《机器学习》读书笔记

黄奕诚

目录

1	绪论		3
	1.1	引言	3
	1.2	基本术语	3
	1.3	假设空间	4
	1.4	归纳偏好	4
	1.5	发展历程	5
	1.6	应用现状	5
2	模型	评估与选择	6
	2.1	经验误差与过拟合	6
	2.2	评估方法	6
		2.2.1 留出法	6
		2.2.2 交叉验证法	7
		2.2.3 自助法	7
		2.2.4 调参与最终模型	8
	2.3	性能度量	8
		2.3.1 错误率与精度	8
			9
			10
		•	11
	2.4		12
			12
			13
			13 14
		2.4.0 IVICINEIII 4 4 4 · · · · · · · · · · · · · · ·	Ľ±

Ma	Machine Learning		
	2.4.4 Friedman 检验与 Nemenyi 后续检验		
3	线性模型	17	
4	决策树	17	
5	神经网络	17	
6	支持向量机	17	
7	贝叶斯分类器	17	
8	集成学习	17	
9	聚类	17	
10	降维与度量学习	17	
11	特征选择与稀疏学习	17	
12	计算学习理论	17	
13	半监督学习	17	
14	概率图模型	17	
15	规则学习	17	
16	强化学习	17	

1 绪论

1.1 引言

- 机器学习致力于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。
- 机器学习研究的主要内容:在计算机上从数据中产生"模型"的算法, 即"学习算法"。

1.2 基本术语

- 数据集 (data set): 一组记录的集合
- 示例 (instance) /样本 (sample): 每条记录, 即关于一个事件或对象 的描述
- 属性 (attribute) /特征 (feature): 反映事件或对象在某方面的表现或 性质的事项
- 属性值 (attribute value): 属性上的取值
- 属性空间 (attribute space) /样本空间 (sample space) /输入空间: 属性张成的空间,记为 X
- 特征向量 (feature vector): 一个示例 (在样本空间对应的坐标向量)
- 学习 (learning) /训练 (training): 从数据中学得模型的过程
- 训练数据 (training data): 训练过程中使用的数据
- 训练样本 (training sample): 训练数据中的每个样本
- 训练集 (training set): 训练样本组成的集合
- 假设 (hypothesis): 对应了关于数据的某种潜在规律的学得模型
- 真实 (ground-truth): 潜在规律自身
- 学习器 (learner): 学习算法在给定数据和参数空间上的实例化
- 标记 (label): 关于示例结果的信息

- 样例 (example): 拥有标记信息的示例
- 标记空间 (label space) /输出空间: 所有标记的集合, 记为 \mathcal{Y}
- 分类 (classification) : 预测的是离散值的学习任务 (二分类 $\mathcal{Y} = \{-1, +1\}$ 或 $\{0, 1\}$; 三分类 $|\mathcal{Y}| > 2$)
- 回归 (regression): 预测的是连续值的学习任务 ($\mathcal{Y} = \mathbb{R}$)
- 测试 (testing): 使用学得模型进行预测的过程
- 测试样本 (testing sample): 被预测的样本
- 无监督学习 (unsupervised learning): 训练数据中没有标记信息的学习任务, 代表是聚类 (clustering)
- 监督学习 (supervised learning): 训练数据中具有标记信息的学习任务, 代表是分类和回归
- 泛化 (generalization) 能力: 学得模型适用于新样本的能力

1.3 假设空间

- "从样例中学习"是一个归纳的过程。
- 可以把学习过程看作一个在所有假设组成的空间中进行搜索的过程, 搜索目标是找到与训练集"匹配"(fit)的假设。
- 假设空间可以表示为一课属性值中通配符逐渐被具体数值取代的树。
- 可以用许多策略对假设空间进行搜索,如自顶向下(从一般到特殊)、 自底向上(从特殊到一般)。
- 可能有多个假设与训练集一致,即存在着一个与训练集一致的"假设集合",称之为"版本空间"(version space)。

1.4 归纳偏好

• 多个与训练集一致的假设所对应的模型在面临新样本时,可能产生不同的输出。而对于一个具体的学习算法而言,必须要产生一个模型。此时学习算法本身的偏好会起到关键的作用。

