



机器学习（研究生）

机器学习基本概念

Basic Concepts, History & Applications

赵凯 上海大学

<https://kaizhao.net/teaching/shu-ml-grad>

本讲内容索引

01 机器学习的定义

定义 · 判据：参数从何而来 · 房价预测

02 发展历程

学习程序 · 反向传播与支持向量机 · 深层网络 · 无标注预训练

03 学习方式与工具

有监督、无监督与强化学习 · 回归与分类 · 自监督学习 · 编程工具

04 应用领域

数据与领域 · 结构预测与药物发现 · 疫苗、天气
与自动驾驶 · 大语言模型

05 适用边界

适用的四个方面 · 不适用的情形

06 小结

本讲要点 · 中英文术语对照 · 延伸阅读

课程信息

课程性质	研究生课程
上课安排	周一下午 · 09/14—11/02
先修要求	线性代数、概率论、多元微积分
课件发布	kaizhao.net/teaching/shu-ml-grad

考核方式

平时成绩	50%
考勤	10%
presentation	30%
QA（问答）	10%
开卷考试（可带教材与笔记）	50%

记号 各项比例均占总成绩；QA：Questions and Answers。

参考教材



周志华《机器学习》
清华大学出版社



李航《统计学习方法》
第 2 版，清华大学出版社

课程安排

2026 年秋季 · 周一下午 · 7 次到课（含考试）；每节课 45 分钟

日期	课堂安排
09/14	教师讲授 3 节 + 分组 1 节
09/21	教师讲授 2 节 + 4 组汇报 2 节
09/28	教师讲授 2 节 + 4 组汇报 2 节
10/05	国庆节放假 · 停课一次
10/12	教师讲授 2 节 + 4 组汇报 2 节
10/19	教师讲授 2 节 + 4 组汇报 2 节
10/26	教师讲授 2 节 + 4 组汇报 2 节
11/02	4 组汇报 90 分钟 + 开卷考试 2 小时

学生汇报：每组 15 分钟，其中 10 分钟 PPT 汇报，其余时间提问交流



填写分组信息



加入课程微信群

学生汇报要求

结合组员的研究方向，选取近五年的一篇机器学习交叉领域研究型论文；不接受综述

① 应用背景

实际问题是什么，为什么值得解决；用一个具体场景说明研究动机

② 任务与学习方式

分类、回归、聚类或决策；有监督、无监督或强化学习，训练信号从哪里来

③ 模型如何工作

用一个样本走完“输入 → 关键步骤 → 输出”；解释核心机制与设计理由

④ 结果与自己的理解

与什么方法比较、改善了什么；选取关键结果，说明适用条件与局限

讲解原则 费曼学习法：用自己的话、从具体例子讲起，首次出现的术语先解释；没有该领域背景的研一同学也能听懂。

任课教师



赵凯 Kai Zhao
上海大学 · 副教授
kz@kaizhao.net

机器学习 · 计算机视觉

教育背景

- 2017—2020 南开大学计算机科学与技术博士（导师：程明明教授）
- 2014—2017 上海大学硕士（导师：沈为教授）
- 2010—2014 上海大学本科

工作经历

- 2025.08—至今 上海大学副教授
- 2022.03—2025.07 加州大学洛杉矶分校博士后
- 2020.10—2022.02 腾讯优图实验室高级研究员
- 2018.09—2019.01 松下研发中心（新加坡）研究实习

记号 个人主页: <https://kaizhao.net>

课程内容

按主题编号；同一次到课可讲授多个主题

- | | |
|-------------------|-------------------|
| 1 机器学习基本概念 | 8 支持向量机与核方法 |
| 2 学习问题的形式化 | 9 无监督学习：聚类与 EM 算法 |
| 3 模型评估与选择 | 10 神经网络与特征提取 |
| 4 有监督学习：线性回归 | 11 特征降维与表示 |
| 5 线性分类：判别分析与多分类学习 | 12 图像的无标注预训练 |
| 6 决策树 | 13 语言模型的无标注预训练 |
| 7 贝叶斯分类器 | |

