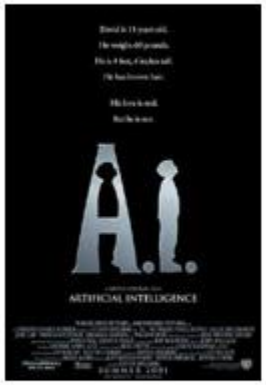
机器学习导论 (2020 春季学期)

一、绪 论

主讲教师：周志华

人工智能

科幻电影中的“人工智能”



常有人问：

“比人类聪明的AI何时出现？”

两种不同的“人工智能”

- **强人工智能**（“科幻人工智能”）

  研制出和人一样聪明，甚至比人更聪明的机器

重要特征：

- **具有自主意识**
- 全面达到、甚至超过人类智能水平
- ……

两种不同的“人工智能”

□ 弱人工智能（“科学人工智能”）

让机器做事时聪明一点

马文·闵斯基
(1927-2016)
人工智能奠基者之一
1969年图灵奖

“人工智能就是让机器来完成那些如果由人来做则需要智能的事情的科学 ”

解读：

- 如果某件事情需要智能，通过机器来做，就是人工智能
- 不要求“全面”达到人类智能水平
- “做事”就行，不必具备“自主意识”
- ……

一个类比

人的智能行为 ⇒ 人工智能

人工智能重要，是因为能造出“智能工具”（类比：飞机）

- 造飞机的人不会关心飞机有没有“意识”、会不会“疼”
- 更不会关心飞机是否“全面达到”鸟的能力（例如：下蛋）

我们讨论的人工智能

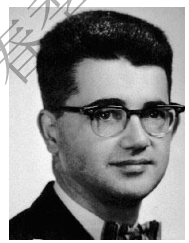
人工智能 ≠ 人造智能

人工智能 = **Intelligence-inspired computing**

人工智能的诞生

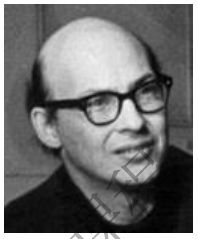
Artificial Intelligence (AI), 1956 -

1956年夏 美国达特茅斯学院



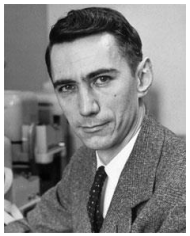
J. McCarthy

“人工智能之父”
图灵奖(1971)



M. Minsky

图灵奖(1969)



C. Shannon

“信息论之父”

H. A. Simon

图灵奖(1975)
诺贝尔经济学奖(1978)

A. Newell

图灵奖(1975)

……

……

达特茅斯会议标志着人工智能这一学科的诞生

第一阶段：推理期

1956-1960s: Logic Reasoning

- 出发点：　“数学家真聪明！”
- 主要成就：自动定理证明系统（例如，西蒙与纽厄尔的“Logic Theorist”系统）

渐渐地，研究者们意识到，仅有逻辑推理能力是不够的 …

赫伯特•西蒙
(1916-2001)
1975年图灵奖

阿伦•纽厄尔
(1927-1992)
1975年图灵奖

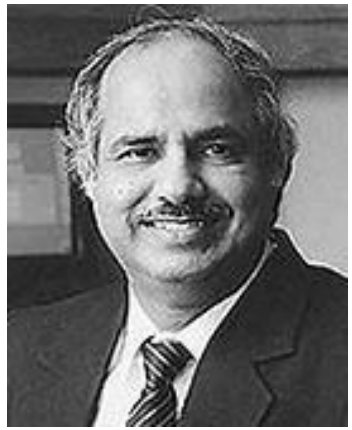
第二阶段：知识期

1970s -1980s: Knowledge Engineering

- 出发点：　“知识就是力量！”
- 主要成就：专家系统（例如，费根鲍姆等人的“DENDRAL”系统）

渐渐地，研究者们发现，要总结出知识再“教”给系统，实在太难了 …

爱德华•费根鲍姆
（1936-　）
1994年图灵奖



瑞吉•芮迪
（1937-　）
1994年图灵奖

第三阶段：学习期

1990s -now: Machine Learning

- 出发点：　“让系统自己学！”
- 主要成就：……

机器学习是作为“突破知识工程瓶颈”之利器而出现的

机器学习

智能化是信息科学技术发展的主流趋势，机器学习是实现智能化的关键

经典定义：利用经验改善系统自身的性能 [T. Mitchell 教科书, 1997]

