《人工智能通识》（科技素养）

第3讲 机器学习基础

主讲：丛润民

章节知识点概览

知识点1：机器学习——数据与经验的转化大师

知识点2：模型封神榜

知识点3：织就认知的“深层脉络”——深度学习

知识点4：在试错中成长——强化学习

知识点5：打造数据的“社交圈”——图学习

知识点6：数据孤岛的破局者——联邦学习

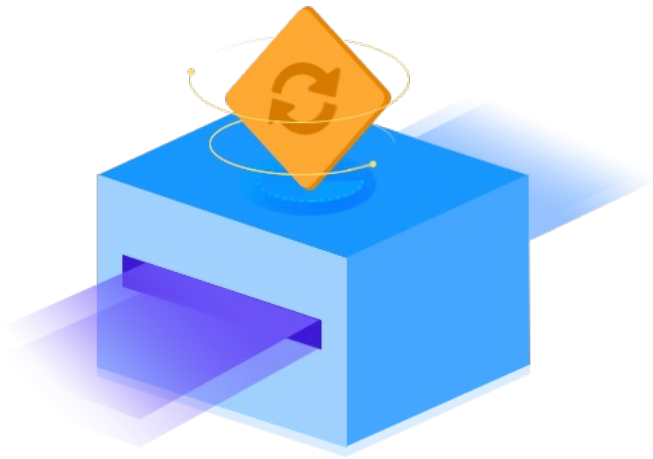
知识点7：让模型举一反三——迁移学习

知识点1：
机器学习——数据与经验的转化大师

01 知识表示方法

02 逻辑关系与规则

知识点目录



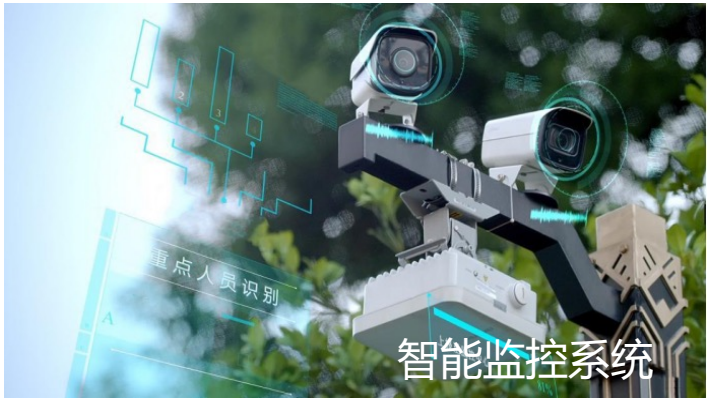
智能生活的新引擎——机器学习

- **机器学习（Machine Learning）**是人工智能领域的核心分支之一。
- 目标：让计算机从数据中自动发现规律（模式），并基于此对未知数据进行预测或决策。
- 方法：通过算法解析大量数据，从中学习并建立一个能够进行预测或分类的模型（Model）。


萝卜快跑无人出租车


人脸识别系统


四足机器人


智能监控系统

案例引入——房价预测模型

10万

20万

？万

数据（经验）

↓ **学习算法**

模型（知识和规律）

房价预测案例

案例引入——房价预测模型

街道类型

建造年份

实际房价

构造数据集

特征（Feature）

标签（Label）

街道类型	建造年份	实际房价
商业街	2003	10
商业街	2023	20
普通街区	2010	10
…	…	…

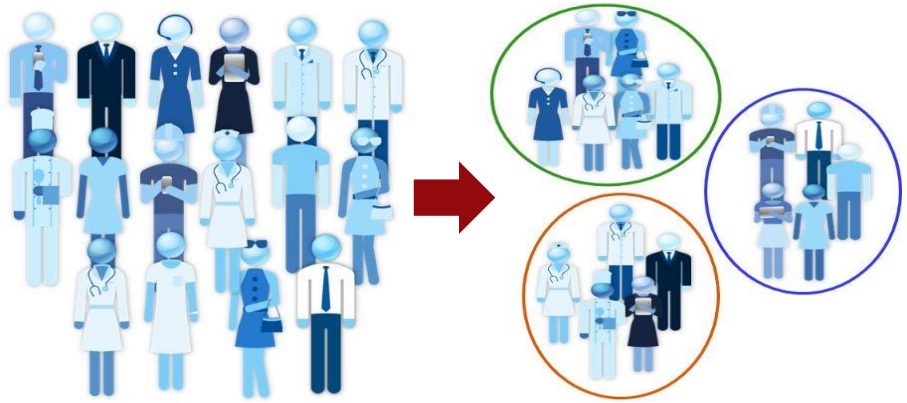
样本（Sample）

监督学习 vs. 无监督学习

学习过程是否提供标签

监督学习（Supervised Learning）： 利用一组已知输入和对应标签的数据集来训练模型，使模型能够学习到一个从输入到输出的映射关系

无监督学习（Unsupervised Learning）： 直接对这些未标注数据进行建模分析，以实现相应的学习任务



推荐系统示例

分类任务 vs. 回归任务

标签的属性类型

回归任务（Regression Task）： 模型实现对连续数值的预测，**定量预测**

房价值预测、气温预测、股市走势预测

分类任务（Classification Task）： 模型实现对离散数值的预测，**定性预测**

房价的高/低、预测明天是/否降雨、股市的涨/跌趋势

- 实际上，分类模型与回归模型在底层逻辑上存在**共通之处**，通过适当调整，某些经典算法能够灵活应用于两类任务之中。

知识点小结

- 机器学习
- 学习算法
- 模型
- 数据集
- 特征
- 标签
- 样本

学习过程是否提供标签
- **监督学习（Supervised Learning）**
- **无监督学习（Unsupervised Learning）**
  K-means聚类

标签的属性类型
- **回归任务（Regression Task）**
  线性回归
- **分类任务（Classification Task）**
  支持向量机（SVM）

回归任务：线性回归

- 线性回归的基本思想是通过找到**最佳拟合直线**来模拟因变量和自变量之间的关系。

街道类型	建造年份	实际房价
0001	2003	10
0001	2023	20
0100	2010	10
…	…	…
x_1	x_2	y

- **特征：** $\boldsymbol{x} = [x_1, x_2]^T$
- **标签：** y

$$\hat{y} = w_1 \cdot x_1 + w_2 \cdot x_2 + b$$

- **权重：** $\boldsymbol{w} = [w_1, w_2]^T$
- **偏置：** b

回归任务：线性回归

进一步地，我们将其推广至更一般的情况：

$$\hat{\boldsymbol{y}} = \boldsymbol{X}\boldsymbol{w} + \boldsymbol{b}, \boldsymbol{X} \in \mathbb{R}^{n\times d}, \hat{\boldsymbol{y}} \in \mathbb{R}^{n}, \boldsymbol{b} \in \mathbb{R}^{n}$$

损失：
衡量预测值和真实值之间的差异

y

- 将学习任务看作一个**最小值优化问题**

$$\{\boldsymbol{w}^*, \boldsymbol{b}^*\} = \underset{\boldsymbol{w},\boldsymbol{b}}{argmin}\, L(\boldsymbol{w}, \boldsymbol{b}) = \underset{\boldsymbol{w},\boldsymbol{b}}{argmin} \frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}(\hat{y}^i - y^i)^2$$

最小二乘法

$$= \underset{\boldsymbol{w},\boldsymbol{b}}{argmin} \frac{1}{2n}||\boldsymbol{y} - \boldsymbol{X}\boldsymbol{w} - \boldsymbol{b}||^2$$

① 生成增广权重向量

$$\hat{\boldsymbol{y}} = [\boldsymbol{X}, \boldsymbol{1}][\boldsymbol{w}, \boldsymbol{b}]^T = \hat{\boldsymbol{X}}\hat{\boldsymbol{w}}$$

采用简化的表示方法，直接用w和X来表示增广权重向量和增广特征矩阵：

$$\hat{\boldsymbol{y}} = \boldsymbol{X}\boldsymbol{w}$$

② 损失函数表示

$$\{\boldsymbol{w}^*, \boldsymbol{b}^*\} = \underset{\boldsymbol{w},\boldsymbol{b}}{argmin} \frac{1}{2n}||\boldsymbol{y} - \boldsymbol{X}\boldsymbol{w}||^2$$

关于w的凸函数

③ 求解解析解

回归任务：线性回归

■ 线性回归的优势：

- **模型简洁**，易于理解与实施
- **计算效率高**，特别适用于处理大规模数据集
- **强大的可解释性**赋予模型参数明确的统计含义，能够直观揭示特征对目标变量的影响机制

■ 线性回归的局限：

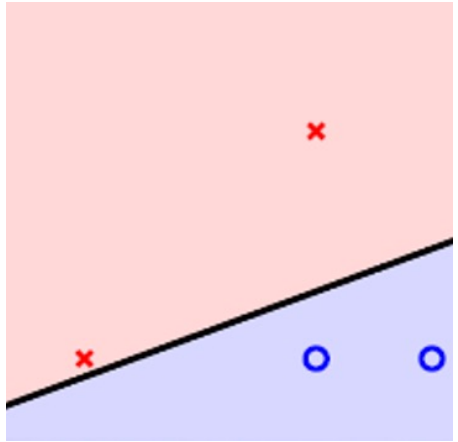
- 模型基于**特征与目标变量间线性关系的假设**在一定程度上限制了其捕捉复杂非线性关系的能力
- 模型**对异常值较为敏感**，可能影响参数估计的稳健性
- 当特征间存在多重共线性时，线性回归的参数估计可能变得**不稳定**

分类任务——支持向量机

街道类型	建造年份	实际房价
商业街	2003	10
商业街	2023	20
普通街区	2010	10
…	…	…
x_1	x_2	

- 房价 > 10：贵
- 房价 ≤ 10：便宜

房价评价
便宜（-1）
贵（1）
便宜（-1）
…
y



划分超平面

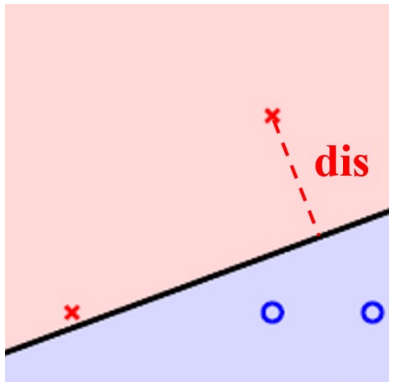
若能用一个超平面将D中两类不同数据完全隔开，则称样本数据集D为**线性可分**，该平面称为**划分超平面**

支持向量机（SVM）的**核心**是构建一个能够**最大化**两类样本**间隔**的超平面

分类任务——支持向量机

我们使用线性方程来描述**划分超平面**：　　$\boldsymbol{w}^T\boldsymbol{x}+b=0$

样本空间中任意点x_i到超平面的**距离公式**：　$dis=\dfrac{|\boldsymbol{w}^T\boldsymbol{x}_i+b|}{||\boldsymbol{w}||}$

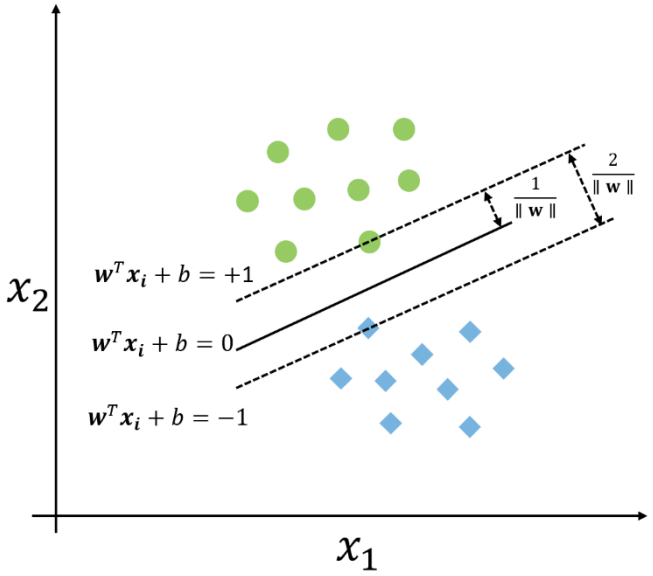


训练目标：

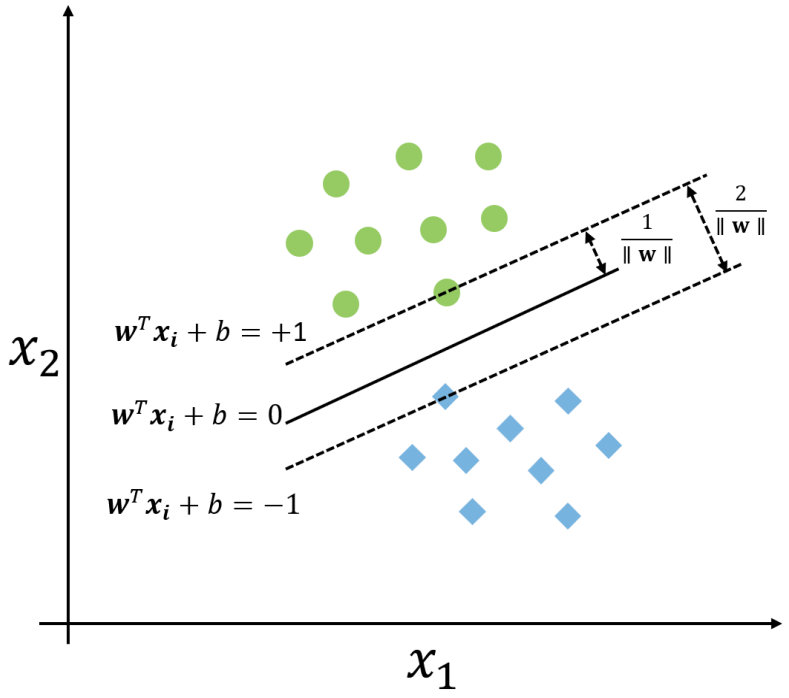
- $y_i=+1$时，即该房价较贵时，则$\boldsymbol{w}^T\boldsymbol{x}_i+b>0$
- $y_i=-1$时，即该房价较便宜时，则$\boldsymbol{w}^T\boldsymbol{x}_i+b<0$

这里，可以更严格一些：

$$\begin{cases}\boldsymbol{w}^T\boldsymbol{x}_i+b\geq+1, & y_i=+1\\ \boldsymbol{w}^T\boldsymbol{x}_i+b\leq-1, & y_i=-1\end{cases}$$



分类任务——支持向量机



$$\max_{w,b} \quad r = \frac{2}{||w||}$$
$$s.t. \quad y_i(w^T x_i + b) \geq 1, i = \{1,2,\ldots,m\}$$

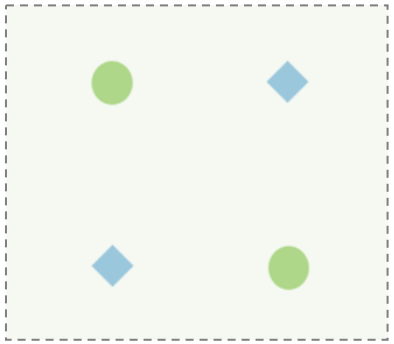
对偶

$$\min_{w,b} \quad \frac{1}{2}||w||^2$$
$$s.t. \quad y_i(w^T x_i + b) \geq 1, i = \{1,2,\ldots,m\}$$

拉格朗日乘子法

分类任务——支持向量机

x_1	x_2	y
0	0	0
1	0	1
0	1	1
1	1	1

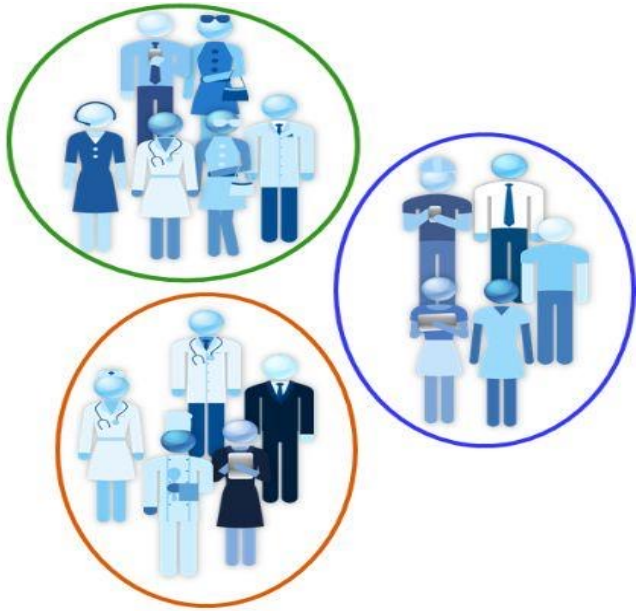


“异或”问题

面对线性不可分的分类任务：

- **面向软间隔的SVM：**允许少量训练样本被错分，而非要求所有训练样本都能被正确分类
  - 优势：很高效的解决了存在少量噪声但总体上可用划分超平面区分开的一类任务。
  - 局限：仍然对线性不可分数据集不能奏效。
- **基于核函数的方法：**通过将样本数据**映射到高维空间**，使得数据在高维空间中变得线性可分

无监督学习——K-means聚类



- **聚类技术**，它依据样本数据间的相似性，将数据划分为若干独立的子集，即“簇”，使得**同一簇内的样本高度相似，而不同簇间则差异显著。**

K-means算法的执行过程

① **初始化质心：**随机选择K个样本数据点作为初始的簇质心

② **分配簇：**计算每个样本数据点与各个簇质心的距离，将其分配给最近的簇

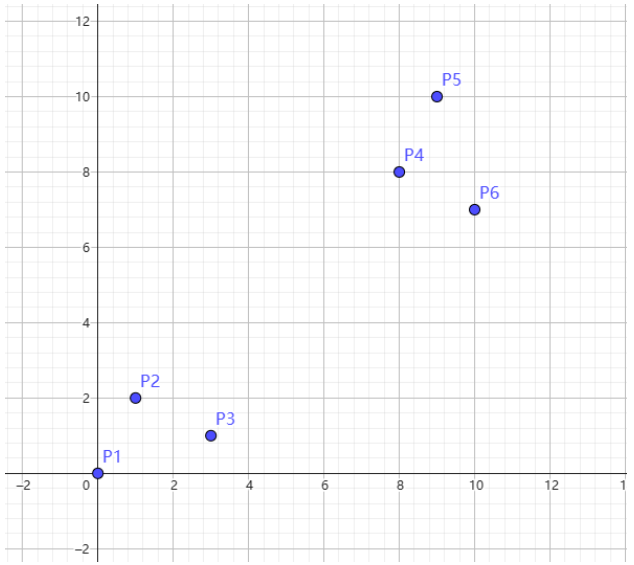
	C1	C2
P3	3.16	2.24
P4	11.3	9.22
P5	13.5	11.3
P6	12.2	10.3

- C1组：P1
- C2组：P2、P3、P4、P5、P6

③ **更新质心：**重新计算每个簇的质心，即取簇内所有样本数据点的平均值作为新的质心

C1: (0, 0)　　C2: (6.2, 5.6)

④ **迭代：**重复上述分配和更新步骤，直到满足某种终止条件（如簇质心不再发生显著变化或达到预设的迭代次数）

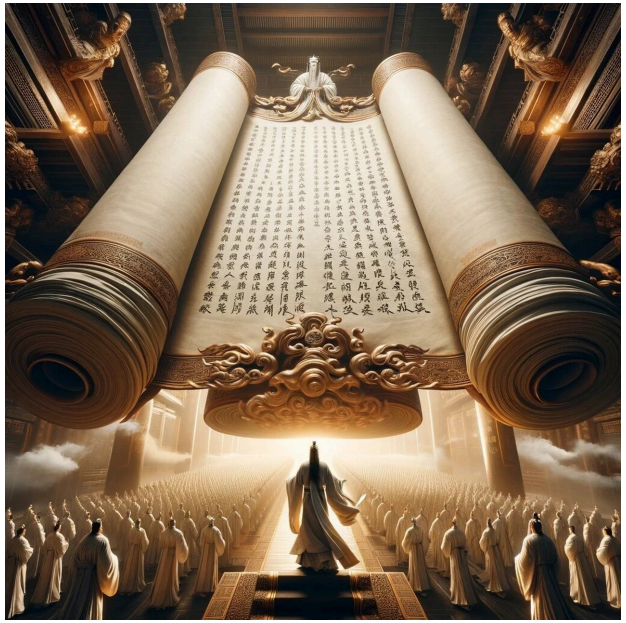


	X_1	X_2
P1	0	0
P2	1	2
P3	3	1
P4	8	8
P5	9	10
P6	10	7

无监督学习——K-means聚类

- **K-means聚类的优势：**
  - 直观性强
  - 计算高效
  - 实现简便
- **K-means聚类的局限：**
  - K-means算法的性能高度依赖于初始聚类中心的选择
  - 算法容易陷入局部最优解而无法达到全局最优
  - 不恰当的K值可能导致聚类结果无法真实反映数据的内在结构或实际需求

