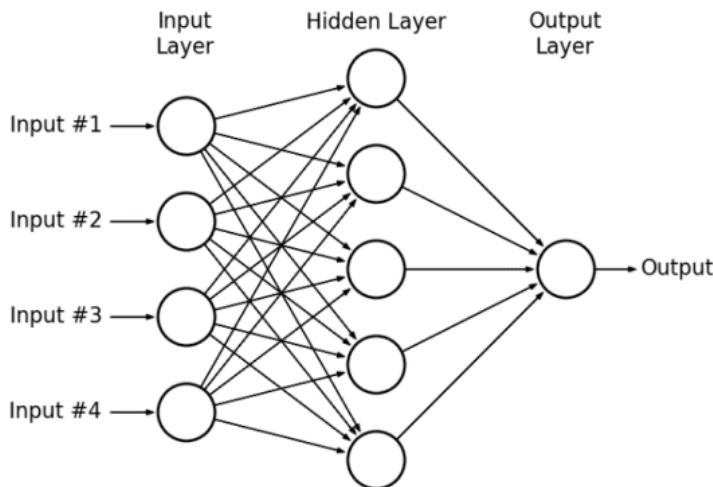


# Lecture1 Introduction to Deep Learning

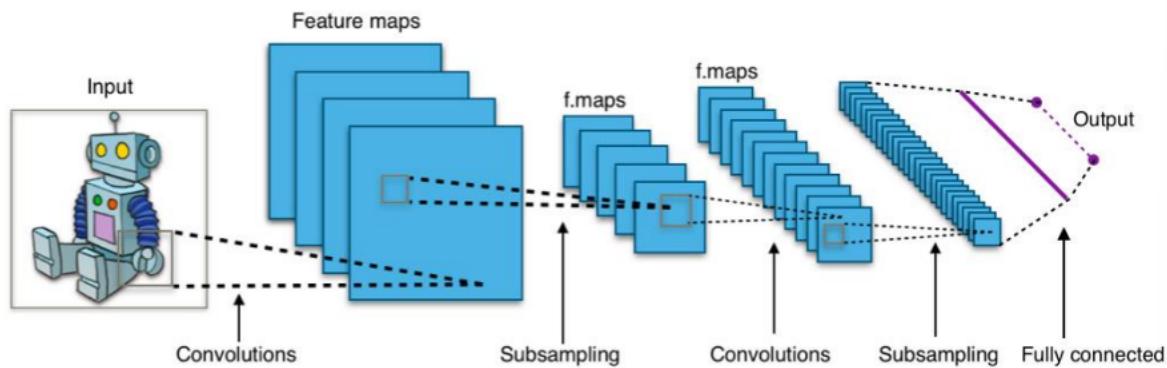
## 1. 课程介绍

课程讨论的主题

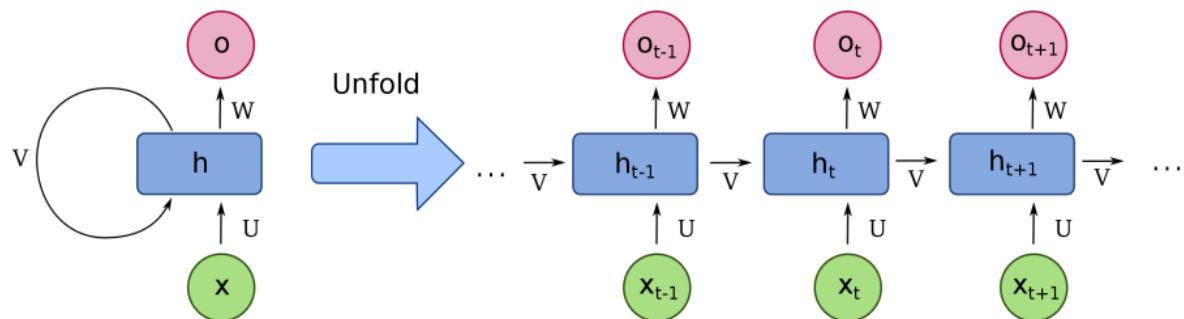
多层感知机 Multi-layer perceptron MLPs



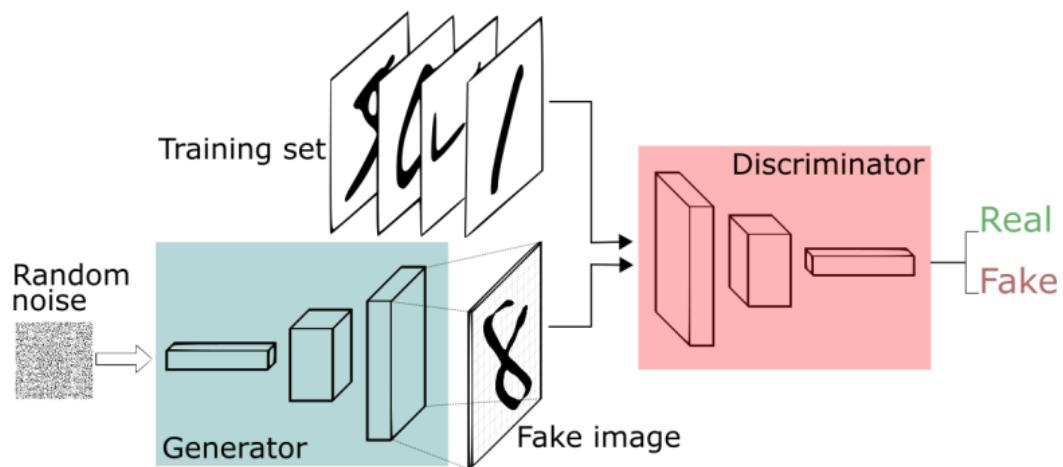
卷积神经网络 Convolutional neural networks (CNNs)



