

## 第3章 学习的类型

### 3.1 不同输出空间的学习

#### 多类别分类：硬币识别与其它应用

任务示例——美国硬币识别 依据“尺寸、质量”两维特征，将硬币分为

$$\mathcal{Y} = \{1\text{¢}, 5\text{¢}, 10\text{¢}, 25\text{¢}\} \text{ 或抽象为 } \mathcal{Y} = \{1, 2, \dots, K\}.$$

二分类仅为  $K = 2$  的特例。

其它常见多类别问题

- 手写数字识别： $\mathcal{Y} = \{0, 1, \dots, 9\}$ ;
- 水果图像分类： $\mathcal{Y} = \{\text{苹果}, \text{橙子}, \text{草莓}\}$ ;
- 邮件优先级： $\mathcal{Y} = \{\text{垃圾}, \text{主要}, \text{社交}, \text{推广}, \text{更新}\}$  (Google)。

多类别分类在实际中应用广泛，尤其在“识别”任务中扮演核心角色。

#### 回归：患者康复预测及其应用

任务示例——患者康复预测

- 二分类：根据患者特征预测 **是否生病**;
- 多分类：根据患者特征预测 **癌症类型**;
- 回归：根据患者特征预测 **康复所需天数**，即

$$y \in \mathbb{R} \text{ 或 } y \in [\text{lower}, \text{upper}] \subset \mathbb{R}.$$

更多回归问题

- 公司数据 → 股价预测;
- 气候数据 → 温度预测。

回归在统计学中被深入研究，并作为众多统计工具的核心构件，应用极其广泛。

#### 结构化学习：序列标注问题

任务示例——词性序列标注

- 多类别分类：把单个单词映射到词性类别;
- 结构化学习：将整个句子视为一条“结构”，即为每个单词同时分配标签

$$\mathcal{Y} = \{\text{PVN}, \text{PVP}, \text{NVN}, \text{PV}, \dots\} \text{ (而非显式枚举所有组合)}.$$

更多结构化学习问题

- 蛋白质数据 → 蛋白质折叠结构预测;
- 语音数据 → 语音解析树。

结构化学习是一类高级且复杂的学习范式，需要同时预测具有内部依赖关系的整体结构。

## 3.2 基于不同数据标签的学习

### 定义 3.2.1 (监督学习 (Supervised Learning))

监督学习是从一组已标记的训练数据

$$\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$$

中学习映射函数

$$f: \mathcal{X} \rightarrow \mathcal{Y},$$

使得对于任意未见样本  $\mathbf{x}' \in \mathcal{X}$ , 模型能够给出正确输出  $y' \in \mathcal{Y}$ 。其中

- $\mathbf{x}_i$  为输入特征向量;
- $y_i$  为对应标签, 取值
  - 离散类别 (分类任务)
  - 连续实数 (回归任务)



### 定义 3.2.2 (无监督学习 (Unsupervised Learning))

无监督学习是一种在没有标签的数据集

$$\mathcal{D} = \{\mathbf{x}_i\}_{i=1}^N$$

上发现隐藏结构或分布规律的机器学习方法。其核心任务包括

- 聚类 (Clustering): 将相似样本划分为若干组;
- 降维 (Dimensionality Reduction): 在保留关键信息的同时压缩特征维度;
- 密度估计 (Density Estimation): 学习数据的概率分布;
- 异常检测 (Anomaly Detection): 识别偏离主流模式的样本。



### 无监督学习：无标签数据的洞察

**核心思想** 在只含输入  $\{\mathbf{x}_n\}$ 、不含任何标签  $y_n$  的数据中学习隐藏结构。

#### 典型无监督任务

- 聚类 (Clustering)
 

$\{\mathbf{x}_n\} \rightarrow \text{cluster}(\mathbf{x})$  ——类似“无监督多类分类”，如文章  $\rightarrow$  主题。
- 密度估计 (Density Estimation)
 

