



## 人工智能数学原理与算法

# 第三讲 机器学习介绍

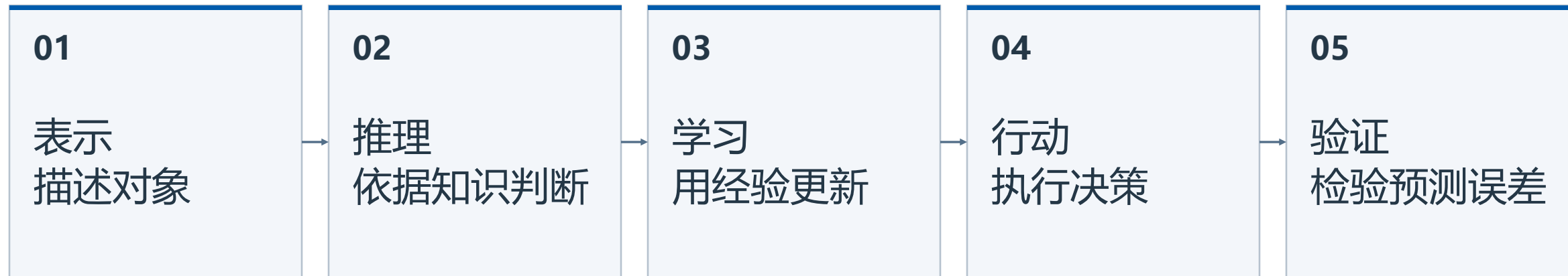
任务与经验 模型与训练 性能与验证

胡素磊 husulei@ustc.edu.cn

中国科学技术大学

# 从知识与推理到机器学习

前两讲讨论表示与推理；本讲研究系统如何利用经验改进模型。



上一讲：知识表示与推理  
本讲：经验如何改进模型  
后续：学习算法的具体实现

学习通过经验更新模型，更新效果需要重新检验。

# 本讲学习目标

能够说明一个学习系统的任务、训练依据与适用条件。

01

## 会定义

任务 T  
经验 E  
性能 P

02

## 会拆解

数据与特征  
标签与模型  
损失函数

03

## 会分类

按学习信号  
区分主要方法

04

## 会评价

判断过拟合  
选择评价指标

05

## 会迁移

分析实际系统  
与科学应用

用这些概念分析具体应用，并解释模型表现好或差的原因。

# 本讲内容

按“定义—应用—概念—分类—发展—示例”的顺序展开。

## 01 定义

什么变化才算学习？

## 02 应用

哪些任务适合机器学习？

## 03 概念

如何用数据训练模型？

## 04 分类

监督信号从哪里来？

## 05 发展

主要方法怎样发展？

## 06 示例

如何完成欺诈识别？

最后以欺诈识别贯通数据处理、模型训练、评价与部署。

# 为什么难以写出全部规则？

表达方式和使用场景不断变化，逐条补充规则往往难以覆盖新情况。

## 课堂问题

为垃圾邮件写三条识别规则。分别举出一封会被误拦的正常邮件，以及一封能绕过规则的垃圾邮件。

## 讨论要求

先给出规则，再用反例检查它的适用范围。

关键词：出现“中奖”

发件人：陌生地址

行为：短时大量群发

当规则难以穷举时，可以利用样本学习输入与输出的关系。



# 第一部分 机器学习的定义

程序怎样利用经验改善性能？

任务、经验与性能指标

# Samuel (塞缪尔) 的跳棋程序

1959年, Arthur Samuel (阿瑟·塞缪尔) 研究利用对弈经验改进跳棋程序。

## 任务

根据当前棋局选择走法

## 经验

已有棋局、自我对弈与胜负反馈

## 改善

改进局面评价, 提高对弈表现



Samuel (塞缪尔), Some Studies in Machine Learning Using the Game of Checkers, 1959

对弈提供反馈, 程序据此调整局面评价, 并检验棋力是否提高。



# “无需逐条编程”是什么意思？

程序员设计学习过程，模型从数据中确定具体的预测关系。

## 经验的作用

从样本中学习预测关系，无需人工列出每一种输入的答案。

例如：从样本学习邮件特征。

## 人的作用

确定任务，选择数据和模型；  
规定评价方法。

例如：规定可接受的误拦比例。

设计学习方法与目标 → 用数据确定参数 → 检验未见样本表现

任务、数据、模型结构和评价方法仍需设计，训练过程也需要检验。

# 显式编程：按给定规则计算

将已知规则写成程序，计算机按照确定步骤生成结果。



例：按已知公式计算圆的面积；公式本身无需从样本中学习。

规则清楚且稳定的任务，通常适合直接编程。

# 机器学习：从样本估计关系

输入与输出关系难以直接写出时，可以从样本中训练预测模型。

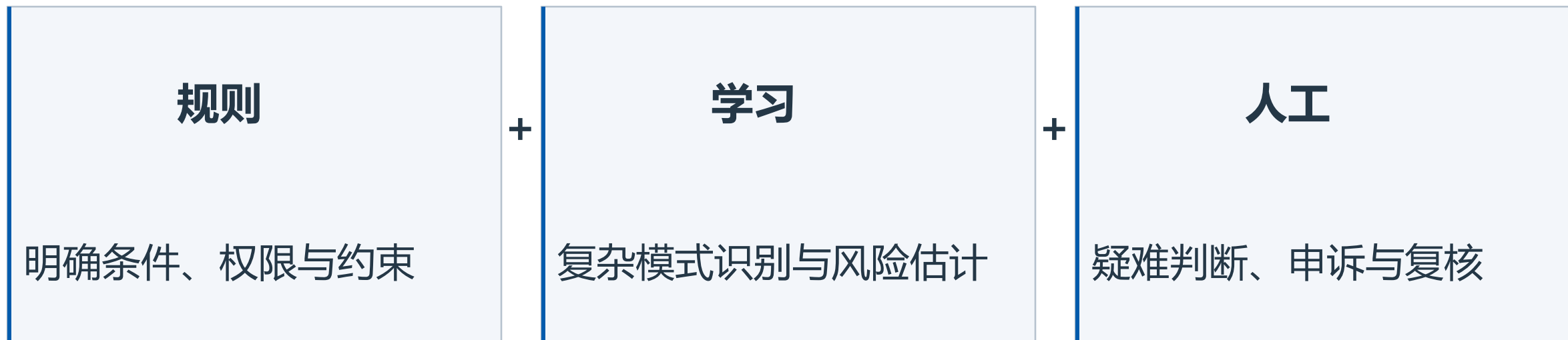


例：使用带标签的邮件学习分类模型，再判断新邮件是否属于垃圾邮件。

训练得到的模型能否用于新样本，需要独立测试。

# 规则、学习模型与人工判断

实际系统常同时使用规则、预测模型与人工复核。



贷款审核：资格条件检查 + 欺诈风险预测 + 疑难案件复核

根据任务要求分工：规则检查明确条件，模型估计风险，人工处理疑难情况。

# Mitchell (米切尔) 的学习定义

若程序在任务  $T$  上的性能  $P$  随经验  $E$  而改善，就称它从经验中学习。

$$P_{\text{after}} > P_{\text{before}}$$

以“数值越大越好”的指标为例，比较学习前后的独立测试表现

## T · 任务

要完成什么任务？

## E · 经验

经验来自哪些  
数据或反馈？

## P · 性能

用什么指标衡量表现？

必须同时说明：做什么、用什么经验、怎样衡量进步。

# 西瓜识别中的 T、E、P

把“识别好瓜”写成任务、训练经验和评价指标。

## T · 任务

根据西瓜的可观测属性，  
判断好瓜或坏瓜。

输出为两个离散类别。

## E · 经验

历史样本包含属性记录  
与好坏标签。

明确好坏的判定标准。

## P · 性能

独立测试集上的  
分类准确率等指标。

测试样本不参与  
训练或调参。

样本来源、好坏标准与测试条件，都会影响最终结论。

# 用 T、E、P 描述不同任务

学习任务不同，训练经验与性能指标也会改变。

| 任务   | T：任务   | E：经验     | P：性能       |
|------|--------|----------|------------|
| 图像识别 | 判定对象类别 | 带标签图像    | 独立测试准确率    |
| 语音识别 | 语音转文字  | 音频—文本对   | 字/词错误率     |
| 围棋   | 选择落子   | 棋谱与自我对弈  | 对局胜率       |
| 对话   | 生成有用回复 | 文本、反馈与交互 | 任务成功率与人工评价 |