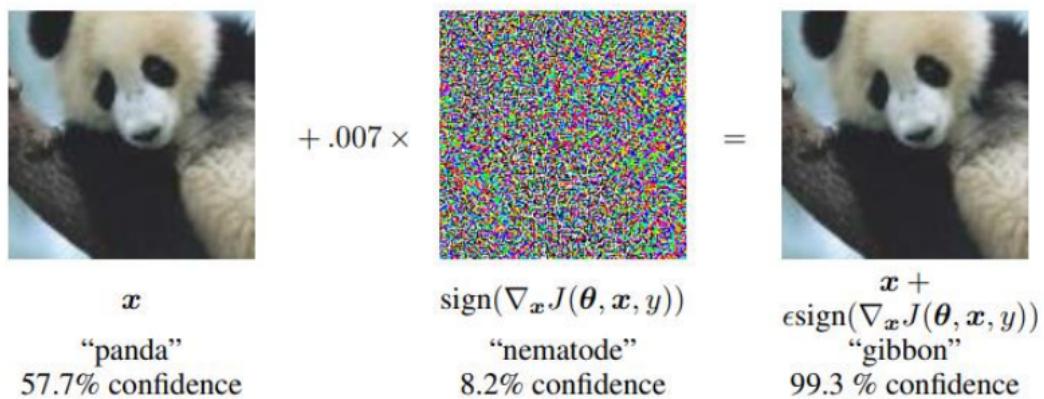
循环神经网络 Recurrent neural networks (RNNs)



## 生成式对抗神经网络 Generative adversarial networks (GANs)



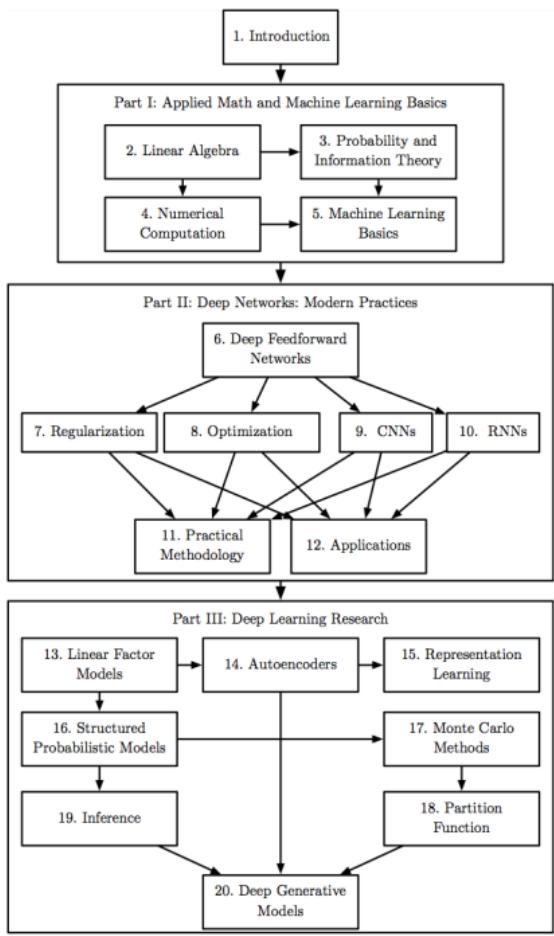
## 对抗性学习 Adversarial Learning



## 深度学习在图论中的研究 Deep learning on graphs



## 课程安排介绍



Lecture	Lab
课程概述 course overview lecture 和 lab 安排 information on lecture & labs schedule 评估结构和规则 assessments structure and rules 什么是深度学习 what is deep learning 你为什么在这里 why are you here	Pytorch 简介和任务概述
简单回顾线性代数, 张量 brief recap of linear algebra; tensors 机器学习简史和基本概念概述 brief history of machine learning and recap of fundamental concepts 生物神经元 biological neurons 感知器 the perceptron	Assignment1 (MLP和反向传播)
浅层网络和隐层 shallow networks and the hidden layer 多层感知器 multi-layer perceptron 梯度下降法 gradient descent 反向传播 back-propagation	Assignment1
批处理梯度下降 batch gradient descent 随机梯度下降法 stochastic gradient descent 在优化的挑战 challenges in optimization 先进的技术 advanced techniques	Assignment1
输入规范化 input normalization l1 和 l2 正则化 l1 and l2 regularization 参数消失 dropout 学习率 learning rate 权重初始化 weight initialization	Assignment1
CNN 是什么?是什么让它们与众不同 what are CNNs and what makes them special CNN 在计算机视觉中的重要性 CNN 模型 CNNs modules 如何训练一个 CNN 网络 how to train a CNN	Assignment2 (CNNs 和 RNNs)
流行的现代 CNN 架构 popular modern CNNs architectures 梯度消失 vanishing gradients 生成模型 inception model	Assignment2
霍普菲尔网络 Hopfield network 序列数据 sequential data RNNs 通过时间的反向传播 backpropagation through time 梯度爆炸和梯度消失 exploding and vanishing gradients LSTM 架构 LSTM architectures	Assignment2
文献阅读和期中展示	Paper reading and middle-term presentation