记号 EM：期望最大化（Expectation-Maximization）。

本讲内容

机器学习是什么、如何发展而来、怎样学习、用在哪里、何时适用

Part 1 概念与发展

从数据中确定规则

机器学习的定义

发展历程

学习方式与工具

Part 2 应用与边界

机器学习在各领域承担的环节

应用领域

适用边界

小结

01

机器学习的定义

What Is Machine Learning

定义 · 判据：参数从何而来 · 房价预测

机器学习的定义

朴素的说法

机器学习是**从数据中确定规则**的方法：人规定候选规则的范围与评判优劣的标准，程序依据数据确定具体的规则，并用于处理未见过的输入。

	人提供	机器给出
传统编程	规则	处理结果
机器学习	数据 + 标准	规则

Mitchell 的形式定义（1997）

一个程序在完成任务 T 时，其由指标 P 度量的性能随着经验 E 的积累而改善，则称该程序就 T 和 P 而言从 E 中学习。

垃圾邮件过滤

T 任务	把邮件判为垃圾或正常
P 指标	判对的比例
E 经验	用户标记过的历史邮件

记号 Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill. 该定义使“学习”可以测量：缺少 P 就无法判定是否发生了学习。周志华《机器学习》第 1 章 1.1 节 p.1 边注亦引用此定义。

判据：参数从何而来

把程序的行为拆成“人写定的代码”和“由数据确定的参数”

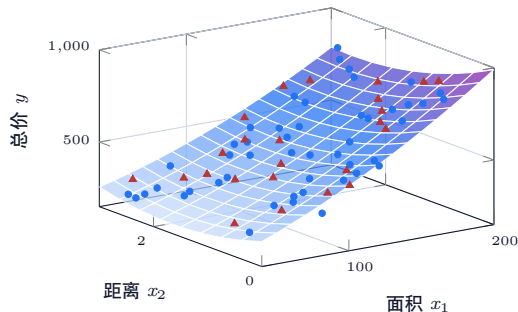
程序	机器学习	理由
快速排序；用高斯消元解线性方程组	否	行为完全由代码决定
风控规则库：月收入 < 5000 且逾期 > 2 次则拒绝	否	阈值由业务专家设定
同一套风控，阈值由历史坏账数据拟合	是	代码不变，数据变则行为变
统计每个词在垃圾邮件中的频率，据此打分	是	参数是数据的统计量（朴素贝叶斯）
数据库查询优化器，代价模型是人写的公式	否	公式与系数由人确定
同一个优化器，代价模型从执行历史学得	是	代价模型的参数由数据确定

要点 由数据确定的参数存在，且对程序行为起决定作用：这是区分机器学习程序与一般程序的实用判据。

记号 第二、三行与第五、六行两两成对：任务与代码结构相同，差别只在于参数的来源。

例：房价预测

输入：面积 x_1 (m^2)、离地铁距离 x_2 (km)；输出：总价 y (万元)



$$\hat{y} = \sum_{i+j \leq n} w_{ij} x_1^i x_2^j$$

次数 n ：人工设定；系数 w_{ij} ：从训练数据学习

次数 n	参数个数	训练误差	测试误差
1	3	27.9	29.9
2	6	21.2	26.2
3	10	15.4	38.3

问题 “由数据确定参数”的思想从何而来，又是如何发展到今天的？

记号 补充示例（非教材例题），合成数据：48 套训练房屋（●）、24 套测试房屋（▲）；曲面为 $n=2$ 的拟合结果；误差为平均绝对误差（万元）。参数个数为 $(n+1)(n+2)/2$ 。训练误差随 n 下降，测试误差先降后升。

