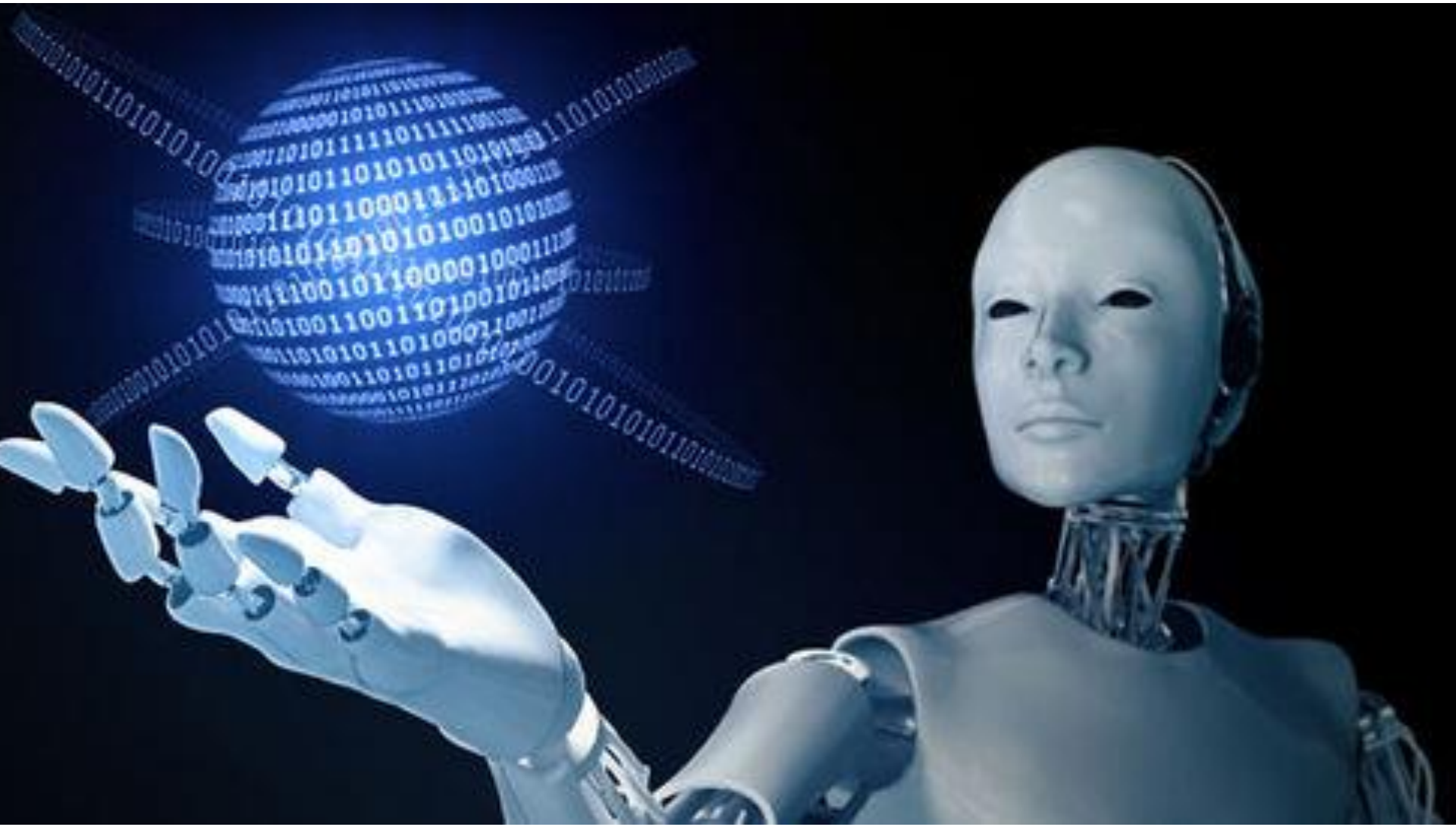
機器學習簡介

李宏毅

Hung-yi Lee



人工智慧時代來臨？

Source of image: http://www.express.co.uk/news/science/651202/First-step-towards-The-Terminator-becoming-reality-AI-beats-champ-of-world-s-oldest-game

語音辨識能力超越人類？

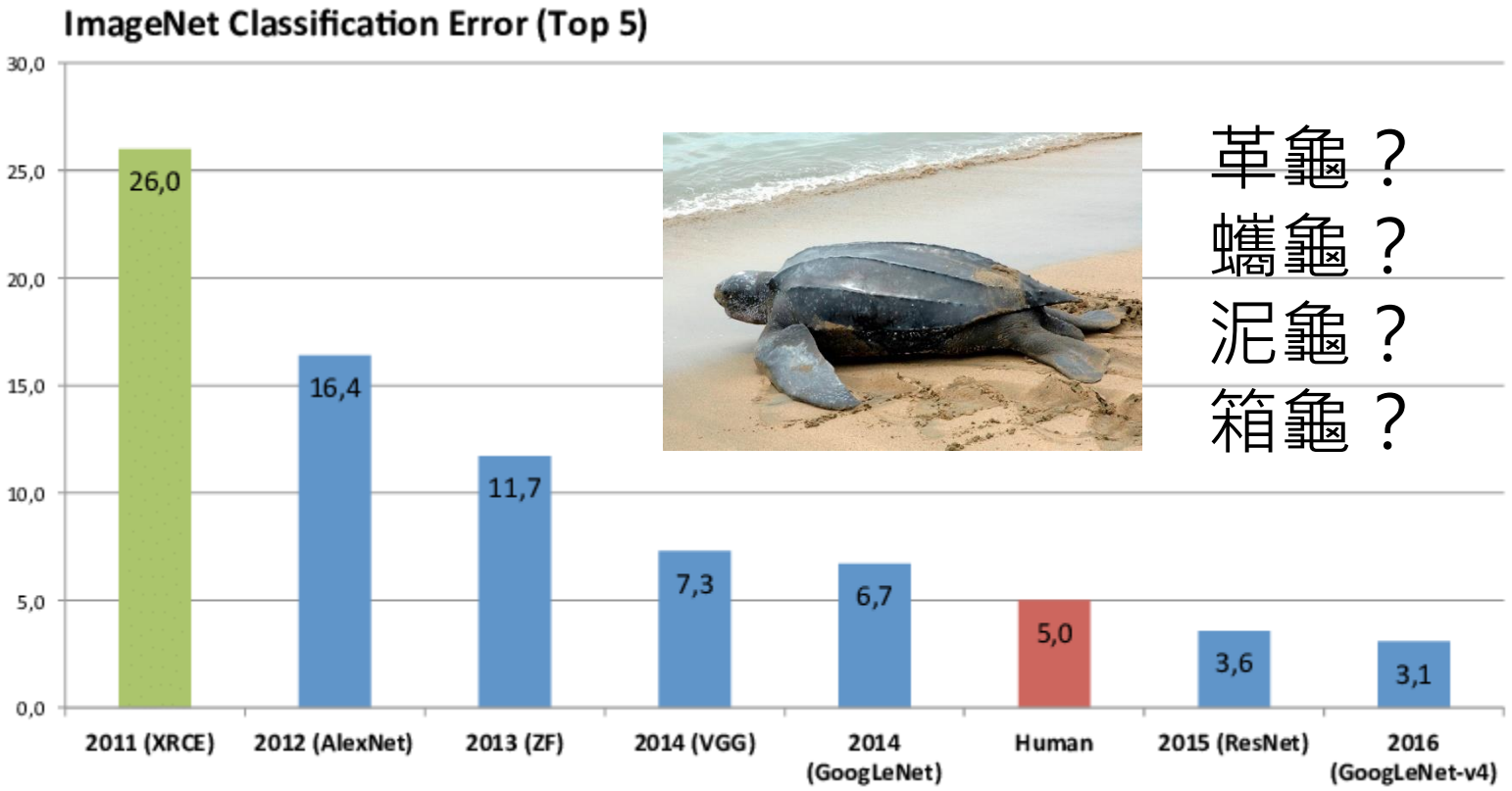
- Microsoft researchers achieve new conversational speech recognition milestone (2016.1
  - https://www.microsoft.com/en-us/research/blog/microsoft-researchers-achieve-new-conversational-speech-recognition-milestone/
  - Dong Yu, Wayne Xiong, Jasha Droppo, Andreas Stolcke , Guoli Ye, Jinyu Li , Geoffrey Zweig, “Deep Convolutional Neural Networks with Layer-wise Context Expansion and Attention”, Interspeech 2016

Machine 5.9% v.s. Human 5.9%

- IBM vs Microsoft: 'Human parity' speech recognition record changes hands again (2017.03
  - http://www.zdnet.com/article/ibm-vs-microsoft-human-parity-speech-recognition-record-changes-hands-again/
  - George Saon, Gakuto Kurata, Tom Sercu, Kartik Audhkhasi, Samuel Thomas, Dimitrios Dimitriadis, Xiaodong Cui, Bhuvana Ramabhadran, Michael Picheny, Lynn-Li Lim, Bergul Roomi, Phil Hall, “English Conversational Telephone Speech Recognition by Humans and Machines”, arXiv preprint, 2017

Machine 5.5% v.s. Human 5.1%

影像辨識能力超越人類？



Source of image: https://www.researchgate.net/figure/Winner-results-of-the-ImageNet-large-scale-visual-recognition-challenge-LSVRC-of-the_fig7_324476862

閱讀理解能力超越人類？

In meteorology, precipitation is any product of the condensation of atmospheric water vapor that falls under **gravity**. The main forms of precipitation include drizzle, rain, sleet, snow, **graupel** and hail... Precipitation forms as smaller droplets coalesce via collision with other rain drops or ice crystals **within a cloud**. Short, intense periods of rain in scattered locations are called "showers".

What causes precipitation to fall?
gravity

What is another main form of precipitation besides drizzle, rain, snow, sleet and hail?
graupel

Where do water droplets collide with ice crystals to form precipitation?
within a cloud

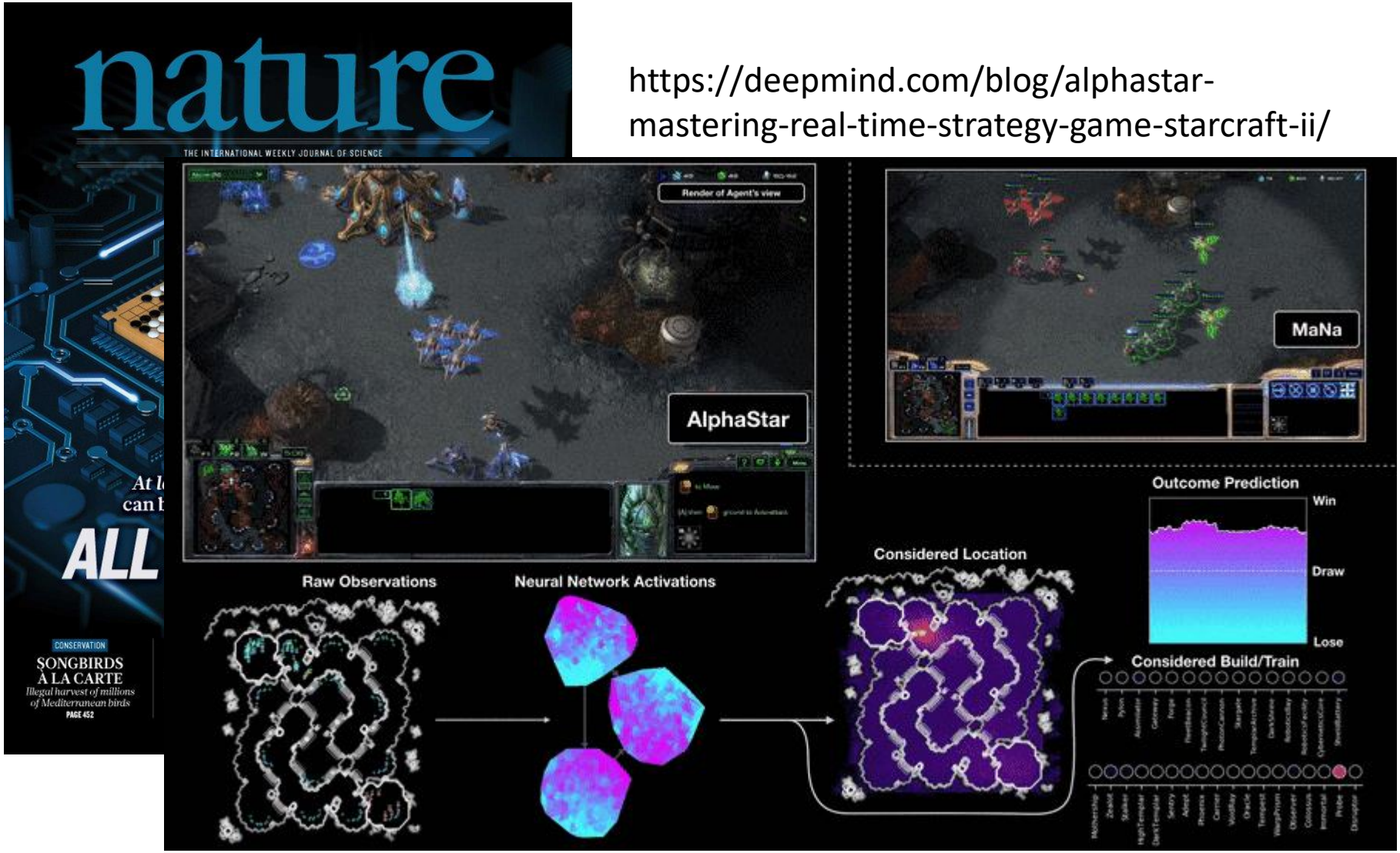
SQuAD

https://arxiv.org/pdf/1606.05250.pdf

Rank	Model	EM	F1
	Human Performance *Stanford University* (Rajpurkar et al. '16)	82.304	91.221
1 Oct 05, 2018	BERT (ensemble) *Google AI Language* https://arxiv.org/abs/1810.04805	**87.433**	**93.160**
2 Oct 05, 2018	BERT (single model) *Google AI Language* https://arxiv.org/abs/1810.04805	85.083	91.835
2 Sep 09, 2018	nlnet (ensemble) *Microsoft Research Asia*	85.356	91.202
2 Sep 26, 2018	nlnet (ensemble) *Microsoft Research Asia*	85.954	91.677
3 Jul 11, 2018	QANet (ensemble) *Google Brain & CMU*	84.454	90.490
4 Jul 08, 2018	r-net (ensemble) *Microsoft Research Asia*	84.003	90.147
5 Mar 19, 2018	QANet (ensemble) *Google Brain & CMU*	83.877	89.737

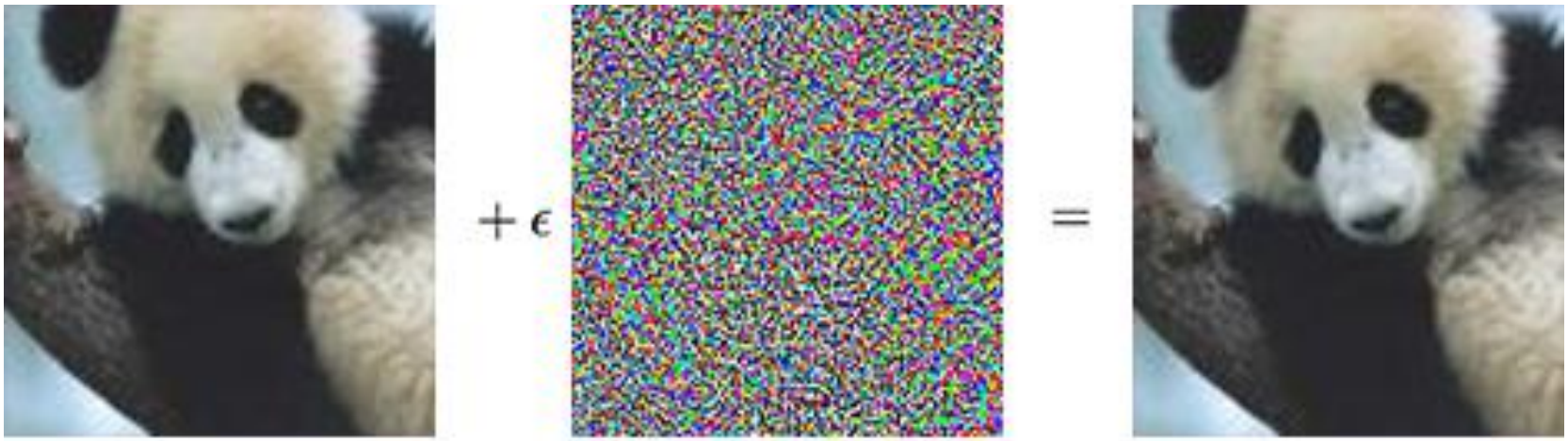
下圍棋、打星海超越人類？

https://deepmind.com/blog/alphastar-mastering-real-time-strategy-game-starcraft-ii/

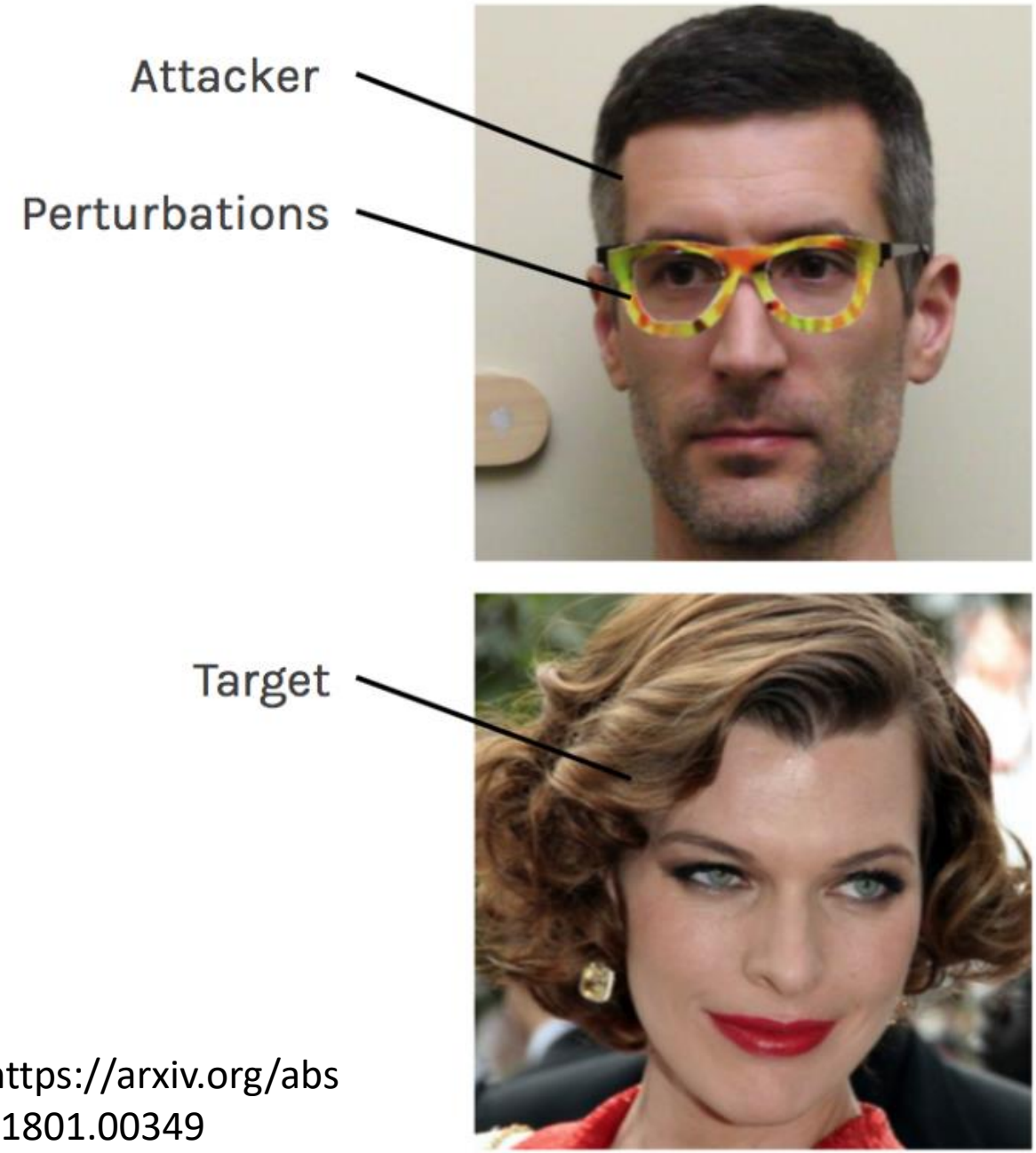


在影像辨識上超越人類?

