

生成式 AI 與 ChatGPT 實戰應用

Dr. Steve Lai
Mathison Intelligence
2024/07/09 @ 東吳大學推廣部

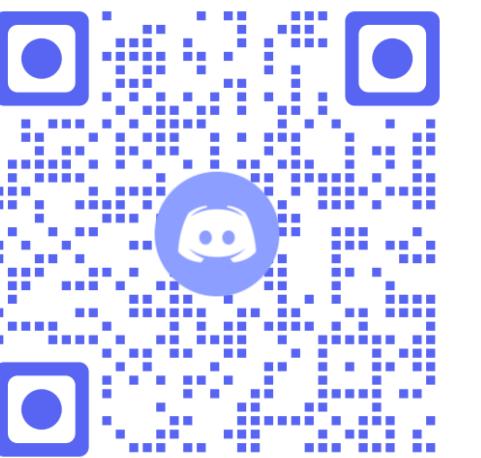
課程目標

- 瞭解何謂 AI 與 生成 AI
- 瞭解何謂機器學習與其技術的變化
- 學會用更好的方式使用 ChatGPT或其他大型語言模型助理
- 學會使用大型語言模型學習程式或其他技能
 - 提示工程的策略
 - 提示工程的原則
 - Agentic design pattern

Resume

- Steve Lai (賴昭榮)
 - 學經歷：
 - Founder and CEO at **Mathison Intelligence** (麥錫森智能)
 - ◆ plusForm — 線上課程品牌
 - 台灣大學資訊工程博士
 - 中央大學資訊工程碩士
- 加入 plusForm 討論群

Discord 語音討論群



Line openChat 討論群



人工智慧的歷史

1950年 - 圖靈測試 (Turing Test)

- 由英國數學家、邏輯學家艾倫·圖靈在1950年提出，在 "Computing Machinery and Intelligence"，在這篇論文中，提出了"機器能否思考"的問題，並設計了一種名為"模仿遊戲" (The Imitation Game) 的遊戲，後來這個遊戲被稱為"圖靈測試"。
- 由人和機器進行對話，當無法由對話中分辨誰是機器，那麼該機器即被認為有人工智能。

**"I propose to consider the question 'can
machines think'?"**

Alan Turing, 1950

人工智慧的歷史

1956年 - AI 的誕生

- 1956年，約翰·麥卡錫 (John McCarthy) 與其他幾位 AI 先驅者在達特茅斯學院舉辦了一個歷時兩個月的研討會。
- 約翰·麥卡錫首次提出了"人工智能" (Artificial Intelligence) 這個術語，並定義了其研究目標：創造出可以執行人類智能任務的機器。
- 達特茅斯會議對人工智能的發展產生了深遠影響，開始了AI的第一個黃金時代，並促進了許多重要的AI研究領域的開創，包括機器學習、自然語言處理和電腦視覺等。

“Artificial intelligence (AI) is the science and engineering of making intelligent machines, especially intelligent computer programs.

It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable”. ”

John McCarthy, 1956

人工智慧的歷史

1956年 - 2011年

- **黃金年代：1956 - 1974**。計算機可以解決代數應用題，證明幾何定理，學習和使用英語。當時大多數人幾乎無法相信機器能夠如此「智能」。其中 1957年，Perceptron提出。
- **第一次AI低谷：1974 - 1980**。AI研究者們對其課題的難度未能作出正確判斷：此前的過於樂觀使人們期望過高，當承諾無法兌現時，對AI的資助就縮減或取消了。
- **繁榮：1980 - 1987**。一類名為"專家系統"的AI程序開始為全世界的公司所採納，而「知識處理」成為了主流AI研究的焦點。其中包含了**聯結主義**（神經網路）的重生。**反向傳播算法**，一種神經網絡訓練方法被推廣
- **AI：1993 - 2011**，AI拆分為各自為戰的幾個子領域。

人工智慧的歷史

深度學習，大資料和人工智慧：2011至今

- 進入21世紀，得益於大資料和計算機技術的快速發展，許多先進的機器學習技術成功應用於經濟社會中的許多問題。
- 2006, Geoffrey Hinton 發表了一篇展示如何訓練深度神經網路的論文，用以辨別手寫數字（MNIST），準確為當時最好的 98%以上。
- 深度學習以神經網路為基礎，引領了人工智慧的新浪潮。

Artificial intelligence is the ability for computers to imitate cognitive human functions such as learning and problem-solving.

Through AI, a computer system uses math and logic to simulate the reasoning that people use to learn from new information and make decisions.

MIT Professional Education

人工智慧 (AI)

- 人工智能 (Artificial Intelligence, 簡稱 AI) 是一個跨領域的科學，它的目標是讓機器能夠執行通常需要人類智慧的任務。這些任務包括學習、推理、問題解決、感知、語言理解和生成等。AI 包括但不限於以下幾個主要領域：
 - 機器學習 (Machine Learning, ML)：AI 的一個子領域，透過從資料中學習模式和規則。常見的機器學習技術包括監督學習、非監督學習和強化學習。
 - 深度學習 (Deep Learning, DL)：機器學習的一個子集，利用多層神經網路來模仿人腦的結構和功能。深度學習在影像辨識、聲音辨識和自然語言處理有很好的成果。
 - 自然語言處理 (Natural Language Processing, NLP)：自然語言處理是研究如何使電腦能夠理解、解釋和生成人類語言的技術。大型語言模型的成功即為其中的成果。
 - 電腦視覺 (Computer Vision)：使電腦能夠解讀和理解影像訊息，如圖片和影片的內容。

生成式AI（Generative AI）

- 生成式AI是一種人工智慧技術，能夠創建新的、類似於訓練資料的內容。這些模型使用大量的資料進行訓練，學習資料中的統計特徵，然後根據這些特徵生成新的資料。生成式AI廣泛應用於各種創意領域，如圖像生成、音樂創作、文本生成等。
- 文字生成
 - ChatGPT、Gemini、Llama、BERT
- 圖片生成
 - Midjourney、Dall-E

大型語言模型

- 大型語言模型（Large Language Models, LLMs）為生成式AI的一種主要的應用。利用大量的文本進行預訓練，進而理解語法語意，進而讀寫語言。可用於文本生成、翻譯、問答系統等。
- 可透過微調（Fine-tuning）、檢索增強生成（RAG）等方式改善回答品質
 - 微調：透過給予一定數量問題與答案的集合，改變LLMs的理解
 - 檢索增強生成（RAG）：針對提供資料產生答案

AI 與機器學習

Artificial
Intelligence

Machine
Learning

Deep
Learning

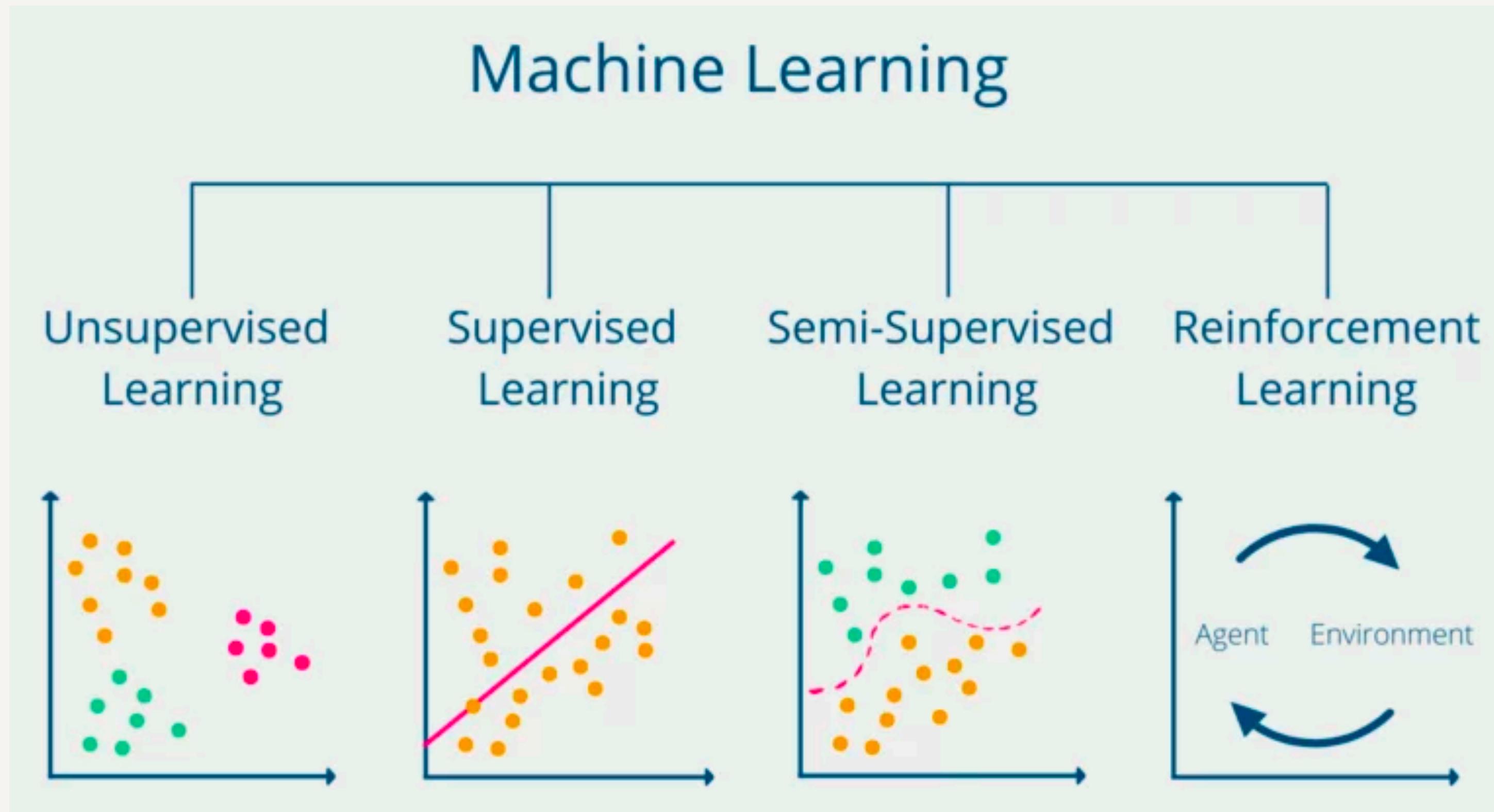
"Machine learning is the field of study that gives computers the ability to learn without being explicitly programmed."

Arthur Samuel, 1959

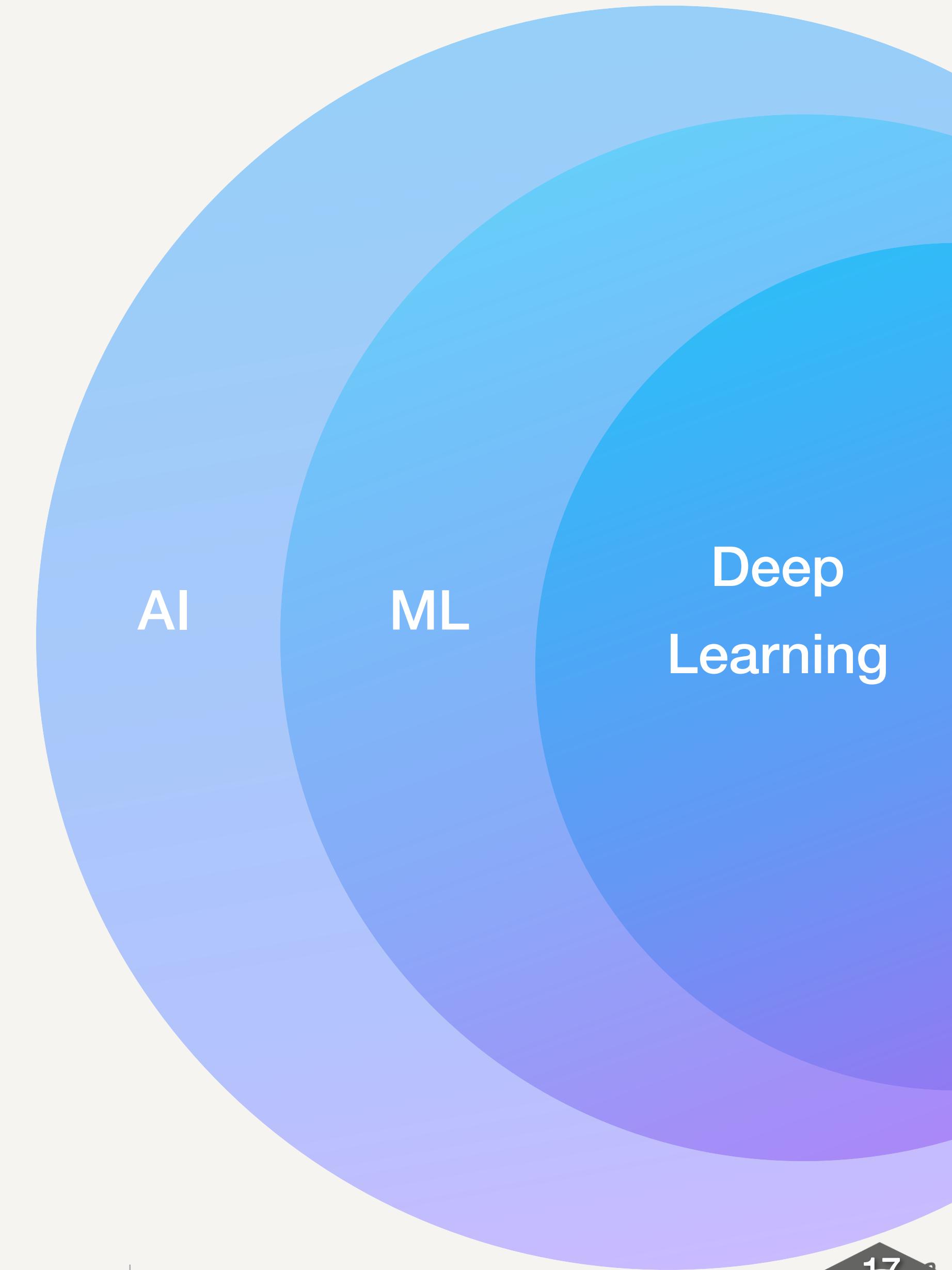
From Data to AI



AI 與機器學習



source: <https://databsecamp.de/en/ml/reinforcement-learnings>



機器學習的分類

- 機器學習技術包括監督學習、非監督學習、半監督式學習和強化學習。
- 監督式學習 (Supervised Learning)
 - 使用帶有正確答案標籤的資料來訓練模型，使其能夠預測新資料的結果。
- 非監督式學習 (Unsupervised Learning)
 - 利用沒有標籤的資料，讓模型自動尋找資料中的模式和結構，如叢集和降維。
- 半監督式學習 (Semi-Supervised Learning)
 - 結合少量帶標籤的資料和大量無標籤的資料來訓練模型，以提高學習效率和準確性。
- 強化學習 (Reinforcement Learning)
 - 通過讓智能體在環境中採取行動並根據獲得的獎勵或懲罰來學習最佳策略。