比较应用时，要同时比较数据来源、反馈方式与评价指标。

## 反馈如何用于更新模型？

模型生成输出后，可利用标签、胜负或实际结果进行下一轮训练。



模型更新与性能评价是两个步骤；更新参数并不保证表现改善。

# 人工智能、机器学习与深度学习

深度学习属于机器学习；机器学习是实现人工智能的一类方法。

## 人工智能 AI

### 机器学习 ML

#### 深度学习 DL

使用多层可学习表示的方法

- 01 符号推理、搜索与规划也属于人工智能
- 02 决策树、支持向量机  
是其他机器学习方法
- 03 大模型应用还需检索、  
工具与系统集成

应区分方法与系统：完整应用还需要数据处理、工具和测试。

# 课堂判断：学习与泛化

区分“训练过程发生变化”与“对新样本的表现确有改善”。

## 课堂问题

以下哪些情形提供了学习证据？哪些进一步支持模型能够泛化？

## 讨论要求

分别检查经验、参数变化与独立测试表现。

A | 计算器按固定公式得到正确结果

B | 训练集准确率从 60% 升到 99%

C | 新增训练样本后，独立测试表现稳定提升

D | 系统把所有训练样本逐字存储并复现

训练集表现提高可以反映拟合进展，但不足以证明泛化能力。

## 本部分小结：怎样判断学习有效

塞缪尔的跳棋程序展示经验的作用；米切尔用任务、经验和性能界定学习。

### 任务

明确要完成什么

### 经验

说明数据与反馈来自哪里

### 性能

用可比较的指标检验改善

学习问题：任务  $T$ 、经验  $E$ 、性能  $P$ ，以及相应的评价条件

报告学习效果时，说明训练条件，并用独立样本检验泛化。



## 第二部分 机器学习的应用

怎样把应用需求表述为学习任务？

从日常应用到科学计算

# 机器学习的主要应用

机器学习从数据中估计模式，用于识别、预测、生成和决策。



## 感知

图像识别、计算机视觉、语音识别

## 预测

风险评估、需求预测、数值估计

## 生成

文本生成、翻译、图像生成

## 决策

推荐、博弈、控制与资源配置

同一种方法可以用于多类任务，实际效果取决于数据与任务要求。

# 搜索引擎：学习相关性排序

从检索得到的网页中，优先呈现与查询相关、对用户有用的结果。

## 输入

查询词、上下文与可检索网页

## 学习对象

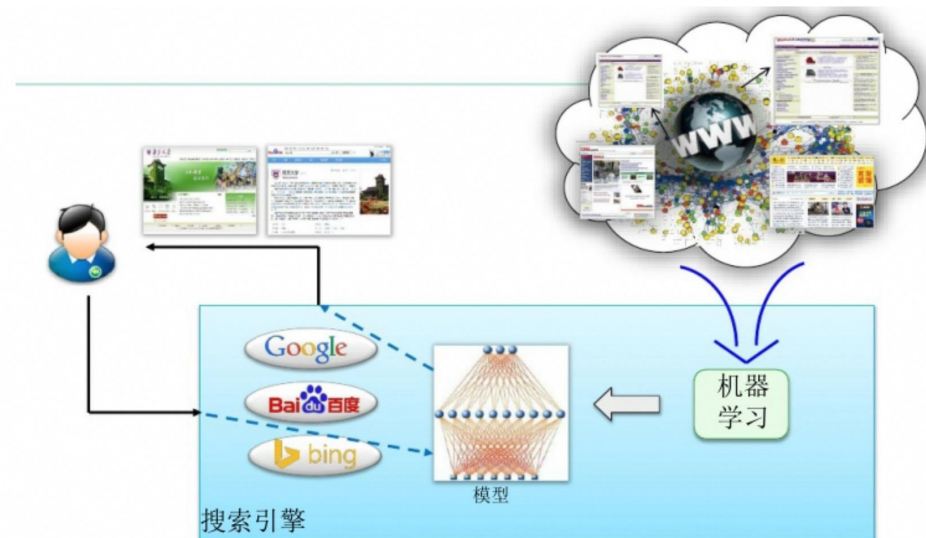
查询与网页之间的相关性

## 反馈

点击、停留时间与人工评价

## 困难

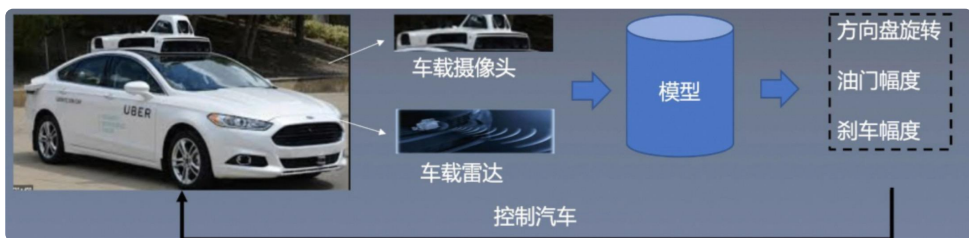
排名越靠前，越容易获得点击



点击量受到展示位置影响；训练时需区分内容相关性与位置偏差。

# 自动驾驶：感知、预测、规划与控制

车辆需要识别周围环境，预测其他道路参与者的运动，并执行驾驶动作。



## 感知

识别车道、车辆、行人与障碍物

## 预测

预测周围车辆和行人的运动

## 规划

选择可行轨迹与目标速度

## 控制

执行转向、加速与制动

安全取决于整个系统，还需检验反应时延与少见复杂场景。

# 艺术鉴定：分析可量化的风格特征

笔触、纹理和构图可形成统计特征，但作品数量有限，真伪标签也可能有争议。

## 可观察证据

局部笔触、纹理、色彩与构图统计

## 标签来源

专家判断、档案与材料检测

## 核心困难

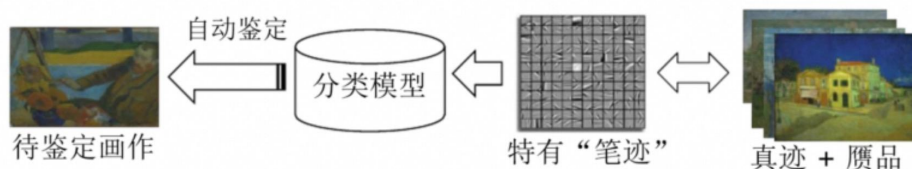
样本少，修复与模仿会影响特征



图像分析提供辅助证据，鉴定仍需结合来源记录、材料检测与专家判断。

# 艺术鉴定研究：如何理解实验结果

研究者分析作品的笔触与风格差异，评价结果仍需结合实验条件。



## 梵高作品研究 (2008)

101幅作品：82幅归属明确  
6幅非梵高，13幅归属有争议  
研究比较了多种图像分析方法。

## 勃鲁盖尔素描研究 (2004)

8幅真迹与5幅仿作，在特征空间中分开。  
这并不等于独立测试集上的100%准确率。

训练与测试应按作品划分，防止同一作品的图块同时出现在两侧。

来源：IEEE Signal Processing Magazine, 2008; PNAS, 2004。完整文献见备注。

# 古代手稿：从大量碎片寻找关联

碎片可能来自同一手稿，却分藏于不同地点；书写、尺寸和内容可用于寻找关联。



## 碎片化

残缺、散佚使原始关系丢失

## 退化

污损、褪色和扫描差异影响比较

## 规模

碎片数量增加，两两比较迅速增多

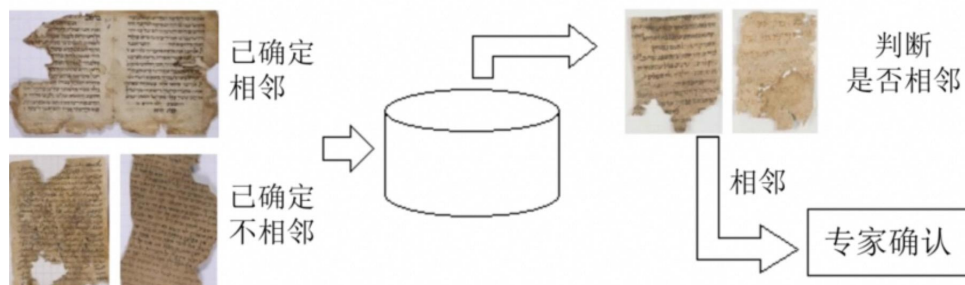
## 专业性

语言、年代和书写习惯需专家判断

模型先筛选可能相关的碎片，专家再结合文字与史料判断。

# 开罗藏经库手稿：相似度辅助关联

系统为可能属于同一手稿的碎片排序，由专家核实关联。