02

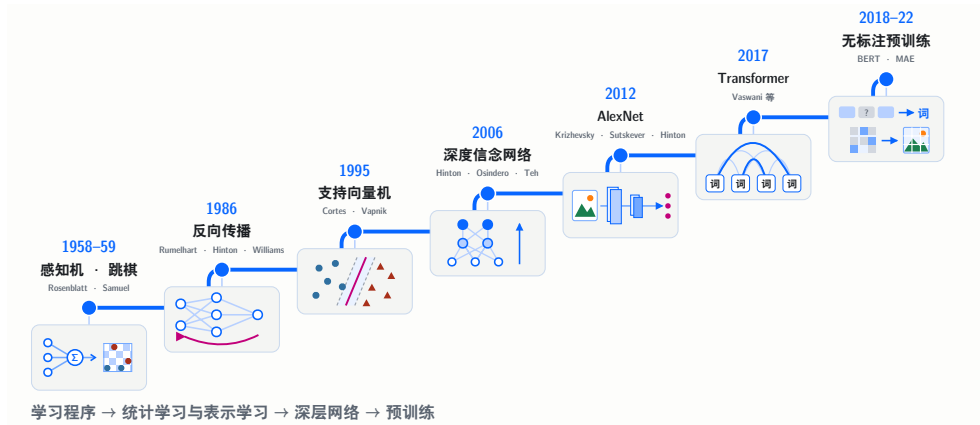
发展历程

A Brief History

学习程序 · 反向传播与支持向量机 · 深层网络 · 无标注预训练

机器学习的发展历程

各条路线长期并行；节点是代表性工作，不表示前一种技术被淘汰

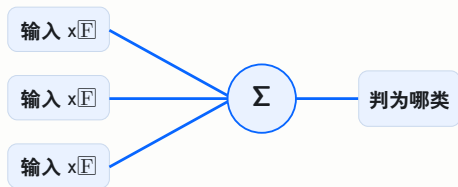


记号 年份间距为示意；上升表示方法与应用的发展，不是统一测试集上的性能曲线。

1950 年代：从经验中调整规则

Frank Rosenblatt · 1958

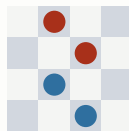
感知机 (perceptron)：学习分类权重



根据分类错误，调整连接权重

Arthur Samuel · 1959

跳棋程序：学习局面评分；论文标题中使用了 machine learning 一词



局面评分函数

对局经验 → 调整评分

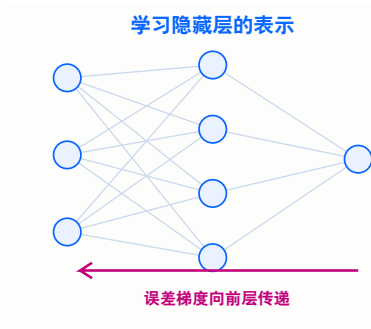
评分影响落子选择

记号 Rosenblatt, F. (1958). The perceptron. *Psychological Review*, 65(6); Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 3(3), 210–229.

1986—1995：表示学习与统计学习

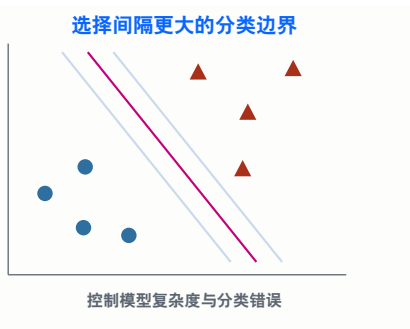
反向传播 · 1986

Rumelhart · Hinton · Williams：训练多层网络，
学习隐藏层的表示



支持向量机 · 1995

Cortes · Vapnik：选择间隔最大的分类边界



记号 Rumelhart, Hinton & Williams (1986). Learning representations by back-propagating errors. *Nature*, 323; Cortes & Vapnik (1995). Support-vector networks. *Machine Learning*, 20。