監督式學習 (Supervised Learning)

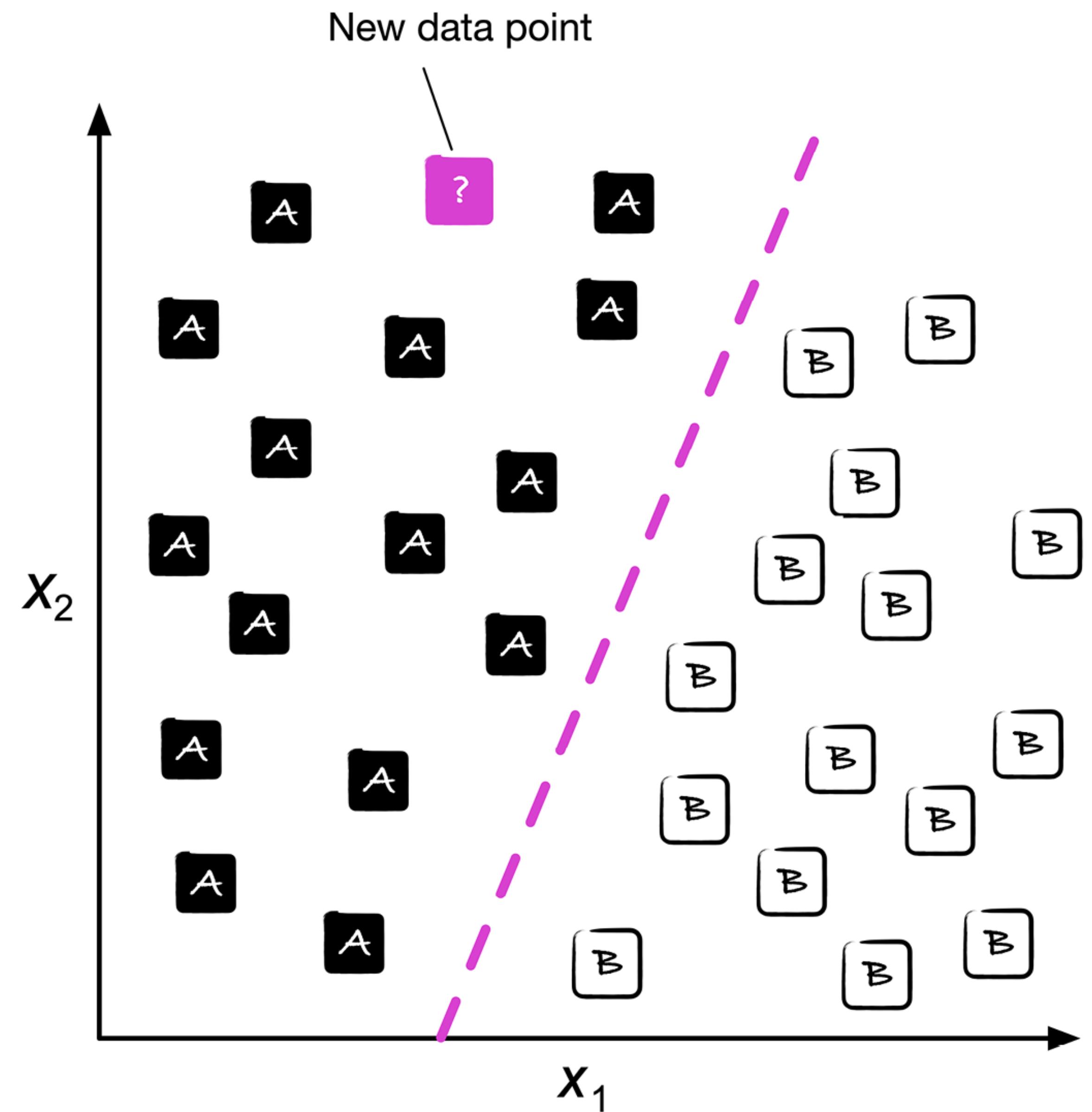
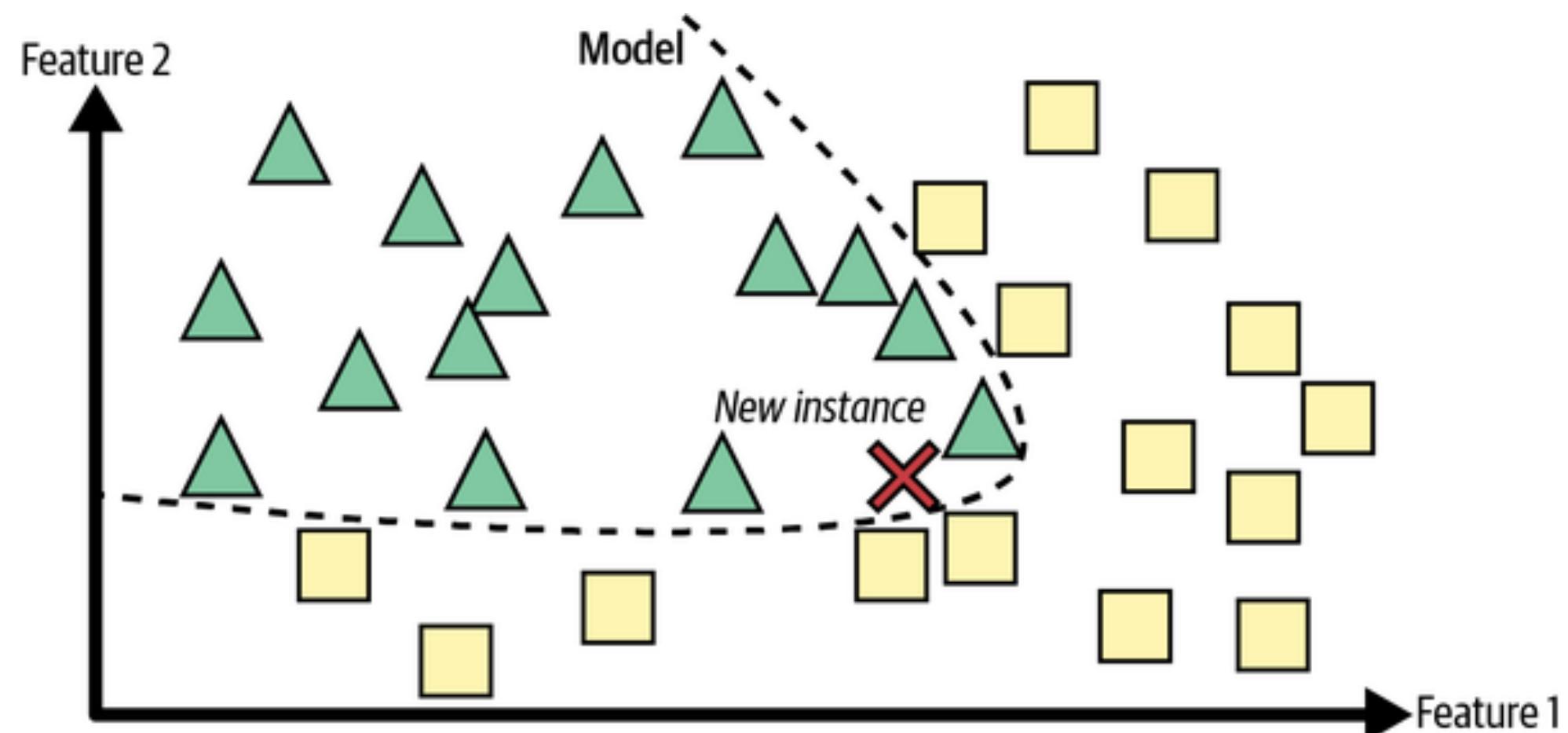
- 模型從標記過的訓練資料（即每筆資料都有明確的答案或標籤）中學習。透過這種方式，模型進行訓練，以便能夠基於輸入特徵預測出對應的輸出。
 - 標籤資料：建立一個垃圾郵件分類器，需要一組郵件，每封郵件都有"垃圾郵件"或"非垃圾郵件"的標記。
 - 特徵（屬性）：垃圾郵件分類器中，特徵可能包括郵件的內容、發送者的mail、信件的長度、標題等。
 - 模型訓練：在訓練過程中，演算法會嘗試找出輸入特徵和輸出標籤之間的關係。
 - 預測：一旦模型訓練完成，它就可以接收新的、未標記的輸入並預測出對應的輸出。垃圾郵件分類器可以接收一封新郵件並預測其是否為垃圾郵件。
- 監督式學習的兩個主要類型是分類（預測的輸出是離散的，如「垃圾郵件」或「非垃圾郵件」）和回歸（預測的輸出是連續的，如一個人的收入或房價）。

Input (X)	Output (Y)	Application
email	spam? (0/1)	spam filtering
audio	text transcripts	speech recognition
English	Spanish	machine translation
ad, user info	click? (0/1)	online advertising
image, radar info	position of other cars	self-driving car
image of phone	defect? (0/1)	visual inspection