Lecture	Lab
监督学习和非监督学习 supervised versus unsupervised learning	
流形假设 manifold hypothesis	
主成分分析 PCA, kernel PCA	Assignment2
自动编码器 auto-encoders	
生成模型与区别模型 generative vs discriminative models	
生成对抗网络 generative adversarial networks	Assignment3 (GANs 和 VAEs)
GAN 的变种 variants of GANs	
有限玻尔兹曼机 restricted Boltzmann machines	
深度玻尔兹曼机 deep Boltzmann machines	Assignment3
变分推断 variational inference	
变分自动编码器 variational auto-encoders	
深度神经网络的安全问题 the safety issues of deep net	
为什么深度神经网络轻易被欺骗 why deep net can be easily fooled	
生成对抗样本 generating adversarial examples	Assignment3
不同的攻击方法 different attack methods	
防御方法 defense	
基于图的学习和神经网络 graph-based learning and neural networks	
基于图的学习和基于向量的学习 graph-based vs vector-based learning	
优点和缺点 advantages and problems	Assignment3
基于图数据的深度学习 deep learning on graph data	
图 CNN graph CNNs	
文献报告 paper presentation	
复习和 QA revision, Q&A	复习

## 成绩评定

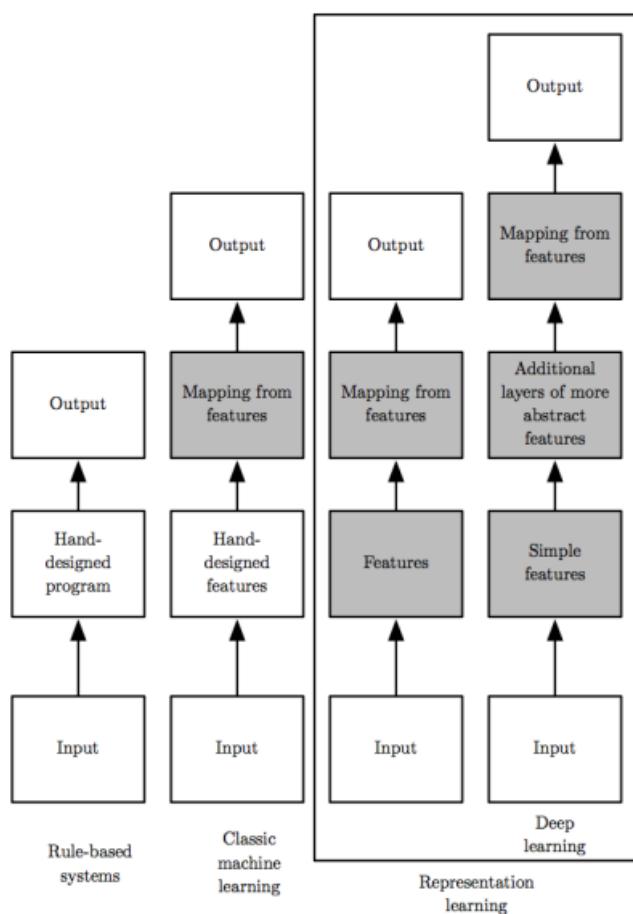
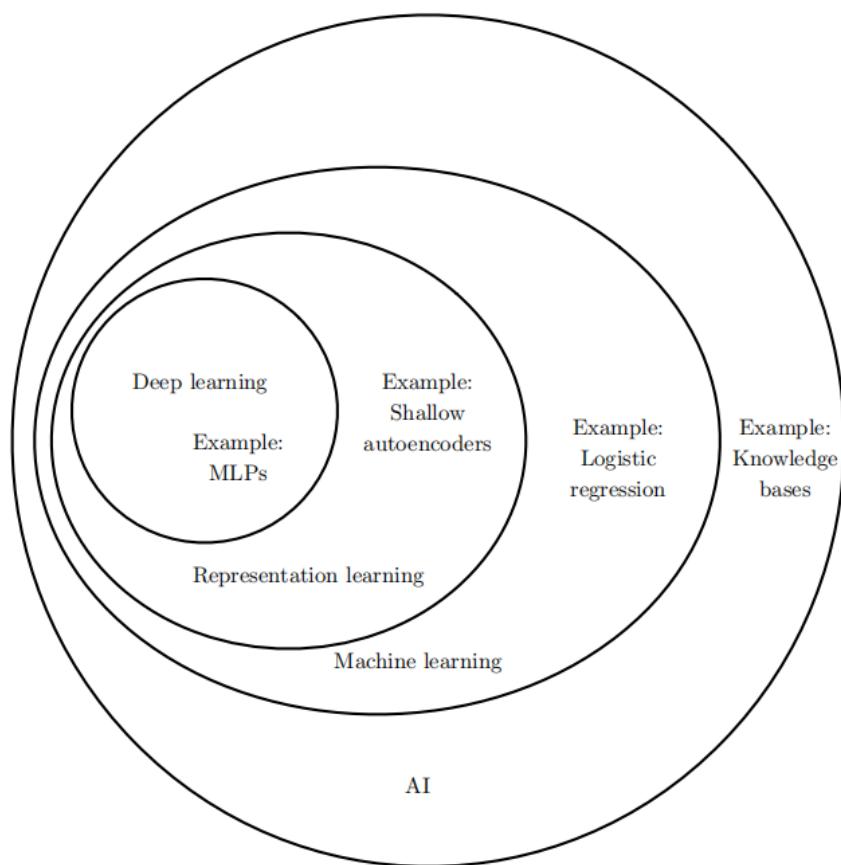
- 3 次实践作业 - 45% (每一次 15%)
- 期中文献阅读 Presentation - 10%
- 期末考试 25%
- 期末 Project Demo AI on Chips 10%

