Contents

[《机器学习》周志华 1](#_Toc498428548)

[基本概念 1](#_Toc498428549)

[模型评估与选择 （数据集=训练集+测试集） 3](#_Toc498428550)

[性能度量 4](#_Toc498428551)

[如何比较学习器？ 5](#_Toc498428552)

[偏差与方差 5](#_Toc498428553)

[线性模型 6](#_Toc498428554)

[决策树 7](#_Toc498428555)

[神经网络 8](#_Toc498428556)

[支撑向量机SVM和支撑向量回归SVR 9](#_Toc498428557)

[Bayes分类器 9](#_Toc498428558)

[集成学习ensemble learning （multi-classifier system, committee-based learning） 10](#_Toc498428559)

[《数据挖掘导论》 13](#_Toc498428560)

[数据 14](#_Toc498428561)

[数据类型 14](#_Toc498428562)

[数据质量 14](#_Toc498428563)

[预处理 15](#_Toc498428564)

[相似性和相异性的度量 17](#_Toc498428565)

[数据探索 18](#_Toc498428566)

[汇总统计 18](#_Toc498428567)

[可视化 18](#_Toc498428568)

[分类 19](#_Toc498428569)

[基本概念 19](#_Toc498428570)

[决策树 19](#_Toc498428571)

[貝叶期分类器 21](#_Toc498428572)

[KNN 22](#_Toc498428573)

[ANN 22](#_Toc498428574)

[SVM 22](#_Toc498428575)

[Emsemble组合方法 22](#_Toc498428576)

[不平衡类问题 23](#_Toc498428577)

[多类问题解决方法？ 24](#_Toc498428578)

[关联分析 25](#_Toc498428579)

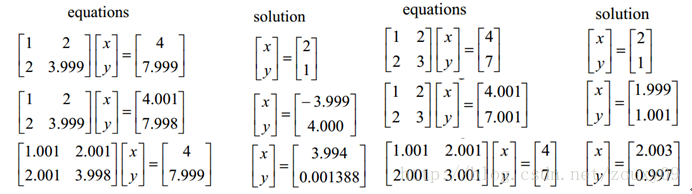
[聚类 25](#_Toc498428580)

[异常检测 27](#_Toc498428581)

数学知识点

病态ill-condition

假设我们有个方程组AX=b，我们需要求解X。如果A或者b稍微的改变，会使得X的解发生很大的改变，那么这个方程组系统就是ill-condition的，反之就是well-condition的



左边方程组系统是ill-conditioned病态的:

第一行假设是我们的AX=b，

第二行我们稍微改变下b，得到的x和没改变前的差别很大

第三行我们稍微改变下系数矩阵A，可以看到结果的变化也很大。

换句话来说，这个系统的解对系数矩阵A或者b太敏感了。又因为一般我们的系数矩阵A和b是从实验数据里面估计得到的，所以它是存在误差的，如果我们的系统对这个误差是可以容忍的就还好，但系统对这个误差太敏感了，以至于我们的解的误差更大，那这个解就太不靠谱了。

右边是well-condition系统

对于一个ill-condition的系统，我的输入稍微改变下，输出就发生很大的改变，这不好啊，这表明我们的系统不能实用啊。你想想看，例如对于一个回归问题y=f(x)，我们是用训练样本x去训练模型f，使得y尽量输出我们期待的值，例如0。那假如我们遇到一个样本x’，这个样本和训练样本x差别很小，面对他，系统本应该输出和上面的y差不多的值的，例如0.00001，最后却给我输出了一个0.9999，这很明显不对呀。就好像，你很熟悉的一个人脸上长了个青春痘，你就不认识他了，那你大脑就太差劲了

如何量化ill-condition的可信度？condition number

condition number衡量的是输入发生微小变化的时候，输出会发生多大的变化。也就是系统对微小变化的敏感度。condition number值小的就是well-conditioned的，大的就是ill-conditioned的。

如果方阵A是非奇异的，那么A的condition number定义为：

http://img.blog.csdn.net/20140504122518843?watermark/2/text/aHR0cDovL2Jsb2cuY3Nkbi5uZXQvem91eHkwOQ==/font/5a6L5L2T/fontsize/400/fill/I0JBQkFCMA==/dissolve/70/gravity/SouthEast

概率与统计

参数估计

已知某个随机样本满足某种概率分布，但是其中具体的参数不清楚，参数估计就是通过若干次试验，观察其结果，利用结果推出参数的大概值

最大似然估计

建立在参数估计的思想上：已知某个参数能使这个样本出现的概率最大

解释：

从分布是p(x|θ)的总体样本中抽取到m个样本的概率，也就是样本集X中各个样本的联合概率

http://img.my.csdn.net/uploads/201301/24/1359003923_8916.jpg

这个函数放映的是在不同的参数θ取值下，取得当前这个样本集的可能性，因此称为参数θ相对于样本集X的似然函数（likehood function）

最大似然估计你可以把它看作是一个反推。多数情况下我们是根据已知条件来推算结果，而最大似然估计是已经知道了结果，然后寻求使该结果出现的可能性最大的条件，以此作为估计值。

例子：

身高分布估计

在学校所有男生（身高）中，独立地按照概率密度p(x|θ)抽取100个（身高），组成样本集X，如何通过样本集X估计未知参数θ。假定概率密度p(x|θ)是高斯分布N(u,∂)，则未知参数是θ=[u, ∂]T

EM算法：是一种从不完全数据或有数据丢失的数据集（存在隐含变量）中求解概率模型参数的最大似然估计方法。

例如：在学校所有人（身高）中，独立地抽取200个（身高），组成样本集，如何通过样本集X估计：高斯混合模型（一是这个人是男的还是女的？二是男生和女生对应的身高的高斯分布的参数是多少？）

先有鸡还是先有蛋: 两种高斯分布的人混在一块了，我们又不知道哪些人属于第一个高斯分布，哪些属于第二个，所以就没法估计这两个分布的参数。反过来，只有当我们对这两个分布的参数作出了准确的估计的时候，才能知道到底哪些人属于第一个分布，那些人属于第二个分布

EM算法的基本思想：为了解决这个你依赖我，我依赖你的循环依赖问题，总得有一方要先打破僵局，说，不管了，我先随便整一个值出来，看你怎么变，然后我再根据你的变化调整我的变化，然后如此迭代着不断互相推导，最终就会收敛到一个解。

EM算法：假设估计A和B两参数，在开始状态下二者都是未知的，但如果知道A信息就可以得到B信息，反过来知道B也就得到A。可以考虑首先赋予A某种初值，以此得到B的估计值，然后从B的当前值出发，重新估计A的取值，这个过程一直持续到收敛为止。

EM = Expectation Maximization，如身高问题？

Expectation阶段：先随便猜一下男生（身高）的正态分布的参数：如均值和方差是多少。例如男生的均值是1米7，方差是0.1米（当然了，刚开始肯定没那么准），然后计算出每个人更可能属于第一个还是第二个正态分布中的（例如，这个人的身高是1米8，那很明显，他最大可能属于男生的那个分布）。

Maximization：有了每个人的归属，或者说我们已经大概地按上面的方法将这200个人分为男生和女生两部分，我们就可以根据之前说的最大似然那样，通过这些被大概分为男生的n个人来重新估计第一个分布的参数，女生的那个分布同样方法重新估计。当我们更新了这两个分布的时候，每一个属于这两个分布的概率又变了，那么我们就再需要调整E步……如此往复，直到参数基本不再发生变化为止。

咋知道新的参数的估计就比原来的好?

数学推导，可以证明

# 《机器学习》周志华

## 基本概念

在计算机系统中，“经验”通常以数据形式存在，因此，机器学习所研究的主要内容是关于在计算机上从数据中产生“模型”的算法，即学习算法

模型：泛指从数据中学得的结果

模式：局部性结果（如一条规则）

学得模型对应了关于数据的某处潜在的规律，因此亦称为“假设”

机器学习的目标：使学得的模型能很好地适用于”新样本”

**尽管训练集通常只是样本空间的一个很小的采样，我们仍希望它能很好地反映出样本空间的特性，否则就很难期望在训练集上学得的模型能在整个样本空间上都工作得很好**。通常假设样本空间中总体样本服从一个未知“分布”D，我们获得的每个样本都是独立地从这个分布上采样获得的，即独立同分布i.i.d

**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”的假设，假设的表示一旦确定，假设空间及其规模大小就确定了**。如我们的假设空间由形如“(色泽=?) and (根蒂=?) and (敲声=?)的可能取值所形成的假设组成。可以有许多策略对这个假设空间进行搜索，搜索过程中可以不断删除与正例不一致的假设、和与反倒一致的假设，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。但学习过程是基于有限样本训练集进行的，因此，可能有多个假设与训练集一致，应该采用哪一些模型（假设）呢？由机器学习算法在学习过程中对某种类型假设的偏好决定，即归纳偏好(inductive bias)。

**任何一个有效的机器学习算法必有其归纳偏好**。比如若认为相似的样本应有相似的输出（例如，在各种属性上都很相像的西瓜，成熟程度应该比较接近），则对应的学习算法可能偏好比较”平滑“的曲线，而不是比较”崎岖“的曲线。再比如Occam’s razor原则，若有多个假设与观察一致，则选最简单的那个。

归纳偏好对应了学习算法本身所做出的关于”什么样的模型更好“的假设，在具体的现实问题中，这个假设是否成立，即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。

若所有”问题“出现的机会相同，或所有问题同等重要，那么无论学习算法a多聪明，学习算法b多笨拙，它们的期望性能是相同的，这就是”没有免费的午餐“定理。然后实现情形并不是这样，很多时候，我们只关注自己正在试图解决的问题（例如某个具体应用任务）。所以**要谈论算法的相对优劣，必须要针对具体的学习问题**，在某些问题上表现好的学习算法，在另一些问题上却可能不尽如人意，学习算法自身的归纳偏好与问题是否相配，往往会起到决定性的作用。

1950 – 1970 推理期

基于符号知识表示、通过演绎推理技术

1970 - 知识期

基于符号知识表示，通过获取和利用领域知识来建立专家系统

机械学习：没有进行真正的学习，仅是在进行信息存储与检索

**归纳学习：从样例中学习，即从训练样例中归纳出学习结果**

= 符号主义学习 （产生明确的概念，如决策树，基于逻辑学习）

连接主义学习 （产生的是黑箱模型，如神经网络，深度网络）

统计学习 （如SVM 以及更一般的核方法）

数据挖掘：从海量数据中发掘知识 = 数据库+机器学习+统计学

离散属性数值化

对离散属性，**若属性值间存在序order关系，可通过连续化将其转化为连续值**，例如值属性“身高”的取值{高，矮}可转化为{1.0, 0.0}，三值属性”高度“的取值{高，中，低}可转化为{1.0, 0.5, 0.0}; **若属性值间不存在序关系，假定有k个属性值，则通常转化为k维向量**。例如属性”瓜类“的取值{西瓜，南瓜，黄瓜}可转化为(0, 0, 1), (0, 1, 0), (1, 0, 0)

多分类学习与多标记学习(multi-label learning)区别?