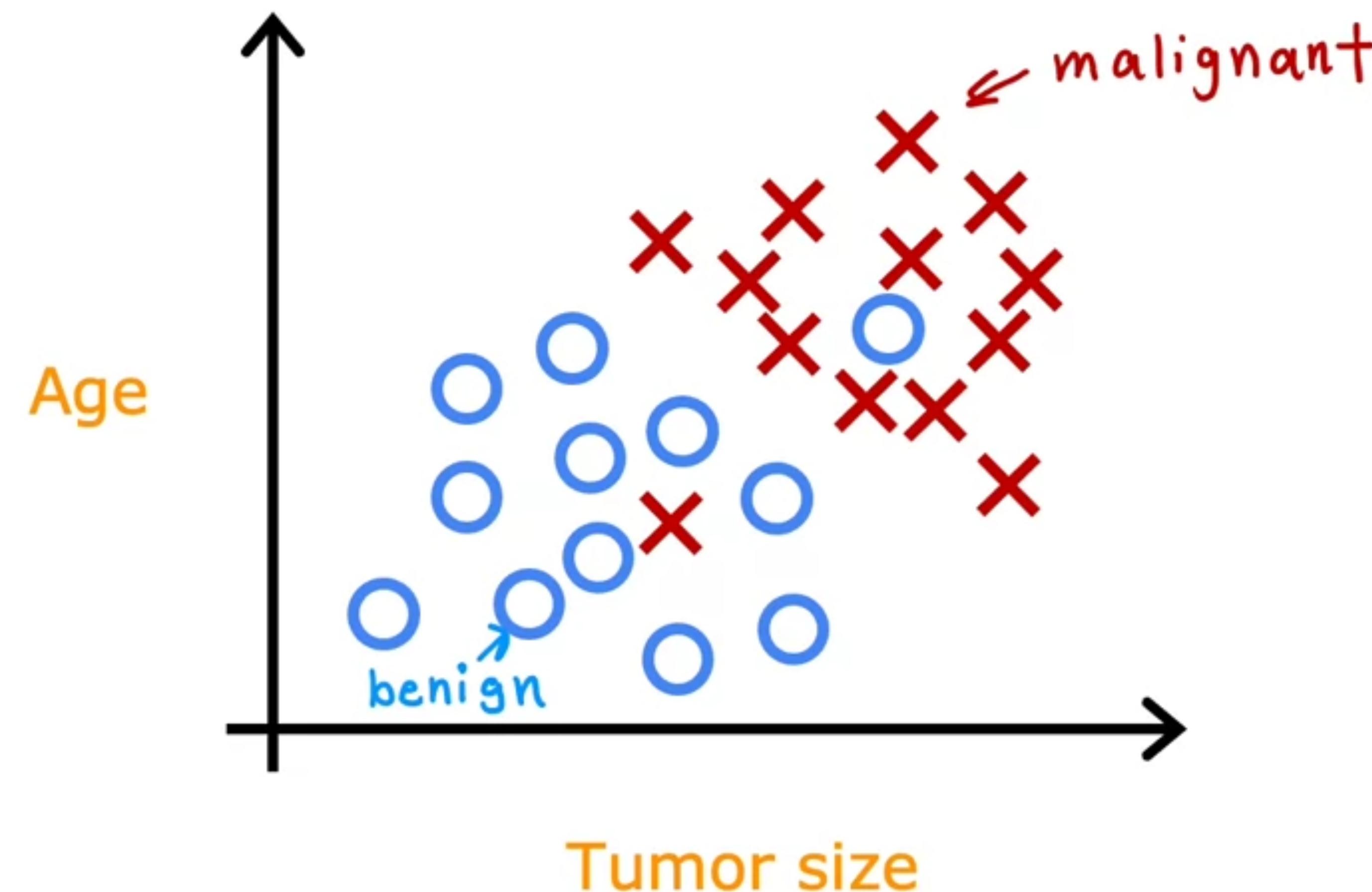
Classification

Predicting Class Labels

- Binary classification



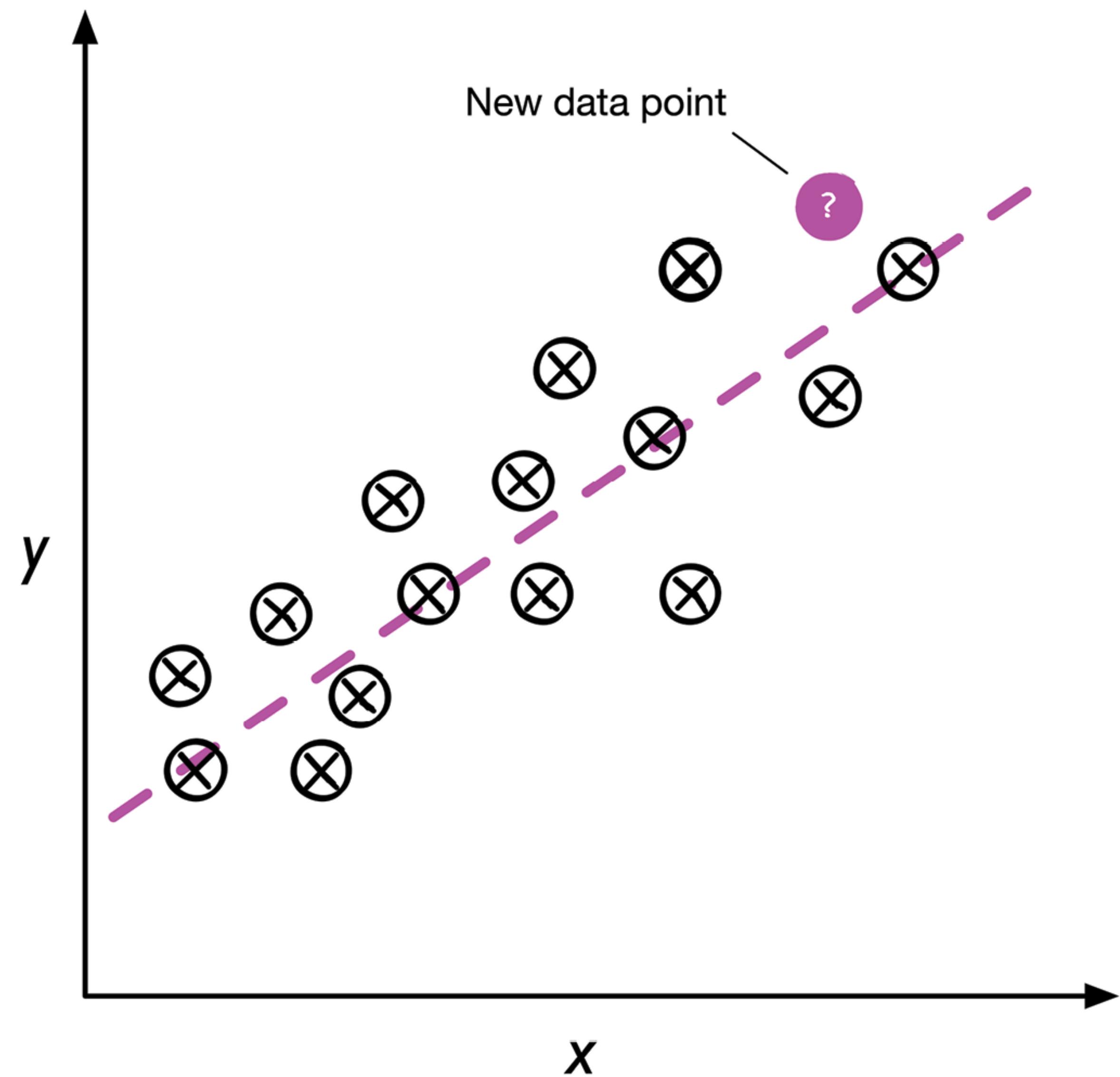
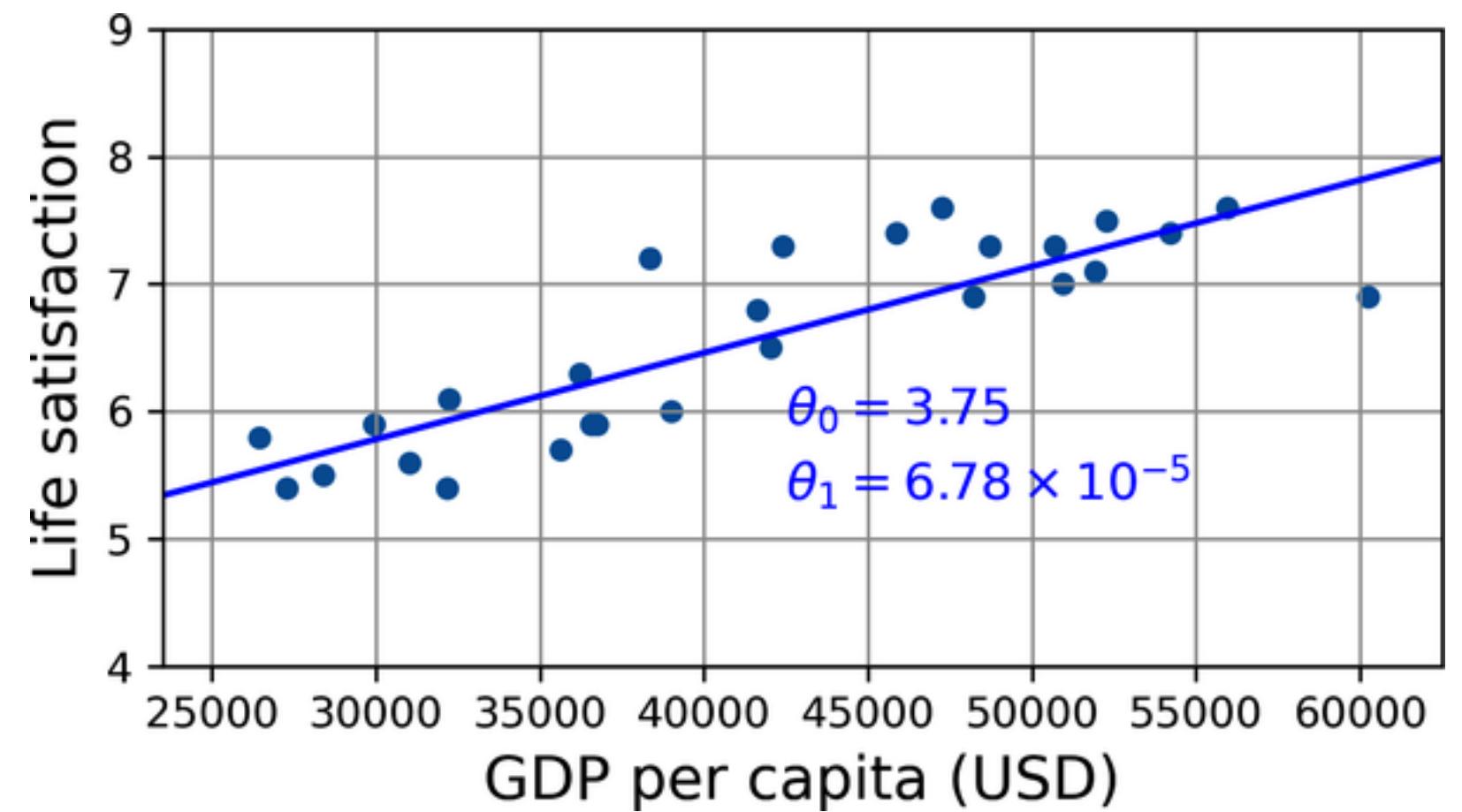
Two or more inputs



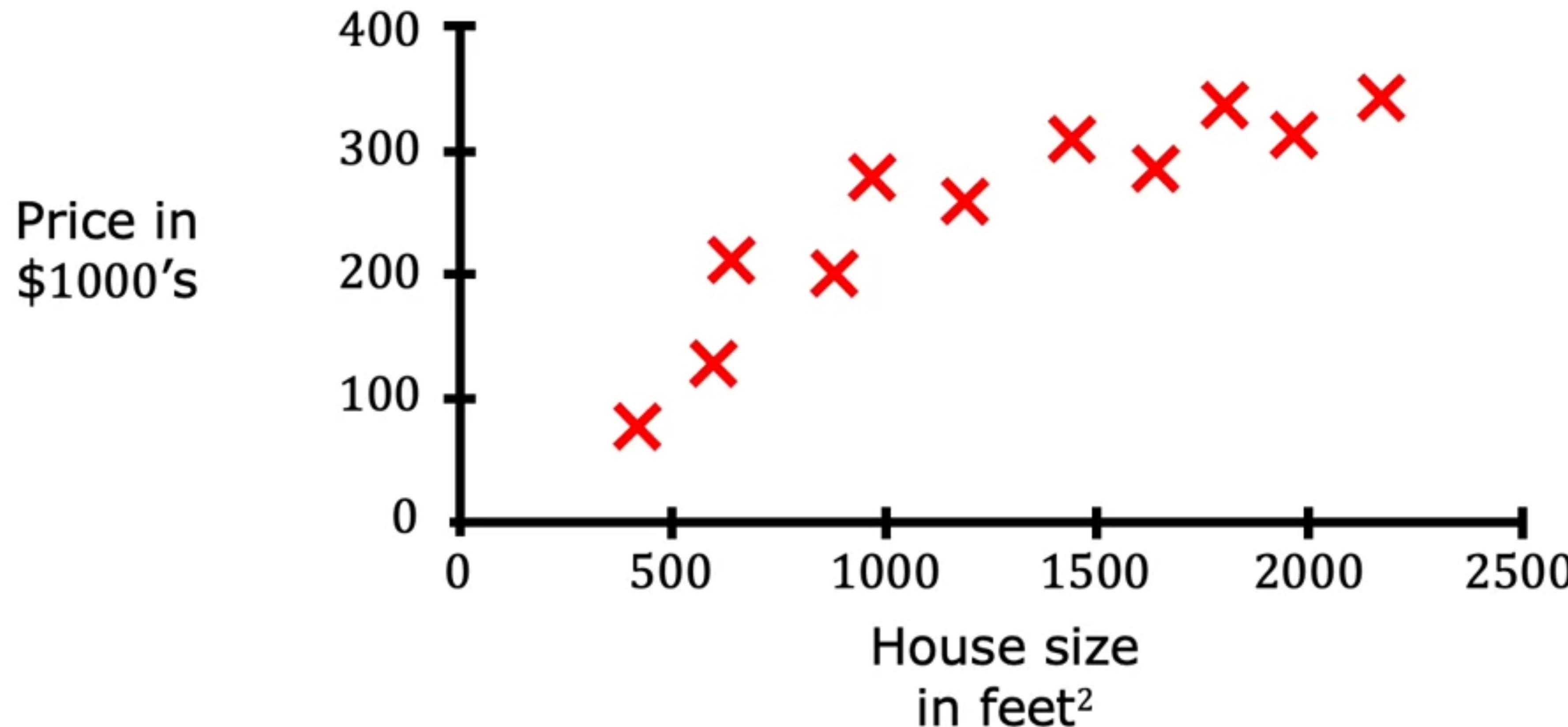
Regression

Predicting Continuous Outcomes

- Linear regression



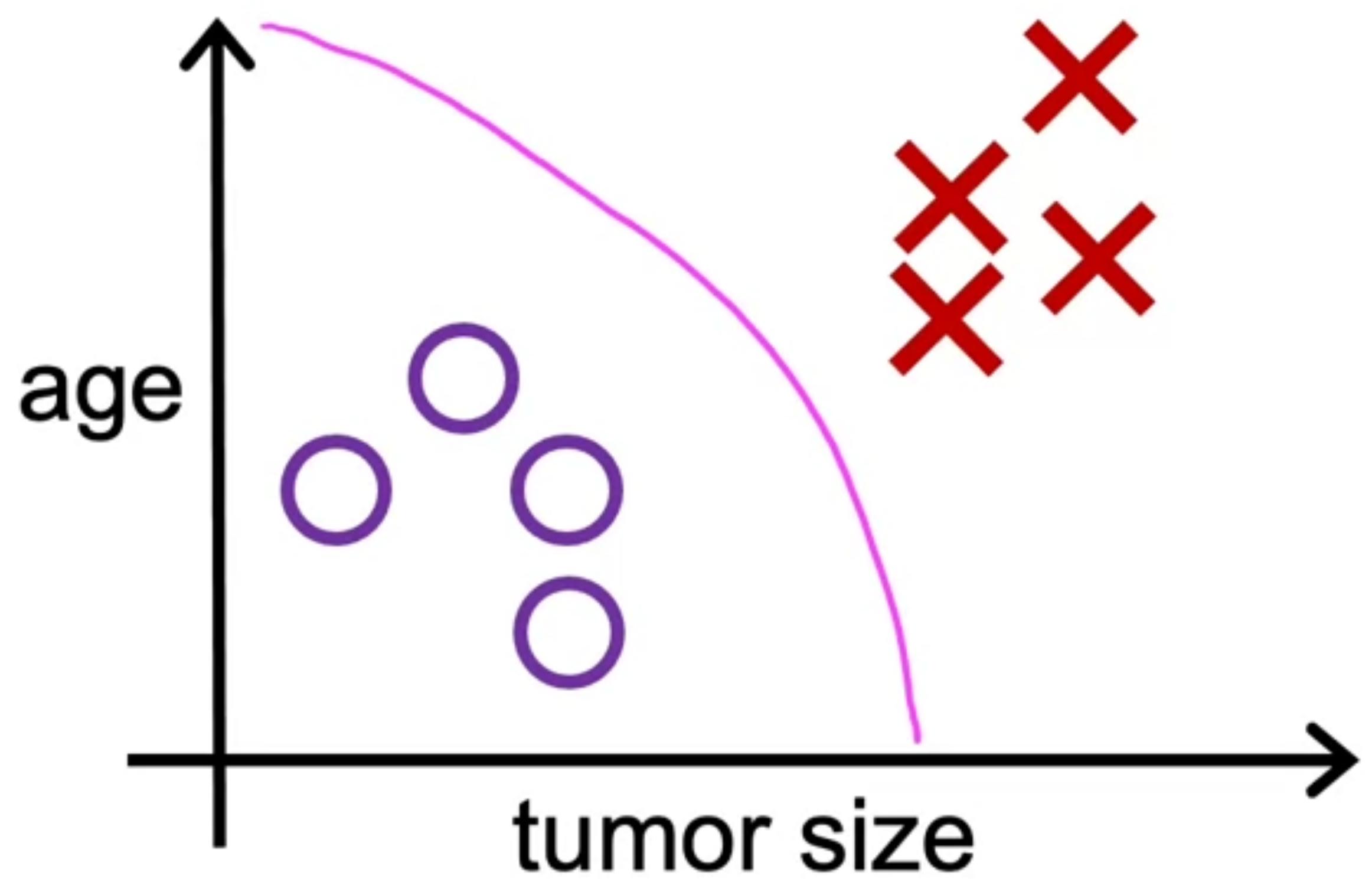
Regression: Housing price prediction



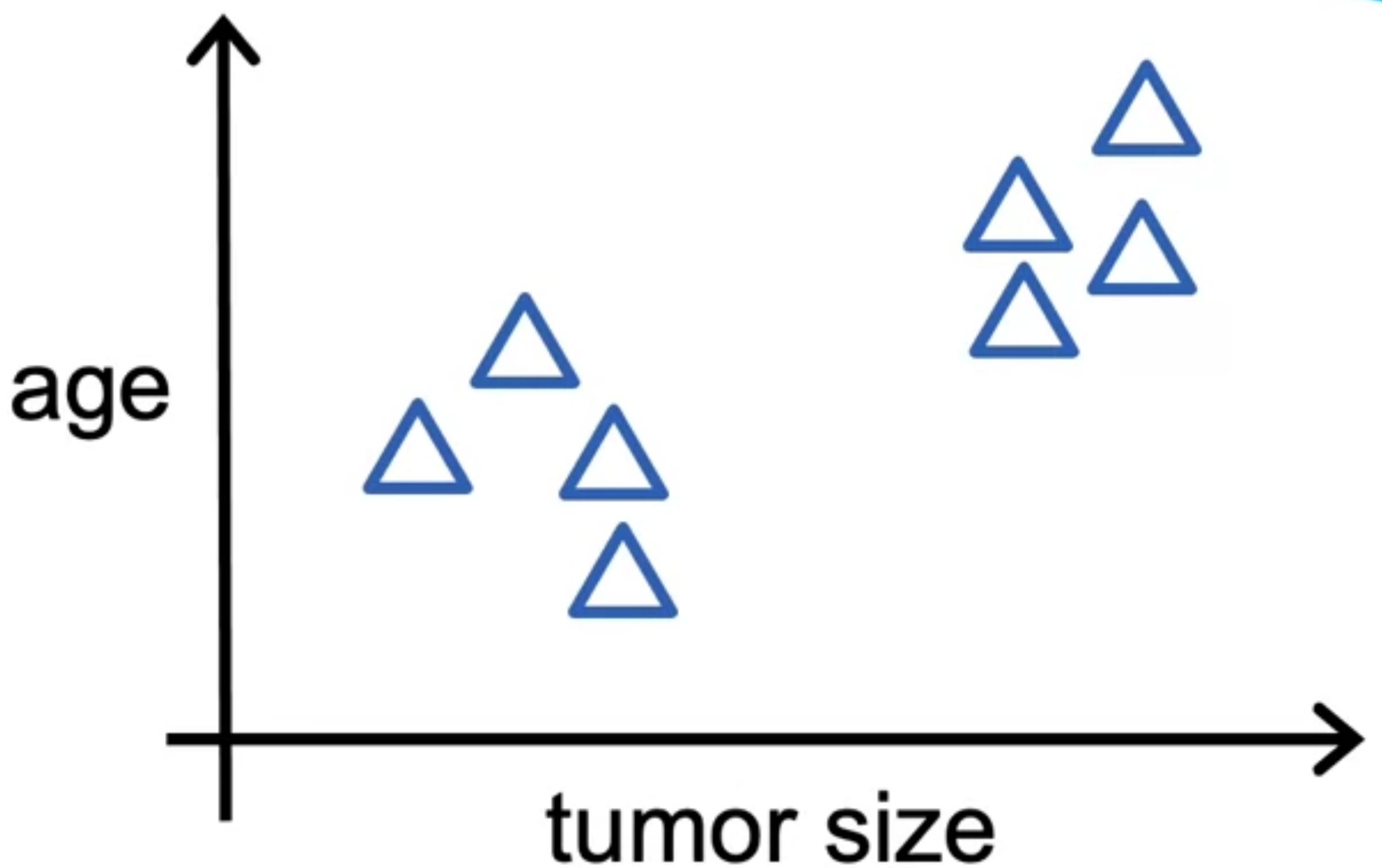
非監督式學習 (Unsupervised Learning)