$\{\mathbf{x}_n\} \rightarrow \text{density}(\mathbf{x})$  ——类似“无监督有界回归”，如交通报告  $\rightarrow$  危险区域。
- 异常检测 (Outlier Detection)
 

$\{\mathbf{x}_n\} \rightarrow \text{unusual}(\mathbf{x})$  ——类似“极端无监督二分类”，如网络日志  $\rightarrow$  入侵警报。

无监督学习形式多样，性能目标各不相同，仍在蓬勃发展！

### 定义 3.2.3 (半监督学习 (Semi-Supervised Learning))

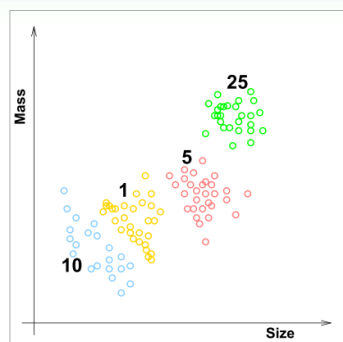
半监督学习是一种介于监督学习与无监督学习之间的混合范式。给定

$$\mathcal{D} = \underbrace{\{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_k, y_k)\}}_{\text{少量标记数据}}, \underbrace{\{\mathbf{x}_{k+1}, \dots, \mathbf{x}_{k+n}\}}_{\text{大量未标记数据}}, \quad k \ll n,$$

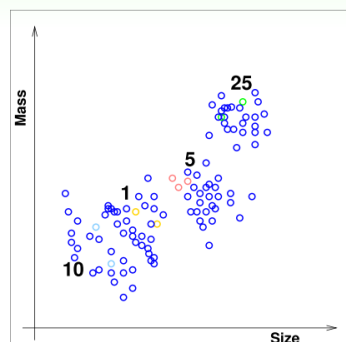
其目标是学习映射  $f: \mathcal{X} \rightarrow \mathcal{Y}$ ，使得模型既能在标记数据上拟合，又能利用未标记数据的潜在结构，从而对未知样本作出准确预测。



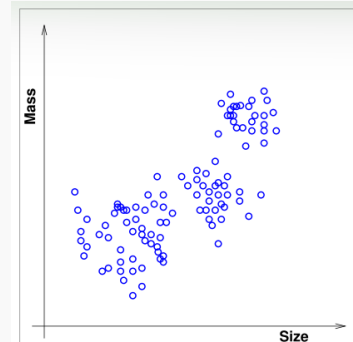
### 半监督学习：部分标签的硬币识别



监督学习



半监督学习



无监督学习

#### 其它半监督应用

- 少量人脸图像  $\Rightarrow$  Facebook 人脸识别器
- 少量医药数据  $\Rightarrow$  药物疗效预测器

核心理念：利用大量未标记数据，避免昂贵的标注成本。

### 定义 3.2.4 (强化学习 (Reinforcement Learning))

强化学习是机器学习的一个子领域，研究智能体在环境中通过执行动作、接收奖励（或惩罚）并观察状态转移，从而学习一个策略  $\pi(s)$ ，使其长期累积奖励

$$\mathbb{E} \left[ \sum_{t=0}^{\infty} \gamma^t r_t \right]$$

最大化，其中  $0 \leq \gamma < 1$  为折扣因子， $r_t$  为时刻  $t$  的即时奖励。



### 强化学习：一种截然不同却自然的学习范式

#### 训狗示例

- 命令：对狗说“坐下”
- 狗坐下  $\Rightarrow$  奖励饼干：好狗！
- 狗乱尿  $\Rightarrow$  惩罚：坏狗！

我们无法直接给出标签  $y$ ，但可通过奖励/惩罚让智能体学会正确行为。

#### 更多强化学习场景

- 顾客, 广告选择, 点击收益  $\rightarrow$  广告推荐系统
- 牌局, 策略, 赢钱金额  $\rightarrow$  二十一点智能体

本质 强化学习利用部分/隐式的奖励信号，通过序列决策不断优化策略。

### 3.3 不同协议的学习

#### 定义 3.3.1 (批量学习 (Batch Learning))

批量学习是一种离线训练方法，要求一次性使用完整数据集  $\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$  训练模型，得到最终假设  $g$ 。训练完成后模型参数冻结；若要吸收新数据，必须重新整合全部数据并重新训练整个模型。