- 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。
- 奥卡姆剃刀 (Occam's razor): 若有多个假设与观察一致,则选最简单的那个。【常用的、自然科学研究中最基本的原则】
- 设 f 为希望学习的真实目标函数,则基于训练数据 X 的算法 \mathcal{L}_a 在训练集之外的所有样本上的误差与学习算法无关,即

$$\sum_{f} E_{ote}(\mathfrak{L}_a|X, f) = \sum_{f} E_{ote}(\mathfrak{L}_b|X, f)$$

"没有免费的午餐"定理 (NFL 定理): 所有学习算法的期望性相同。

1.5 发展历程

- 1. 二十世纪五十年代到七十年代初:"推理期"——赋予机器逻辑推理能力
- 2. 二十世纪七十年代中期开始:"知识期"
 - a. 机械学习(信息存储与检索)
 - b. 示教学习(从指令中学习)
 - c. 类比学习 (通过观察和发现学习)
 - d. 归纳学习(从样例中学习)
 - 符号主义学习(决策树、基于逻辑的学习)
 - 连接主义学习(神经网络)
 - 统计学习(支持向量机、核方法)
 - 深度学习

1.6 应用现状

- 计算机科学诸多分支学科领域(如计算机视觉、自然语言处理)
- 交叉学科(如生物信息学)
- 数据挖掘(机器学习领域和数据库领域是数据挖掘的两大支撑)
- 人类日常生活 (天气预报、搜索引擎、自动驾驶、政治选举等)
- 促进人们理解"人类如何学习"

2 模型评估与选择

2.1 经验误差与过拟合

- 设在 m 个样本中有 a 个样本分类错误,则错误率 (error rate) 为 E=a/m,精度 (accuracy) 为 1-a/m。
- 误差 (error): 学习器的实际预测输出与样本的真实输出之间的差异。训练误差 (training error) /经验误差 (empirical error): 学习器在训练集上的误差。泛化误差 (generalization error): 学习器在新样本上的误差。想要使泛化误差最小,而新样本未知,所以努力使经验误差最小化。
- 过拟合 (overfitting): 学习器将训练样本自身的一些特点当作为所有 潜在样本都会具有的一般性质。【关键障碍、无法彻底避免】欠拟合 (underfitting): 学习器对训练样本的一般性质尚未学好。【较容易克服】若"P≠NP", 过拟合就不可避免。

2.2 评估方法

为了对学习器对泛化误差进行评估,需要使用一个测试集(testing set) 来测试学习器对新样本的判别能力,然后以测试集上的测试误差(testing error)作为泛化误差的近似。

若当前只有一个包含 m 个样例的数据集

$$D = \{(x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)\}\$$

,则对其进行适当的处理,从中产生训练集S和测试集T。

2.2.1 留出法

直接将数据集 D 划分为两个互斥的集合,其中一个作为训练集 S,另一个作为测试集 T,即 $D=S\cup T,S\cap T=\emptyset$,在 S 上训练出模型后,用 T 来评估其测试误差,作为对泛化误差的估计。

划分尽可能保持数据分布的一致性,例如在分类任务中至少要保持样本的类别比例相似(分层采样)。

- 一般采用若干次随机划分、重复进行实验评估后取平均值作为评估结果。
- $S \to D$ 大小权衡没有完美的解决方案,常见做法是 $2/3\sim4/5$ 的训练样本比例。

2.2.2 交叉验证法

将数据集 D 划分为 k 个大小相似的互斥子集,即

$$D = D_1 \cup D_2 \cup \cdots \cup D_k, D_i \cup D_j = \emptyset (i \neq j)$$

每个子集 D_i 都尽可能保持数据分布的一致性(分层抽样)。然后从中选取 k-1 个子集为训练集,剩下一个子集为测试集。可进行 k 次训练和测试,最终返回 k 个测试结果的均值。也称为 "k 折交叉验证" (k-fold cross validation)。

- k 最常用的取值是 10, 常用的还有 5、20 等。
- 留一法 (Leave-One-Out) 不受随机样本划分的影响,评估结果比较准确,但计算开销大。

2.2.3 自助法

以自助采样法 (bootstrap sampling) 为基础, 给定包含 m 个样本的数据集 D, 每次随机从 D 中挑选一个样本, 将其拷贝放入 D', 再将该样本放回初始数据集 D 中。这个过程重复执行 m 次后, 得到了包含 m 个样本的数据集 D'。此时将 D' 用作训练集, $D\backslash D'$ 用作测试集。