- 使用未標記的資料來訓練模型。這種學習方式的目標是讓模型從輸入資料的特徵中，學習其結構或模式。
 - Cluste) : 將資料透過其相似度分組。
 - 降維：目的是減少資料的維度（即特徵的數量），通常用於資料的視覺化或者是在進行監督式學習之前的資料預處理過程。
 - 異常檢測：在異常檢測中，模型被訓練來識別出資料中與其他樣本顯著不同的樣本。例如，信用卡公司可能使用異常檢測來識別可能的詐騙交易。
- 由於非監督式學習不依賴於標記資料，所以它在處理大量無標籤資料時，尤其有用。

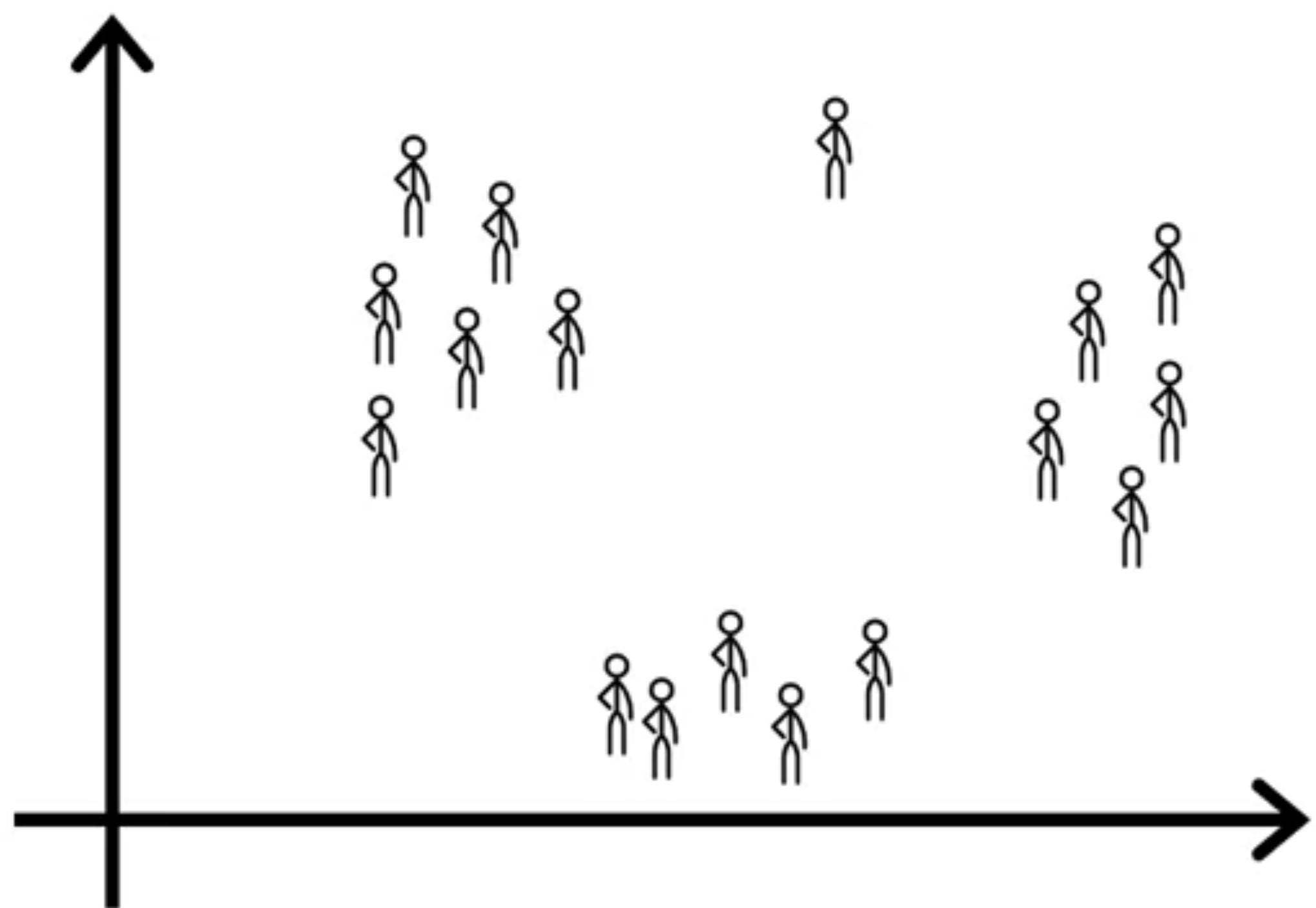
Supervised learning
Learn from data **labeled**
with the “**right answers**”



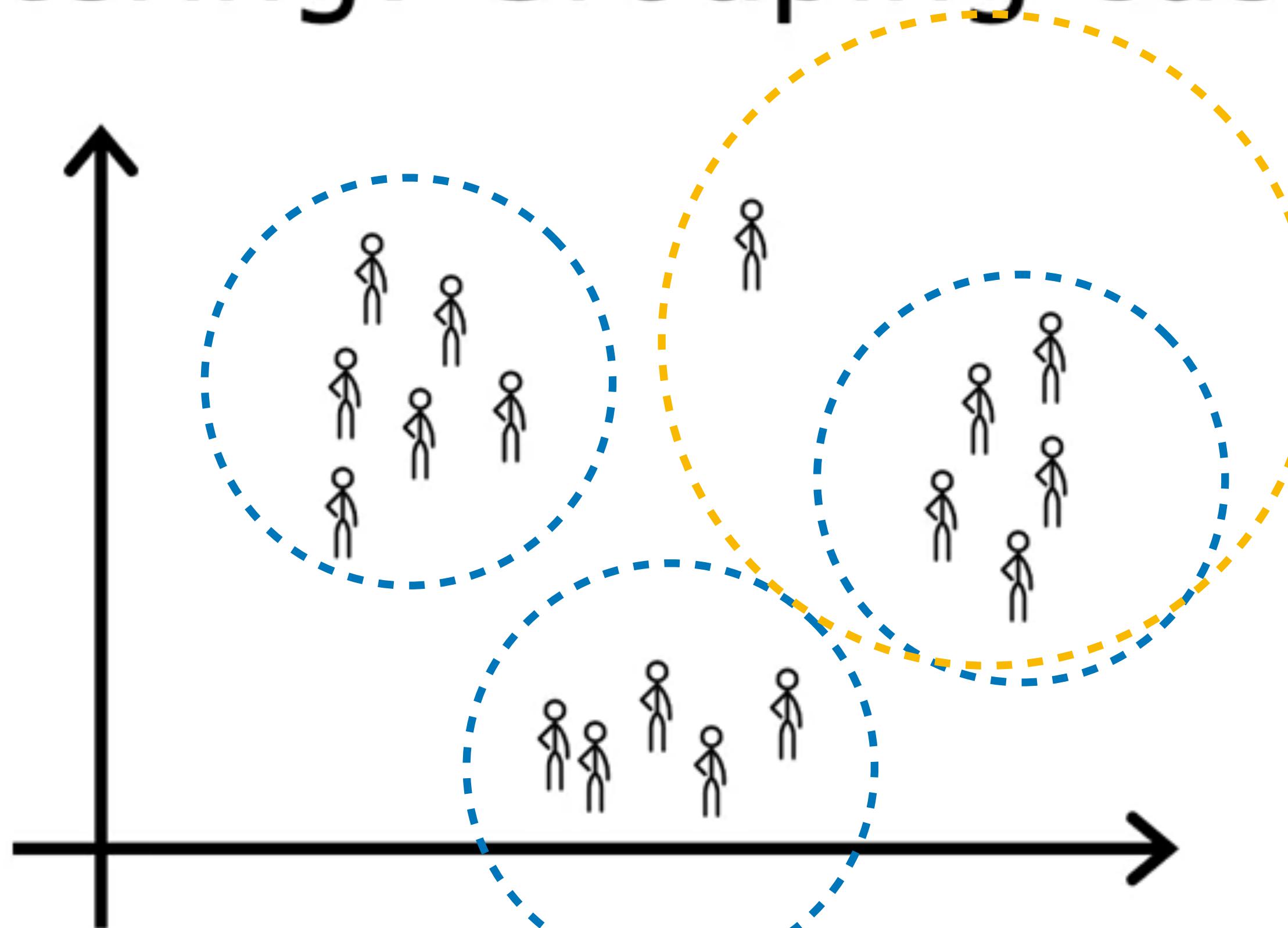
Unsupervised learning



Clustering: Grouping customers

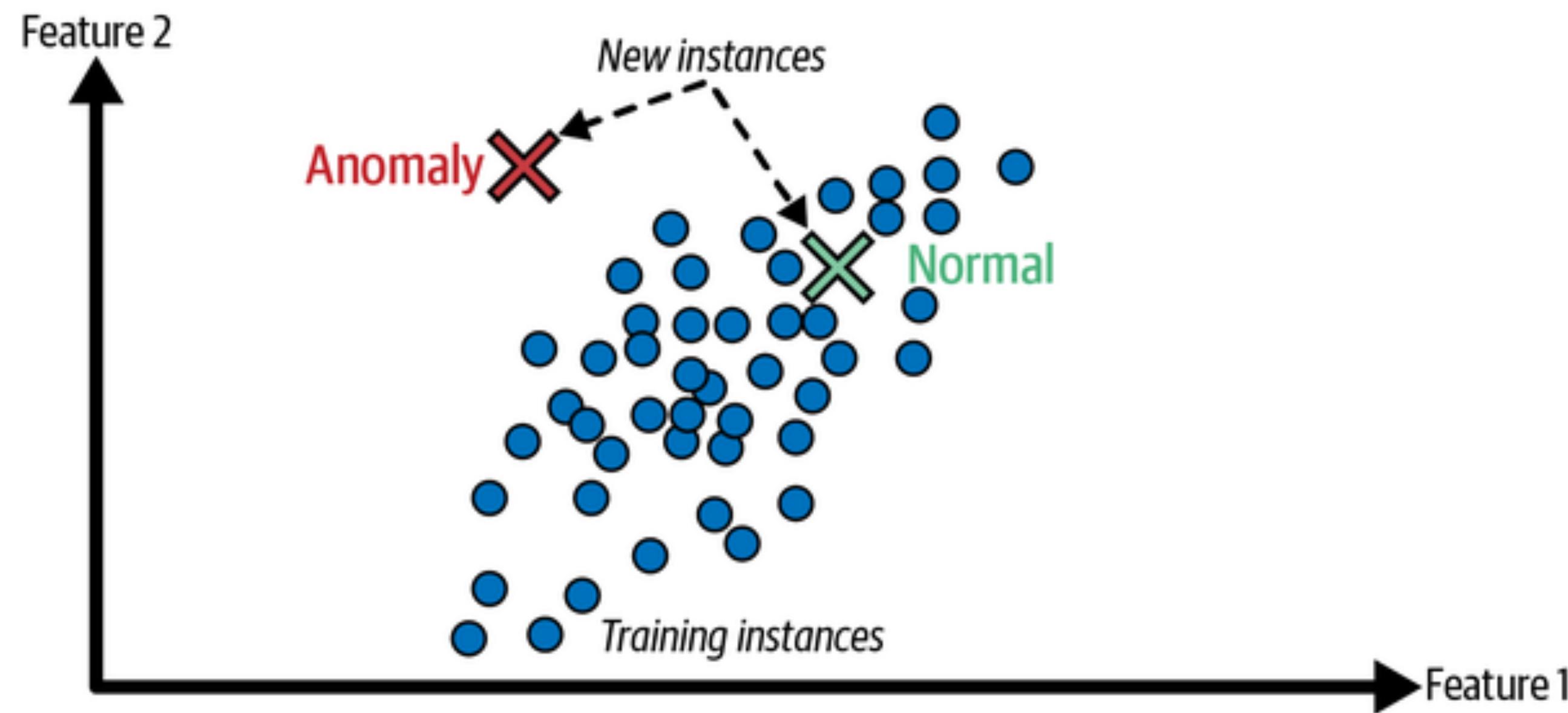


Clustering: Grouping customers



Anomaly Detection

- Detecting unusual credit card transactions to prevent fraud,
- Catching manufacturing defects
- Automatically removing outliers from a dataset