#### 批量学习：以硬币识别为例

##### 问题设定

未知目标函数  $f: \mathcal{X} \rightarrow \mathcal{Y}$ ，其中  $\mathcal{Y} = \{1\text{¢}, 5\text{¢}, 10\text{¢}, 25\text{¢}\}$ 。

##### 批量监督多类别分类流程

1. 收集训练数据一次性获得批量样本

$$\mathcal{D} = \{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_N, y_N)\}.$$

2. 学习阶段利用全部已知数据，在假设空间  $\mathcal{H}$  中学习最终假设  $g \approx f$ 。
3. 部署阶段用学得  $g$  对新硬币进行预测。

##### 更多批量学习场景

- 批量 (邮件, 是否为垃圾?)  $\Rightarrow$  垃圾邮件过滤器
- 批量 (患者, 是否患癌?)  $\Rightarrow$  癌症分类器
- 批量患者数据  $\Rightarrow$  患者群体画像

**特点** 批量学习是最常见、最直观的训练协议：一次性收集全部数据  $\rightarrow$  一次性训练  $\rightarrow$  一次性部署。

#### 定义 3.3.2 (在线学习 (Online Learning))

在线学习是一种机器学习方法，其中数据按序列顺序到达。学习者在每一步  $t$  观察样本  $(\mathbf{x}_t, y_t)$  (或其部分信息)，并立即更新模型参数  $\mathbf{w}_t$ ，使得对未来数据  $\mathbf{x}_{t+1}$  的预测误差最小化。与一次性使用全部数据的批量学习不同，在线学习能够实时适应数据流和概念漂移，尤其适用于大规模或实时场景。



**在线学习：持续进化的垃圾邮件过滤器****批量垃圾邮件过滤器**

一次性学习已标记样本  $\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$ ，之后用固定假设  $g$  进行预测。

**在线垃圾邮件过滤器（顺序流程）**

1. 观察邮件  $\mathbf{x}_t$ ;
2. 用当前假设  $g_t$  预测是否垃圾;
3. 获得期望标签  $y_t$ ，立即更新  $g_t \leftarrow g_t + \Delta(\mathbf{x}_t, y_t)$ 。

**与所学知识的联系**

- PLA 可直接改为在线协议（逐点更新）;
- 强化学习常采用在线方式（奖励信号逐帧到达）。

**核心思想** 通过顺序接收数据实例，使假设持续自我改进。

**定义 3.3.3 (主动学习 (Active Learning))**

主动学习是一种半监督机器学习范式，其训练集由

$$\mathcal{D} = \{\text{少量标记样本}(\mathbf{x}_i, y_i)\}_{i=1}^k \cup \{\text{大量未标记样本}\mathbf{x}_j\}_{j=k+1}^N$$

组成。算法通过

$$\mathbf{x}_q = \arg \max_{\mathbf{x} \in \mathcal{U}} \text{Uncertainty}(\mathbf{x})$$

主动选取最不确定或信息量最大的样本  $\mathbf{x}_q$ ，向标注者查询标签  $y_q$ ，然后迭代更新模型，从而在总标注量远小于随机标注的情况下达到同等甚至更高的预测精度。

**主动学习：通过提问来学习****协议对比**

- 批量：一次性“填鸭式”喂数据
- 在线：被动地顺序接收数据
- 主动：顺序地提问

**未知目标函数**  $f: \mathcal{X} \rightarrow \mathcal{Y}$

**主动学习流程**

1. 学习器主动选择最有价值的样本  $\mathbf{x}_n$ ;
2. 查询其标签  $y_n$ （由人工或 oracle 提供）;
3. 用新样本  $(\mathbf{x}_n, y_n)$  更新假设，使  $g \approx f$ 。