## 教材

- Goodfellow, Ian, Yoshua Bengio, Aaron Courville, and Yoshua Bengio. Deep learning. Vol. 1. Cambridge: MIT press, 2016. <https://www.deeplearningbook.org/>
- Chollet, Francois. Deep learning with python. Manning Publications Co., 2017
- Nielsen, Michael A. Neural networks and deep learning. Vol. 25. USA: Determination press, 2015.

## 2. 什么是深度学习

### 人工智能的范围介绍



- 流程图展示了 AI 系统的不同部分如何在不同的 AI 学科中彼此相关
- 阴影框表示能从数据中学习的组件

## 人工智能 Artificial Intelligence

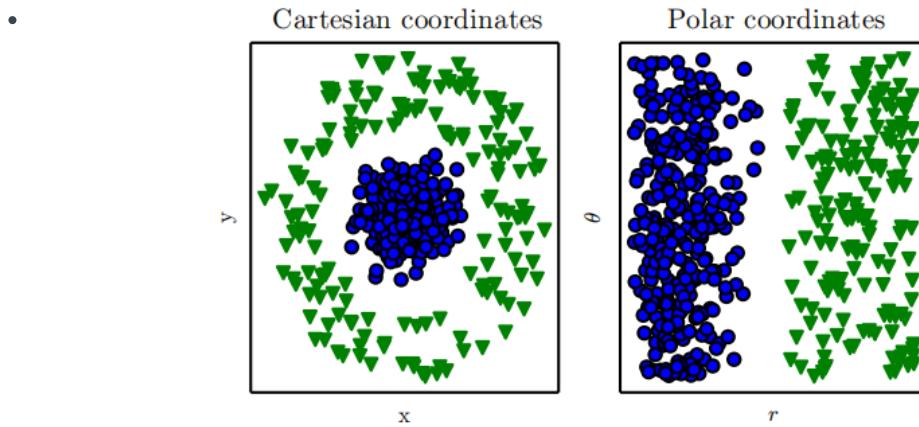
我们希望通过智能软件自动地处理常规劳动、理解语音或图像、帮助医学诊断和支持基础科学的研究

- 早期的时候，对人类来说**计算困难**，但对计算机来说**相对简单的问题**得到迅速解决（数学规则等）
- 人工智能的真正挑战在于解决那些对人来说**很容易执行、但很难形式化描述的任务**，如识别人们所说的话或图像中的脸
- **知识库 Knowledge Base**：一些人工智能项目力求将关于世界的知识用形式化的语言进行**硬编码**，计算机可以使用**逻辑推理规则**来自动地理解这些形式化语言中的声明

## 机器学习 Machine Learning

AI 系统需要具备**自己获取知识**的能力，即**从原始数据中提取模式**的能力，这种能力被称为**机器学习**

- 一些简单的机器学习算法的性能在很大程度上依赖于给定数据的**表示 (representation)**
  - **逻辑回归 Logistic Regression**：一种简单的机器学习算法，可以用于推理是否建议剖腹产
    - 医生需要告诉系统几条信息：如是否存在子宫疤痕
    - 表示患者的每条信息被称为一个**特征**
  - **朴素贝叶斯 Naïve Bayes**：一种朴素的机器学习算法，可以区分垃圾电子邮件和合法电子邮件



- 假设我们想在散点图中画一条线来分隔两类数据
  - 左图：笛卡尔坐标（无法完成）
  - 右图：极坐标（可以垂直简单解决这个任务）

## 表示学习 Representation Learning

许多人工智能任务都可以通过以下方式解决：**先提取一个合适的特征集，然后将这些特征提供给简单的机器学习算法**，然而，对于许多任务来说，**很难知道应该提取哪些特征**

使用机器学习**来发掘表示本身，而不仅仅把表示映射到输出**，这种方法称之为**表示学习**

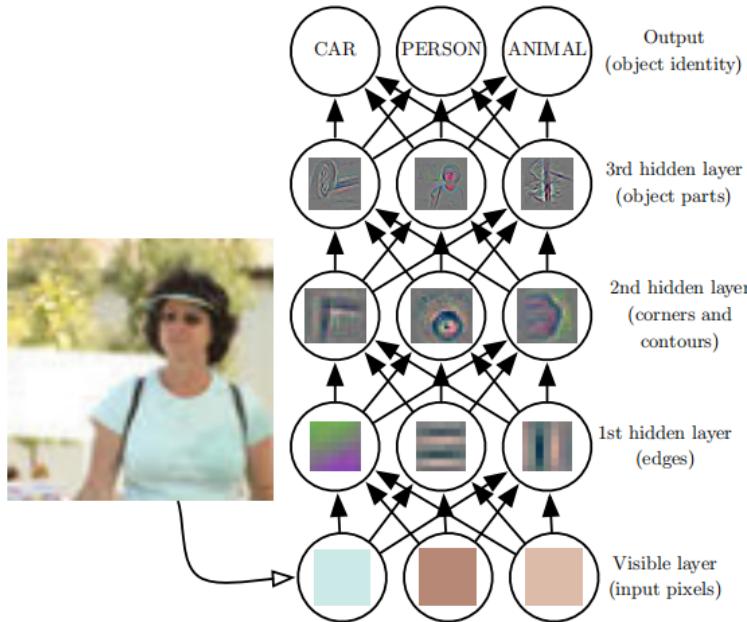
- **自编码器 autoencoder**：由一个**编码器 (encoder)** 函数和一个**解码器 (decoder)** 函数组合而成
  - 编码器：将输入数据转换成一种不同的**表示**
  - 解码器：将这个新的表示转换成原来的形式
  - 期望输入数据经过编码器和解码器之后**尽可能多地保留信息**，同时希望新的表示有各种好的特性