- D 有约 36.8% 的样本未出现在采样数据集 D' 中。
- 亦称为"包外估计" (out-of-bag estimate)。
- 自助法在数据集较小、难以有效划分训练/测试集时很有用,且能从初始数据集中产生多个不同的训练集。
- 因为自助法产生的数据集改变了初始数据集的分布,会引入估计偏差。

2.2.4 调参与最终模型

- 常用的调参做法:对每个参数选定一个范围和变化步长,进行计算开 销和性能估计之间的折中。
- 在模型选择完成后,学习算法和参数配置已选定,此时用数据集 D 重新训练模型,使用所有 m 个样本,得到最终提交给用户的模型。

2.3 性能度量

给定样例集

$$D = \{(\boldsymbol{x}_1, y_1), (\boldsymbol{x}_2, y_2), \dots, (\boldsymbol{x}_m, y_m)\}\$$

其中 y_i 是示例 x_i 的真实标记。要评估学习器 f 的性能,即把学习器预测结果 f(x) 与真实标记 y 进行比较。

回归任务中最常用的性能度量:"均方误差"(mean squared error)

$$E(f; D) = \frac{1}{m} \sum_{i=1}^{m} (f(\boldsymbol{x}_i) - y_i)^2$$

更一般地,对于数据分布D和概率密度函数 $p(\cdot)$,均方误差可描述为

$$E(f; \mathcal{D}) = \int_{x \sim \mathcal{D}} (f(\boldsymbol{x}) - y)^2 p(\boldsymbol{x}) d\boldsymbol{x}$$

对于分类任务——

2.3.1 错误率与精度

• 分类错误率

$$E(f; D) = \frac{1}{m} \sum_{i=1}^{m} \mathbb{I}(f(\boldsymbol{x}_i) \neq y_i)$$

精度

$$acc(f; D) = \frac{1}{m} \sum_{i=1}^{m} \mathbb{I}(f(x_i) = y_i) = 1 - E(f; D)$$

• 对于数据分布 \mathcal{D} 和概率密度函数 $p(\cdot)$, 错误率

$$E(f; \mathcal{D}) = \int_{x \sim \mathcal{D}} \mathbb{I}(f(x) \neq y) p(x) dx$$

精度

$$acc(f; \mathcal{D}) = \int_{x \sim \mathcal{D}} \mathbb{I}(f(x) = y) p(x) dx = 1 - E(f; \mathcal{D})$$

2.3.2 查准率、查全率与 F1

古宁桂汉	预测结果		
真实情况	正例	反例	
正例	TP (真正例)	FN(假反例)	
反例	FP (假正例)	TN (真反例)	

查准率 (precision)

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

查全率 (recall)

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

- 平衡点 (Break-Even Point, BEP): R = P 时的取值,数值越高可以认为学习器越优。
- F1 度量

实际上 F1 是 R 和 P 的调和平均

$$\frac{1}{F1} = \frac{1}{2}(\frac{1}{P} + \frac{1}{R})$$

• F_{β} 度量: 考虑 R 与 P 的不同偏好,设 β 为查全率 R 对查准率 P 的相对重要性,则

$$F_{\beta} = \frac{(1+\beta^2) \times P \times R}{(\beta^2 \times P) + R}$$

实际上 F_{β} 是加权调和平均

$$\frac{1}{F_{\beta}} = \frac{1}{1+\beta^2} (\frac{1}{P} + \frac{\beta^2}{R})$$

• 宏F1: 在各混淆矩阵上分别计算出各自的 (P_i, R_i) , 再计算平均值:

$$macro-P = \frac{1}{n} \sum_{i=1}^{n} P_i$$

$$macro - R = \frac{1}{n} \sum_{i=1}^{n} R_i$$

$$\text{macro}{-F1} = \frac{2 \times \text{macro}{-P} \times \text{macro}{-R}}{\text{macro}{-P} + \text{macro}{-R}}$$