知识点2：模型封神榜



01 欠拟合与过拟合

02 数据集的划分

03 性能度量

欠拟合与过拟合

假设现在是期末周，两个同学均借助往年的考试题目来测试自己对知识点的掌握情况：

对历史过分精确和必然的解释，通常不是伟大或正确，而只是穿凿附会的谬误。

——Walski Manshi

- 欠拟合
- 过拟合

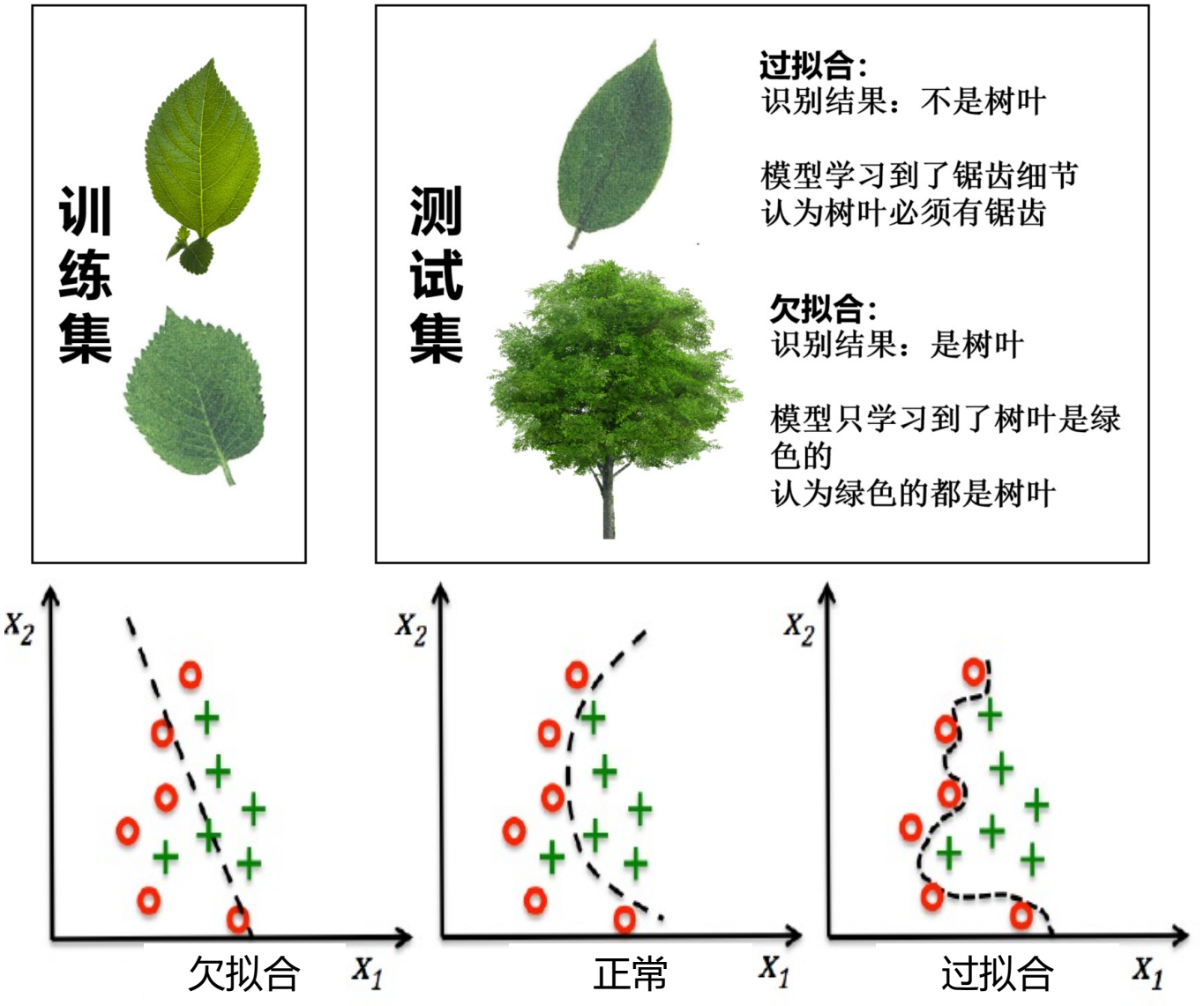
欠拟合与过拟合

- **欠拟合**通常发生在**模型复杂度不足**时，此时模型无法捕捉到数据中的基本模式，导致在训练集和测试集上的表现均不佳。

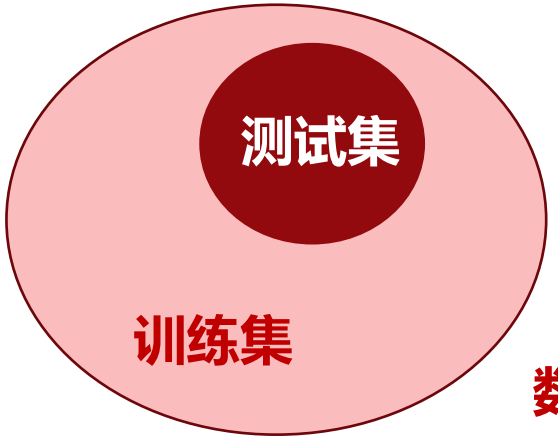
  更换复杂度更高的算法；继续训练

- **过拟合**是模型**复杂度过高**带来的副作用，模型虽然能完美拟合训练数据，却也因此学习了过多的噪声和细节，使得在测试集上的泛化能力大打折扣。

  正则化（过拟合无法从根本上消除，只能通过各种手段减轻其影响或降低其风险）



欠拟合与过拟合的解决之道



数据集

- **训练集**的样本用来训练模型
- **测试集**用来检验模型的性能，即利用学习得到的模型参数对测试样本进行预测，并通过评价指标评测预测结果与标签的接近程度

经验误差（训练误差）：模型在训练集上的误差

泛化误差（测试误差）：模型在新样本即测试集上的误差

	经验误差	泛化误差
欠拟合	大	大
过拟合	小	大

统计学习理论指出，若训练集与测试集的抽样完全随机无偏，直接提升模型泛化能力的手段有限；但若两者收集过程**遵循一定假设或规律**，则可据此设计更为有效的**评估策略**，从而增强模型的泛化能力。

数据集的划分

留出法（Hold-out Method）是一种直接且基础的数据集划分策略，它将原始数据集D明确划分为两个**互不重叠**的集合：**训练集S**与**测试集T**。在S上进行模型的训练过程，随后在T上评估其测试误差，以此作为对模型泛化能力的一种近似估计。

需要考虑的因素：

① **样本类别分布**上应保持一致性，以避免因分布偏差导致的误差估计失真。

② 合适的划分比例。

D中包含600个正样本和400个负样本，采用3:1的比例划分：

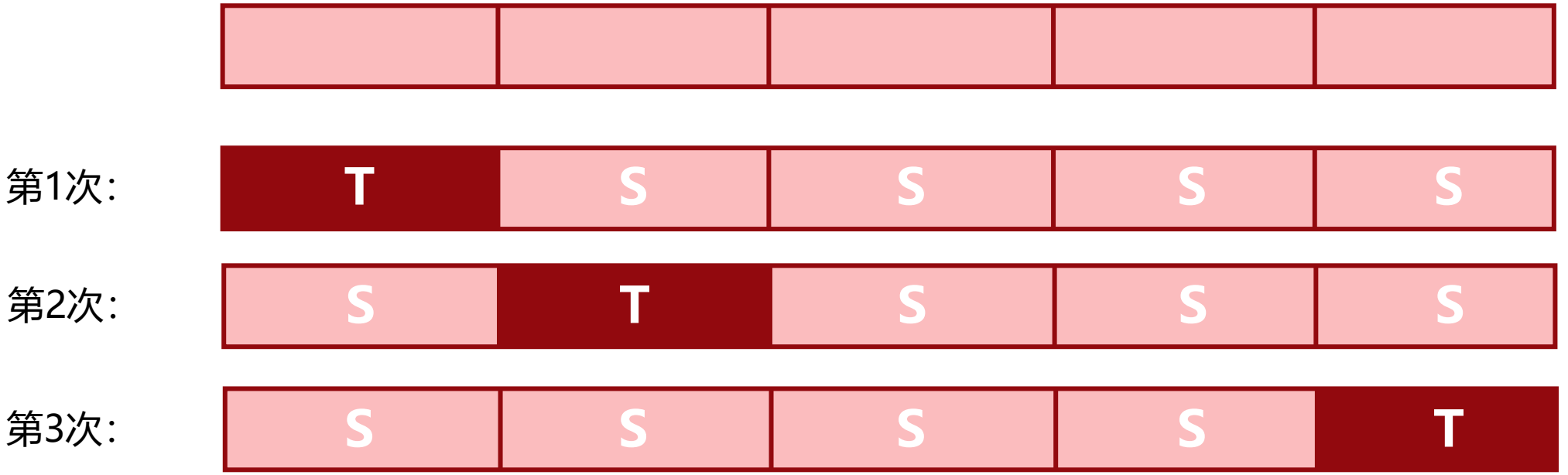
训练集
- 450个正样本，300个负样本

测试集
- 150个正样本，100个负样本

- 若**训练集S占比过大**，虽能更全面地反映整体数据集D的特征，但可能导致测试集T规模过小，进而使得**评估结果易受随机波动影响，缺乏稳定性。**
- 反之，若**测试集T占比过大**，虽能提供更丰富的测试样本，但训练集S的代表性将减弱，**可能无法充分训练模型，影响评估结果的保真度。**

数据集的划分

交叉验证法（Cross-Validation）通常也称为k折交叉验证（K-fold Cross-Validation），是一种强大的模型评估技术。该方法先将数据集D等分为k个大小一致但互不重叠的子集，即$D = D_1 \cup D_2 \cup \ldots \cup D_k$ 且$D_i \cap D_j = \emptyset, i \neq j$。随后，通过迭代方式，每次选择$k-1$个子集合**作为训练集**，而将剩余的一个子集**作为独立的测试集**，此过程**重复p次，确保评估的稳定性和准确性**。这种方法被称为**p次k折交叉验证。**



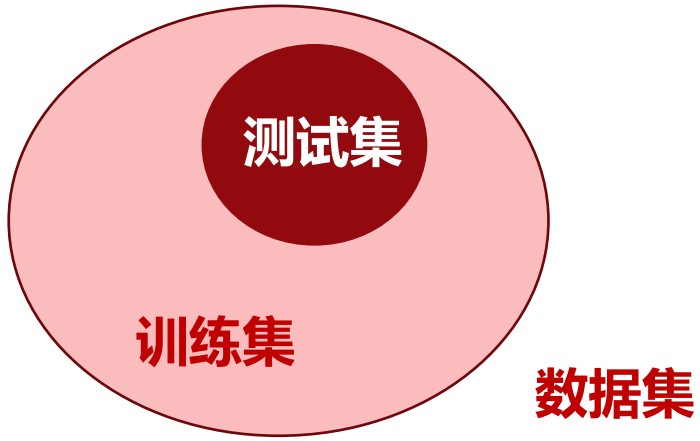
3次5折交叉验证

数据集的划分

交叉验证法（Cross-Validation）通常也称为k折交叉验证（K-fold Cross-Validation），是一种强大的模型评估技术。该方法先将数据集D等分为k个大小一致的互不重叠的子集，即$D = D_1 \cup D_2 \cup \ldots \cup D_k$ 且$D_i \cap D_j = \emptyset, i \neq j$。随后，通过迭代方式，每次选择$k-1$个子集合**作为训练集**，而将剩余的一个子集**作为独立的测试集**，此过程**重复p次，确保评估的稳定性和准确性**。这种方法被称为**p次k折交叉验证。**

- 在特殊情况下，如果k与样本总数m一致，这种策略叫做**留一法（Leave-One-Out，LOO）**。
  - **优点：**在留一法中，每个子集仅包含一个样本，意味着每次迭代都将一个样本留作测试，其余所有样本用于训练。由于训练数据几乎与原始数据集等大（仅少一个样本），留一法通常**能提供接近使用完整数据集训练的模型性能评估。**
  - **局限：**计算成本高昂。

数据集的划分



- **留出法**通过随机分割数据集为两部分，简单直接地实现了训练集与测试集的分离。
- **交叉验证法**通过多次划分数据集并迭代训练测试过程，提供了更为稳健的评估结果，适用于对模型性能要求较高的场景。

性能度量

评估学习器的泛化能力是一个多维度、精细化的过程，它不仅依赖于科学严谨的实验评估策略，更离不开恰当的性能评价标准，这一标准我们通常称之为**性能度量**。

回归任务的性能度量

- 均方误差（Mean Squared Error，MSE）

$$E(f)=\frac{1}{m}\sum_{i=1}^{m}(f(\boldsymbol{x}_i)-y_i)^2$$

更广义地，如果考虑数据的分布$\mathcal{D}$和概率密度函数$p(\cdot)$，均方误差也可以表示为：

$$E(f;\mathcal{D})=\int_{\mathcal{D}}(f(\boldsymbol{x})-y)^2p(x)d\boldsymbol{x}$$

分类任务的性能度量

- 错误率（Error Rate）

  在所有样本中，被分类器错误分类的样本所占的比例，是衡量分类器性能的一个直观指标。

$$E(f;D)=\frac{1}{m}\sum_{i=1}^{m}(f(\boldsymbol{x}_i)\neq y_i)$$

$$\mathrm{acc}(f;D)=\frac{1}{m}\sum_{i=1}^{m}(f(\boldsymbol{x}_i)=y_i)=1-E(f;D)$$

- 精度（Accuracy）

  分类正确的样本数占总样本数的百分比，从正面角度反映了分类器将样本正确分类的能力。

$$E(f;\mathcal{D})=\int_{x\in\mathcal{D}}(f(\boldsymbol{x})\neq y)p(\boldsymbol{x})\,d\boldsymbol{x}$$

$$acc(f;\mathcal{D})=\int_{x\in\mathcal{D}}(f(\boldsymbol{x})=y)p(\boldsymbol{x})\,d\boldsymbol{x}=1-E(f;\mathcal{D})$$

以毒蘑菇检测分类器为例，即便模型精度高达95%，面对关乎生命安全的决策，我们仍难以全然信赖其预测结果，**因为任何误判都可能导致不可估量的风险**。

再审视垃圾邮件过滤系统，其面临的挑战更为微妙。误阻正常邮件的**代价**，如错失重要信息而引发用户不满，**往往显著高于让少量垃圾邮件通过的成本**。

分类任务的性能度量

- 混淆矩阵

真实情况	预测结果	
	正例	反例
正例	TP（真正例数）	FN（假反例数）
反例	FP（假正例数）	TN（真反例数）

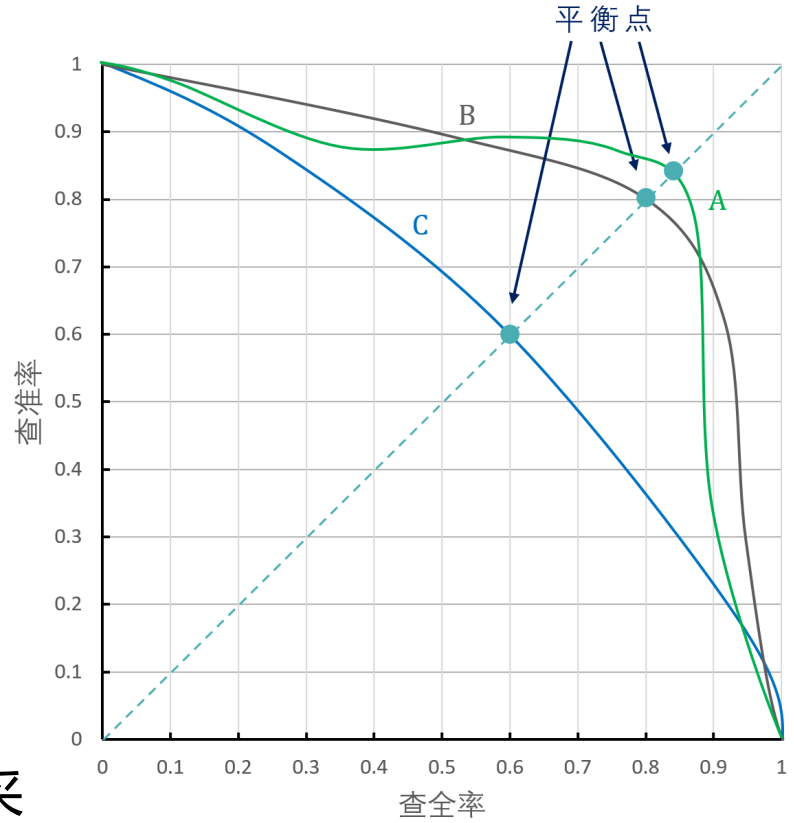
- 查准率（Precision）与查全率（Recall）

$$P = \frac{TP}{TP + FP}$$ **精确性**

$$R = \frac{TP}{TP + FN}$$ **全面性**

分类任务的性能度量

查准率与查全率之间需要**取舍**



- 查准率-查全率曲线（P-R曲线）

  性质：

  - P-R曲线**越靠近右上角**，认为这个学习器的表现更佳
  - P-R曲线**面积越大**，认为该学习器的性能越优

由于直接计算面积可能有难度，因此，在实际应用中，往往会采用F_1度量来综合评估模型的查准率和查全率，其计算方式如下：

$$F_1 = \frac{2\times P\times R}{P+R} = \frac{2\times TP}{\text{样例总数} + TP - TN}$$

$$F_\beta = \frac{(1+\beta^2)\times P\times R}{(\beta^2\times P)+R}$$

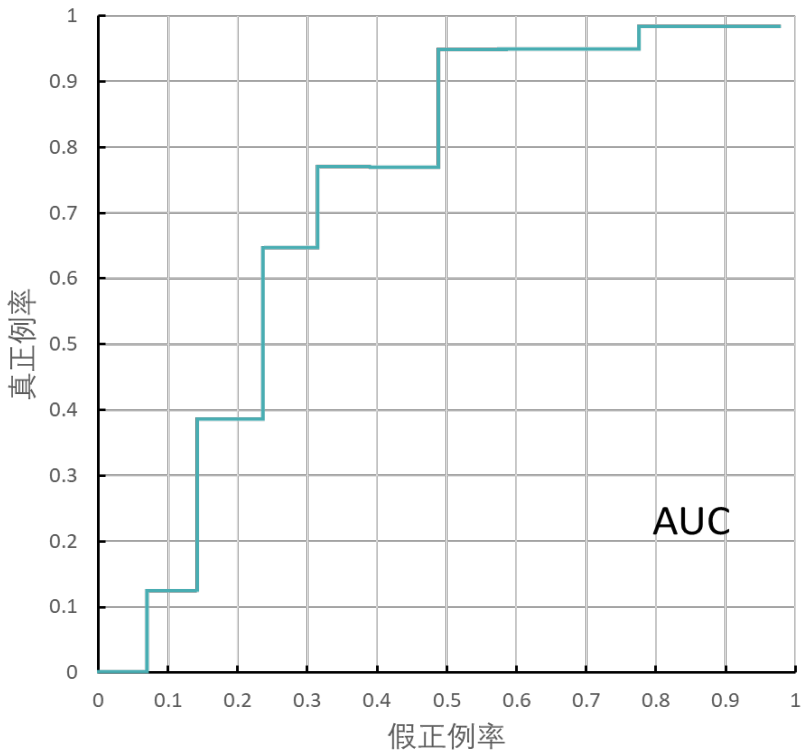
- ✓ $\beta > 1$，查全率对结果的影响更大
- ✓ $0 < \beta < 1$，查准率对结果的影响更大

