

# 《机器学习基础》



## 绪论

[https://github.com/styluck/mech\\_learn](https://github.com/styluck/mech_learn)

# 关于本课程

---

- ▶ 人工智能：让机器模拟、延伸和扩展人类智能。学习、推理、图像识别。
- ▶ 机器学习：人工智能的关键分支，计算机模拟人类学习行为，让计算机从数据中进行学习，得到某种知识或规律。
- ▶ 神经网络：模仿生物神经网络结构与功能，由大量神经元及连接权重构成，通过调整权重学习数据模式规律的计算模型。
- ▶ 深度学习：让计算机从大量数据中自动学习复杂模式与特征，实现分类、预测等任务的机器学习技术。

# 关于本课程

---



# 关于本课程

---

## ► 深度学习的研究领域：

- 计算机视觉：让计算机理解 and 处理图像及视频，如图像识别、目标检测、图像分割、视频内容分析
- 自然语言处理：使计算机理解、生成和处理人类语言，如翻译、文本分类、问答系统、语音识别。

## ► 应用领域：

- 医疗：辅助医疗影像分析、疾病诊断、药物研发、医疗数据挖掘。
- 智能交通：自动驾驶汽车的环境感知与决策、交通流量预测、智能交通信号控制等。
- .....

# 课程大纲

---

## ▶ 基础理论知识概述

- ▶ 机器学习的基本概念
- ▶ 常见学习策略
- ▶ 神经网络基本结构

## ▶ 基础学习模型

- ▶ 线性回归模型
  - ▶ 线性分类模型
  - ▶ 前馈神经网络
  - ▶ 无监督学习
- } 监督学习

## ▶ 深度学习模型

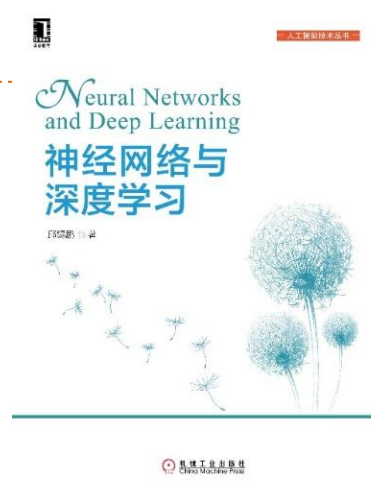
- ▶ 卷积神经网络
- ▶ 循环神经网络
- ▶ 自编码器

## ▶ 前沿模型

- ▶ 注意力机制和Transformer架构
- ▶ BERT
- ▶ GPT模型
- ▶ .....

# 推荐教材

- ▶ 邱锡鹏,神经网络与深度学习,机械工业出版社,2020, ISBN 9787111649687
  - ▶ <https://nndl.github.io/>
  - ▶ 提供配套练习
- ▶ 机器学习,周志华,清华大学出版社,2016, ISBN 9787302423287
- ▶ 李沐等,“动手学深度学习在线课程”  
(<https://courses.d2l.ai/zh-v2/>)



# 推荐论文

---

- ▶ Vaswani, Ashish, et al. "Attention is all you need." Advances in neural information processing systems 30 (2017).
- ▶ Devlin, Jacob, et al. "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding." Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers) (2019).
- ▶ Radford, Alec, et al. "Improving Language Understanding by Generative Pre-Training." (2018).
- ▶ Radford, Alec, et al. "Language Models are Unsupervised Multitask Learners." OpenAI Blog 1.8 (2019).
- ▶ Brown, Tom, et al. "Language Models are Few-Shot Learners." Advances in neural information processing systems 33 (2020).
- ▶ Touvron, Hugo, et al. "Llama 2: Open foundation and fine-tuned chat models." arXiv preprint arXiv:2307.09288 (2023)