## 深度学习 Deep Learning

计算机难以理解原始感观输入数据的含义，很难通过这种方式自动从原始数据中提取出来，如表示为像素值集合的图像，将一组像素映射到对象标识的函数非常复杂，如果直接处理，学习或评估此映射似乎是不可能的

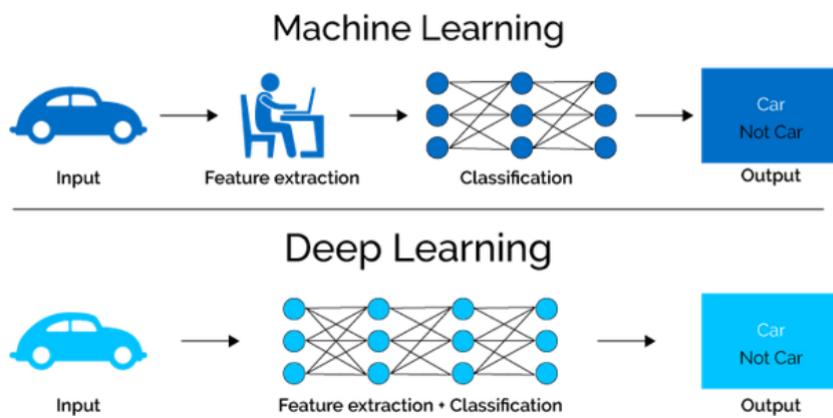
深度学习让计算机通过较简单概念构建复杂的概念

- **多层感知机 MultiLayer Perception**: 是一个将一组输入值映射到输出值的数学函数，该函数由许多较简单的函数复合而成



- **可见层 visible layer**: 输入，它包含我们能观察到的变量
- **隐藏层 hidden layer**: 从图像中提取越来越多抽象特征，因为它们的值不在数据中给出，所以将这些层称为“隐藏”

深度学习与机器学习的区别

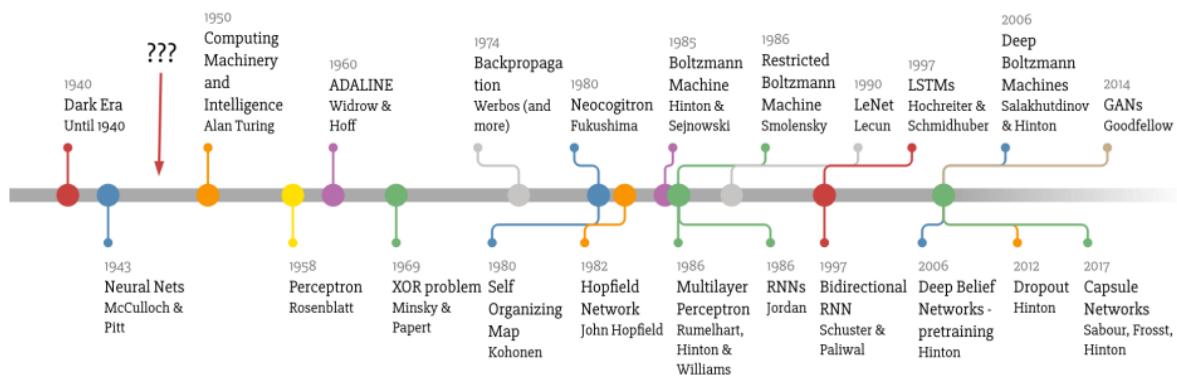


- 深度学习不仅学习映射，还学习特征的提取与表示

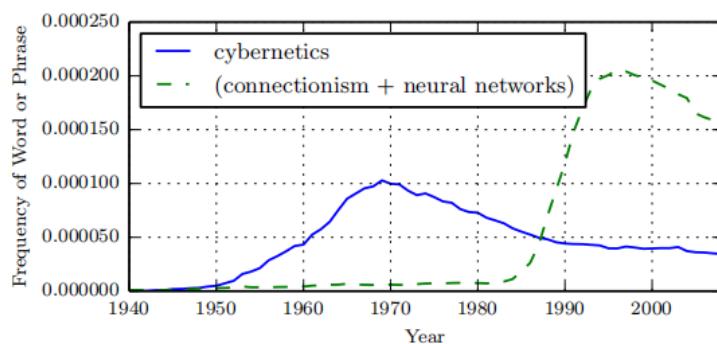
# 深度学习历史变迁

- 深度学习有着悠久而丰富的历史，与之对应的名称也渐渐尘封
- 随着可用的训练数据量不断增加，深度学习变得更加有用
- 针对深度学习的计算机软硬件基础设施都有所改善，深度学习模型的规模也随之增长
- 深度学习已经解决日益复杂的应用，并且精度不断提高

