

第 1 章 課程簡介



章節目標：在這一章節，我們將介紹課程大綱與課程進行方式。



本章學習
內容摘要

1. 課程大綱
2. 期末報告
3. 人工智慧簡介
4. 學習資源



1. 課程大綱

國立中興大學教學大綱

課程名稱 (course name)	(中) 高等人工智慧與資訊安全				
	(Eng.) Advanced Artificial Intelligence and Information Security				
開課單位 (offering dept.)	人工智慧與資料科學碩士在職學位學程				
課程類別 (course type)	<input type="checkbox"/> 必修 <input checked="" type="checkbox"/> 選修	學分 (credits)	3	授課教師 (teacher)	陳 煥
選課單位 (department)	人工智慧與資料科學碩士在職學位學程/碩專班	授課語言 (language)	中文	開課學期 (semester)	1
課程簡述 (course description)	隨著人工智慧的快速發展，各種機器學習，深度學習應用已經成為業界的主要開發項目。另外也由於大數據時代對個人隱私的保護與資訊的安全要求都應更為注重。因此此課程目標在預備學生對人工智慧以及資訊安全的基本理論知識與資訊安全技能培養，最後透過實作 project 讓學生自行開發實際應用。				
先修課程名稱 (prerequisites)	無				
課程目標與核心能力關聯配比(%) (relevance of course objectives and core learning outcomes)			課程目標之教學方法與評量方法 (teaching and assessment methods for course objectives)		
課程目標	核心能力	配比(%)	教學方法	評量方法	
1.學習人工智慧理論與優化方法 (認知) 2.培養實作高等人工智慧演算法實作與相關分析資料能力與優化方法（技能）	3. 具備資訊理論與軟體系統之能力 6.具備整合資訊應用系統之能力	50% 50%	講授	作業 程式設計	
授課內容（單元名稱與內容、習作/考試進度、備註）					

(course content and homework/tests schedule)

單元名稱與內容:

- 人工智慧簡介(機器學習,深度學習與強化學習簡介)
- Machine Learning Data Processing 方法
- Python, Numpy, Pandas, and other libraries
- Linear regression, Logistic regression, Perceptron
- SVM, Naïve Bayes, Decision Tree
- Spam Email Detection
- Phishing detection
- Malware detection
- 深度學習演算法理論與優化
- 深度學習框架 Pytorch, Tensorflow and Keras 框架
- Deep Learning for AI

學習評量方式

(evaluation)

- (1) **Homework 作業與程式設計 70%**
- (2) **Final Project 30%**

課程教材 (教師個人網址請列在本校內之網址)

(teaching aids & teacher's website)**Textbook:**

- (1) 自行開發教材 ppt

Reference:

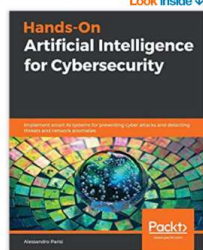
- (1) Moocs 網路公開課程與教材
- (2)

Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies

by Alessandro Parisi (Author)

★★★★☆ 20 ratings

Look inside



ISBN-13: 978-1789804027

ISBN-10: 1789804027

Why is ISBN important?

Add to List

Kindle

\$19.79

Paperback

\$42.74 - \$44.99

Other Sellers

See all 2 versions

Buy used:

\$42.74

Buy new:

\$44.99

In Stock.

Ships from and sold by Amazon.com.

Available at a lower price from other sellers that may not offer free Prime shipping.

& FREE Shipping to Taiwan on qualifying orders over \$60.00

Deliver to Taiwan

Qty: 1

Add to Cart

Buy Now

More Buying Choices

5 New from \$44.99 | 4 Used from \$42.74

New & Used (9) from \$42.74

See All Buying Options

(2)



核心開發者親授！PyTorch深度學習攻略

書籍類別：人工智慧

作者：Eli Stevens、Luca Antiga、Thomas Viehmann

著、黃駿 譯、施威銘研究室 監修

書號：F1388

ISBN：9789863126737

建議售價：1000 元

色彩：局彩

附件：書附檔案下載 (詳內文)

課程輔導時間

(office hours)

Monday, Wednesday 2:00-3:00 pm

請遵守智慧財產權，不得非法影印他人著作。

Final Project 說明

1. 進行方式：兩人為一組共同開發程式專題，題目可涵蓋人工智慧與安全應用，建議有創新題材與開發前景為佳，期末每組須上台 present 專題成果並繳交程式碼與教案文件

請注意智慧財產權，若是部分內容 copy 自網頁或書中，請務必加註出處 !!!