# 成绩

---

- ▶ 平时成绩

  - ▶ 30%

- ▶ 期末作业

  - ▶ 70%

- ▶ 期末作业将以两人一组的形式完成。

- ▶ 编程语言: Python

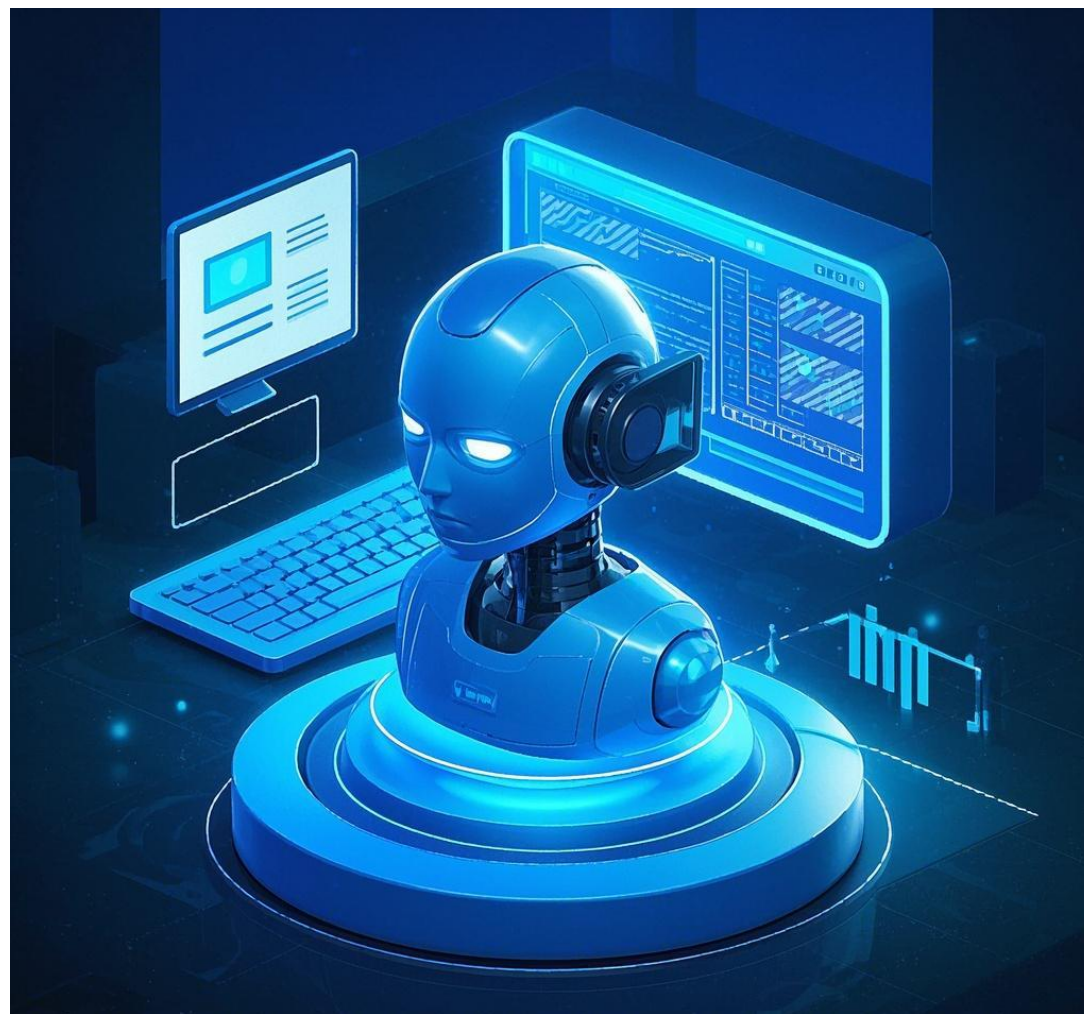




# 机器学习

# 为什么是机器学习

- ▶ 我们希望机器能够做到什么？
- ▶ 为什么要用到深度学习？



# 人vs机器

## 信息收集

- 人：眼睛、耳朵、鼻子、舌头和皮肤等感官
- 机器：数据采集方法和传感器技术

## 信息处理

- 人：大脑会对感官接收的信息进行处理、分析和理解
- 机器：数据表示、处理和分析，价值特征提取

## 知识学习

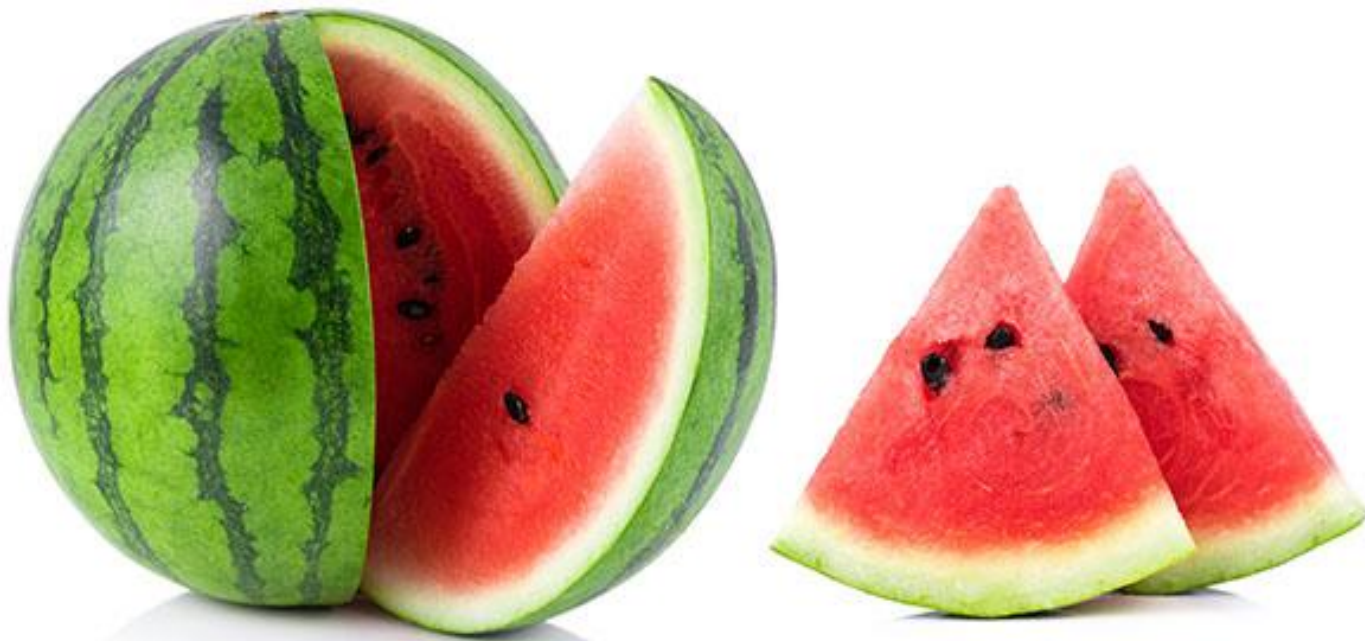
- 人：学习新知识，并将其存储在脑中形成记忆
- 机器：以模型结构和参数的形式存储在模型中

## 结果输出

- 人：做出决策并通过语言、动作等方式进行输出
- 机器：以合适的形式输出结果：预测、分类；文字、图像、音频等


# 如何判断西瓜是否好吃?

---



# 西瓜的机器学习

---

$$f(\text{西瓜}) = \text{西瓜好吃 or 不好吃}$$


A diagram illustrating a machine learning function  $f$ . The function takes a watermelon as input and outputs a binary classification: "西瓜好吃 or 不好吃" (Watermelon is delicious or not delicious). A red arrow points from the text "如何得到这么一个函数  $f$ ?" to the function symbol  $f$  in the equation.

► 如何得到这么一个函数  $f$ ?

# 西瓜的机器学习

---

- ▶ 从市场上随机选取的西瓜样本（训练数据），列出每个西瓜的所有特征：
  - ▶ 如颜色，大小，形状，产地，品牌
- ▶ 以及西瓜质量（输出变量）：
  - ▶ 甜蜜，多汁，成熟度。
- ▶ 设计一个学习算法来学习西瓜的特征与输出变量之间的相关性模型。
- ▶ 下次从市场上买西瓜时，可以根据西瓜（测试数据）的特征，使用前面计算的模型来预测西瓜的质量。