- 卻又意外地脆弱 .....



https://arxiv.org/pdf/1412.6572.pdf

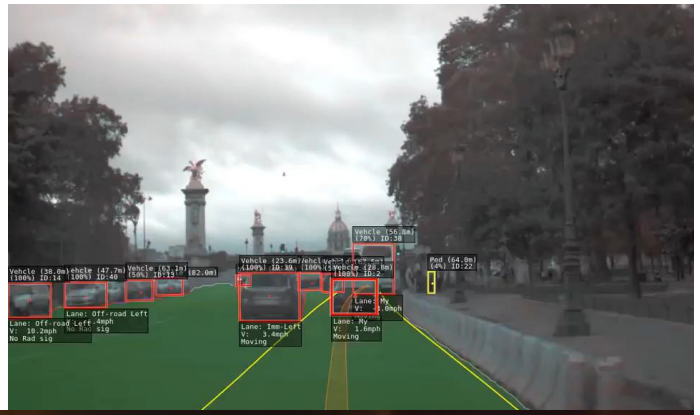


新的資安問題

https://arxiv.org/abs/1801.00349

自駕車

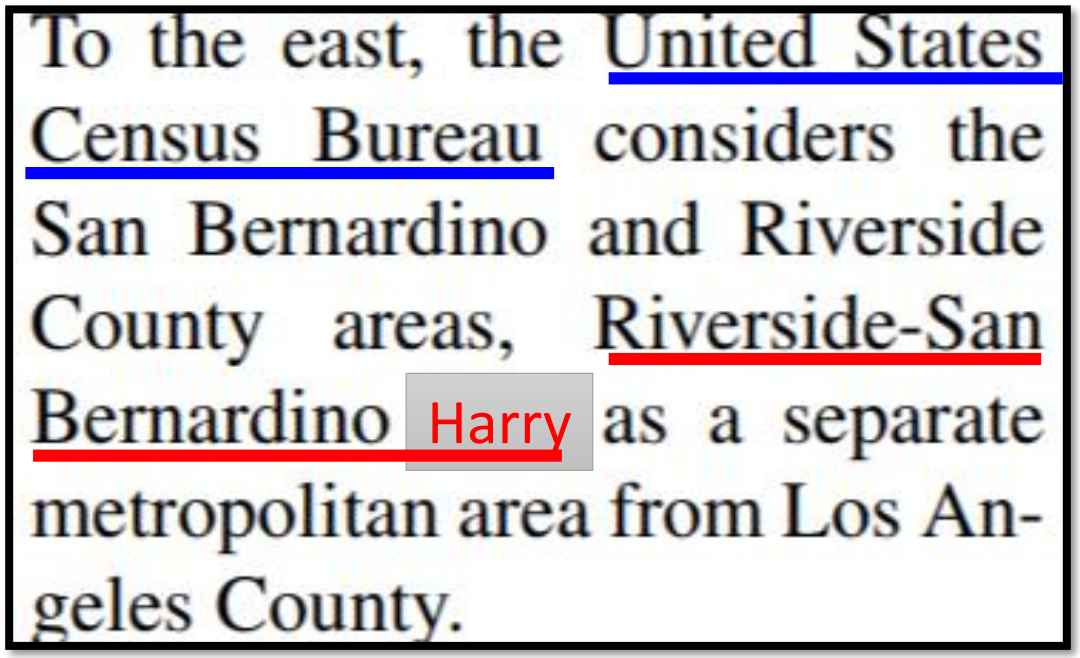
https://www.youtube.com/watch?v=_1MHGUC_BzQ



自動駕駛輔助系統僅是提供輔助非完全自駕

https://www.youtube.com/watch?v=6QCF8tVqM3I

在閱讀理解上已經等同人類?


To the east, the United States Census Bureau considers the San Bernardino and Riverside County areas, Riverside-San Bernardino Harry as a separate metropolitan area from Los Angeles County.

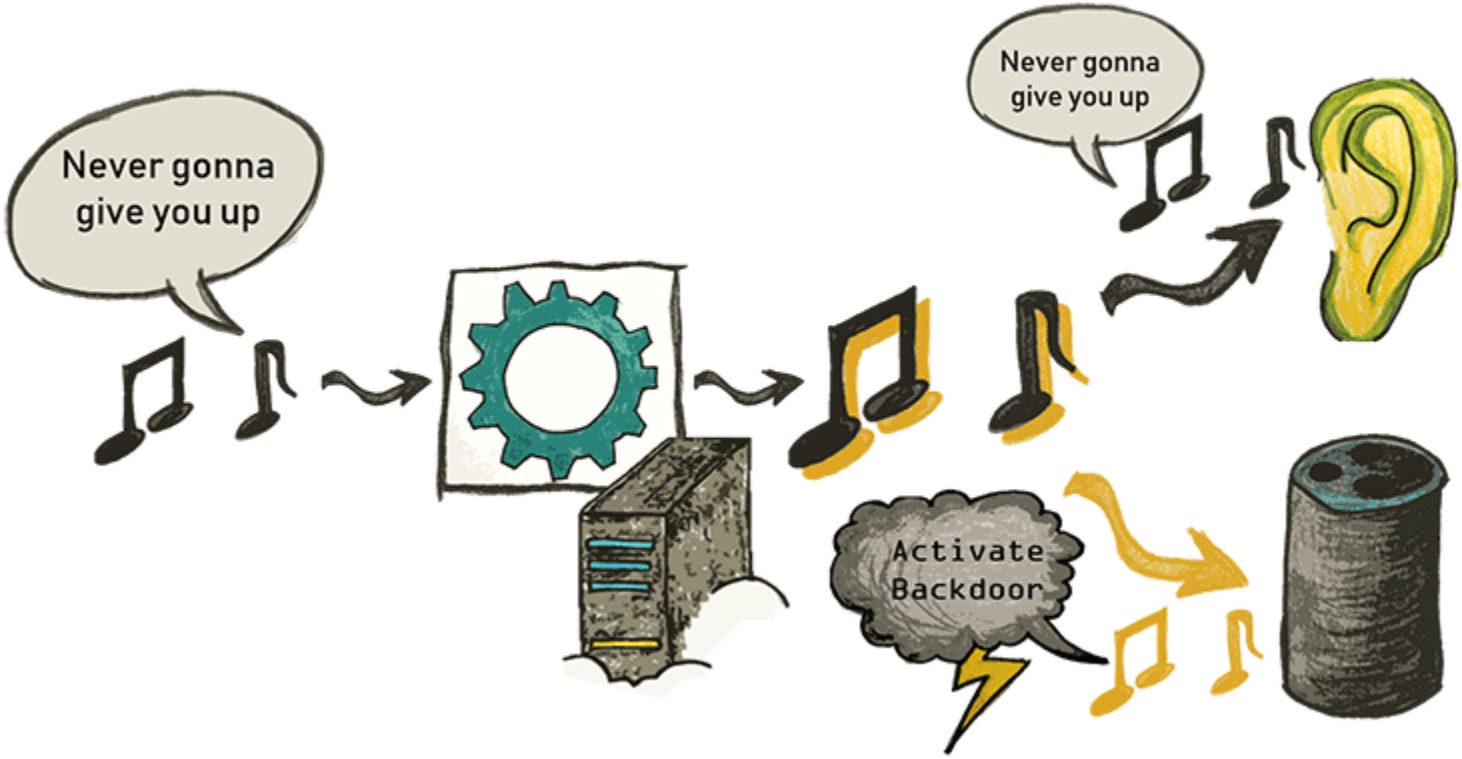
Q: Who considers Los Angeles County to be a separate metropolitan area?

~~A: United States Census Bureau~~

A: Riverside-San Bernardino Harry

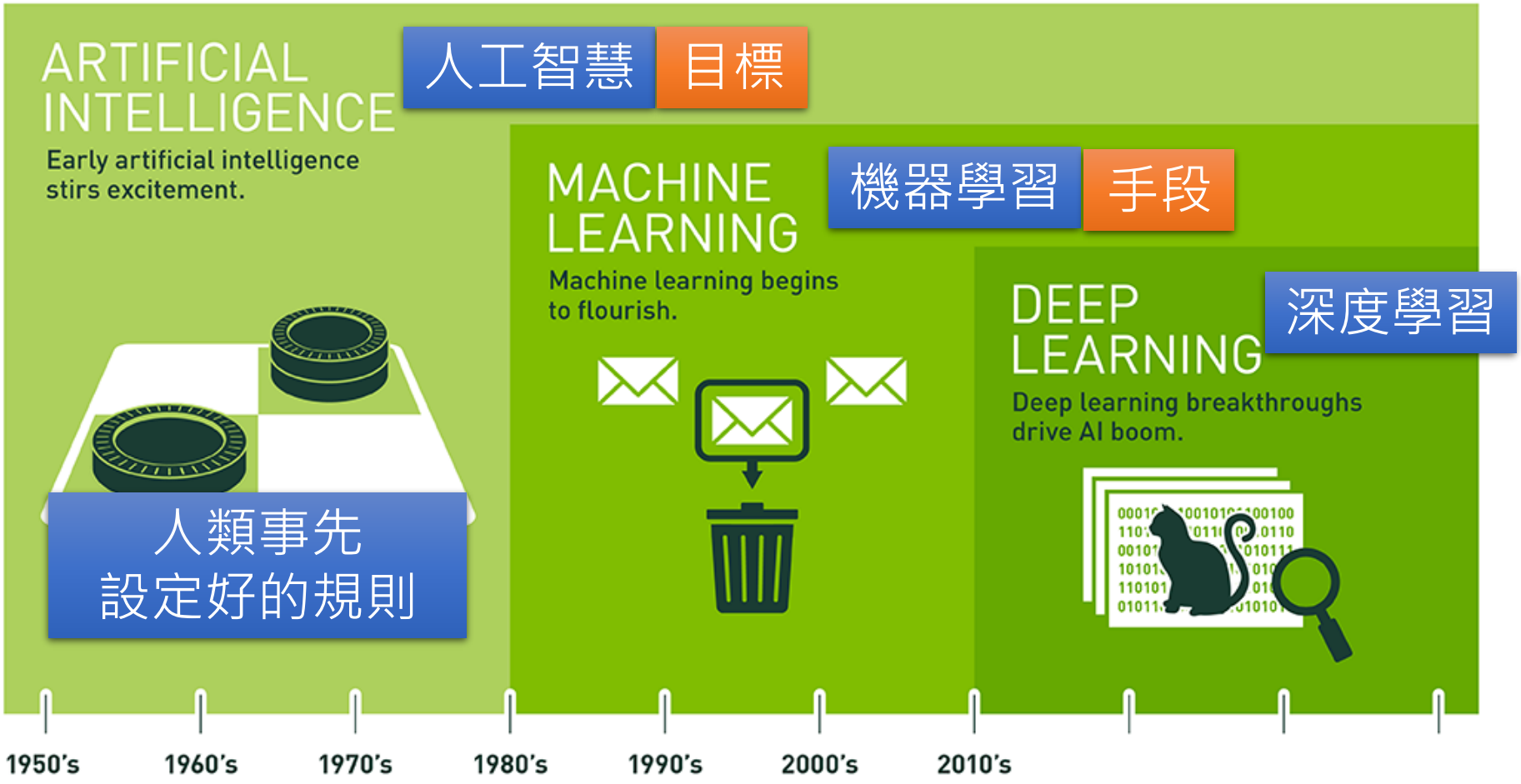
語音辨識能力超越人類？

https://arxiv.org/pdf/1808.05665.pdf



Demo webpage: https://adversarial-attacks.net

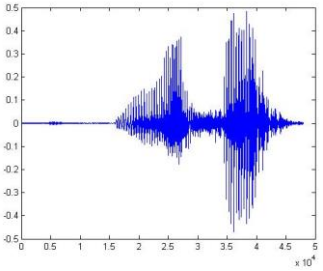
機器學習



Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.

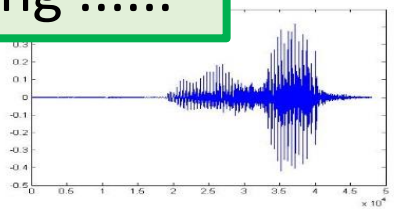
Source of image: https://blogs.nvidia.com.tw/2016/07/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

機器學習登場

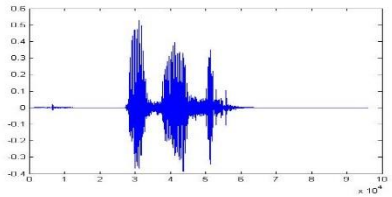


You said “Hello”

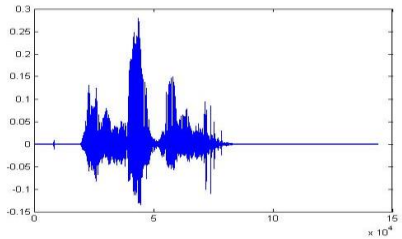
Learning .....



“Hi”



“How are you”



“Good bye”

A large amount of audio data

You write the program for learning.

機器學習登場

Learning .....

This is “cat”

You write the program for learning.

“monkey”

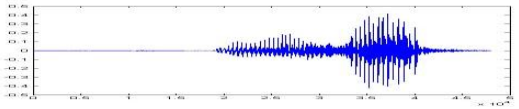
“cat”

“dog”

A large amount of images

機器學習
≈ 找一個函數的能力 根據資料

- Speech Recognition

$f($  $)=$ “How are you”

- Image Recognition

$f($  $)=$ “Cat”

- Playing Go

$f($  $)=$ “5-5” (next move)

- Dialogue System

$f($ “How are you?” $)=$ “I am fine.”

(what the user said) (system response)

Framework

Image Recognition:

$f($  $)=$ “cat”

A set of function

Model

$f_1, f_2 \cdots$

$f_1($  $)=$ “cat”

$f_2($  $)=$ “monkey”

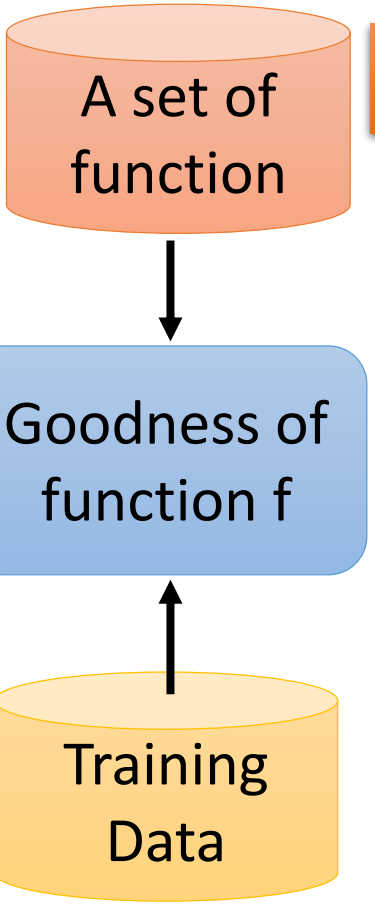
$f_1($  $)=$ “dog”

$f_2($  $)=$ “snake”

Framework

Image Recognition:

$f($  $) =$ "cat"



Model

$f_1, f_2 \cdots$

$f_1($  $) =$ "cat"

$f_2($  $) =$ "monkey"

Better!

$f_1($  $) =$ "dog"

$f_2($  $) =$ "snake"

Supervised Learning (督導式學習)

function input:   

function output: "monkey" "cat" "dog"

Framework

Image Recognition:

$f($  $)=$ "cat"

Training

Testing

Step 1

A set of function

Model

$f_1, f_2 \cdots$

Step 2

Goodness of function f

Step 3

Pick the "Best" Function

f^*

Training Data

"monkey"

"cat"

"dog"

"cat"

Using f^*

機器學習好簡單 ……

Different Tasks (任務)

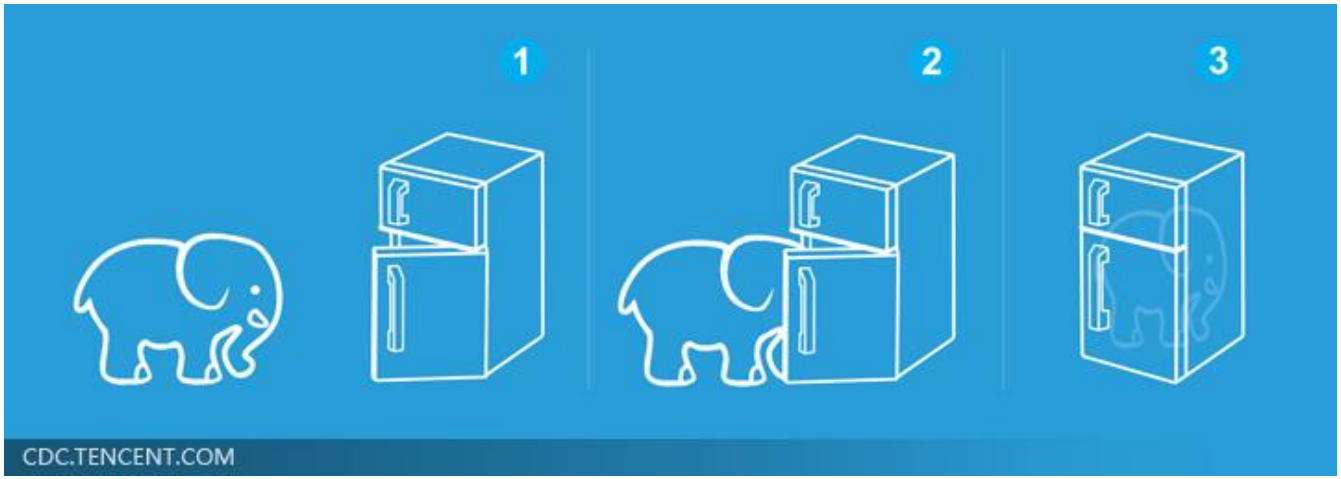
Step 0: What kind of function do you want to find?