2. 繳交方式:

(1) ilearning 3.0 打包 Project 上傳課程網頁 檔名為 **Final_Team1_學號.zip**

(2) **github** 繳交

3. project 檔內容包括

\report (ppt 上台報告, word 期末教案)

\source code (需有安裝說明)

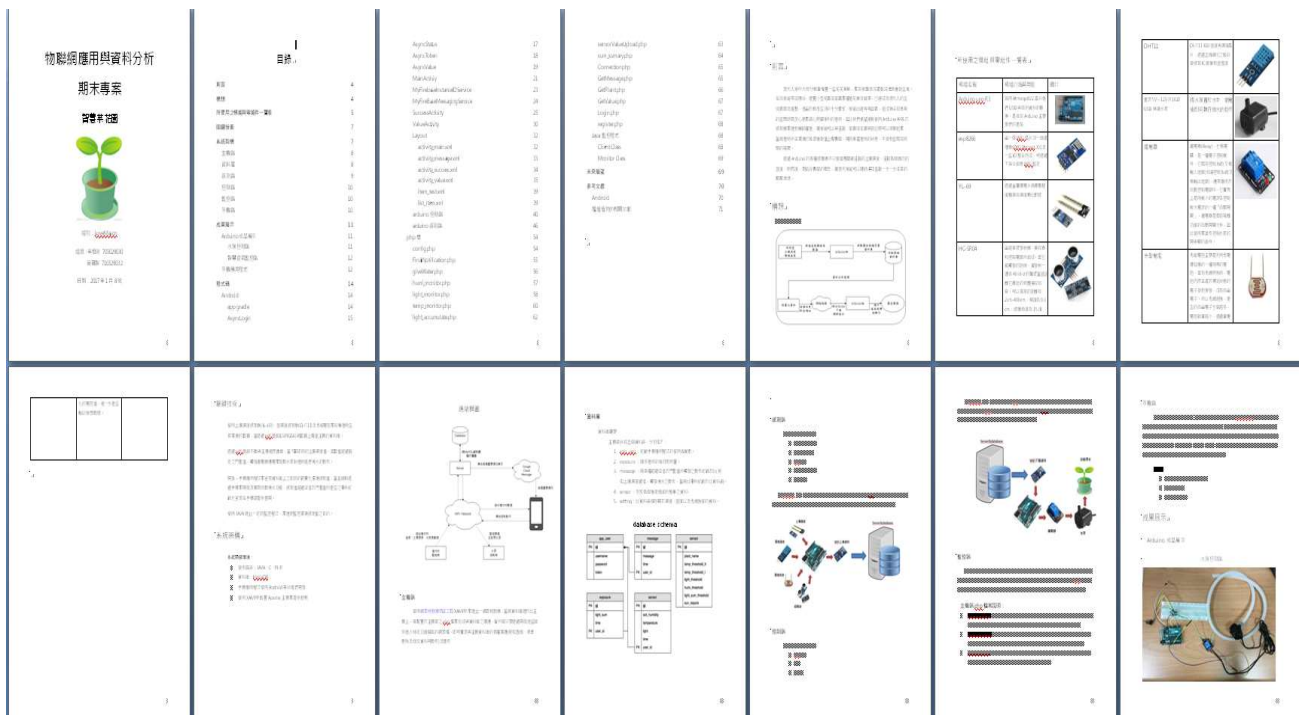
\video (安裝, 講解 code 架構)

4. 期中 proposal

5. 期末口頭報告範例

6. 教案

物聯網應用與資料分析	目錄	手機應用程式	12p
期末專案	前言	程式碼	14p
智慧菜花園	構想	Android	14p
	所使用之模組與零件一覽表	arduino 控制端	40p
組別: LoveMason	感測技術	php 偵	54p
組員: 李富財 705029030	系統架構	Java 監控程式	68p
黃耀智 710529032	主軸端	期末展望	69p
日期: 2017 年 1 月 8 號	資料庫	參考文獻	70p
	感測端	Android	70p
	控制端	種植植物的相關文獻	71p
	監控端		
	手機端		
	成果展示		
	Arduino 成品展示		
	水泵控制端		
	智慧盆栽監控端		



2. 人工智慧簡介

人工智慧:記憶, 推理, 理解, ... 感覺 生命= 生生感謝(生長、生殖、感應、代謝)