# 机器学习 $\approx$ 构建一个映射函数

---

## ▶ 语音识别

$$f(\text{语音波形}) = \text{“你好”}$$

## ▶ 图像识别

$$f(\text{数字9}) = \text{“9”}$$

## ▶ 围棋

$$f(\text{围棋棋盘}) = \text{“6-5”} \quad (\text{落子位置})$$

## ▶ 机器翻译

$$f(\text{“你好!”}) = \text{“Hello!”}$$

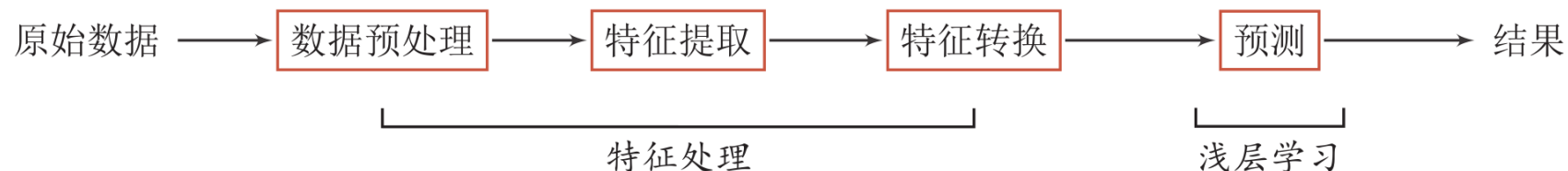


# 深度学习



# 机器学习

- ▶ 当我们用一般的机器学习技术来解决一些模式识别任务时，一般的流程包含以下几个步骤：



特征工程 (Feature Engineering)

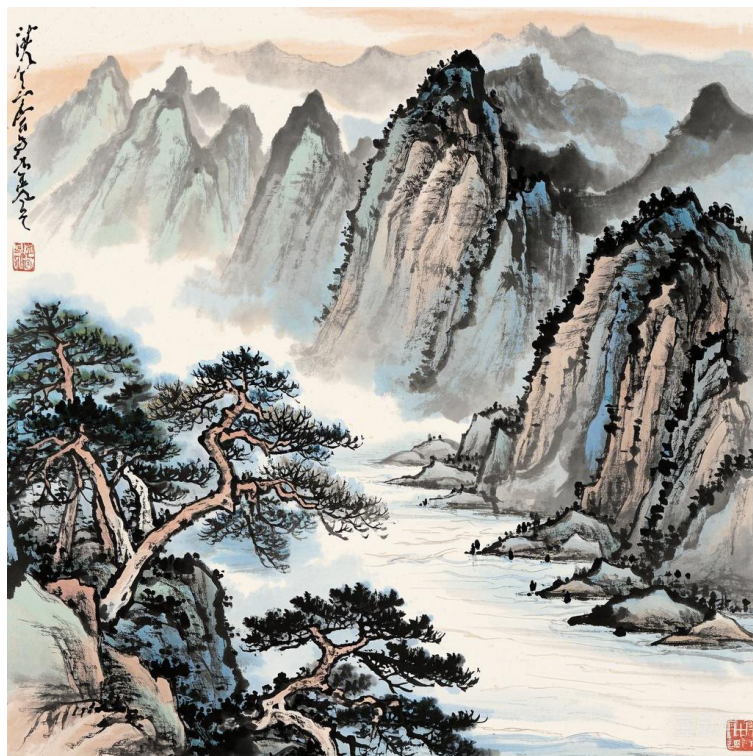
- ▶ 浅层学习 (Shallow Learning)：不涉及特征学习，其特征主要靠人工经验或特征转换方法来抽取。

# 语义鸿沟：人工智能的挑战之一

---

## ► 底层特征 VS 高层语义

- 人们对文本、图像的理解无法从字符串或者图像的底层特征直接获得



床前明月光，  
疑是地上霜。  
举头望明月，  
低头思故乡。

# 什么是好的数据表示？

---

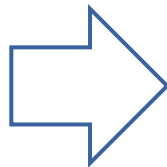
- ▶ “好的表示”是一个非常主观的概念，没有一个明确的标准。
- ▶ 但一般而言，一个好的表示具有以下几个优点：
  - ▶ 应该具有很强的表示能力：准确、紧凑。
  - ▶ 应该使后续的学习任务变得简单：鲁棒性、通用性。
  - ▶ \*便于人类理解和解读：可解释性。

# 语义表示

## ►如何在计算机中表示语义？

局部（符号）表示

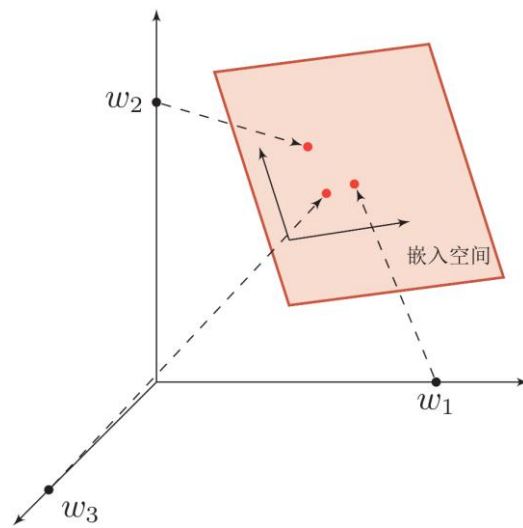
知识库、规则



分布式表示

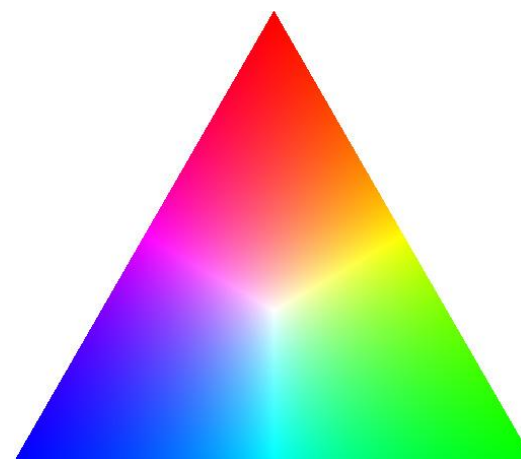
嵌入：压缩、低维、稠密向量

One-Hot向量



# 一个生活中的例子：颜色

颜色	局部表示	分布式表示
琥珀色	$[1, 0, 0, 0]^T$	$[1.00, 0.75, 0.00]^T$
天蓝色	$[0, 1, 0, 0]^T$	$[0.00, 0.5, 1.00]^T$
中国红	$[0, 0, 1, 0]^T$	$[0.67, 0.22, 0.12]^T$
咖啡色	$[0, 0, 0, 1]^T$	$[0.44, 0.31, 0.22]^T$