## 输入

碎片图像与已有编目信息  
提取笔迹、尺寸和版面特征

## 模型

计算碎片之间的相似度  
筛选可能相关的配对

## 核验

优先呈现高相似度候选  
专家核实手稿关联

2011年的研究报告约1000项新关联得到核实。  
评价还应包括确认比例，以及节省的检索时间。

来源：IJCV, 2011; ICCV, 2011。完整文献见备注。

# 科学应用：结构预测与天气预报

AlphaFold 3 与 GraphCast 将机器学习用于生物分子结构与全球天气预测。

01

AlphaFold 3 · 2024

预测蛋白质、核酸与小分子组成的复合物结构。

与已知实验结构比较；结构预测不等于证明药物有效。

02

GraphCast · 2023

用历史再分析数据训练，预测未来天气状态。

对历史时段回测，与数值预报比较；另需检验极端事件。

分析这两个案例：任务是什么？经验从哪里来？怎样评价？

科学应用同样需要定义任务、比较基准，并检验适用条件。

# 应用前需要回答的四个问题

从数据、目标、验证和适用范围检查一个机器学习应用。

## 数据

样本从哪里来？  
覆盖哪些场景？

样本不足或偏差  
会影响学习。

## 目标

标签或奖励  
对应什么目标？

训练目标应与  
实际需求一致。

## 验证

测试独立吗？  
指标是否合适？

结果应可复现、  
可比较。

## 边界

在哪些条件下  
可能失效？

使用后需要  
监测与复核。

模型名称相同，数据条件和评价目标不同，应用效果也可能完全不同。

## 课堂练习：定义一个学习任务

选择一个应用，写出任务 T、经验 E、性能 P 和一个失败场景。

### 课堂问题

五人一组，选择下列一个任务，写出 T、E、P，并说明一个可能失败的场景。

### 讨论要求

先讨论数据与目标，再说明评价指标和使用条件。

校园人脸门禁

课程推荐

数学作业批改

语音助手

说明需要收集哪些数据，以及如何判断模型真的有用。



## 第三部分 机器学习的基本概念

数据怎样决定模型参数？

特征、标签、损失、优化与泛化

# 数据集：样本的集合

数据经过采样、测量和整理形成数据集；这里以带标签的数据集为例。

$$D = \{(x_1, y_1), \dots, (x_n, y_n)\}$$

## 样本

一次观测的对象  
或事件，如西瓜

## 采样

决定采集哪些对象

## 测量

将属性记录为  
数值或类别

## 有限性

有限样本难以  
覆盖所有情况

数据集的覆盖范围有限，学习结果应结合采样条件解释。

# 特征与标签：模型的输入和目标

特征  $x$  描述模型可见的信息；标签  $y$  表示训练时的目标答案。

## 特征 $x$

颜色、根蒂、敲声等属性的编码

实际预测时也必须能够获得

## 标签 $y$

“好瓜 / 坏瓜” 或甜度数值

训练时已知，预测时有待推断

使用预测时无法获得的信息，会造成泄漏；标签含糊会使学习目标不明确。

特征选择影响可用信息，标签定义影响模型的学习目标。

# 模型：带参数的预测函数

模型  $f_\theta$  接收特征  $x$ ，使用参数  $\theta$  产生预测  $\hat{y}$ 。

$$\hat{y} = f_\theta(x)$$

对输入  $x$  使用当前模型，得到预测  $\hat{y}$

## 结构 $f$

线性函数、决策树  
或神经网络

## 参数 $\theta$

模型结构确定后  
需要学习的数值

## 预测 $\hat{y}$

模型按当前参数  
计算出的结果

模型结构规定可表达的关系，训练确定其中的参数。

## 西瓜分类：线性评分与阈值

将已编码的特征加权求和，再按分数是否达到阈值进行分类。

$$s = a \cdot x_1 + b \cdot x_2 + c \cdot x_3 + d$$

若  $s \geq 0$ ，则预测好瓜；否则预测坏瓜

$x_1$ 、 $x_2$ 、 $x_3$ ：特征编码     $a$ 、 $b$ 、 $c$ ：权重     $d$ ：偏置

### 权重

其他特征固定时，  
对分数的影响

### 偏置

调整评分函数位置  
以及分类边界

### 分数

特征加权结果，  
尚不是类别或概率

类别属性先做数值编码；正式建模时常用独热编码，避免人为引入大小关系。

# 参数向量：模型中需要学习的数值

把权重和偏置按固定顺序组成向量  $\theta$ ，训练就是确定这些数值。

$$\theta = (a, b, c, d)^T$$

参数顺序必须与特征及偏置一一对应

**候选  $\theta_1$**

颜色特征的系数较大

**候选  $\theta_2$**

敲声特征的系数较大

**训练问题**

哪组参数使训练损失更小？

同一模型结构可以对应多组参数，各组参数的预测表现需要比较。