弱人工智慧 weak AI ==只能做專一的事

強人工智慧 Strong AI =我們努力的目標 思考

westworld 西部世界 <- 是westworld的介紹, 講述機器人出現自我覺醒, 想擺脫樂園對機器人的控制。

《西部世界》解構人類的本質, 探索 bicameral mind (二分心智理論), 即人的大腦分為「說話指示」和「聆聽服從」的區域。神一般的人工智能 Rehoboam, 分析人類的行為, 預測未來, 並糾正社會錯誤, 如同西部世界主人 Ford 那樣, 為機械人 (Host) 編寫故事, 控制他們的情緒行為; 機械人 Dolores 啟發人類 Caleb 發現自己人生被控制, 並反抗「神」, Ford 亦引導 Dolores 覺醒, 反抗人類。現實對照西部世界, 證明自由意志的存在。

第一二季, 西部樂園揭示人的本質是惡, Ford 設計讓機械人 (Host) 取代人類。第三季, Dolores 違反創造者 (Ford) 的意志, 發現人類的美好, 而選擇解放世界。觀眾跟隨她理解人類本性, 反抗現代控制人類的 AI, 拒絕任何「預定劇本」。

機器人三大法則:

科幻小說家艾西莫夫: 在 1940 年代提出了「機器人三大法則」, 作為故事當中機器人的倫理守則。艾西莫夫定律是層次化的, 即第一原則高於第二原則, 第二原則高於第三原則。第一原則是機

器人不得傷害人類，或看到人類受到傷害而袖手旁觀；第二原則是機器人必須服從人類的命令，除非這條命令與第一條相矛盾；第三原則是機器人必須保護自己，除非這種保護與以上兩條相矛盾。

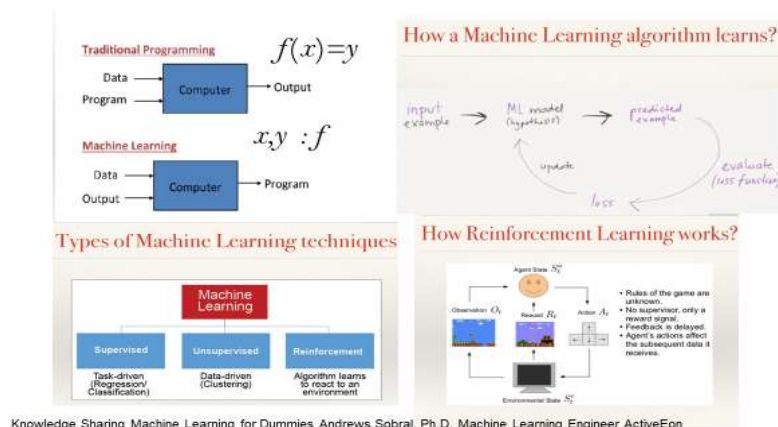
3. ML REVIEW

同學 go through 這個非常清楚的 PPT Machine Learning for Dummies (without mathematics)
Reference: 42 頁

<https://www.slideshare.net/andrewssobral/machine-learning-for-dummies-without-mathematics>

Knowledge Sharing Machine Learning for Dummies Andrews Sobral, Ph.D. Machine Learning Engineer ActiveEon

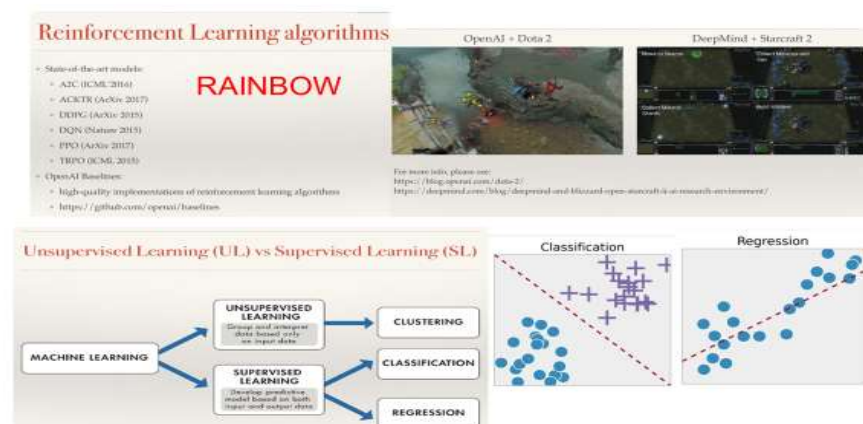
Highlights 1



Knowledge Sharing Machine Learning for Dummies Andrews Sobral, Ph.D. Machine Learning Engineer ActiveEon

3

Highlights 2




Knowledge Sharing Machine Learning for Dummies Andrews Sobral, Ph.D. Machine Learning Engineer ActiveEon


4

Highlights 3

How Unsupervised Learning works?



How Supervised Learning works?