多分类学习中，每个样本仅属性一个类别，多标记学习中一个样本同时预测出多个类别标记，如一幅图像可同时标注为“蓝天”，“白云”，“羊群”，“自然场景”

多分类学习 见p63

基本策略：拆解法，将多分类任务拆为若干个二分类任务求解。**关键是如何对多分类任务进行拆分，以及如何对多个分类器进行集成**。

一对一：将N个类别两两配对 ，从而产生N(N-1)/2个二分类任务。在测试阶段，新样本同时提交给所有分类器，得到N(N-1)/2分类结果，最终结果通过投票产生。

一对多：每次将一个类的样例作为正例，所有其他类作为反例，从而训练N个分类器，在测试时若仅有一个分类器预测为正类，则对应的类别标记作为最终分类结果，若有多个分类器预测为正类，选择置信度最大的类别标记作为分类结果

多对多：每次将若干个类作为正类，若干个其他类作为反类，需要特殊的设计，不能随意选取，常见的有”纠错输出码”方法

类别不平衡问题 则p66

* 一个基本策略：再缩放rescaling

线性分类器，预测出的y值与一个阈值进行比较，通常y>0.5时判别为正例，否则为反例。阈值为0.5表明分类器认为真实正反例可能性相同，即分类器决策规则为若y / (1-y) > 1， 则预测为正例

若类别不平均，要强调类少的重要性，用观测几率代表真实几度，即只要分类器的预测几率高于观测几率就应判定为正例，即若y / ( 1-y) > m+ / m-, 则预测为正例

相当于对预测值进行调整

y’ / (1 – y’) = 1 / (1 – y) \* m+ / m-

rescaling不常用，因为“训练集是真实样本总体的无偏采样”这个假设往往并不成立，也就是说，我们未必能有效地基于训练集观测几率来推断出真实几率。

常采用做法：

* 欠采样：

丢弃很多反倒，当然不能随机丢弃反倒，因为可能丢失一些重要信息；欠采样法的代表性算法EasyEnsemble[Liu et al., 2009]则是利用集成学习机制，将反倒划分为若干个集合供不同学习器使用，这样对每个学习器来看都进行了欠采样，但在分局来看却不会丢失重要信息。

* 过采样：

不能简单地对初始正例样本进行重复采样，否则会招致严重的过拟合

阈值移动threshold-moving: 直接基于原始训练集进行学习，但在用训练好的分类器进行预测时，将rescaling嵌入到其决策过程中。

增量学习 incremental learning

在学得模型后，再接收到训练样例时，仅需根据新样例对模型进行更新，不必重新训练整个模型，并且先前学得的有效信息不会被“冲掉”

在线学习

指每获得一个新样本就进行一次模型更新

竞争型学习的“可塑性-稳定性窘境”

可塑性指神经网络要有学习新知识的能力，稳定性则指神经网络在学习新知识时要保持对旧知识的记忆。

## 模型评估与选择 （数据集=训练集+测试集）

经验误差（训练误差）：学习器在训练集上的误差

Overfitting: 应该从训练样本中尽可能学出适用于所有潜在样本的“普遍规律“，如果学习器把训练样本学得“太好”了的话，很可能已经把样本自身的一些特点当作了所有潜在样本都会具有的一般性质，这样就会导致泛化性能下降

**很多因素导致过拟合，最常见的情况是由于学习能力过于强大，以至于把训练样本所包含的不太一般的特性都学到了**，过拟合是无法彻底避免的，我们所能做的只是“缓解”，或者说减小其风险。

测试误差：测试集上的“测试误差”作为泛化误差的近似，通常我们假设测试样本也是从样本真实分布中独立分布采样而得。

训练集与测试集如何划分？

训练/测试集的划分要尽可能保持数据分布的一致性，避免因数据划分过程引入额外的偏差而对最终结果产生影响

* **分层采样(stratified sampling)**:

保留类别比例的采样方式

* **留出法hold-out**:

单次使用hold-out得到的估计结果往往不够稳定可靠，在使用hold-out时，一般要采用若干次随机划分、重复进行实验评估后取平均值作为hold-out的评估结果。常见做法是将大约2/3-4/5的样本用于训练，剩余样本用于测试

* **交叉验证法cross validation**:

数据集D划分k个大小相似的互斥子集, 每个子集都尽可能保持数据分布的一致性，即从D中通过分层采样得到。通常把交叉验证法称为“k折交叉验证”k-fold cross validation, k最常用的取值是10. 与hold-out相似，将数据集D划分为k个子集同样存在多种划分方式，为减少因样本划分不同而引入的差别，k折交叉验证通常要随机使用不同的划分重复p次，最终结果取均值. 若令k = 数据集数目，则为留一法leave-one-out. 留一法中被实际评估的模型与期望评估的用D训练出的模型很相似。

* **自助法bootstrapping**:

希望评估的是用D训练出的模型，而保留了一部分样本用于测试，因此实际评估的模型所使用的训练集比D小，这必然会引入一些因训练样本规模不同而导致的估计偏差。有没什么办法可以减少样本规模不同造成的影响？

自助法是一个比较好的解决方案，有放回抽样，则样本在m次采样中始终不被采到的概率是(1-1/m)m，取极限得到1/e = 0.368，即通过自助采样，初始数据集D中约有36.8%的样本未出现在采样数据集中。M个样本（含重复样本）作为训练集，未被采样的样本用于测试，亦称包外估计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； 此外，自助法能从初始训练集中产生多个不同的训练集，这对集成学习等方法有很大的好处。然后自助法产生的数据集改变了初始数据集的分布，这会引入估计偏差。因此在初始数据量足够时，留出法和交叉验证法更常用一些。

调参与最终模型 （训练集 = 训练集 + 验证集）

在研究对比不同算法的泛化性能时，我们用测试集上的判别效果来估计模型在实际使用时的泛化能力，而把训练数据另外划分为训练集和验证集，基于验证集上的性能来进行模型选择和调参。模型选择完成后，学习算法和参数配置已选定，此时应该用数据集D重新训练模型。

## 性能度量

* Error
* Accuracy
* precision(挑出的西瓜中有多少比例是好瓜？)
* recall(所有好瓜中有多少比例被挑了出来？)
* P-R曲线

预测结果是概率，将测试集的样例预测结果排序，顺序逐个把样本作为正例进行预测，每次计算出当前的precision and recall, 以precision为x轴，以recall为y轴作图

F1：precision and recall的调和平均

1/F1 = 1/2 \* (1/P + 1/R)

在一些应用中，对precision and recall的重视程度有所不同，例如在商品推荐中， 为了尽可能少打扰用户，更希望推荐内容确是用户感兴趣的，此时precision更重要；而在逃犯信息的信息检索系统中，更希望尽可能少漏掉逃犯，此时recall更重要，需要用加权F1

* 加权F1: 加权调和平均

1/Fb = 1/(1+b2)(1/P + b2/R)

(Note: 与算术平均(P+R)/2 和几何平均(P+R)1/2相比，调和平均更重视较小值

* ROC:

预测结果是概率，将测试集的样例预测结果排序，顺序逐个把样本作为正例进行预测，每次计算出当前的真正率True Positive Rate = TP/(TP+FN), 假正率False Positive Rate = FP/(TN+FP), 以假正率为x轴，以真正率为y轴作图

## 如何比较学习器？

基于实验评估方法和性能度量，如何比较学习器？ 见page 37 -

比想像中的困难，有两个因素：

1. 因为比较的是泛化性能，然后实验评估方法获得的是测试集上的性能
2. 测试集上的性能与测试集本身的选择有很大关系

需要基于统计假设检验hypothesis test，即若在测试集上观察到学习器A比B好，则A的泛化性能是否在统计意义上优于B，以及这个结论的把握有多大？

* 对单个学习器泛化性能

1. 假设检验

假设检验中的”假设“是对学习器泛化错误率分布的某种判断或猜想，例如泛化错误率是否不大于0.3, 即error <= 0.3

已知测试错误率，在一定置信度下，接受还是拒绝假设

估推出泛化错误率的分布

假定泛化错误率为error, 测试错误率为error\_t (意味着在m个测试样本中恰有error\_t \* m个被误分类)

误分类样本数的概率分布满足二项分布

P(error\_t; error) = Cmn \* errorerror\_t\*m \* (1-error)m-(error\_t\*m)

假设error <= e0, 求得在置信度1 – alpha的概率内所能观测到的最大错误率max\_error

若测试错误率error\_t<最大错误率max\_error，则假设error<= e0不能被拒绝，即以1-alpha的置信度认为，学习器的泛化错误率不大于e0

1. t检验(t-test)

若通过多次重复hold-out or cross-validation进行多次训练/测试，会得到多个测试错误率，此时用t检验(t-test)

* 对多个学习器泛化性能

1. 交叉验证t检验
2. McNemar检验

## 偏差与方差

对学习算法除了通过实验估计其泛化性能，还可以借助“偏差-方差分解”

偏差-方差分解试图对学习算法的期望泛化错误率进行拆解。

x: 测试样本

yD: 数据集中的标记

y: x的真实标记

f(x; D)：训练集D上学得模型f在x上的预测输出

f\_t = ED[f(x; D)]: 学习算法的期望预测

**var(x) = ED[(f – f\_t)2]: 使用样本数相同的不同训练集**

e\_n2 = ED[(yD – y )2]: 噪声产生的误差

**bias = f\_t – y: 偏差 （期望输出与真实标记的差别）**

算法的期望泛化误差：

ED[( f(x; D) – yD)2] = bias2 + var(x) + e\_n2

泛化误差可分解为偏差、方差与噪声之和

**偏差度量了学习算法的期望预测与真实结果的偏离程度，即刻画了学习算法本身的拟合能力**

**方差度量了同样大小的训练集的变动所导致的学习性能的变化，即刻画了数据扰动所造成的影响**

噪声则表达了在当前任务上任何学习算法所能达到的期望泛化误差的下界，即刻画了学习问题本身的难度。

**偏差-方差分解说明：泛化性能是由学习算法的能力、数据的充分性以及学习任务本身的难度所共同决定的。**

给定学习任务，为了取得好的泛化性能，则需使偏差较小，即能够充分拟合数据，并且使方差较小，即使得数据扰动产生的影响小

一般来说，偏差与方差是有冲突的。**给定学习任务，若在训练不足时，学习器的拟合能力不强，训练数据的扰动不足以使学习器产生显著变化，此时偏差主导了泛化错误率； 随着训练程度的加深，学习器的拟合能力逐渐增强，训练数据发生的扰动渐渐能被学习器学到，方差逐渐主导了泛化错误率； 在训练程度充足后，学习器的拟合能力非常强，训练数据发生的轻微扰动都会导致学习器发生显著变化，若训练数据自身的、非全局的特性被学习器学到了，则将发生过拟合。**

## 线性模型

线性模型有很好的可解释性

线性回归：y = WTx + b

Wopt = (XTX)-1XTy

**现实任务中XTX往往不是满秩，例如在许多任务中我们会遇到大量的变量，其数目甚至超过样例数，此时可解出多个w, 它们都能使均方误差最小化，选择哪一个解作为输出，将由学习算法的归纳偏好决定，常见的做法是引入正则化regularization项。**

（稀疏表示sparse representation：本质上对应L0范数的优化，这在通常条件下是NP难题，LASSO通过L1范数来近似L0范数，是求取稀疏解的重要技术）