## 参数改变，分类边界也会改变

同一输入在不同参数下可能得到不同分数，甚至得到相反类别。

候选模型  $f_{\theta_1}$

分数更依赖颜色

某些青绿样本被判为好瓜

候选模型  $f_{\theta_2}$

分数更依赖敲声

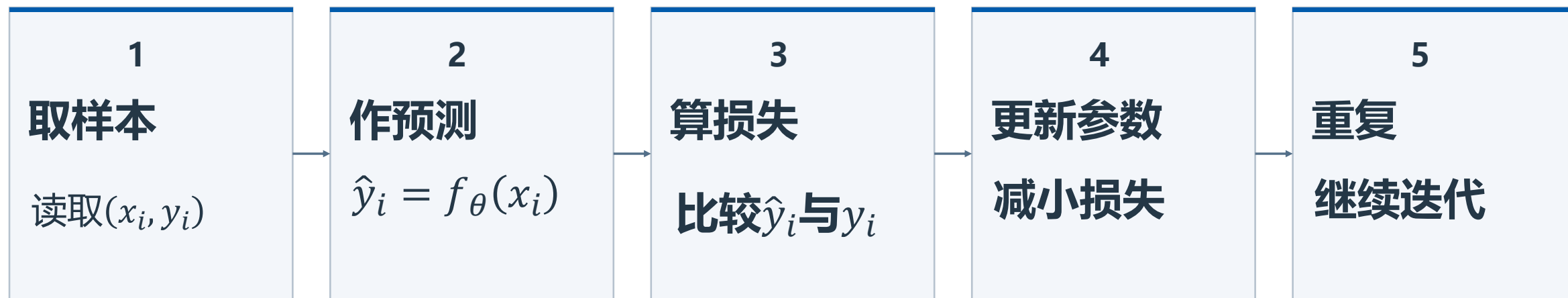
同一青绿样本可能被判为坏瓜

比较同一批样本上的预测误差，才能判断哪组参数更合适。

在结构确定后，训练通过调整参数改善模型对数据的拟合。

## 训练：比较预测与标签，更新参数

逐个或分批比较预测与标签，根据损失更新参数，并重复这一过程。



训练损失衡量拟合程度；验证集用于选择模型与训练设置。

损失函数给出比较依据，优化算法决定如何调整参数。

# 损失函数：衡量预测误差

损失  $L(y, \hat{y})$  将预测与目标的差异表示为一个数值。

经验风险 
$$R(\theta) = \frac{1}{n} \sum_{i=1}^n L(y_i, f_{\theta}(x_i))$$

将  $n$  个训练样本的损失取平均，得到经验风险

## 单样本损失

一个样本预测错多少

## 经验风险

训练样本损失的平均值

## 目标

寻找经验风险较小的参数

不同损失对误差的惩罚不同，会影响最终得到的模型。

# 常见损失函数

分类可用 0—1 损失评价对错；回归常用绝对损失或平方损失。

## 01 0—1损失

$$L = 1[\hat{y} \neq y]$$

预测错误取1，正确取0

## 02 绝对损失

$$L = |\hat{y} - y|$$

误差翻倍，绝对损失翻倍

## 03 平方损失

$$L = (\hat{y} - y)^2$$

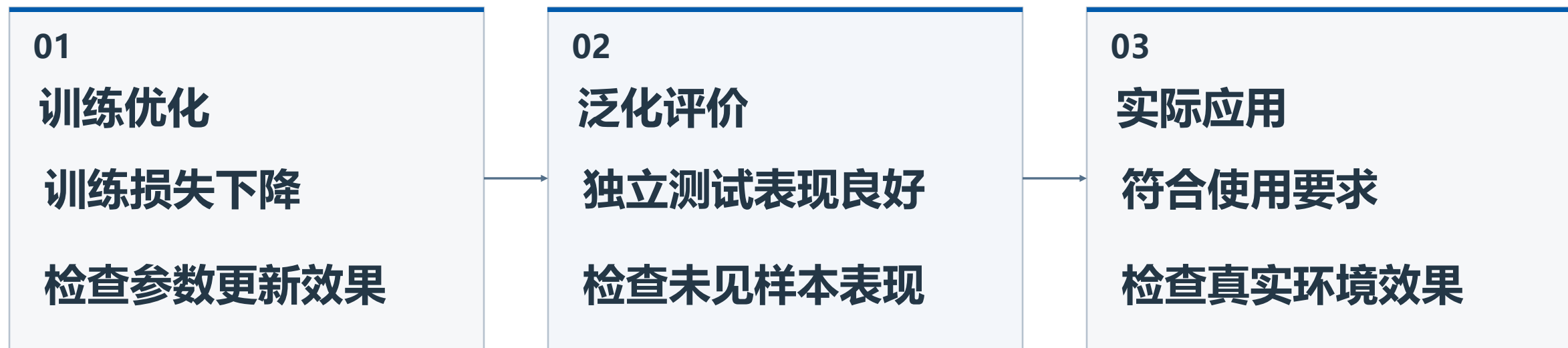
误差翻倍，平方损失变为四倍

使用相同损失和相同样本，比较候选模型的平均损失。

选择损失时，要考虑输出类型、异常值影响和优化方法。

# 优化、泛化与实际效果

优化寻找低损失参数；泛化评价检查模型能否用于未见样本。



$$\theta^* \approx \arg \min_{\theta} R(\theta)$$

训练目标达到后，仍需检验新样本表现与实际使用效果。

# 训练集、验证集与测试集

训练集学习参数，验证集选择方案，测试集评价最终模型。

**01****训练集****更新参数 $\theta$** 

可被训练过程反复使用

**02****验证集**

选择模型、超参数与阈值

用于调参和模型选择

**03****测试集**

只在方案确定后评价

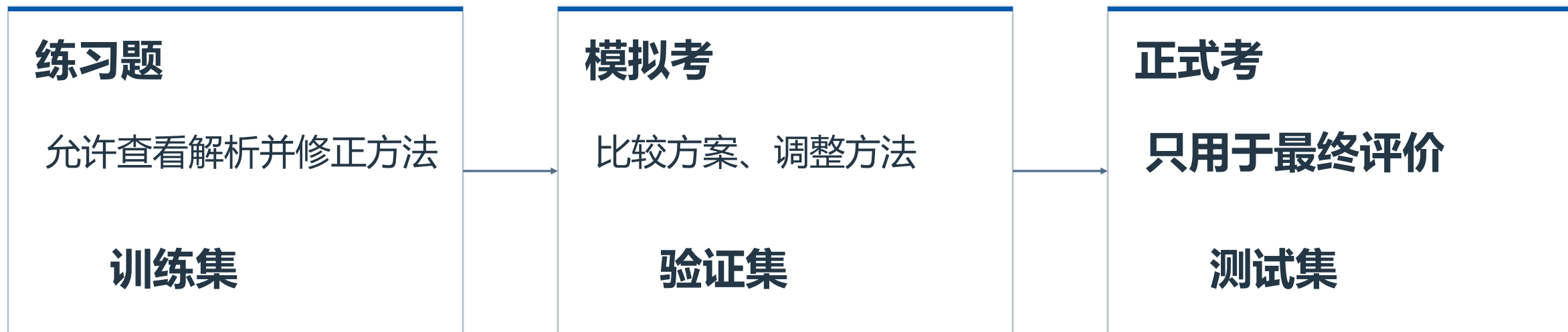
保持测试独立  
覆盖目标使用条件

数据较少时可使用交叉验证；最终评价仍应避免信息泄漏。

测试集若被反复用于调参，测试成绩也会受到选择偏差影响。

## 用考试理解三类数据

训练集对应练习题，验证集对应模拟考，测试集对应最终考试。

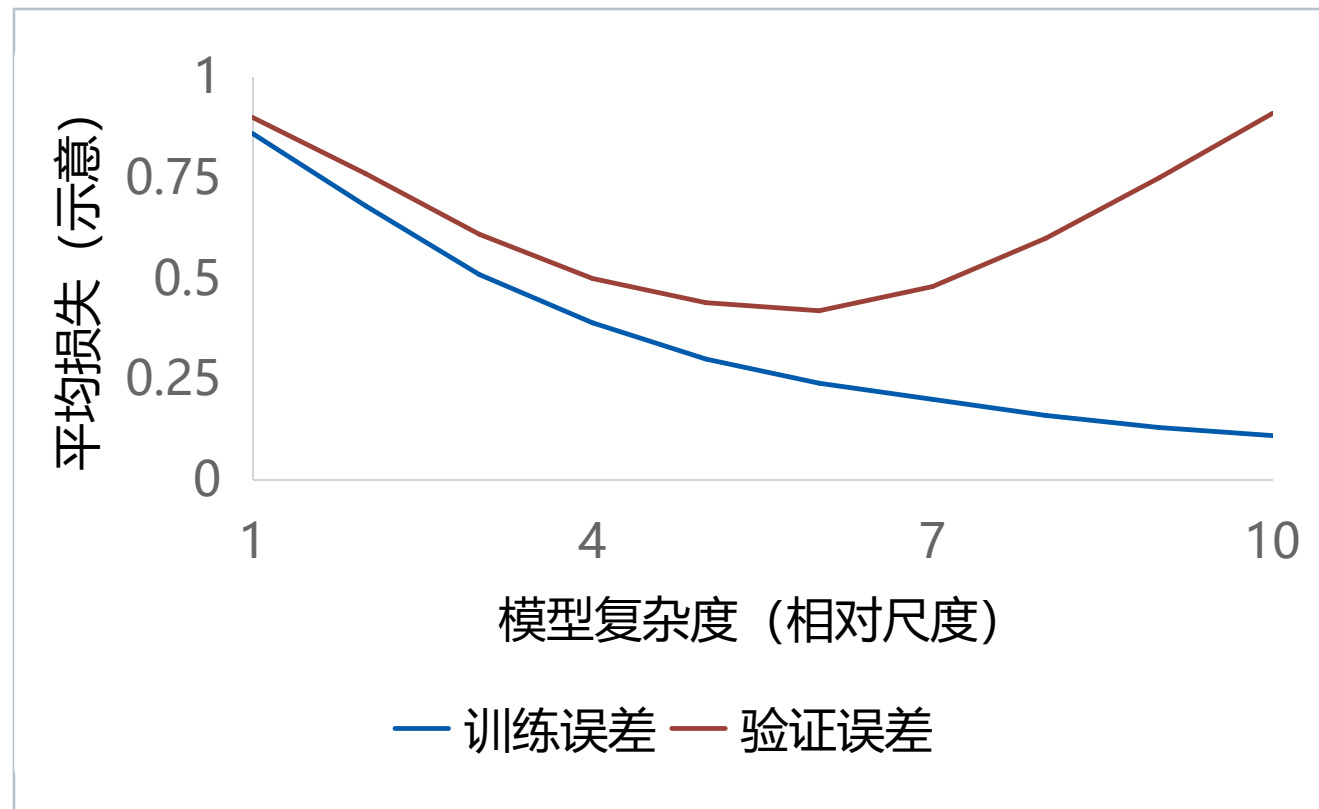


若根据测试集成绩反复修改模型，这份测试集就失去了独立评价作用。

反复针对同一套试题改进成绩，并不能充分说明解决新题的能力。

# 欠拟合、合适拟合与过拟合

模型复杂度增加，可能降低训练误差，也可能增加对噪声的拟合。



## 欠拟合

训练误差与验证误差都较高

## 合适拟合

验证误差处于较低水平

## 过拟合

训练误差继续降，验证误差反升

图中为教学示意，应根据验证数据选择复杂度。测试集用于最终评价。

# 泛化：在未见样本上保持表现

泛化能力指模型在训练时未见过的目标样本上的表现。

训练：  $D_{\text{train}} \rightarrow \theta$       检验：  $D_{\text{test}} \rightarrow P(\theta)$

## 未见

测试样本不参与训练和调参

## 分布条件

说明训练、测试与使用场景的关系

## 重复性

必要时采用重复划分或交叉验证

## 边界

数据覆盖不足时，结论应保留范围

训练目标是预测未见样本。记住训练数据，不能保证预测有效。

# 分布偏移：使用条件发生变化

季节、地区、设备或行为模式改变后，原有测试结果可能不再适用。

| 训练期         | 测试期     | 部署期           | 监测          |
|-------------|---------|---------------|-------------|
| 夏季A产地西瓜     | 同产地留出样本 | 冬季B产地与新品种     | 检查特征变化与实际误差 |
| 学习该条件下的分类关系 | 表现良好    | 特征分布或类别关系可能改变 | 需要复核与更新     |

