

## 1 机器学习概念

研究如何通过计算的手段，利用经验来改善系统自身的性能。

## 2 基本术语

一批数据的集合称为**数据集**(data set)，其中每条数据称为一个**示例**(instance)或**样本**(sample)。

反应事件性质的事项称为**属性**(attribute)或**特征**(feature)，属性的取值称为**属性值**(attribute value)，属性张成的空间称为**属性空间**(attribute space)、**样本空间**(sample space)或**输入空间**，一个示例也可称为**特征向量**(feature vector)。

每个示例的属性个数称为这个示例的**维数**(dimensionality)。

从数据中学得模型的过程称为**学习**(learning)或**训练**(training)。每个数据称为一个**训练样本**(training sample)，样本的集合为**训练集**(training set)。学得模型为某种规律，称为**假设**(hypothesis)。规律本身称为**真相或真实**(ground-truth)。

如果预测的是离散值，这类学习任务称为**分类**(classification)。如果是连续值，称为**回归**(regression)。

学得模型后，使用模型进行预测的行为称为**测试**(testing)，用到的样本称为**测试样本**(testing sample)。将训练集分组的行为称为**聚类**(clustering)，每组称为一个**簇**(cluster)。

训练数据有标记的学习任务称为**监督学习**(supervised learning)，如分类和回归。没有标记的称为**无监督学习**(unsupervised learning)，如聚类。学得模型适用于新样本的能力称为**泛化**(generalization)能力。

### 3 假设空间

**归纳**(induction)与**演绎**(deduction)是科学推理的两大基本手段。归纳是从特殊到一般的**泛化**(generalization)过程，演绎是从一般到特殊的**特化**(specialization)过程。

在已知属性和属性值的情况下，所有可能满足目标的假设的集合称为**假设空间**。在假设空间中，与训练集一致的假设的集合称为**版本空间**(version space)。我们可以把学习过程看作一个在假设(hypothesis)组成的空间中进行搜索的过程。搜索过程中可以不断删除与正例不一致的假设、和(或)与反例一致的假设(因为学些的目的是能判断出正例)。最终将会获得与训练集一致(即对所有训练样本能够进行正确判断)的假设，这就是我们学得的结果，即版本空间。

### 4 归纳偏好

学习过程中，算法对某种类型假设的偏好，称为**归纳偏好**(inductive bias)。怎样选择正确的偏好？**奥卡姆剃刀**(Occam's razor)是一种常用原则，即若有多个假设与观察一致，则选最简单的那个。

**“没有免费的午餐”定理**(no free lunch theorem, NFL)：没有适用所有数据的最优算法。一种算法(算法 A)在特定数据集上的表现优于另一种算法(算法 B)的同时，一定伴随着算法 A 在另外某一个特定的数据集上有着不如算法 B 的表现。

### 5 发展历程

1950s~1980s:人工智能推理期。特点是基于符号知识表示，采用演绎推理技术。典型成果包括逻辑理论家(Logic Theorist)和通用问题求解(General Problem Solving)程序。

1970s~:人工智能知识期。特点是基于符号知识表示,通过获取和利用领域知识建立专家系统。典型成功包括决策树和基于逻辑的学习,如归纳逻辑程序设计(Inductive Logic Programming, ILP)。

~1995:神经网络称为“从样例中学习”的主流技术。

1995~: 统计学习。典型算法如支持向量机(Support Vector Machine, SVM)和更一般的“核方法”(kernel methods)。

2000~: 连接主义学习。典型技术为深度学习,即多层神经网络。