**目标** 通过战略性提问，用更少的标签获得同等甚至更优的性能。

## 3.4 不同输入空间的学习

### 定义 3.4.1 (具体特征 (Concrete Features))

具体特征是直接从领域知识或物理测量中获得、具有明确物理意义的输入变量。它们通常表现为可解释的数值、类别或简单统计量，例如：

- 硬币识别中的“尺寸、质量”；
- 信用审批中的“年龄、年薪、负债”；
- 医疗诊断中的“血压、体温、肿瘤直径”。

与原始或抽象特征相比，具体特征无需额外转换即可被机器学习算法直接利用，因而更易于解释与建模。



### 具体特征示例

#### 信用审批实例

年龄 = 23 岁

性别 = 女

年薪 = NTD 1,000,000

居住年限 = 1 年

工作年限 = 0.5 年

当前负债 = NTD 200,000

#### 更多具体特征

- 硬币识别：尺寸、质量
- 信用审批：客户信息
- 癌症诊断：患者信息

**特点** 具体特征往往融入人类领域知识，是机器学习中最易于利用的输入。

### 定义 3.4.2 (原始特征 (Raw Features))

原始特征是从原始数据源直接获取、未经任何转换或加工的基本属性或测量值，例如图像的像素值、文本中的单词、传感器的原始读数等。这些特征通常：

- 具有明确的物理意义；
- 可能包含噪声、冗余或高维信息；
- 需要经过清洗、降维或特征提取才能有效应用于机器学习模型。



### 原始特征：数字识别问题

**任务描述** 数字识别是典型的监督多类别分类问题：将输入特征映射为数字含义。

#### 原始特征示例

- **16×16 灰度图像**  
 $\mathbf{x} = (0, 0, 0.9, 0.6, \dots) \in \mathbb{R}^{256}$ ，像素值物理意义简单，对机器学习更具挑战。
- **人工提取的“具体特征”**  
 如对称性、密度等，便于模型直接使用。

#### 其他原始特征场景

- 图像像素、语音信号等
- 通常需人工或机器进一步转换为具体特征后方可高效学习。

**结论** 原始特征往往缺乏明确的物理意义，需要额外处理才能被机器学习算法充分利用。

### 定义 3.4.3 (抽象特征 (Abstract Features))

抽象特征是指从原始数据经人工或算法加工后得到、不再具备直观物理意义的中间表示，例如：

- 用户-商品 ID 对（用于评分预测）；
- 节点编号或哈希编码（用于图网络）；
- 高维稀疏向量（如 one-hot 编码的广告 ID）。

这些特征需进一步转换或嵌入才能被机器学习模型有效利用。



### 抽象特征：评分预测问题

**任务描述** KDDCup 2011 评分预测：给定历史 (userid, itemid, rating) 三元组，预测某用户对新商品的评分。这是一个回归问题，其中

$$y \in \mathbb{R} \text{ (评分)}, \quad \mathbf{x} = (\text{userid}, \text{itemid}) \in \mathbb{N} \times \mathbb{N}.$$

**特点** 特征本身缺乏物理意义，对机器学习更具挑战。

#### 更多抽象特征场景

- 在线辅导系统中的学生 ID (KDDCup 2010)
- 在线广告系统中的广告 ID

**结论** 抽象特征必须借助特征转换、提取或构造，才能被模型有效利用。

## 3.5 总结



### 笔记 [学习的类型]

- 输出空间不同：分类、回归、结构化学习。
- 数据标签不同：监督学习、无监督学习、半监督学习、强化学习。
- 交互协议不同：批处理、在线学习、主动学习。
- 输入空间不同：具体特征、原始数据、抽象表示。