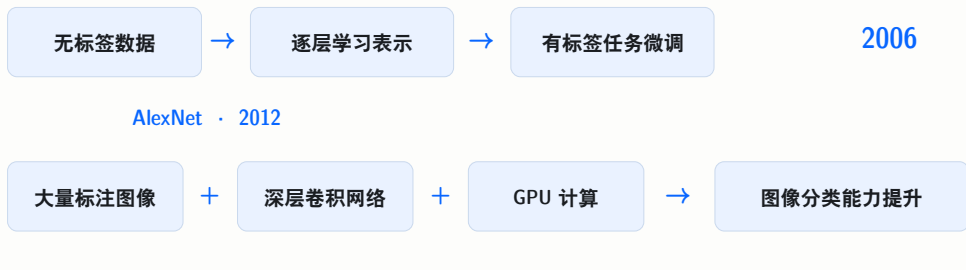
2006—2012：深层网络与图像识别

深度信念网络 · 2006

Hinton · Osindero · Teh: **逐层预训练**，为深层网络提供初始化

AlexNet · 2012

Krizhevsky · Sutskever · Hinton: 大规模标注图像 + 卷积网络 + 图形处理器



记号 Hinton, Osindero & Teh (2006). A fast learning algorithm for deep belief nets. *Neural Computation*; Krizhevsky, Sutskever & Hinton (2012). ImageNet classification with deep convolutional neural networks. NIPS。

2017—2022：注意力与无标注预训练

Vaswani 等：Transformer, 2017；用数据自身构造学习目标



问题 从房价预测到文本预训练，模型从哪里获得训练信号？不同的信号对应不同的学习方式。

记号 Vaswani 等 (2017). Attention is all you need; BERT (Bidirectional Encoder Representations from Transformers): Devlin 等, 2018 年预印本、2019 年正式发表; 遮挡自编码器: He 等, 2021 年预印本、2022 年正式发表。

03

学习方式与工具

Learning Paradigms & Tools

有监督、无监督与强化学习 · 回归与分类 · 自监督学习 · 编程工具

学习方式与训练信号

按训练信号的来源划分

有监督学习

supervised learning

面积、距离
↓ 配对
成交总价

给定输入与标签 (x, y) ；学习
输入到输出的映射

无监督学习

unsupervised learning



只给定数据 x ；发现结构、
分组或表示

强化学习

reinforcement learning

智能体 → 动作 → 环境
↑ 奖励与新状态

通过交互获得奖励；学习长
期回报更高的策略

要点 回归、分类描述**预测任务**；有监督、无监督、强化描述学习方式。二者是两个独立的维度。

回归与分类

同一套房屋的特征 x （面积、位置、户型……），预测不同的目标 y

回归 (regression): 输出**连续数值**

房屋总价

328.5 万元



分类 (classification): 输出**离散类别**

房屋用途

住宅

住宅

商铺

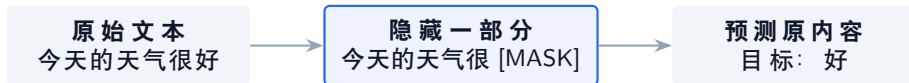
办公

要点 按预测目标 y 划分任务；回归与分类都可以用**有监督学习**完成。

记号 328.5 万元为示例输出。把类别编码为 0、1、2 不会使任务变成回归；聚类、生成等任务不属于这两类。

自监督学习：从数据自身获得目标

自监督学习（self-supervised learning）：遮住一部分数据，让模型预测被遮住的内容



预训练

用大量无人工标注的数据学习表示

下游任务

用已学到的表示完成分类、回归或生成

记号“无标注”指没有人工逐条提供的任务标签，训练时仍有目标：被遮住的原内容。自监督学习属于哪一类，见下页。

监督信息的类型

“监督”指训练时是否有人工提供的标记 y ；按标记的有无与质量划分

学习方式	训练数据中的人工标记	例
全监督学习	所有样本都有准确的人工标记	房价预测、垃圾邮件分类
弱监督学习	有人工标记，但不完全（只有部分样本有）、不确切（粗粒度）或不精确（有噪声）	只标图像类别，不标物体位置
半监督学习	少量有标记样本 + 大量未标记样本；属于不完全监督	少量标注的医学影像
无监督学习	没有任何人工标记	聚类

自监督学习 模型有目标 y （被遮住的原内容），但 y 由数据自身构造；整个学习过程不使用人工提供的标记，属于无监督学习。

记号 弱监督的三种类型见 Zhou, Z.-H. (2018), *National Science Review*, 5(1), 44–53；监督与无监督学习的划分见周志华《机器学习》第1章1.2节，p.3；半监督学习见第七讲。