• 徽 F1: 先将各混淆矩阵的对应元素进行平均得到四个指标, 再基于这 些平均值计算 F1:

$$micro-P = \frac{\overline{TP}}{\overline{TP} + \overline{FP}}$$

$$\text{micro}{-R} = \frac{\overline{TP}}{\overline{TP} + \overline{FN}}$$

$$\text{micro}-F1 = \frac{2 \times \text{micro}-P \times \text{micro}-R}{\text{micro}-P + \text{micro}-R}$$

△ 混淆矩阵介绍:每一列代表了预测类别,每一列的总数表示预测为该类别的数据的数目;每一行代表了数据的真实归属类别,每一行的数据总数表示该类别的数据实例的数目。例如共有 150 个样本数据,预测为 1、2、3 类各 50 个,分类结束后得到的混淆矩阵为

		预测		
		类 1	类 2	类 3
	类 1	43	2	0
实际	类 2	5	45	1
	类 3	2	3	49

2.3.3 ROC 与 AUC

ROC 全称是"受试者工作特征"(Receiver Operating Characteristic)曲线。横轴为"假正例率"(FPR),纵轴为"真正例率"(TPR)。

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

$$FPR = \frac{FP}{TN + FP}$$

- 现实任务中 ROC 曲线的绘制方法: 给定 m^+ 个正例和 m^- 个反例,根据学习器预测结果对样例进行排序,然后把分类阈值设为最大,此时 FPR 和 TPR 都为 0. 在坐标 (0,0) 处标记一个点,然后将分类阈值依次设为每个样例的预测值。设当前一个标记点坐标为 (x,y),若当前为真正例,则对应标记点坐标为 $(x,y+\frac{1}{m^+})$;若当前为假正例,则对应标记点坐标为 $(x+\frac{1}{m^-},y)$,然后用线段连接相邻点即得。
- AUC (Area Under ROC Curve) 即为 ROC 曲线下各部分的面积之和。设 ROC 曲线是由坐标为 $\{(x_i,y_i)|1\leq i\leq m\}$ 的点按序连接而成,则 AUC 可估算为

$$AUC = \frac{1}{2} \sum_{i=1}^{m-1} (x_{i+1} - x_i) \cdot (y_i + y_{i+1})$$

• 给定 m^+ 个正例和 m^- 个反例,令 D^+ 和 D^- 分别表示正、反例集合,则排序"损失" (loss) 定义为

$$\ell_{rank} = \frac{1}{m^+m^-} \sum_{\boldsymbol{x}^+ \in D^+} \sum_{\boldsymbol{x}^- \in D^-} \left(\mathbb{I}\big(f(\boldsymbol{x}^+) < f(\boldsymbol{x}^-)\big) + \frac{1}{2} \mathbb{I}\big(f(\boldsymbol{x}^+) = f(\boldsymbol{x}^-)\big) \right)$$

它对应 ROC 曲线之上的面积,有

$$AUC = 1 - \ell_{rank}$$

2.3.4 代价敏感错误率与代价曲线

- 不同类型的错误可能造成不同损失, 所以为错误赋予"非均等代价" (unequal cost)。
- 以二分类为例,可以设定一个"代价矩阵",如下表所示。

真实类别	预测类别		
共大大 加	第 0 类	第1类	
第 0 类	0	$cost_{01}$	
第1类	$cost_{10}$	0	

• "代价敏感" (cost-sensitive) 错误率

$$E(f; D; cost) = \frac{1}{m} \left(\sum_{\boldsymbol{x}_i \in D^+} \mathbb{I}(f(\boldsymbol{x}_i) \neq y_i) \times cost_{01} + \sum_{\boldsymbol{x}_i \in D^-} \mathbb{I}(f(\boldsymbol{x}_i) \neq y_i) \times cost_{10} \right)$$

• 在非均等代价下,"代价曲线"(cost curve)可以刻画期望总体代价。设 p 是样例为正例的概率。横轴为正例概率代价

$$P(+)cost = \frac{p \times cost_{01}}{p \times cost_{01} + (1-p) \times cost_{10}}$$

纵轴为取值为[0,1]的归一化代价

$$cost_{norm} = \frac{\text{FNR} \times p \times cost_{01} + \text{FPR} \times (1-p) \times cost_{10}}{p \times cost_{01} + (1-p) \times cost_{10}}$$