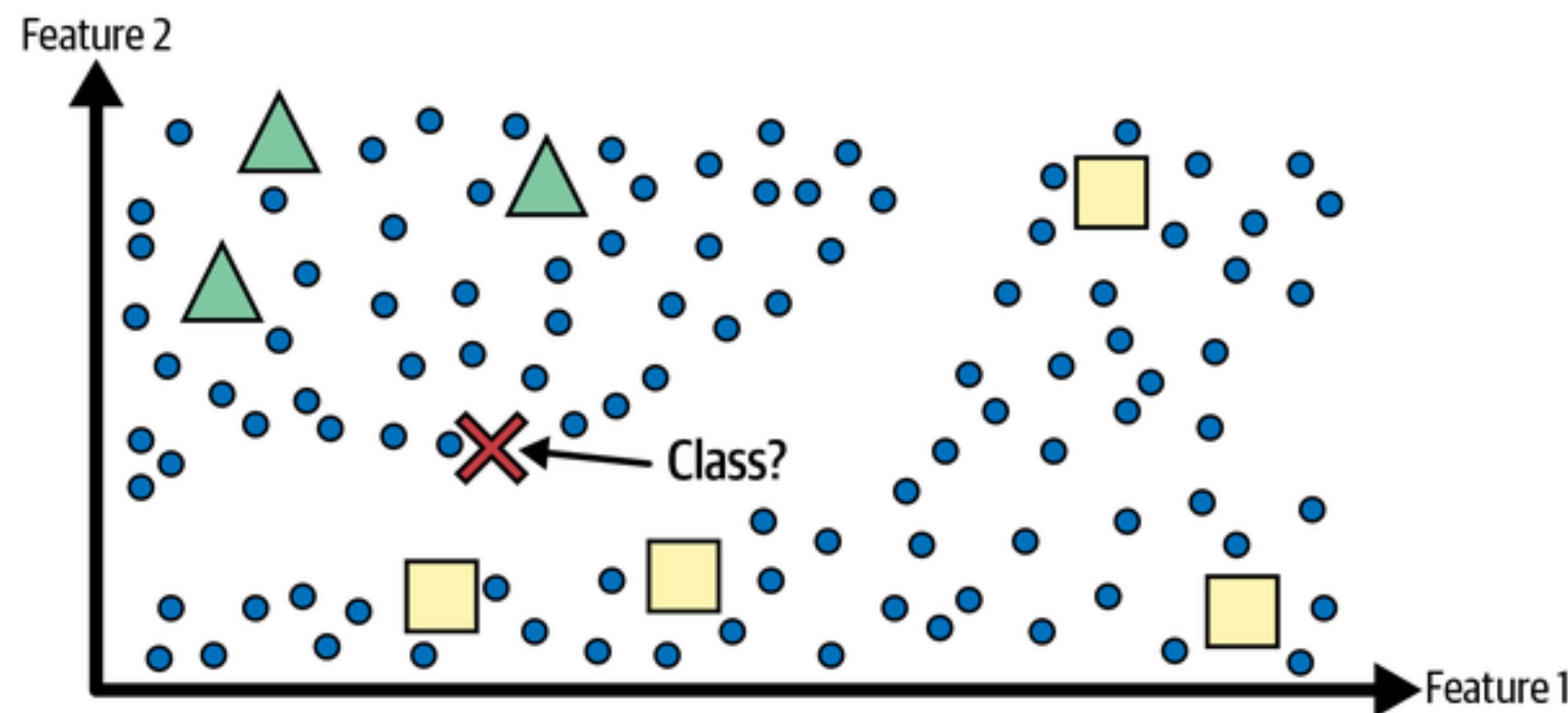


半監督學習 (Semi-supervised Learning)

- 結合了監督式學習和非監督式學習的特點。在半監督學習中，模型被訓練在少部分被標籤的資料用以建構基礎模型，和大量的未被標籤的資料上用以產生新的資料。
 - 利用未標籤的資料：雖然未標籤的資料不能直接用於訓練或預測，但可用於其資料分布或結構
 - 自我訓練：模型首先在標籤資料上進行訓練，然後使用該模型來產生未標籤資料的預測，這些預測接著被作為新的標籤再次用於訓練。
- 半監督學習尤其適合在有大量未標籤資料和少量標籤資料的情況下使用。
- 由於標籤資料的收集過程通常既費時又昂貴，所以在許多實際情況中，半監督學習可以提供一種有效的解決方案。

Semi-Supervised Learning

- Two classes (triangles and squares)
- The unlabeled examples (circles) help classify a new instance (the cross)



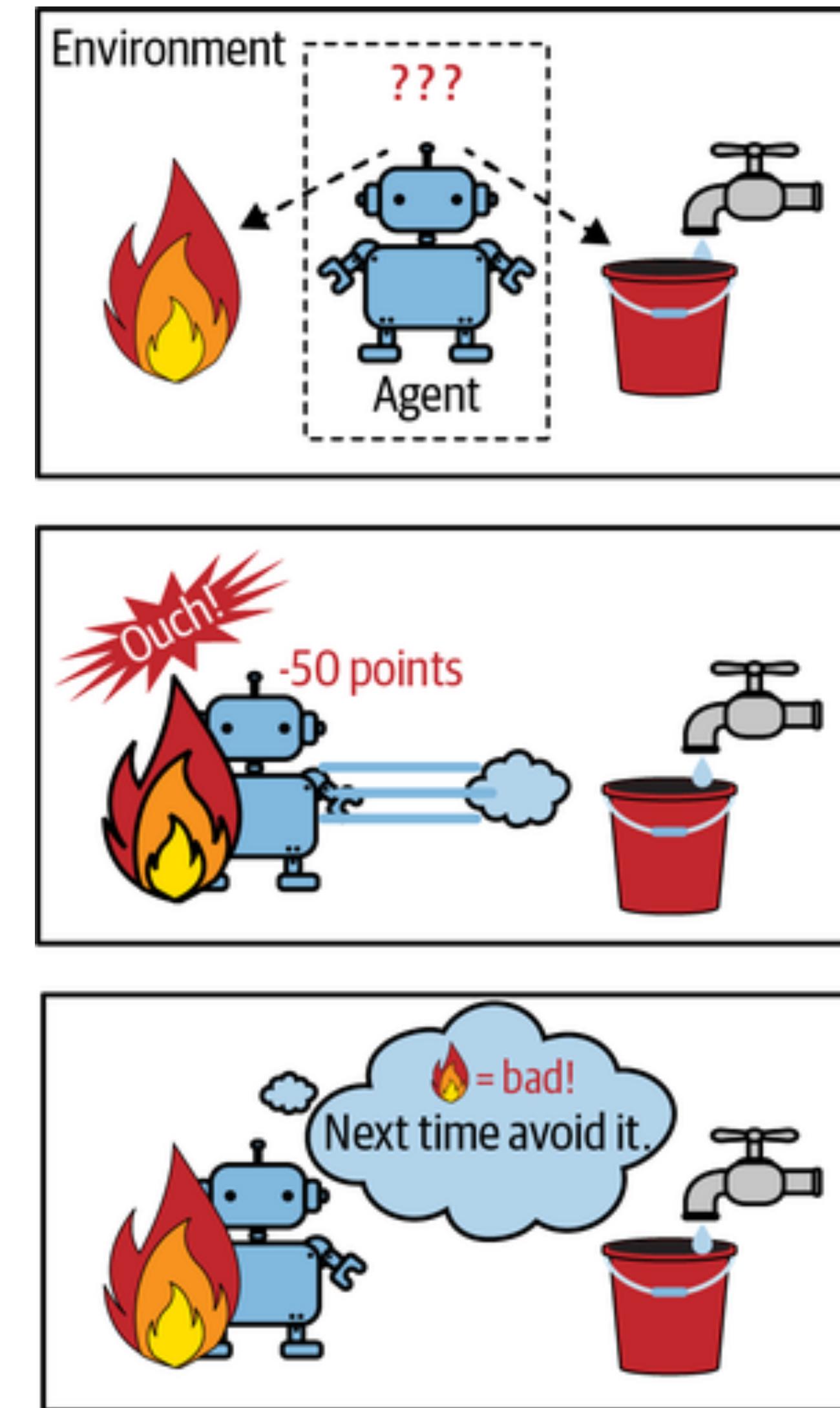
強化式學習 (Reinforcement Learning)

- 一個智能體 (agent) 在與環境 (environment) 的互動中學習如何行動 (action) ，計算其在長期中最大化累計獎勵的一種學習形式 (reward) 。
 - 智能體 (Agent) 、環境 (Environment) 、行動 (Actions) 、狀態 (States) 、獎勵 (Reward) 、政策 (Policy)
- 在強化學習中，智能體的目標是學習一個最佳政策，該政策將在給定狀態下選擇能最大化長期獎勵的行動。
- 這個學習過程通常涉及到探索 (嘗試新的行動) 和利用 (採取已知最佳行動) 之間的平衡，以及處理即時獎勵與長期獎勵之間的權衡。source: <https://www.synopsys.com/ai/what-is-reinforcement-learning.html>
- 強化學習的範例包括棋盤遊戲如圍棋、遊戲、機器人導航，以及在不確定環境中進行資源管理等許多其他類型的問題。