机器学习的编程工具

开发环境：Python 语言 · JupyterLab 交互笔记本 · VS Code 编辑器 · Conda 环境管理

环节	工具	用途
数据模型	pandas、NumPy、SciPy	表格清洗；多维数组与数值运算；优化与统计方法
	scikit-learn	回归、分类、聚类与评估
	PyTorch、TensorFlow	张量、自动求导、神经网络训练
实验	Matplotlib、MLflow、Git	可视化；记录参数与指标；代码版本与协作
加速	CUDA	NVIDIA 图形处理器的并行计算平台，由训练框架调用

问题 同一套方法与工具，在不同领域处理的数据各不相同。机器学习在各领域承担哪些环节？

记号 CUDA：Compute Unified Device Architecture；安装 CUDA 不会使 pandas、scikit-learn 等代码自动在图形处理器上运行。

04

应用领域

Applications

数据与领域 · 结构预测与药物发现 · 疫苗、天气与自动驾驶 · 大语言模型

不同的输入数据与应用领域

机器学习从各领域的输入 x 中学习规律

图像与视频



↓
计算机视觉

目标识别 · 图像分割

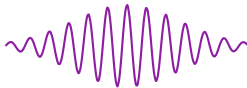
语言与文本

这篇论文研究什么？
从文本中提取信息

↓
自然语言处理

翻译 · 问答 · 文本生成

语音与音频



↓
语音与音频处理

识别 · 合成 · 分离

蛋白质与分子序列

M A L W M R L L
P L L A L L A L

↓
计算生物学

结构预测 · 分子设计

要点 领域决定数据与问题，机器学习提供从数据学习模型的方法。

记号 计算机视觉 (Computer Vision, CV); 自然语言处理 (Natural Language Processing, NLP); 各领域还有机理模型、信号处理与数值方法，机器学习是其中的重要工具。

前沿应用：六个案例

关注每个案例的输入、输出，以及机器学习承担的环节

① 蛋白质结构预测

序列 → 结构

② 小分子药物发现

分子筛选

③ 个体化癌症疫苗

抗原排序

④ 数值天气预报

预报

⑤ 自动驾驶

感知 · 规划

⑥ 大语言模型

文本生成

① 蛋白质结构预测

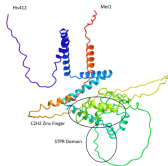
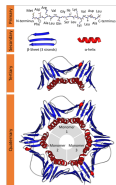
由氨基酸序列推定三维结构：生物学中悬置半个世纪的问题

基因测序
得到氨基酸序列

预测三维结构
序列 $\rightarrow$ 原子坐标

推断功能
活性位点、
结合口袋

下游应用
药物设计、酶工程



输入 x
输出 y
训练数据
替代的环节

氨基酸序列 + 同源序列比对
每个原子的三维坐标
已有的实验结构数据库（约 20 万个）
实验测定：单个蛋白耗时数月至数年

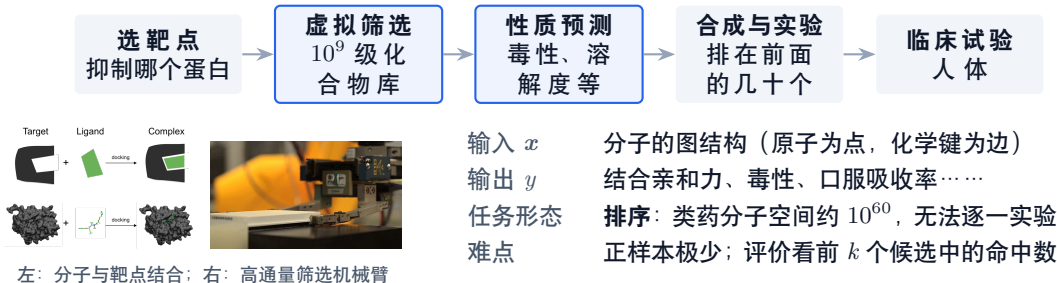
左：一级到四级结构；右：预测的三维结构

要点 蛋白质结构预测与蛋白质设计相关工作获 2024 年诺贝尔化学奖。

记号 实验测定方法：X 射线晶体学、冷冻电镜；大量蛋白无法结晶。图片：Thomas Shafee (CC BY 4.0)、Glitt006 (CC BY-SA 4.0)，维基共享资源。