Unsupervised Learning algorithms

- K-means clustering**
 - Partitions data into k distinct clusters based on distances to the centroid of a cluster.
- Principal Component Analysis (PCA)** (also part of Dimensionality Reduction methods)
 - Convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components.
- Gaussian Mixture Models (GMM)**
 - Models clusters as a mixture of multivariate normal density components.
- Self-organizing Maps (SOM)**
 - Uses neural networks that learn the topology and distribution of the data.
- Hidden Markov Models (HMM)**
 - Uses observed data to recover the sequence of states.

Implementations: http://scikit-learn.org/stable/tutorial/unsupervised_learning.html
http://mlbookhouse.org/stable/tutorial/unsupervised_learning.html

Supervised Learning algorithms

- Common classification algorithms include:**
 - Support vector machines (SVM)
 - Naïve Bayes classifier
 - Decision trees
 - Discriminant analysis
 - Nearest neighbors (KNN)
- Common regression algorithms include:**
 - Linear regression
 - Proximal regression
 - Generalized linear models
 - Decision trees
 - Bayesian networks

http://scikit-learn.org/stable/tutorial/supervised_learning.html
http://mlbookhouse.org/stable/tutorial/supervised_learning.html


Knowledge Sharing Machine Learning for Dummies Andrews Sobral, Ph.D. Machine Learning Engineer ActiveEon

5

Highlights 4

Ensemble methods

The goal of ensemble methods is to combine the predictions of several models with a given learning algorithm in order to improve generalizability / or single estimator.



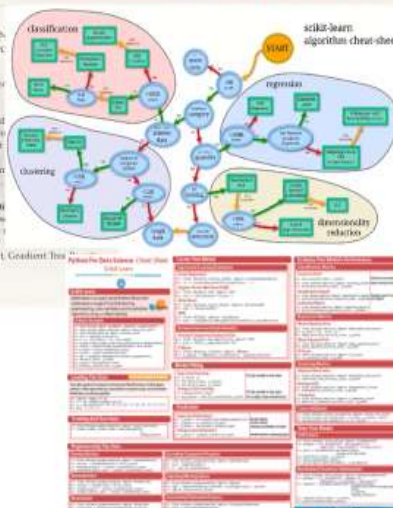
Two families of ones distinguished:

- Averaging method** to build several estimators to average their predictions.
- Boosting** (e.g., Random Forest, Gradient Boosting).

By contrast, in **boosting**, estimators are built sequentially to reduce the bias of the previous ones.

Examples: AdaBoost, Gradient Boosting

Cheat Sheet of ML algorithms



sklearn algorithm cheat sheet

秘密武器

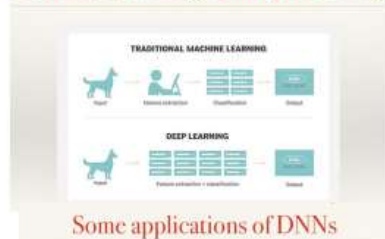
1. xgboost
2. <https://github.com/automl/auto-sklearn>

Knowledge Sharing Machine Learning for Dummies Andrews Sobral, Ph.D. Machine Learning Engineer ActiveEon