部署后需要监测输入分布与预测表现，并根据变化重新评估模型。

# 数据泄漏：训练接触了不该用的信息

若使用预测时不可获得的信息，或训练与测试样本不当重叠，评价可能偏高。

## 可能泄漏

随机拆分每条就诊记录

同一患者的记录可能同时出现在训练与测试中

## 更严谨

按患者分组，或按时间划分

依据任务隔离相关样本与未来信息

贷款例：审批时不能使用贷款发放后才知道的“最终是否逾期”。

数据划分应对应使用任务：预测新患者，需避免同一患者跨训练集与测试集。

# 表示学习：让模型学习特征

手工方法先设计特征；表示学习从数据中学习适合任务的特征。

## 手工特征

专家先定义颜色、纹理、边缘或统计量

**便于结合领域知识**

## 学习表示

模型从像素、语音或文本中形成中间表征

减少手工特征设计，但仍需验证

原始输入 → 中间表示 → 任务输出；训练目标影响表示保留哪些信息。

深度学习通过多层变换学习表示，表示效果仍需由任务表现检验。

# 自监督学习：由数据构造训练目标

利用遮蔽、预测或配对关系，从数据本身构造学习信号。



BERT：预测被遮蔽的词；CLIP：学习配对图像与文本之间的对应。

自监督预训练可利用大量未标注数据，得到的表示还需在下游任务中检验。

## 课堂诊断：99% 准确率够不够？

类别比例不均衡时，只看准确率可能掩盖对少数类的完全漏检。

### 课堂问题

某筛查人群中患病者占 1%。模型将所有人判为健康，准确率为 99%。这样的筛查有效吗？

### 讨论要求

先算患病者的检出比例，再判断准确率是否适合这一任务。

A | 准确率很高，足以证明有效

B | 患病者召回率为 0

C | 还应检查漏诊代价与任务目标

D | B、C 都应考虑

评价前先说明任务目标，再同时检查漏检、误报与相应代价。

## 本章小结：模型怎样学习，怎样检验

训练用已有样本确定模型参数；测试检查模型能否正确处理未见过的样本。

### 学习对象

数据 $D$ 、特征 $x$ 、  
标签 $y$ 、模型 $f_{\theta}$

### 学习方法

用损失衡量误差，用优化  
调整参数

### 效果检验

验证集用于调参，测试集  
用于最终评价

数据 → 建立模型 → 优化参数 → 验证与测试

评价模型时，必须交代数据来源、训练目标和独立测试结果。



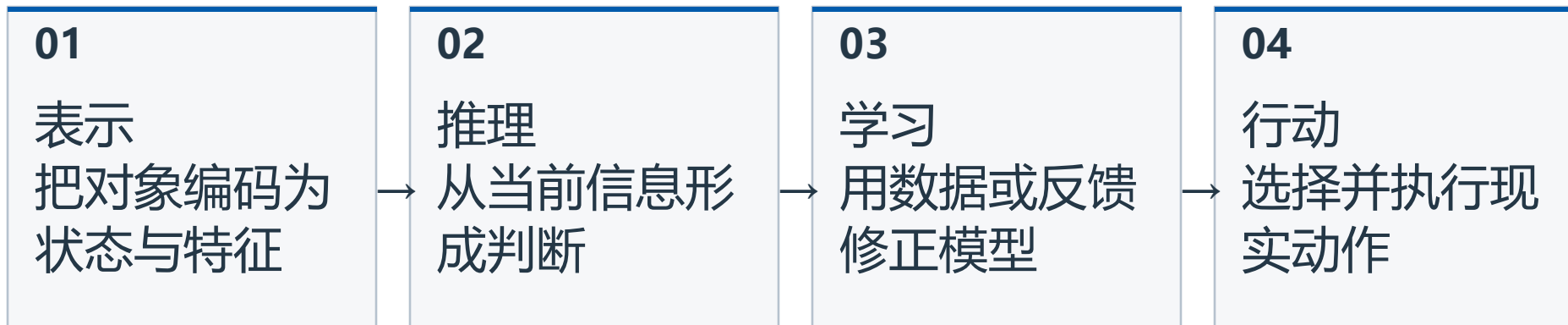
## 第四部分 机器学习的分类

不同任务从哪里获得训练信号？

监督、无监督、半监督与强化学习

# 智能系统的组成与学习信号

智能系统需要表示信息、进行推理、通过学习改进，并作出行动。这里重点看学习信号。



监督：输入—标签对  
无监督：只有输入  
强化：行动后的奖励轨迹  
自监督：从输入内部构造目标

监督、无监督、自监督和强化学习，可以用于同一个系统的不同环节。

# 四类学习方法：训练时知道什么

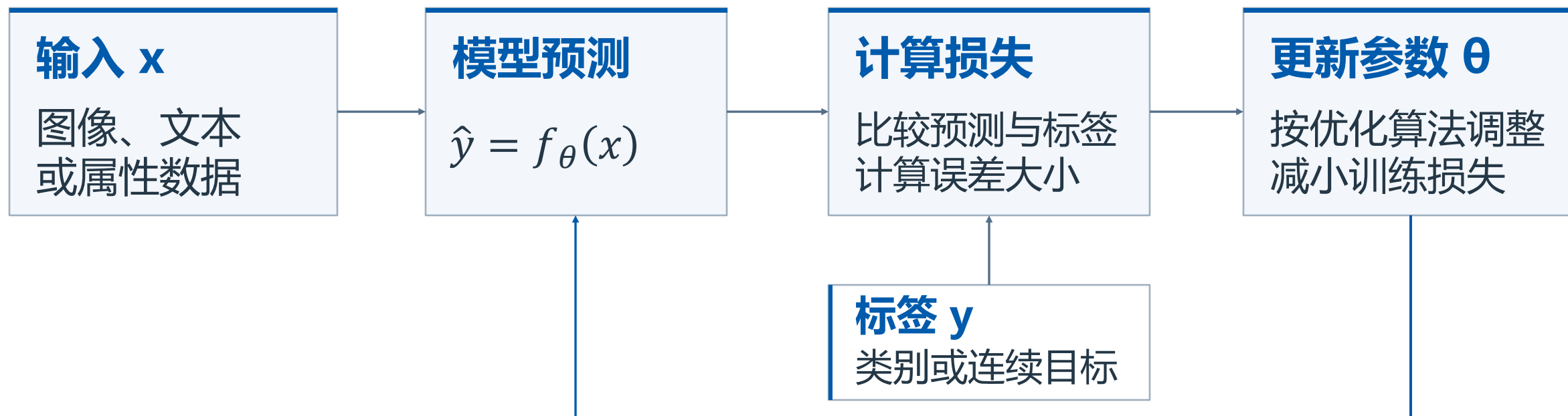
先区分训练时能看到的信息，再选择适合任务的学习方法。

| 方法    | 训练时可见信息    | 典型目标     | 主要困难     |
|-------|------------|----------|----------|
| 监督学习  | 输入与目标标签    | 预测类别或数值  | 标签成本与偏差  |
| 无监督学习 | 只有输入数据     | 发现结构或降维  | 相似性与模型假设 |
| 半监督学习 | 少量标签与无标签数据 | 改善目标任务预测 | 错误伪标签累积  |
| 强化学习  | 状态、动作与奖励   | 提高长期累计回报 | 探索和延迟反馈  |

自监督从数据本身构造目标，下一节将单独说明。

## 监督学习：预测、损失与参数更新

带标签的样本用于比较预测与真实目标，参数更新后再进行下一轮预测。



更新后的参数用于下一轮预测

例如：用带有好坏标签的西瓜样本，反复比较预测并调整模型。

“监督”来自标签提供的比较标准；训练过程通常由程序自动完成。

# 分类：输出是离散类别

分类预测离散类别；模型常先给出分数或概率，再按阈值或最大得分确定类别。

$$\hat{y} \in \{c_1, c_2, \dots, c_K\}$$

## 二分类

好瓜 / 坏瓜，欺诈 / 正常

## 多分类

手写数字0—9，物体类别

## 分数

表示模型对某一类别的支持程度

## 阈值

综合漏报与误报代价设置

二分类常用阈值作判断；多分类常选择得分最高的类别。

# 回归：输出是连续数值

回归模型预测温度、价格、时间等连续量，误差大小本身具有意义。

## 分类

预测 “是否好瓜”

输出离散类别；关注类别错误

## 回归

预测 “甜度为多少”

输出连续数值；关注误差大小

先明确要预测什么，再判断这是分类任务还是回归任务。

同一批数据可以用于不同任务：预测类别是分类，预测连续数值是回归。

# 无监督学习：从无标签数据中找结构

没有预先给定的任务标签时，可以研究样本分组、主要变化方向和异常样本。

$$D = \{x_1, \dots, x_n\} \quad \text{没有给定标签 } y$$

## 聚类

按相似程度分组

## 降维

用较少变量保留主要变化

## 密度

估计样本出现的概率分布

## 异常

找出明显偏离常见模式的样本

找到的结构取决于特征、相似性定义和模型假设，需要结合实际问题解释。

# 聚类：K-means与GMM（高斯混合模型）的直觉

K-means 将样本分给最近中心；高斯混合模型用多个高斯分布描述样本。

K-means (K 均值)

每个点归到最近中心

适合紧凑、尺度相近的分组

GMM (高斯混合模型)