② 小分子药物发现

新药研发周期约十年，投入达十亿美元量级，九成以上在临床阶段失败



要点 机器学习承担第 2、3 步；药效与安全性仍须由实验与临床试验判定。

记号 图片：Scigenis (CC BY-SA 4.0)，维基共享资源；美国国家过敏与传染病研究所（公有领域）。

3 个体化癌症疫苗

Moderna 与默沙东联合开发的 V940：为每位患者定制



机器学习承担第 3、4 步

- 每位患者的肿瘤突变不同
- V940 编码最多 34 种肿瘤新抗原
- 优先筛选可能激活免疫反应的候选

输入	肿瘤突变 + 患者免疫特征
输出	被呈递的概率
任务形态	排序，筛选候选新抗原

结果 三期试验中，V940 与免疫治疗联用，较单用免疫治疗延长了黑色素瘤患者术后无复发、无远处转移的生存时间。

记号 呈递：细胞把抗原片段展示在表面，供 T 细胞识别；新抗原：肿瘤突变产生、可被免疫系统识别的蛋白片段；信使 RNA (messenger RNA, mRNA)。来源：Moderna 与默沙东联合公告，2026-08-19。

④ 数值天气预报

观测同化这一步不变；被替换的是“时间推进”这一环

传统做法

观测同化
卫星、探空
→ 初始场

解偏微分方程
逐步推进，
超算数小时

机器学习做法

观测同化
这一步不变

神经网络推进
学习“当前场
→ 6 小时后”



输入 / 输出 当前 / 数小时后全球网格上的气压、温度、湿度、风场

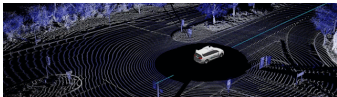
训练数据 四十余年的再分析资料

要点 欧洲中期天气预报中心的机器学习预报 2025 年 2 月转入业务运行；热带气旋路径等指标提升可达约 20%，算力低几个数量级。

记号 再分析资料 (reanalysis)：历史观测经同化得到的规整网格数据；图片：NASA / NOAA (公有领域)。

⑤ 自动驾驶：感知与预测

传感器 → 感知（目标识别与定位）→ 预测（其他参与者的未来轨迹）



左：图像中的目标识别；右：激光雷达点云中的三维目标

环节	模型输出
感知	类别、位置、速度
预测	未来轨迹的分布



Waymo：多传感器融合

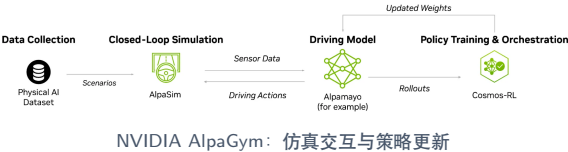
记号 感知动图截帧：© Waymo LLC, Waymo Driver Handbook: Perception (2021-10-28); 车辆照片：Dilu (CC BY 4.0), 维基共享资源。

5 自动驾驶：决策与规划

“别人可能怎么走”之后，决定“自己准备怎么走”

环节	输出
决策	让行、跟车、变道
规划（planning）	位置与速度轨迹
控制	转向、加速、制动

强化学习：在仿真交互中优化驾驶策略
奖励：避碰、行驶进度、舒适性



记号 强化学习（Reinforcement Learning, RL）；规划也可采用搜索与数值优化，不必全部由强化学习完成。图：© NVIDIA，官方技术文章 Figure 1。