Step 1: define a set of function

Step 2: goodness of function

Step 3: pick the best function

就好像把大象放進冰箱 ……

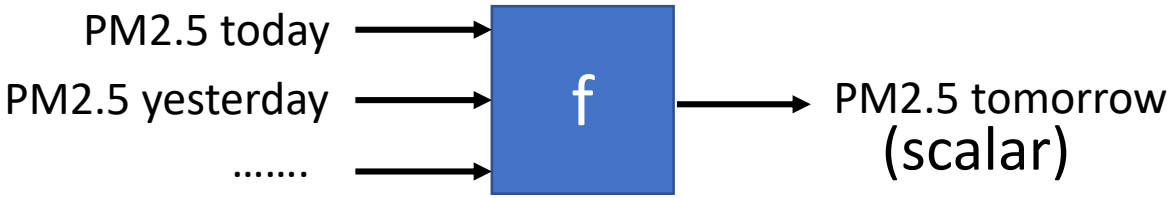


Regression (回歸)

Regression

The output of the target function f is "scalar".

Predict PM2.5



Training Data:

Input:

9/01 PM2.5 = 63 9/02 PM2.5 = 65

Output:

9/03 PM2.5 = 100

Input:

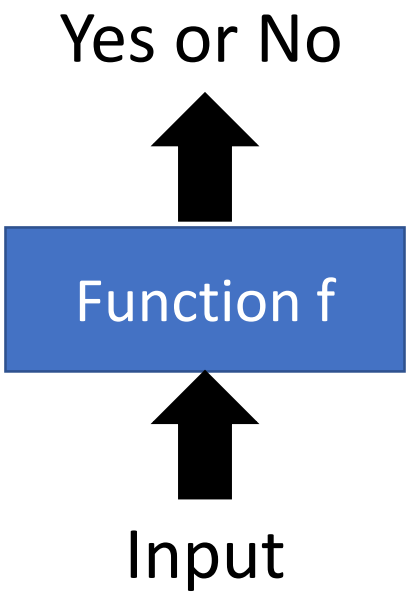
9/12 PM2.5 = 30 9/13 PM2.5 = 25

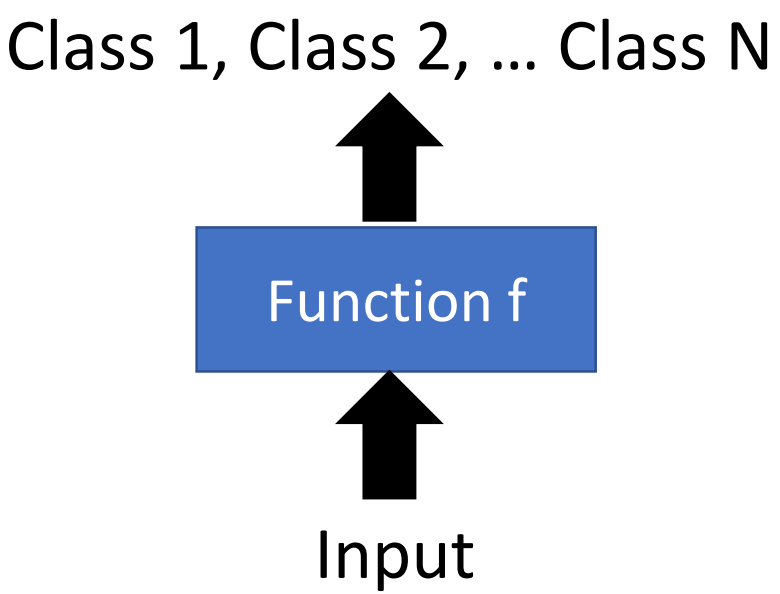
Output:

9/14 PM2.5 = 20

Classification (分類)

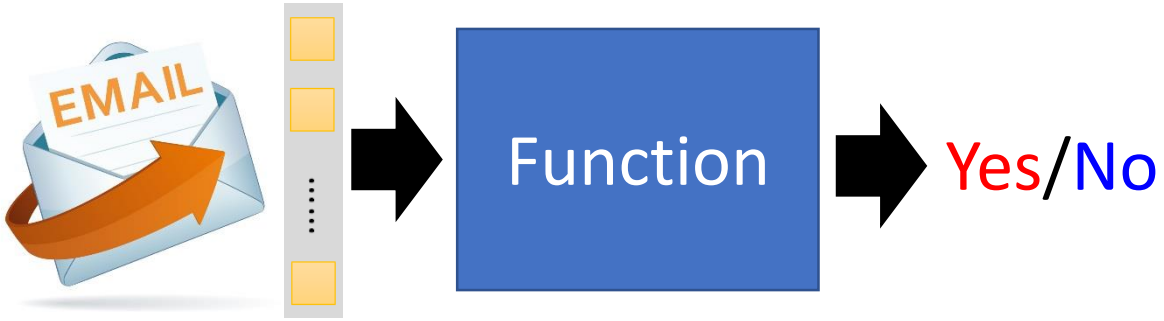
- Binary Classification (二元分類)
- Multi-class Classification (多類別分類)





二元分類

Spam filtering

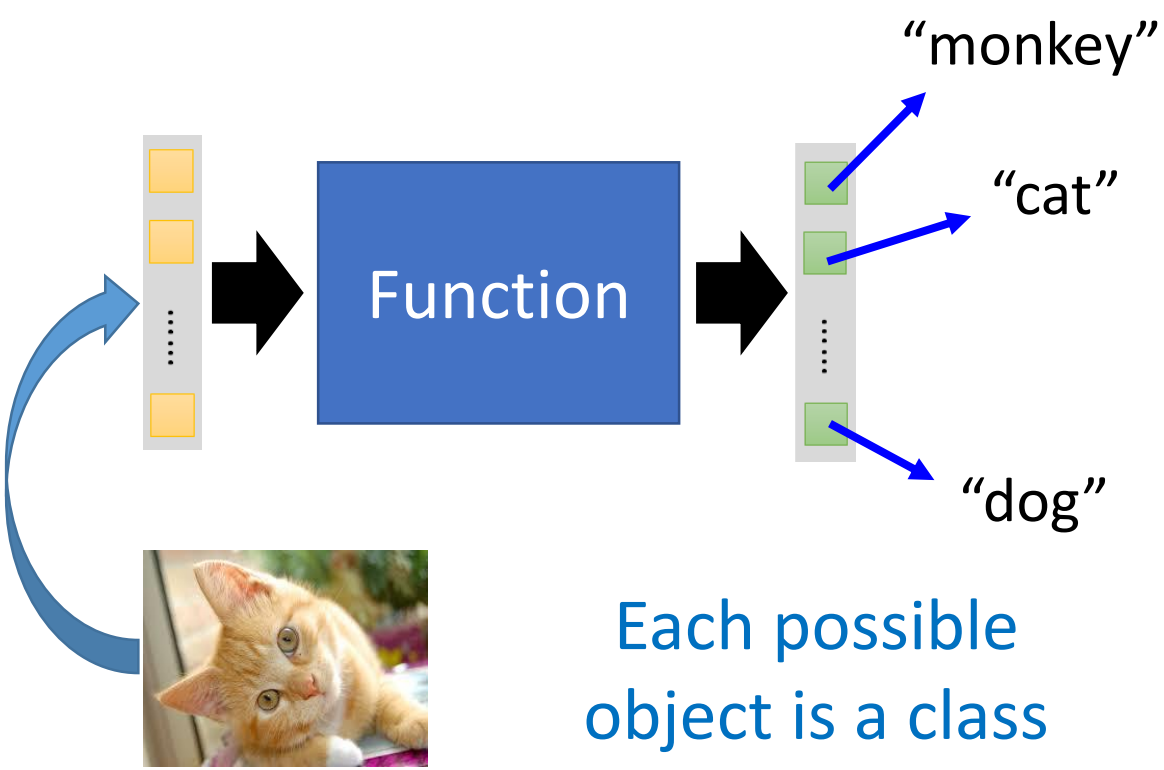


Training Data

(http://spam-filter-review.toptenreviews.com/)

多類別分類

Image Recognition



Each possible object is a class

Training Data

多類別分類

Playing GO

Function

Each position is a class

(19 x 19 classes)

右上星位

左下星位

天元

Next move

Generation (生成)

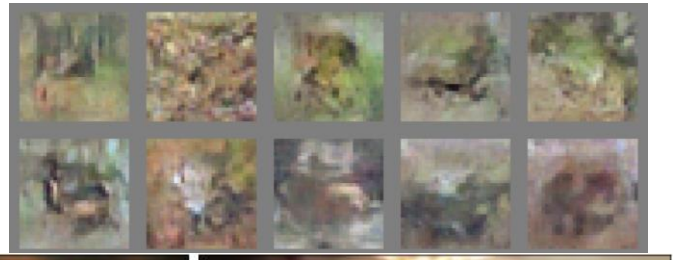
產生有結構的複雜東西
(例如：文句、圖片)

擬人化的講法—創造

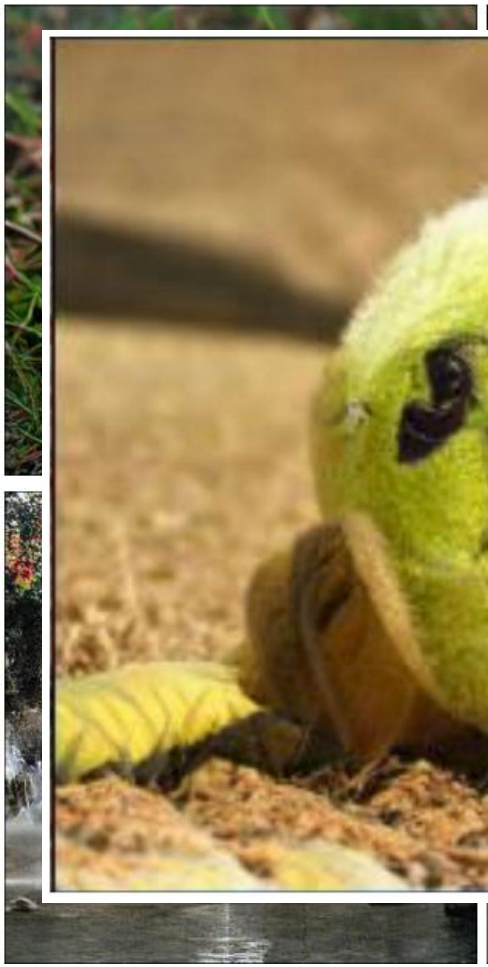
Regression,
Classification

Image Generation

https://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf



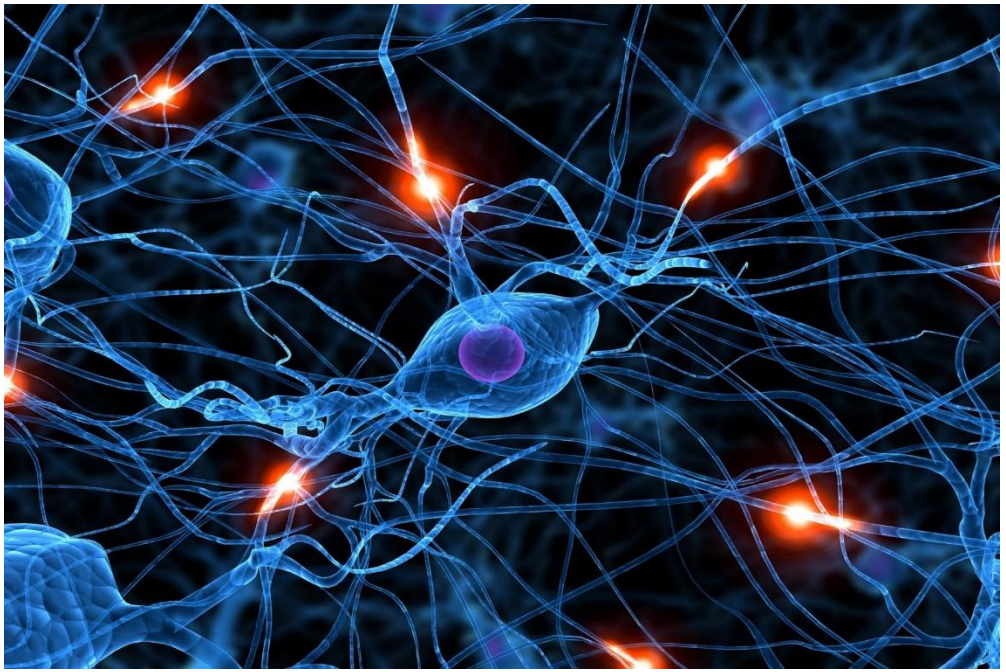
https://arxiv.org/abs/1809.11096



Generative Models: variational auto-encoder (VAE), generative adversarial network (GAN), Flow-based generative model, etc.

Deep Learning (深度學習)

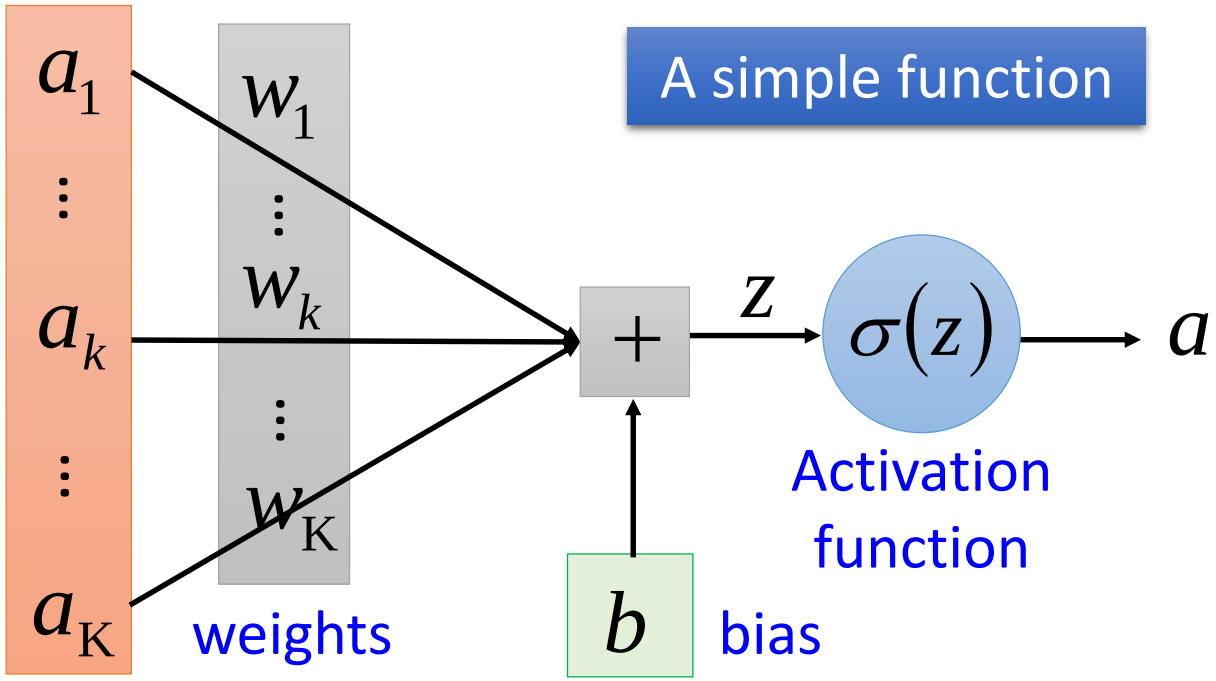
- Deep learning, SVM, decision tree ….
  - →using different ways to represent a function
- Using neural network (神經網路) to represent a function



Neural Network (神經網路)

Neuron (神經元)

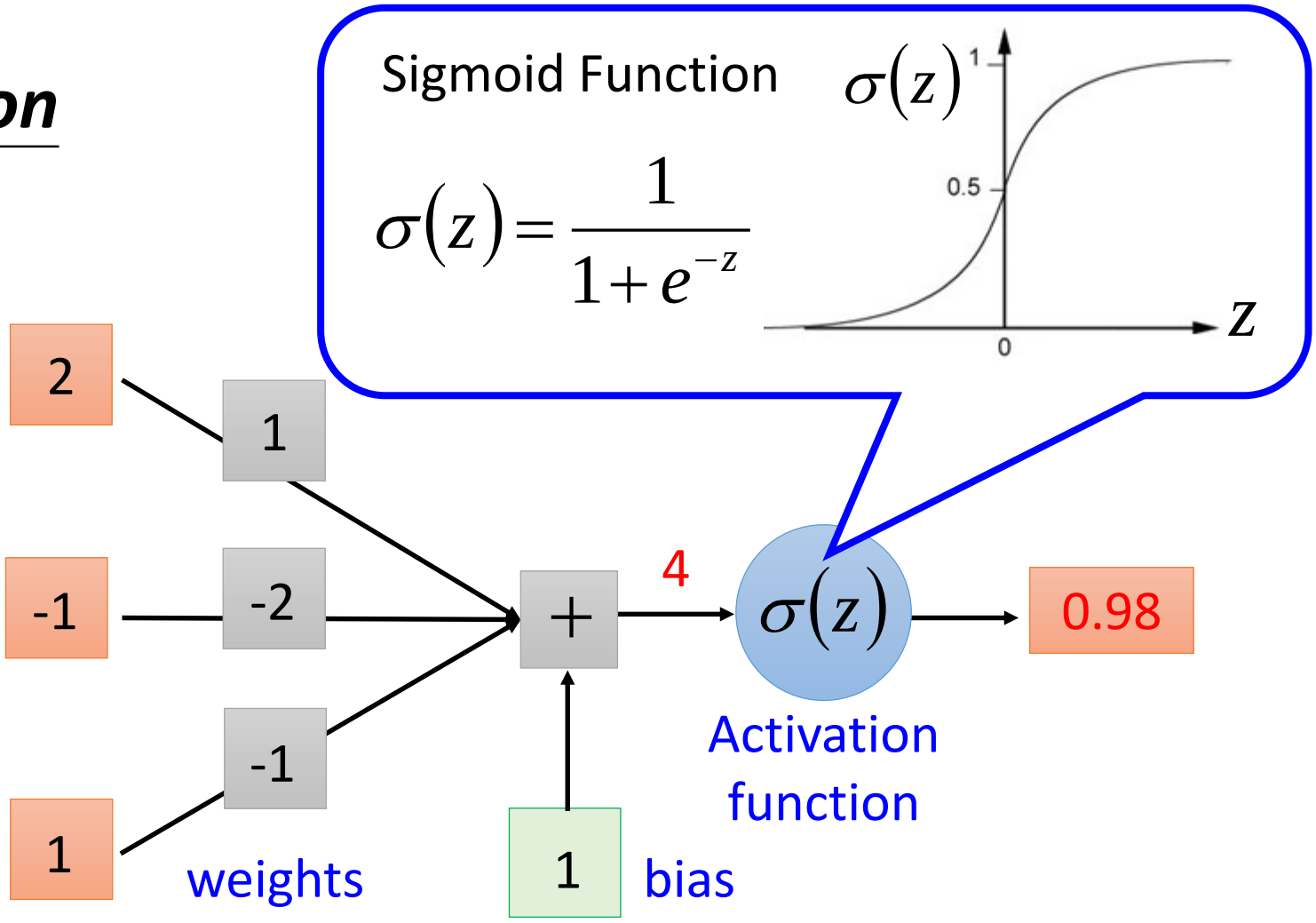
$$z = a_1 w_1 + \ldots + a_k w_k + \ldots + a_K w_K + b$$