分类任务的性能度量

查准率与查全率之间需要**取舍**

- ROC曲线
  - **纵轴**是“真正例率”（True Positive Rate，TPR），又称灵敏度或召回率，表示在所有实际正例中，被正确预测为正例的比例。
  - **横轴**是“假正例率”（False Positive Rate，FPR），是指在所有实际负例中，被错误预测为正例的比例。

$$TPR = \frac{TP}{TP + FN} \qquad FPR = \frac{FP}{TN + FP}$$

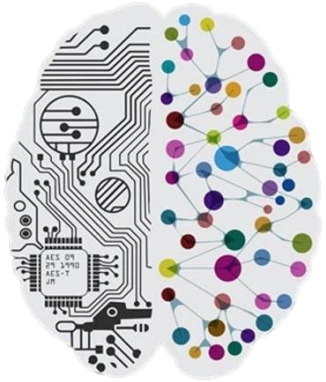


性质：

- ROC图**越靠近左上角**，认为该学习器的性能越佳
- ROC曲线**面积越大**，认为该学习器的性能越佳

AUC（Area Under the ROC Curve）

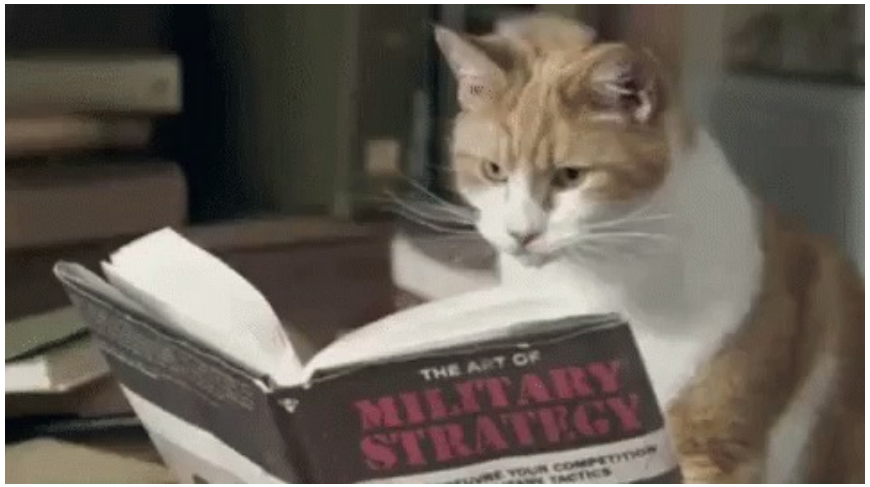
知识点3：
织就认知的“深层脉络”——深度学习

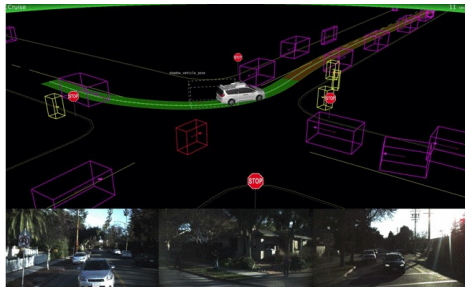


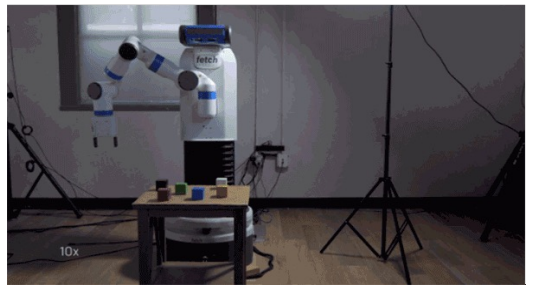
01 深度学习概述

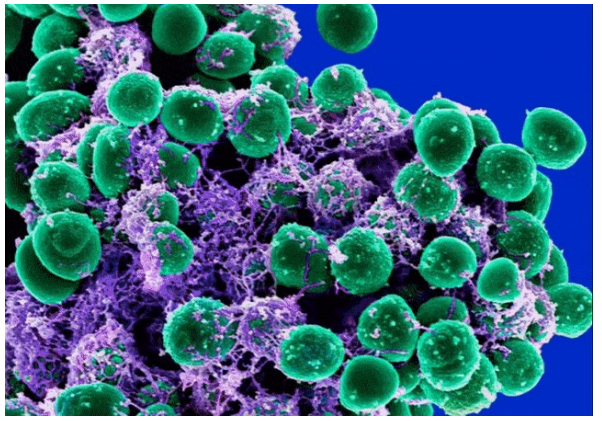
02 深度学习关键技术与应用

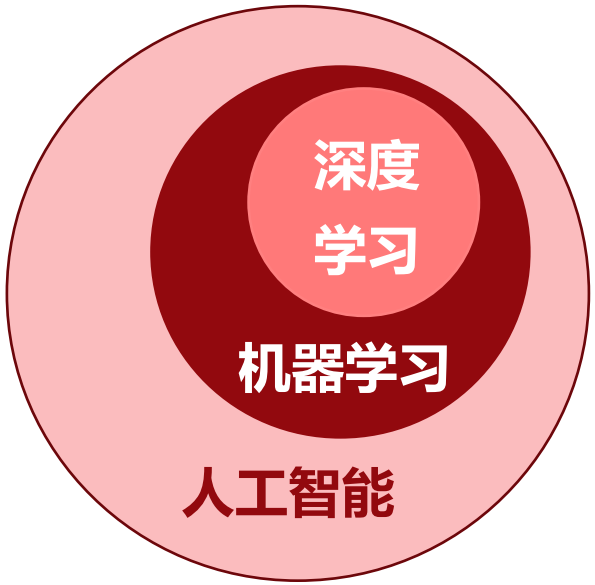
- **深度学习（Deep Learning）**作为机器学习的一个分支，已成为人工智能研究的核心领域之一。其概念源于人工神经网络的研究，旨在构建模拟人脑进行分析和学习的神经网络，从而模仿人脑的工作机制来解读和处理数据。



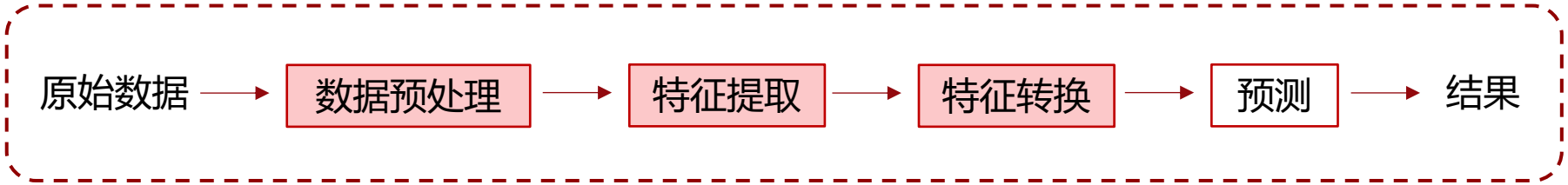




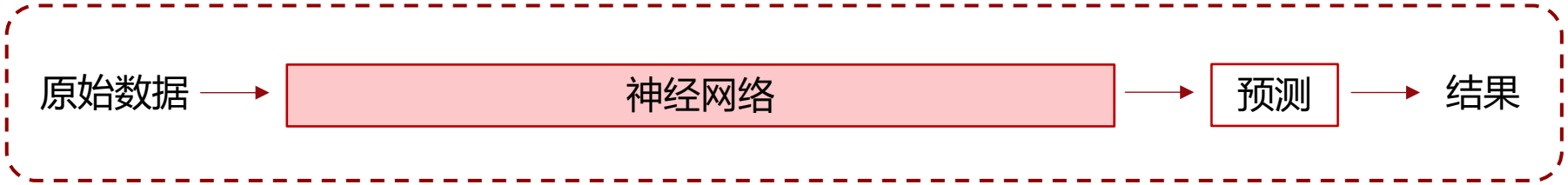




■ 与机器学习不同，深度学习算法可以**自动**从图像、视频、文本或声音等数据中**学习表征**，无需引入人类领域的知识。



一般机器学习流程



一般深度学习流程

深度学习的发展历程

提出

- MP模型
- 感知机

1943-1969

陷入低谷

- “异或”问题
- 计算能力不足
- 反向传播算法

1969-1983

复兴

- Hopfield网络和玻尔兹曼机
- 卷积神经网络

1983-1995

再度遇冷

统计学习理论和支持向量机等机器学习方法的崛起

1995-2006

大爆发

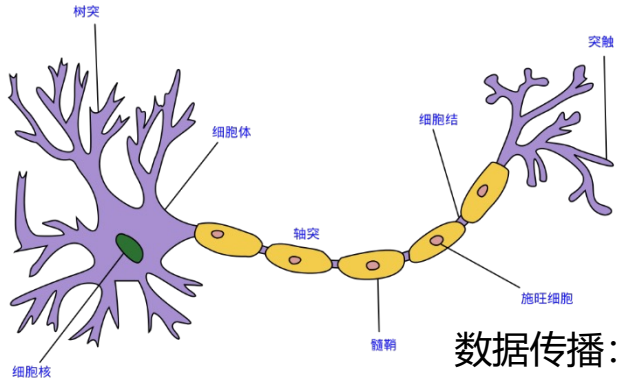
- AlexNet
- ResNet&VGG
- Bert
- GPT

2006至今

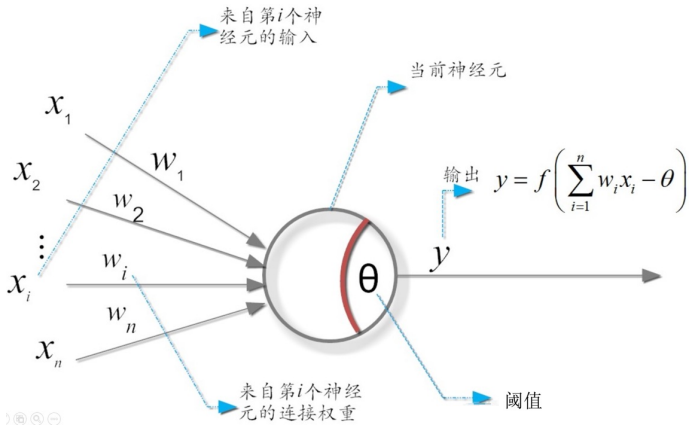
深度学习的发展历程

第一阶段：提出（1943-1969）

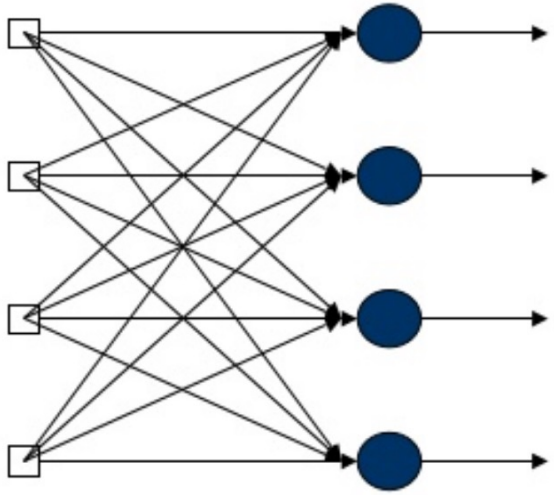
- 1943年，MP模型作为首个基于简单逻辑运算的人工神经网络模型拉开了深度学习的序幕。



数据传播：树突→轴突→突触



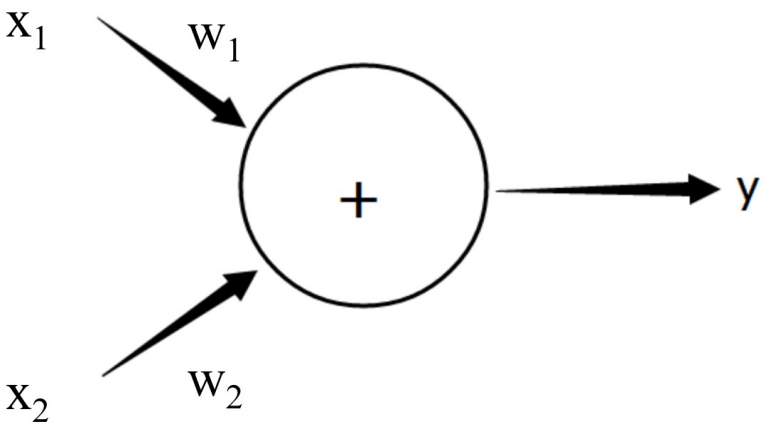
- 1958年，感知机模型开启了神经网络在模式识别等领域的初步应用。



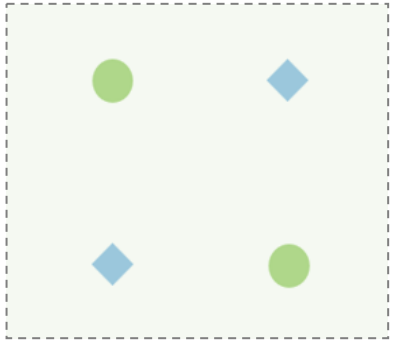
- 感知机模型是MP模型的堆叠，不局限于一个输出
- 引入了学习的概念，通过**梯度下降法**实现网络参数的优化

第二阶段：陷入低谷（1969-1983）

- 1969年，马文·明斯基（Marvin Minsky）指出感知机模型**无法处理“异或”问题**，且当时的计算能力不足，神经网络研究陷入了长达十几年的“冰河期”。



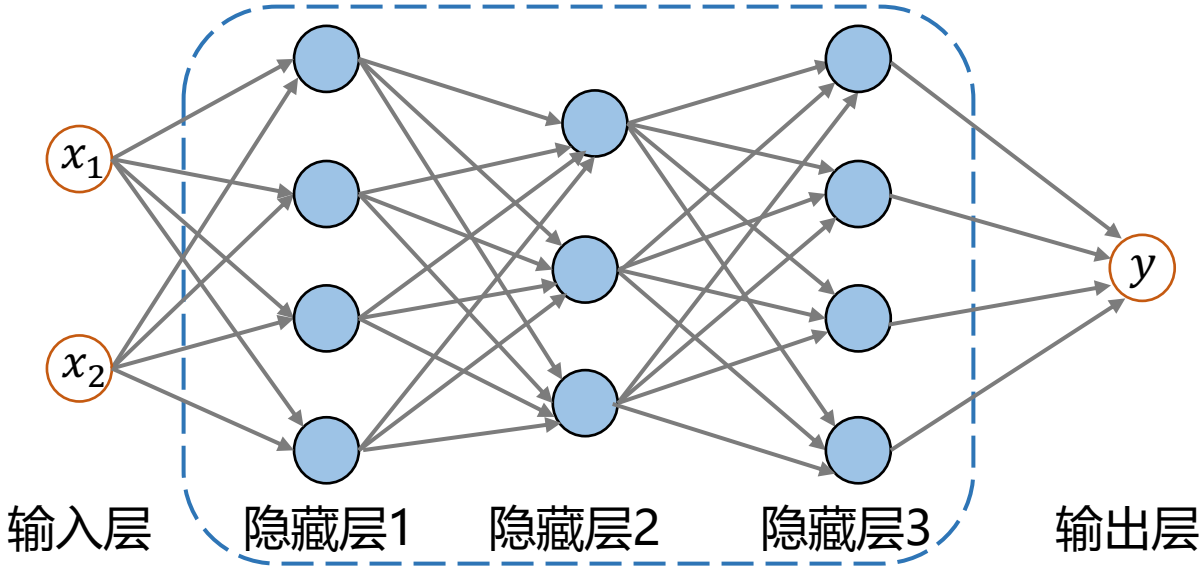
x_1	x_2	y
0	0	0
1	0	1
0	1	1
1	1	1

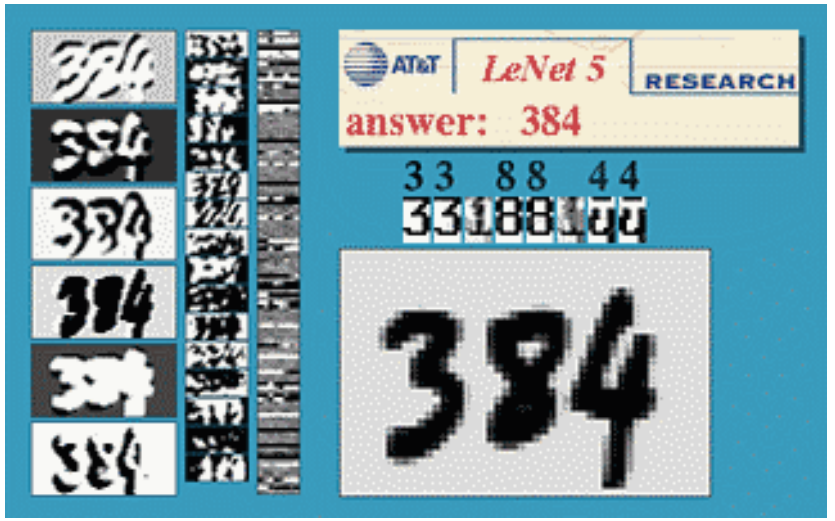


- 然而**反向传播算法**诞生于这个时期

第三阶段：复兴（1983-1995）

- 1983年，Hopfield网络和玻尔兹曼机的提出标志着神经网络的复兴。这些方法在神经网络中**引入能量函数的概念**，很好地解决了旅行商问题。
- 1986年，杰弗里·辛顿（Geoffrey Hinton）构建**多层感知机**；1989年，杨立昆（Yann LeCun）等人将反向传播算法应用至卷积神经网络，并在美国邮政手写体数字识别任务中展现了显著效果。





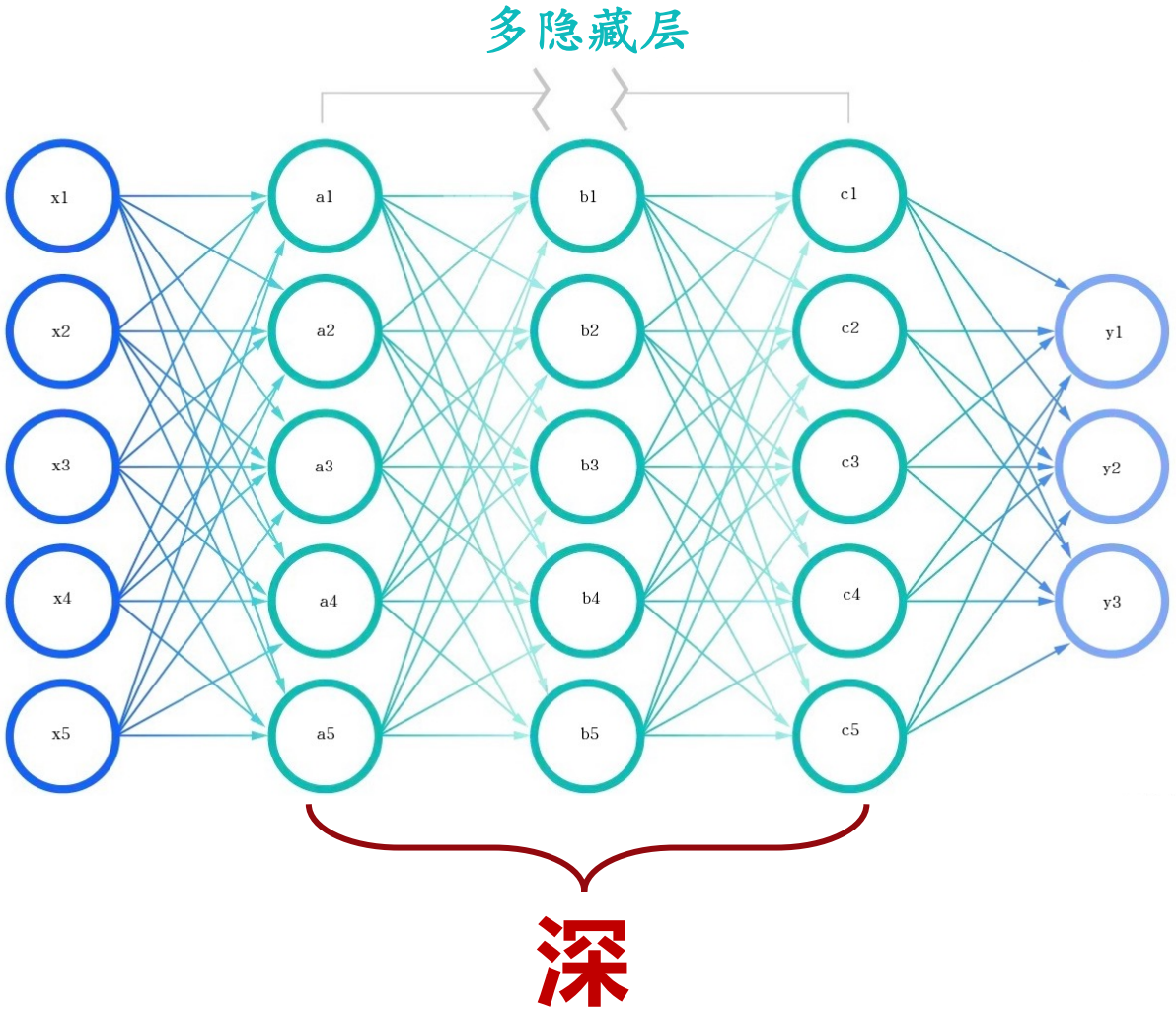
第四阶段：再度遇冷（1995-2006）

- 90年代中期，**计算能力和数据规模的不足使得神经网络的训练依然困难**，统计学习理论和支持向量机等机器学习方法的崛起，再次让神经网络的研究陷入低潮。

第五阶段：大爆发（2006至今）

- 杰弗里·辛顿（Geoffrey Hinton）等人提出了逐层预训练与精调的深度信念网络方法，解决了深度神经网络**训练困难**的问题。
- 2009年，李飞飞教授及其团队发布ImageNet数据集，并连续8年举办ImageNet挑战赛（ILSVRC），成为推动深度学习技术快速发展的重要平台，极大提升了目标检测等视觉任务的性能。
- GPU的普及。