对数线性回归：lny = WTx + b

广义线性模型：y = g-1(WTx + b) g(.)单调可微函数

Sigmoid函数：y = 1/(1+e-z), z = WTx + b

等价于 ln(y/(1-y)) = WTx + b 其中ln(y/(1-y))称为对数几率

**优点：直接对分类可能性进行建模，无需事先假设数据分布，这样就避免了假设分布不准确所带来的问题，它不是仅预测出“类别”，而是可得到近似概率预测**，这对许多需利用概率辅助决策的任务很有用。

线性判别分析LDA = Linear Discriminant Analysis

思想：给定训练集，设法将样例投影到一条直线上，使得同类样例的投影点尽可能接近，异类样例的投影点尽可能远。

y = WTx

Sw: 类内散度矩阵 within-class scatter matrix

Sb: 类间散度矩阵between-class scatter matrix

Wopt = Sw-1 (u0 – u1)

考虑到数值解的稳定性，在实践中通常是对Sw进行奇异值分解

## 决策树

决策过程中提出的每个判定问题都是对某个属性的“测试”，例如“色泽=？”； 每个测试的结果或是导出最终结论，或是导出进一步的判定问题，其考虑范围是在上次决策结果的限定范围之内

一棵决策树包含一个根结点、若干个内部结点和若干个叶结点；叶结点对应于决策结果，其他每个结点则对应于一个属性测试。

一般而言，随着划分过程不断进行，我们希望决策树的分支结点所包含的样本尽可能属于同一类别，即结点的“纯度”越来越高

度量样本集合纯度purity的指标：

信息熵information entropy: - 类k比例\*log(类k比例)的求和 k个类别

基尼指数Gini index: 反映了从数据集D中随机抽取两个样本，其类别标记不一致的概率

剪枝

**决策树分支过多，会把训练样本学得过好，以致于把训练集自身的一些特点当作所有数据都具有的一般性质而导致过拟合，因此可通过主动去掉一些分支来降低过拟合的风险**

预剪枝pre-pruning 和后剪枝post-pruning

预剪枝：在决策树生成过程中，对每个结点在划分前先进行估计，若当前结点的划分不能带来决策树泛化性能提升，则停止划分并将当前结点标记为叶结点

**有些分支的当前划分虽不能提升泛化性能、甚至可能导致泛化性能暂时下降，但在其基础上进行的后续划分却有可能导致性能显著提高**，而预剪枝基于贪心本质禁止这些分支展开，给预剪枝决策树带来了欠拟合的风险

后剪枝：先从训练集生成一棵完事的决策树，然后自底向上地对非叶结点进行考察，若将该结点对应的子树替换为叶结点能带来决策树泛化性能提升，则将该子树替换为叶结点

后剪枝决策树通过比预剪枝保留了更多的分支，一般情形下，**后剪枝决策树的欠拟合风险很小，泛化性能往往优于预剪枝。**

**如何判断决策树泛化性能是否提升呢？从训练集中预留一部分用作验证集以进行性能评估**

多变量决策树

决策树所形成的分类边界有一个明显的特点：轴平行，即它的分类边界由若干个与坐标轴平行的分段组成。

显然，**分类边界的每一段都是与坐标轴平行的，这样的分类边界使得学习结果有较好的可解释性，因为每一段划分都直接对应了某个属性取值。但在学习任务的其实分类边界比较复杂时，必须使用很多段划分才能获得较好的近似。**

如何使用斜的划分边界甚至更复杂划分的决策树？

采用多变量决策树，非叶结点不再是仅对某个属性，而是对属性的线性组合（对应斜划分边界）进行测试。

信息增益，增益率，基尼指数等准则对决策树的尺寸有较大影响，但对泛化性能影响有限，大约2%左右

**剪枝方法和程度对决策树泛化性能影响相当显著**，在数据带有噪声时通过剪枝甚至可将决策树的泛化性能提高25%

## 神经网络

Sigmoid函数，它把可能在较大范围内变化的输入值挤压到(0, 1)输出范围内，因此有时也称为“挤压函数”squashing function

过拟合

BP神经网络，由于其强大的表示能力，BP神经网络经常遭遇过拟合，其训练误差持续降低，但测试误差却可能上升，两种策略：

Early stopping：将数据分为训练集和验证集，验证集误差升高，则停止训练，返回具有最小验证集误差的连接权和阈值

正则化：在误差目标函数中增加一个用于描述网络复杂度的部分

局部权小问题

以多组不同参数初始化多个神经网络，相当于从多个不同的初始点开始搜索

模拟退火：在每一步都以一定的概率接受比当前解更差的结果

遗传算法

常见神经网络：

RBF网络

单隐层前馈神经网络，使用径向基函数作为隐层神经元激活函数，而输出层则是对隐层神经输出的线性组合。

ART网络 （竞争型学习，无监督学习）

比较层+识别层+识别阈值+重置模块

比较层负责接收输入样本，并将其传递给识别层神经元，识别层神经元对应一个模式类，神经元数目可以训练过程中动态增长以增加新模式类

在接收到比较层的输入信号后，识别层神经元之间相互竞争以产生获胜神经元。竞争的最简单方式：计算输入向量与每个识别层神经元所对应的模式类的代表向量之间的距离，距离最小者胜。若输入向量与获胜神经元的相似度大于识别阈值，则当前输入样本将被归为获胜神经元的向量集，同时，网络连接权将会更新，使得以后在接收到相似输入样本时该模式类会计算出更大的相似度，从而使该获胜神经元有更大可能获胜；若相似度不大于识别阈值，则重置模块奖在识别层增设一个新的神经元，其代表向量就设置为当前输入向量

SOM网络

级联相关网络Cascade-Correlation网络

Recurrent neural networks递归神经网络

隐层神经元的输出被反馈回来，与下一时刻输入层神经元提供的信号一起，作为隐层神经元在下一时刻的输入。

Boltzmann机

深度学习

深层神经网络：通过多层处理，逐渐将初始的“低层”特征表示转化为“高层”特征表示后，用“简单模型”即可完成复杂的分类等学习任务。深度学习也可理解为“特征学习”或表示学习representation learning

参数越多的模型，复杂度越高，容量capacity越大，意味着它能完成更复杂的学习任务

逐层训练 = 预训练pre-training + 微调fine-tuning

每次训练一层隐结点，训练时将上一层隐结点的输出作为输入，而本层隐结点的输出作为下一层隐结点的输入 (预训练)；在预训练全部完成后，再对整个网络进行“微调”

## 支撑向量机SVM和支撑向量回归SVR

基于训练集D在样本空间中找到一个划分超平面，将不同类别的样本分开，但能将训练样本分开的划分超平面可能有很多

SVM目标：找最大间隔maximum margin

训练完成后，大部分的训练样本都不需要保留，最终模型仅与支持向量有关

在现实任务中，原始样本空间内也许并不存在一个能正确划分两类样本的超平面，幸运的是，如果原始空间是有限维，即属性数有限，那么一定存在一个高维特征空间使样本可分

我们希望样本在特征空间内线性可分，因此特征空间的好坏对支持向量机的性能至关重要。在不知道特征映射的形式时，我们并不知道什么样的核函数是合适的，若核函数选择不合适，则意味着将样本映射到了一个不合适的特征空间

核函数直接决定了支持向量机与核方法的最终性能，但遗憾的是，核函数的选择是一个未决问题

无法SVM or SVR, 学得的模型总能表示成核函数的线性组合

核方法：基于核函数的学习方法

最常见的是，通过“核化”（即引入核函数）来将线性学习器拓展为非线性学习器，如核线性判别分析kernelized linear discriminant analysis

线性核SVM迄今仍是文本分类 的首选技术。一个重要原因可能是：若将每个单词作为文本数据的一个属性，则该属性空间维数很高，冗余度很大。其描述能力足以将不同文档打散

支持向量机的求解通常是借助于凸优化技术

## Bayes分类器

决策树、BP神经网络、支持向量机等属于判别式模型

Bayes分类器属于生成式模型

类后验概率p(c | x) = p( c) \* p(x | c) / p(x)

p(x): 归一化因子

p(c): 类先验概率，表达了样本空间中各类样本所占的比例，根据大数定律，当训练集包含充足的独立同分布样本时，p(c)可通过各类样本出现的频率来进行估计

p(x | c):似然（也称为类条件概率），样本x相对类标记c的类条件概率。涉及关于x所有属性的联合概率，直接根据样本出现的频率来估计将会遇到严重的困难。例如，假设样本的d个属性都是二值的，则样本空间将有2d种可能的取值，在现实应用中，这个值往往远大于训练样本数m

估计似然的一种常用策略：先假定其具有某种确定的概率分布形式，再基于训练样本对概率分布的参数进行估计，事实上概率模型的训练过程就是参数估计parameter estimation过程。

频率主义学派的极大似然估计maximum likelihood estimation：根据数据采样来估计概率分布参数的经典方法，极大似然估计是试图在参数所有可能的取值中，找到一个能使数据出现的“可能性”最大的值

参数化的方法虽能使似然估计变得相对简单，但估计结果的准确性严重依赖于所假设的概率分布形式是否符合潜在的真实数据分布。在现实应用中，欲做出能较好地接近潜在真实分布的假设，往往需要一定程度上利用关于应用任务本身的经验知识

朴素Bayes分类器：似然是所有属性上的联合概率，难以从有限的训练样本直接估计而得。为避开这个障碍，朴素Bayes分类器采用了“属性条件独立性假设”，对已知类别，假设所有属性相互独立。

这个假设在现实应用中往往很难成立，但有趣的是，native bayes在很大情形下都能获得相当好的性能，为什么？若属性间依赖对所有类别影响相同，或依赖关系的影响能相互抵消，则属性条件独立性假设在降低计算开销的同时不会对性能产生负面影响。

Native bayes在信息检索领域尤为常用

Bayes network (也称为belief network)

表示任意属性间的依赖性，借助有向无环图来刻画属性之间的依赖关系，并使条件概率表来描述属性的联合概率分布

= 结构学习 + 参数学习

半朴素Bayes分类器

适当考虑一部分属性间的相互依赖信息，从而既不需要进行完全联合概率计算，又不至于彻底忽略了比较强的属性依赖关系。

TAN (Tree Augmented native Bayes)： 求解强相关属性之间的依赖性

1. 计算任意两个属性之间的条件互信息
2. 以属性为结点构建完全图，任意两个结点之间权重设为条件互信息
3. 构建此完全图的最大带权生成树，挑选根变量，将边置为有向
4. 加入类别结点y, 增加从y到每个属性的有向边

## 集成学习ensemble learning （multi-classifier system, committee-based learning）

集成学习通过构建并结合多个学习器来完成学习任务

在一般经验中，如果把好坏不等的东西掺到一起，那么通常结果会是比最坏的要好一些，比最好的要坏一些，集成学习把多个学习器结合起来，如何能获得比最好的单一学习器更好的性能呢？