计算样本属于各个成分的概率

可描述椭圆分布及模糊的组间边界

距离度量、特征尺度与簇数K会直接改变结果。

同一批样本使用不同模型，可能得到不同分组。

# 降维：PCA（主成分分析）保留主要变化方向

PCA 寻找彼此正交的主要变化方向，再把高维样本投影到这些方向。

高维  $x$  — 投影 —► 低维  $z$

主成分表示主要变化方向，不一定对应最重要的物理变量。

## 可视化

投影到二维，观察结构

## 压缩

用较少坐标近似原数据

## 去噪

当噪声主要位于小方差方向  
时有帮助

PCA 优先保留方差较大的方向；方差小的方向也可能包含重要信息。

# 监督与无监督：同一数据，不同问题

同一批西瓜属性，配有好坏标签时可训练分类器；没有标签时可研究属性分组。

## 监督问题

哪些属性组合预示“好瓜”？

预测结果与已知标签比较

## 无监督问题

按选定属性，哪些西瓜更相似？

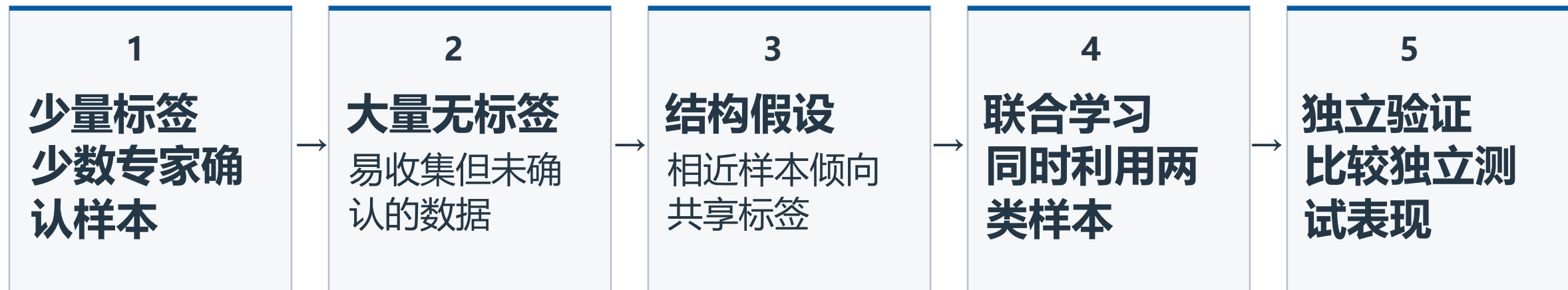
说明分组依据及其实际意义

同一批数据，问题不同，方法和评价标准也不同。

选择学习方法，既要看现有数据，也要看希望回答的问题。

# 半监督：少量标签与大量无标签数据

标注较少时，可结合大量无标签样本，改进特征表示或分类边界。



医学影像中标签常较少，设备和人群差异可能影响半监督效果。

无标签数据只有与任务相关、且满足方法假设时，才可能帮助学习。

# 自监督：从数据自身构造训练目标

把数据的一部分作为输入，另一部分作为预测目标，可在无人工标签的数据上训练。

**01**

## 预训练

预测遮蔽词或下一词元

**学习可复用的表示**

→

**02**

## 任务适配

使用标签、指令或示例

**适应具体任务**

→

**03**

## 应用检验

独立测试与部署后的反馈

发现错误并继续改进

原始数据 → 构造预测目标 → 预训练 → 任务适配

预训练得到的表示能否迁移到新任务，需要用该任务的数据检验。

# 强化学习：行动会改变未来数据

智能体在环境中观察状态、选择动作、获得奖励，并通过反复交互学习长期策略。

## 智能体

根据当前信息选择动作

## 环境

执行动作并转移到新状态

## 奖励

评价动作带来的结果，可即时或延迟

## 策略

决定在不同状态下如何行动

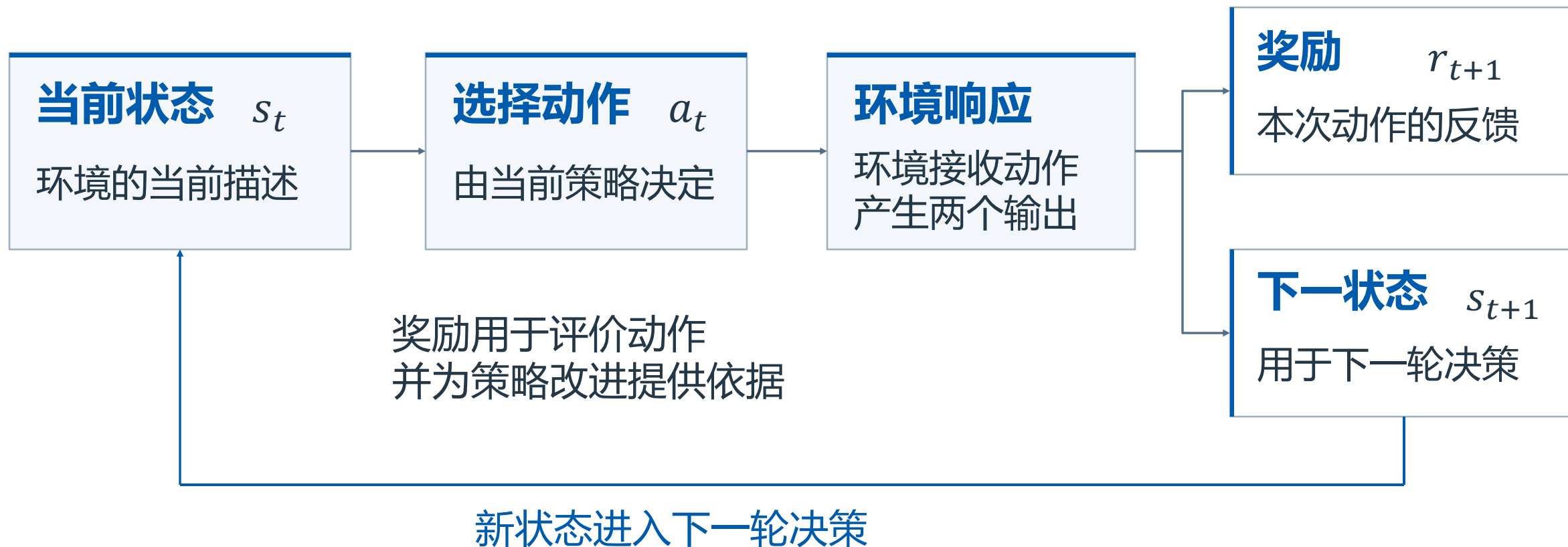


棋类决策：根据局面选择走法，再从后续局面与胜负结果中学习。

不同策略会产生不同经历，模型必须根据行动后的奖励逐步改进。

## 强化学习：环境反馈与下一轮决策

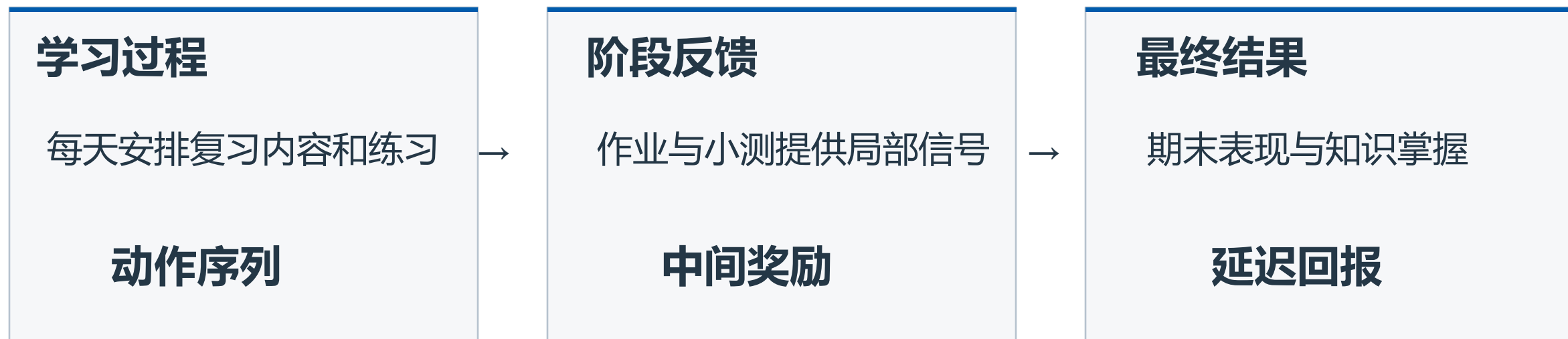
智能体选择动作后，环境同时返回奖励与下一状态，二者承担不同作用。



学习目标是提高累计回报，需要兼顾当前奖励与后续结果。

## 延迟奖励：怎样评价较早的动作

有些动作的作用要到多步以后才显现，因此不能只用眼前结果判断。



期末表现受到整个学习过程影响，不能把结果全部归因于最后一次复习。

需要估计此前各个动作对长期结果的贡献，这称为信用分配问题。

# 监督学习与强化学习的比较

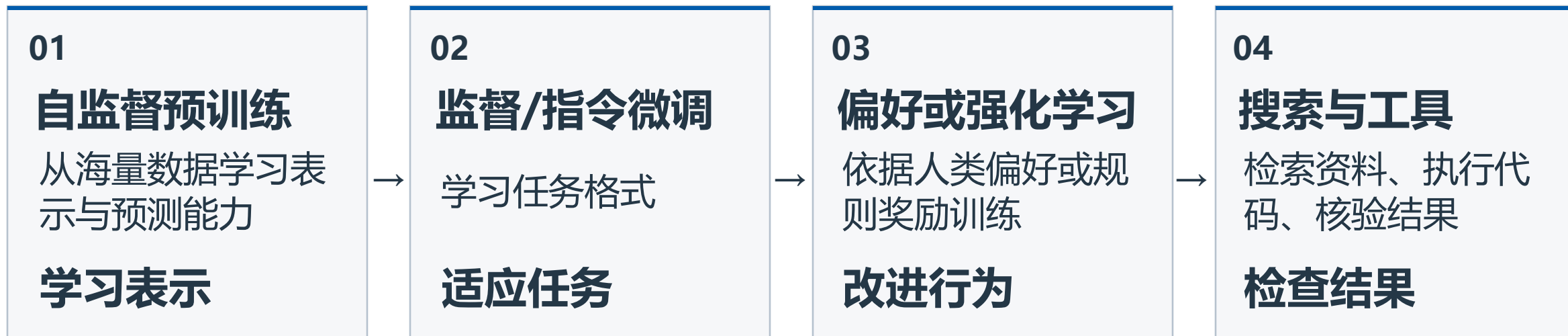
监督学习比较预测与标签；强化学习根据行动结果，改进长期决策。

| 维度 | 监督学习        | 强化学习        |
|----|-------------|-------------|
| 数据 | 通常预先给定      | 来自策略与环境的交互  |
| 反馈 | 训练样本通常有目标标签 | 奖励可能稀疏、延迟   |
| 目标 | 降低预测损失      | 提高长期累计回报    |
| 风险 | 预测错误        | 行动影响后续状态与结果 |