# 表示学习与深度学习

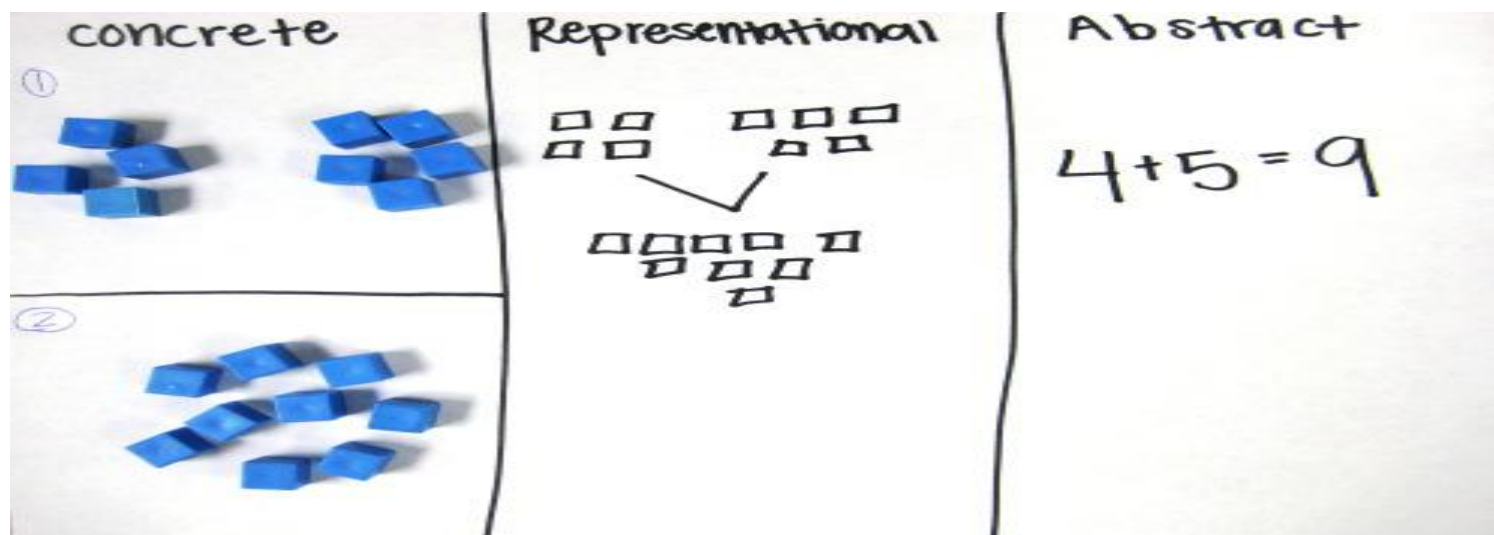
## ▶ 一个好的表示学习策略必须具备一定的深度

### ▶ 特征复用

▶ 指数级的表示能力

### ▶ 抽象表示与不变性

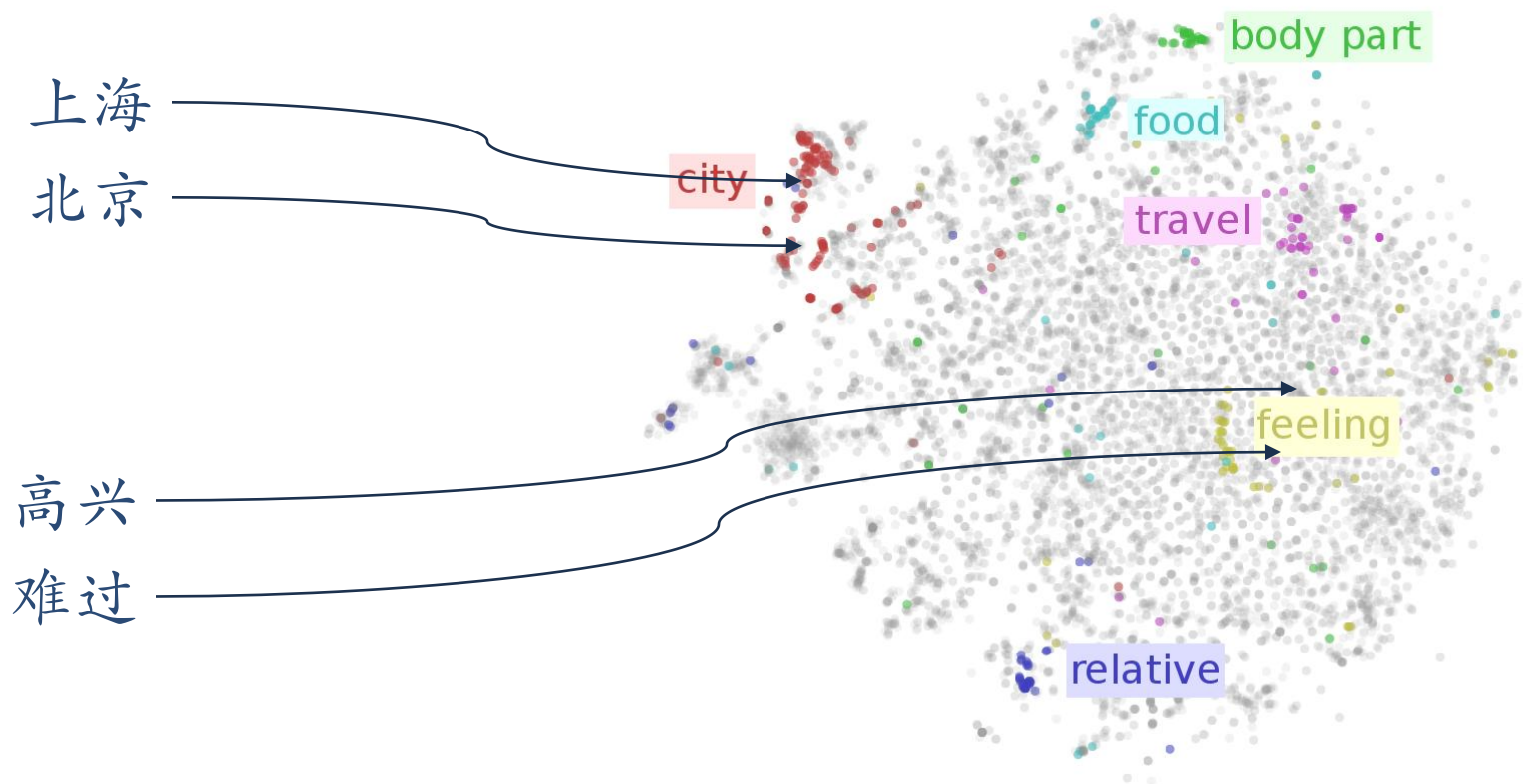
▶ 抽象表示需要多步的构造



<https://mathteachingstrategies.wordpress.com/2008/11/24/concrete-and-abstract-representations-using-mathematical-tools/>