当然有要求，要获得好的集成，个体学习器应“好而不同”，即学习器要有一定的准确性和多样性（即学习器间具有差异），如下：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 测试例1 | 2 | 3 |  | 1 | 2 | 3 |  | 1 | 2 | 3 |
| H1 | 分类正确 | 正确 | 错误 | H1 | 正确 | 正确 | 错误 | H1 | 正确 | 错误 | 错误 |
| H2 | 分类错误 | 正确 | 正确 | H2 | 正确 | 正确 | 错误 | H2 | 错误 | 正确 | 错误 |
| H3 | 分类正确 | 错误 | 正确 | H3 | 正确 | 正确 | 错误 | H3 | 错误 | 错误 | 正确 |
| 集成 | 分类正确 | 正确 | 正确 | 集成 | 正确 | 正确 | 错误 | 集成 | 错误 | 错误 | 错误 |

左表格集成提升性能，中表格集成不起作用，右表格集成起负作用

如何产生并结合“好而不同”的个体学习器，恰是集成学习研究的核心

基学习器：同种类型的个体学习器，如决策树集成

个体学习器

弱学习器：泛化性能略优于随机猜测的学习器，如在二分类问题上精度略高于50%的分类器，虽然从理论上来说使用弱学习器集成足以获得好的性能，但在实践中出于种种考虑，例如希望使用较少的个体学习器，人们往往会使用比较强的学习器

序列化方法

个体学习器间存在强依赖关系，如Boosting, AdaBoost

Boosting是一族将弱学习器提升为强学习器的算法，先从初始训练集训练出一个基学习器，再根据其学习器的表现对训练样本分布进行调整，使得先前基学习器做错的训练样本在后续受到更多关注，然后基于调整后的样本分布来训练下一个基学习器，如此重复进行，直到基学习器数目达到事先指定的值T，最终将这T个基学习器进行加权结合

AdaBoost算法：

1. 初始化样本权值分布
2. 基于分布Dt从数据集D中训练出分类器ht
3. 估计ht的测试误差
4. 确定分类器ht的权重
5. 更新样本分布，使下一轮的基学习器Ht+1能纠正Ht的一些错误

Boosting算法要求基学习器能对特定的数据分布进行学习，这可通过re-weighting实施，即在训练过程的每一轮中，根据样本分布为每个训练样本重新赋予一个权重，对无法接受带权样本的基学习算法，则可通过re-sampling来处理，即在每一轮学习中，根据样本分布对训练集重新进行采样，再用重采样而得的样本集对基学习器进行训练。

Boosting算法在训练的每一轮都要检查当前生成的基学习器是否满足基本条件（是否比随机猜测好）

从偏差-方差分解的角度看，Boosting主要关注降低偏差，因此Boosting能基于泛化性能相当弱的学习器构建出很强的集成

并行化方法

个体学习器间不存在强依赖关系，可并行生成，如Bagging, Random Forest

Bagging

自助采样法采样出T个含m个训练样本的采样集，然后基于每个采样集训练出一个基学习器，再将这些基学习器进行结合

在对预测输出进行结合时，Bagging通常对分类任务使用简单投票法，对回归任务使用简单平均法

自助采样过程还给Bagging带来了另一个优点：由于每个基学习器只使用了初始训练集中约63.2%的样本，剩下约36.8%的样本可用作验证集来对泛化性能进行”包外估计“out-of-bag estimate

从偏差-方法角度看，Bagging主要关注降低方差，因此它在不剪枝决策树、神经网络等易受样本扰动的学习器上效用更为明显

Random Forest

在以决策树为基学习器构建Bagging集成的基础上，进一步在决策树的训练过程中引入了随机属性选择。具体来说，传统决策树在选择划分属性时是在当前结点的属性集合中选择一个最优属性；而在RF中，对基决策树的每个结点，先从该结点的属性集合中随机选择一个包含k个属性的子集，然后再从这个子集中选择一个最优属性用于划分。一般推荐值k取属性数目的log2。

随机森林对Bagging只做了小改动，但是与Bagging中基学习器的”多样性“仅通过样本扰动（通过对初始训练集采样）而来不同，随机森林中基学习器的多样性不仅来自样本扰动，还来自属性扰动，这就使得最终集成的泛化性能可通过个体学习器之间差异度的增加而进一步提升。

随机森林的起始性能往往相对较差，特别是在集成中只包含一个基学习器时，这很容易理解，因为通过引入属性扰动，随机森林中个体学习器的性能往往有所降低，然而随着个体学习器数目的增加，随机森林通常会收敛到更低的泛化误差，值得一提的是，随机森林的训练效率常优于Bagging.

如何组合个体学习器？

简单平均法

加权平均法

加权平均法的权重一般是从训练数据中学习而得，现实任务中的训练样本通常不充分或存在噪声，这将使得学出的权重不完全可靠，尤其是对规模比较大的集成来说。一般而言，在个体学习器性能相差较大时宜使用加权平均法，而在个体学习器性能相近时宜使用简单平均法

绝对多数投票法majority voting

若某标记得票过半数，则预测为该标记，否则拒绝预测

Majority voting提供了”拒绝预测“选项，这在可靠性要求较高的学习任务中是一个很好的机制

相对多数投标法plurality voting

预测得票最多的标记，若同时有多个标记获得最高票，先置信度高的

加权投票法weighted voting

学习法

当训练数据很多时，通过另一个学习器来进行结合，如Stacking

个体学习器称为初始学习器，用于结合的学习器称为次级学习器

Stacking算法

初始数据集训练出初始学习器

生成次级学习器的训练集

次级训练集是由初始学习器的输出产生，作为输入特征，标记仍是初始样本的标记

若直接用初始学习器的训练集来产生次级训练集，则过拟合风险会比较大；因此一般是通过使用交叉难或留一法这样的方式，用训练初始学习器未使用的样本来产生次级学习器的训练样本

如将初始学习器的输出类概率作为次级学习器的输入属性，用多响应性回归作为次级学习算法

如何提升多样性？

一般思路是在学习过程中引入随机性，常见做法主要是对数据样本、输入属性、输出表示、算法参数进行扰动

**数据样本扰动**：常基于采样法，在Bagging中使用自助采样，在AdaBoost中使用序列采样。训练样本稍加变化就会导致学习器有显著变动如决策树、神经网络等，数据样本扰动法对这个的”不稳定学习器“很有效。然而有一些基学习器对数据样本的扰动不敏感，例如线性学习器，支持向量机，朴素贝叶斯，k近邻学习器，这样的基学习器称为稳定学习器

**输入属性扰动**：对包含大量冗余属性的数据，在子空间中训练个体学习器能产生多样性大的个体，由于冗余属性多，减少一些属性后训练出的个体学习器也不至于太差，若数据只包含少量属性，或冗余属性很少，则不宜使用输入属性扰动法

**算法参数扰动**：通过随机设置不同的参数，往往可产生差别’较大的个体学习器。注意，使用单一学习器时通常需使用交叉验证等方法来确定参数，这事实 已使用了不同参数训练出多个学习器，只不过最终仅选择其中一个学习器进行使用，而集成学习则相当于把这些学习器都利用起来。

无监督学习 = 聚类， 密度估计， 异常检测

聚类

聚类过程仅能自动形成簇结构，族所对应的概念语义需由使用者来把握和命名

物以类聚，即同一族的样本尽可能彼此相似，不同族的样本尽可能不同

Voronoi剖分

对任意样本x，它将被划入与其距离最近的原型向量pi所代表的簇中；换言之，每个原型向量定义了与之相关的一个区域Ri, 该区域中每个样本与pi的距离不大于它与其他原型向量的距离，由此形成了对样本空间的簇划分

聚类性能度量

考虑聚类结果的族划分C = {C1, C2, … Ck}

avg(C ): 簇内样本间的平均距离

diam(C ): 族内样本间的最远距离

dmin(Ci, Cj): 两个簇样本间的最近距离

dcen(Ci, Cj): 两个族中心的距离

指标有DB指数，Dunn指数，见p199

距离计算

Minkowski distance: distmk(xi, xj) = (xi – xj)pp

当p=2， 欧式距离

当p=1, 曼哈顿距离

连续值属性和有序属性，均可用Minkowski距离计算

对无序属性，采用以VDM距离(value difference metric) 见p201

加权距离计算：distwmk(xi, xj) = w\*(xi – xj)pp

原型聚类

假设聚类结构能通过一组原型向量来刻画

如k均值算法，通过k个簇内均值刻画

1. 初始化k个均值向量 （随机选取样本），代表k个簇
2. 考察每个样本，划分到最近的k个簇 (比较样本与k个均值向量的距离)
3. 更新k个族的刻画（计算族均值向量）
4. 重复上述过程，直到算法停止

学习向量量化learning vector quantization ： 有监督聚类

假设数据样本带有类别标记，学习过程利用样本的这些监督信息来辅助聚类

1. 初始化k个原型向量 （分层随机选取样本）
2. 考察每个样本，找到距离最近的原型向量
3. 根据类别标记是否一致，更新原型向量。

若最近的原型向量与样本的类别标记相同，则令原型向量靠拢该样本；

若类别标记不同，则令原型向量远离该样本

1. 重复上述过程

如高斯混合聚类，采用k个高斯分布来刻画

假设样本的生成过程由高斯混合分布给出：首先，根据a1, a2, … ak定义的先验分布选择高斯混合成分，其中ai为选择第i个混合成分的概率；然后，根据被选择的混合成分的概率密度函数进行采样，从而生成相应的样本。

1. 初始化高斯混合分布：k个混合系数ai和高斯分布的模型参数（均值向量，协方差矩阵）
2. 由样本计算各混合成分生成的后验概率
3. 更新k个混合系数和高斯分布的模型参数
4. 重复上述过程

密度聚类

假设聚类结构能通过样本分布的紧密程度确定

DBSCAN: 基于一组“邻域”参数(距离，最小样本数)来刻画样本分布的紧密程度

根据邻域参数，找出所有核心对象

以任一核心对象为出发点，找出由密度可达的样本生成聚类簇，直至所有核心对象均被访问

层次聚类

先将数据集中的每个样本看作一个初始聚类簇，然后在算法运行的每一步中找出距离最近的两个聚类簇进行合并，该过程不断重复，直到预设的聚类簇个数

关键是如何计算聚类簇之间的距离？

集合间的距离计算：

最小/最大距离：两个簇的最近/最远样本确定

平均/hausdorff距离：两个簇的平均/见图像分割结果的比较

异常检测，常借助于聚类或距离计算进行，如将远离所有簇中心的样本作为异常点，或将密度极低处的样本作为异常点

降维

维数灾难

在高维情形下出现的数据样本稀疏、距离计算困难等问题，是所有机器学习方法共同面临的严重障碍

降维：即通过某种数学变换将原始高维属性空间转变为一个低维“子空间”

为什么能进行降维？

因为在很多时候，人们观测或收集到的数据样本虽是高维的，但与学习任务密切相关的也许仅是某个低维分布，即高维空间中的一个低维“嵌入”embedding

多维缩放multiple dimensional scaling：若要求原始空间中样本之间的距离在低维空间中得以保持，具体算法见p229

对降维效果的评估，通常是比较降维前后学习器的性能，若性能有所提高则认为降维起到了作用，若将维数降至二维或三维，则可通过可视化技术来直观地判断降维效果

PCA

使所有样本的投影尽可能分开，则需最大化投影点的方差。

PCA是一种线性投影，新空间的轴与最大方差的方向对齐

新的特征是现有特征的线性组合（即旋转）

算法：

输入：样本集，低维空间维数d’