经验 → 数据

随着该领域的发展，目前主要研究智能数据分析的理论和方法，并已成为智能数据分析技术的源泉之一

图灵奖在近十年中三次授予在该领域取得突出成就的学者

2010年度

Leslie Valiant

“计算学习理论”奠基人

2011年度

Judea Pearl

“图模型学习方法”先驱

2018年度

Geoff Hinton

Yann LeCun

Yoshua Bengio

“深度学习”三架马车

第三阶段：学习期

1990s -now: Machine Learning

- 出发点：　“让系统自己学！”
- 主要成就：……

机器学习是作为“突破知识工程瓶颈”之利器而出现的

恰好在20世纪90年代中后期，人类发现自己淹没在数据的汪洋中，对自动数据分析技术——机器学习的需求日益迫切

大数据时代

大数据 ≠ 大价值

机器学习

有效的数据分析

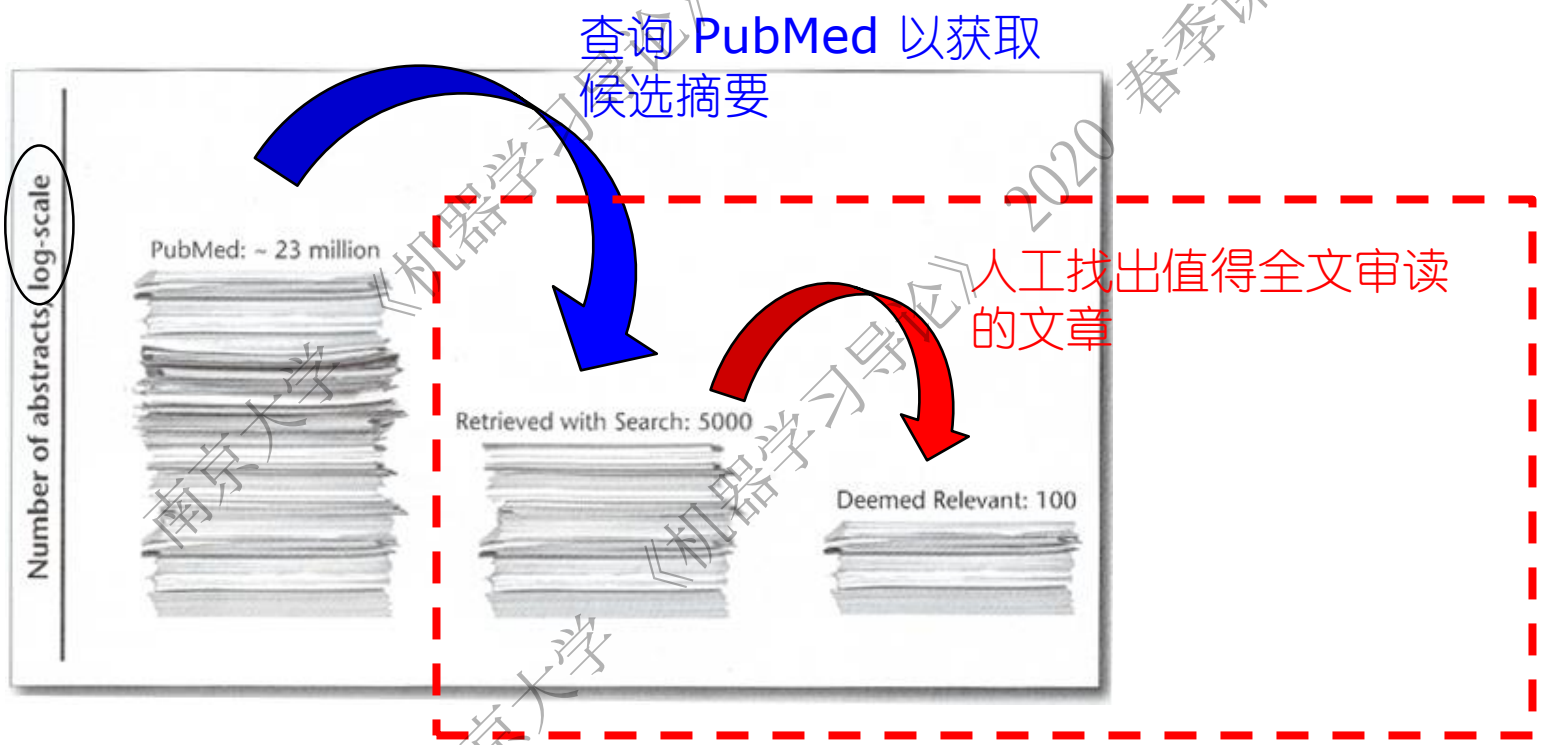
机器学习
(Machine Learning)