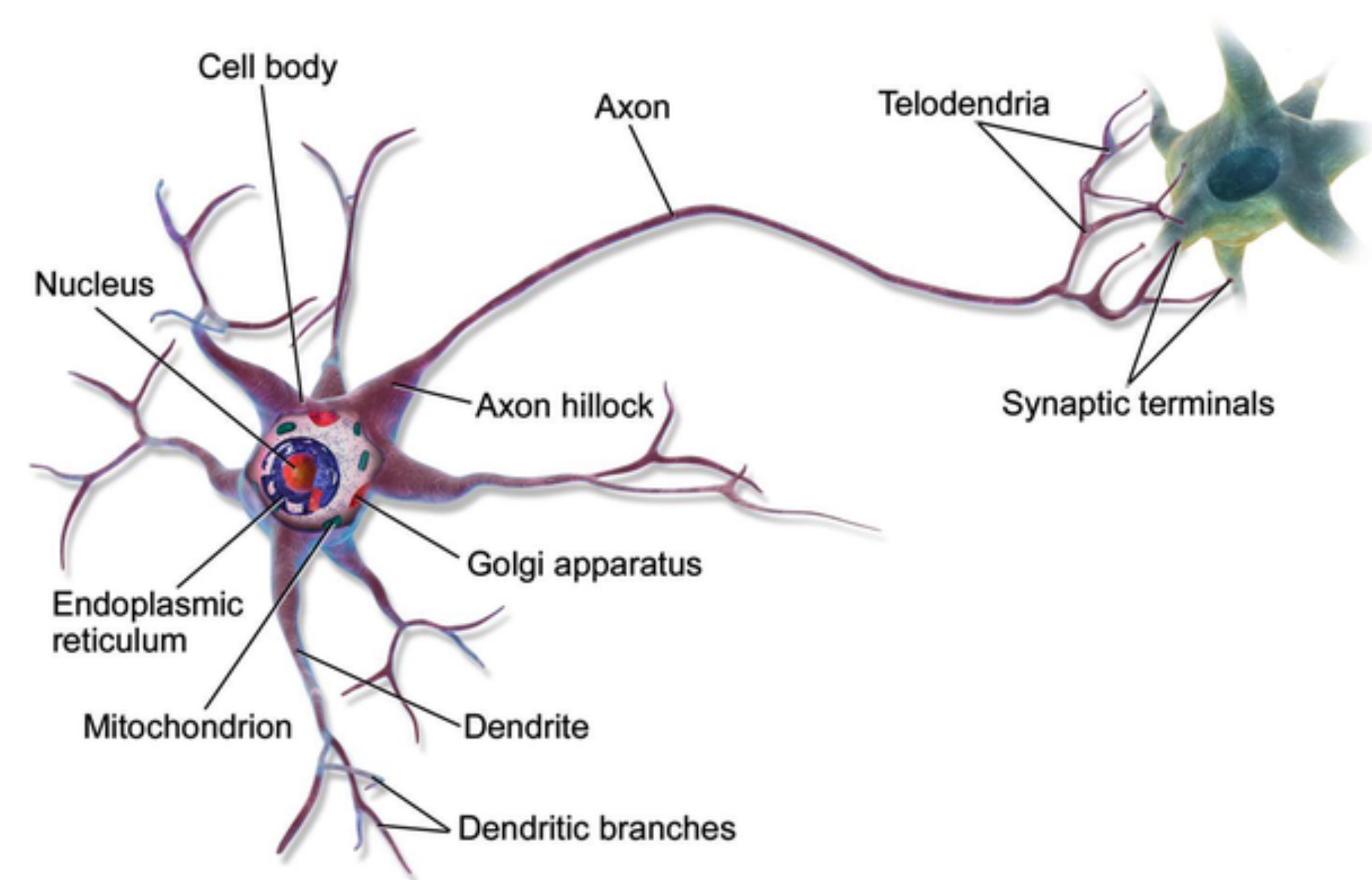
Reinforcement Learning

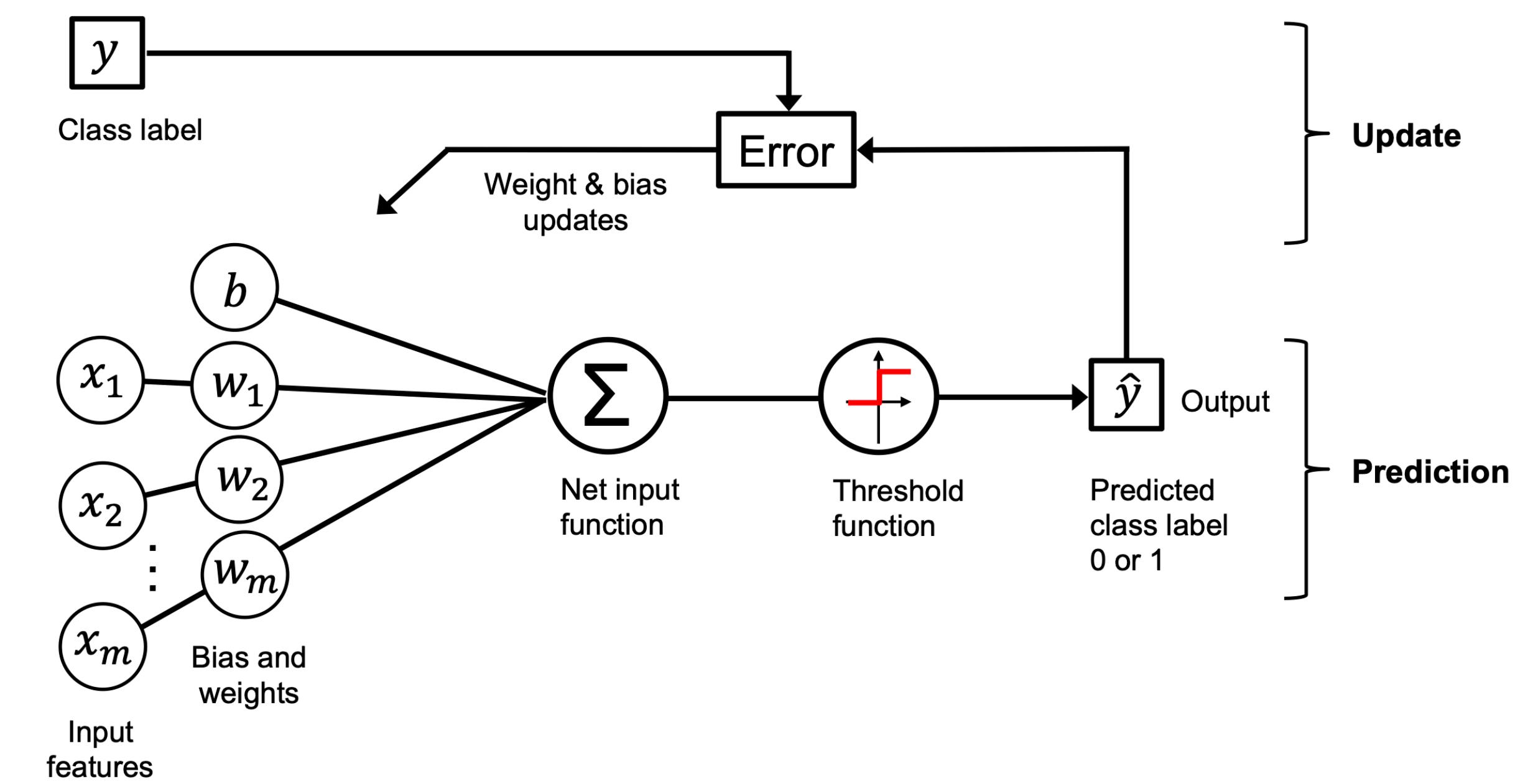
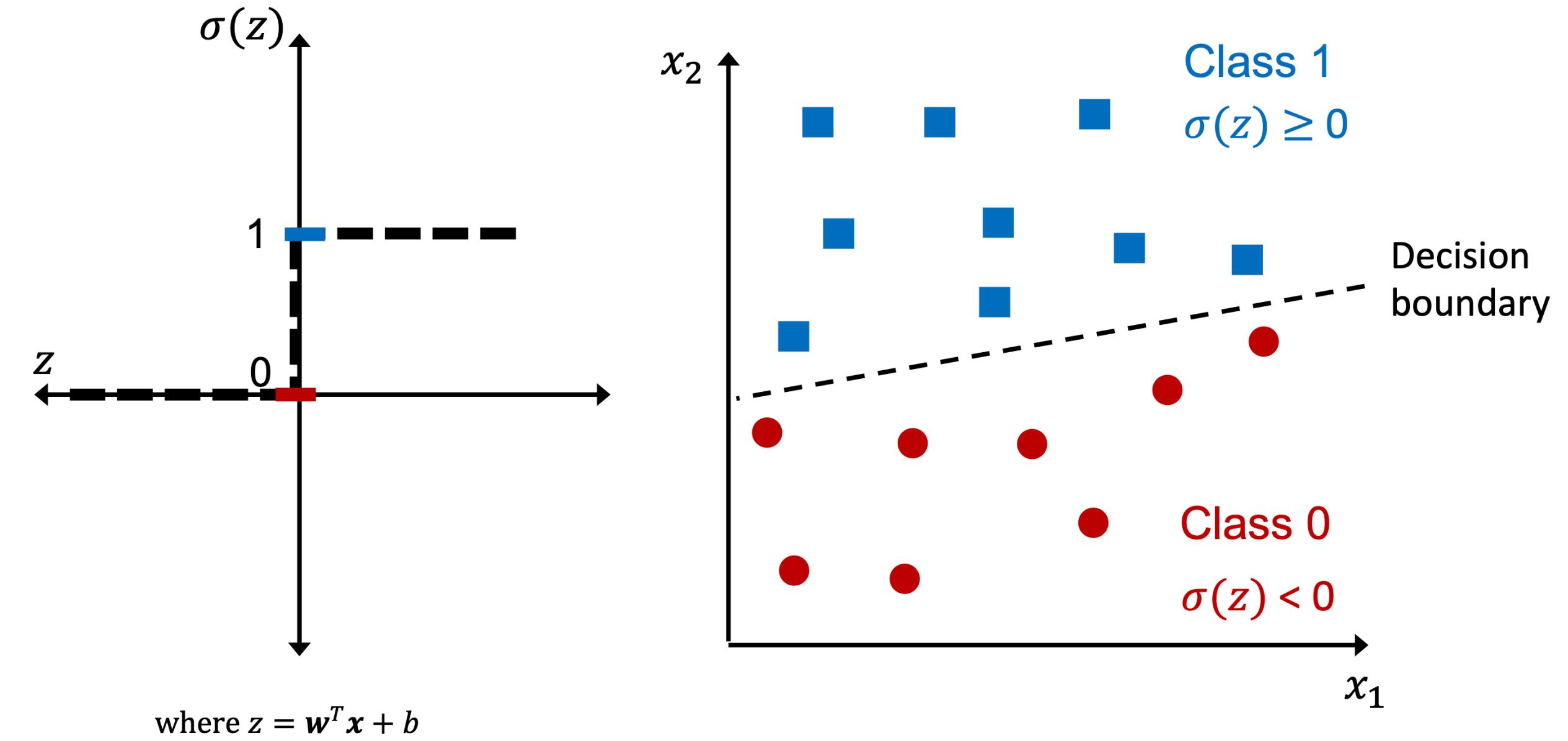
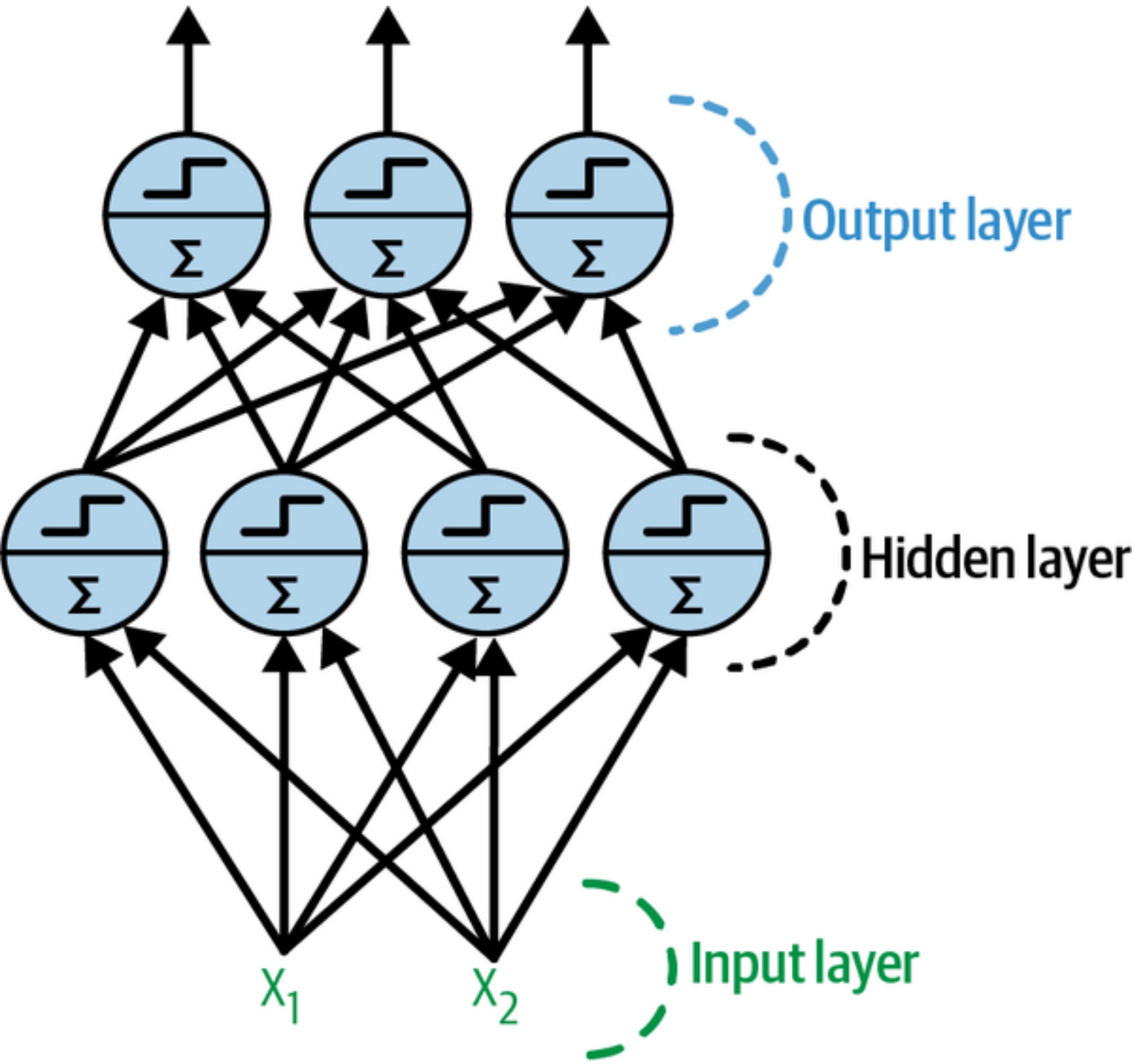
- The learning system, called an agent.
- Observe the environment, select and perform actions, and get rewards in return.
- Learn by itself what is the best strategy, called a policy, to get the most reward over time.
- A policy defines what action the agent should choose when it is in a given situation.

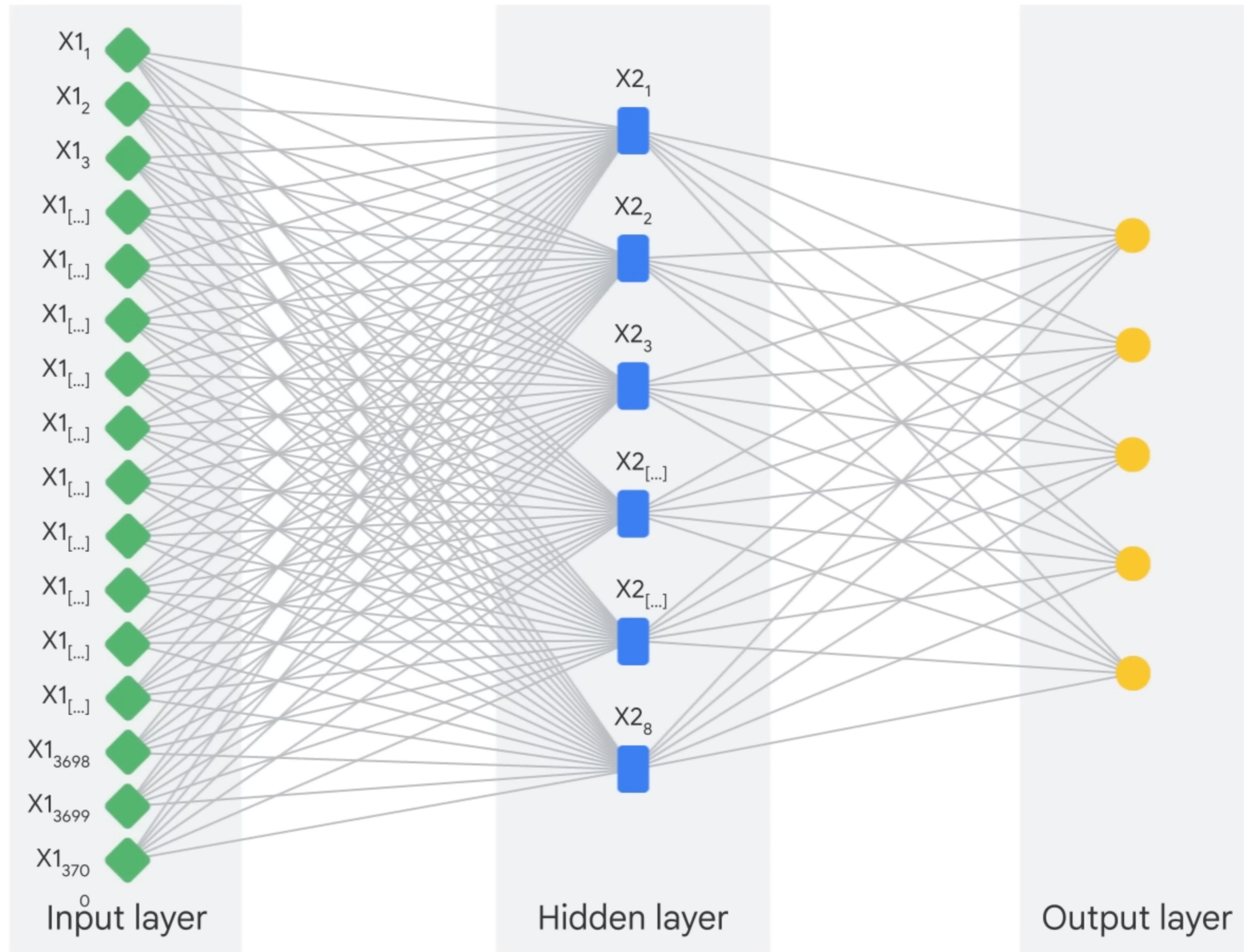


深度學習 (Deep Learning)

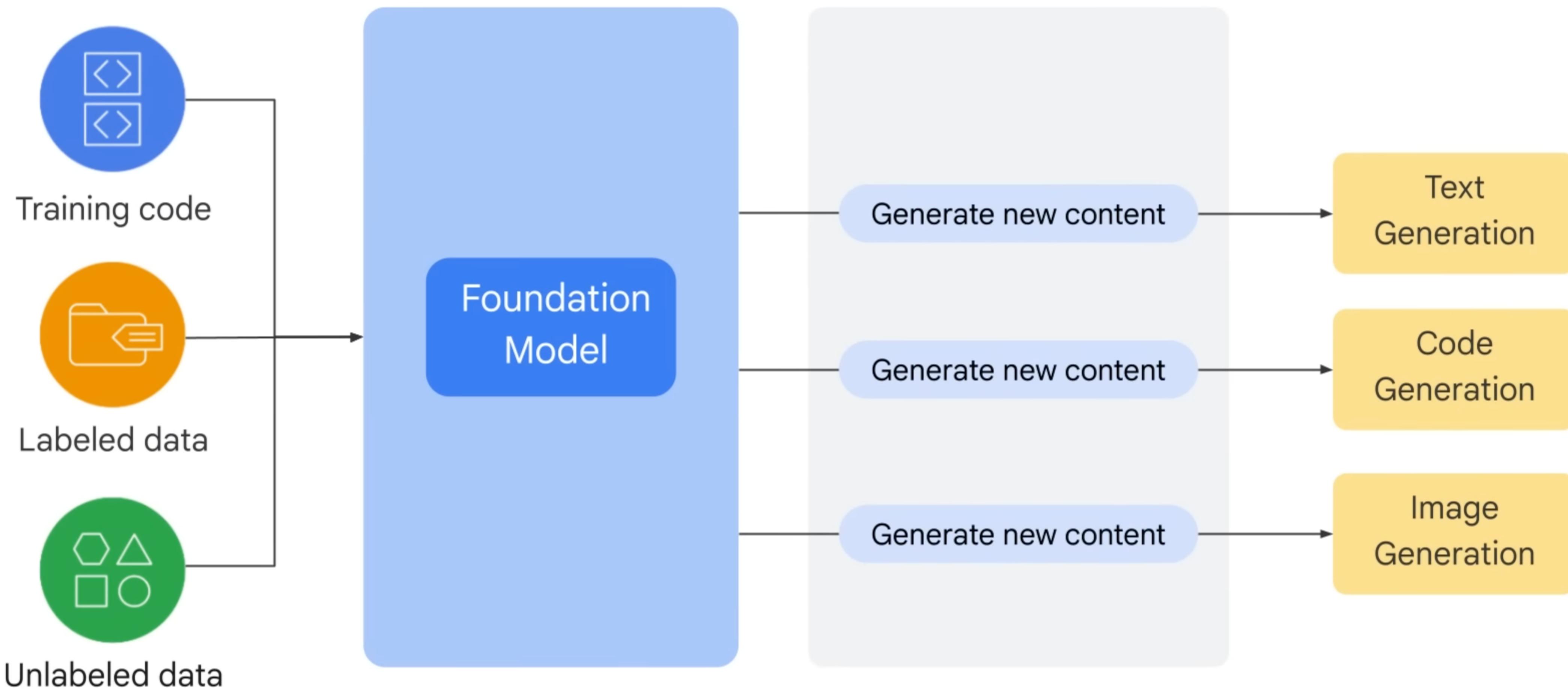
- 專注於利用稱為類神經網路 (Neural Network, NN) 的模型方法來模擬人腦神經元的工作方式。
- "深度"一詞，來自於這種神經網路可以由多個"層"組成，每一層都對應於更高層次的特徵或抽象概念。
- 深度學習模型通過這樣的多層神經網絡來進行學習和預測。