过程：

1. 对所有样本进行中心化
2. 计算样本的协方差矩阵
3. 对协方差矩阵做特征值分解
4. 取最大的d’个特征值所对应的特征向量

输出：投影矩阵=（特征向量1, 特征向量2, …）

实践中常通过对X进行奇异值分解来代替协方差矩阵的特征值分解，主成分是X的右奇异

降维后低维空间的维数通常是由用户事先指定 （比如交叉验证选取较好的d’值）

还可从重构的角度设置一个重构阈值，降维后的特征值总和比例

PCA仅需保留降维后的特征向量和样本的均值向量，最小的d-d’特征向量被舍弃，舍弃这部分信息往往是必要的？

一方面，舍弃这部分信息之后能使样本的采样密度增大，这正是降维的重要动机

另一方面，当数据受到噪声影响时，最小的特征值所对应的特征向量往往与噪声有关，将它们舍弃能在一定程度上起到去噪的效果

流行学习manifold learning

流行: 指在局部具有欧氏空间的性质

等度量映射isometric mapping: 低维嵌入流形上的测地线距离不能用高维空间的直线距离计算（如测地线距离），但能用低邻距离来近似

计算两点之间测地线距离的问题，可以转变为计算近邻连接图上两点之间的最短路径问题

算法：

输入：样本集D, 近邻参数k, 低维空间维d’

过程：

1. for i = 1, 2, … m do
   1. 确定xi的k近邻
   2. Xi与k近邻点之间的距离设置为欧氏距离，与其他点的距离设置为无穷大
2. 调用最短路径算法计算任意两样本点之间的距离dist(xi, xj)
3. 将dist(xi, xj)作为MDS算法的输入，返回低维空间坐标

输出：样本集在低维空间的投影

Isomap仅是得到了训练样本在低维空间的坐标，对新样本，如何将其映射到低维空间？常用解决方案是，将训练样本的高维空间坐标作为输入，低维空间坐标作为输出，训练一个回归学习器来对新样本的低维空间坐标进行预测

近邻参数的选择？

若近邻范围指定得较大，则距离很远的点可能被误为近邻，这样就出现“短路”问题；近邻范围指定得较小，则图中有些区域可能与其他区域不存在连接，这样就出现“断路”问题

特征选择与稀疏学习

特征选择过程必须确保不丢失重要特征

“无关特征”

冗余特征

如已有特征“长”，“宽”，“高”，那么“面积”，“体积”就是冗余特征。冗余特征很多时候不起作用，去除它们会减轻学习过程的负担。但有时冗余特征会降低学习任务的难度。比如某个冗余特征恰好对应了完成学习任何所需的“中间概念“，（如目标是体积，冗余特征面积），那么该冗余特征就是有用的

特征选择 = 特征子集搜索机制 +子集评价机制

特征子集搜索机制

前向搜索：逐渐增加相关特征的策略

后向搜索：逐渐减少特征的策略

子集评价：

对每个候选特征子集，我们可基于训练数据集D来计算其信息增益

一般地，特征子集A实际上确定了对数据集D的一个划分，每个划分区域对应着A上的一个取值，而样本标记信息Y则对应着对D的真实划分，通过估算这两个划分的差异，就能对A进行评价。

三种方法：

过滤式filter

先对数据集进行特征选择，然后再训练学习器，特征选择过程与后续学习器无关

包裹式wrapper

直接把最终将要使用的学习器的性能作为特征子集的评价准则

1. 随机产生特征子集
2. 基于交叉验证估计学习器误差
3. 若有改进，更新最优特征子集

嵌入式embedding

将特征选择过程与学习器训练过程融为一体，两者在同一个优化过程中完成，即在学习器训练过程中自动地进行了特征选择

典型的例子是基于L1正则化的学习方法

稀疏表示sparse representation

特征选择所考虑的问题是特征具有“稀疏性“，即矩阵中的许多列与当前学习任务无关。

数据集具有稀疏性，即D所对应的矩阵中存在很多元素，而且这些0元素并不是以整列、整行形式存在，在不少现实应用中我们会遇到这样的情形，如在文档分类任务中，通常将每个文档看作一个样本，每个字（词）作为一个特征，字（词）在文档中出现的频率或次数作为特征的取值。

当样本具有这样的稀疏表达形式时，对学习任务来说会有不少好处，例如线性支持向量机之所以能在文本数据上有很好的性能，恰是由于文本数据在使用上述的字频表示后具有高度的稀疏性，使大多数问题变得线性可分。

若给定数据集D是稠密的，能否将其转化为稀疏表示呢？

给普通稠密表达的样本找到合适的字典，将样本转化为合适的稀疏表示形式，从而使学习任务得以简化，模型复杂度得以降低，通常称为”字典学习“dictionary learning”，亦称“稀疏编码”sparse coding

在很多应用中均可获得稀疏性的表示，例如图像或声音的数字信号通常在时域上不具有稀疏性，但经过傅里叶变换，余弦变换，小波变换等处理后却会转化为频域上的稀疏信号

压缩感知 = 感知测量 + 重构恢复

在现实任务中，我们常希望根据部分信息来恢复全部信息。如采样后的数字信号恢复成模拟信号（只要满足Nysquist采样定理，采样频率是模拟信号最高频率的两倍以上）

那如果欠采样，能否重构原信号吗？

通过压缩感知技术恢复欠采样信号的前提条件：信号有稀疏表示

如客户对书的喜好程度评分，一般来说相似题材的书籍会有相似的读者，若能将书籍按题材归类，则题材总数必然远远少于书籍总数，因此从题材的角度，评分矩阵是稀疏的

矩阵补全matrix completion技术

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 笑傲江湖 | 万历十五年 | 人间词话 | 神雕侠侣 | 人类的故事 |
| 用户1 | 5 | ？ | ？ | 3 | 2 |
| 用户2 | ？ | 5 | 3 | ？ | 5 |
| 用户3 | 5 | 3 | ？ | ？ | ？ |
| 用户4 | 3 | ？ | 5 | 4 | ？ |

min rank(X) subject to (X)ij = (A)ij i, j 属于A非零元素下标

X表示待恢复的稀疏信号

A表示如表格评分矩阵的已观测信号

理论研究表明，在满足一定条件时，若rank(A) = r, n << m, 则只需观察到O(mr\*logm)个元素就能完美恢复A

机器学习中的范数规则化：L0, L1, L2

blog.csdn.net/zouxy09/article/details/24971995

监督机器学习问题无非就是“minimizeyour error while regularizing your parameters”，也就是在规则化参数的同时最小化误差。最小化误差是为了让我们的模型拟合我们的训练数据，而规则化参数是防止我们的模型过分拟合我们的训练数据。多么简约的哲学啊！因为参数太多，会导致我们的模型复杂度上升，容易过拟合，也就是我们的训练误差会很小。但训练误差小并不是我们的最终目标，我们的目标是希望模型的测试误差小，也就是能准确的预测新的样本。所以，我们需要保证模型“简单”的基础上最小化训练误差，这样得到的参数才具有好的泛化性能（也就是测试误差也小），而模型“简单”就是通过规则函数来实现的。另外，规则项的使用还可以约束我们的模型的特性。这样就可以将人对这个模型的先验知识融入到模型的学习当中，强行地让学习到的模型具有人想要的特性，例如稀疏、低秩、平滑等等。要知道，有时候人的先验是非常重要的。前人的经验会让你少走很多弯路，这就是为什么我们平时学习最好找个大牛带带的原因。一句点拨可以为我们拨开眼前乌云，还我们一片晴空万里，醍醐灌顶。对机器学习也是一样，如果被我们人稍微点拨一下，它肯定能更快的学习相应的任务。只是由于人和机器的交流目前还没有那么直接的方法，目前这个媒介只能由规则项来担当了。

还有几种角度来看待规则化的。

1. 规则化符合奥卡姆剃刀(Occam's razor)原理。这名字好霸气，razor！不过它的思想很平易近人：在所有可能选择的模型中，我们应该选择能够很好地解释已知数据并且十分简单的模型。

2. 从贝叶斯估计的角度来看，规则化项对应于模型的先验概率。民间还有个说法就是，规则化是结构风险最小化策略的实现，是在经验风险上加一个正则化项(regularizer)或惩罚项(penalty term)。

一般来说，监督学习可以看做最小化下面的目标函数：

http://img.blog.csdn.net/20140504122253546?watermark/2/text/aHR0cDovL2Jsb2cuY3Nkbi5uZXQvem91eHkwOQ==/font/5a6L5L2T/fontsize/400/fill/I0JBQkFCMA==/dissolve/70/gravity/SouthEast

其中，第一项L(yi,f(xi;w)) 衡量我们的模型（分类或者回归）对第i个样本的预测值f(xi;w)和真实的标签yi之前的误差。因为我们的模型是要拟合我们的训练样本的嘛，所以我们要求这一项最小，也就是要求我们的模型尽量的拟合我们的训练数据。

但正如上面说言，我们不仅要保证训练误差最小，我们更希望我们的模型测试误差小，所以我们需要加上第二项，也就是对参数w的规则化函数Ω(w)去约束我们的模型尽量的简单。

机器学习的大部分带参模型都和这个神似。是的，其实大部分无非就是变换这两项而已。对于第一项Loss函数，如果是Square loss，那就是最小二乘了；如果是Hinge Loss，那就是著名的SVM了；如果是exp-Loss，那就是牛逼的 Boosting了；如果是log-Loss，那就是Logistic Regression了；还有等等。不同的loss函数，具有不同的拟合特性，这个也得就具体问题具体分析的。但这里，我们先不究loss函数的问题，我们把目光转向“规则项Ω(w)”。

规则化函数Ω(w)也有很多种选择，一般是模型复杂度的单调递增函数，模型越复杂，规则化值就越大。比如，规则化项可以是模型参数向量的范数。然而，不同的选择对参数w的约束不同，取得的效果也不同，但我们在论文中常见的都聚集在：零范数、一范数、二范数、迹范数、Frobenius范数和核范数等等。这么多范数，到底它们表达啥意思？具有啥能力？什么时候才能用？什么时候需要用呢？

L0范数是指向量中非0的元素的个数

L1范数是指向量中各个元素绝对值之和，也叫“稀疏规则算子”（Lasso regularization）

L2范数是指向量各元素的平方和然后求平方根

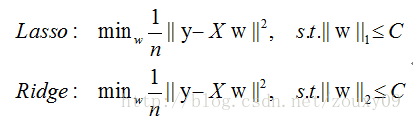
如果我们用L0范数来规则化一个参数矩阵W的话，就是希望W的大部分元素都是0。

为什么L1范数会使权值稀疏？

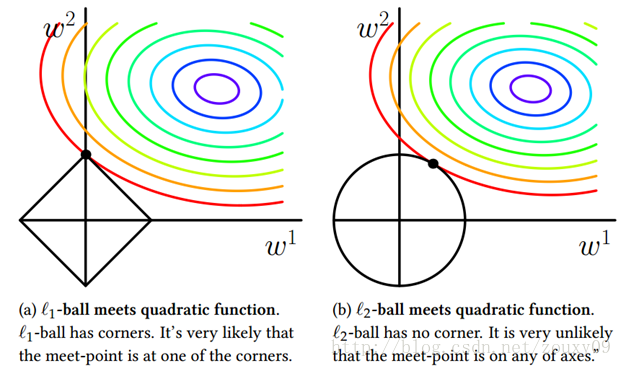
理想的情况是使用L0范数，但L0范数不连续，难以优化求解（NP难问题），而L1范数是L0范数的最优凸近似，且它比L0范数要容易优化求解。