究竟是什么东东？

看两个例子 ⇨

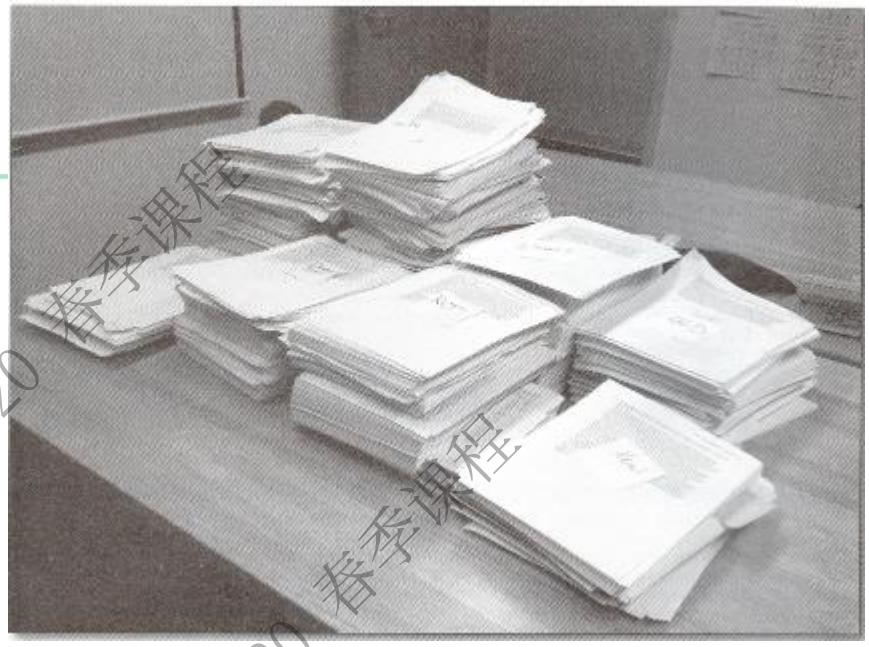
医学文献筛选

在“循证医学”（evidence-based medicine）中，针对特定的临床问题，先要对相关研究报告进行详尽评估



医学文献筛选

在一项关于婴儿和儿童残疾的研究中，美国Tufts医学中心筛选了约 33,000 篇摘要



a portion of the 33,000 abstracts

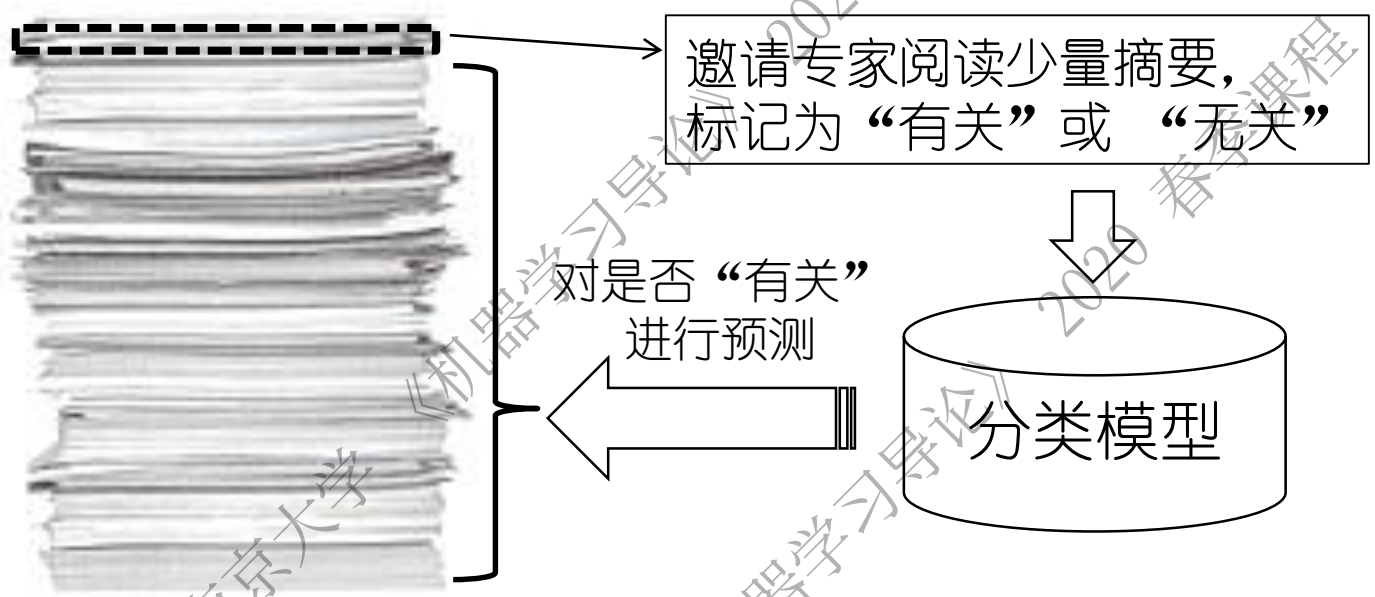
尽管Tufts医学中心的专家效率很高，对每篇摘要只需 30 秒钟，但该工作仍花费了 250 小时

每项新的研究都要重复这个麻烦的过程！

需筛选的文章数在不断显著增长！

医学文献筛选

为了降低昂贵的成本，Tufts医学中心引入了**机器学习**技术



人类专家只需阅读 **50** 篇摘要，系统的自动筛选精度就达到 **93%**

人类专家阅读 **1,000** 篇摘要，则系统的自动筛选敏感度达到 **95%**

(人类专家以前需阅读 **33,000** 篇摘要才能获得此效果)

[C. Brodley et al., 2012]