⑥ 大语言模型



ChatGPT
OpenAI



Claude
Anthropic



Gemini
Google DeepMind



DeepSeek
深度求索

常见训练流程

预训练：海量文本上预测下一个 token，无需人工标注

监督微调：少量高质量问答示范

偏好对齐：人工成对比较
→ 奖励模型 → 强化学习

训练目标

训练方法

注意力机制

后训练

预测下一个 token

梯度更新参数

利用上下文信息

改善指令遵循与回答质量

记号 预训练的标签就是文本自身的下一个位置，属于自监督学习；实际模型的后训练配方不尽相同。各标识为相应公司的商标，仅用于指代。

六个案例的共同点

机器学习承担其中一个或几个环节，其余环节仍由实验、计算或人完成

案例	输入 x	输出 y	学习方式
蛋白质结构	氨基酸序列	原子坐标	有监督
药物发现	分子图	亲和力、毒性	有监督（排序）
癌症疫苗	突变 + 免疫特征	呈递概率	有监督（排序）
天气预报	当前大气场	数小时后的大气场	有监督
自动驾驶	图像、点云	目标、轨迹、动作	有监督 + 强化
大语言模型	前文	下一个 token	自监督 + 强化

问题 这些问题为什么适合用机器学习？反过来，什么问题不该用机器学习？

05

适用边界

When to Use Machine Learning

适用的四个方面 · 不适用的情形

什么问题适合用机器学习

适用性判断的四个方面

条件	反例
① 存在模式	彩票号码、公平硬币的下一次结果
② 模式无法显式表述	判断闰年、计算圆面积、求最短路
③ 有代表性的数据：训练分布 $\approx$ 部署分布	最常被低估的一条
④ 错误可以承受	统计模型通常会产生错误

要点 能够凭经验做到，但无法准确描述：形式逻辑或闭式表达难以写出完整的规则。

记号 四项用于判断采用机器学习的价值与可行性，并非严格的必要条件。参考：Borwein & Crandall, Closed forms: What they are and why we care。

什么问题不该用机器学习

情形	原因	替代做法
问题可以精确求解	确定性算法有正确性保证，机器学习只给出统计意义上的近似	数值方法、组合优化
拿不到数据，或数据与部署场景差异大	验证集上的成绩不具参考价值	先解决数据问题
每个决定都须逐条解释、可追责	信贷、司法、医疗有法律与伦理要求	可解释模型，或仅作参考
样本极少，且无先验知识	估计误差占主导，模型主要反映噪声	机理模型、专家规则
目标本身定义不清	缺少可测量的指标 P ，无法优化与评判	先把目标变成可测量的量
输出会反过来改变数据分布	推荐改变用户行为、交易策略被对手学习	因果推断、在线学习

要点 最后一项代价最大且最易忽视：**模型上线后即成为未来数据的成因之一**，训练时的分布假设不再成立（第 2 讲）。

06

小结

Summary

本讲要点 · 中英文术语对照 · 延伸阅读

本讲要点

- 核心** 从数据中确定模型的参数；判据是参数的来源
- 发展** 学习规则 → 学习表示 → 迁移预训练模型
- 学习方式** 有监督、无监督、强化学习；自监督从数据自身构造目标
- 任务** 回归、分类，以及预测、筛选、生成与决策
- 适用** 规律存在但难以显式表述、数据有代表性、错误可承受

问题 “从数据中确定规则”如何写成数学问题？候选规则的范围、评判的标准、数据与未见输入之间的关系，是下一讲的内容。

中英文术语对照

英文全称	缩写	中文
Questions and Answers	QA	问答
Expectation–Maximization	EM	期望最大化
Computer Vision	CV	计算机视觉
Natural Language Processing	NLP	自然语言处理

英文全称	缩写	中文
messenger RNA	mRNA	信使 RNA
Reinforcement Learning	RL	强化学习
Compute Unified Device Architecture	CUDA	统一计算设备架构
Bidirectional Encoder Representations from Transformers	BERT	基于 Transformer 的双向编码表示

延伸阅读

教材对应章节

- 周志华《机器学习》第 1 章
1.1–1.2: 基本术语与研究对象
- 李航《统计学习方法》第 1 章
1.1–1.2: 统计学习的定义与三要素

案例的原始来源

蛋白质结构预测	2024 年诺贝尔化学奖公告（瑞典皇家科学院）
个体化癌症疫苗	三期试验 INTerpath-001 (NCT05933577) 结果公告；二期 KEYNOTE-942, <i>The Lancet</i> 2024
天气预报	欧洲中期天气预报中心业务化运行公告, 2025-02
自动驾驶	Waymo Driver Handbook; NVIDIA AlpGym 技术文档