从模型空间的限制角度解释：

L1和L2规则化的代价函数



考虑两维的情况，在(w1, w2)平面上可以画出目标函数的等高线，而约束条件则成为平面上半径为C的一个 norm ball 。等高线与 norm ball 首次相交的地方就是最优解



L1-ball 与L2-ball 的不同就在于L1在和每个坐标轴相交的地方都有“角”出现，而目标函数的测地线除非位置摆得非常好，大部分时候都会在角的地方相交。注意到在角的位置就会产生稀疏性，例如图中的相交点就有w1=0

L2-ball 就没有这样的性质，因为没有角，所以相交的地方出现在具有稀疏性的位置的概率就变得非常小了

让L2范数的规则项||W||2最小，可以使得W的每个元素都很小，都接近于0，但与L1范数不同，它不会让它等于0，而是接近于0

L2正则项的回归叫“岭回归”（Ridge Regression），也称为“权值衰减weight decay”

L1正则项的回归叫LASSO回归

L1会趋向于产生少量的特征，而其他的特征都是0，而L2会选择更多的特征，这些特征都会接近于0。Lasso在特征选择时候非常有用，而Ridge就只是一种规则化而已。

半监督学习

未标记样本虽未直接包含标记信息，但若它们与有标记样本是从同样的数据源独立同分布采样而来，则它们所包含的关于数据分布的信息对建立模型将大有裨益

要利用未标记样本，必然要做一些将未标记样本所揭示的数据分布信息与类别标记相联系的假设。如a. 聚类假设(cluster assumption),即假设数据存在簇结构，同一个簇的样本属于同一个类别；b. 流形假设(manifold assumption), 即假设数据分布在一个流形结构上，邻近的样本拥有相似的输出值。无论聚类假设还是流形假设，其本质都是“相似的样本拥有相似的输出”这个基本假设

直推学习transductive: 假定学习过程中所考虑的未标记样本恰是待预测数据，学习的目的就是在这些未标记样本上获得最优泛化性能

纯半监督学习：假定训练数据中的未标记样本并非待预测的数据

self-training算法:

标签传播算法，它假设距离样本点最近的数据点的标签就是该样本点的标签，需要经过迭代，每次迭代只赋予一个样本点标签。**该算法受离群点和偶然性因素影响太大**，效果不佳。

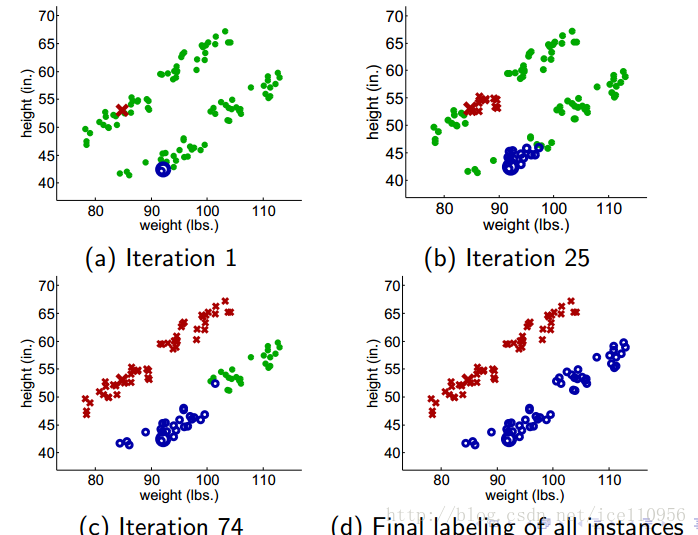
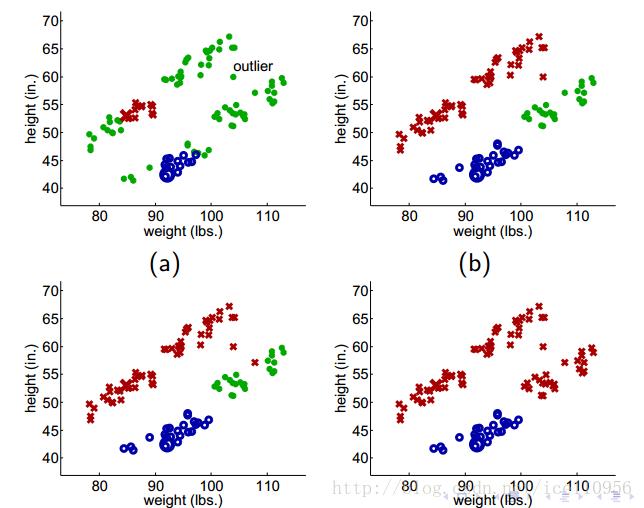
Repeat:

用L（有标记样本集）生成分类策略F;

用F分类U（无标记样本集）,计算误差

选取U的子集u,即误差小的,加入标记.L=L+u;

重复上述步骤,直到U为空集.

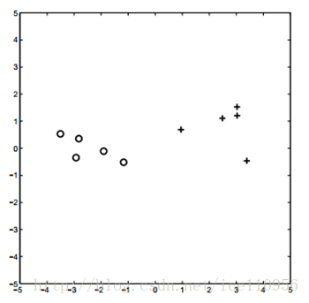
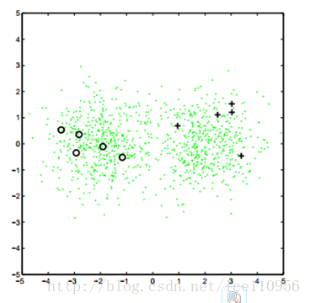
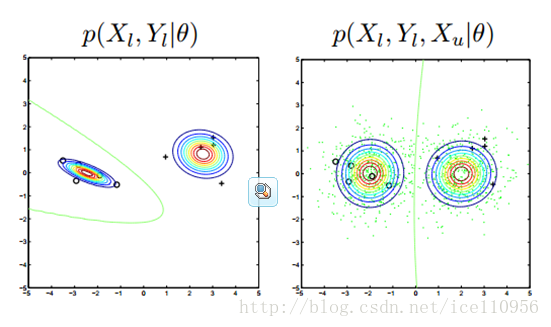
右图有噪声点，导致分类出错

生成式方法

假设所有数据（无论是否有标记）都是由同一个潜在的模型“生成”的

未标记数据与学习目标是通过假设同一个潜在模型的参数联系在一起，未标记数据的标记则可看作模型的缺失参数，通常可基于EM算法进行极大似然估计求解

常用的高斯混合模型(GMM)

右图：前者最大化标记样本出现概率,后者加入了无标记样本出现概率.

基于生成式模型的半监督学习方法简单、直观，并且在训练样本，特别是有标记样本极少时能够取得比判别式模型更好的性能，但是**当模型假设与数据分布不一致时，使用大量的未标记数据来估计模型参数反而会降低学得模型的泛化能力**。由于寻找合适的生成式模型来为数据建模需要大量领域知识，这使得基于生成式模型的半监督学习在实际问题中的应用有限

图半监督学习

数据集 -> 图

做法：数据集中每个样本对应于图中一个结点，若两个样本之间的相似度很高，则对应的结点之间存在一条边，边的强度正比于样本之间的相似度。

将有标记样本所对应的结点染颜色，未标记样本样本所对应的结点尚未染色，于是半监督学习就对应于“颜色”在图上扩散或传播的过程

设计能量函数满足：

1. 标记样本的预测与真实标记尽可能相同
2. 相似样本具有相似标记

图的质量极为重要，常见的有高斯距离图，k近邻图等

半监督SVM 见p299

试图找到能将两类有标记样本分开，且穿过数据低密度区域的划分超平面

典型算法是Transductive SVM: 试图考虑对未标记样本进行各种可能的标记指派label assignment,即尝试将每个未标记样本分别作为正例或反例，然后在所有这些结果中，寻求一个在所有样本（包括有标记样本和进行了所有标记指派的未标记样本）上间隔最大化的划分超平面

如何设计出高效的优化求解策略，此外，训练数据中存在多个”低密度划分“

基于分歧的方法

起源于协同训练co-training，多视图学习multi-view learning的代表

在不少现实应用中，一个数据对象往往同时拥有多个”属性集“，每个属性集构成了一个视图

如对一部分电影来说，它拥有多个属性集：图像画面属性集，声音信息属性信，字幕属性集等

假设数据拥有两个充分且条件独立视图，若两个视图充分具条件独立，则可利用未标记样本通过协同训练将弱分类器的泛化性能提升到任意高

事实上无需数据拥有多视图，仅需弱学习器之间具有显著的分歧（或差异），即可通过相互提供伪标记样本的方式来提升泛化性能（所以叫基于分歧的方法），不同视图、不同算法、不同数据采样、不同参数设置等，都能导致学习器之间的分歧

充分指每个视图都包含足以产生最优学习器的信息

条件独立则是指在给定类别标记条件下两个视图独立

视图的条件独立性在现实任务中通常很难满足，因此性能提升幅度不会那么大。

半监督聚类

约束k均值 constrained k-means

和k均值算法流程相同，只是将样本划分时多一个约束：检测将x划入聚类簇是否会违背”必连“集must-link（指样本必属于同一个簇）与勿连集cannot link（样本必不属于同一个簇）

约束种子k均值constrained seed k-means

用有标记样本初始化簇中心，在聚类簇迭代更新过程中，不改变种子样本的簇隶属关系

# 《数据挖掘导论》

抛开理解数据的人和数据所处的领域而简单地使用数据分析技术是不可行的

数据挖掘技术可以用来支持广泛的商务智能应用，如顾客分析、定向营销、工作流管理、商店分布和欺诈检测等

**数据挖掘**技术用来探查大型数据库，发现先前未知的有用模式，预测未来观测结果

**信息检索**：使用数据库管理系统查找个别的记录，或通过因特网的搜索引擎查找特定的web页面。它们主要依赖传统的计算机科学技术和数据的明显特征来创建索引结构，从而有效地组织和检索信息

输入**数据存储**：可以以各种形式存储如平展文件、电子数据表或关系表，并且可以驻留在集中的数据存储库中，或分布在多个站点上。

**数据预处理**：融合来自多个数据源的数据，清洗数据以消除噪声或重复的观测值，选择与当前数据挖掘任务相关的记录和特征

**可视化**：从各种不同的视角探查数据和数据挖掘结果。在后处理阶段，还能使用统计度量或假设检验，删除虚假的数据挖掘结果

**数据挖掘的难点：**

可伸缩：处理海量数据集，算法必须是可伸缩的。许多数据挖掘算法使用特殊的搜索策略处理指数级搜索问题

高维性：成百上千属性的数据集

异种数据和复杂数据

**数据挖掘与传统统计方法的比较？**

传统的**统计方法**基于一种假设检验模式，即提出一种假设，设计实验来收集数据，然后针对假设分析数据。当前的数据分析任务常常需要产生和评估数千种假设，因此需要自动地产生和评估假设。

数据挖掘所分析的数据集通常不是精心设计的实验的结果，并且它们通常代表数据的时机性样本（opportunistic sample），而不是随机样本(random sample).