画作鉴别

画作鉴别(painting authentication)：确定作品的真伪


勃鲁盖尔（1525-1569）的作品？



梵高（1853-1890）的作品？

该工作对专业知识要求极高

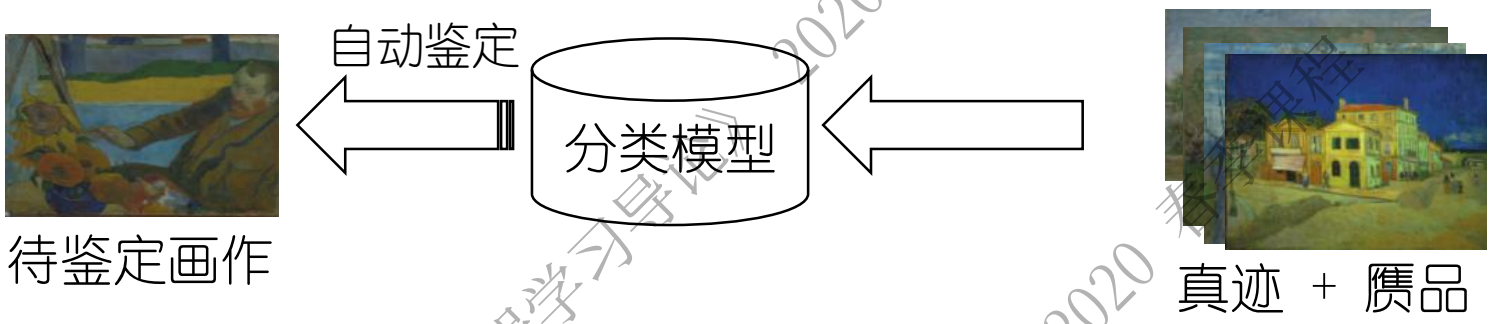
- 具有较高的绘画艺术修养
- 掌握画家的特定绘画习惯

只有少数专家花费很大精力才能完成分析工作！

很难同时掌握不同时期、不同流派多位画家的绘画风格！

画作鉴别

为了降低分析成本，**机器学习**技术被引入



Kröller Müller美术馆与Cornell等大学的学者对82幅梵高真迹和6幅赝品进行分析，自动鉴别精度达 **95%**

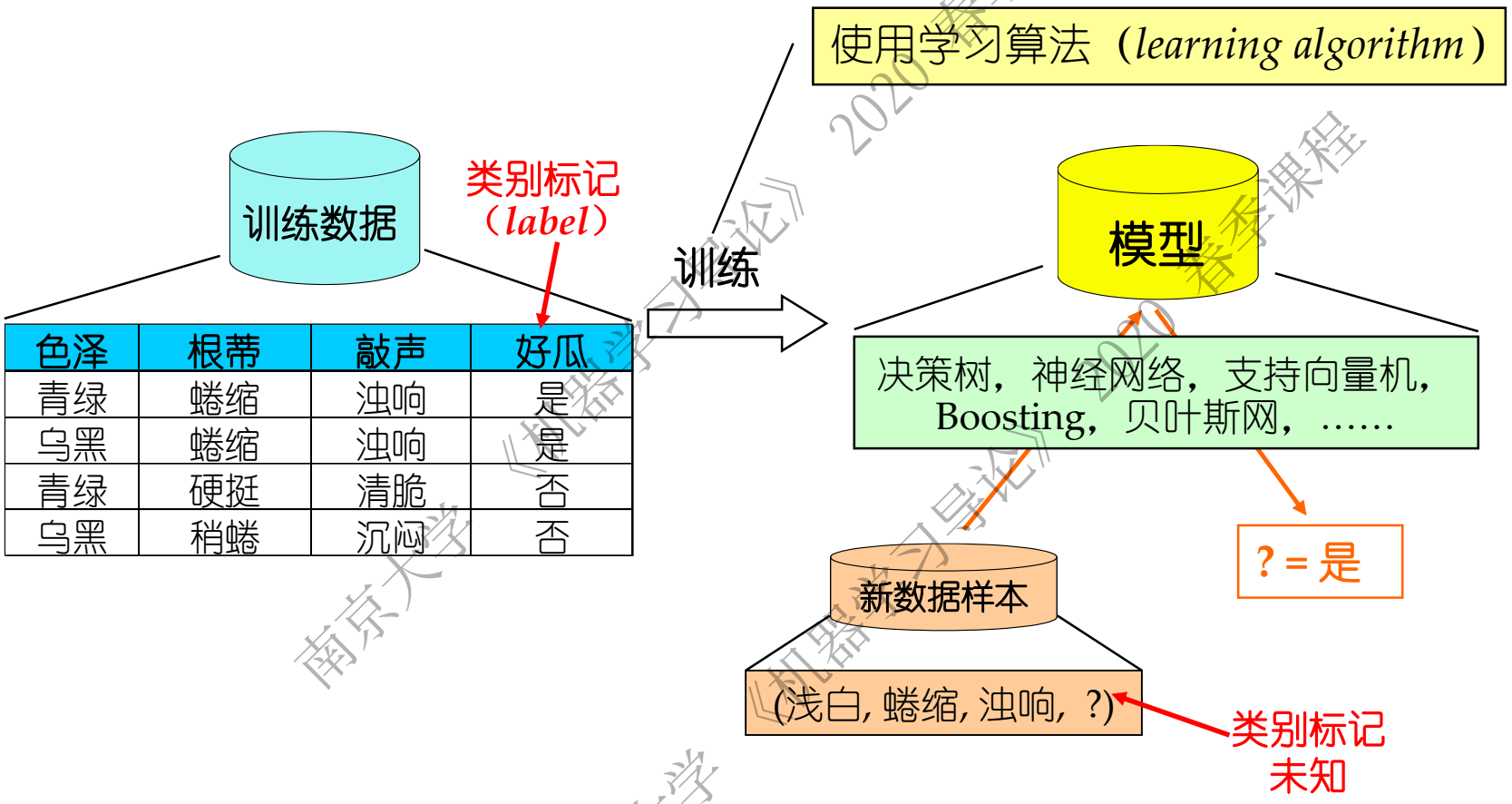
[C. Johnson et al., 2008]