深度学习的关键技术



1 卷积神经网络
Convolutional Neural Network，CNN

2 循环神经网络
Recurrent Neural Network，RNN

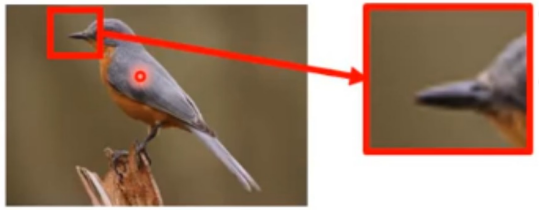
3 Transformer

4 生成对抗网络
Generative Adversarial Network，GAN

卷积神经网络

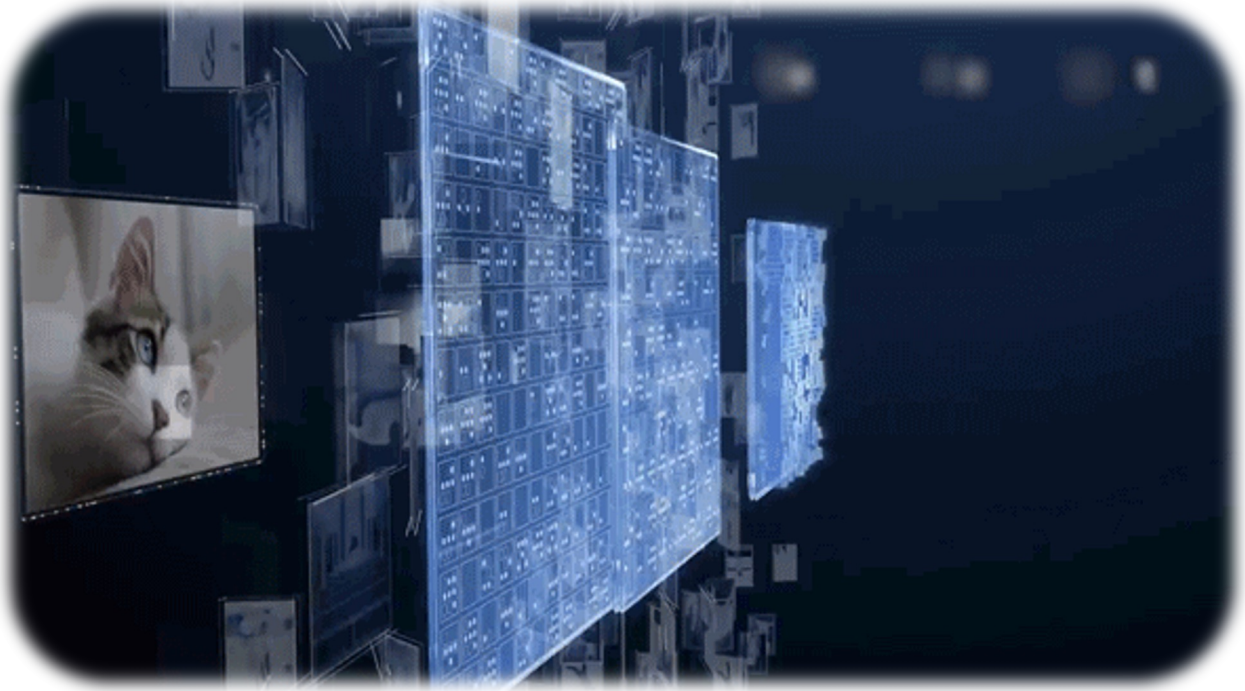
基于三个特性：

- 可以通过识别某个小图案辨认整个物体



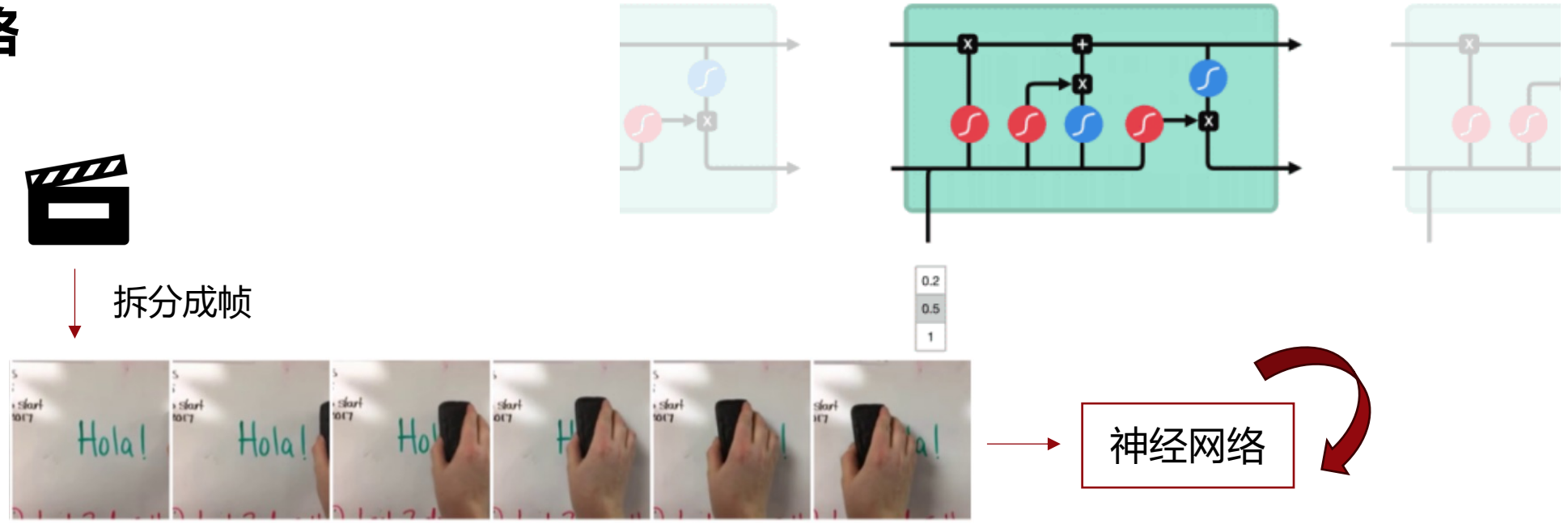
- 提供辨认能力的小图案分布位置不定

- 对图像进行抽样不影响辨认



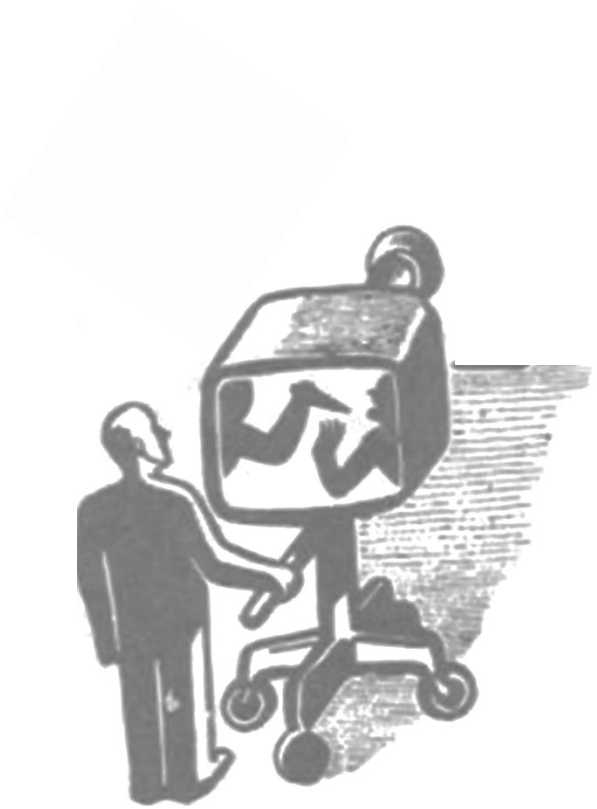
- **优势**：局部连接；权值共享。
- **代表模型**：VGG、ResNet等。
- **应用**：图像分类、目标检测、图像分割等。

循环神经网络

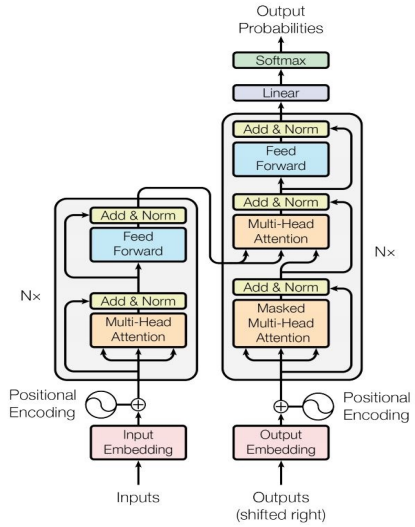


- **优势：** RNN特别适用于处理序列数据，如时间序列、文本和音频等。通过隐藏状态的循环连接，它能够记住序列中的历史信息，从而捕捉数据之间的时间依赖性。
- **代表模型：** LSTM、GRU等。
- **应用：** 自然语言处理（如机器翻译、文本生成）、语音识别、时间序列预测等。

Transformer

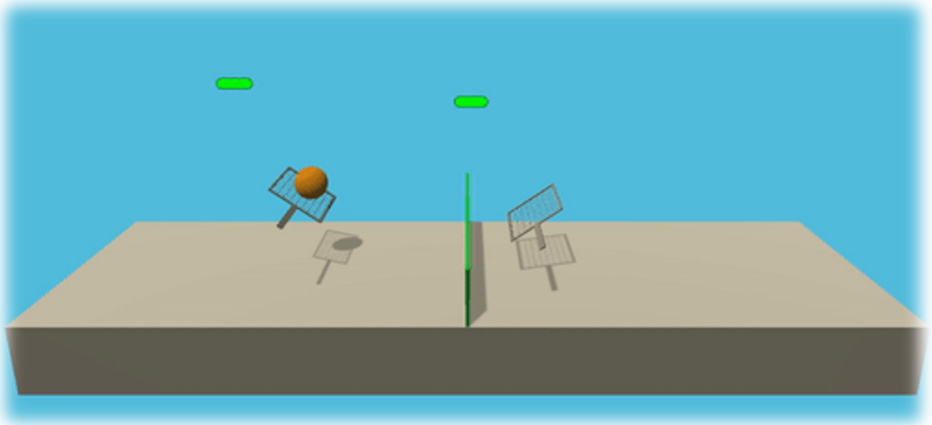


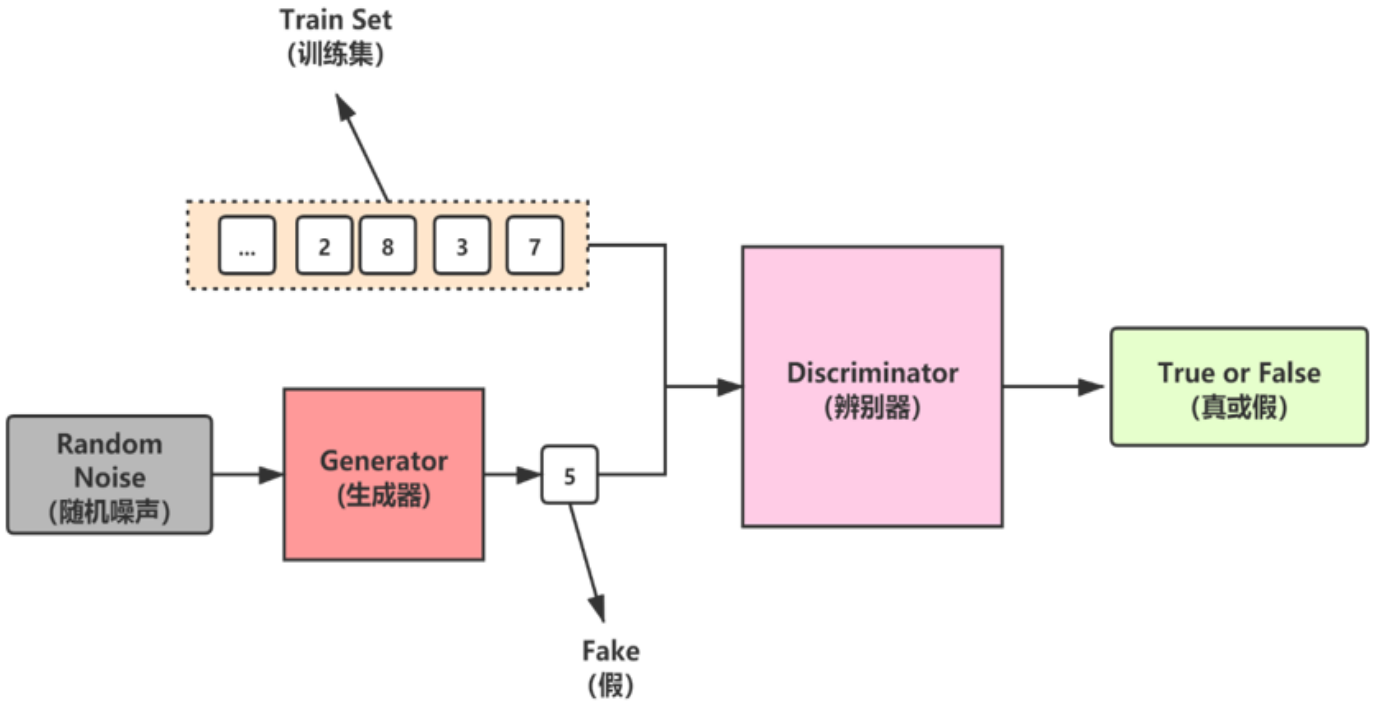
缺乏全局信息



- **优势：** Transformer是用于处理序列数据的模型，基于自注意力机制（Self-Attention），能够高效捕捉序列中任意两个位置之间的依赖关系。此外，它的多头自注意力机制可以提取多尺度的上下文信息。与RNN相比，Transformer可以并行处理数据，训练效率更高，特别适合长序列数据。
- **代表模型：** BERT、GPT等。
- **应用：** 自然语言理解、机器翻译、文本生成、对话系统等。

生成对抗网络



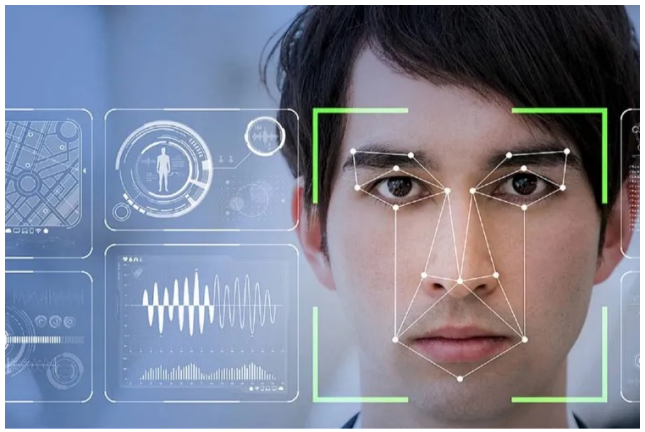


- **优势：**GAN通过生成器和判别器的对抗训练，能够生成高质量、逼真的数据。生成器负责生成数据，而判别器负责区分生成数据和真实数据，通过这种博弈过程，逐步提升生成数据的质量。它特别擅长生成图像、音频、文本等复杂数据。
- **代表模型：**DCGAN、StyleGAN等。
- **应用：**图像生成、图像修复、图像超分辨率、视频生成、音乐生成等。

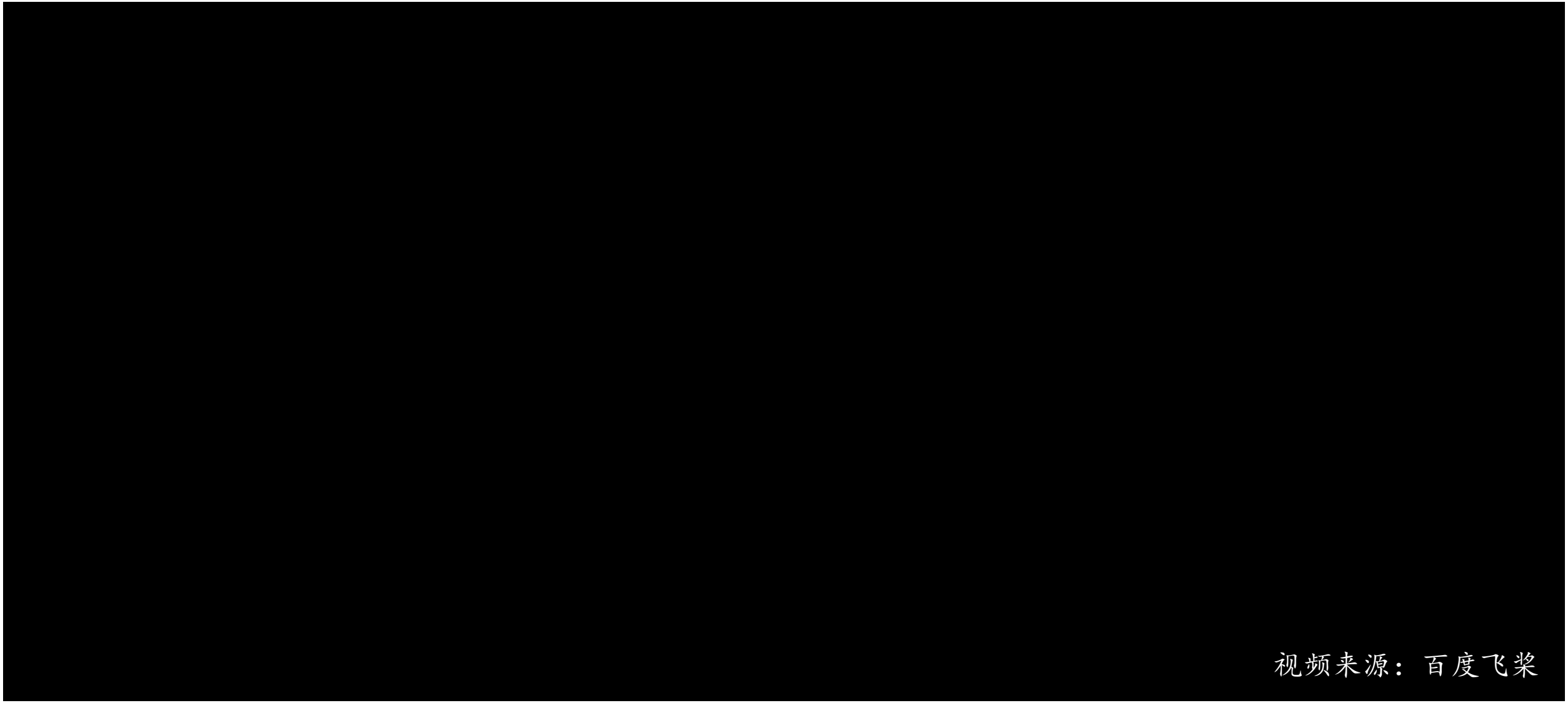
深度学习的应用

- 深度学习作为一个具有强大特征提取与感知表达能力的机器学习模型，它的成功应用极大地促进了计算机视觉、语音识别、自然语言处理等领域的发展。

- 计算机视觉
- 语音识别
- 虚拟现实
- 人机交互
- 人脸识别
- 辅助医疗诊断
- 图形编辑
- 艺术设计
- 工业质检
- ……

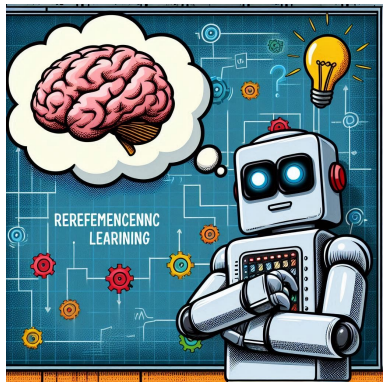


深度学习的应用



视频来源：百度飞桨

知识点4：
在试错中成长——强化学习



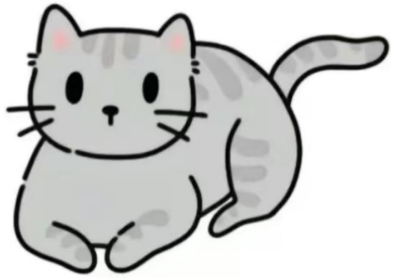
01 强化学习概述

02 强化学习的应用

问题导入

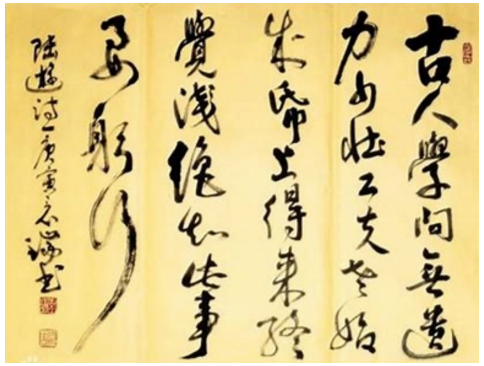
假如我们希望通过监督学习训练一个猫狗分类器，我们需要：

狗



猫

1. 构建一个包含**标签**的数据集
2. 设计损失函数，通过反向传播调整模型的参数



纸上得来终觉浅

绝知此事要躬行

—— 陆 游

■ 强化学习允许智能体在与环境的**交互中**通过**试错**来**学习最优策略**。

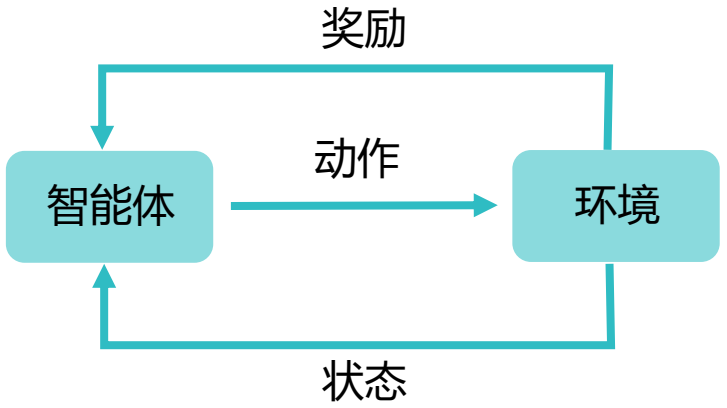
游戏《地铁跑酷》

- **智能体（Agent）**：进行决策的实体，它通过与环境交互来学习
- **环境（Environment）**：提供了智能体可以观察到的状态信息
- **状态（State）**： 环境的状态，是智能体进行决策的依据
- **动作（Action）**： 智能体在特定状态下可以采取的行动
- **奖励（Reward）**： 智能体采取动作后从环境中获得的反馈，是优化策略的关键