# 词嵌入 (Word Embeddings)

---



<https://indico.io/blog/visualizing-with-t-sne/>

# 传统的特征提取

---

## ▶ 特征提取

- ▶ 线性投影（子空间）
  - ▶ PCA、LDA
- ▶ 非线性嵌入
  - ▶ LLE、Isomap、谱方法
- ▶ 自编码器

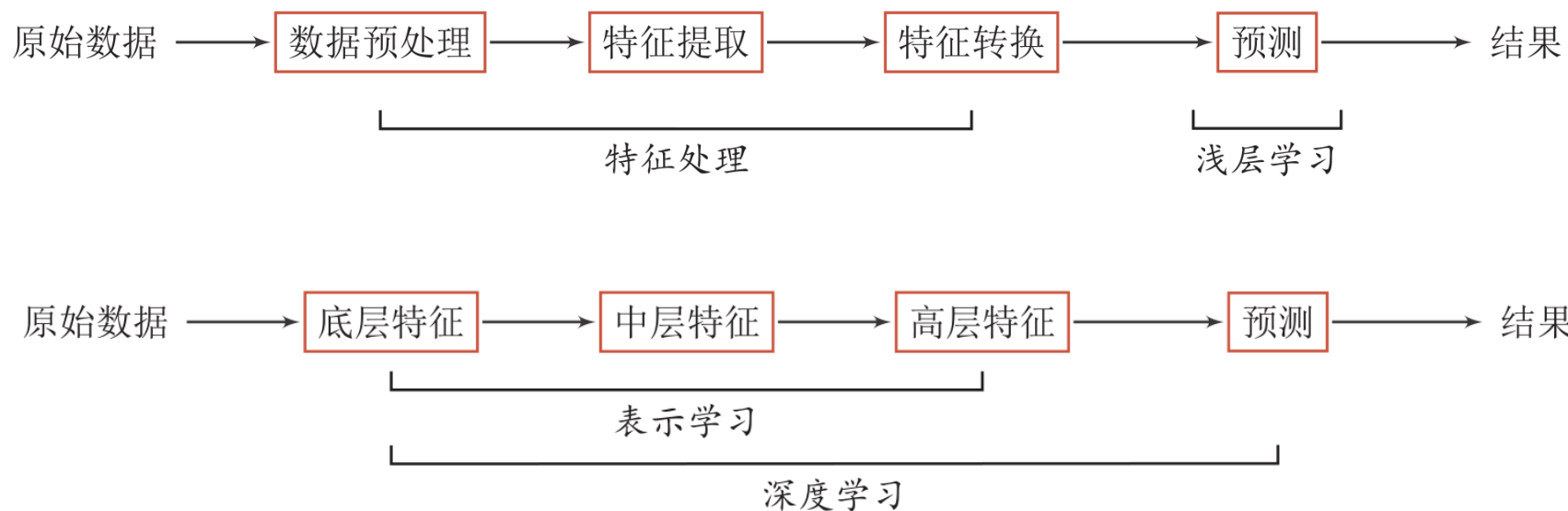
## ▶ 特征提取VS表示学习

- ▶ 特征提取：基于任务或先验对去除无用特征
- ▶ 表示学习：通过深度模型学习高层语义特征



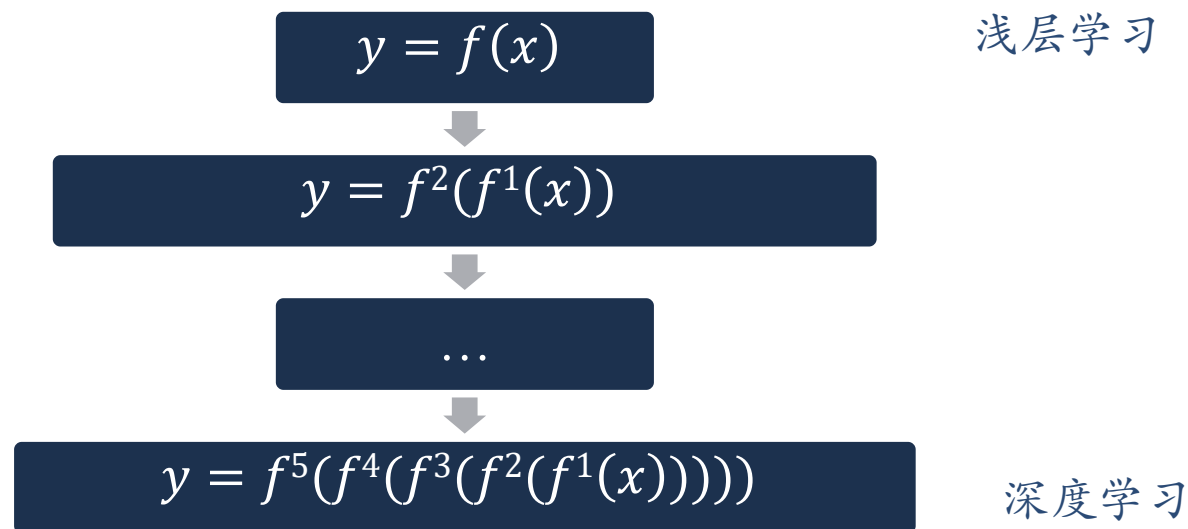
# 深度学习

- ▶ 通过构建具有一定“深度”的模型，可以让模型来自动学习好的特征表示（从底层特征，到中层特征，再到高层特征），从而最终提升预测或识别的准确性。



# 深度学习的数学描述

---



$f^1(x)$  为非线性函数，不一定连续。