## 名称和命运变迁



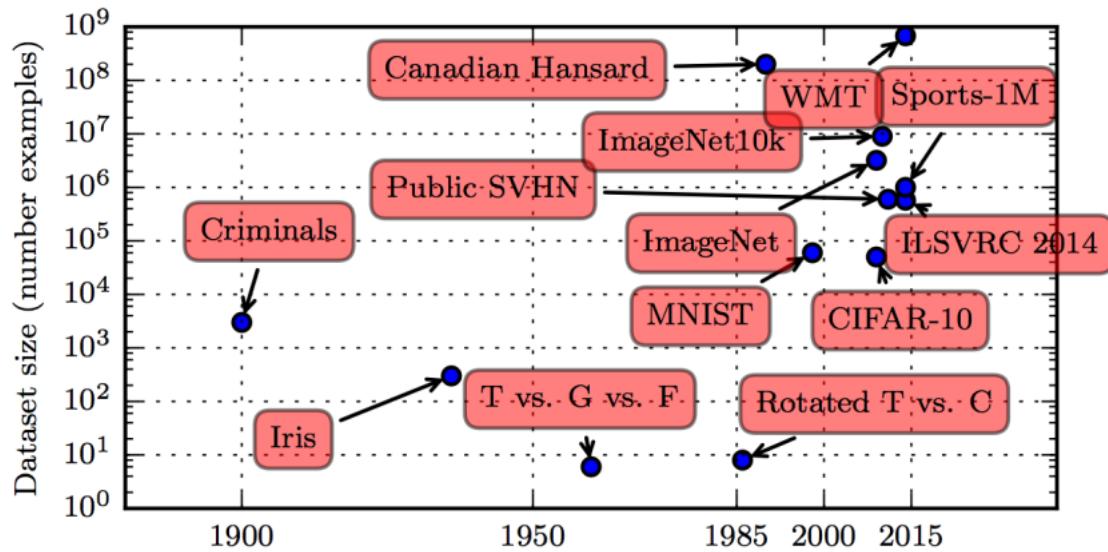
目前深度学习经历了三次发展浪潮



- 控制论 (cybernetics)** : 20世纪40年代到60年代
  - 随着生物学系理论的发展，和第一个模型（感知机）的实现，能实现**单个神经元**的训练
- 联结主义 (connectionism)** : 20世纪80年代到90年代
  - 可以使用**反向传播**训练具有**一两个隐藏层的神经网络**
- 深度学习 (deep learning)** : 2006年后
  - 超越了目前机器学习模型的神经科学观点，重心放在**学习多层次组合**这一更普遍的原理

## 数据规模变迁

深度学习是对大数据的渴望，更多的数据，更好的模型



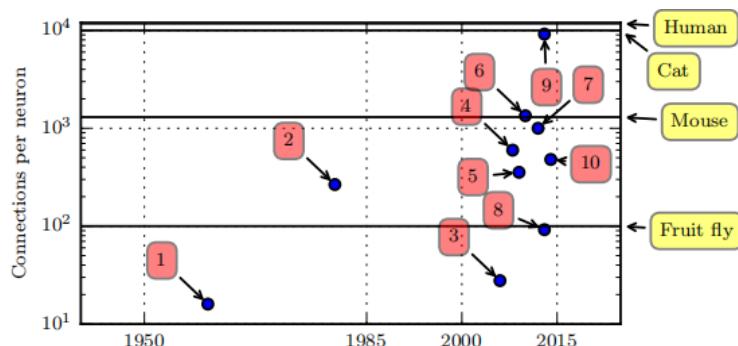
- 20世纪初：统计学家使用数百或数千的手动制作的度量来研究数据集
- 1950 - 1980：受生物启发的机器学习开拓者通常使用小的合成数据集
- 1980 - 1990：机器学习变得更加统计，并开始利用包含成千上万个样本的更大数据集
  - 如手写扫描数字的 MNIST 数据集
- 2000 - 2010：相同大小更复杂的数据集持续出现，
  - CIFAR-10 数据集
- 2010 - 2015：明显更大的数据集（包含数万到数千万的样例）完全改变了深度学习的可能实现的事
  - 公共 Street View House Numbers 数据集
  - ImageNet 数据集
  - Sports-1M 数据集
  - IBM 数据集
  - WMT 2014 英法数据集

## 模型规模变迁

现在神经网络非常成功的另一个重要原因是我们现在拥有的**计算资源可以运行更大的模型**

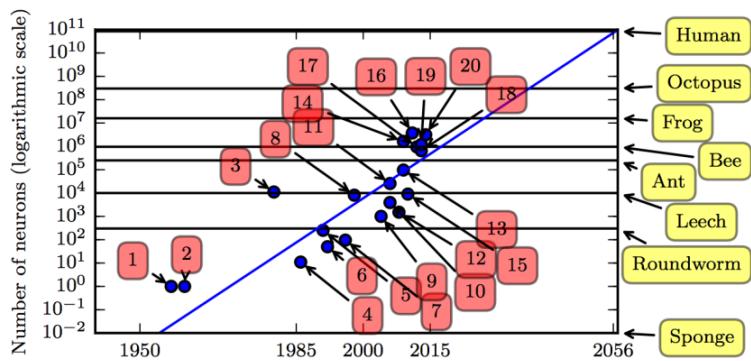
- 由于更快的 CPU、通用 GPU 的出现、更快的网络连接和更好的分布式计算的软件基础设施，模型规模随着时间的推移不断增加