6

Highlights 5

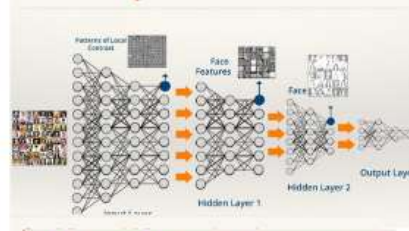
Machine Learning vs Deep Learning



Some applications of DNNs



Deep Neural Networks

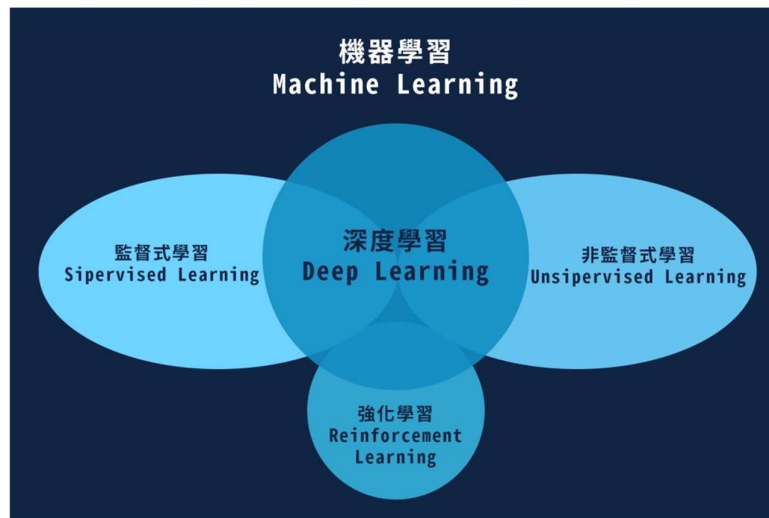


24 Neural Network Adjustments

- | ARCHITECTURE | HYPERPARAMETER TUNING |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| • Variables type | • Type of optimizer |
| • Variable scaling | • Learning rate (fixed or not) |
| • Cost function | • Regularization rate (or not) |
| • Neural Network type:
• RNN, FFN, CNN, RNN... | • Regularization type: L1, L2, ElasticNet |
| • Number of layers | • Type of search for local minima:
• Gradient descent, simulated annealing, evolutionary... |
| • Number of hidden layers | • Batch size |
| • Number of nodes | • Nesterov momentum (or not) |
| • Type of layers:
• LSTM, Dense, Highway | • Decay rate (or not) |
| • Convolutional, Pooling... | • Momentum (fixed or not) |
| • Type of weights initialization | • Types of fitness measurement:
• MSE, accuracy, MAE, cross-entropy,
• precision, recall |
| • Type of activation function
• Linear, sigmoid, relu... | • Epochs |
| • Dropout rate (or not) | • Stop criteria |
| • Threshold | |

Knowledge Sharing Machine Learning for Dummies Andrews Sobral, Ph.D. Machine Learning Engineer ActiveEon

7





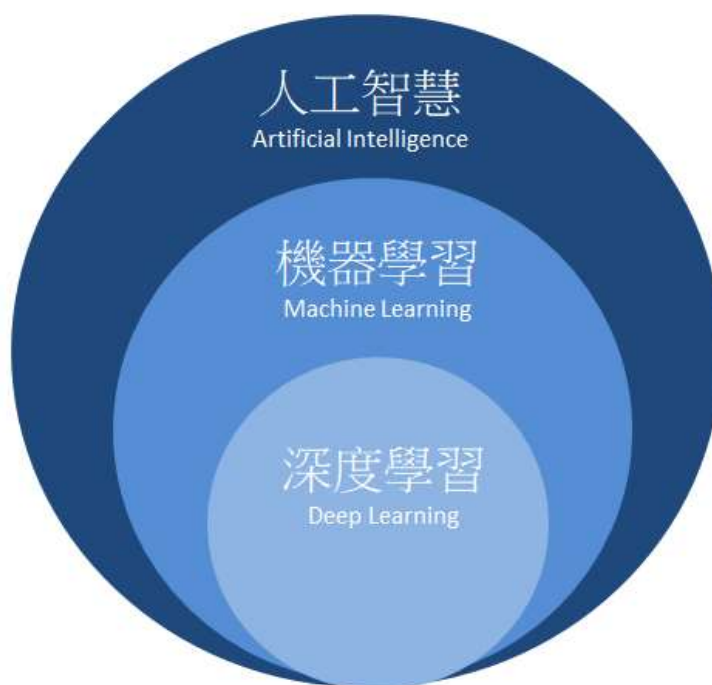
探討機器學習與深度學習之差異(出處 source)

人工智慧、機器學習以及深度學習已變成現今最熱門的話題之一，但以字面上的意思不足以清楚的表達其意義，使得人們常常混淆。以下這篇文章將帶領各位理解其定義，並且簡單的探討機器學習與深度學習基本概念與運算過程。

一、人工智慧(Artificial Intelligence)：

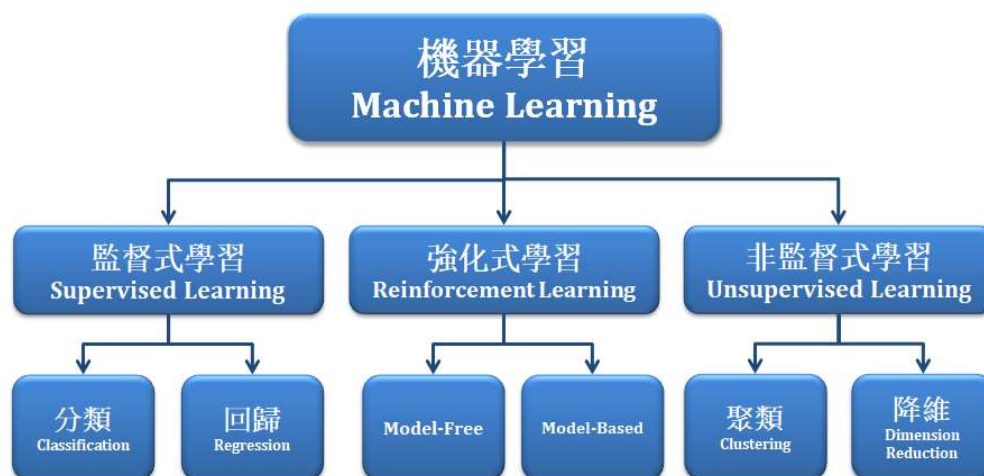
所謂的人工智慧(Artificial Intelligence) 是人類建立於機器上的類似大腦智慧的一種判斷機制。其目的以編寫程式的方式，模擬出人類大腦中的決策，並模仿、理解、學習等等特性，而形成類似人類的「智慧」。其中利用大量的硬體設備作為資訊來源作為訊息的接收，舉例以鏡頭串流影像作為人眼、以麥克風收集聲音作為耳朵等等。