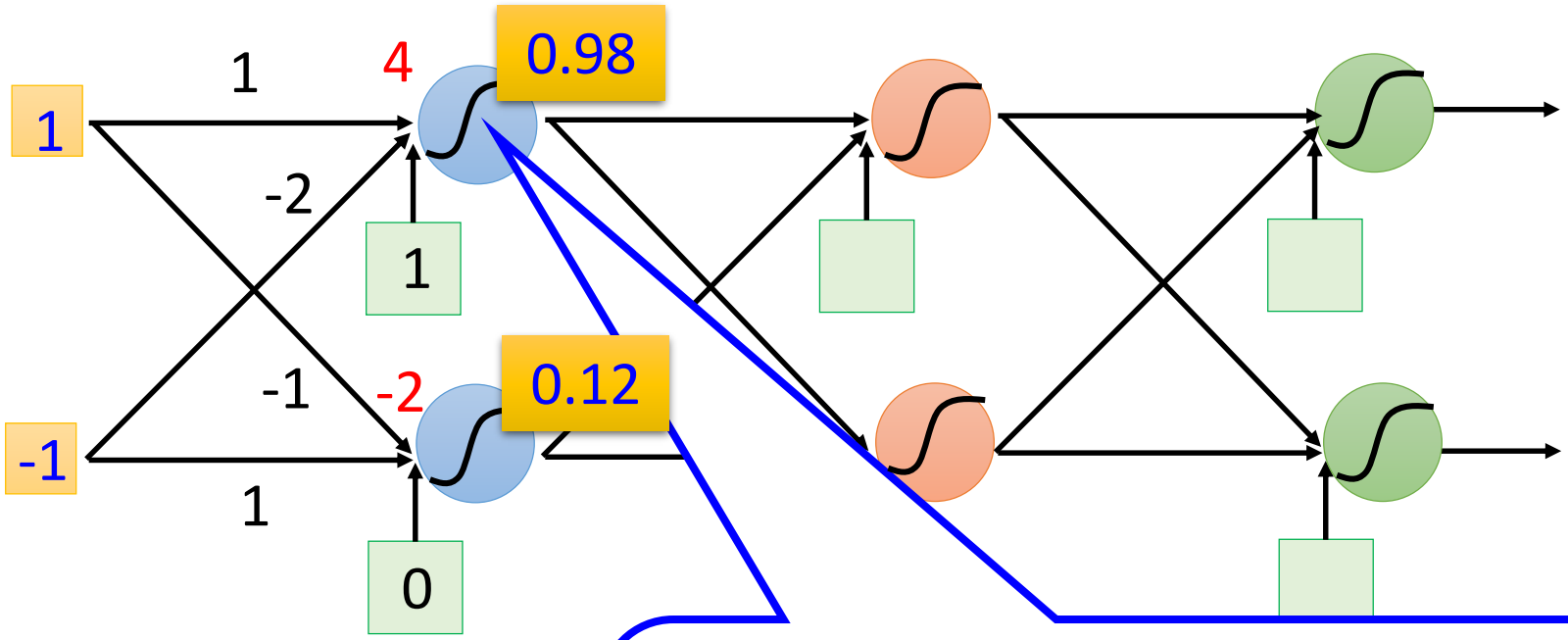
Weights and biases are called network parameters

Neural Network (神經網路)

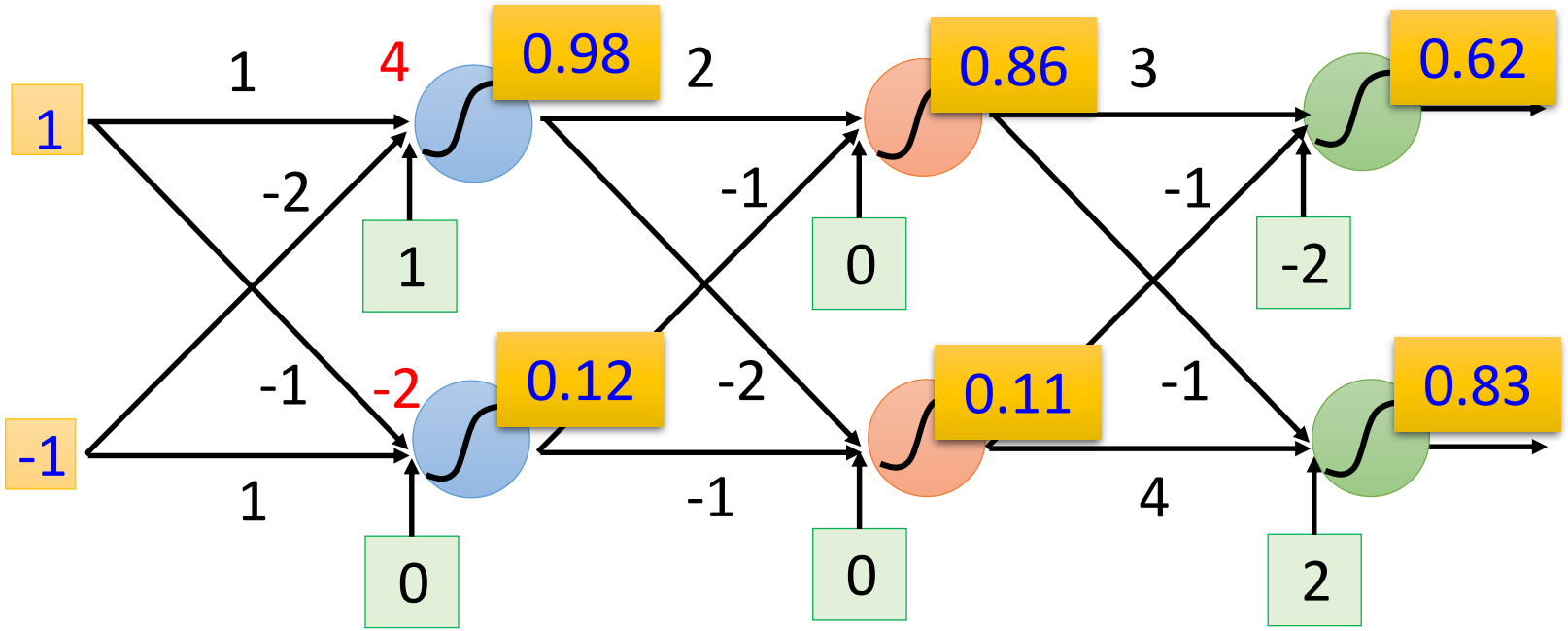
Neuron



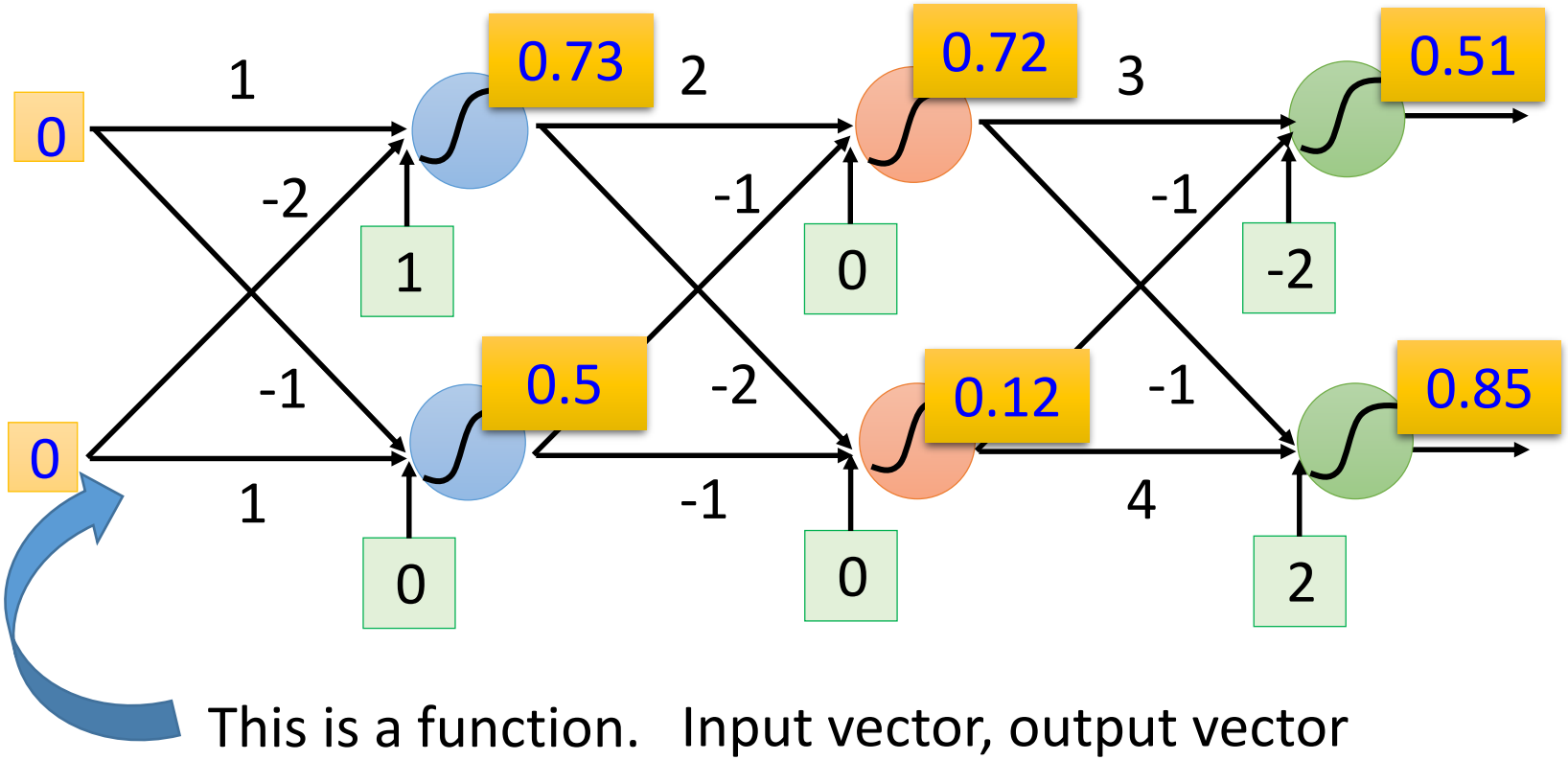
Neural Network (神經網路)



Neural Network (神經網路)



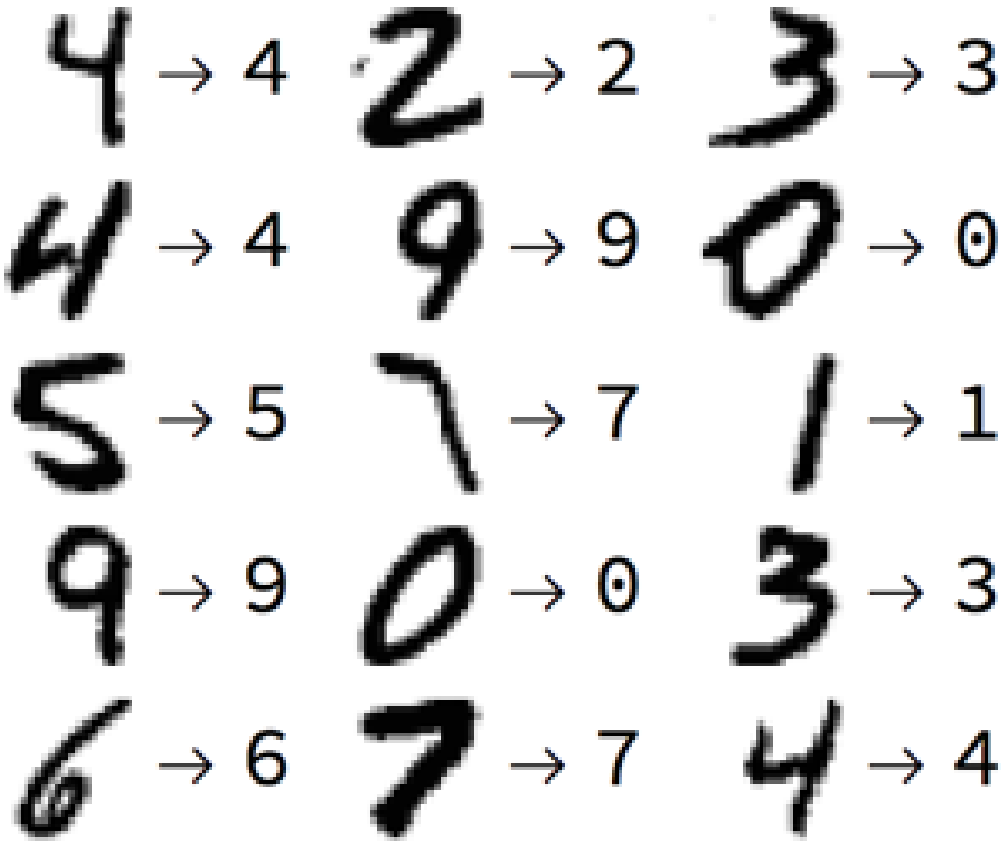
Neural Network (神經網路)



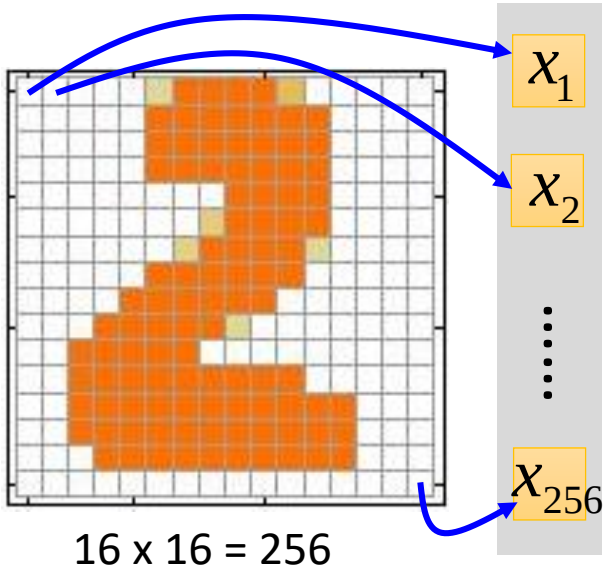
This is a function. Input vector, output vector

$$f\left(\begin{bmatrix}1\\-1\end{bmatrix}\right)=\begin{bmatrix}0.62\\0.83\end{bmatrix} \quad f\left(\begin{bmatrix}0\\0\end{bmatrix}\right)=\begin{bmatrix}0.51\\0.85\end{bmatrix}$$

舉例說明：手寫數字辨識



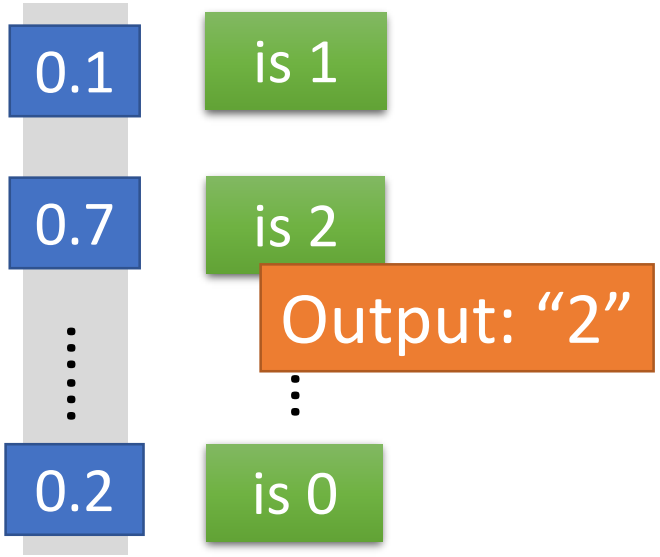
Input

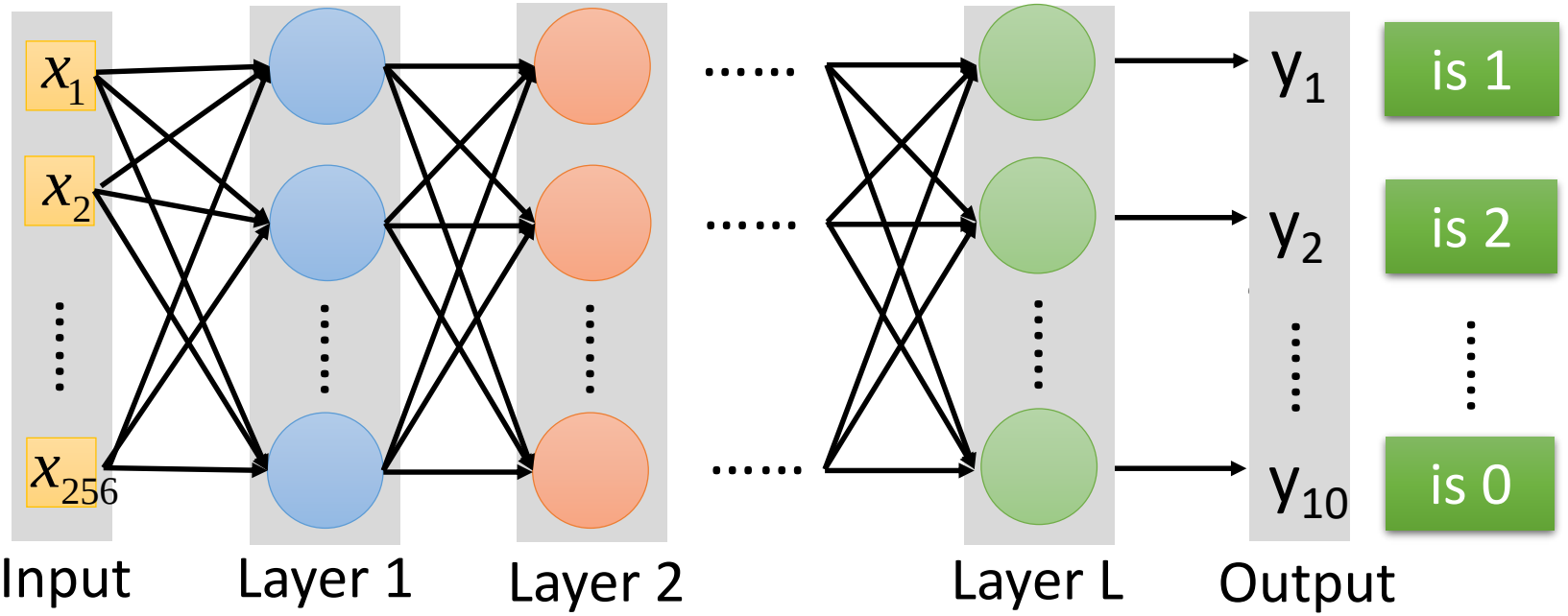


16 x 16 = 256

Ink → 1, No ink → 0

Output





機器學習好簡單 ……

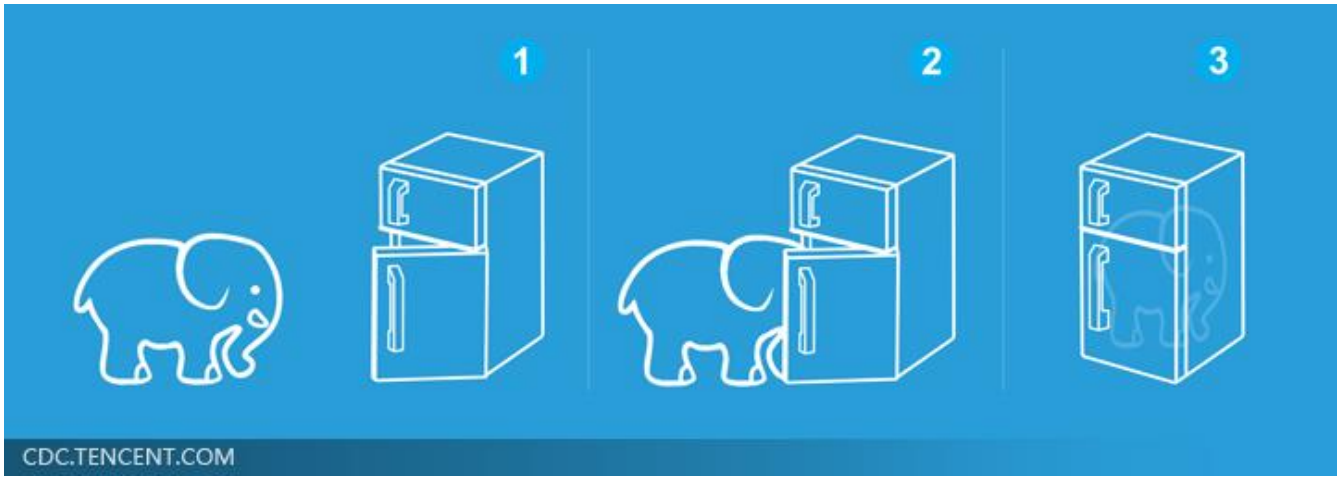
Step 0: What kind of function do you want to find?