数据挖掘来自如下领域思想：1统计学的抽样、估计和假设检验。2人工智能、模式识别和机器学习的搜索算法、建模技术和学习理论。3最优化、进化计算、信息论、信号处理、可视化和信息检索

**数据挖掘任务：**

1预测任务

以说明变量函数的方式为目标变量建立模型，有两类预测建模任务：分类（用于预测离散的目标变量）和回归（用于预测连续的目标变量）。目标都是训练一个模型，使目标变量预测值与实际值之间的误差达到最小。常见的应用：检查结果判断病人是否患有某种疾病。

2描述任务

其目标是导出概括数据中潜在联系的模式（相关、趋势、聚类、轨迹和异常）。本质上，描述性数据挖掘任务通常是探查性的，并且常常需要后处理技术验证和解释结果。

## 数据

### 数据类型

决定我们应使用何种工具和技术来分析数据。

知道属性的类型是重要的，因为它告诉我们测量值的哪些性质与属性的基本性质一致，从而使得我们可以避免诸如计算雇员的平均ID这样的愚蠢行为

不同的属性类型

分类的(定性的)

标称 区分对象(=, ~=) 一对一变换

序数 确定对象的序(>, <) 值的保序变换，即新值=f(旧值)，f是单调函数

数值的（定量的）

区间 值之间的差(+, -) 新值=a\*旧值+b

比率 差和比率(\*, /) 新值=a\*旧值

数据集特性：维度，稀疏性和分辨率（常常可以在不同的分辨率下得到数据，并且在不同的分辨率下数据的性质也不同，即**数据的模式也依赖于分辨率，如果分辨率太高，模式可能看不出，或者掩埋在噪声中；如果分辨率太低，模式可能不出现**）

### 数据质量

如存在噪声和离群点，数据遗漏、不一致或重复，数据有偏差或者不能代表它应该描述的现象或总体情况

数据挖掘常常不能“在数据源头控制质量。相比之下，统计学的实验设计或调查往往其数据质量都达到了一定的要求。由于无法避免数据质量问题，因此数据挖掘着眼于两个方面：1数据质量问题的检测和纠正.2使用可以容忍低质量数据的算法。

测量和数据收集问题

1. 测量误差和数据收集错误
2. 噪声和伪像

噪声通常用于包含时间或空间分量的数据。在这些情况下，常常可以使用信号或图像处理技术降低噪声，从而帮助发现可能”淹没在噪声中“的模式（信号）

**伪像**：数据错误可能是更确定性现象的结果，**即数据的某种确定性失真。如一组照片在同一地方出现条纹**

1. 精度、偏倚和准确率
2. 离群点

在某种意义上具有不同于数据集中其他大部分数据对象的特征的数据对象，或是相对于该属性的典型值来说不寻常的属性值。Outlier可以是合法的数据对象或值。因此不像噪声，离群点本身有时是人们感兴趣的对象

1. 遗漏值

处理遗漏值的策略：

* 删除数据对象或属性
* 估计遗漏值。如果属性是连续的，则可以使用最近邻的平均属性值；如果属性是分类的，则可以取最近邻中最常出现的属性
* 在分析时忽略遗漏值。如果某对的一个对象或两个对象都有某些属性有遗漏值，则可以仅使用没有遗漏值的属性来计算相似性

1. 不一致的值
2. 重复数据

数据集 = 数据对象的集合

数据对象 = {属性：值}

记录数据

数据表病人信息

事务数据如购物蓝信息

数据矩阵如特征空间

文档-词矩阵

序列数据 = 记录数据 + 时间信息（或空间信息）

**时间自相关**：分析时间数据时，如果两个测量的时间很接近，则这些测量的值通常非常相似

**空间自相关**：物理上靠近的对象趋向于在其他方面也相似。如地球上相互靠近的两个点通常具有相近的气温和降水量

### 预处理

原始数据必须加以处理才能适合于分析。如将连续值属性如长度转换成具有离散的分类值的属性如短中长；如数据集属性的数目常常需要减少，因为属性较少时许多技术用起来更加有效

* 聚集

将多个对象合并成单个对象，聚集是删除属性（如商品类型）的过程，或者是压缩特定属性不同值个数的过程

好处：1数据归约导致较小数据集需要较少的内存和处理时间2通过高层而不是低层数据视图，聚集起到了范围或标度转换的作用3对象或属性群的行为通常比单个对象或属性的行为更加稳定

缺点：丢失有趣的细节

* 抽样

统计学使用抽样是因为得到感兴趣的整个数据集的费用太高、太费时间；

数据挖掘使用抽样是因为处理所有的数据的费用太高、太费时间

**有效抽样**：样本是代表性的，前提是它近似地具有与原数据集相同的感兴趣的性质。如果数据对象的均值是感兴趣的性质，而样本具有近似于原数据集的均值，则样本就是有代表性的。我们所能做的最好的抽样方案就是选择一个确保以很高的概率得到有代表性的样本

抽样方法

**无放回抽样和有放回抽样**。当样本与数据集相比相对较小时，两种方法产生的样本差别不大。但是对于分析，有放回抽样较为简单，因为在抽样过程中，每个对象被选中的概率保持不变

**分层抽样**：从预先指定的组开始抽样。在最简单的情况下，尽管抽样的大小不同，但是从每组抽取的对象个数相同。另一种变形是从每一组抽取的对象数量正比于该组的大小。

**渐进抽样（自适应抽样）**：从一个小样本开始，然后增加样本容量直至得到足够容量的样本。尽管这种技术不需要在开始就确定正确的样本容量，但是需要评估样本的方法，确定它是否足够大。尽管预测模型的准确率随样本容量增加，但是在某一点准确率的增加趋于确定

* 维归约

好处：1维归约可以删除不相关的特征并降低噪声，一部分是因为维灾难。2维归约可以使模型更容易理解，因为模型可能只涉及较小的属性3数据也可通过观察属性或对三元组属性达到可视化4使用维归约降低了数据挖掘算法的时间和内存需求

维灾难：随着数据维度的增加，许多数据分析变得非常困难。特别是随着维度增加，数据在它所占据的空间中越来越稀疏。对于分类，这可能意味着没有足够的数据对象来创建模型，将所有可能的对象可靠地指派到一个类。对于聚类，点之间的密度和距离的定义失去了意义

最常用的方法：线性代数技术，将数据由高维空间投影到低维空间。如主成分分析PCA:找出新的属性（主成分），这些属性是原属性的线性组合，是相互正交的，并且捕获了数据的最大变差；如奇异值分解

* 特征子集选择

看起来这种方法可能丢失信息，但是在存在冗余或不相关特征的时候，情况并非如此。冗余特征重复了包含在一个或多个其他属性中的许多或所有信息。不相关特征包含对于手头的数据挖掘任务几乎完全没用的信息。冗余和不相关的特征可能降低分类的准确率，影响所发现的聚类的质量

* 特征创建

特征提取：对数据进行处理，获得一些较高层次的特征。最常使用的特征提取技术都是高度针对具体领域

映射数据到新的空间：使用一种完全不同的视角挖掘数据可能揭示出重要和有趣的特征。如果有大量周期模式，并且存在大量噪声，则很难检测这些模式。尽管如此，通过对该时间序列实施傅里叶变换，将它转换成频率信息明显的表示，就能检测到这些模式

特征构造：使用专家的意见构造特征

* 离散化和二元化

非监督离散化

用于分类的离散化方法之间的根本区别在于使用类信息还是不使用类信息。如果不使用类信息，则常使用一些相对简单的方法，如等宽，等频

监督离散化

如熵entropy,区间的熵是区间纯度的度量。如果一个区间只包含一个类的值（该区间非常纯），则其熵为0并且不影响总熵。如果一个区间中的值类出现的频率相等（该区间心可能不纯），则其熵最大。

* 变量变换

在统计学中，变量变换（特别是平方根、对数和倒数变换）常用来将不具有高斯（正态）分布的数据变换成具有高斯（正态）分布的数据。

使用变量变换时需要小心，因为它们改变了数据的特性。

**标准化或规范化**：目标是使整个值的集合具有特定的性质。统计学中术语规范化可能与使变量正态（高斯）的变换相混淆。对变量标准化是为了避免具有较大值域的变量左右计算结果。均值和标准差受离群点的影响很大，因此通常需要修改，用中位数取代均值，用绝对标准差取代标准差

### 相似性和相异性的度量

邻近度：表示相似性或相异性，由于两个对象之间的邻近度是两个对象对应属性之间的邻近度的函数

相似度：[0, 1]

相异度：>0

相关性：[-1, 1]

如果邻近度度量原来在区间[0, ]上取值，则需要使用非线性变换，d’ = d/(d+1)， 注意logistic函数就是ea/(ea + 1)

任意单调减函数都可以用来将相异度转换到相似度（或相反）

#### 简单属性的相异度

标称属性：

序数属性：

, 值映射到整数0~n-1,其中n是值的个数

区间或比率的属性：

d =|x-y|

数据对象之间的相异度

Minkowski distance, 见page42

#### 记录之间的相似性度量

对称二元属性：简单匹配系数simple Matching Coefficient

SMC = 值匹配的属性个数/属性个数

SMC可以在一个仅包含是非题的测验中用来发现回答问题相似的学生

**非对称二元属性**：Jaccard系数，忽略0-0度量，因为稀疏性大多0

J = 匹配的个数/不涉及0-0匹配的属性个数

多元属性：余弦相似度

余弦相似度实际上是x和y之间夹角（余弦）的度量，如果余弦相似度为1,则x and y之间夹角是0.余弦相似不考虑两个数据对象的量值。

#### 记录之间的相关性度量

Person’s correlation:

连续变量：Corr(x,y) = covariance(x, y) / (standard\_deviation(x) \* standard\_deviation(y))

二元变量：

is defrieved from Pearson’s chi-squared test

如果相关度为0,则两个数据对象的属性之间不存在线性关系。然而仍然可能存在非线性关系。

#### 邻近度计算

若属性不同尺度，但属性之间独立，只需要对变量标准化，然后计算欧几里得距离

若属性不同尺度，且属性之间相关，需要计算Mahalanobis距离

## 数据探索

### 汇总统计

频率：frequency(vi) = 具有属性值vi的对象数/m

众数: 最高频率值

百分位数

位置度量：均值和中位数

**均值对离群值很敏感，对于包含离群值的数据，中位数可以更稳健地提供值集中间的估计**

散布度量：极差和方差 (表明属性值是否散布很宽，或是否相对集中在均值附近

极差：range(x) = max(x)-min(x)