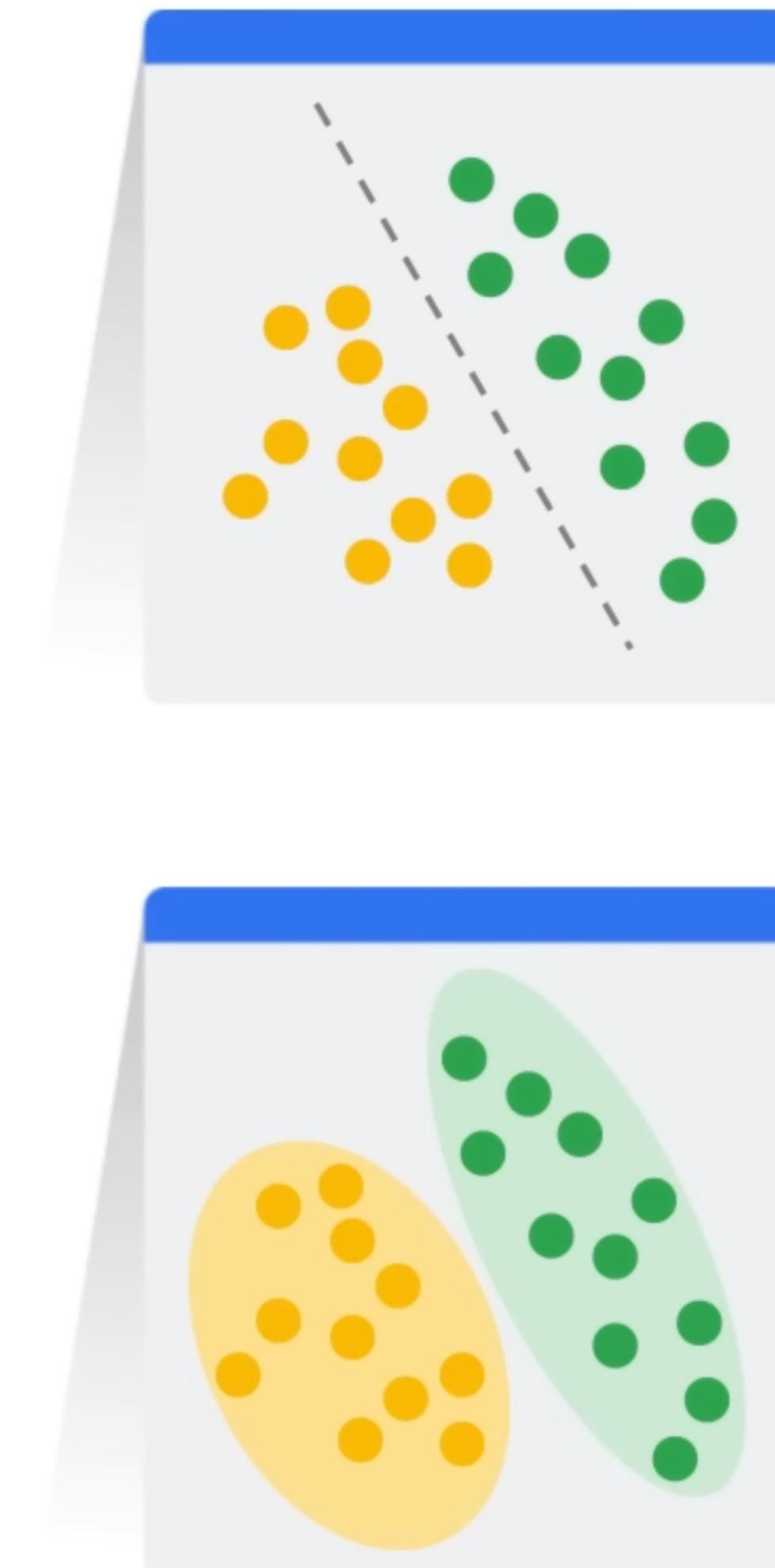




Gen AI Supervised, Semi-Supervised & Unsupervised Learning



Deep Learning Model Types



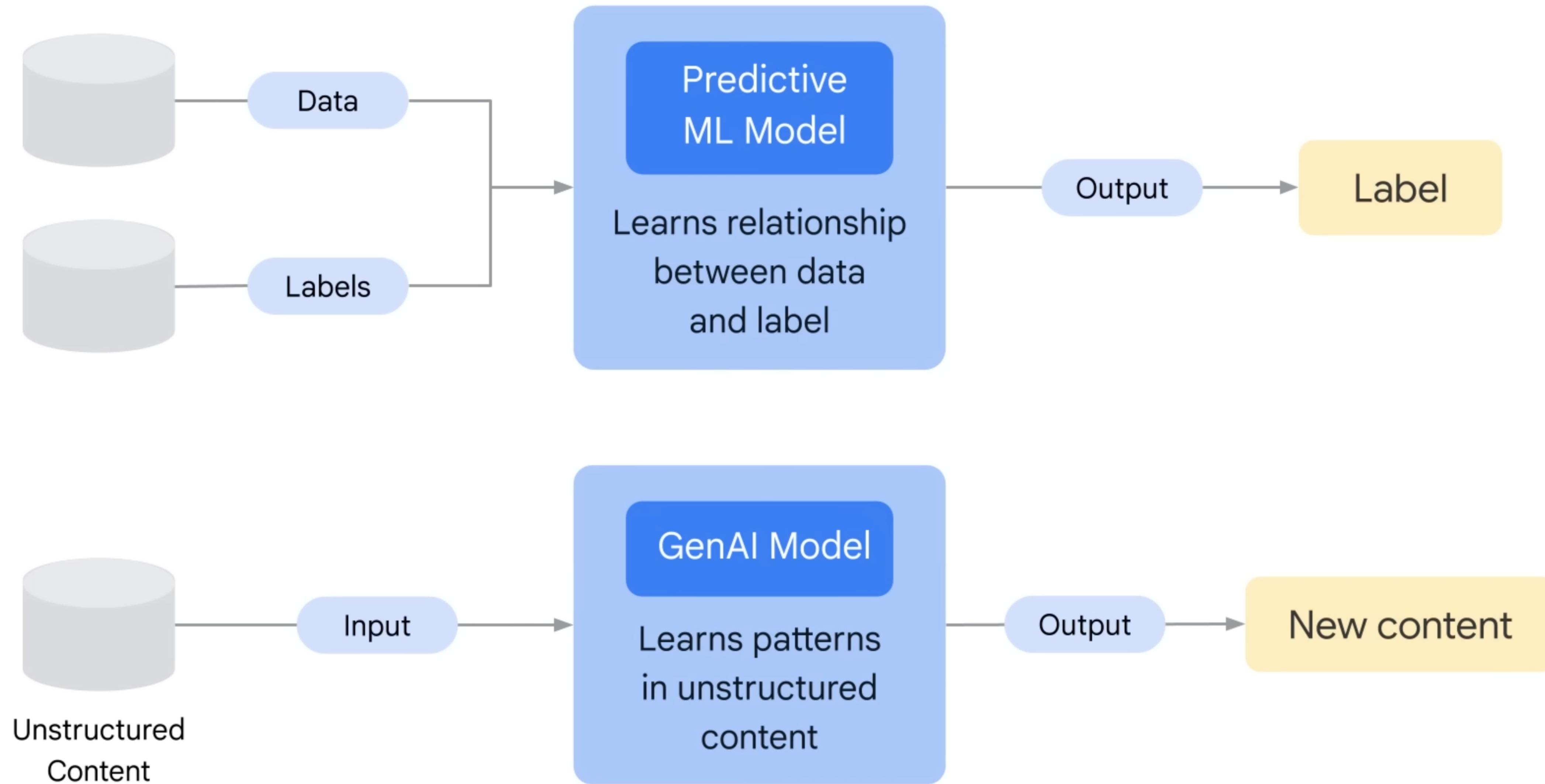
Discriminative

- Used to classify or predict
- Typically trained on a dataset of labeled data
- Learns the relationship between the features of the data points and the labels

Generative

- Generates new data that is similar to data it was trained on
- Understands distribution of data and how likely a given example is
- Predict next word in a sequence

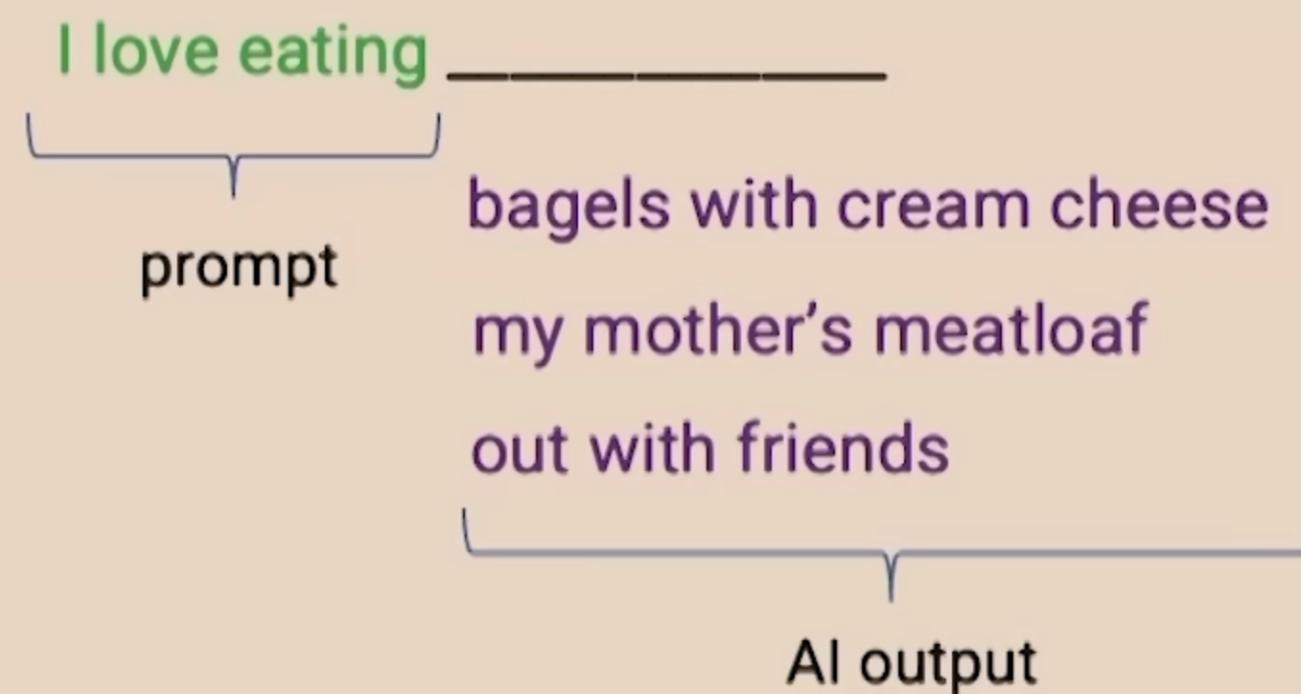




文字生成過程

This decade: Generative AI

Text generation process



How it works

Generative AI is built by using supervised learning ($A \rightarrow B$) to repeatedly predict the next word.

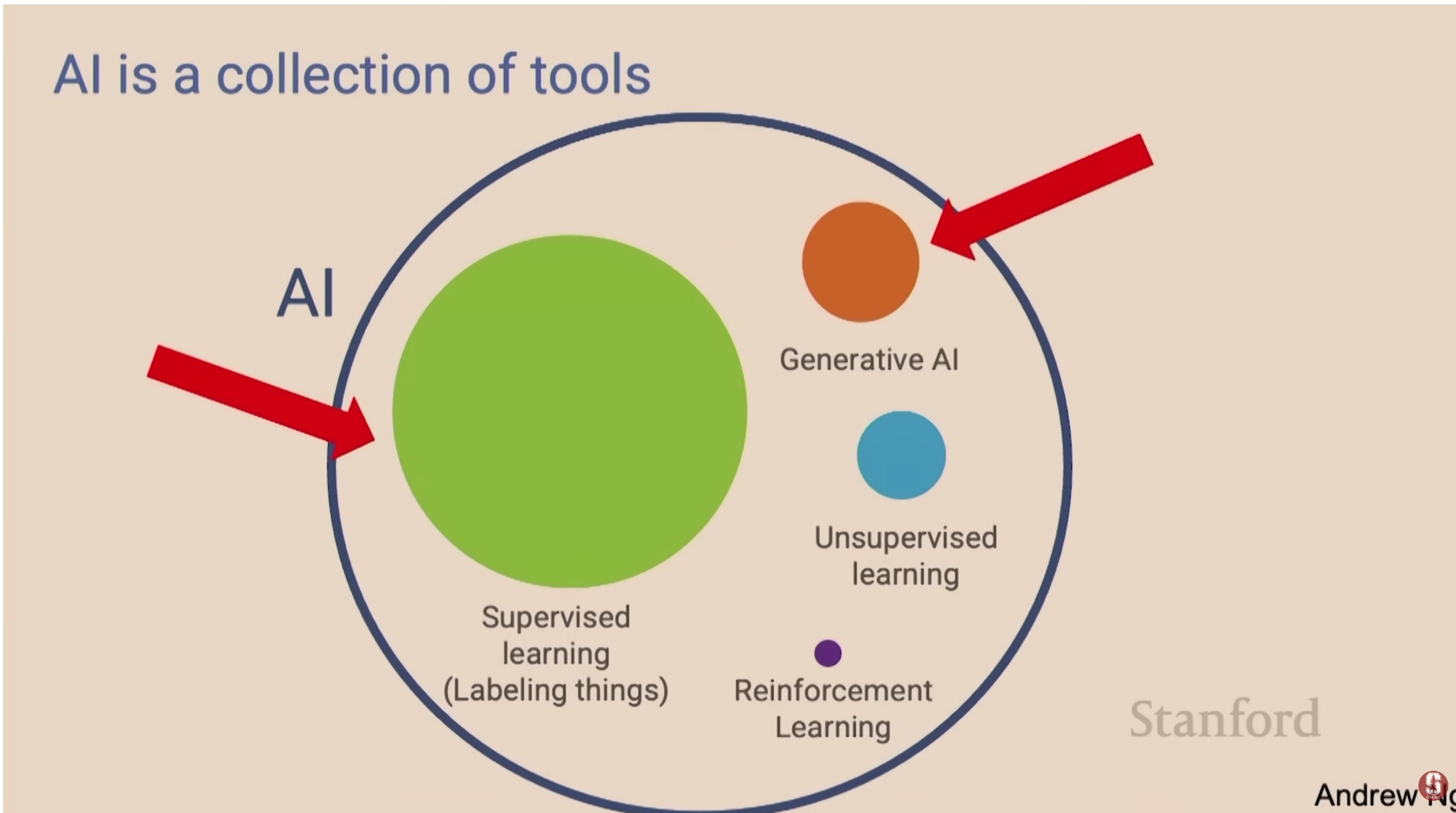
My favorite food is a bagel with cream cheese and lox.