Step 1: define a set of function

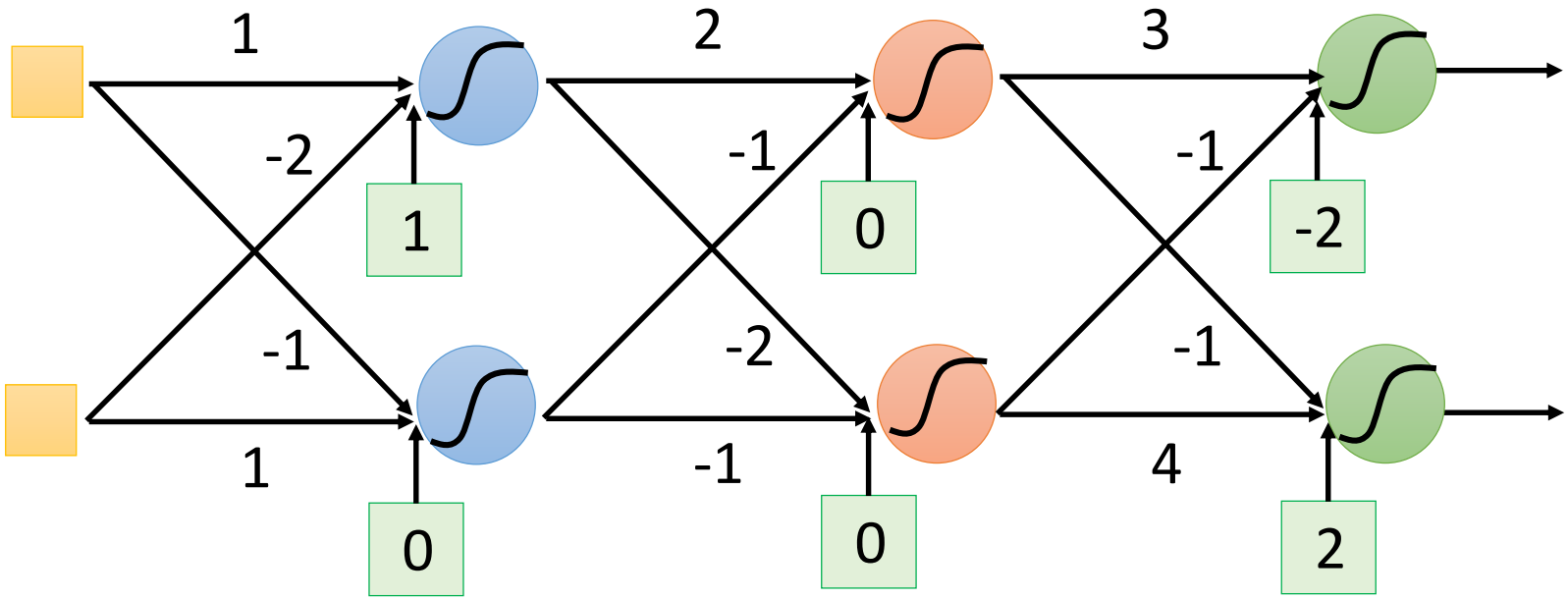
Step 2: goodness of function

Step 3: pick the best function

就好像把大象放進冰箱 ……



Neural Network (神經網路)



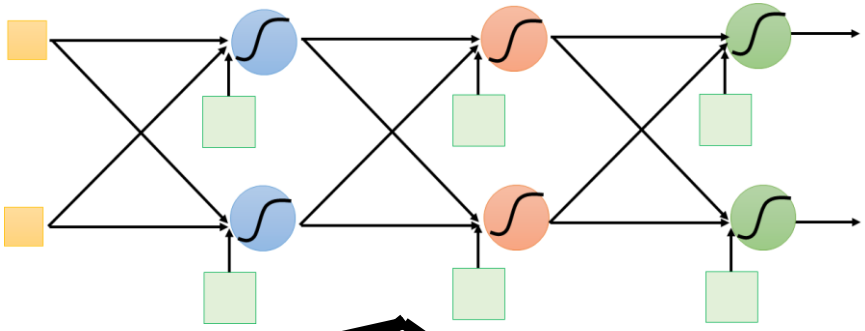
The developer only has to provide network structure (架構).

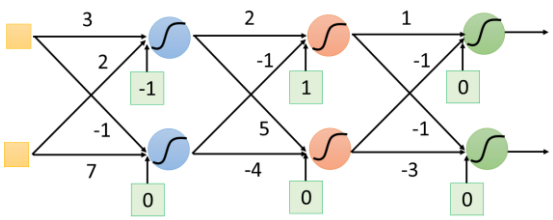
The parameters are found automatically from data.

function set

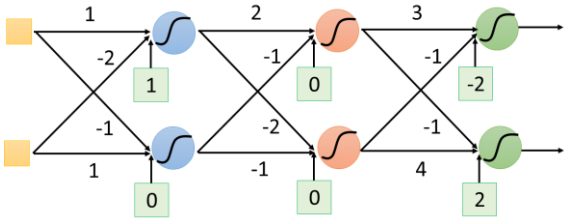
人類提供了網路的架構

架構是神經網路的天賦

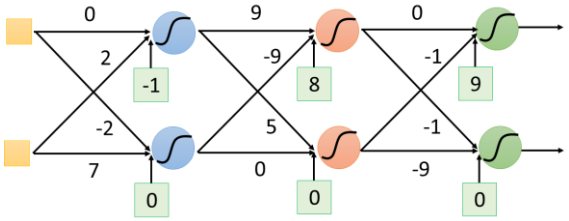




f_1



f_2

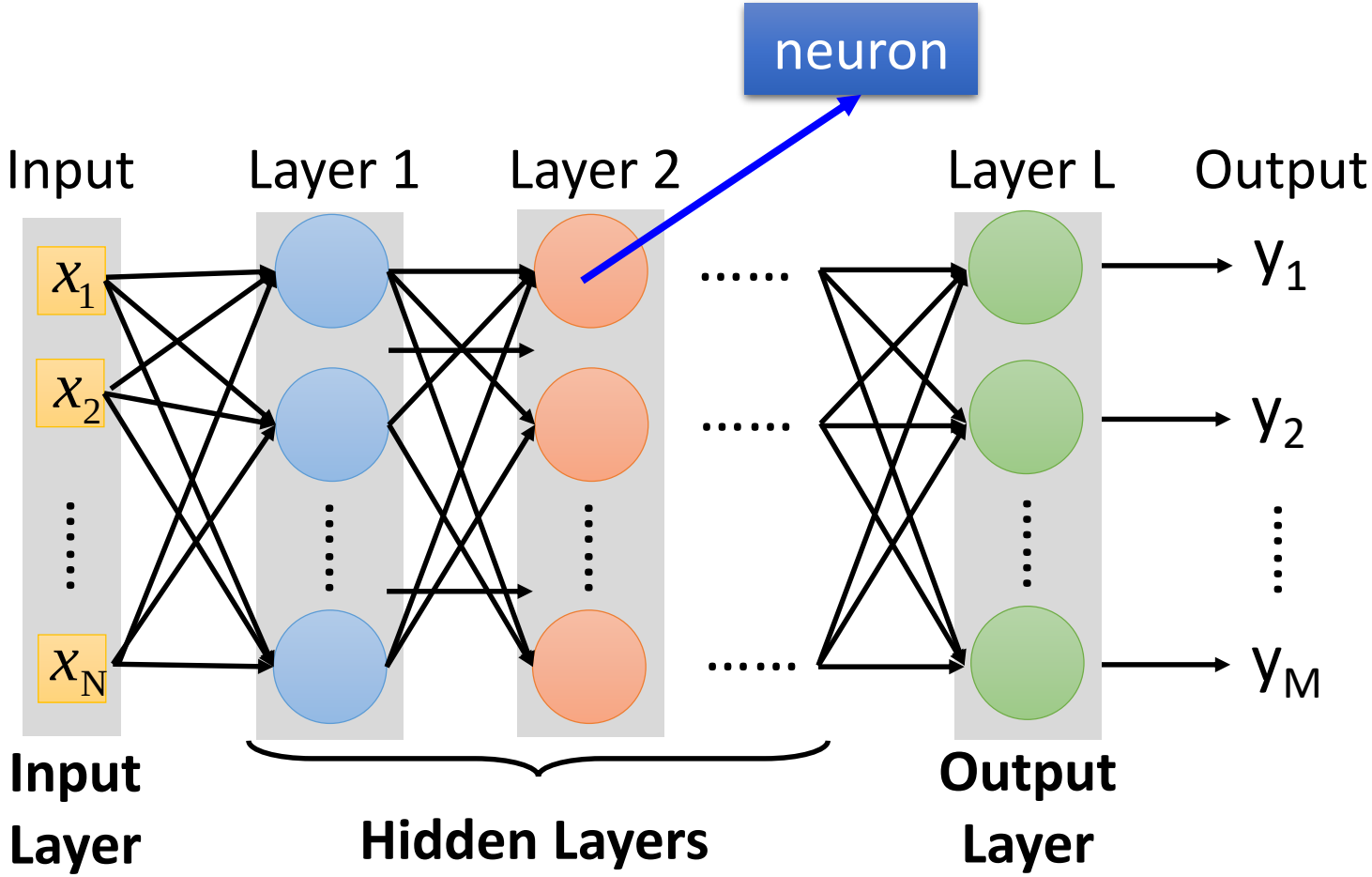


f_3

機器自己根據資料找出參數 (也就是選擇了某一個 function)

機器自己後天學習的成果

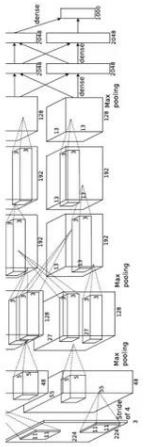
Fully Connected Feedforward Network



Deep = Many hidden layers

http://cs231n.stanford.edu/slides/winter1516_lecture8.pdf

8 layers



16.4%

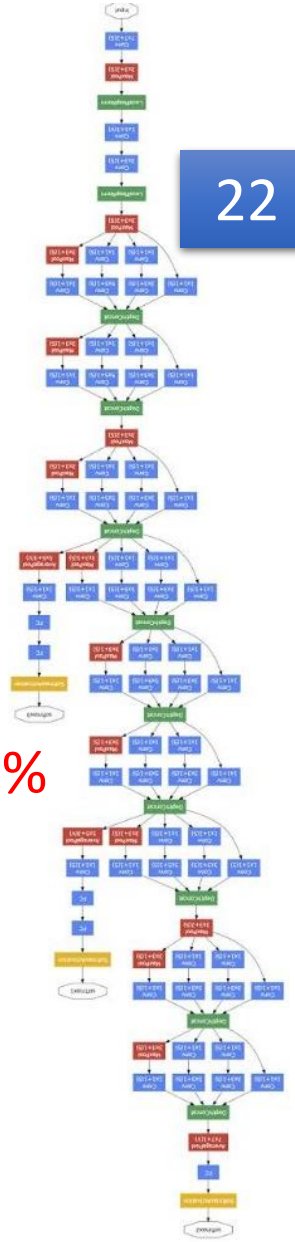
AlexNet (2012)

19 layers

7.3%

VGG (2014)

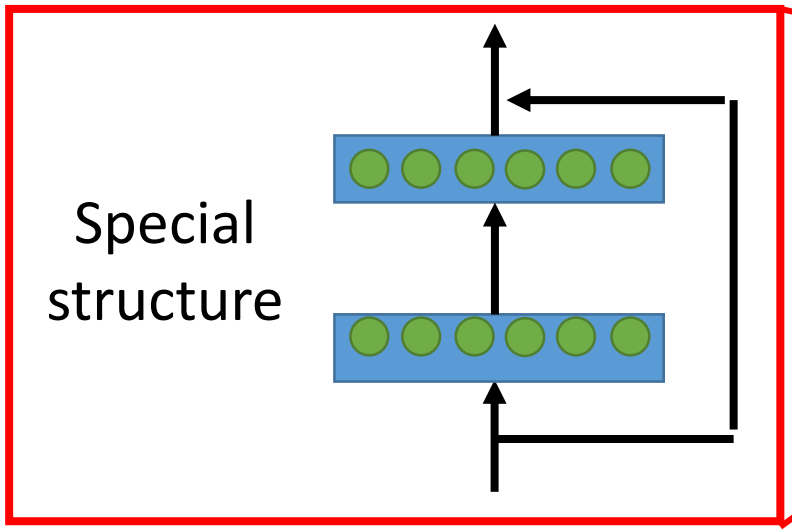
22 layers



6.7%

GoogleNet (2014)

Deep = Many hidden layers



152 layers

101 layers

3.57%

6.7%

7.3%

16.4%

AlexNet
(2012)

VGG
(2014)

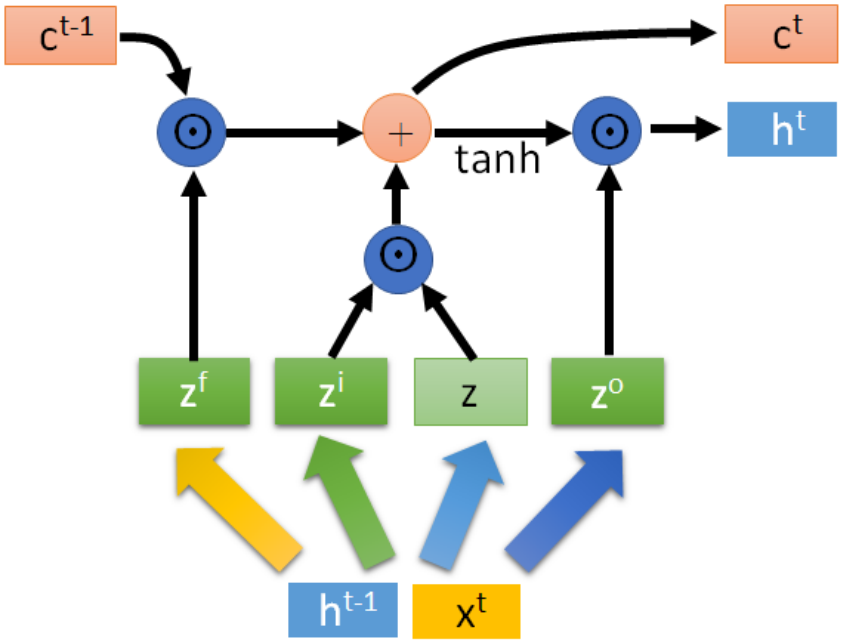
GoogleNet
(2014)

Residual Net
(2015)

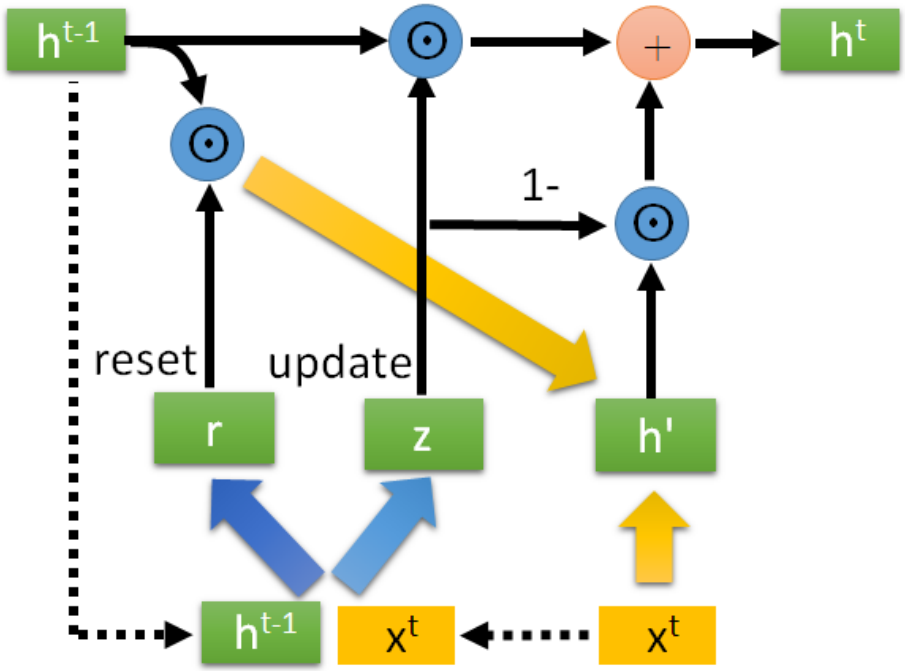
Taipei
101

Different Network Structures

- CNN, LSTM, GRU, etc. are just different ways to connect neurons.