Dartmouth学院、巴黎高师的学者对8幅勃鲁盖尔真迹和5幅赝品进行分析，自动鉴别精度达 **100%**

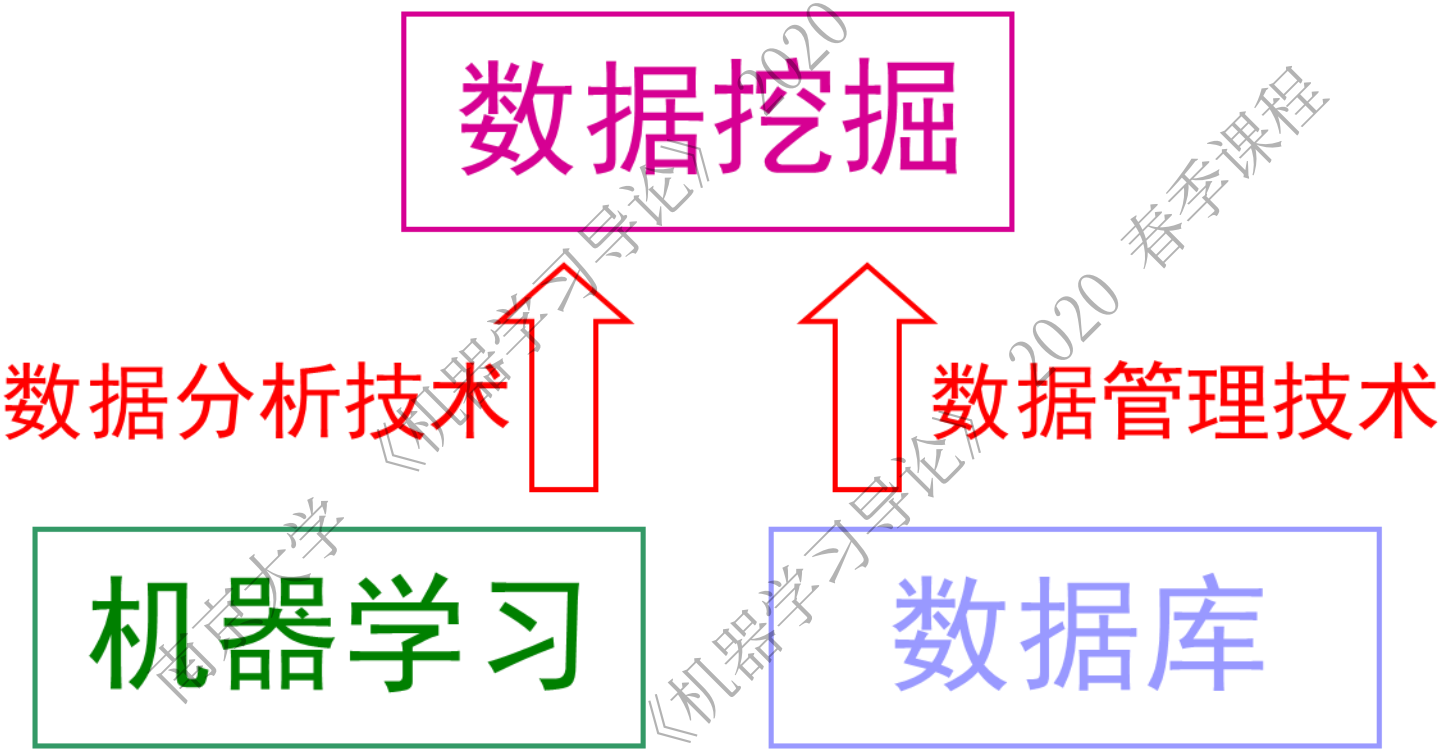
[J. Hughes et al., 2009][J. Mairal et al., 2012]

（对用户要求低、准确高效、适用范围广）

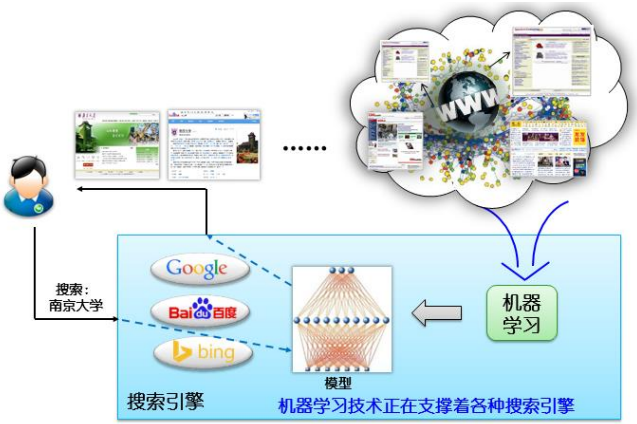
典型的机器学习过程



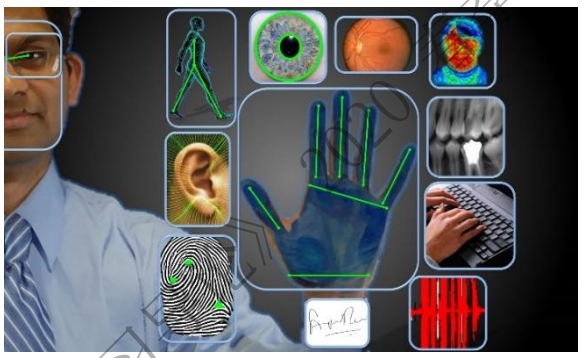
机器学习与数据挖掘



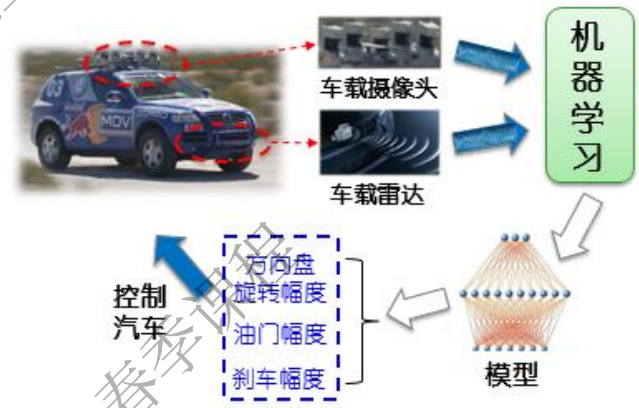
机器学习已经“无处不在”