■ 强化学习允许智能体在与环境的**交互中**通过**试错**来**学习最优策略**。

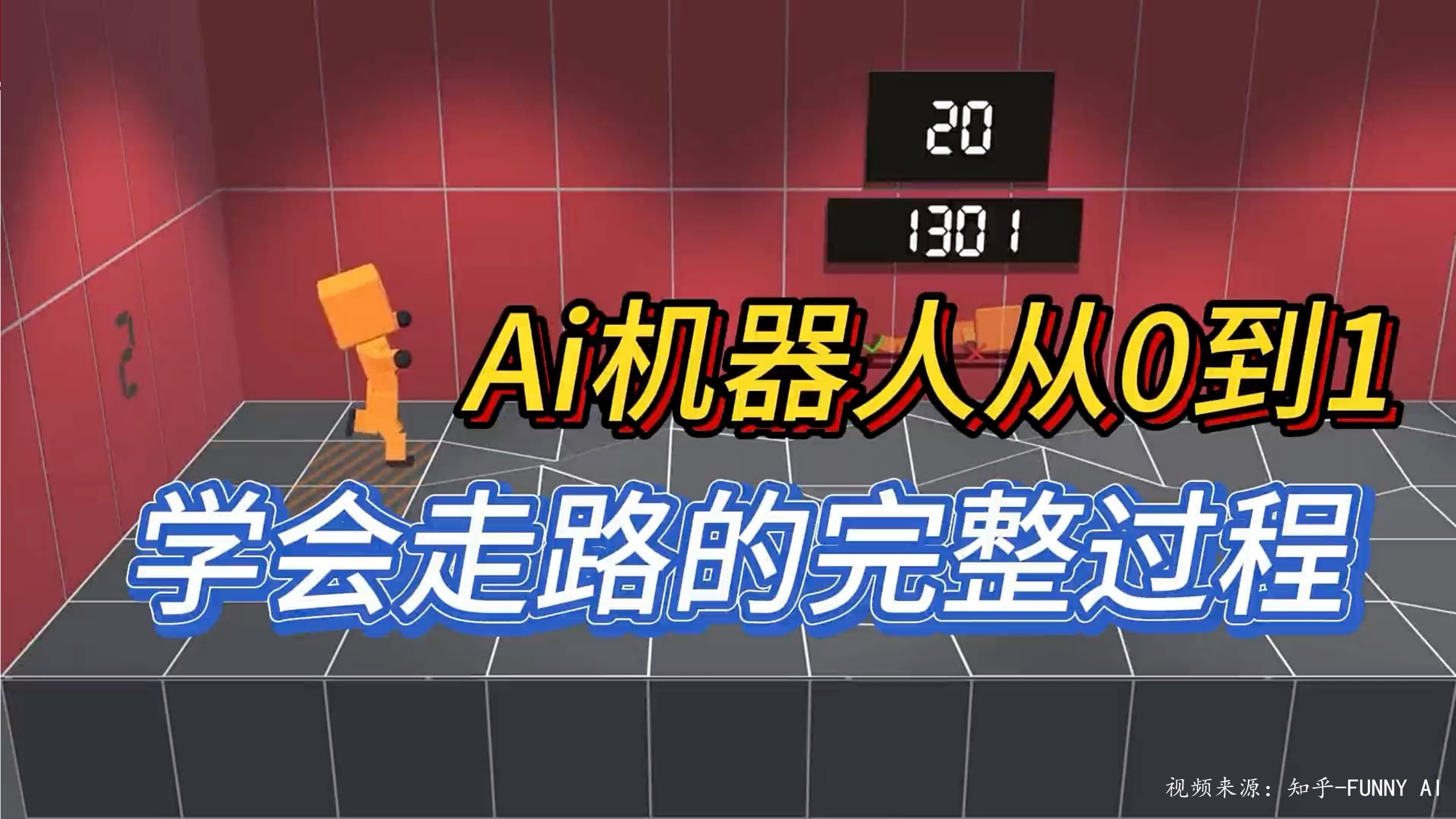
一道：距火车100pixel
二道：距栏杆100pixel
三道：距火车0pixel

游戏《地铁跑酷》



强化学习困难之处在于智能体**不能获得即时的反馈**

- **智能体（Agent）**：进行决策的实体，它通过与环境交互来学习
- **环境（Environment）**：提供了智能体可以观察到的状态信息
- **状态（State）**： 环境的状态，是智能体进行决策的依据
- **动作（Action）**： 智能体在特定状态下可以采取的行动
- **奖励（Reward）**： 智能体采取动作后从环境中获得的反馈，是优化策略的关键


20
1301
Ai机器人从0到1
学会走路的完整过程
视频来源：知乎-FUNNY AI

■ 强化学习的特性

- 强化学习**依赖试错探索**，通过与环境的不断互动获取对环境的理解。

- 强化学习智能体从环境中获得**延迟的奖励**，而非即时反馈。

- 在强化学习训练过程中，**时间因素非常重要**。因为数据是具有时间相关性的，而非独立同分布的数据。由于数据之间的强相关性，强化学习的训练过程往往并不稳定。

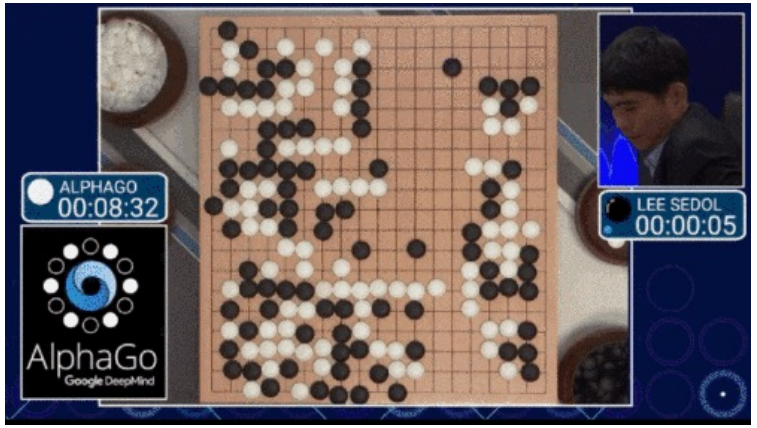
- 智能体的**动作直接影响它随后接收到的数据**。在智能体的训练过程中，许多数据是通过学习中的智能体与环境的交互获得的。如果智能体在训练中不稳定，收集到的数据质量可能很差，而数据的质量直接影响训练效果。

■ 与监督学习的区别

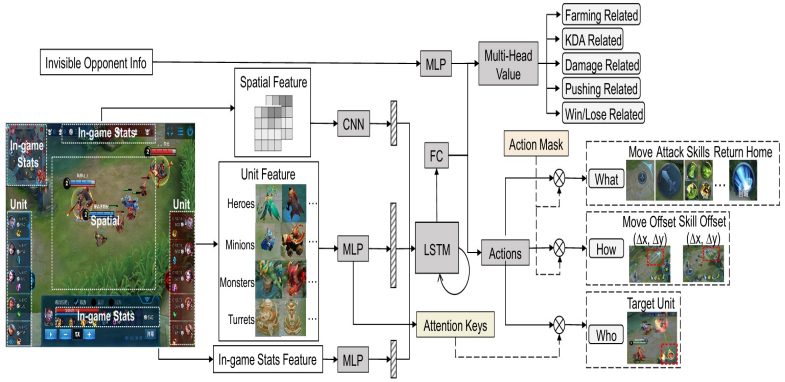
- 强化学习输入的样本是**序列数据**，而不像监督学习里面样本都是**独立**的。
- 学习器并没有**告诉**我们每一步正确的动作应该是什么，学习器需要**自己去发现**哪些动作可以带来最多的奖励，只能通过不停地尝试来发现最有利的动作。
- 智能体获得自己能力的过程，其实是不断地进行**探索与利用**的过程。其中，探索指尝试一些新的动作，这些新的动作有可能会使我们得到更多的奖励，也有可能使我们“一无所有”；利用指采取已知的可以获得最多奖励的动作，重复执行这个动作，因为我们知道这样做可以获得一定的奖励。因此，我们需要在探索和利用之间进行权衡，这也是在监督学习里面没有的情况。
- 在强化学习过程中，没有非常强的**监督者**，只有**奖励信号**，并且奖励信号是延迟的，即环境会在很久以后告诉我们之前采取的动作到底是不是有效的。

强化学习的应用

■ 游戏领域



通过强化学习，AlphaGo学会了超越人类的围棋策略，展示了强化学习在复杂策略游戏中的强大潜力。

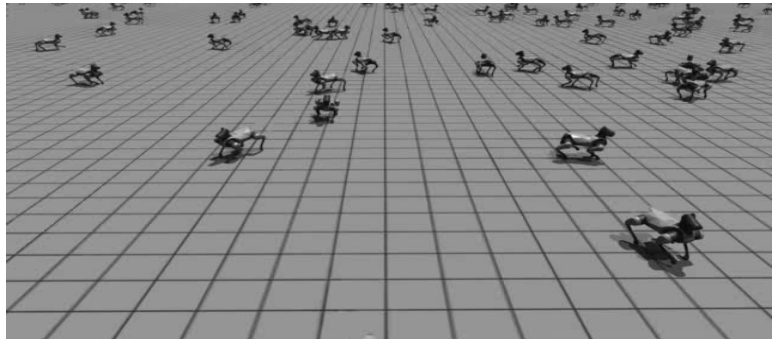


通过强化学习提升MOBA游戏中人机英雄的战斗素质，增强玩家体验。

Ye D, Chen G, Zhang W, et al. Towards playing full moba games with deep reinforcement learning[J]. Advances in Neural Information Processing Systems, 2020, 33: 621-632.

强化学习的应用

■ 机器人领域（详见知识点27）

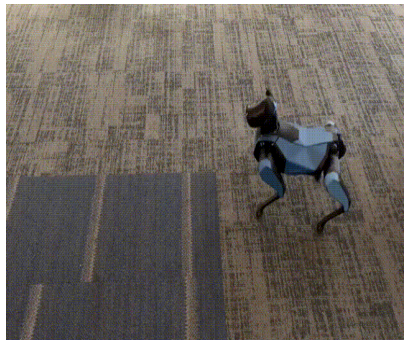


自主学习高动态动作

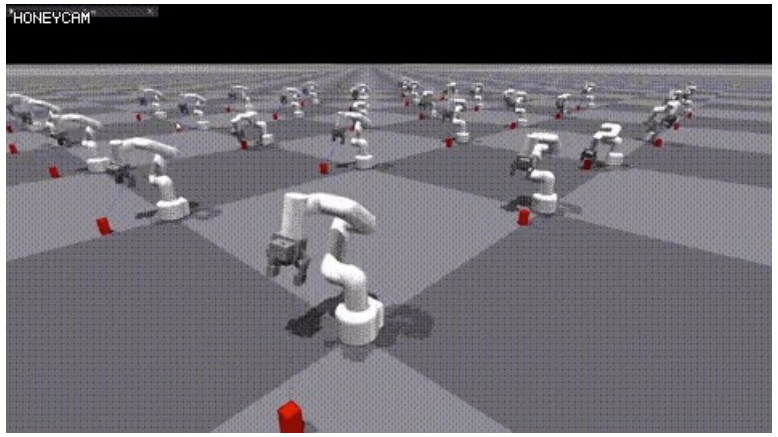
倒地起身

转圈圈

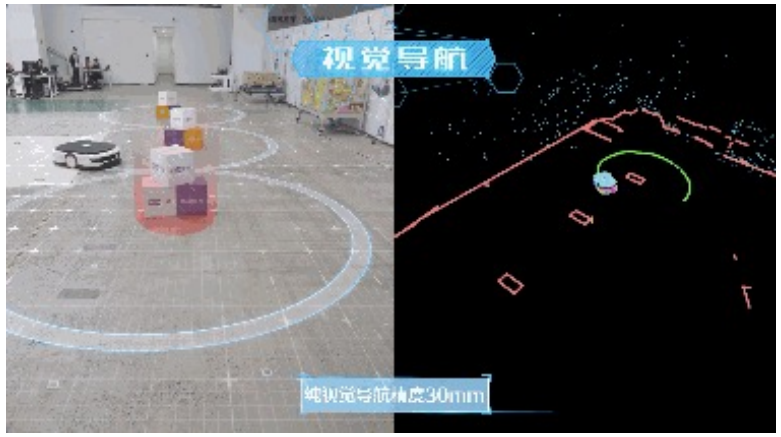
侧空翻

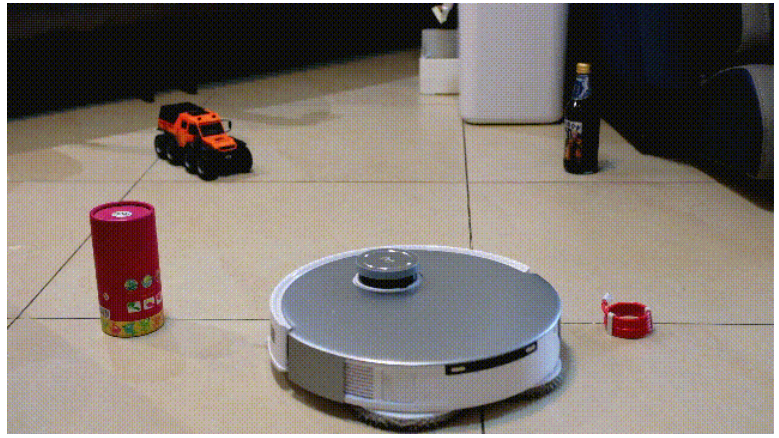


蹦蹦跳



定位抓取



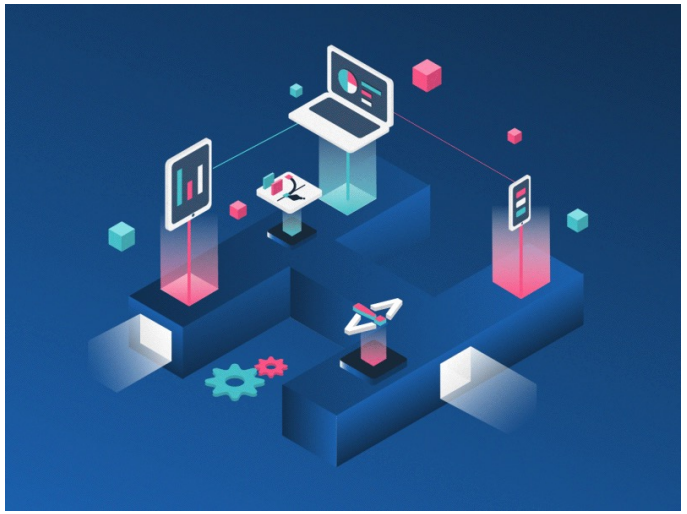


自主导航避障

强化学习的应用

■ 金融领域

强化学习被用来优化交易策略，通过实时市场数据，智能体能够动态调整投资组合以获得最大收益。

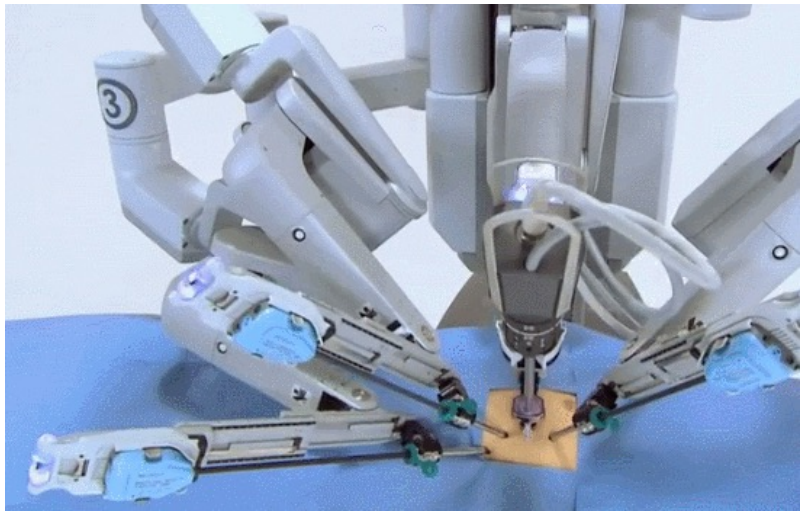


■ 自动驾驶

自动驾驶汽车通过强化学习技术，能够学习在复杂路况中的最佳驾驶策略，如避开障碍物、优化驾驶路径。

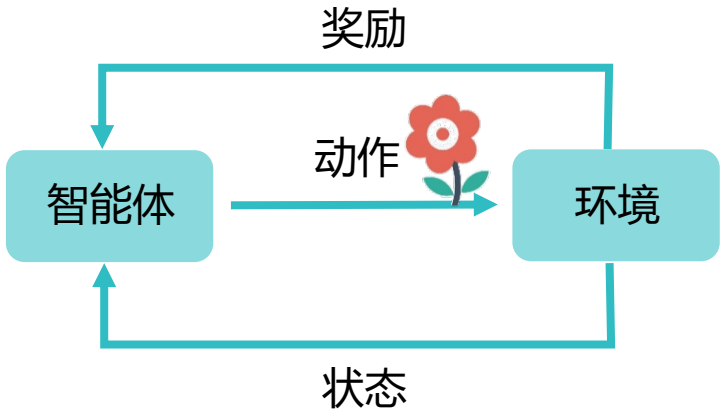
■ 医疗领域

通过强化学习，手术机器人能够在复杂的手术场景中实时学习并调整操作策略。



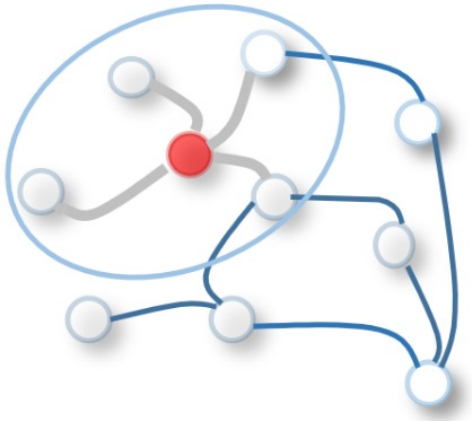
强化学习的哲学思想

强化学习任务要求智能体在面对复杂、动态变化的环境时，**聚焦于当前的状态和决策**，**而不会过分纠结于历史经验或未来的不确定性**，然后通过迭代来寻求**长期的**最大化累积奖励。



- 看清状态
- 做出决策

知识点5：
打造数据的“社交圈”——图学习



01 图学习概述

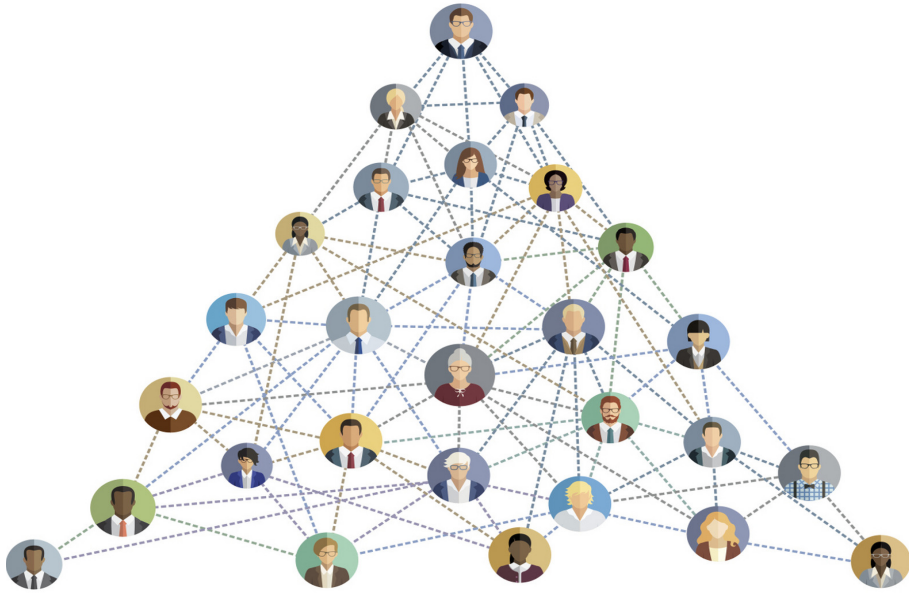
02 图学习的应用

问题导入

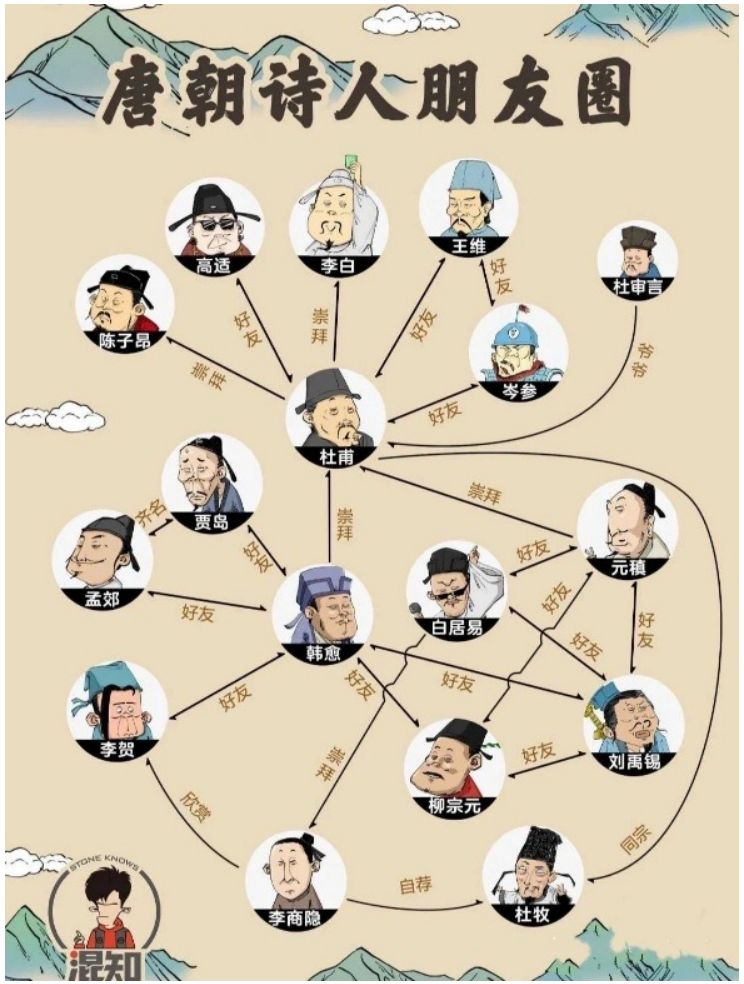
六度分隔（Six Degrees of Separation）理论：你和任何一个陌生人之间所间隔的人不会超六个，也就是说，最多通过六个人你就能够认识任何一个陌生人。”六度分隔理论揭示社会网络紧密、具有小世界特性，凸显弱关系力量，表明信息传播高效及社会结构关联有序 。

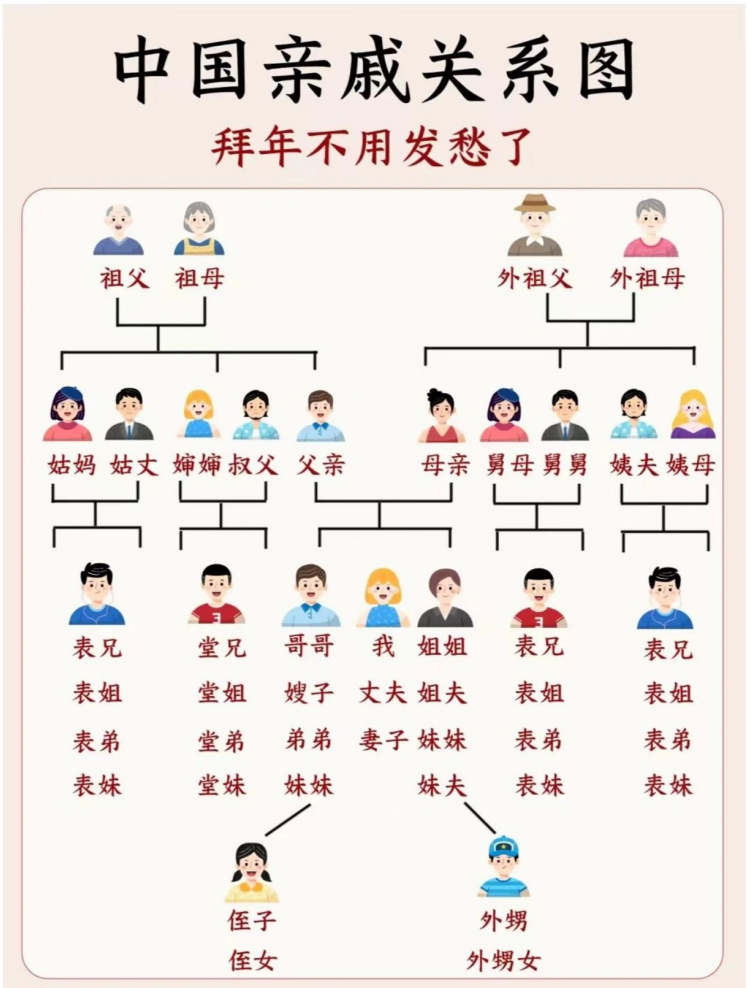
2B的你

奥巴马

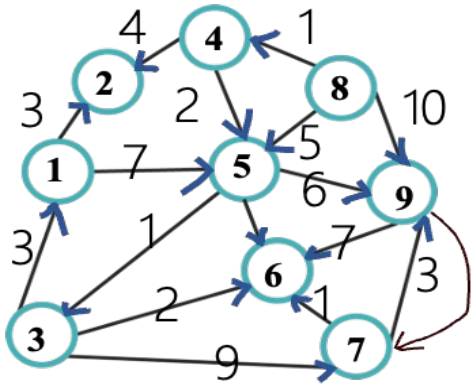


如何表示物体之间的关系呢?