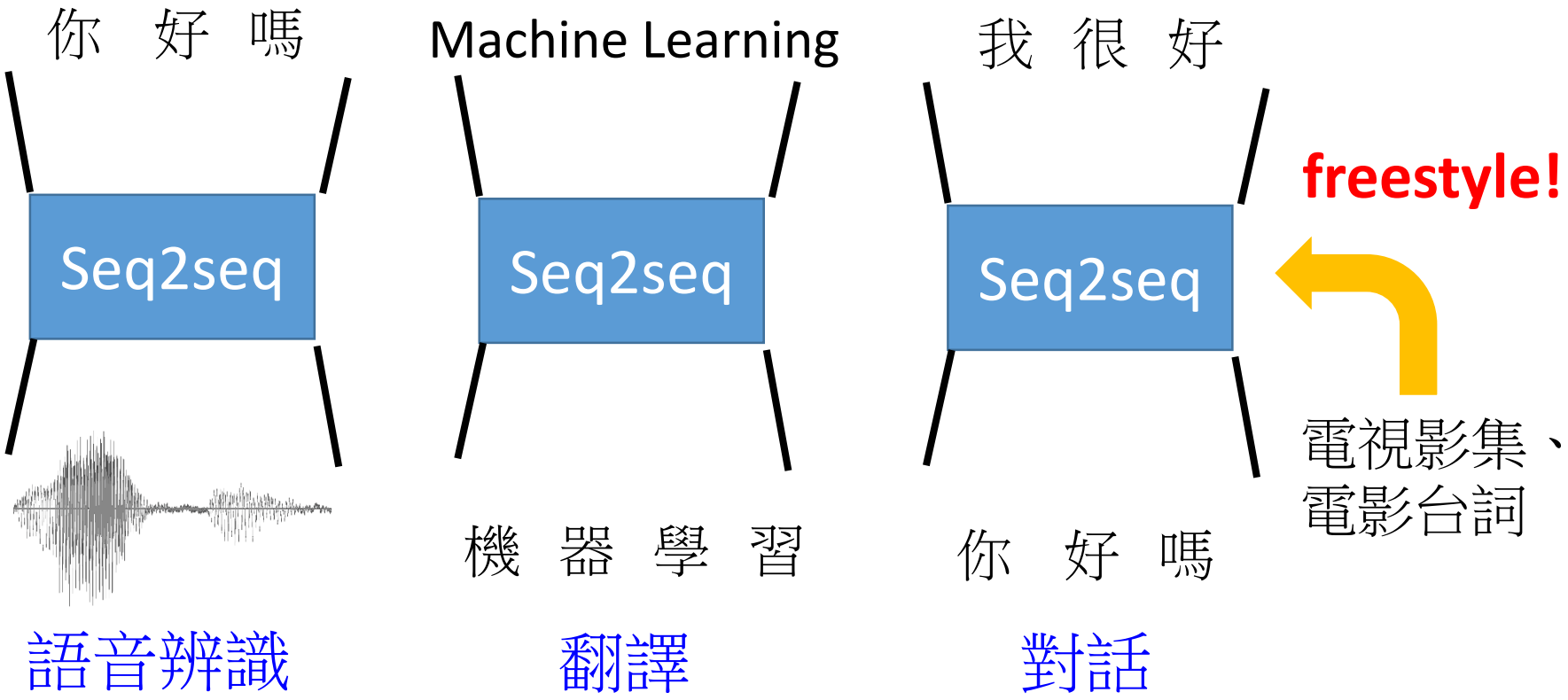
LSTM



GRU

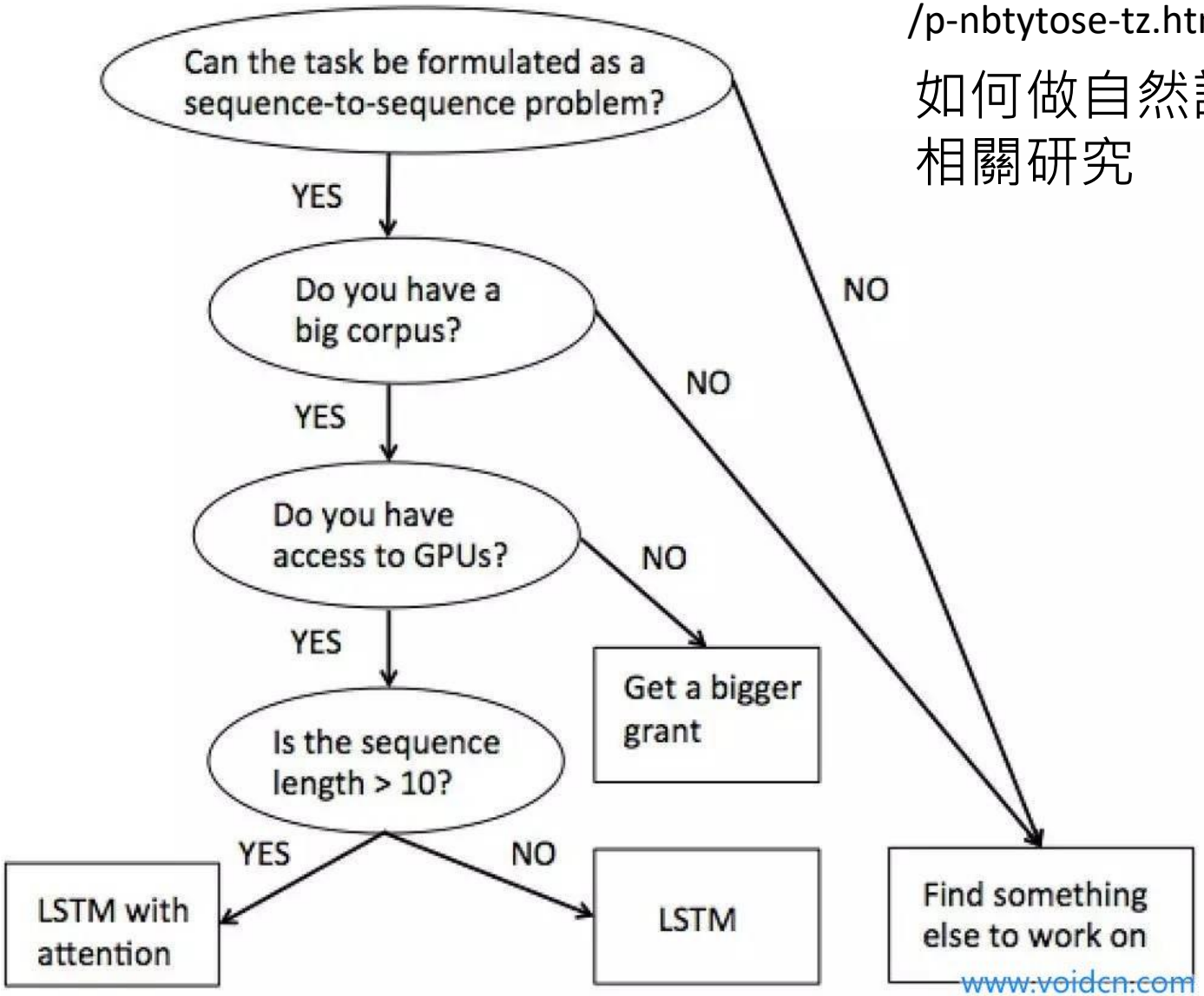
Sequence-to-sequence (Encoder-Decoder Architecture)

- Both input and output are both sequences ***with different lengths***.



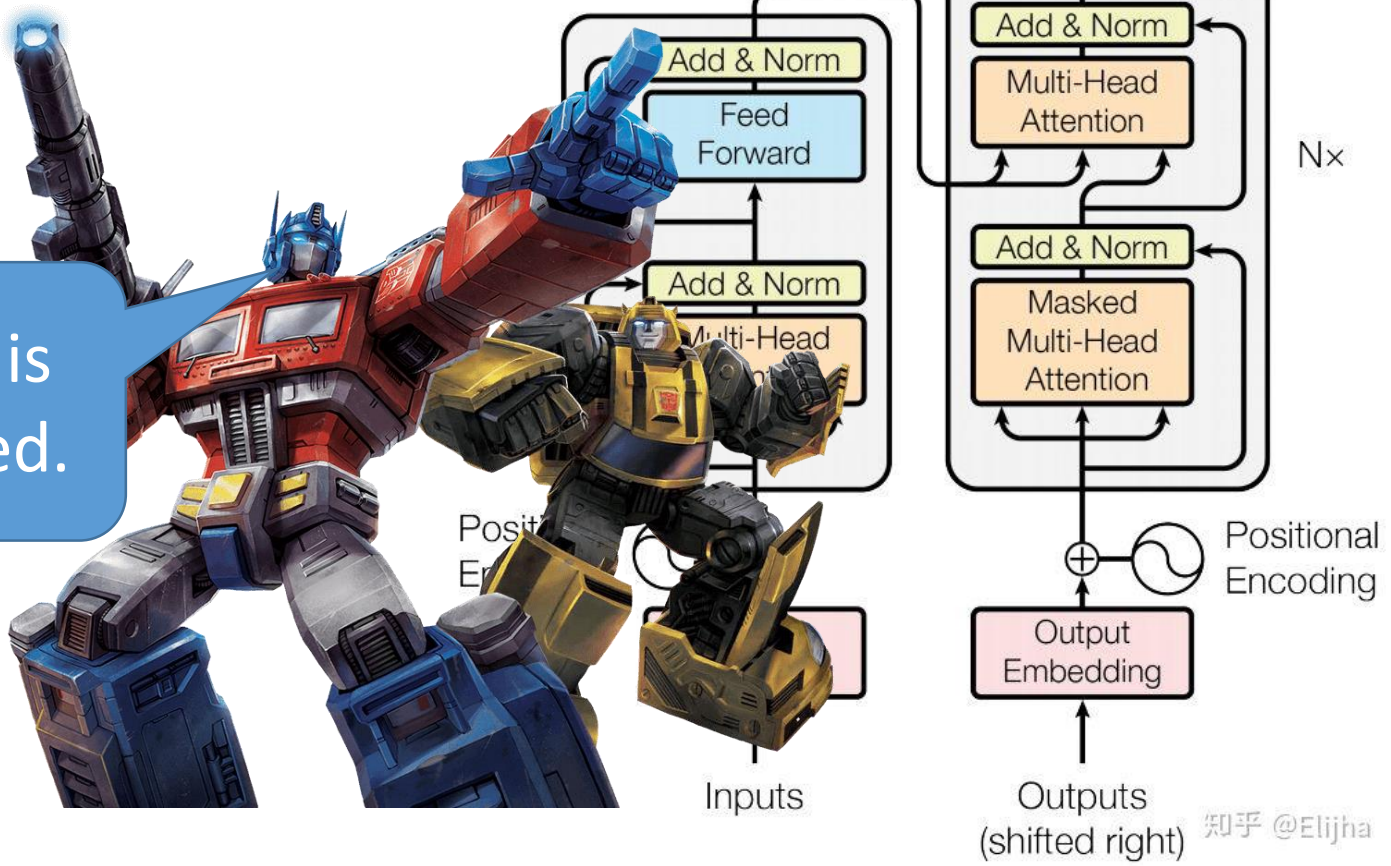
http://www.voidcn.com/article/p-nbtytose-tz.html

如何做自然語言處理相關研究



Sequence-to-sequence

- Transformer



機器學習好簡單 ……

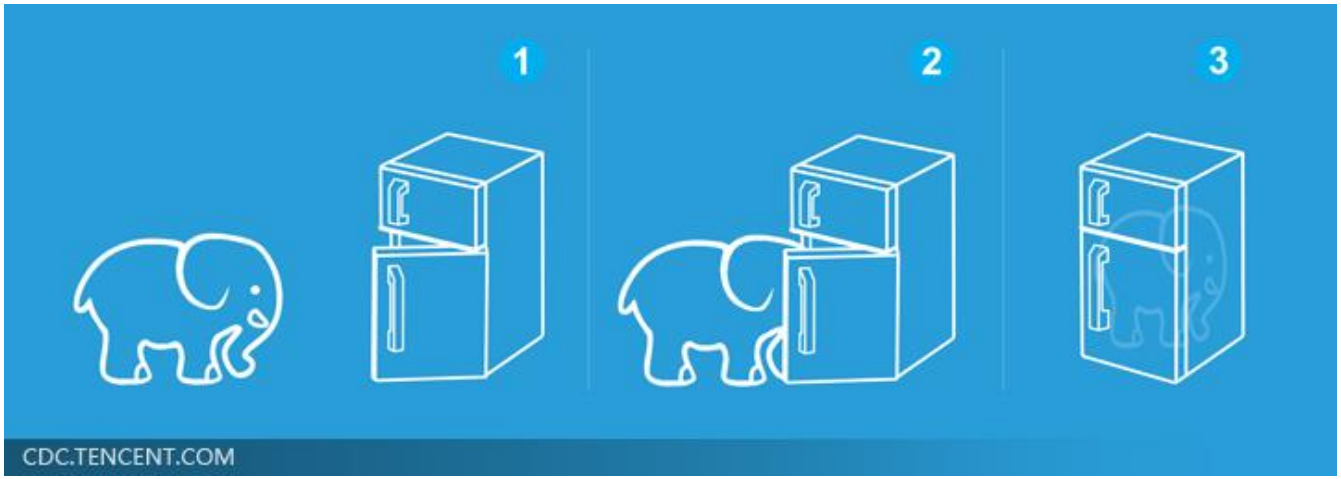
Step 0: What kind of function do you want to find?

Step 1: define a set of function

Step 2: goodness of function

Step 3: pick the best function

就好像把大象放進冰箱 ……



Semi-supervised (半督導)

For example, recognizing cats and dogs

Labelled data

cat

dog

Unlabeled data

(Images of cats and dogs)

Transfer Learning (遷移學習)

For example, recognizing cats and dogs

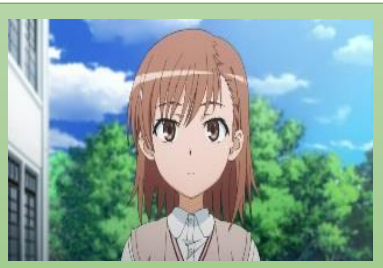
Labelled data

cat

dog

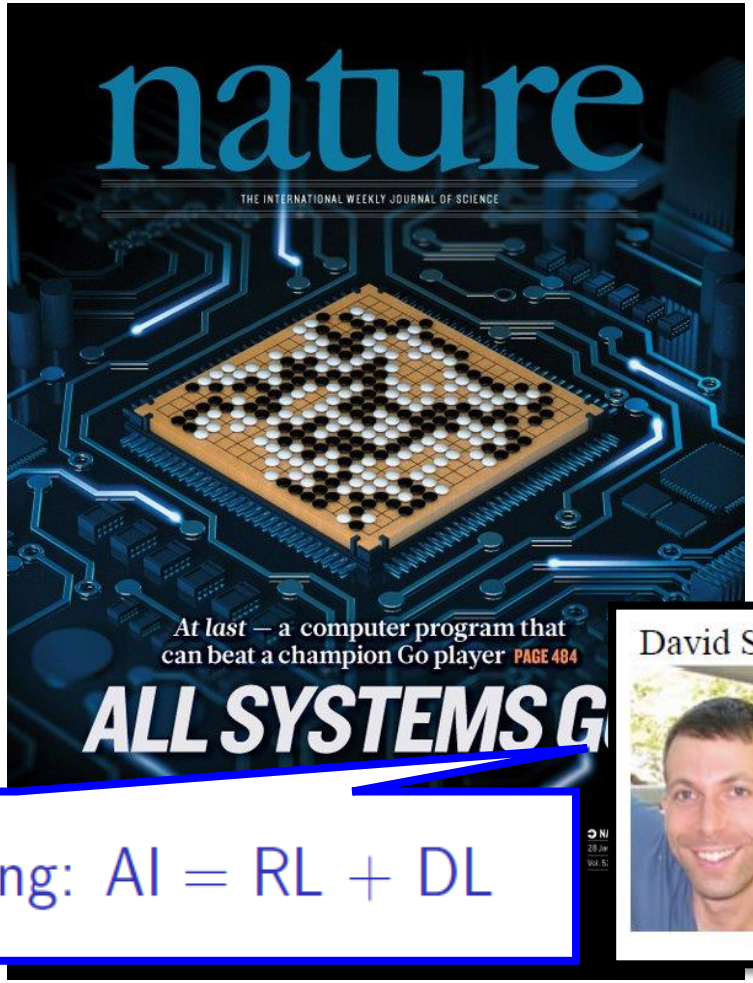
elephant

Haruhi



Data not related to the task considered
(can be either labeled or unlabeled)

Reinforcement Learning (增強式學習)

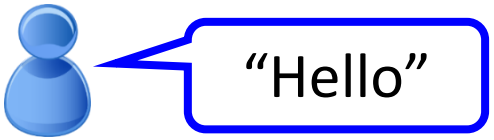


Deep Reinforcement Learning: AI = RL + DL

Supervised v.s. Reinforcement

- Supervised

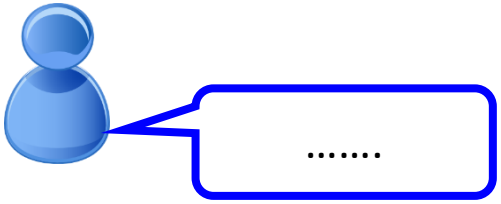
Learning from teacher

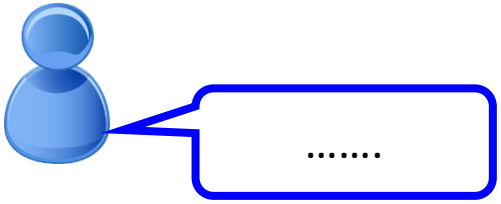


Say “Hi”

Say “Good bye”

- Reinforcement

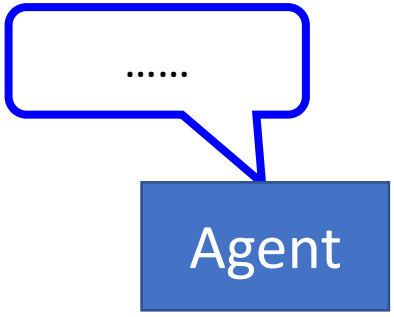




.....

Bad

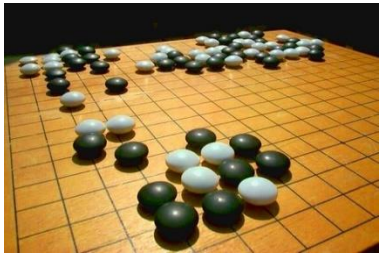
Learning from critics



Supervised v.s. Reinforcement

- Supervised:

Next move:
"5-5"



Next move:
"3-3"

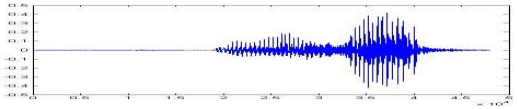
- Reinforcement Learning

First move → …… many moves …… → Win!

Alpha Go is supervised learning + reinforcement learning.