互联网搜索



生物特征识别



汽车自动驾驶

火星机器人

美国总统选举

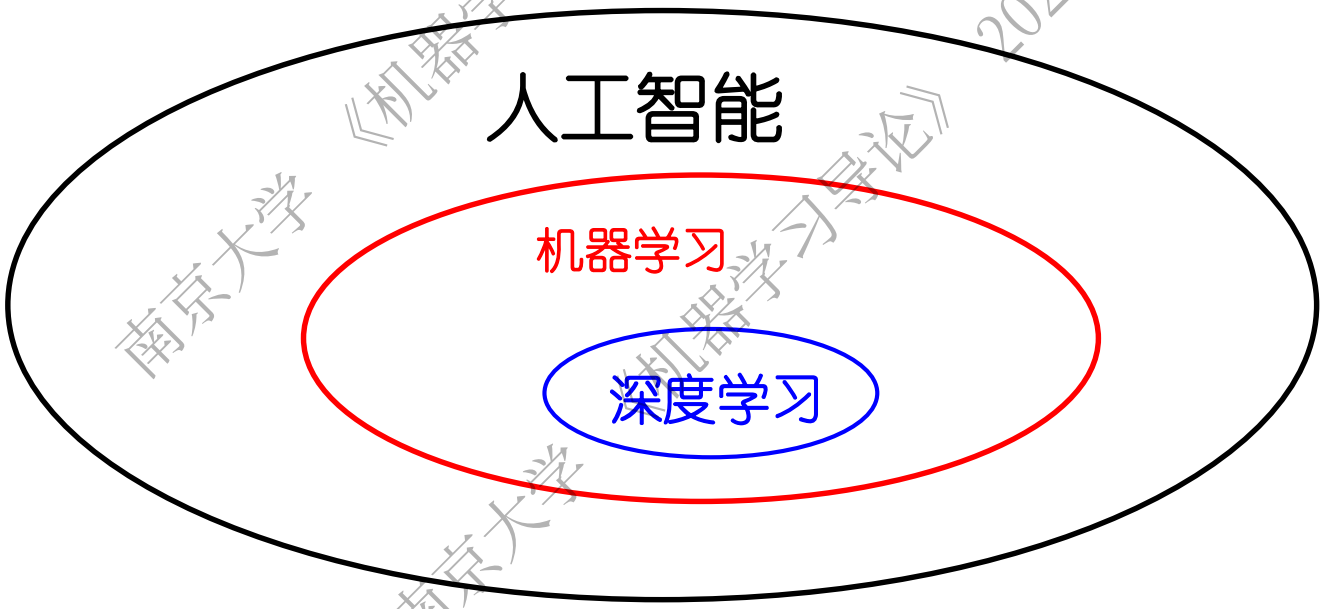
军事决策助手 (DARPA)

人工智能 vs. 机器学习 vs. 深度学习

今天的“人工智能热潮”

正是由于机器学习、尤其深度学习技术取得了巨大进展

基于大数据、大算力发挥出巨大威力



机器学习很强大，但是……

并非“一切皆可学”

- 特征信息不充分
  - 例如，重要特征信息没有获得
- 样本信息不充分
  - 例如，仅有很少的数据样本

机器学习有坚实的理论基础

Leslie Valiant
(莱斯利•维利昂特)
(1949-)
2010年图灵奖

计算学习理论

Computational learning theory

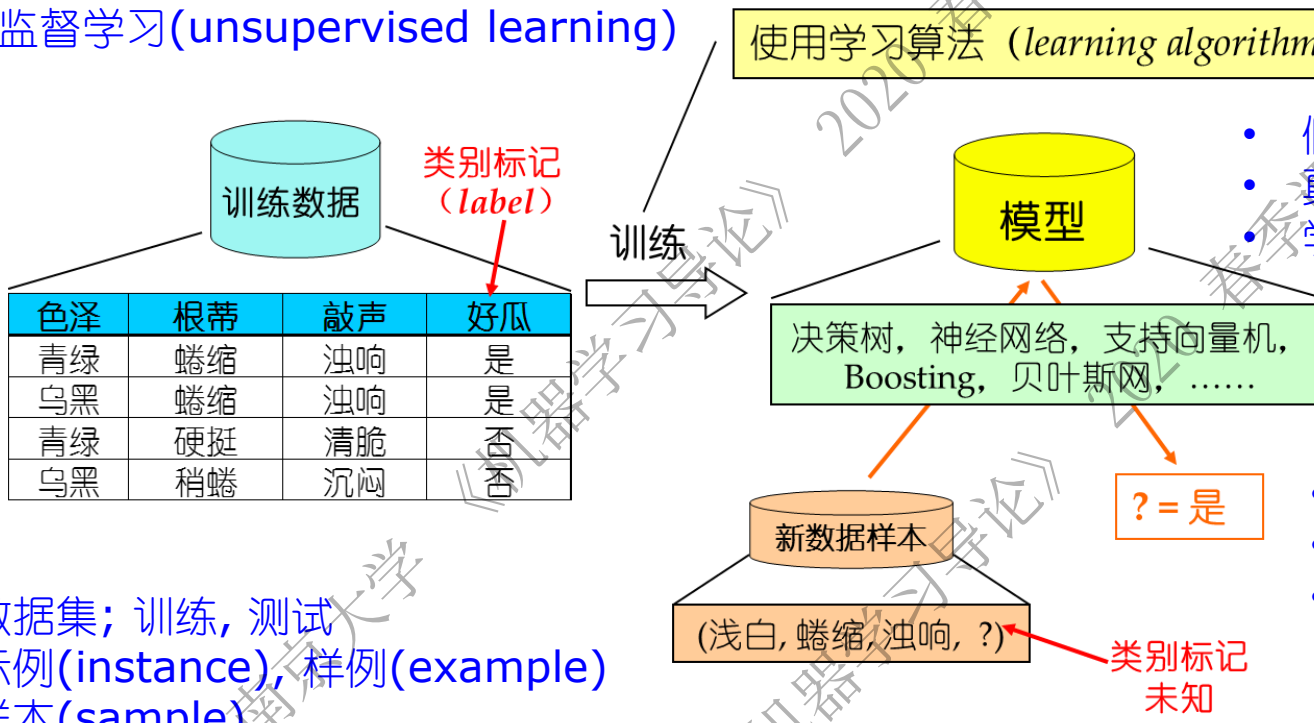
最重要的理论模型：

PAC (Probably Approximately Correct, 概率近似正确) learning model [Valiant, 1984]

$$P(|f(\boldsymbol{x}) - y| \leqslant \epsilon) \geq 1 - \delta$$

基本术语

- 监督学习(supervised learning)
- 无监督学习(unsupervised learning)