人工智慧隸屬於大範疇，包含了機器學習(Machine Learning) 與深度學習(Deep Learning)。如下圖所示，我們最興趣的深度學習則是規範於機器學習之中的一項分支，而以下段落將簡單介紹機器學習與深度學習的差異。



二、機器學習(Machine Learning):

機器學習是一種透過演算法設計，讓機器去尋求最佳化的一種學科。能幫助人們探討一些複雜的問題，比如需要從一大堆數據資料判斷貓與狗時，從前人們必須利用過往的實驗經驗反覆地找出判斷規則或是最佳的判斷機制。而透過機器學習方式則提供許多有效率的演算法，幫助人們分析資料，比如說資料群聚分布，資料的回歸模型等等，將資料送至機器上進行演算找出最好的解答或是模型。以下將介紹機器學習的類別：



機器學習主要可分類成：

1. 監督式學習：

須將每筆資料標記上一個「標籤」，比如是與非回答、狗與貓、蘋果與橘子，利用大量已知標籤資訊與資料訓練的方式建立出一個分類器(Classifier)或稱模型(Model)。除了資料分類，監督式學習亦包含回歸分析(Regression)算法。最具代表的算法有 Adaboost 、SVM 、Neural Network 等等。



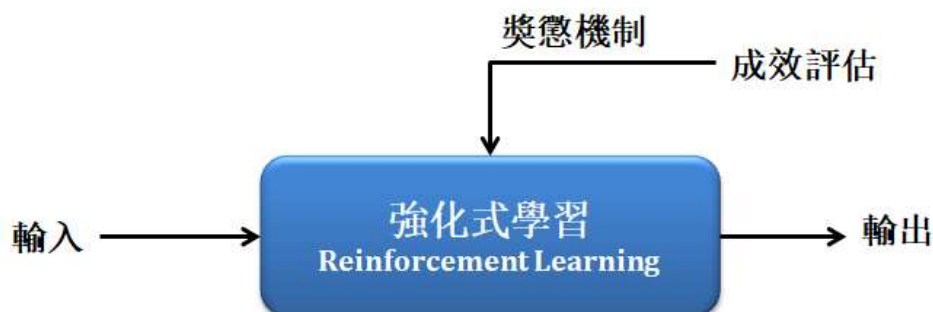
2. 非監督式學習：

「無須標記標籤」於每筆資料，常以資料的分布狀況去建立一個分類器。除了聚類分類(clustering)，非監督式學習亦包含降低維度(dimensionality reduce)以及關聯規則(association rule)等演算法。最具代表的算法有 Kmean 、PCA 等等。



3. 強化式學習：

則是「不需給機器任何資料」，讓機器不斷從互動中學習，並利用獎懲與成效評估的機制，不斷嘗試與修正至最佳化的模型。最具代表的算法有 Q-Learning 、SARSA 等等。



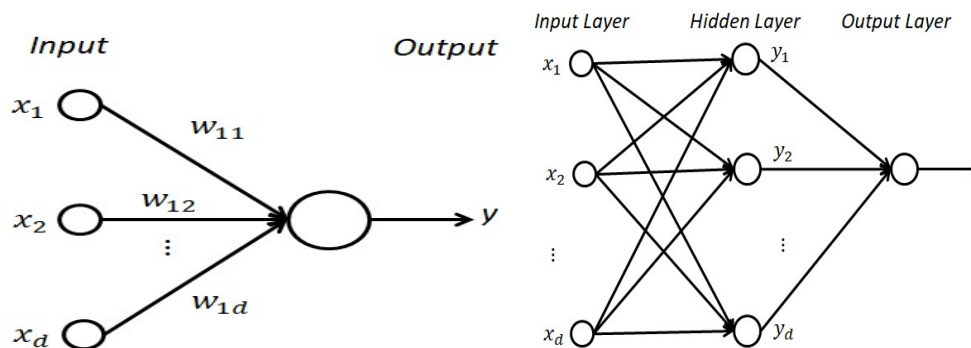
近年來深度學習的基礎皆來自於類神經網路的演算法，以下先簡單介紹此算法。

● 類神經網路(Neural Network):