• 代价曲线的绘制方法: 将 ROC 曲线上的每一点转化为代价平面上的 一条线段,取所有线段的下界,围成的面积即为所有条件下学习器的 期望总体代价。

2.4 比较检验

本节默认以错误率 ϵ 为性能度量。

2.4.1 假设检验

• 设一个学习器的泛化错误率为 ϵ , 在 m 个样本中的测试错误率为 $\hat{\epsilon}$, 则 其被测得测试错误率为 $\hat{\epsilon}$ 的概率为

$$P(\hat{\epsilon}; \epsilon) = \binom{m}{\hat{\epsilon} \times m} \epsilon^{\hat{\epsilon} \times m} (1 - \epsilon)^{m - \hat{\epsilon} \times m}$$

它在 $\epsilon = \hat{\epsilon}$ 时最大。

• 二项检验: 假设 $\epsilon \leq \epsilon_0$, 则在 $1-\alpha$ 的概率内所能观测到的最大错误率为

$$\sum_{i=\epsilon_0\times m+1}^m \binom{m}{i} \epsilon^i (1-\epsilon)^{m-i} < \alpha$$

 $\bar{\epsilon} = \max \epsilon$

若测试错误率 $\hat{\epsilon}$ 小于临界值 $\bar{\epsilon}$,则能以 $1-\alpha$ 的置信度认为学习器的 泛化错误率不大于 ϵ_0 ,否则假设被拒绝。

• t 检验: 若得到了 k 个测试错误率 $\hat{\epsilon}_1, \hat{\epsilon}_2, \ldots, \hat{\epsilon}_k$, 则平均测试错误率 μ 和方差 σ^2 为

$$\mu = \frac{1}{k} \sum_{i=1}^{k} \hat{\epsilon}_i$$

$$\sigma^{2} = \frac{1}{k-1} \sum_{i=1}^{k} (\hat{\epsilon}_{i} - \mu)^{2}$$

它们可看作泛化错误率 ϵ_0 的独立采样,则变量

$$\tau_t = \frac{\sqrt{k}(\mu - \epsilon_0)}{\sigma}$$

服从自由度为 k-1 的 t 分布。若 $|\mu-\epsilon_0|$ 位于 $[t_{-\alpha/2},t_{\alpha/2}]$ 内,则接受假设 $\mu=\epsilon_0$,否则拒绝该假设。

2.4.2 交叉验证 t 检验

• k 折交叉验证 "成对 t 检验": 对每对结果求差 $\Delta_i = \epsilon_i^A - \epsilon_i^B$,若两个学习器性能相同,则差值均值为 0。做 t 检验,在显著度 α 下,若

$$\tau_t = |\frac{\sqrt{k}\mu}{\sigma}| < t_{\alpha/2,k-1}$$

则接受假设。其中 $t_{\alpha/2,k-1}$ 指自由度为 k-1 的 t 分布上尾部累积分 布为 $\alpha/2$ 的临界值。

• 考虑到交叉验证法等实验估计方法,不同轮次的训练集会有一定程度的重叠,导致测试错误率并不独立。故可采用 5×2 交叉验证法 $(5 \times 2$ 折交叉验证)。每次 2 折交叉验证之前随机将数据打乱,使得 5 次交叉验证中的数据划分不重复。设 Δ_k^k 表示第 i 次第 k 上的差值。

$$\mu = 0.5(\Delta_1^1 + \Delta_1^2)$$

$$\sigma_i^2 = \left(\Delta_i^1 - \frac{\Delta_i^1 + \Delta_i^2}{2}\right)^2 + \left(\Delta_i^2 - \frac{\Delta_i^1 + \Delta_i^2}{2}\right)^2$$

变量

$$\tau_t = \frac{\mu}{\sqrt{0.2 \sum_{i=1}^5 \sigma_i^2}}$$

服从自由度为 5 的 t 分布, 其双边检验的临界值为 $t_{\alpha/2.5}$ 。

2.4.3 McNemar 检验

对于二分类问题,可统计两个学习器 A 和 B 的分类结果样本数差别, 列出"列联表"(contingency table)