神经元连接数的增加



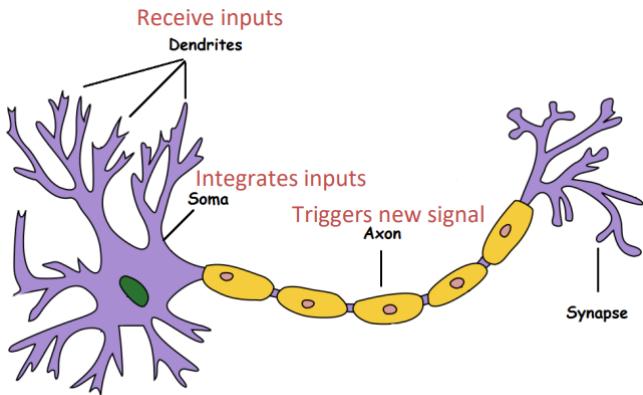
- 机器学习模型中每个神经元的连接数量已经与哺乳动物的大脑在同一数量级上

神经元（神经网络规模）的增加



## 深度学习的演变

### 控制论 Cybernetics

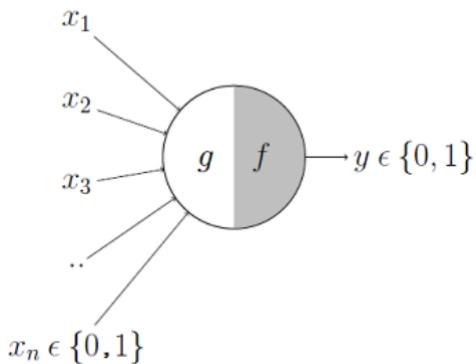


深度学习最早前身为从神经科学角度出发的简单线性模型

- 使用一组  $n$  个输入  $x_1, \dots, x_n$
- 将它们与一个输出  $y$  相关联
- 这些模型希望学习一组权重  $w_1, \dots, w_n$
- 并且计算它们的输出  $f(\mathbf{x}, \mathbf{w}) = x_1 w_1 + \dots + x_n w_n$

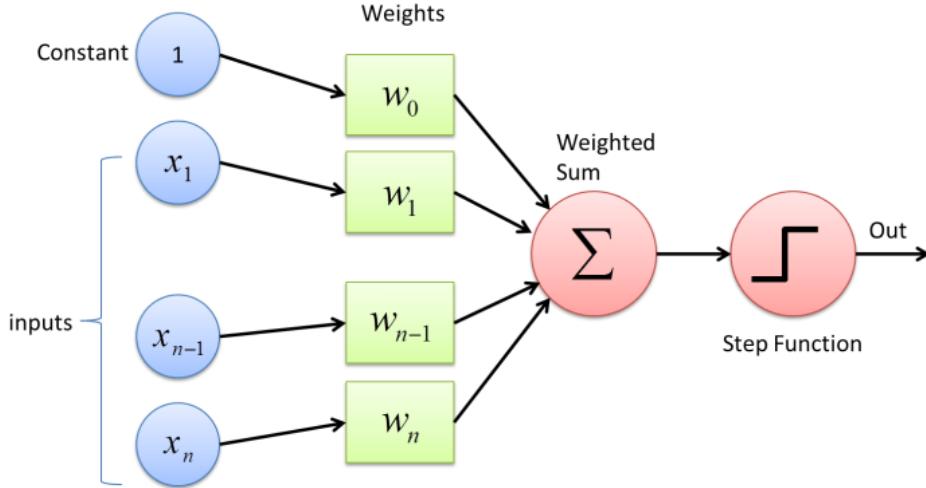
随后，出现了感知机 (Perceptron)，自适应线性单元 (Adaptive Linear Element., ADALINE)

- McCulloch Pitts 神经元是脑功能的早期模型，通过检验函数  $f(\mathbf{x}, \mathbf{w})$  来识别不同类别的输入



- 模型的权重需要人工设定

- 感知机成为第一个根据每个类别的输入样本来学习权重的模型



- 主要的创新是学习算法

1. 从随机的权重开始
2. 输入一个样本  $x_i = [x_{i1}, \dots, x_{in}]$  然后预测  $\hat{y}_i$
3. 如果  $\hat{y}_i = 0$  但是样本标签  $y_i = 1$ , 那么减少权重
4. 如果  $\hat{y}_i = 1$  但是样本标签  $y_i = 0$ , 那么增加权重
5. 重复上述流程直到收敛

基于感知机和 ADALINE 中使用的函数  $f(\mathbf{x}, \mathbf{w})$  的模型被称为**线性模型 linear model**

- 目前仍是最广泛使用的机器学习模型
- 线性模型有很多局限性, 最著名的是, 它们**无法学习异或函数**

## 联结主义 Connectionism

联结主义, 或者**并行分布处理 (parallel distributed processing)**, 是在认知科学的背景下出现的, 它的中心思想是, **当网络将大量简单的计算单元连接在一起时可以实现智能行为**