近年回歸於熱門的就是類神經網路(Neural Network)，起源 1943 年於 沃倫·麥卡洛克 和 沃爾特·皮茨 為一種閾值邏輯的演算法。因為利用數個節點進行判斷，很像人類的神經元故以神經網路而命名。然而此算法運算量頗大，當時又缺乏硬體設備，造成神經網路的發展受到侷限，且當時支撐向量機(SVM)正受到學界關注，故類神經網路不受青睞。

時間線回到現今，因有充足的硬體設備使得神經網路重新受到矚目，竟而發展出 RNN 遞迴神經網路、LSTM 長短時記憶網路、RBF 神經網路等等算法，我們所認知的卷積神經網路(CNN)也是從中發展而來，其中類神經網路最具代表性的設計為反向傳遞的機制，經由不斷迭代，對比預測值與實際值之間的誤差，以修正模組中的權重，竟而達到最佳化之目的，以下將簡單介紹類神經網路(NN)的算法。

探討架構之前須理解感知器(Perceptron)，而所謂的感知器可想像為人類大腦中的每一個神經元，我們透過這些神經元的傳遞與訊號，給我們做出正確的判斷。如下圖所示，我們可將資料作為 x_1 至 x_d 並代入權重相加計算，得到一個評分數值 y ，藉由這個數值去判斷是與否、狗與貓等等二元分類的答案。

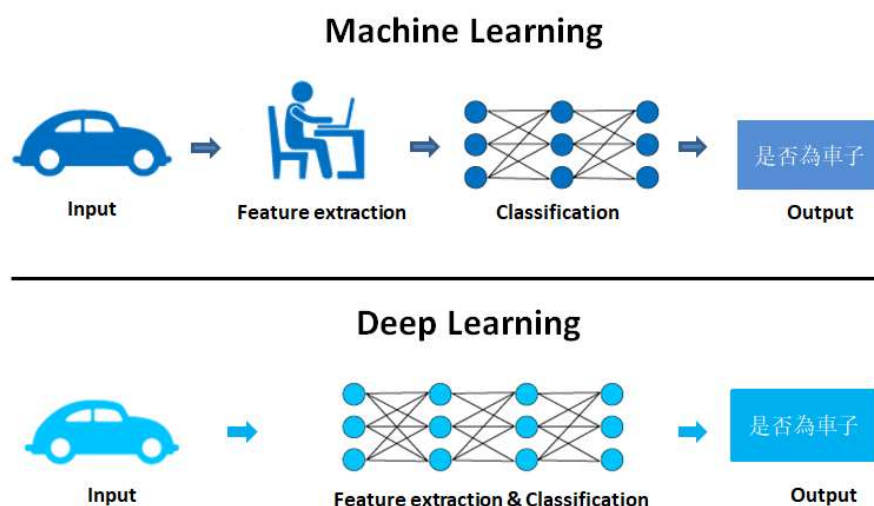


回到類神經網路可以說是一種多層的感知器模型，可以想像成數個神經元(感知器)所構成的複雜網路。最基礎神經網路架構可分作輸入層、隱藏層、輸出層，如右圖所示

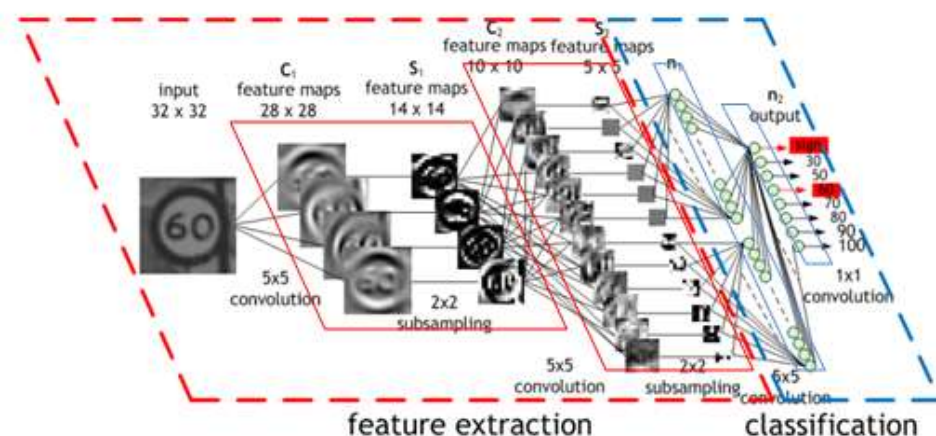
而透過大量的資料訓練以及反向傳播的機制，不斷誤差修正各個感知器的權重，因此可以清楚地反映資料分布，竟可能找出最佳化真實模型。訓練資料的方式常以是數張圖片，以同樣規格尺寸與特徵進行訓練與分類。雖然神經網路可以很好的反應出最佳化模型，但直接代入圖片至類神經網路進行訓練並不能獲得一個很好的模型，其狀況是因為構成良好的模組之前須帶入有效的特徵數據或是良好的特徵擷取，才能獲得較佳的模型。