管 计 D	算法 A		
算法 B	正确	错误	
正确	e_{00}	e_{01}	
错误	e_{10}	e_{11}	

假设两学习器性能相同,则 $e_{01}=e_{10}$, 于是 $|e_{01}-e_{10}|$ 服从正态分布,变量

$$\tau_{\chi^2} = \frac{(|e_{01} - e_{10}| - 1)^2}{e_{01} + e_{10}}$$

服从自由度为 1 的 χ^2 分布,若其小于临界值 χ^2_α 则接受假设,否则拒绝假设,较小者性能更优。

2.4.4 Friedman 检验与 Nemenyi 后续检验

- 在多个数据集上比较算法。
- 算法排序:使用留出法或交叉验证法得到每个算法在每个数据集上的测试结果,然后在每个数据集上根据测试性能由好到坏排序,序值从1递增,若相同则平分序值。
- "原始 Friedman 检验": 假定在 N 个数据集上比较 k 个算法,令 r_i 表示第 i 个算法的平均序值,暂不考虑平分序值,则 r_i 均值为 (k+1)/2,方差为 $(k^2-1)/12$ 。变量

$$\tau_{\chi^2} = \frac{k-1}{k} \cdot \frac{12N}{k^2 - 1} \sum_{i=1}^k \left(r_i - \frac{k+1}{2} \right)^2 = \frac{12N}{k(k+1)} \left(\sum_{i=1}^k r_i^2 - \frac{k(k+1)^2}{4} \right)$$

当 k 和 N 都较大时服从自由度为 k-1 的 χ^2 分布。

• Friedman 检验: 变量

$$\tau_F = \frac{(N-1)\tau_{\chi^2}}{N(k-1) - \tau_{\chi^2}}$$

服从自由度为 k-1 和 (k-1)(N-1) 的 F 分布。

• Nemenyi 检验: 若"所有算法的性能相同"这一假设被拒绝,此时计算 出平均序值差别的临界值域

$$CD = q_{\alpha} \sqrt{\frac{k(k+1)}{6N}}$$

若某两个算法的平均序值之差超出了CD,则以相应的置信度拒绝"这两个算法性能相同"这一假设。

Friedman 检验图: 横轴为平均序值,纵轴为各个算法,对每个算法以一个圆点表示平均序值,以圆点为中心的横线段表示临界值域的大小。若两个算法的横线段有交叠,则说明它们没有显著区别,否则可以进行显著比较。

2.5 偏差与方差

- 偏差-方差分解: 对学习算法的期望泛化错误率进行拆解。
- 学习算法的期望预测

$$\bar{f}(\boldsymbol{x}) = \mathbb{E}_D[f(\boldsymbol{x}; D)]$$

• 使用样本数相同的不同训练集产生的方差

$$var(\boldsymbol{x}) = \mathbb{E}[(f(\boldsymbol{x}; D) - \bar{f}(\boldsymbol{x})^2]]$$

噪声

$$\varepsilon^2 = \mathbb{E}_D \big[(y_D - y)^2 \big]$$

• 偏差 (期望输出与真实标记的差别)

$$bias^2(\boldsymbol{x}) = (\bar{f}(\boldsymbol{x}) - y)^2$$

• 假定 $\mathbb{E}_D[y_D - y] = 0$, 则可通过多项式展开得到

$$E(f;D) = \mathbb{E}_D [(f(\boldsymbol{x};D) - y_D)^2] = bias^2(\boldsymbol{x}) + var(\boldsymbol{x}) + \varepsilon^2$$

泛化误差可分解为偏差、方差与噪声之和。

- 偏差: 学习算法本身的拟合能力; 方差: 数据的充分性; 噪声: 学习问题本身的难度
- 偏差-方差窘境 (bias-variance dilemma): 训练不足时偏差主导,训练 加深时方差主导,训练充足时容易发生过拟合。

- 3 线性模型
 - 4 决策树
- 5 神经网络
- 6 支持向量机
- 7 贝叶斯分类器
 - 8 集成学习
 - 9 聚类
- 10 降维与度量学习
- 11 特征选择与稀疏学习
 - 12 计算学习理论
 - 13 半监督学习
 - 14 概率图模型
 - 15 规则学习
 - 16 强化学习