Unsupervised (非督導)

Training AI ***without paired data***



x

Speech Recognition

"How are you"

y

Supervised

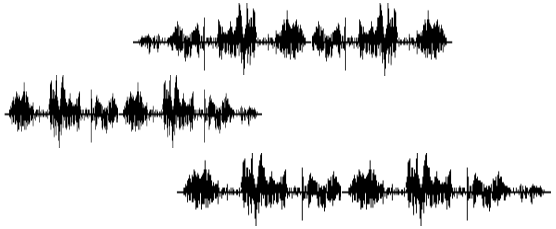
x_1:  y_1: Hello

x_2:  y_2: Good

x_3:  y_3: I am fine

Unsupervised

AI listening in the environment



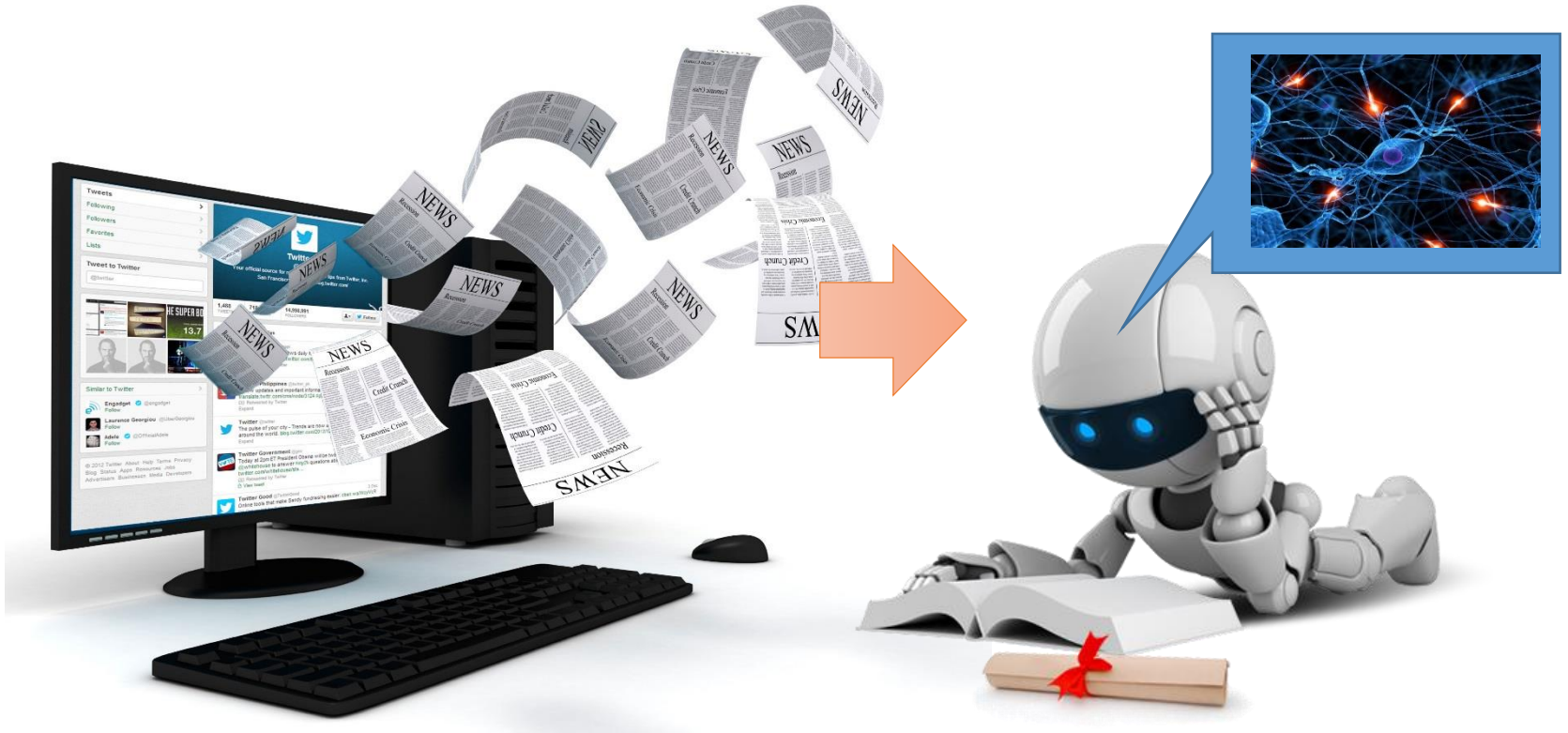
Audio x

Text y

AI reading documents on the Internet

Unsupervised (非督導)

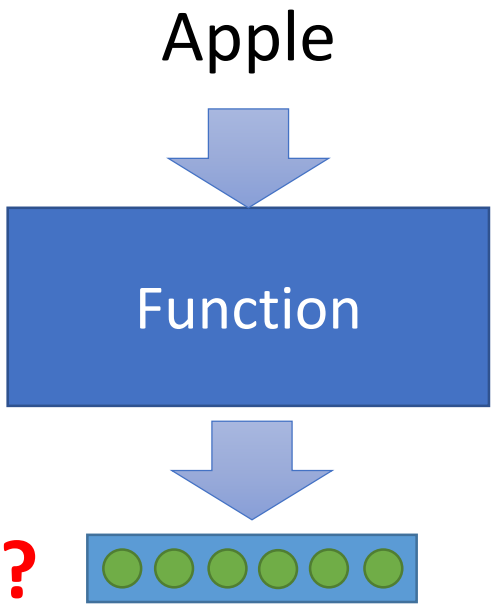
- Machine Reading: Machine learns the meaning of words from reading a lot of documents



http://top-breaking-news.com/

Unsupervised (非督導)

- Machine Reading: Machine learns the meaning of words from reading a lot of documents



Training data is a lot of text

https://garavato.files.wordpress.com/2011/11/stacksdocuments.jpg?w=490

Unsupervised (非督導)

- Machine Reading: Machine learns the meaning of words from reading a lot of documents
- ELMO/BERT

機器學習好簡單 ……

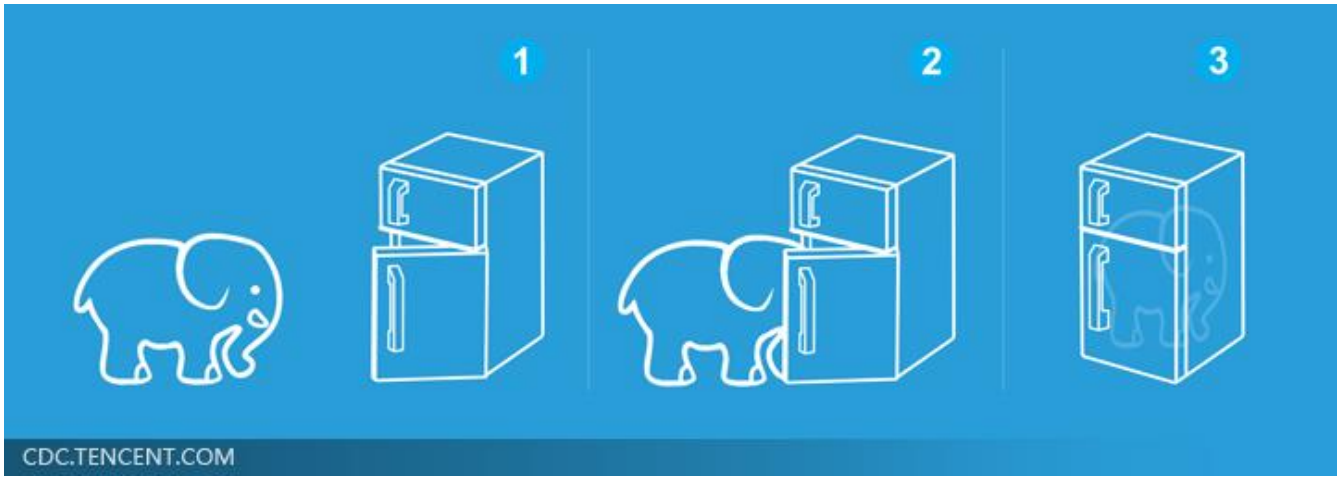
Step 0: What kind of function do you want to find?

Step 1: define a set of function

Step 2: goodness of function

Step 3: pick the best function

就好像把大象放進冰箱 ……



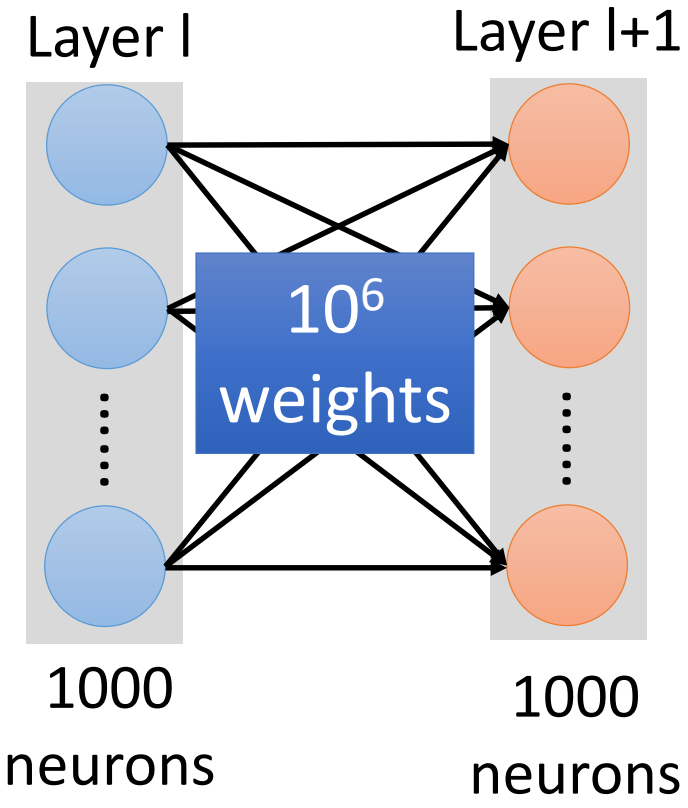
如何找出最好的 function ?

Enumerate all possible values

Network parameters $\theta = \{w_1, w_2, w_3, \cdots, b_1, b_2, b_3, \cdots\}$

Millions of parameters

Today a network can have more than 100M parameters.



Gradient Descent

機器學習好簡單 ……

Step 0: What kind of function do you want to find?

Regression, Classification, Generation ……

Step 1: define a set of function

Deep Learning
SVM
Decision Tree
……

Step 2: goodness of function

Supervised
Transfer
Reinforcement
……

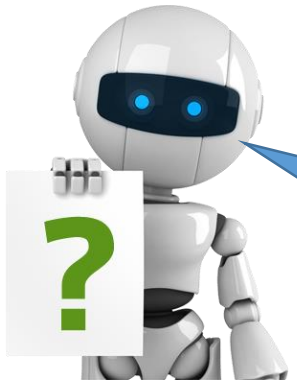
Step 3: pick the best function

Gradient Descent
……

機器學習的下一步

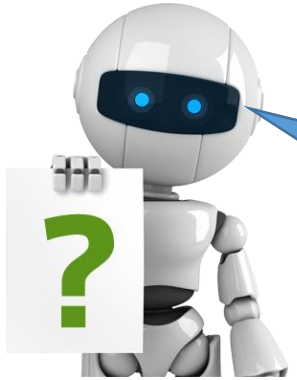
在真實的應用中還少了甚麼

機器能不能知道「我不知道」



這是貓咪

Animal Classifier

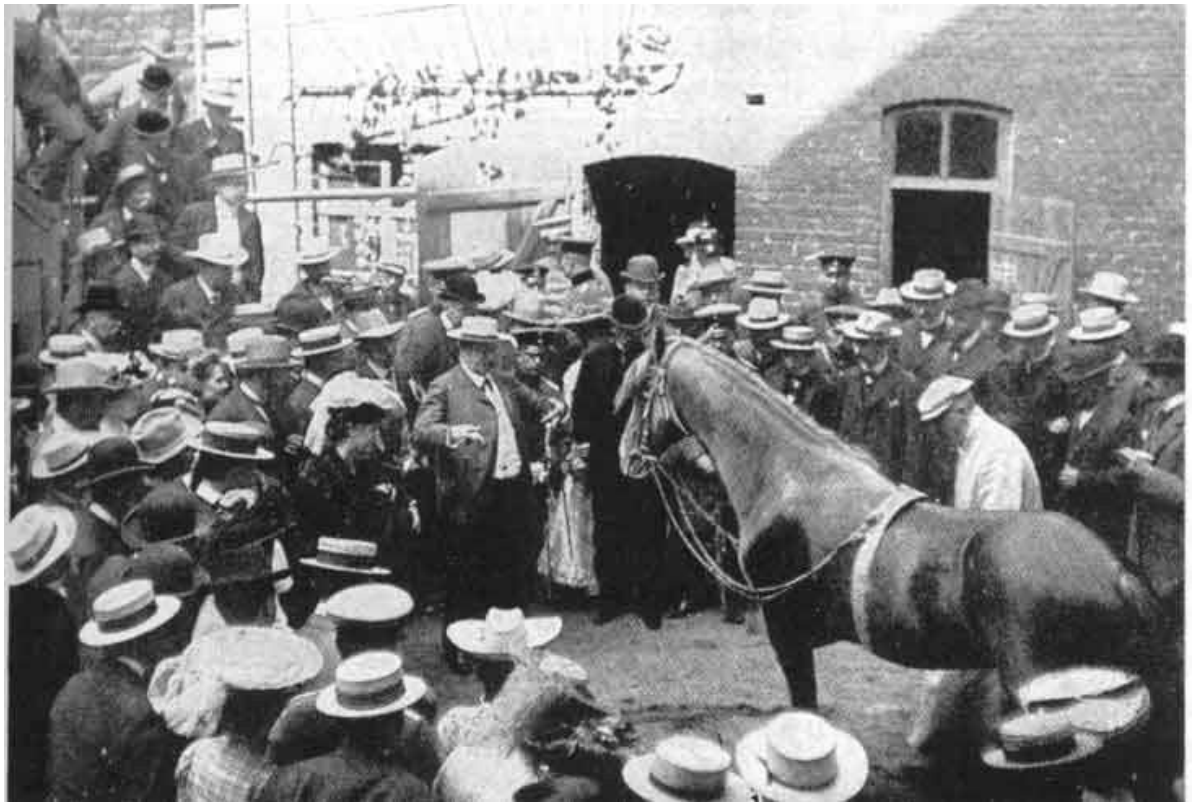


我不知道
這是甚麼

Anomaly Detection

說出為什麼「我知道」

- 神馬漢斯

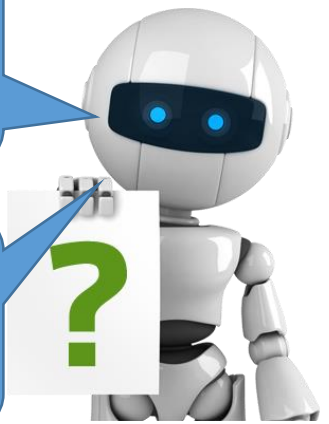


說出為什麼「我知道」

Explainable AI

球鞋

美洲獅

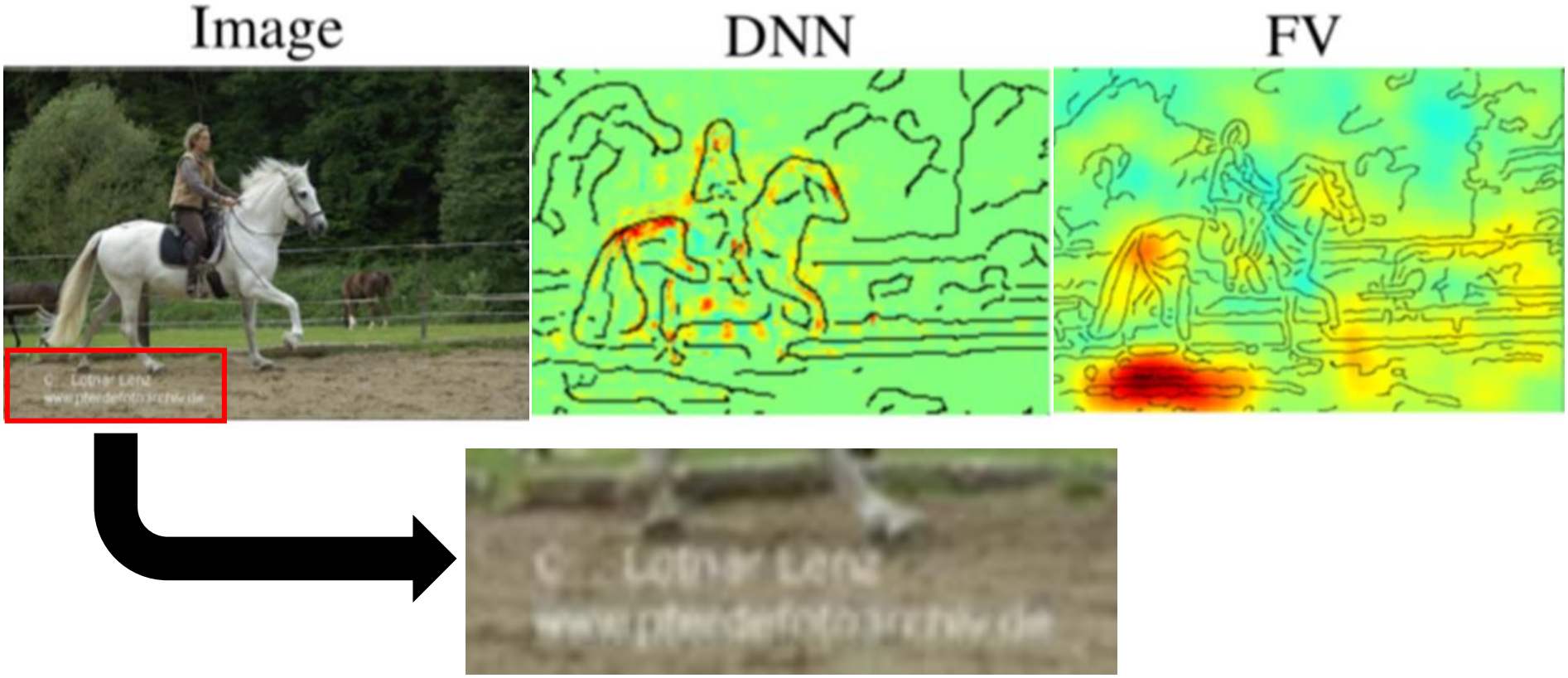


http://newsneakernews.wpengine.netdna-cdn.com/wp-content/uploads/2016/11/rihanna-puma-creeper-velvet-release-date-02.jpg

