人相仿與理性決策

如果自駕車決定死一個人比死兩個人好—但死的那個會是你？ (The Washington Post http://wpo.st/ZK-51)

You're humming along in your self-driving car, chatting on your iPhone 37 while the machine navigates on its own. Then a swarm of people appears in the street, right in the path of the oncoming vehicle.

自駕車與人相仿的動作

以乘客(老闆)的性命爲先，向前撞上去

自駕車理性決策的動作

命命等值，撞牆犧牲乘客，保住行人安全

哪個比較聰明？

自駕車的車禍責任(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抗辯認爲，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。
- 加州陪審團在今年4月21日，駁回徐小姐的起訴，認爲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：現在與未來

2010–2015: AI |

人工智慧初放光明

- 傳統機器學習模型成熟
- 新興深度學習大幅進步

2016–2020: AI +

人工智慧展現競爭力

- 在圍棋等問題超越人類
- 大型公司開始以人工智慧爲優先

2021–: AI ×

人工智慧無所不在

- 「我們不會被人工智慧取代，但會被更懂得用人工智慧的人取代」：沛星科技首席人工智慧科學家孫民博士

總結

機器學習是什麼？

- 由(巨量)資料實現人工智慧的熱門工具

機器學習怎麼做？

- 知錯能改法
- 分而治之法
- 眾志成城法
- 層層堆疊法

機器學習爲什麼？

- 訓練/測試關聯、訓練最佳化、舉一反三

機器學習怎麼用？

- 由辨識系統到「人需」人工智慧

謝謝聆聽！