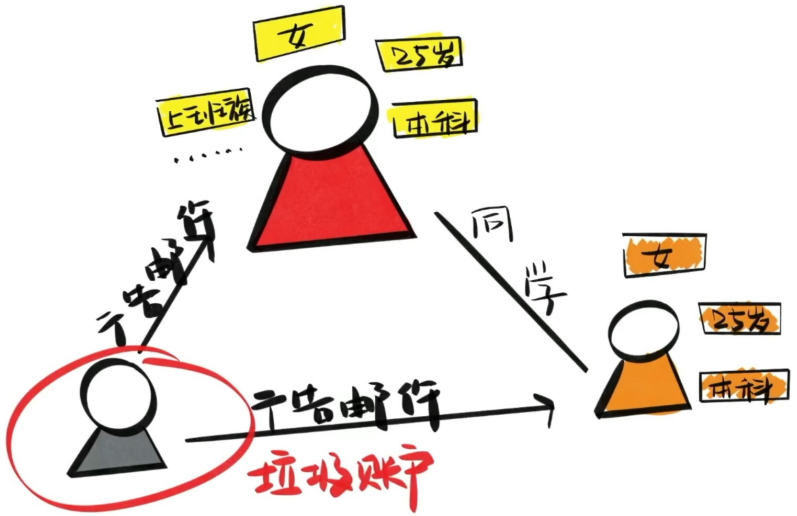
图结构，它是由**节点**和**边**组成的结构节点可以代表一个对象、一个位置或任何其他可以形成关系的实体，边表示两个顶点之间的一种联系或路径。



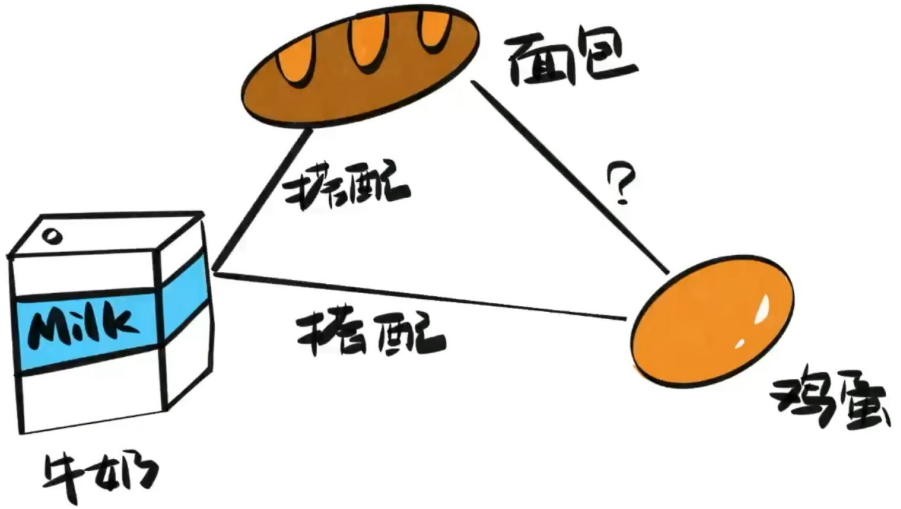
- **无向图**
- **有向图**
- **加权图**
- **多重图**

图学习方法——图神经网络

图学习旨在从图数据中提取有用的信息和知识，代表性方法便是**图神经网络（Graph Neural Network，GNN）**，通过有效利用这种图结构信息，捕捉节点之间的关系和相互作用，从而实现对图数据的深度学习。

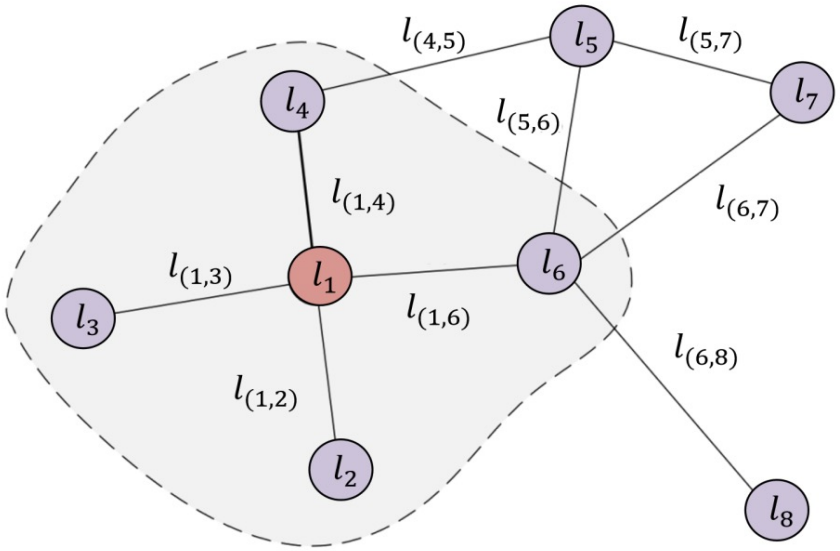


对节点展开预测



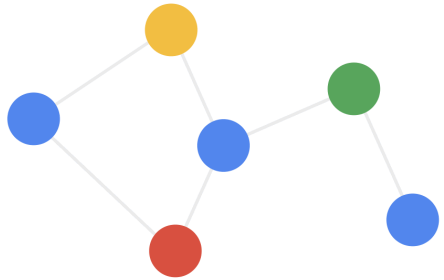
对边展开预测

以边预测任务为例



使用l_v表示节点v：

- 输入特征： $\boldsymbol{x}_v$
- 边集合：$co[l_v]$
- 邻居节点输入特征集合： $ne[l_v]$



$$co[l_1] = \{l_{(1,2)}, l_{(1,3)}, l_{(1,4)}, l_{(1,6)}\}$$

$$ne[l_1] = \{\boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4, \boldsymbol{x}_6\}$$

- **目标：**利用节点的**输入特征**，对其**邻居节点特征**进行编码，获得该节点的**状态表示**$\boldsymbol{h}_v$，进一步获得该节点的**输出**$\boldsymbol{o}_v$

$$\begin{cases} \boldsymbol{h}_v = f(\boldsymbol{x}_v, \boldsymbol{x}_{co[l_v]}, \boldsymbol{h}_{ne[l_v]}, \boldsymbol{x}_{ne[l_v]}) \\ \boldsymbol{o}_v = g(\boldsymbol{h}_v, \boldsymbol{x}_v) \end{cases}$$

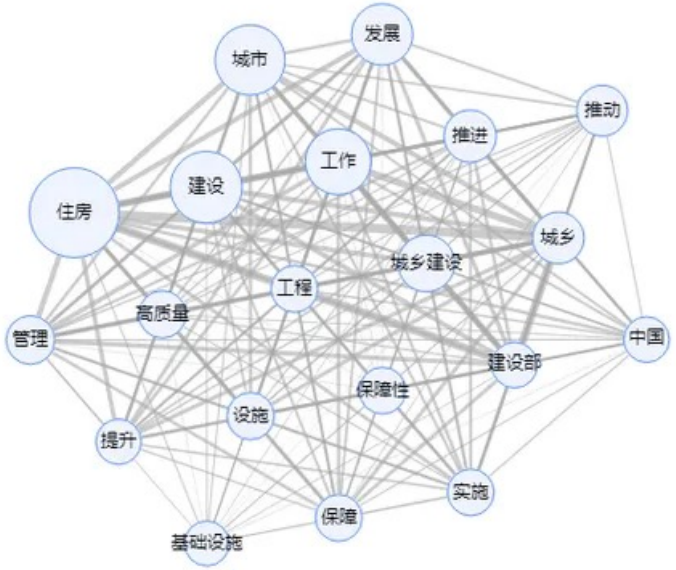
施加监督

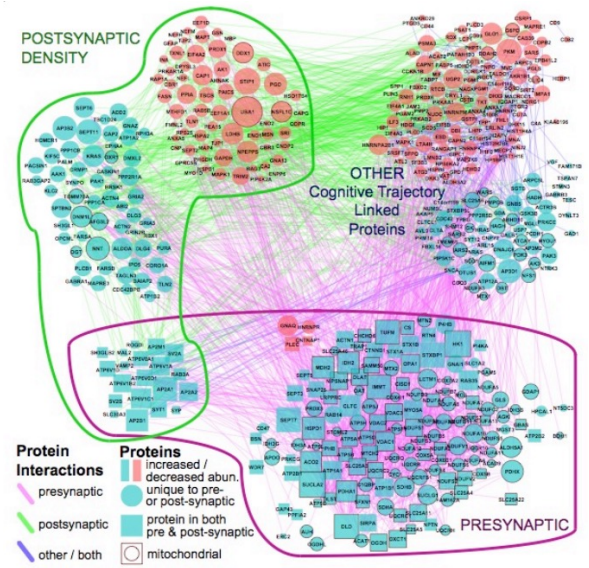
局部函数可通过前馈神经网络构建

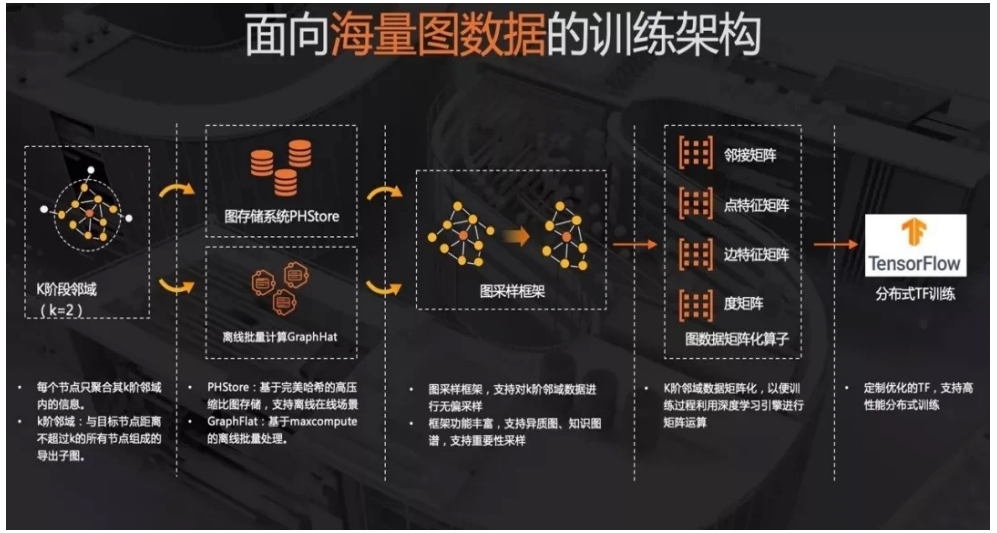
Scarselli F, Gori M, Tsoi A C, et al. The graph neural network model[J]. IEEE Transactions on Neural Networks, 2008, 20(1): 61-80.

图学习的应用

- 图学习可用于分析用户的社交关系，进行好友推荐、用户兴趣预测等；
- 图学习可用于分析蛋白质相互作用网络等，发现生物分子之间的关系和功能；
- 图学习可用于分析金融交易中的节点关系，识别异常交易模式和潜在的欺诈行为；
- 图学习可用于研究量子多体系统中的相互作用和量子态；
- 图学习可用于优化物流配送路径，提高配送效率，降低成本。

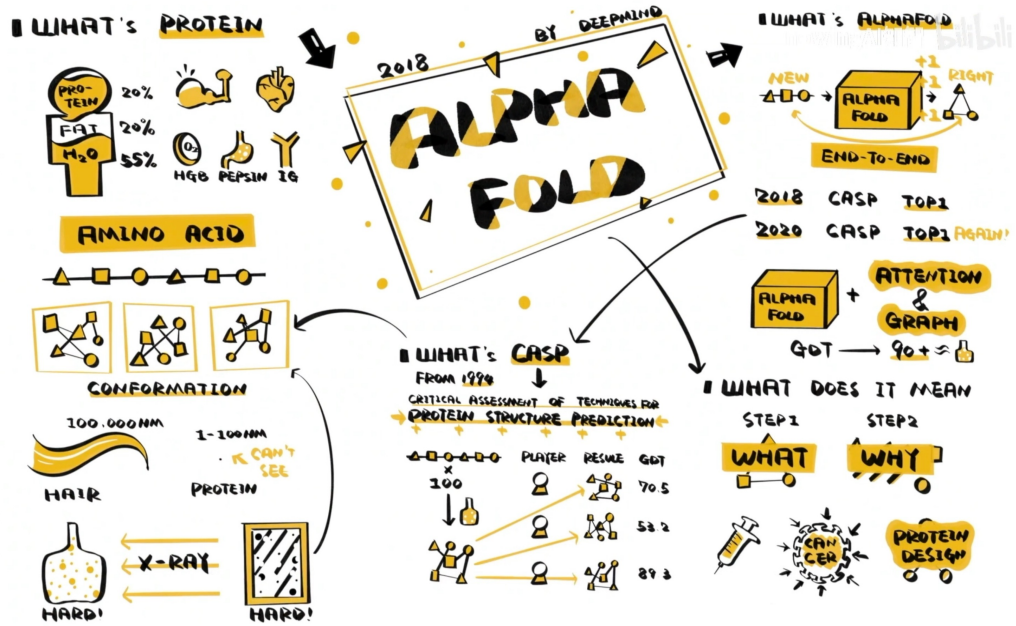




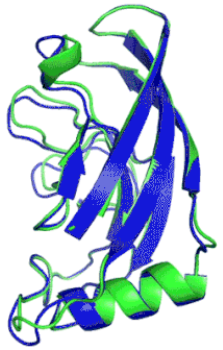


图学习的应用

2024年诺贝尔化学奖授予了伦敦谷歌DeepMind的John Jumper和Demis Hassabis，以表彰他们开发出了一个颠覆性的**可预测蛋白质结构的AI工具AlphaFold**；此外，西雅图的华盛顿大学的David Baker也因其在计算蛋白质设计领域的贡献而获奖。

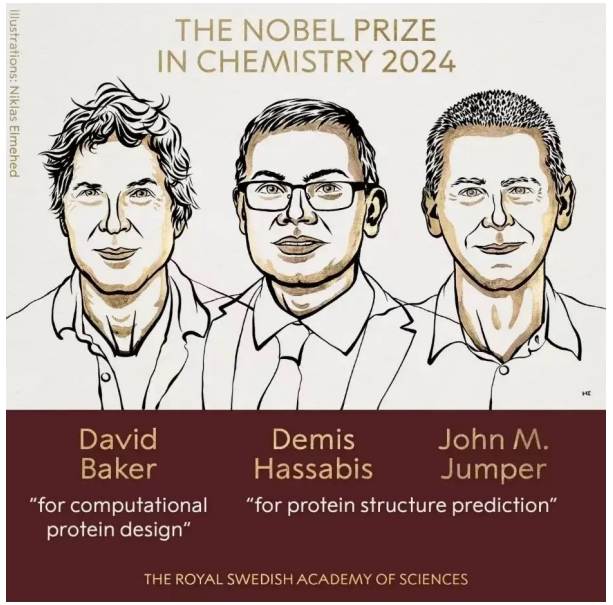


T1037 / 6vr4
90.7 GDT
(RNA polymerase domain)



T1049 / 6y4f
93.3 GDT
(adhesin tip)

Experimental result
Computational prediction



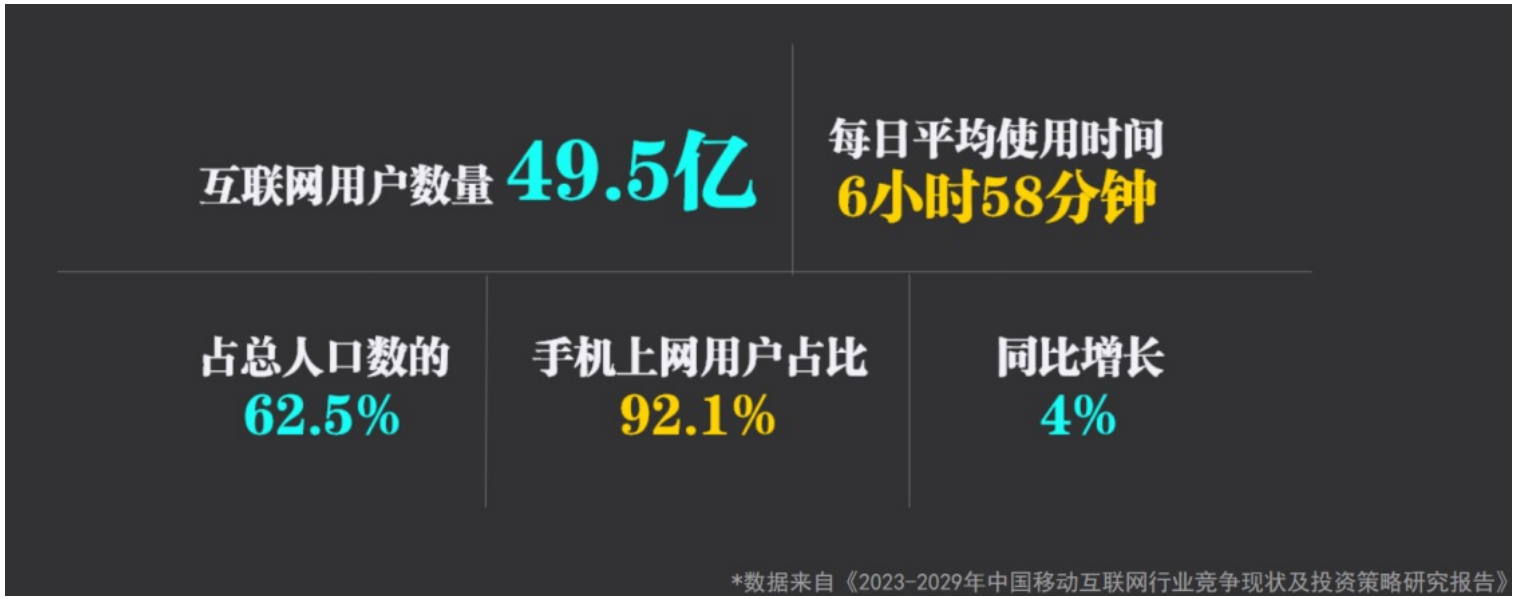
知识点6：
数据孤岛的破局者——联邦学习

01 联邦学习概述

02 联邦学习的应用

问题导入

身处数字时代，我们的互联网活动无时无刻不在产生数据，网络不知不觉间成为日常生活中必不可少的“第五空间”。网民在网络上进行的搜索记录、位置记录、通讯记录以及购物、出行等行为轨迹均属于**有价值的数据**，这些数据与用户身份、喜好、行为习惯等隐私信息紧密相连。繁多的个人信息的生产和传播，让**隐私泄露**问题的处理变得日益棘手。