色泽	根蒂	敲声	好瓜
青绿	蜷缩	浊响	是
乌黑	蜷缩	浊响	是
青绿	硬挺	清脆	否
乌黑	稍蜷	沉闷	否

- 假设(hypothesis)
- 真相(ground-truth)
- 学习器(learner)

- 分类, 回归
- 二分类, 多分类
- 正类, 反类

- 数据集; 训练, 测试
- 示例(instance), 样例(example)
- 样本(sample)
- 属性(attribute), 特征(feature); 属性值
- 属性空间, 样本空间, 输入空间
- 特征向量(feature vector)
- 标记空间, 输出空间

- 未见样本(unseen instance)
- 未知 “分布”
- 独立同分布(i.i.d.)
- 泛化**(generalization)**

假设空间

表 1.1 西瓜数据集

编号	色泽	根蒂	敲声	好瓜
1	青绿	蜷缩	浊响	是
2	乌黑	蜷缩	浊响	是
3	青绿	硬挺	清脆	否
4	乌黑	稍蜷	沉闷	否

(色泽=?)∧(根蒂=?)∧(敲声=?)↔好瓜

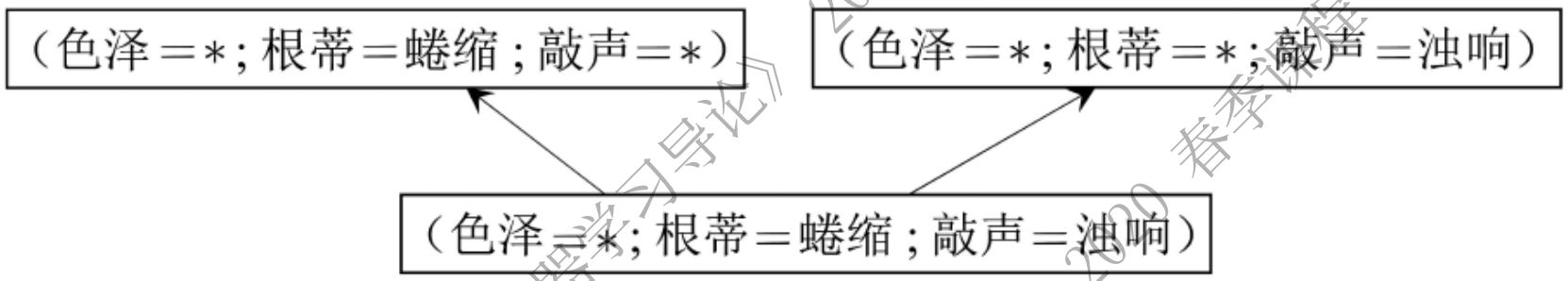
学习过程 → 在所有假设(hypothesis)组成的空间中进行**搜索**的过程

目标：找到与训练集“匹配”(fit)的假设

假设空间的大小：(n1+1) x (n2+1) x (n3+1) + 1

版本空间

版本空间(version space)：与训练集一致的假设集合



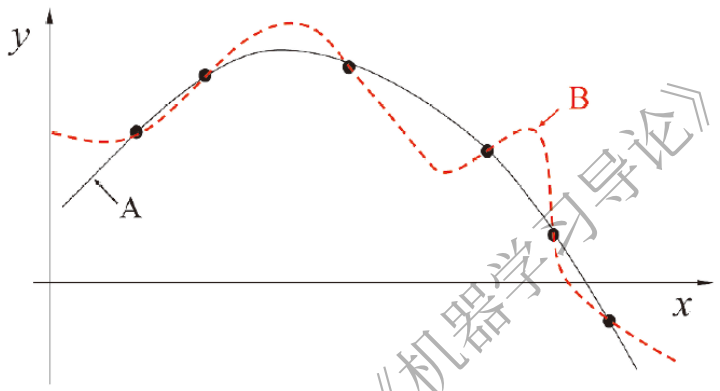
在面临新样本时，会产生不同的输出

例如：(青绿；蜷缩；沉闷)

应该采用哪一个模型(假设)?