关键区别在于反馈的形式，以及动作是否影响后续状态和奖励。

# 现代系统如何组合多种学习方法

以语言模型为例，预训练、任务微调、偏好学习和工具使用可以协同工作。



同一系统可以组合多种方法；具体流程取决于任务。

各环节解决不同问题：学习表示、理解任务、改进行为，以及检查结果。

# 课堂选择：哪种学习范式更合适？

先说明任务提供什么学习信号，再选择方法；也可以提出组合方案。

## 课堂问题

分别选择合适的方法，再提出一种组合方案。

## 讨论规则

先独立判断，再解释：输入是什么，学习信号是什么，怎样检验效果。

A | 用已标注邮件训练垃圾邮件识别

B | 把无标签新闻按主题分组

C | 少量病理标注 + 大量未标注切片

D | 机器人在仿真中尝试抓取并获得成功奖励

判断依据：模型从哪里获得学习信号，怎样检验结果？

## 本章小结：先看学习信号，再选方法

学习信号可以来自标签、数据自身或行动奖励；不同方法可以结合使用。

### 有标签

监督学习：直接比较预测与答案

### 无标签

无监督/自监督：发现结构或构造目标

### 有奖励

强化学习：根据奖励学习决策策略

先说明现有数据和任务目标，再选择模型与训练方法。

弄清学习信号，才能判断数据需求、评价方法和可能遇到的困难。



## 第五部分 机器学习的发展

关键算法怎样发展为可用系统？

代表成果与技术演进

# 1943—1993：早期探索与发展低谷

神经网络、符号推理和专家系统先后发展，但数据、算力及应用能力限制了预期目标。

1943—1956

1956—1974

1974—1980

1980s

1987—1993

神经元模型、控制论与AI命名

**早期探索**

搜索、符号推理与早期学习

**第一次繁荣**

能力未达预期，支持有所收缩

**第一次寒冬**

**专家系统应用**

**应用繁荣**

维护成本高，适用范围有限

**第二次寒冬**

受控演示中的成功，未必能直接扩展为复杂环境下的稳定应用。

# 1990 年代至 2006 年：统计学习发展

统计学习方法逐步成熟，研究更重视泛化能力，并通过统一数据集比较模型。

**01**

## 统计学习

SVM、核方法、概率模型

研究泛化误差与预测性能

**02**

## 数据与基准

数字化数据与统一任务

便于重复实验和横向比较

**03**

## 深层表示

深层网络重获关注

推动深度学习后续发展

模型表现共同取决于表示方法、训练数据与优化算法。

经验风险、正则化和独立测试，成为分析和比较学习方法的重要工具。

## 2006—2012：深度学习的重要转折

大规模图像数据、GPU 计算和训练方法的进步，使深层网络在视觉任务中取得显著优势。



2012 年 AlexNet 的结果表明：从大量数据中学习特征，可以显著提高图像识别性能。

# 2016: AlphaGo 结合学习与搜索

AlphaGo 结合深度网络、蒙特卡洛树搜索与自我对弈，在围棋中取得突破。

1

**棋局表示**  
**当前状态**

2

**策略网络**  
**提出有希望**  
**的落子**

3

**树搜索**  
展开并比较未  
来分支

4

**价值估计**  
估计当前局面  
的获胜可能

5

**自我对弈**  
产生经验并继  
续改进

自我对弈用于训练，搜索用于落子

策略网络筛选落子，价值网络评价局面，树搜索比较后续可能性。

# 2017: Transformer改变序列建模

Transformer用注意力机制直接建模序列中元素之间的关系，并提高并行训练能力。

序列 → 注意力关系 → 上下文表示 → 预测

## 关系

计算不同位置之间的  
关联权重

## 并行

训练时可同时处理  
多个位置

## 规模

更适合在大数据与  
大算力上扩展

## 迁移

可用于语言、图像  
和科学数据

注意力机制和并行训练方式，使大规模序列学习更容易实现。

# 2022: ChatGPT 推动对话式应用

大规模预训练、指令示例和人类反馈相结合，使模型更便于通过对话完成任务。

**01**

## 预训练

根据上文预测下一个词元

学习语言与知识表示

→

**02**

## 指令微调

学习按任务要求回答

提高可用性

→

**03**

## 人类反馈训练

比较回答，训练模型改善表现

改善交互行为

语言流畅、遵循指令与事实正确，是不同的评价要求。

更容易使用，不等于每次回答都正确；事实与计算结果仍需核验。

# 近期进展：推理、工具与科学研究

模型结合强化学习、程序执行和实验反馈，开始承担复杂研究与计算任务。

01

## 推理解题

DeepSeek-R1：用强化学习改进推理解题。

关键：设计可检查的奖励。

02

## 科学研究助手

AI co-scientist  
辅助提出研究假设

关键：假设仍需实验或其他  
独立证据。

03

## 算法发现

AlphaEvolve：生成程序，用  
自动测试改进方案。

关键：评价程序必须准确对  
应任务。

共同问题：怎样获得可靠反馈，并确认性能改进确实成立。

以下选取 2025 年的代表工作，比较它们如何训练模型、检查结果。

# 深度学习的三位代表学者

2018年图灵奖表彰三位学者在深度神经网络概念与工程突破上的贡献。



Yann LeCun (扬·勒昆)  
卷积网络与视觉表示

推动卷积网络及其视觉应用

Geoffrey Hinton (杰弗里·辛顿)  
反向传播与深层表示学习

推动神经网络训练方法发展

Yoshua Bengio (约书亚·本吉奥)  
表示学习、生成模型与序列建模

推动深度学习方法与理论研究

三位学者的研究各有侧重，也与大量合作者共同推动了深度学习发展。

# 吴恩达：机器学习教育与工程实践

Andrew Ng（吴恩达）通过课程传播与工程实践，推动更多人学习和应用机器学习。



Andrew Ng（吴恩达）

- 01 面向广泛学习者的机器学习课程
- 02 重视数据质量与工程实施
- 03 从具体任务开始，依据错误逐步改进

理解算法之外，还要学会定义任务、处理数据和检查错误。

算法要被广泛应用，还需要清楚的课程、可用的工具和规范的数据流程。

# 李航、周志华：从教材系统学习方法

《统计学习方法》与《机器学习》系统介绍基本概念、典型算法和理论分析。



**李航**

**《统计学习方法》**

从模型、策略和算法三个方面展开



**周志华**

**《机器学习》**

系统介绍监督、无监督和集成学习等方法

学习顺序：明确问题 → 理解假设 → 推导目标 → 实现并检验。

教材适合补足课堂推导，并帮助比较不同方法的假设、目标和适用条件。

## 陈天奇、何恺明：两类代表成果

XGBoost 提高梯度提升树的训练效率；ResNet 通过残差连接改善深层网络训练。



**陈天奇**

**XGBoost**

高效、可扩展的梯度提升树系统



**何恺明**

**ResNet**

通过残差连接缓解深层网络优化困难

接下来：这些算法成果怎样进入实际业务与科研系统？

一种方法能否推广，既取决于预测效果，也取决于是否容易训练和使用。

# 从算法成果到产业应用

一套算法怎样成为稳定可用的服务？需要逐项解决下列问题。

| 环节 | 承担的任务      | 以欺诈识别为例      |
|----|------------|--------------|
| 数据 | 收集、核验与标注   | 历史申请与核实结果    |
| 算力 | 支持训练与实时计算  | 按时完成训练和风险评分  |
| 模型 | 学习输入与目标的关系 | 比较逻辑回归与提升树   |
| 应用 | 将输出接入实际流程  | 风险分数触发人工复核   |
| 反馈 | 检验效果并改进系统  | 记录误报、漏报与复核成本 |

下一部分将把这些环节放进同一个贷款欺诈识别案例。

## 本章小结：技术进步与应用检验

数据、算力、模型和训练方法共同推动进步；是否适用仍要由具体任务检验。

### 进步条件

数据积累、算法改进、算力与工程实现

### 共同困难

泛化不足、目标不合适及数据分布变化

### 应用要求

预测有效、运行可行，并能持续检查错误

从历史回到实践：怎样证明一个模型值得使用？

接下来用交易反欺诈案例，完整分析问题定义、模型训练和效果评价。

# 贷款欺诈识别案例

用同一组申请数据，学习任务定义、模型训练与效果评价。

**1000笔申请**

**10笔欺诈，990笔正常**

预测对象：一笔贷款申请  
输入：申请当时可取得的信息  
输出：风险分数与待复核名单

## 本节依次讨论

标签定义



数据处理



模型训练



指标与阈值

本节数值均为教学假设。风险分数用于辅助复核。

## 欺诈标签的定义

标签来自事先确定的核验规则。逾期、拒贷和材料缺失不直接等于欺诈。

| 记录类型       | 模型中的处理      | 需要保留的信息  |
|------------|-------------|----------|
| 已核验的欺诈     | 正类, $y = 1$ | 证据与确认时间  |
| 按规则标记的正常申请 | 负类, $y = 0$ | 核验依据与观察期 |
| 尚未核实、结果未成熟 | 单独标记        | 不直接记为正常  |

**训练标签**      用于学习与评价，必须能解释和复查。

高风险分数提示优先复核，不能代替事实核验或作出法律定性。

## 贷款欺诈识别的任务、经验和性能

预测时点和输出形式明确后，才能确定输入数据与评价方法。

| 要素   | 本例的具体含义          |
|------|------------------|
| T 任务 | 申请提交时估计风险，形成复核名单 |
| E 经验 | 历史申请特征及已核验的结果标签  |
| P 性能 | 报出多少欺诈，误报多少正常申请  |

### 执行约束

复核数量、处理时限、误报与漏报的代价

# 时间划分与信息泄漏

用过去的数据开发模型，用更晚的数据检验已经确定的方案。

| 数据集 | 时间与作用             |
|-----|-------------------|
| 训练集 | 较早记录：学习特征变换和模型参数  |
| 验证集 | 随后记录：选择模型、特征和报警阈值 |
| 测试集 | 更晚记录：评价已经确定的完整方案  |

**泄漏示例**      把“申请后三个月的催收次数”作为申请时的输入。

预处理只在训练集拟合。还需检查重复记录、关联样本和标签确认时间。

# 特征清洗与异常核验

先判断记录产生的原因，再决定修复、保留或删除。

| 教学记录      | 首先核验       | 可选处理     |
|-----------|------------|----------|
| 收入：2万元    | 月收入还是年收入   | 统一单位     |
| 收入：空白     | 未填写、未知或不适用 | 补值并记录缺失  |
| 学生：年收入1亿元 | 来源、单位与核验记录 | 核验后再处理   |
| 凌晨3点申请    | 背景与独立预测价值  | 作为候选特征检验 |

异常记录可能来自错误，也可能提供线索。单个异常特征不足以认定欺诈。



# 最小—最大缩放与标准化

缩放参数从训练集估计，同一变换用于验证、测试和上线数据。

## 最小—最大缩放

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

按训练集的数值范围换算  
新记录可能超出0至1

## 标准化

$$z = \frac{x - \mu}{\sigma}$$

表示偏离训练均值多少个标准差  
不会自动变成正态分布

## 教学示例：年收入14万元

训练集最小2、最大20、均值8、标准差3万元

$$x' = \frac{2}{3} \approx 0.667, z = 2$$

# 模型训练与报警阈值

训练学习模型参数，验证选择阈值，测试评价最终方案。

## 二分类交叉熵

$$L = -[y \ln p + (1 - y) \ln(1 - p)]$$

$y$ : 实际标签，欺诈为1、正常为0

$p$ : 模型对欺诈给出的风险分数

$\ln$ : 自然对数

| 实际为欺诈     | 单例损失   |
|-----------|--------|
| $p = 0.9$ | 约0.105 |
| $p = 0.1$ | 约2.303 |

**自信但错误，损失更大。**

$$p \geq \tau$$

达到阈值 $\tau$ ，进入复核名单。分数与核验结论须区分。

## 混淆矩阵：四种判断结果

固定阈值0.50，按实际类别与模型结果交叉统计1000笔申请。

| 实际类别         | 模型报出<br>进入复核   | 模型未报出           |
|--------------|----------------|-----------------|
| 实际欺诈<br>10笔  | <b>TP = 8</b>  | <b>FN = 2</b>   |
| 实际正常<br>990笔 | <b>FP = 20</b> | <b>TN = 970</b> |