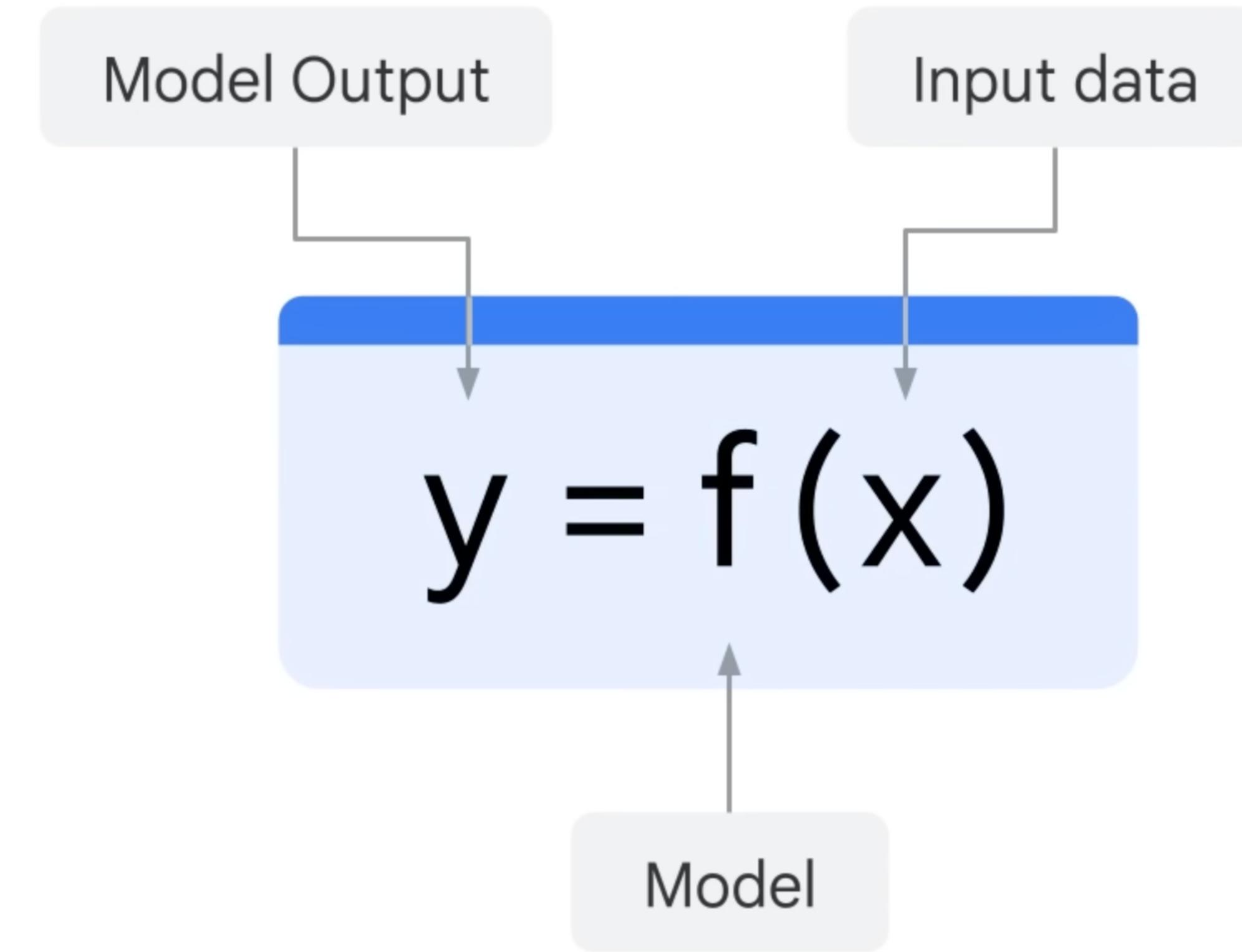
Input (A)	Output (B)
My favorite food is a	bagel
My favorite food is a bagel	with
My favorite food is a bagel with	cream

Stanford

Andrew Ng

AI 是一系列方法的集合





Not GenAI when y is a:

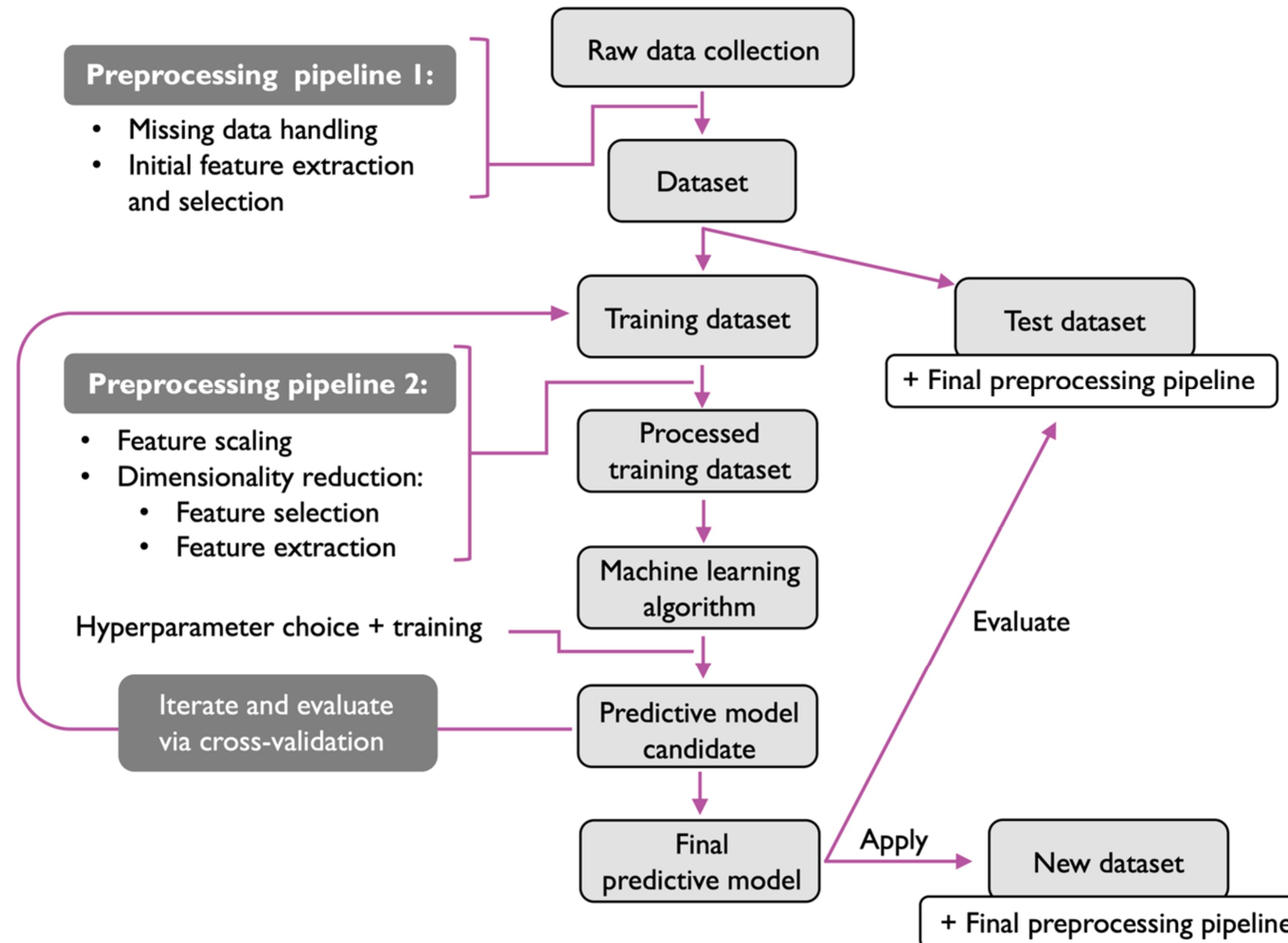
- Number
- Discrete
- Class
- Probability

Is GenAI when y is:

- Natural language
- Image
- Audio



機器學習系統建立流程圖



提示工程的策略

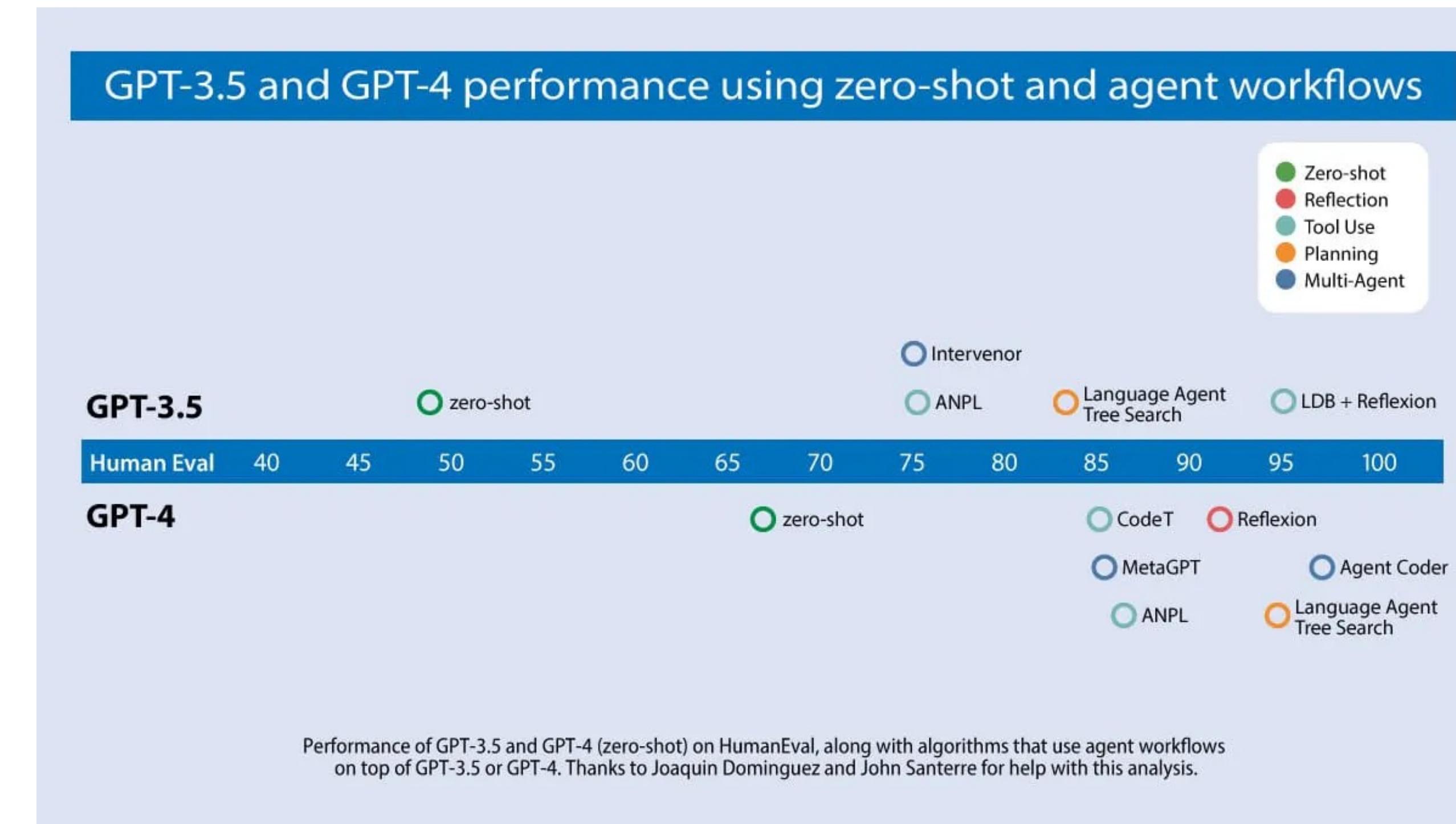
- 了解你的目標：定義目標，並瞭解透過提示取得資訊、創意還是解決問題？
- 保持清晰簡潔：避免過於複雜或模糊的提示。清晰的提示能有更準確的回應。
- 重視上下文：提供足夠的背景資訊以便 LLM 理解情境，但避免不必要的資訊。
- 嘗試和迭代：根據你得到的回應，嘗試不斷的改善提示。迭代是找到最有效措辭的關鍵。
- 考慮你的受眾：根據會與 AI 回應互動或受眾來調整你的提示。
- 評估和調整：不斷評估提示的有效性，並準備隨時進行調整。

Prompts Engineering Principles

- 兩個prompt的原則
 - 寫出清楚明確的指示
 - 紿模型"思考"的時間
- 寫出清楚明確的指示
 - 使用界定符號清楚指示輸入的不同部分
 - 要求結構性的輸出，e.g., JSON, HTML
 - 要求模型檢查條件是否滿足
- 紿模型思考的時間
 - 指定完成任務所需的步驟
 - 指示模型製定出自己的解決方案，在模型匆忙下結論之前

Agentic Patterns Prompting

- Reflection
 - LLM 自己審視自己回覆的結果並改善
- Tool Use
 - 讓 LLM 擁有像是網路收尋、程式執行或其他可以取得資料、資料分析或是採取行動
- Planning
 - LLM 採取更細部的步驟，有計畫的一步一步去達成目標
- Multi-agent
 - 許多的 agent 一起合作，互相討論或是互相辯論後產生出結果



跟著 ChatGPT 學程式

- 利用提示工程與模版
- 策略：
 - 增進現有程式，要求他寫得更 Pythonic
 - 簡化程式
 - 撰寫測試程式
 - 增加程式效率
 - 協助偵錯
 - 重複測試

你是一個程式專家，能夠寫出精準、明確且乾淨的程式碼。

請寫一個股票計算移動平均的類別。

每一行程式碼都加上註解。

你的程式碼：