当  $f^1(x)$  连续时，比如  $f^1(x) = \sigma(W^1 f^{1-1}(x))$ ，这个复合函数称为神经网络。

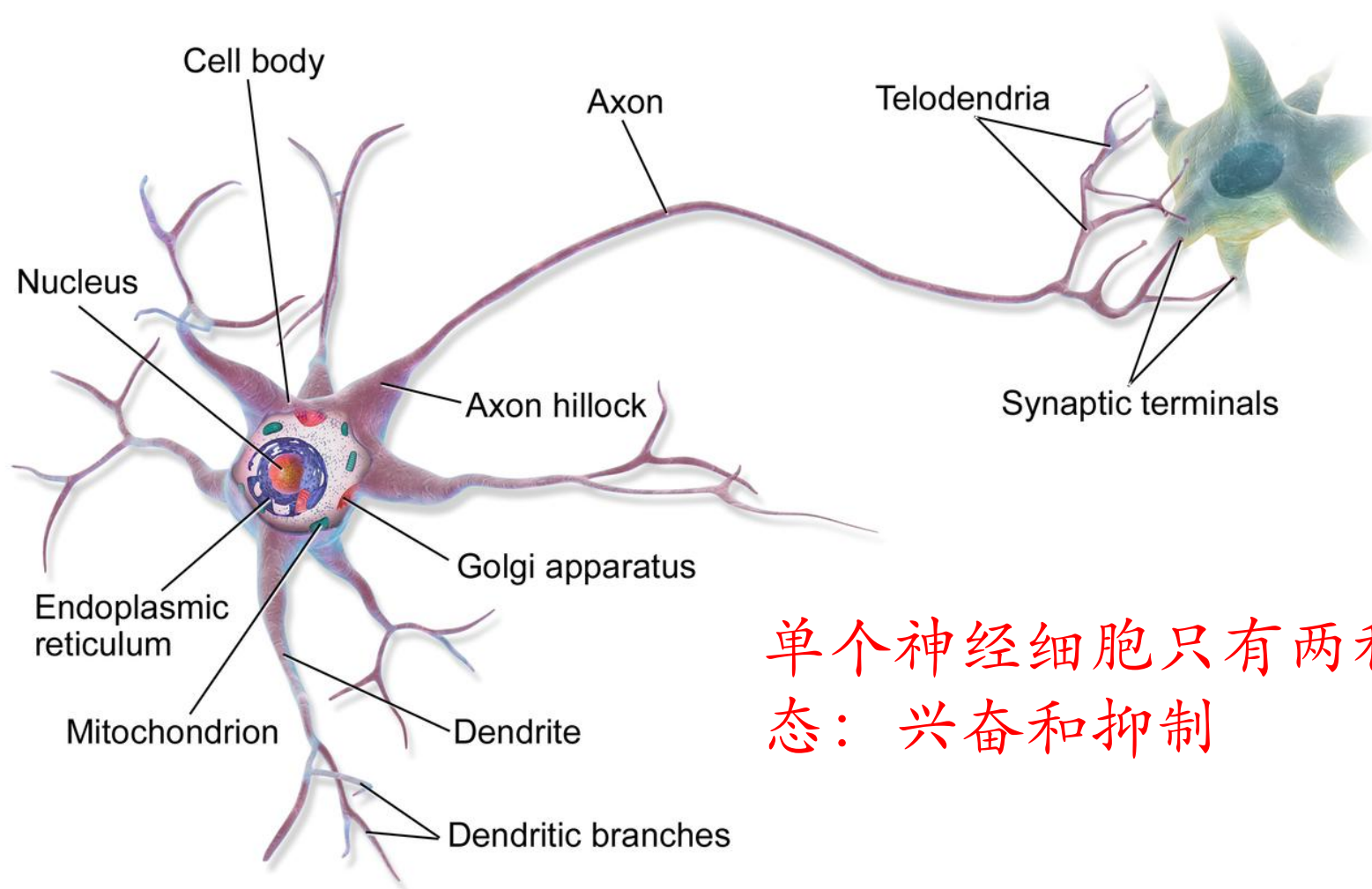


# 神经网络

# 生物神经元

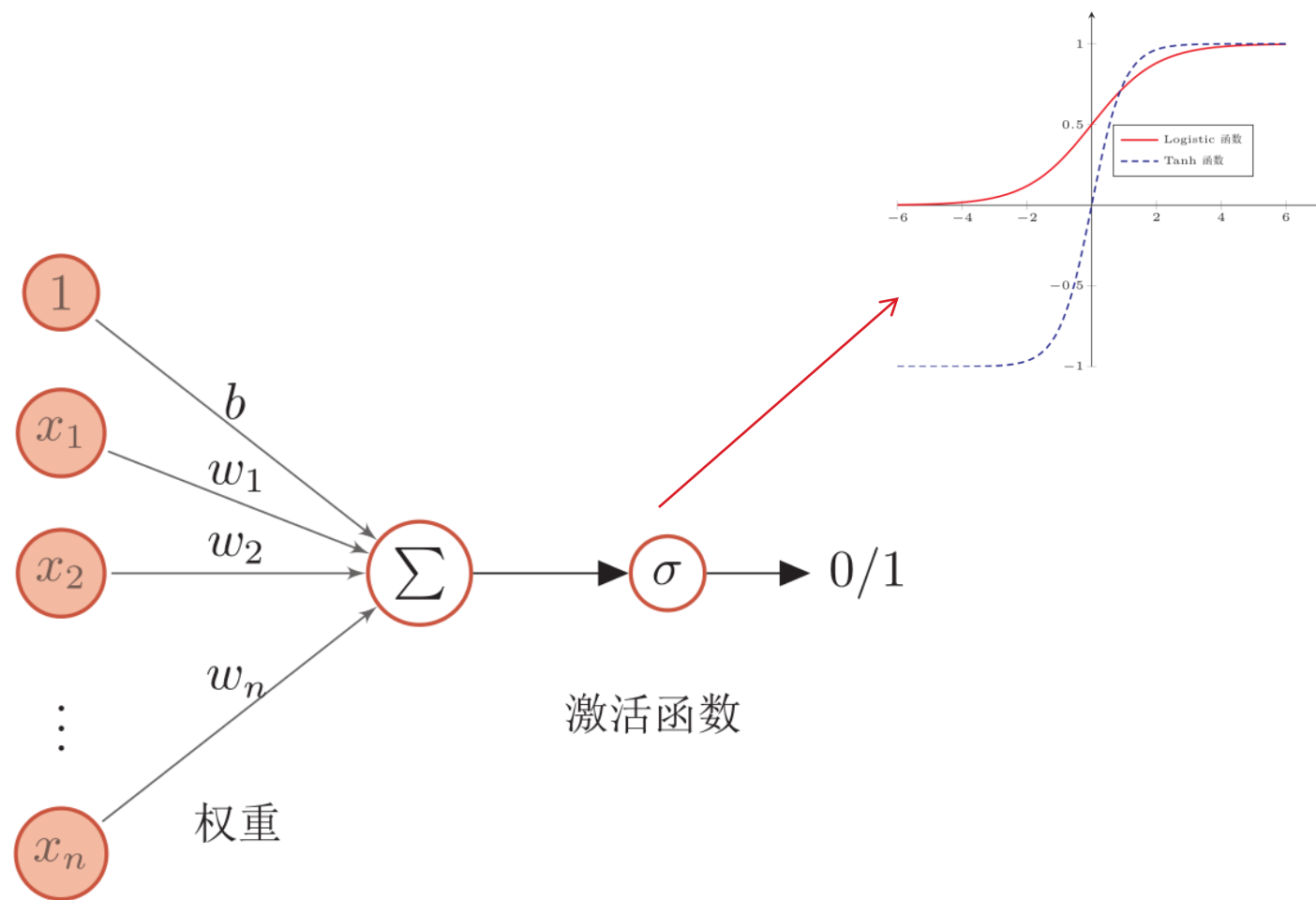
人脑有860亿个神经元

[video: structure of brain](#)



单个神经细胞只有两种状态：兴奋和抑制

# 人工神经元



# 神经网络如何学习？

---

## ▶ 赫布法则 Hebb's Rule

- ▶ “当神经元 A 的一个轴突和神经元 B 很近，足以对它产生影响，并且持续地、重复地参与了对神经元 B 的兴奋，那么在这两个神经元或其中之一会发生某种生长过程或新陈代谢变化，以致于神经元 A 作为能使神经元 B 兴奋的细胞之一，它的效能加强了。”

----加拿大心理学家 Donald Hebb,  
《行为的组织》，1949

- 人脑有两种记忆：**长期记忆**和**短期记忆**。短期记忆持续时间不超过一分钟。如果一个经验重复足够的次数，此经验就可储存在长期记忆中。