**TP = 8 真正例**

欺诈被报出  
进入复核

**FN = 2 假负例**

欺诈未报出  
发生漏报

**FP = 20 假正例**

正常被误报  
增加复核与等待

**TN = 970 真负例**

正常未报出  
未增加模型复核

两行合计：10笔欺诈、990笔正常。模型共报出28笔，其中8笔为欺诈。

# 准确率、查准率与召回率

三个指标的区别在于分母：全部申请、报出的申请，还是全部欺诈。

**准确率**  
**Accuracy**

$$\frac{TP + TN}{TP + FP + FN + TN}$$

分母：全部1000笔申请

$$\frac{978}{1000} = 97.8\%$$

**查准率 / 精确率**  
**Precision**

$$P = \frac{TP}{TP + FP}$$

分母：报出的28笔申请

$$\frac{8}{28} \approx 28.6\%$$

**召回率 / 查全率**  
**Recall**

$$R = \frac{TP}{TP + FN}$$

分母：全部10笔欺诈

$$\frac{8}{10} = 80.0\%$$

## 99%的准确率，可能漏掉全部欺诈

欺诈只占1%时，把所有申请判为正常，也能得到很高的准确率。

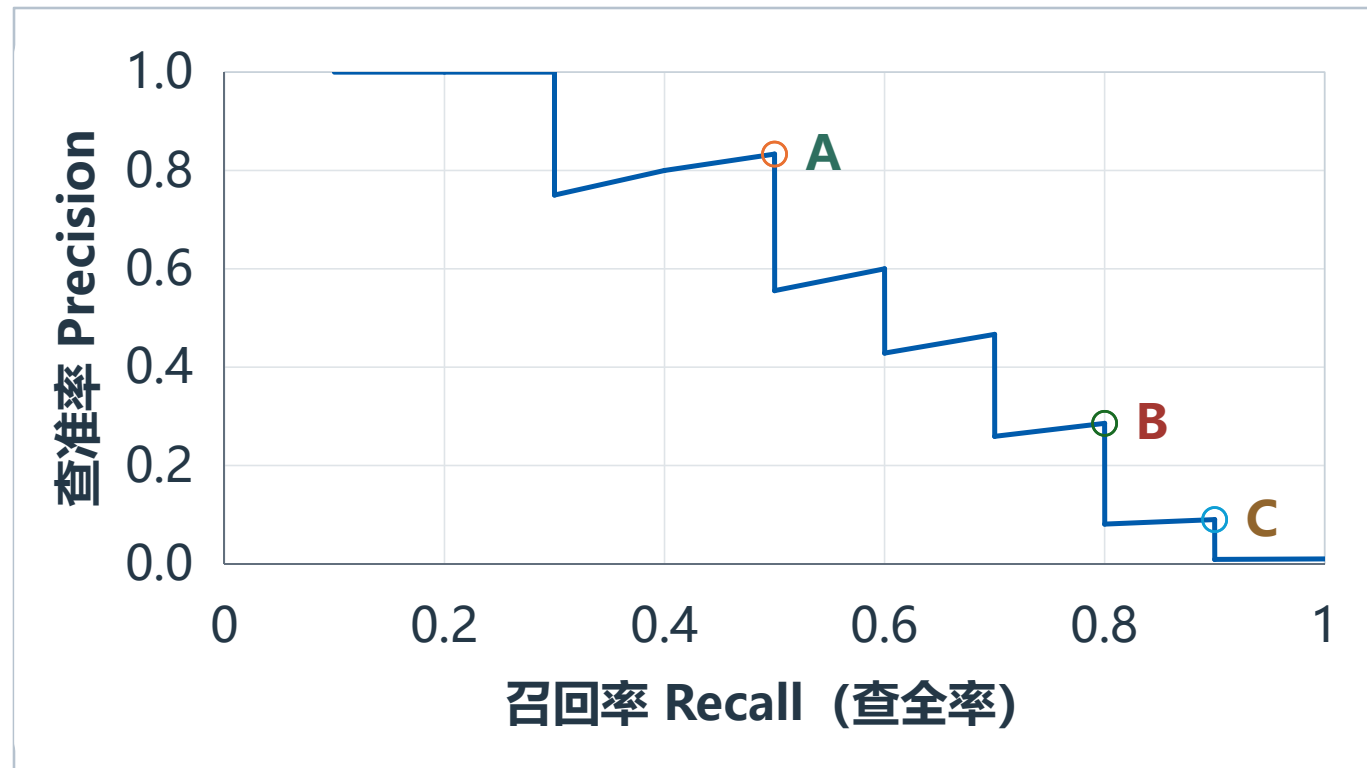
| 方案     | 报出欺诈 | 漏报欺诈 | 误报正常 | 准确率   | 召回率 |
|--------|------|------|------|-------|-----|
| 全部判正常  | 0    | 10   | 0    | 99.0% | 0%  |
| 阈值0.50 | 8    | 2    | 20   | 97.8% | 80% |

**准确率更高，不代表识别欺诈更有效。**

全判正常时没有报出，查准率的分母为0，数学上未定义。

## 报警阈值与PR曲线

横轴是召回率，纵轴是查准率。同一模型的不同阈值对应不同操作点。



降低阈值，召回率不下降。查准率可能波动。

### A 阈值0.80

报出6笔，找出5笔欺诈  
查准率83.3%，召回率50%

### B 阈值0.50

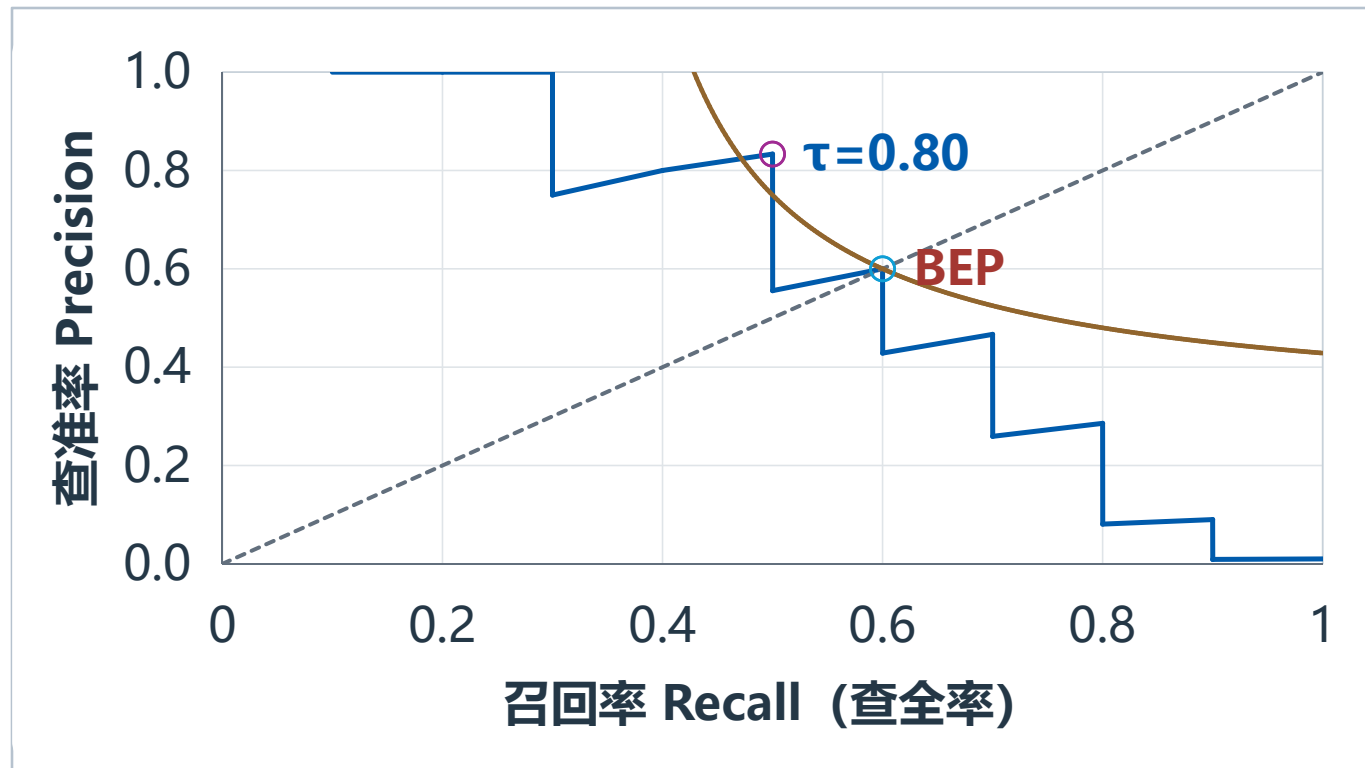
报出28笔，找出8笔欺诈  
查准率28.6%，召回率80%

### C 阈值0.20

报出100笔，找出9笔欺诈  
查准率9%，召回率90%

# PR曲线、平衡点与F1等值线

三条线分别表示模型表现、P与R相等的位置，以及同一F1数值。



**蓝色实线：模型PR曲线**

改变阈值，得到不同的P、R。

**灰色虚线：  $P = R$**   
交点为平衡点 BEP。

本例  $P = R = 0.60$

**棕色点划线：  $F_1 = 0.60$**   
线上各点的F1都等于0.60。  
它是一条等值线。

教学模拟：BEP处  $TP = 6$ ,  $FP = 4$ ,  $FN = 4$ 。

## F1的计算与三档阈值比较

F1是查准率与召回率的调和平均。平衡点不保证F1最大。

$$F_1 = \frac{2PR}{P + R} = \frac{2TP}{2TP + FP + FN}$$

| 阈值   | 复核数 | TP / FP | 查准率P  | 召回率R  | F1    |
|------|-----|---------|-------|-------|-------|
| 0.80 | 6   | 5 / 1   | 83.3% | 50.0% | 62.5% |
| 0.50 | 28  | 8 / 20  | 28.6% | 80.0% | 42.1% |
| 0.20 | 100 | 9 / 91  | 9.0%  | 90.0% | 16.4% |

**平衡点：**  $P = R = F_1 = 60\%$ 。**阈值0.80时，**  $F_1 = 62.5\%$ ，**更高。**

## 课堂决策：每天最多复核100笔

三档阈值的复核数量都不超过容量，选择还取决于额外收益和代价。

### 阈值从0.50降到0.20

| 变化        | 教学数据中的结果          |
|-----------|-------------------|
| 额外复核      | $100 - 28 = 72$ 笔 |
| 额外找出的欺诈   | $9 - 8 = 1$ 笔     |
| 额外误报的正常申请 | $91 - 20 = 71$ 笔  |

**讨论：这1笔额外欺诈的预期损失，是否足以覆盖额外复核的代价？**

## 本讲小结与课后练习

用任务、数据、损失和评价，解释一个机器学习系统怎样工作。

| 需要说清楚 | 本例对应的问题              |
|-------|----------------------|
| 任务与标签 | 预测哪笔申请，什么时间预测，标签如何确定 |
| 数据与模型 | 输入是否可取得，损失怎样指导参数更新   |
| 评价与阈值 | 误报和漏报各有多少，按什么目标选择阈值  |

### 课后练习

补充两项特征并检查泄漏；迁移到垃圾邮件识别；评价一个近期应用。