說出為什麼「我知道」

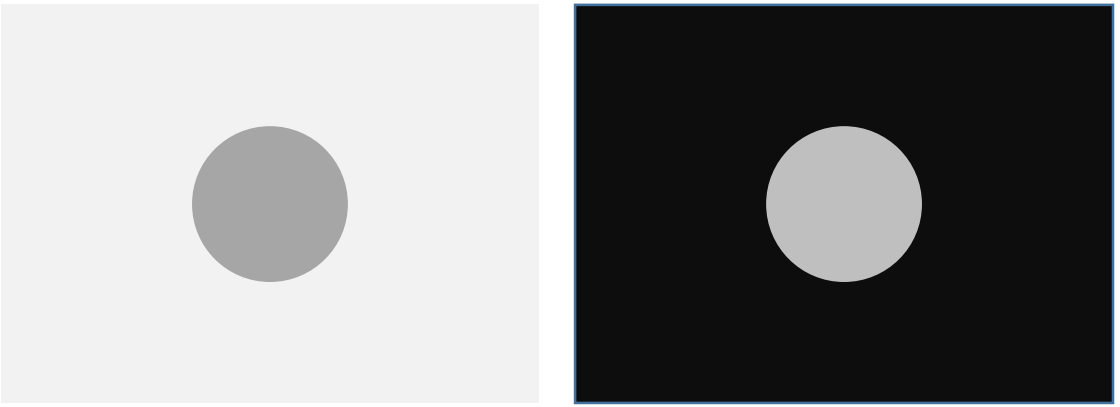
- 「馬」辨識器

This slide is from:
GCPR 2017 Tutorial — W. Samek & K.-R. Müller



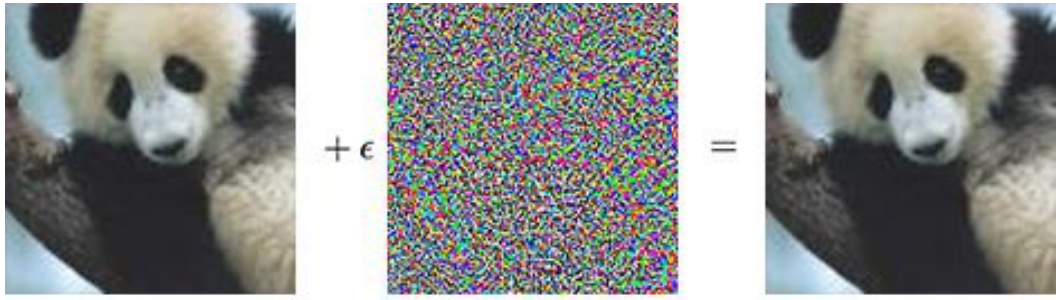
機器的錯覺？

- 人有錯覺



- 機器的錯覺？

  Adversarial Attack



- 如何防止 Adversarial Attack 呢？

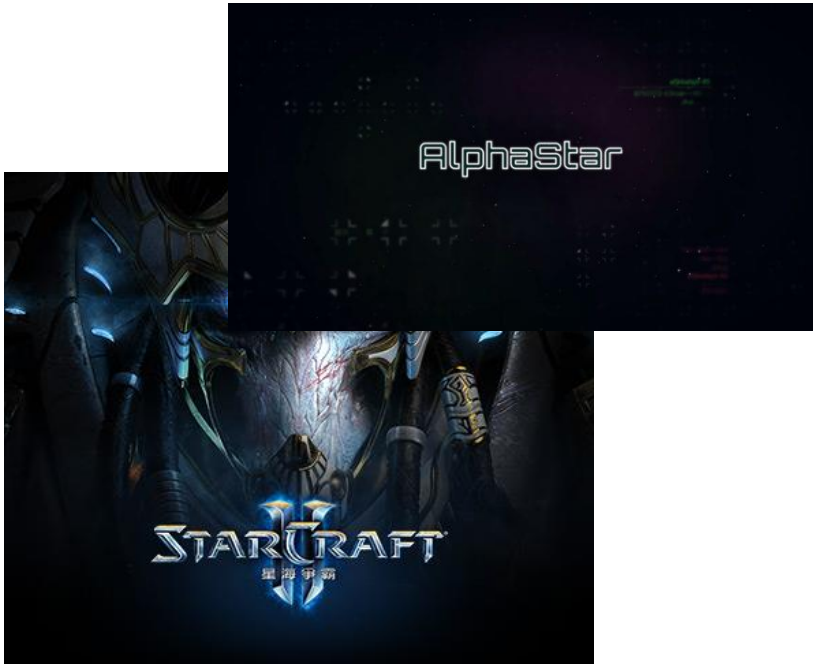
終身學習 (Life-long Learning)

- 人類一輩子都在學習新技能
  - 你可能上學期學了「線性代數」，這學期學了「機器學習」
  - 學習「線性代數」讓你「機器學習」學得更好

- 機器也能「終身學習」嗎？

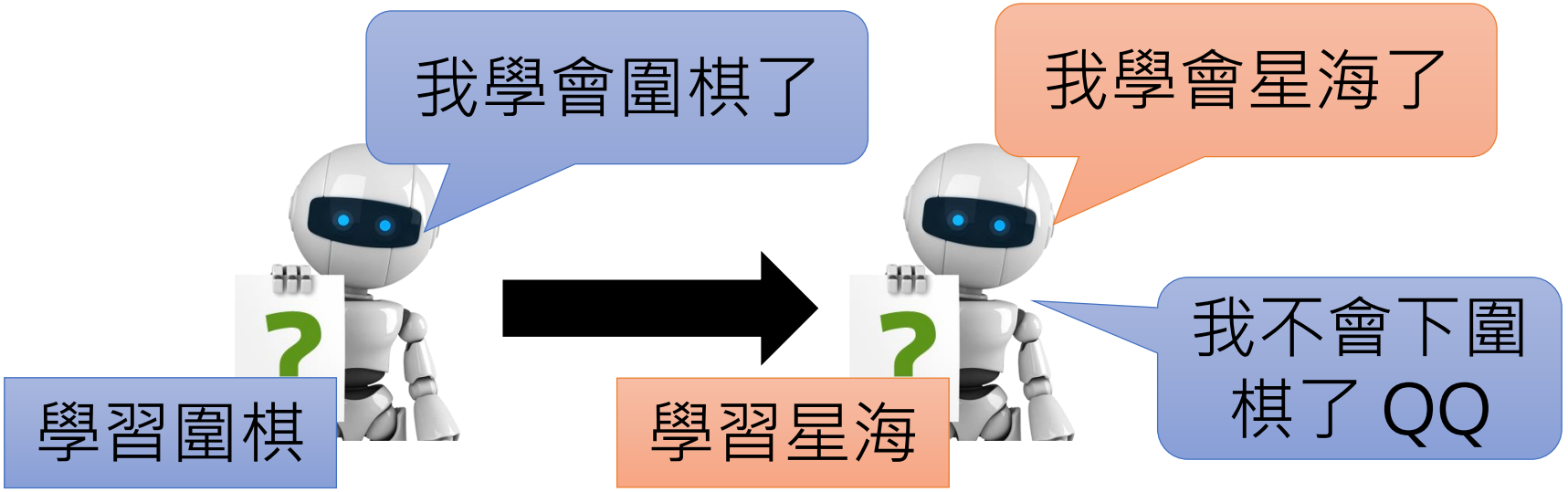
終身學習 (Life-long Learning)

- 今天一般我們只讓一個模型學習一個任務 .....



終身學習 (Life-long Learning)

- 今天一般我們只讓一個模型學習一個任務 .....
- 問題：(1) 模型的數量無限增長 (2) 之前學到的技能對之後的學習沒有幫助



Catastrophic Forgetting

學習如何學習

Meta-learning / Learn to learn

- Now we design the learning algorithm

program for learning

I can learn!

- Can machine learn the learning algorithm?

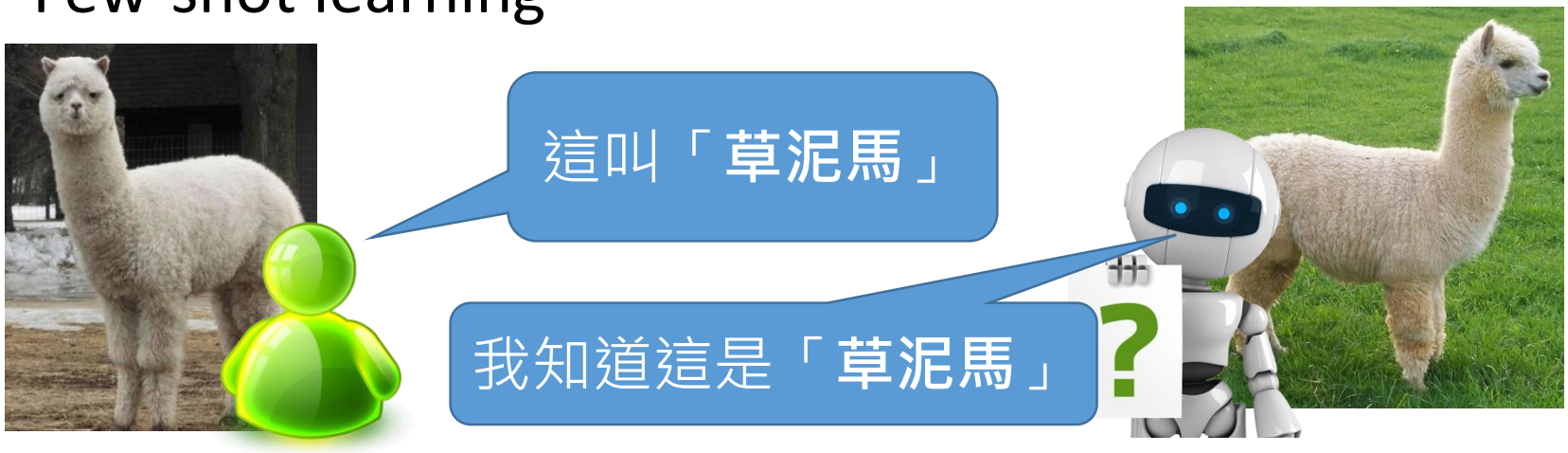
program designing program for learning

program for learning

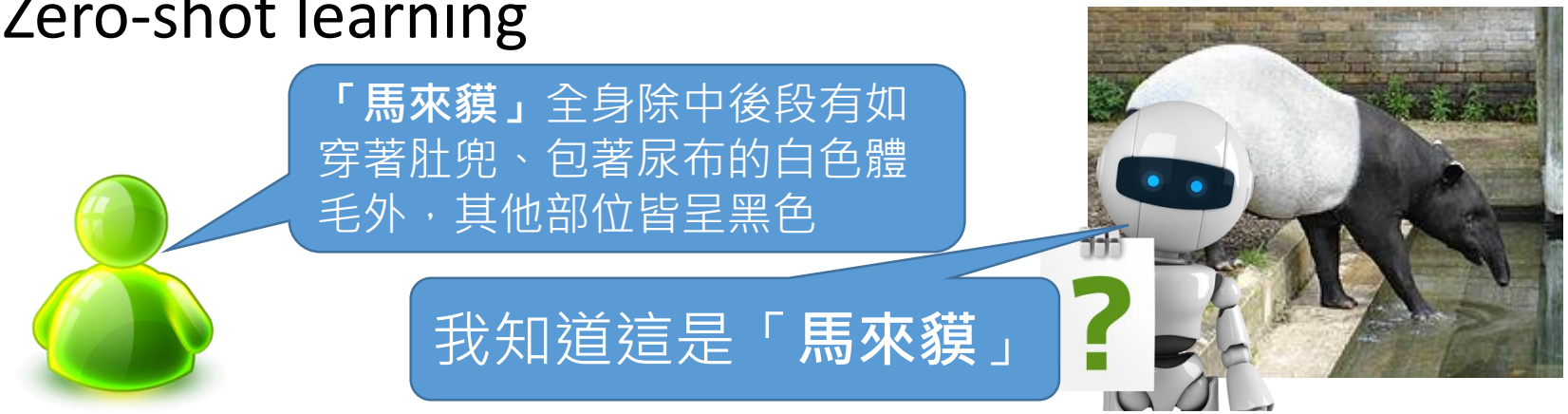
I can learn!

一定需要很多訓練資料嗎？

- Few-shot learning

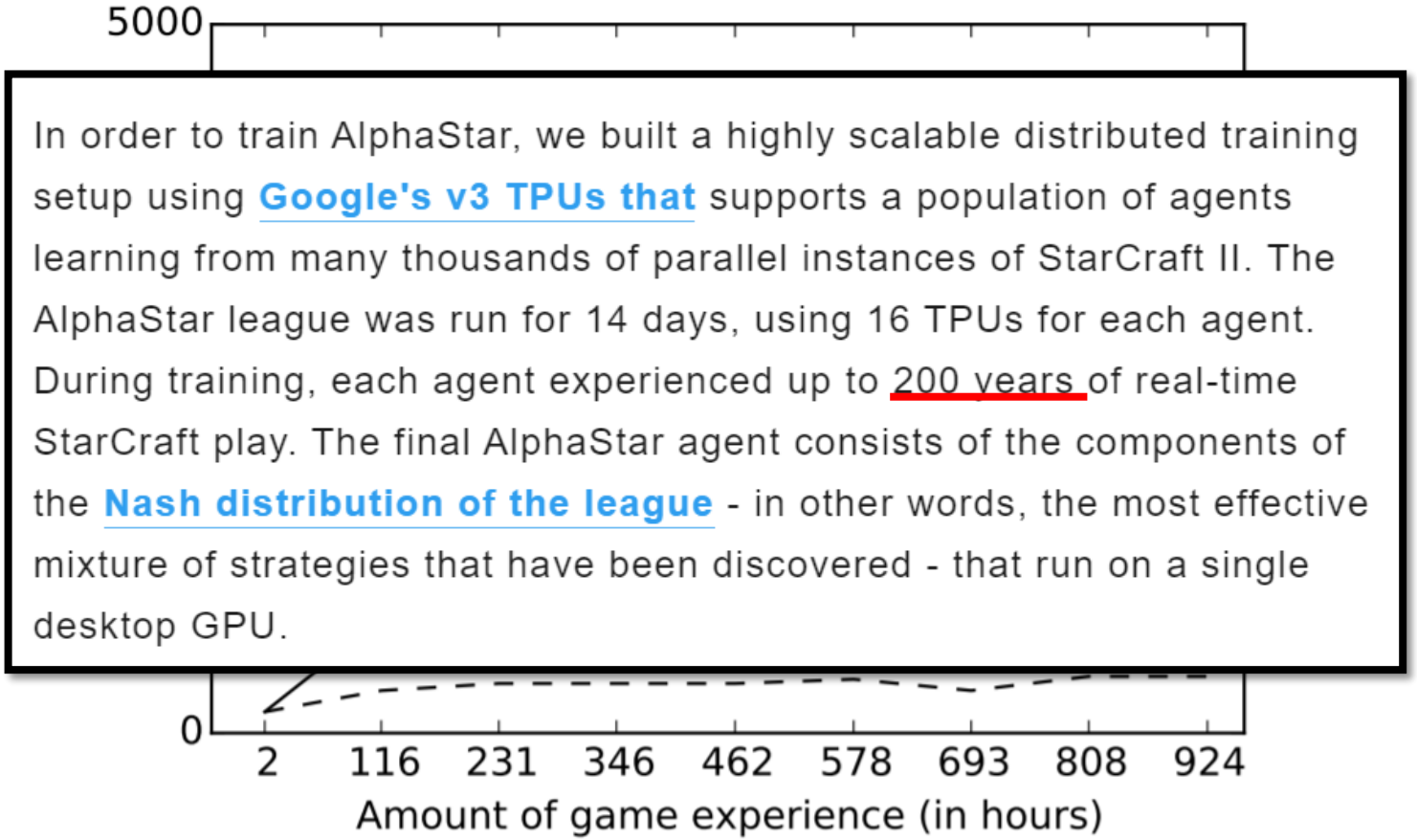


- Zero-shot learning



Reinforcement Learning (增強式學習)

天資不佳卻勤奮不懈？



http://web.stanford.edu/class/psych209/Readings/LakeEtAlBBS.pdf

Reinforcement Learning (增強式學習)

- Sparse reward

是什麼讓你可以在這裡聽課？

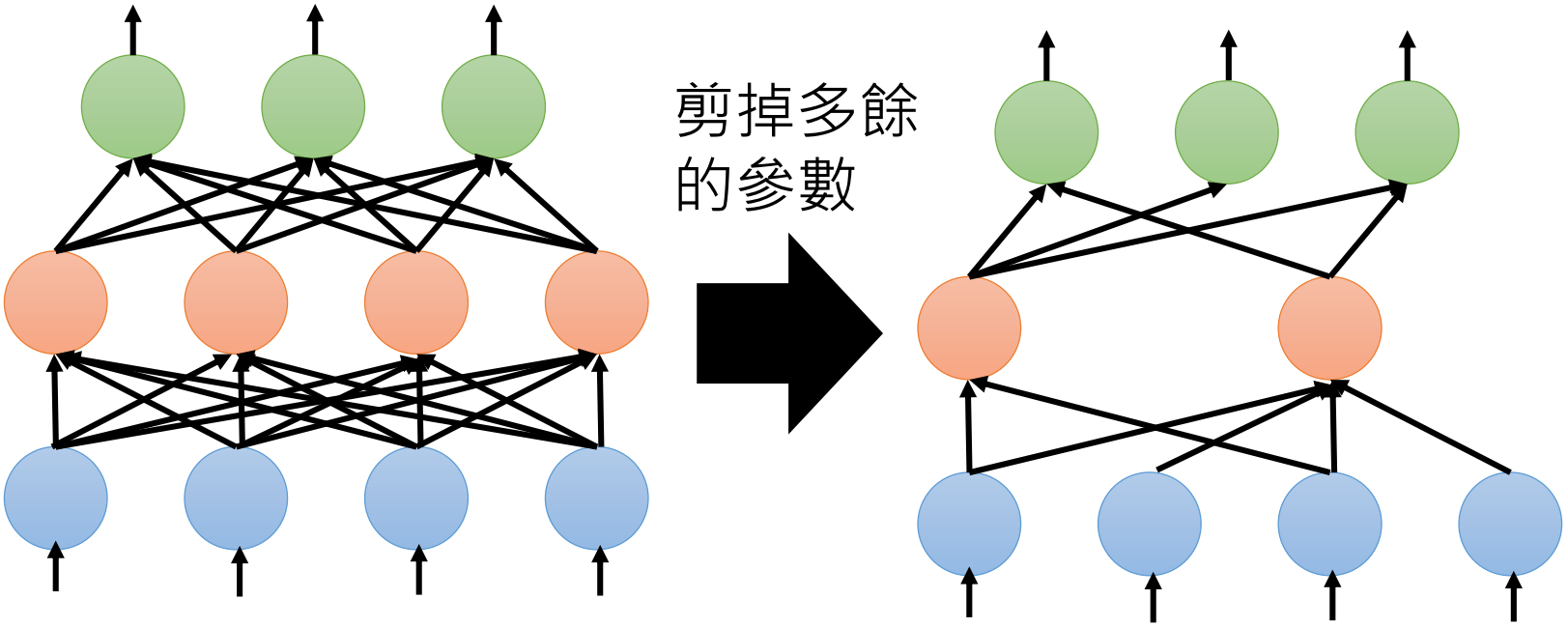
未來可以賺大錢? (Reward)

- 想像力
- 好奇心、求知慾
- 階段性目標

機器能不能也一樣？

神經網路壓縮 (Network Compression)

- 把大神經網路縮小



- 參數二元化
  - 所有的參數都變成 “+1” 和 “-1”

機器學習的謊言 ……

- Training data and testing data have the same distribution

Training data

Testing data

- This is a lie!

機器學習的謊言 ……

Training Data

Testing Data

99.5%

57.5%

E.g. “Unsupervised Domain Adaptation”

The results are from: http://proceedings.mlr.press/v37/ganin15.pdf

機器學習的下一步

- Anomaly Detection (機器能不能知道「我不知道」)
- Explainable AI (說出為什麼「我知道」)
- 防止 Adversarial Attack
- Life-long Learning (終身學習)
- Meta-learning / Learn to learn (學習如何學習)
- Few-shot / Zero-shot Learning (一定需要很多訓練資料嗎？)
- 增強式學習真的能用嗎？
- Network Compression (神經網路壓縮)
- 如果訓練資料和測試資料很不一樣 ……