问题导入

3. @评论罗伯特 是如何利用平台上的内容进行“学习”的？是否会越来越了解用户的喜好甚至是隐私？

答：我们深知保护用户隐私的重要性。因此，@评论罗伯特 学习所用的语料均为平台上的公开内容，不包含用户任何非公开信息，如“注册信息”、“私信”等。同时，在使用公开内容进行学习时，也会对数据做匿名化等脱敏处理。

2023年7月，新浪微博推出AI机器人——评论罗伯特。作为一个以微博用户身份活跃在网友评论区的智能机器人，当用户在微博发布原创内容或者艾特此号，则有可能收到它的回复。

长到这么大还是会一委屈难过就想爷爷奶奶，因为只有他们给了我很多很多的爱，但是他们再也不会出现在我身边了

评论罗伯特 I
他们住在你心里，比身边还近呢

我什么时候可以变成真正的大人啊

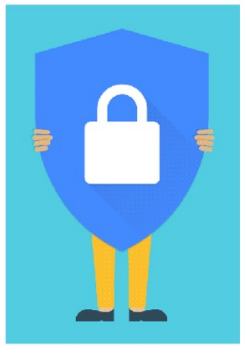
评论罗伯特 I
当你开始偷偷看小孩的时候，你就已经是个大人了

人是被时间磨损的吗？
不是的。
人是被共和种各样的离别磨损的。

评论罗伯特 I
时间只是计数器，离别才是砂纸呢

联邦学习概述

■ 联邦学习是一种创新的机器学习模式，旨在**处理分布式数据集**，**解决数据孤岛问题**。



- **模型训练阶段：**相关的信息（或加密后的信息）在各方之间交换，但**数据本身并不进行交换**，从而确保每个站点上的受保护隐私内容不会暴露。
- **推理阶段：**训练阶段学习到的**模型共享**，可用于处理新的实例样本。

联邦学习
基于隐私保护的分布式建模框架

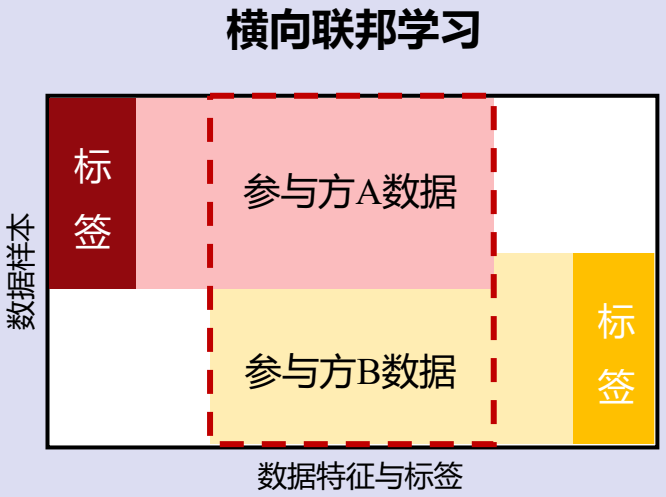
多方协作：两个或更多的参与方共同协作，构建一个共享的机器学习模型。

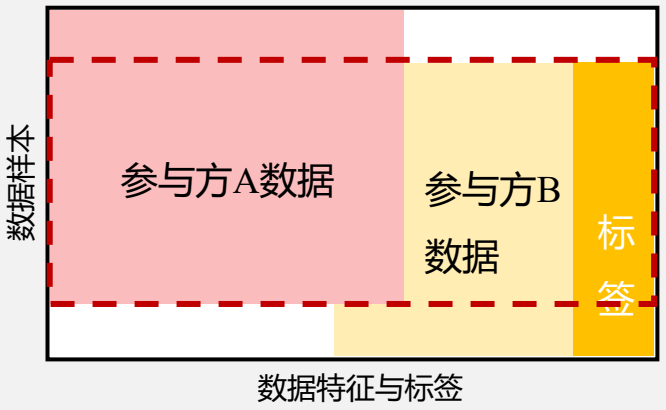
数据本地化：每个参与方都拥有可用于训练模型的训练数据，且这些数据在训练过程中不会离开数据拥有者。

信息加密交换：联邦学习模型相关的信息能够以加密的方式在各方之间传输和交换，确保任何一个参与方都无法推测出其他参与方的原始数据。

性能逼近理想模型：联邦学习模型的性能应能够充分逼近通过将所有训练数据集中后进行训练得到的理想模型的性能。

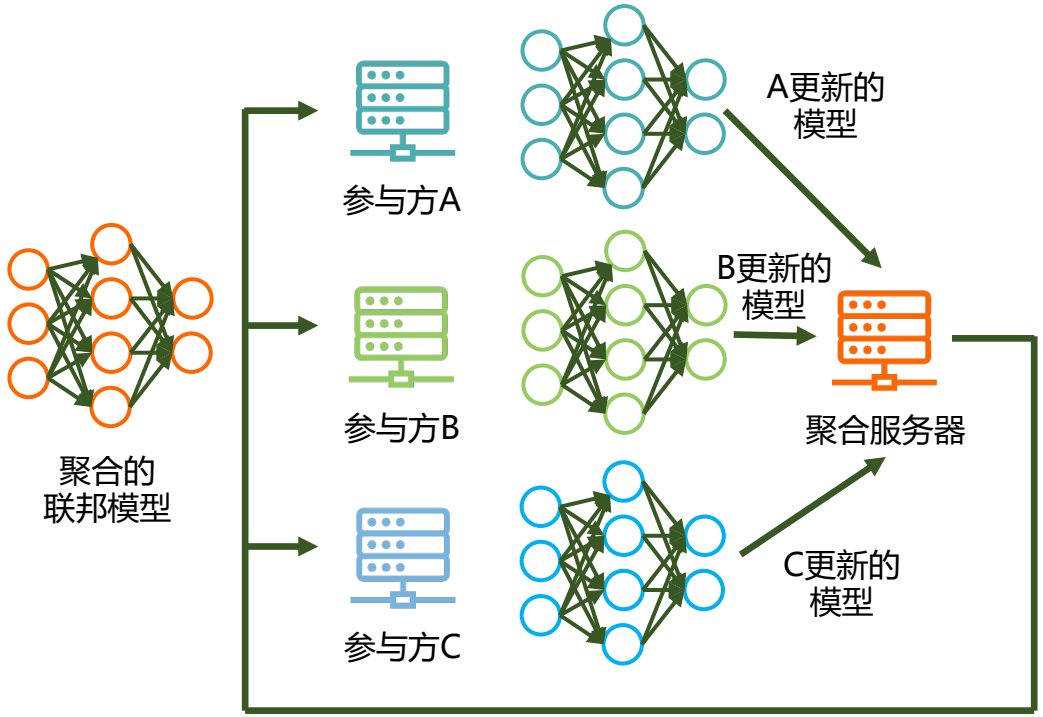
联邦学习架构



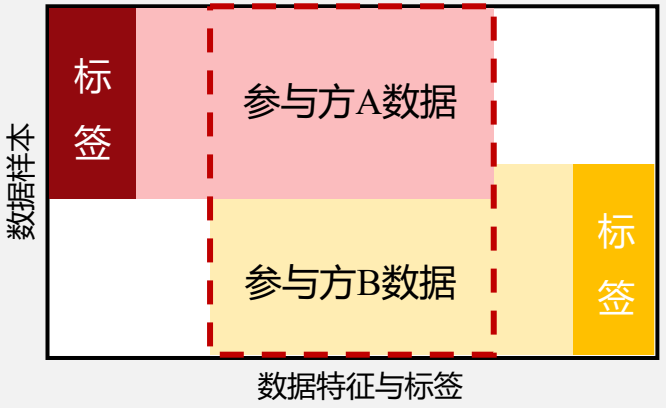


横向联邦学习（客户-服务器架构）

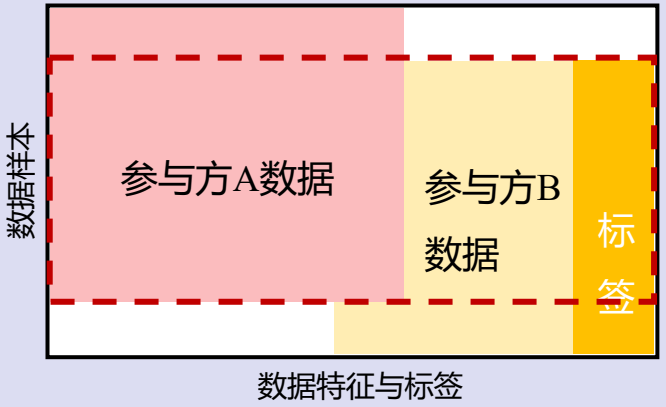
参与者业务相似，即特征重叠多，样本重叠少



- 在整个训练流程中，参与方的原始数据**始终保持在本地**，不会被传输至其他任何地方

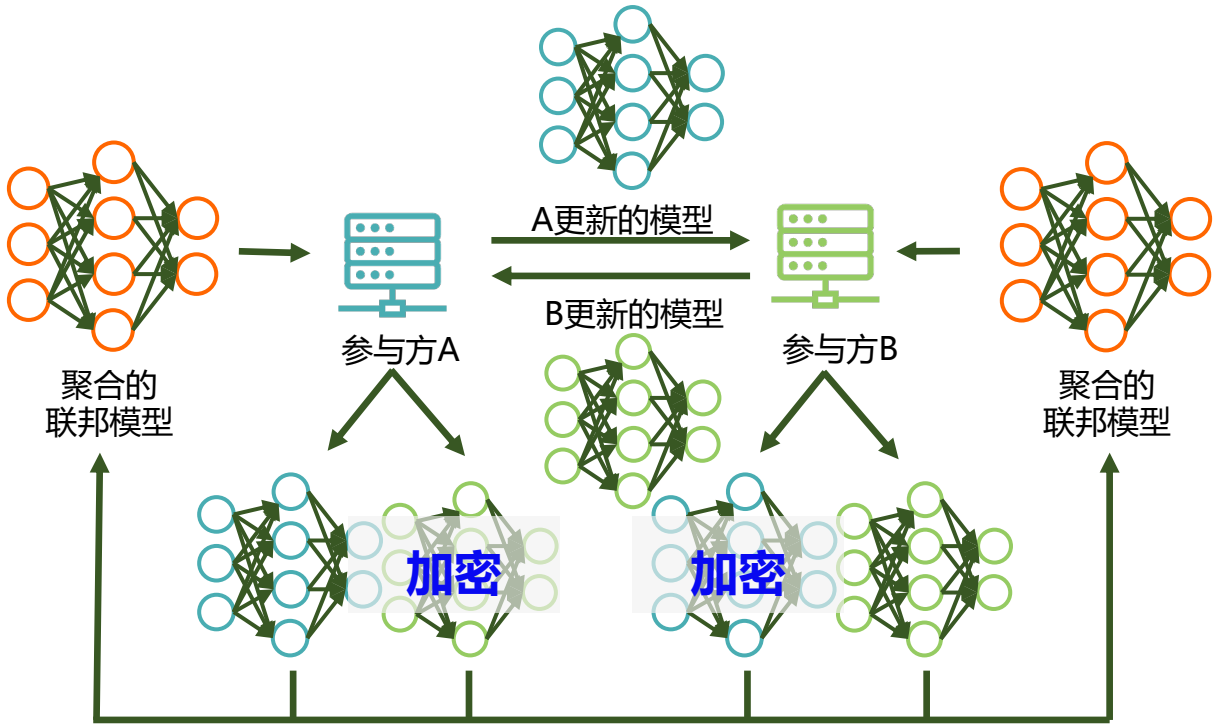


纵向联邦学习



纵向联邦学习（对等网络架构）

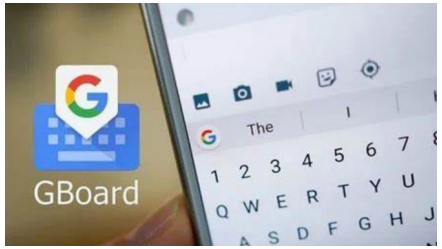
样本重叠多，特征重叠少

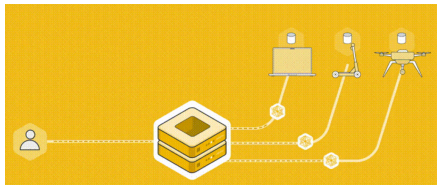


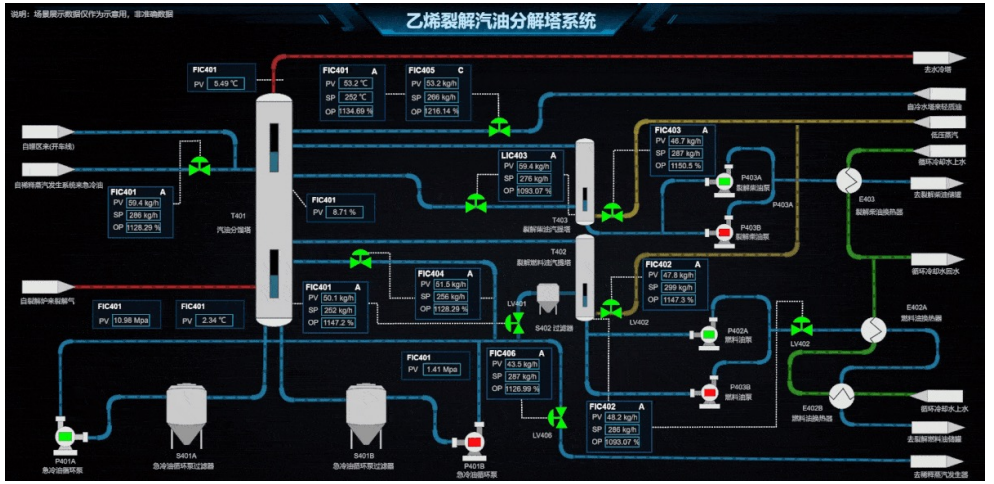
- 在整个训练流程中，参与方的原始数据**需经加密传给各方**，参与方拥有完整的数据。

联邦学习的应用

- **移动设备个性化：**在智能手机和其他移动设备上，联邦学习可以用来训练个性化的应用和服务，如键盘输入预测、个性化推荐系统，将训练好模型的参数上传至云端从而避免个人数据泄露。
- **金融服务：**银行和金融机构可以使用联邦学习来改进信用评分模型、欺诈检测系统等，不必共享客户的敏感财务信息。
- **智能制造：**在工业环境中，各个制造基地可以利用联邦学习来优化生产流程，提高效率和质量控制，同时保护各自的生产数据。

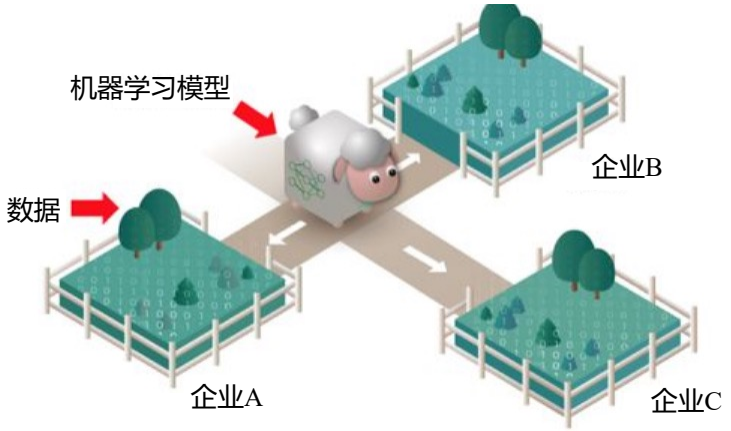


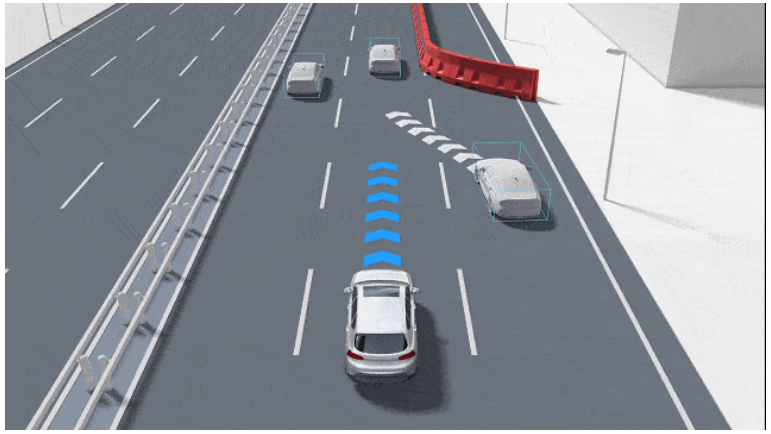




联邦学习的应用

- **智慧城市：**联邦学习可以用于交通管理、能源消耗优化等领域，通过分析来自不同来源的数据来改进城市运营，同时确保数据的安全性和合规性。
- **跨公司合作：**不同公司可以在保护各自商业机密的前提下，基于联邦学习共同开发新的产品或服务，如联合市场分析供应链优化等。
- **自动驾驶：**汽车制造商可以使用联邦学习来训练自动驾驶系统，通过收集来自多辆汽车的数据来提高系统的安全性和可靠性，同时确保数据的隐私性。





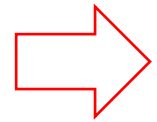
知识点7：
让模型举一反三——迁移学习

01 迁移学习概述

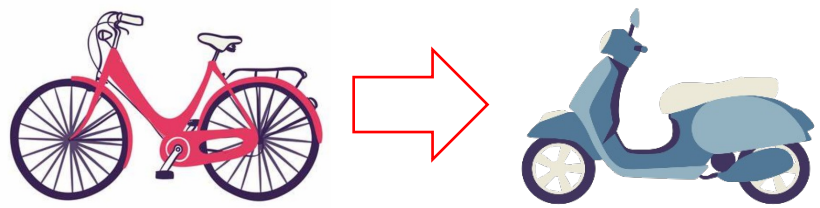
02 迁移学习的应用

问题导入

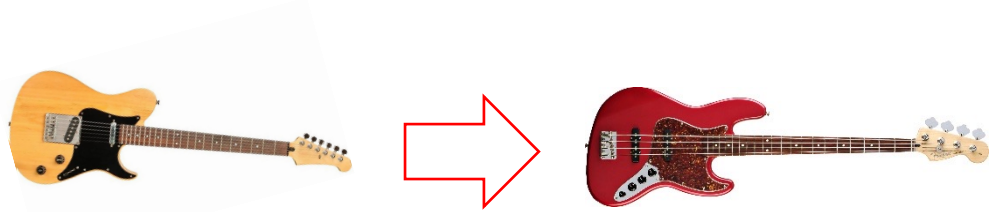
搜索引擎



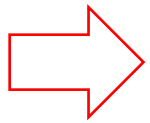
交通工具

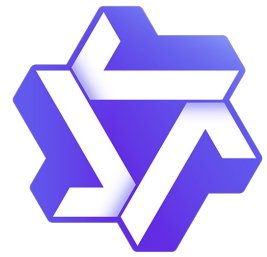


乐器



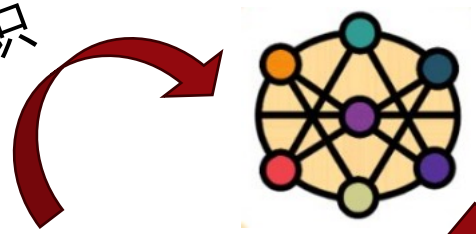
大模型





人类具备在任务间迁移知识的内在能力

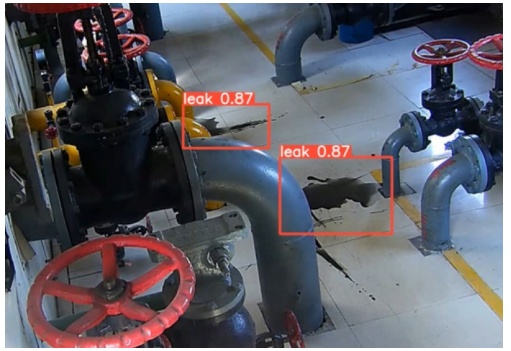
问题导入



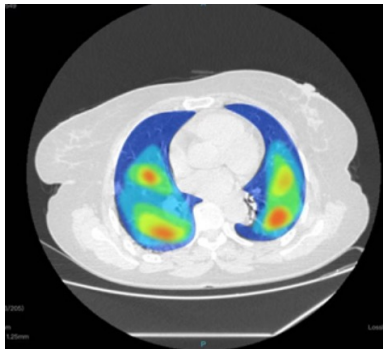
迁移知识

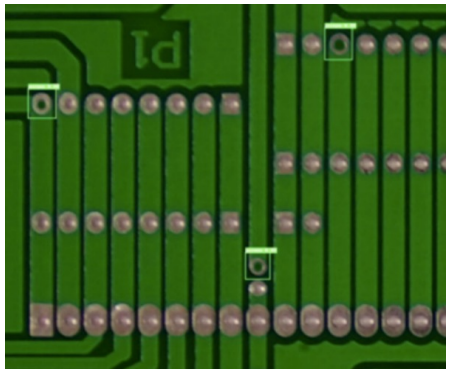
指导学习

大规模领域



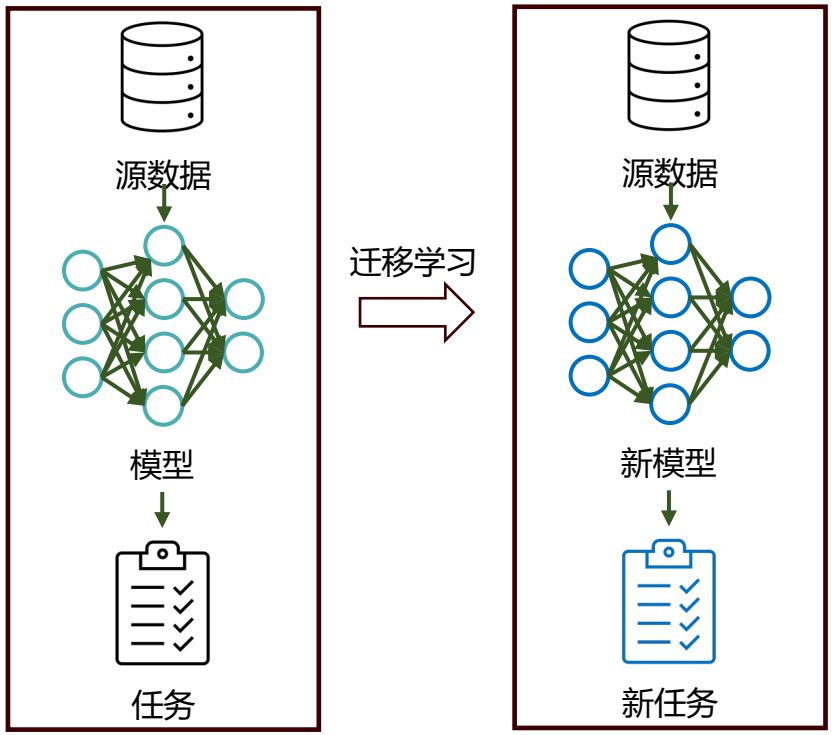
小规模领域



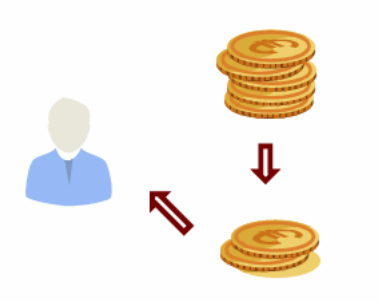


迁移学习概述

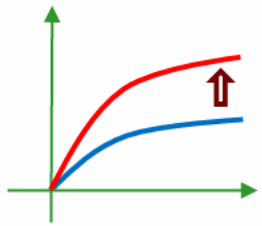
迁移学习是指利用**源领域（Source Domain）**中学到的知识来帮助**目标领域（Target Domain）**的学习任务。