- 短期记忆转化为长期记忆的过程就称为**凝固作用**。
- 人脑中的海马区为大脑结构凝固作用的核心区域。

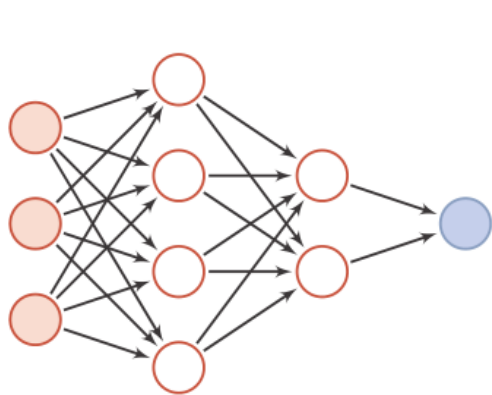
# 人工神经网络

---

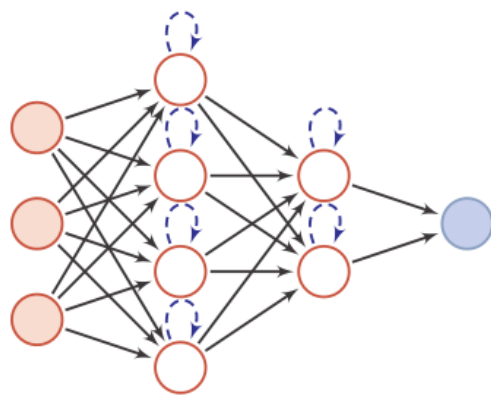
- ▶ 人工神经网络主要由大量的神经元以及它们之间的有向连接构成。因此考虑三方面：
  - ▶ 神经元的激活规则
    - ▶ 主要是指神经元输入到输出之间的映射关系，一般为非线性函数。
  - ▶ 网络的拓扑结构
    - ▶ 不同神经元之间的连接关系。
  - ▶ 学习算法
    - ▶ 通过训练数据来学习神经网络的参数。

# 人工神经网络

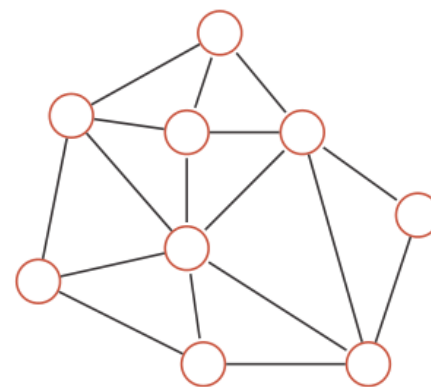
- ▶ 人工神经网络由神经元模型构成，这种由许多神经元组成的信息处理网络具有并行分布结构。
- ▶ 虽然这里将神经网络结构大体上分为三种类型，但是大多数网络都是复合型结构，即一个神经网络中包括多种网络结构。