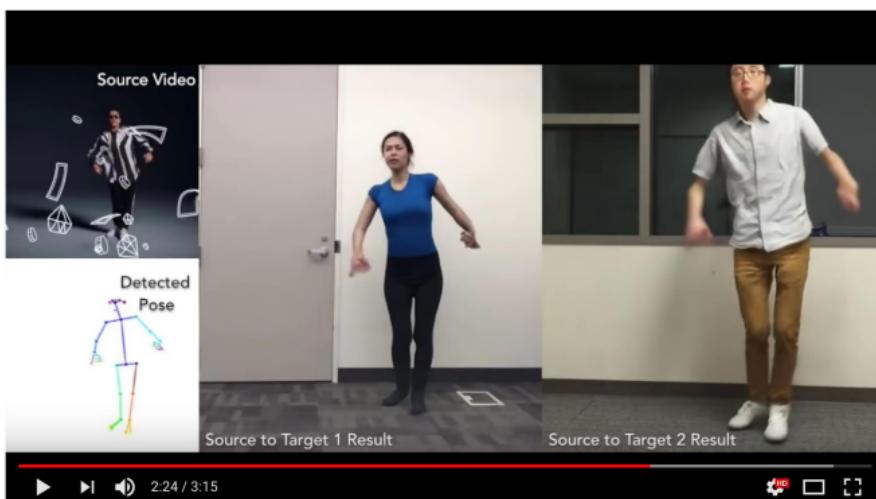
联结主义期间形成的几个关键概念在今天的深度学习中仍然是非常重要

- **分布式表示:** 系统的每一个输入都应该由多个特征表示, 并且每一个特征都应该参与到多个可能输入的表示
- **反向传播:** 训练具有内部表示的深度神经网络中的成功

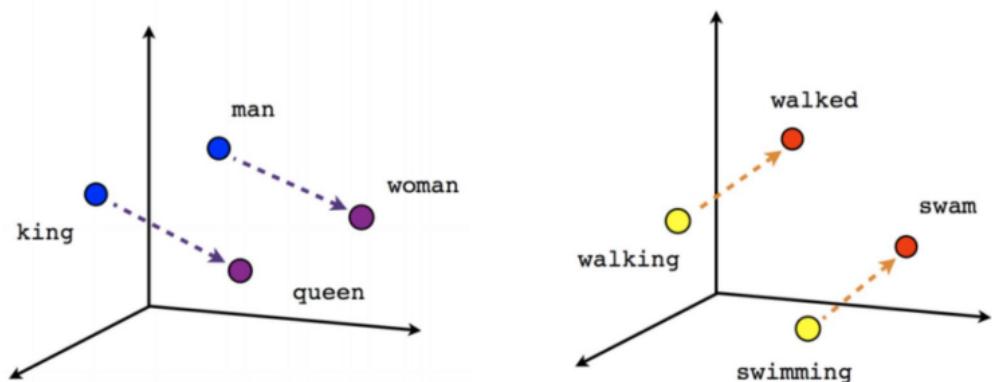
## 深度学习的应用

CV

## Pose-to-Body Results



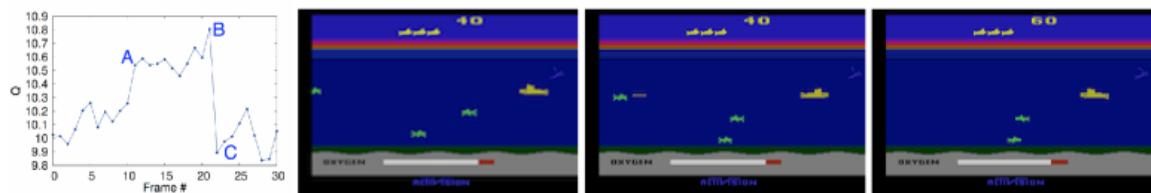
NLP



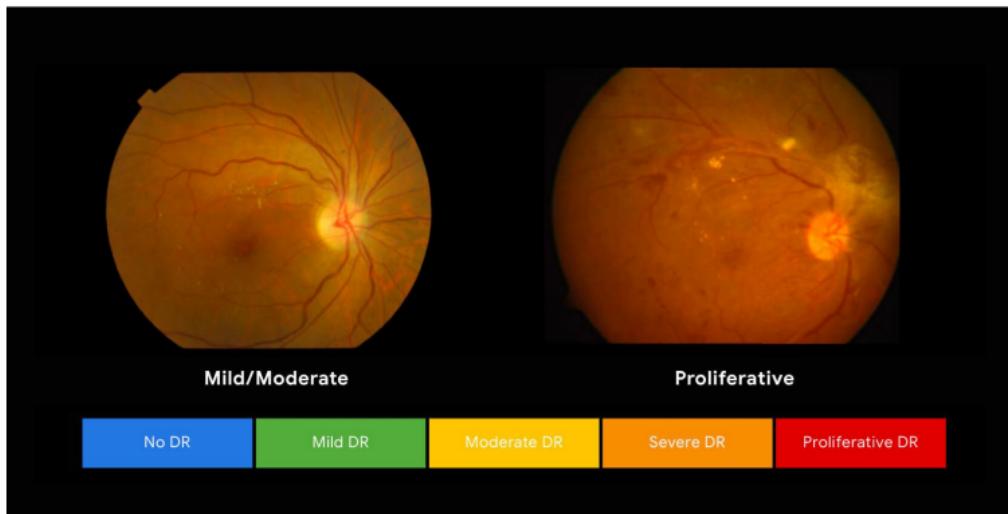
Male-Female

Verb tense

## 游戏



## 医疗



## 视频



## 美术