归纳偏好 (inductive bias)

机器学习算法在学习过程中对某种类型假设的偏好



A更好？
B更好？

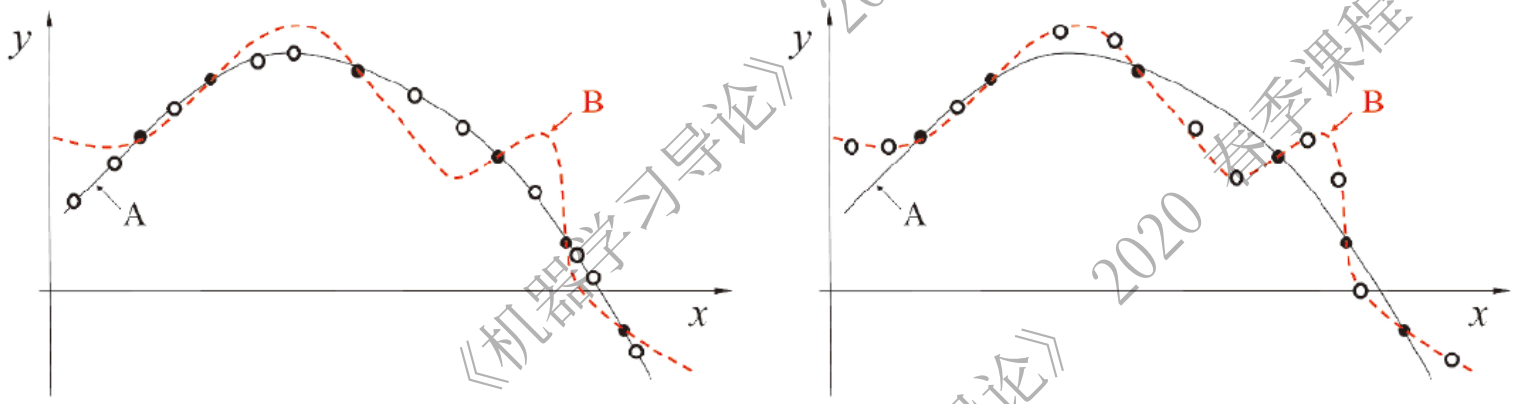
一般原则：
奥卡姆剃刀
(Ocam's razor)

任何一个有效的机器学习算法必有其偏好

学习算法的归纳偏好是否与问题本身匹配，
大多数时候直接决定了算法能否取得好的性能！

哪个算法更好？

没有免费的午餐！



(a) A 优于 B　　(b) B 优于 A

图 1.4 没有免费的午餐. (黑点: 训练样本; 白点: 测试样本)

NFL定理：一个算法 $\mathfrak{L}_a$ 若在某些问题上比另一个算法 $\mathfrak{L}_b$ 好，必存在另一些问题，$\mathfrak{L}_b$ 比 $\mathfrak{L}_a$ 好。

NFL定理

简单起见，假设样本空间 $\mathcal{X}$ 和假设空间 $\mathcal{H}$ 离散，令 $P(h|X,\mathfrak{L}_a)$ 代表算法 $\mathfrak{L}_a$ 基于训练数据 X 产生假设 h 的概率，f 代表要学的目标函数，$\mathfrak{L}_a$ 在训练集之外所有样本上的总误差为

$$E_{ote}(\mathfrak{L}_a|X,f)=\sum_h\sum_{\boldsymbol{x}\in\mathcal{X}-X}P(\boldsymbol{x})\,\mathbb{I}\left(h\left(\boldsymbol{x}\right)\neq f\left(\boldsymbol{x}\right)\right)P\left(h\mid X,\mathfrak{L}_a\right)$$

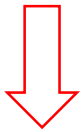
考虑二分类问题，目标函数可以为任何函数 $\mathcal{X}\mapsto\{0,1\}$，函数空间为 $\{0,1\}^{|\mathcal{X}|}$，对所有可能的 f 按均匀分布对误差求和，有

$$\sum_f E_{ote}(\mathfrak{L}_a|X,f)=\sum_f\sum_h\sum_{\boldsymbol{x}\in\mathcal{X}-X}P(\boldsymbol{x})\,\mathbb{I}(h(\boldsymbol{x})\neq f(\boldsymbol{x}))\;P(h\mid X,\mathfrak{L}_a)$$

NFL定理

$$
\begin{aligned}
\sum_f E_{ote}(\mathfrak{L}_a|X,f) &= \sum_f \sum_h \sum_{\boldsymbol{x}\in\mathcal{X}-X} P(\boldsymbol{x})\,\mathbb{I}(h(\boldsymbol{x})\neq f(\boldsymbol{x}))\,P(h\mid X,\mathfrak{L}_a) \\
&= \sum_{\boldsymbol{x}\in\mathcal{X}-X} P(\boldsymbol{x}) \sum_h P(h\mid X,\mathfrak{L}_a) \sum_f \mathbb{I}(h(\boldsymbol{x})\neq f(\boldsymbol{x})) \\
&= \sum_{\boldsymbol{x}\in\mathcal{X}-X} P(\boldsymbol{x}) \sum_h P(h\mid X,\mathfrak{L}_a) \frac{1}{2} 2^{|\mathcal{X}|} \\
&= \frac{1}{2} 2^{|\mathcal{X}|} \sum_{\boldsymbol{x}\in\mathcal{X}-X} P(\boldsymbol{x}) \sum_h P(h\mid X,\mathfrak{L}_a) \\
&= 2^{|\mathcal{X}|-1} \sum_{\boldsymbol{x}\in\mathcal{X}-X} P(\boldsymbol{x})\cdot 1
\end{aligned}
$$

总误差与学习算法无关！



所有算法一样好！

NFL定理的寓意

NFL定理的重要前提：

所有“问题”出现的机会相同、或所有问题同等重要

实际情形并非如此；我们通常只关注自己正在试图解决的问题

脱离具体问题，空泛地谈论“什么学习算法更好”毫无意义！

具体问题，具体分析！

现实机器学习应用中 ……

把机器学习的“十八般兵器”都弄熟，
逐个试一遍，是不是就OK了？

NO！

机器学习不是“十八般兵器” 的堆积

在现实任务中，很少能“照搬”兵器取得好结果

按需设计、度身定制

前往第二站.....