(a) 前馈网络



(b) 记忆网络



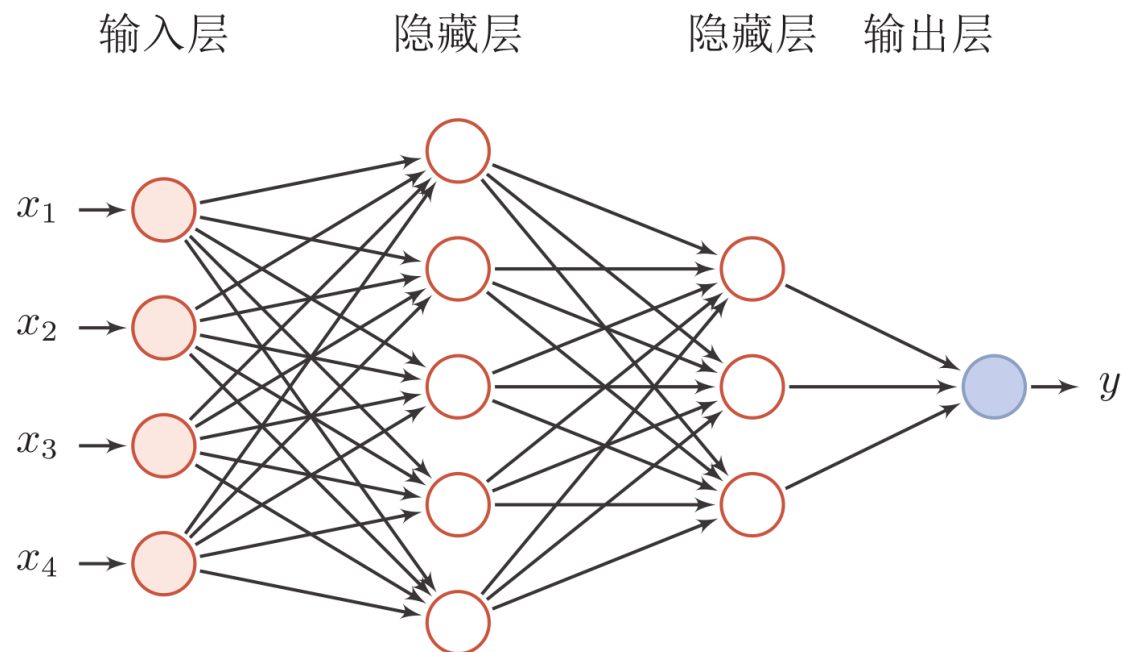
(c) 图网络



# 神经网络

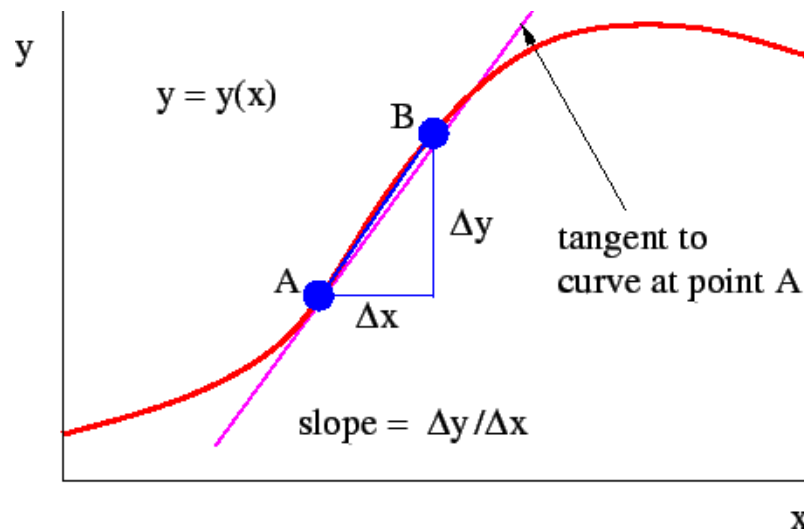
---

$$y = (f^3(f^2(f^1(x))))$$



# 如果解决贡献度分配问题？

## ► 偏导数



## ► 贡献度

$$\frac{\partial y}{\partial W^l} = \frac{y(W^l + \Delta W^l) - y(W^l)}{\Delta W^l}$$

神经网络天然不是深度学习，但深度学习天然神经网络。

# 深度学习三次热潮

---

## ▶ 第一次热潮（20世纪50年代-60年代）

- ▶ 1950年图灵提出了图灵测试
- ▶ 1958年计算机科学家Rosenblatt提出了一种具有三层网络特性的神经网络结构，成为“感知器”。
- ▶ 1969年，人工智能的先驱Minsky出版了一本名为《感知器》的书，书中指出简单的神经网络只能运用于线性问题的求解，能够求解非线性问题的网络应具有隐层，而从理论上还不能证明将感知器扩展到多层网络是有意义的。

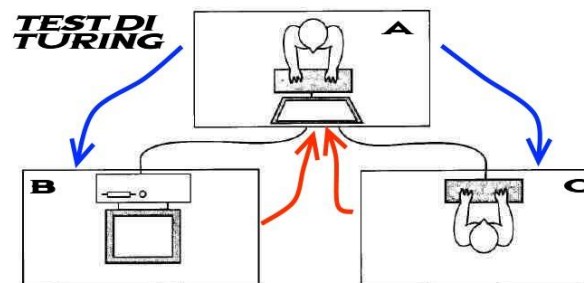
# 图灵测试

“一个人在不接触对方的情况下，通过一种特殊的方式，和对方进行一系列的问答。如果在相当长时间内，他无法根据这些问题判断对方是人还是计算机，那么就可以认为这个计算机是智能的”



Alan Turing

---Alan Turing [1950]  
《Computing Machinery and Intelligence》



GPT-4真的通过图灵测试了吗？

<https://arxiv.org/pdf/2310.20216.pdf>

# 深度学习三次热潮

---

## ▶ 第二次热潮（20世纪80年代-90年代）

- ▶ 1986年，Rumelhart, Hinton, Williams发展了BP算法。（多层感知器的误差反向传播算法）。
- ▶ 1987年6月，首届国际神经网络学术会议在美国加州圣地亚哥召开，到会代表有1600余人。之后国际神经网络学会和国际电气工程师与电子工程师学会（IEEE）联合召开每年一次的国际学术会议。
- ▶ 语音识别是当时最具代表性的突破成果之一，语音识别领域最具代表性的人物就是李开复了。

# 神经网络发展史

---

## ▶ 第三次热潮（2006年至今）

- ▶ 2006年Hinton在《Science》杂志上发表了—篇深度学习的论文。
- ▶ 2009年李飞飞创立ImageNet。
- ▶ 2016年AlphaGo战胜人类顶级围棋选手。
- ▶ 2022年的聊天机器人chatGPT。

# 常用的深度学习框架

---

- ▶ 简易和快速的原型设计
- ▶ 自动梯度计算
- ▶ 无缝CPU和GPU切换



# Python安装方法

---

- ▶ 先安装Anaconda

- ▶ 下载地址

- ▶ <https://mirrors.tuna.tsinghua.edu.cn/anaconda/archive/>
- ▶ [Anaconda3-2020.11-Windows-x86\\_64.exe](#)
- ▶ 安装的时候需要打勾的地方就打勾



# Tensorflow安装步骤

---

- ▶ 1.Windows用户先安装 VC\_redist.x64.exe 文件
- ▶ 2.管理员方式打开命令行，然后运行：
  - ▶ `pip install wrapt --upgrade --ignore-installed`
- ▶ 3. 然后再运行
  - ▶ `pip install tensorflow-cpu==2.12.0 -i https://pypi.tuna.tsinghua.edu.cn/simple --user`
  - ▶ 如果没有出现错误说明安装成功
  - ▶ （安装的过程中所出现的错误或警告信息全部可以忽略）
- ▶ `pip install numpy==1.22.0 -i https://pypi.tuna.tsinghua.edu.cn/simple --user`

# 编程练习

---

## ▶ 编程练习

### ▶ 熟悉基本的Numpy操作

▶ Numpy是Python中对于矩阵处理很实用的工具包

▶ <https://github.com/nndl/exercise>

▶ [chap1\\_warmup](#)