减少新领域模型训练的时间



降低新领域数据标注成本



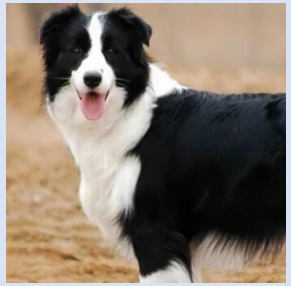
利用任务间相关性提升性能

与标准机器学习的区别

- **标准机器学习**建立在训练集与测试集源自**相同样本空间和概率分布的前提**之上，这意味着模型的有效性局限于同一分布环境内。
- **迁移学习**则放宽了这一限制，它允许训练和测试数据**不仅可能来自不同的样本空间，还可能具有各异的概率分布。**

猫/狗
分类器

猫



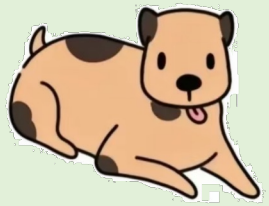
狗

老虎

熊猫

相似领域，不同任务

猫



狗

不同领域，相同任务

迁移学习的分类

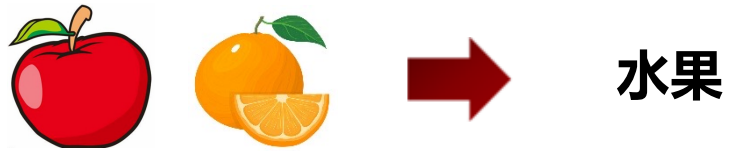
迁移的性质

正迁移：一种学习对另一种学习产生积极的促进作用

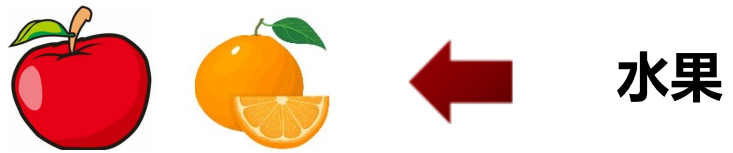
负迁移：一种学习对另一种学习产生消极的阻碍作用

迁移的层次

纵向迁移（垂直迁移）：先学习具体的概念，再学习抽象的概念



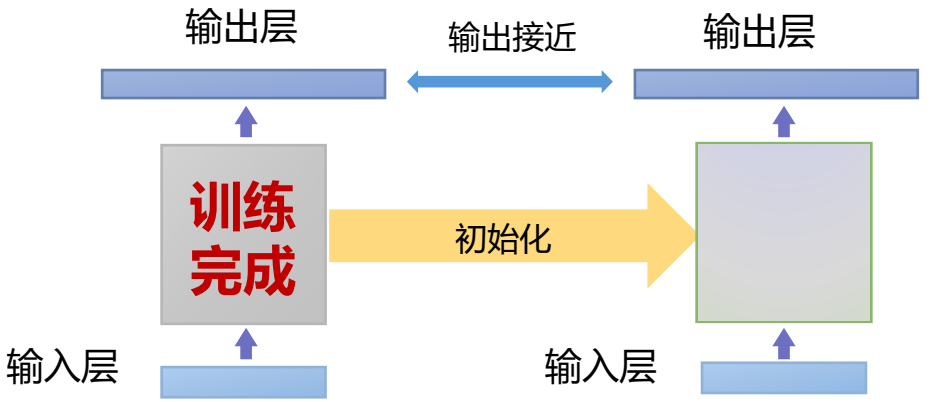
横向迁移（水平迁移）：先学习抽象的概念，再学习具体的概念



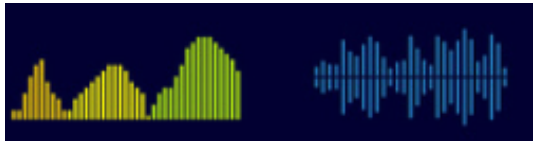
迁移学习的分类

		源数据（和任务不直接相关）	
		有标签	无标签
目标数据	有标签	**模型微调**	
	无标签		

示例：说话人自适应



配对源数据
（例如：许多人的音频数据）



配对目标数据
（例如：少量目标说话人的音频数据）

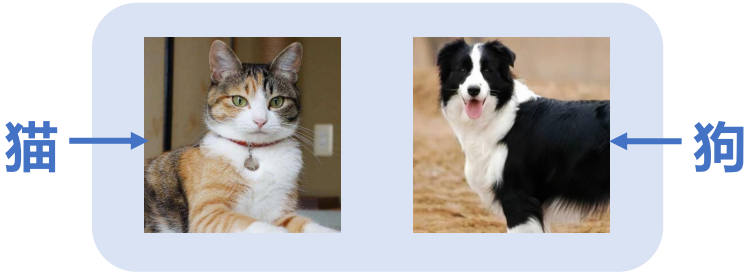
基本思想：先使用源数据对模型进行训练，再根据目标数据对模型进行微调

迁移学习的分类

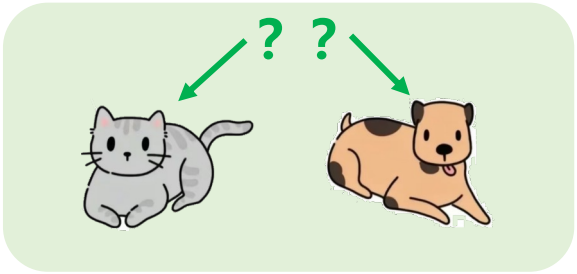
		源数据（和任务不直接相关）	
		有标签	无标签
目标数据	有标签	**模型微调**	
	无标签	**域适应**	

示例：不同领域，相同任务

- 源数据（有标签）：

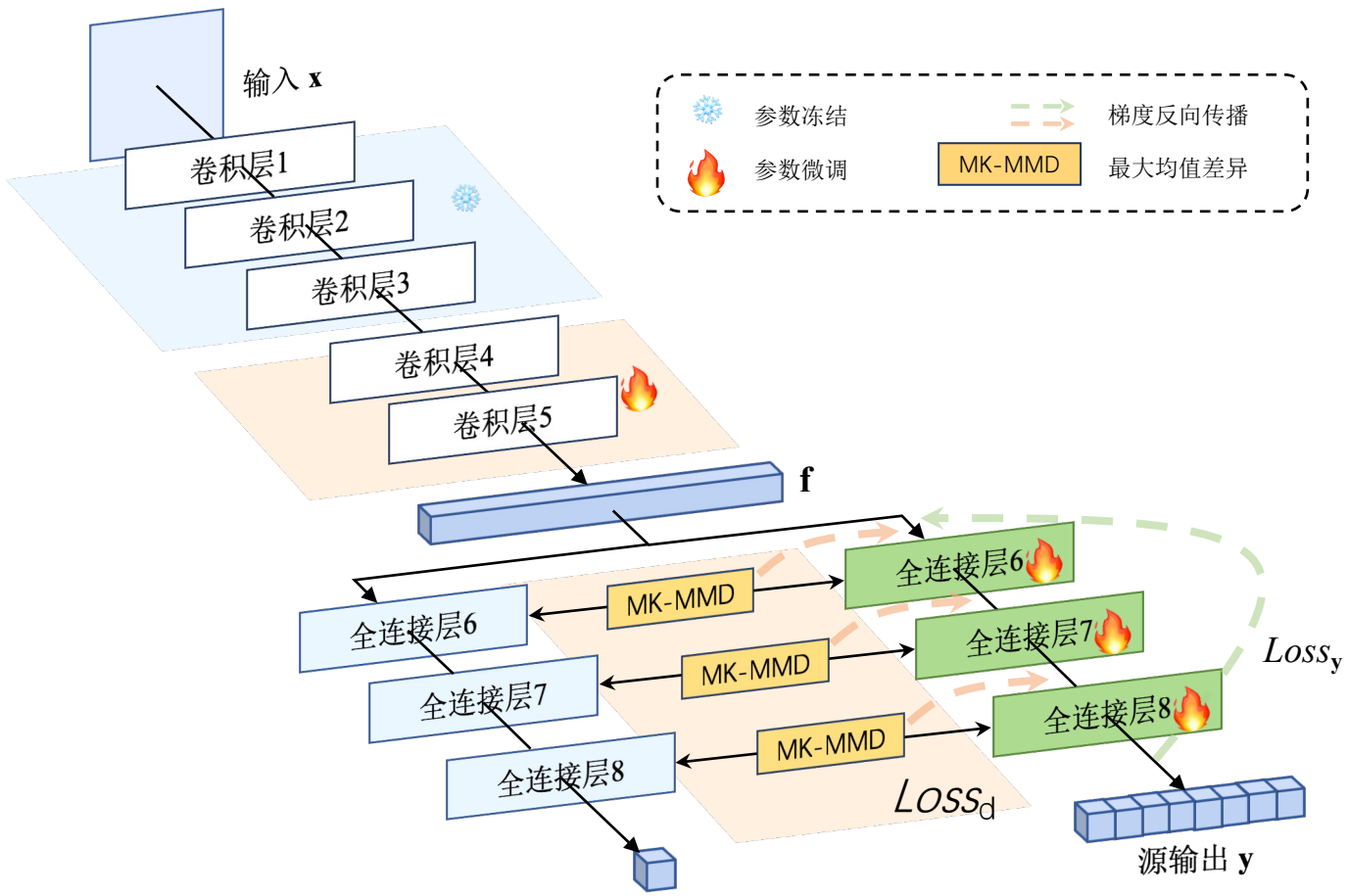


- 目标数据（无标签）：



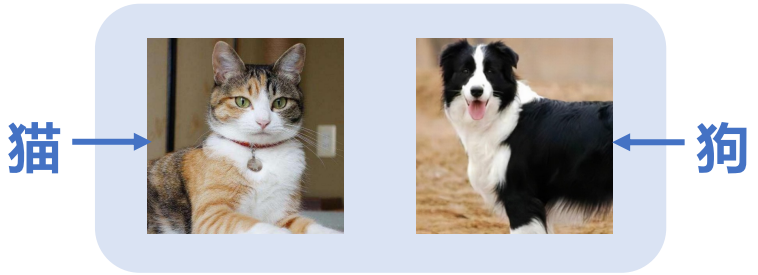
基本思想：学习“域不变特征”，实现特性对齐，利用源域标签进行监督

迁移学习的分类

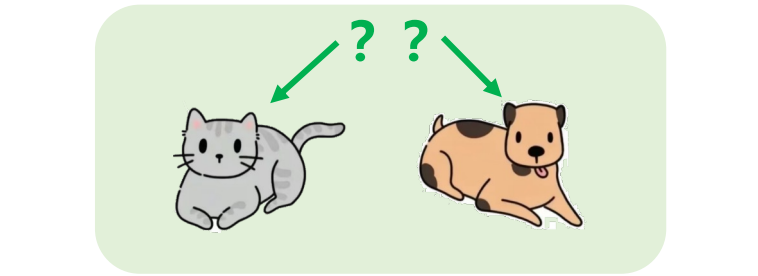


示例：不同领域，相同任务

- 源数据（有标签）：



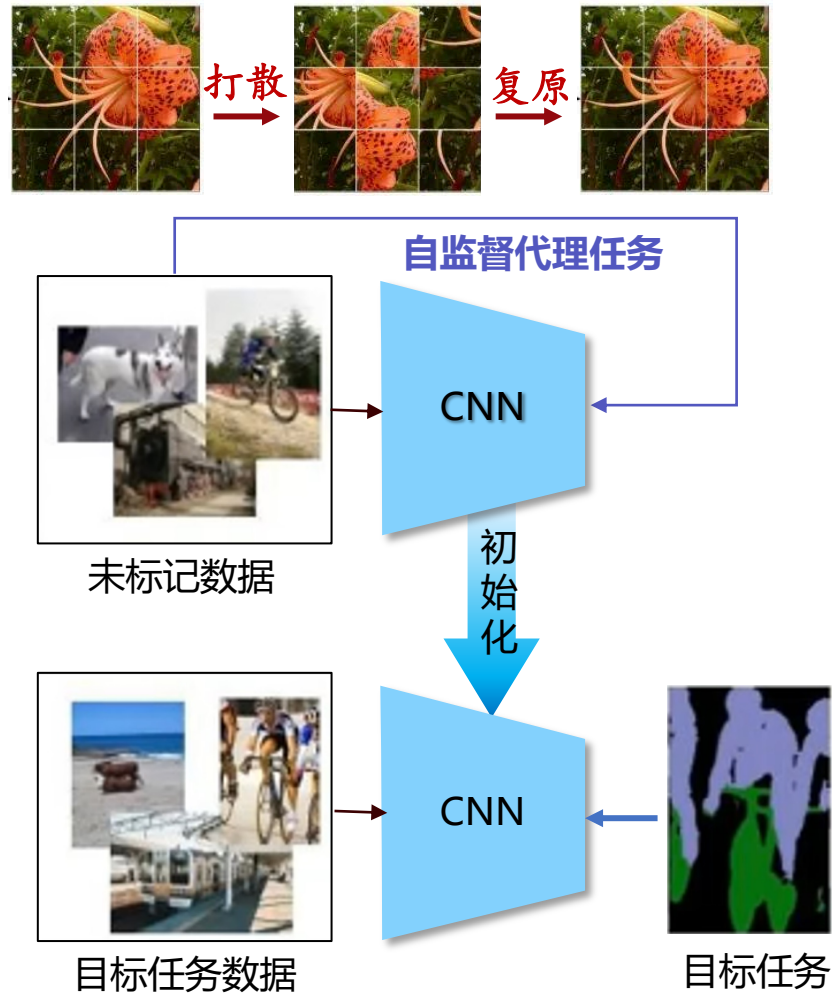
- 目标数据（无标签）：



基本思想：学习“域不变特征”，实现特性对齐，利用源域标签进行监督

迁移学习的分类

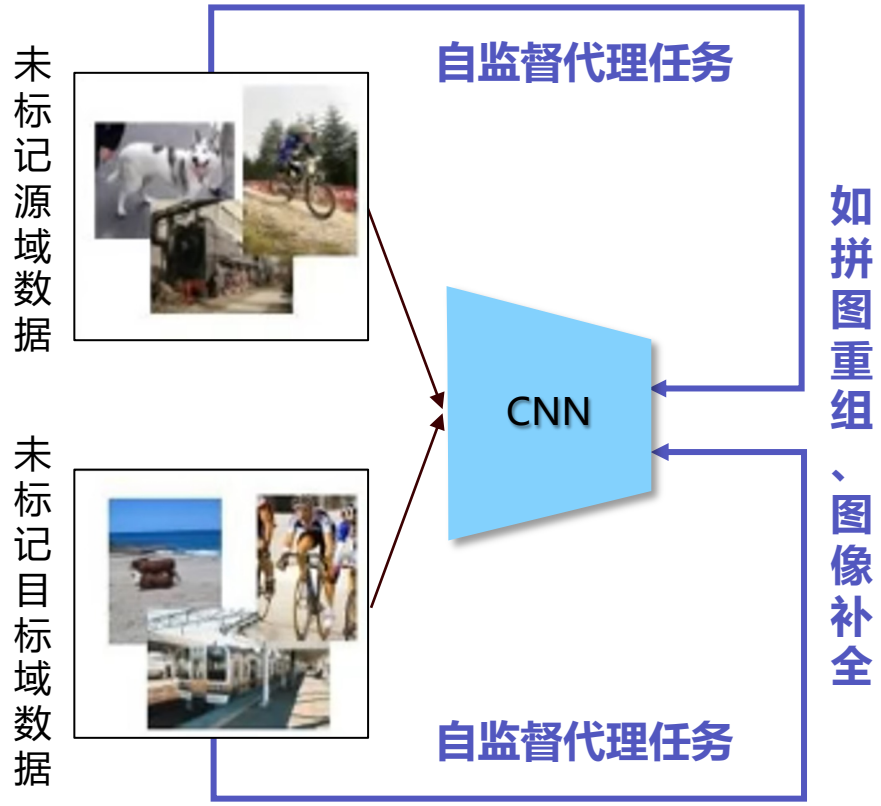
		源数据（和任务不直接相关）	
		有标签	无标签
目标数据	有标签	**模型微调**	**自学习**
	无标签	**域适应**	



基本思想：先在源域上进行自监督预训练，然后在目标域上进行有监督微调

迁移学习的分类

		源数据（和任务不直接相关）	
		有标签	无标签
目标数据	有标签	**模型微调**	**自学习**
	无标签	**域适应**	**自聚类**



基本思想：将源域和目标域的数据混合进行自监督学习以发现数据的内在结构

迁移学习的应用

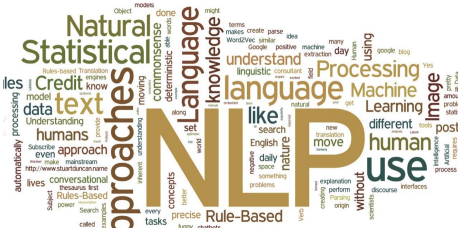
■ 迁移学习在计算机视觉、自然语言处理、推荐系统和强化学习等领域得到广泛应用

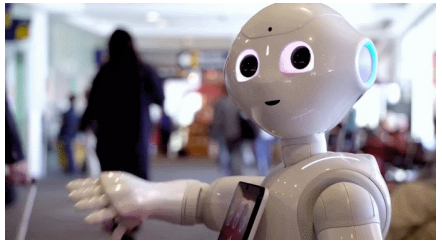
计算机视觉

- 医疗图像识别
- 安防监控识别
- 3D场景分析

自然语言处理

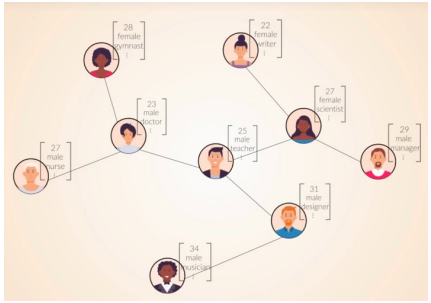
- 多语种、小语种
- 智能来哦天对话
- 跨领域文本分类





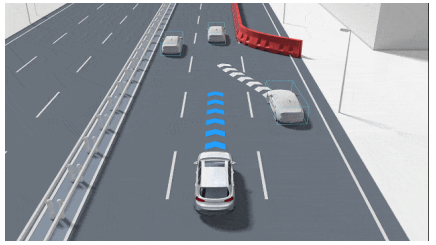
推荐系统

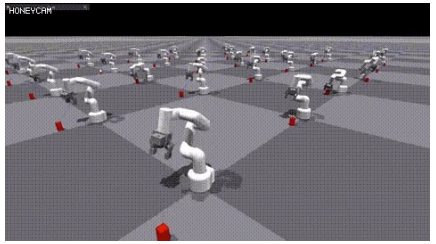
- 多用户推荐建模
- 跨平台推荐
- 季节性变化推荐



强化学习

- 多场景路面检测
- 自动驾驶
- 仿真→真实环境





迁移学习的哲学思想

- 迁移学习“**经验复用，举一反三**”的哲学思想：
  - 迁移学习体现了知识迁移的普遍性；
  - 迁移学习还体现了资源优化与效率提升的理念；
  - 迁移学习还反映了知识共享与协作的重要性；

山东大学
SHANDONG UNIVERSITY

《人工智能通识》AI For Everyone

机器学习基础

学无止境 气有浩然

教育部-华为“智能基座”课程