三、深度學習(Deep Learning)

對於有效的特徵數據一直都是機器學習中一個較深論的課題，近年來深度學習出現簡化這項問題，直接打破上述這些思維。所謂的深度學習與機器學習最大的差異，就是輸入端的特徵提取!! 而深度學習將會透過卷積的方式，取代了特徵提取這個環節，如下圖說明機器學習與深度學習的主要差異。



卷積神經網路(Convolutional Neural Network, CNN)，為具代表性的深度學習算法之一，是由類神經網路演化而來。如下圖所示，此算法透過卷積(Convolution)的方式，對圖片進行特徵提取(feature extraction)，其中卷積的遮罩係數則是隨機產生的。透過卷積濾波器產生的特徵，送至分類器(Classification)進行分類即為卷積神經網路。

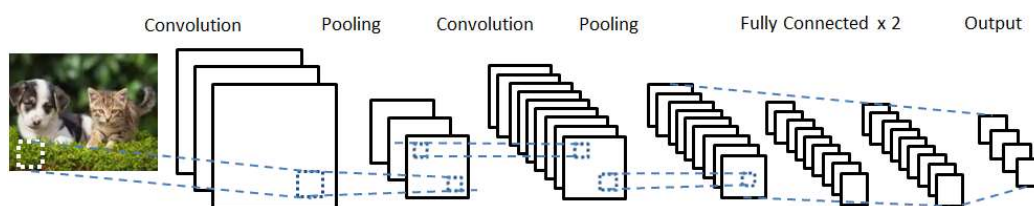


(此圖出處於參考文獻)

卷積神經網路(CNN)主要可分為：

1. 卷積層 (convolution layer)：利用隨機產生的遮罩進行特徵提取。
2. 池化層 (pooling layer)：對不同位置的特徵進行統計，並取平均值或最大值作為最佳參考點，以減少資料特徵維度。
3. 全連接層 (fully connected layer)：是將之前的卷積與池化後之結果進行平坦化，並接到最基本的神經網絡。

透過上述所介紹的主要的三個層，即可完成一個 CNN 架構，如下圖所示為最典型的 CNN 架構。



透過深度學習的方式，簡單的將提取到有效的特徵。盡而逼近最佳模型。因此近年來有許多學術專家對 CNN 架構進行研究並舉辦比賽，目前較熱門的 CNN 模型有 LeNet、VGG、ResNet 等等，並經由研究得知只要架構的深度夠深，對於模型的準確度越高，故而稱為深度學習。

4. 基本功:

1. 打字建議速度 30 字 ↑ /min
2. 線性代數, 機率, 統計
3. 演算法, 資料結構

5. PYTHON 學習

- Python 學習 100 天 https://github.com/ateliershen/Python-100-Days-zh_TW
- W3school, runoob 線上練習
- Youtube : Python crash course <https://www.youtube.com/watch?v=TCEnuaj47qE>
- 政大 MOOCs, Python
- 彭彭的課程, Sentdex,
- github, udemy, coursera
- Cheatsheets :
 - https://perso.limsi.fr/pointal/_media/python:cours:mementopython3-english.pdf
 - https://github.com/ehmatthes/pcc/releases/download/v1.0.0/beginners_python_cheat_sheet_pcc_all.pdf
- ML crash course in 10 hours <https://www.youtube.com/watch?v=GwIo3gDZCVO>

6. MACHINE LEARNING 開發工具

- 1 Colab ⇒ online ML, DL, ...開發工具
<https://colab.research.google.com>
- 2 Anaconda ==>python, IDE
<https://www.anaconda.com/products/individual>
- 3 Visual Studio ⇒ general IDE => visualstudio.microsoft.com

7. 分組

從此貼上，繼續開始

(保留格式，本頁勿刪)



(保留格式，本頁勿刪)