标准差：与均值差平方和除以(m-1) = 方差的平方根

**因为方差用均值计算，因此它也对离群值敏感。**

对于多元数据，数据的散布用协方差矩阵表示。协方差矩阵的对角线上是属性的方差。

两个属性的协方差是两个属性一起变化并依赖于变量大小的度量。协方差的值接近

### 可视化

数据对象、它们的属性，以及数据对象之间的联系要转换成诸如点、线、形状和颜色等图形元素。

1. Stem and leaf plot
2. Histogram
3. 2D historgram
4. Box plot
5. Pie chart
6. Scatter plot

散布图的作用：图形化显示两个属性之间的关系。当类标给出时，可以使用散布图考察两个属性将类分开的程度。

1. Contour plot （等高线图）
2. Surface plot （曲面图）

可视化高维数据

1. 图像
2. 平等坐标系

记录用线表示，每个属性值对应坐标轴上的点

缺点：图中模式的检测可能取决于坐标轴的序

联机分析处理(OLAP)

在不同的维上或不同的属性值上聚集数据

多维数据分析的关键目标是观察聚集量，如总和或平均值

## 分类

### 基本概念

应用场景：根据电子邮件的标题和内容检查出垃圾邮件；根据核磁共振扫描的结果区分肿瘤是恶性的还是良性的？

分类任务的输入数据是样例的集合，用元组(X, y)表示，其中X是属性的集合，y是样例类标号。类桔必须是离散属性。

区别分类与回归？回归也是一种预测建模任务，其中目标属性是连续

分类任务是通过学习得到一个目标函数f,把每个属性集X映射到一个预先定义的类标号y. 目标函数也称为分类模型

分类模型的有两个目的：

描述性建模

分类模型可以作为解释性的工具，用于区分不同类中的对象

预测性建模

分类模型还可以用于预测未知记录的类标号

分类技术非常适合预测或描述二元或标称类型的数据集，对于序数分类（如把人分类为高收入，中等收入或低收入组），分类技术不太有效，因为分类技术不考虑隐含在目标类中的序关系。

分类法：根据输入数据集建立分类模型的系统方法。如**决策树，基于规则，神经网络，支持向量机和贝叶斯**。这些技术都使用学习算法确定分类模型，该模型能很好地拟合输入数据中类标号和属性集之间的联系。学习算法很到的模型不仅要很好地拟合输入数据，还要能够正确地预测未知样本的类标号。

### 决策树

决策树是一种由结点和有向边组成的层次结构

在决策树中，每个**叶结点都赋予一个类标号**。**非终结点（包含根结点和内部结点）包含属性测试条件**，用以分开具有不同特性的记录。

如何建立决策树？

原则上讲，对于给定的属性集，可以构造的决策树的数目达指数级。由于搜索空间是指数规模的，找出最佳决策树在计算上是不可行的。所以算法的目的是能够在合理的时间内构造出具有一定准确率的局部最优决策树

Hunt算法是许多决策树算法的基础，如CART

1. 假定分类问题的初始决策树只有一个结点，因为根结点包含超过一个类的记录，所以需要进一步的细化
2. 根据一个属性测试条件，数据集被划分为较小的子集
3. 对根结点的每个子女递归地调用Hunt算法

核心：

**如何选择一个属性测试条件，作为划分数据的最优标准**？也就是说，算法必须提供为不同类的属性指定测试条件的方法，并且提供评估每种测试条件的客观度量

**选择最佳划分的度量通常是：根据划分后子女结点不纯性的程度。不纯的程度越低，类分布就越倾斜。均衡分布(0.5, 0.5)的结点具有最高的不纯性**

其中t是给定结点t的总数

其中表示给定结点t中属性类i的记录所占的比例

例子：

如何用决策树分类法区分正常的用户访问，还是由Web爬虫产生的访问？

输入数据：Web服务器日志

Web日志记录的字段：包括客户端的IP地址、请求的时间戳、请求访问的文档的网址、文档的大小、客户的身份（通过用户代理字段获得）。

Web会话是客户在一次网站访问期间发出的请求序列，每个Web会话都可以用有向图来建模，其中结点对应于网页，而有向边对应于连接网页的超链。

目标：对Web会话进行分类

特征构建：构造描述每次会话特性的特征，如遍历的深度和宽度…

训练的模型：（作为描述性模型）

* Web机器人的访问倾向于宽而浅，而正常用户访问比较集中（窄而深）
* 与正常用户不同，Web机器人很少访问与Web文档相关的图片页
* Web机器人的会话的长度趋于较长，包含了大量请求页面
* Web机器人更可能对相同的文档发出重复的请求，因为正常用户访问的网页常常会被浏览器保存

决策树归纳的特点：

* 非参数方法，也就是说，它不要求任何先验假设，不假定类和其他属性服从一定的概率分布。
* NP完全问题，一般采用启发式方法指导对假设空间的搜索
* 容易解释
* 对噪声的干扰具有相当好的鲁棒性
* 冗余属性（一个属性在数据中与另一个属性是强相关的）不会对决策树的准确率造成不利的影响。但是**如果数据集中含有很多不相关的属性（即对分类任务没有用的属性），则某些不相关属性可能在树的构造过程中偶然被选中，导致决策树过于庞大。**
* 大多数的决策算法采用自顶向下的递归划分方法，因此沿着树向下，记录会越来越少。**在叶结点，记录可能太少，对于叶结点代表的类，不能做出具有统计意义的判决，这就是所谓的数据碎片问题。**

决策树的物理解释：

可以将决策树的生长过程看成划分属性空间不相交的区域的过程，直到每个区域都只包含同一类的记录。**由于测试条件只涉及单个属性，因此决策边界是直线，即平行于坐标轴，这就限制了决策树对连续属性之间复杂关系建模的表达能力。**

模型存在的一般问题？

过分拟合

决策树过大容易受所谓过分拟合(overfitting)现象的影响。通过修剪初始决策树的分支，剪枝有助于提高决策树的泛化能力。模型越是复杂，出现过分拟合的几率就越高，可以采用**奥卡姆剃刀原则：给定两个具有相同的泛化误差的模型，较简单的模型比较复杂的模型更可取**

过分拟合会导致低训练误差，但高泛化误差。

两种可能：噪声导致的过分拟合，缺乏代表性样本导致的过分拟合

如何解决？

先剪枝（提前终止规则）：当观察到的不纯性度量的增益（或估计的**泛化误差的改进**）低于某个确定的阈值时就停止扩展叶结点。然而很难为提前终止选取正确的阈值，阈值太高将导致拟合不足，阈值太低就不能充分解决过分拟合的问题

后剪枝（常用方法）：初始决策树按照最大规模生长，然后自底向上的方式修剪完全增长的决策树。1)用新的叶结点替换子树，该叶结点的类标号由子树下记录中的多数类确定；2）用子树中最常使用的分支代替子树。

拟合不足

决策树过小会导致高训练误差和高泛化误差。因为模型尚未学习到数据的真实结构。

分类器性能的评估

在检验集上评估模型的性能。

1. Holdout方法

数据集 = 训练集 + 测试集

训练集越小，模型的方差越大；若训练集太大，较小的检验集估计的准确率不太可靠

1. 交叉验证法

K折交叉验证 （若k=2, 则二折交叉；k=10 常见；若k=N，则留一法）

误差为K个检测集的误差总和

### 貝叶期分类器

在很多应用中，**属性集和类变量之间的关系是不确定的。換句话说，尽管测试记录的属性集和某些训练样例相同，但是也不能正确地预测它的类标号**。Bayes是对属性集和类变量的概率关系建模的方法

若X表示属性集，Y表示类变量， 若类变量和属性之间的关系不确定，**可以把X和Y看作随机变量**

若假定测试记录有属性集：X=（有房＝否，婚姻状况＝已婚，年收入＝$120k)，预测该记录属于拖欠贷款 YES or 还清贷款NO

即求P(YES|X) and P(NO|X)

P(Y|X) = P(X|Y)\*P(Y) / P(X)

因为先验概率P(Y) and P(X)是常数

所以argmaxP(Y|X) = argmaxP(X|Y)

朴素Bayes分类器：假定属性之间相互独立，则

P(X|Y) = P(x1|Y) \* P(x2|Y) \* … \* P(xd|Y) 假定d个属性

argmaxP(No|X) = argmaxP(X|No) = argmax(

p(有房＝否|No) \* p(婚姻状况＝已婚 | No) \* p(年收入＝$120k|No) )

若属性是分类的：P(xi|Y): 类y中等于xi的训练实例的比例

若属性是连续的：假设连续变量服从某种概率分布，然后使用训练数据估计分布的参数。高斯分布通常被用来表示连续属性的类条件概率分布。该分布有两个参数：mean and std.

P(xi|Y) = exp(-(xi-mean)\*(xi-mean)/(2\*std\*std) / (sqrt(2pi)\*std)

mean: 类yi所有训练记录关于Xi的样本均值

std: 类yi所有训练记录关于Xi的样本标准差

计算结果若P(No|X) > P(Yes|X), 则估计为还清贷款

Bayes特点：

1. 面对孤立的噪声点，朴素Bayes分类器是健壮的。因为在从数据中估计条件概率时，这些点被平均。
2. 若Xi是无关属性，那么P(Xi|Y)几乎变成了均匀分布，不会对总的估计产生影响
3. 相关属性会降低朴素Bayes分类器的性能

基于规则分类器

### KNN

### ANN

### SVM

### Emsemble组合方法

Bagging(装袋)

Adaboost

random forest

随机森林是一类专门为决策树分类器设计的组合方法，它**组合多棵决策树**作出的预测，其中每棵树都是基于随机向量的一个独立集合的值产生的。与AdaBoost使用的自适应方法不同，AdaBoost中概率分布是变化的，以关注难分类的样本，而随机森林则采用一个固定的概率分布来产生随机向量。

## 不平衡类问题

稀有类的正确分类比多数类的正确分类更有价值。准确率经常用来比较分类器的性能，然而它可能不适合评价从不平衡数据集得到的模型。

检测稀有类的实例好比大海捞针。因为这些实例很少出现，因此描述稀有类的模型趋向于高度特殊性。例如，在基于规则的分类器中，为稀有类提取的规则通常涉及大量的属性，并很难简化为更一般的，具有很高覆盖率的规则。这样的模型很容易受训练数据中噪声的影响。

对于二元分类，稀有类通常记为正类，而多数类被认为是负类。

不平衡类一般用precesion, recall, and F1

ROC曲线：显示分类器真正率和假正率之间折中的一种图形化方法。ROC曲线中，真正率沿y轴，假正率沿x轴上，沿着曲线每个点对应于一个分类器

如何解决不平衡类问题？

1. 代价敏感学习

将一个类错分另一个类的代价是不一样的，可以用代价矩阵表达将一个类的记录分类到另一个类的惩罚进行编码　C = [c(i, j)]，

|  |  |  |  |
| --- | --- | --- | --- |
|  | | 预测的类 | |
| 类=+ | 类=- |
| 实际的类 | 类=+ | -1 | 100 |
| 类=- | 1 | 0 |

可以证明　：在0/1代价矩阵中，总代价等于误分类的数目

C = TP\*c(+,+) + FP\*c(-, +) + FN\*c(+,-) + TN\*c(-,-)

　= TP\*0 + FP\*1 + FN\*1 + TN\*0

= FP + FN = N\*Err

医学上，宁可误判为恶性，但不可漏了一个恶性，也就是说假阴性代价远高于假阳性，对应代价矩阵中c(+, -)=100 > c(-, +)=1

如何将代价信息引入分类算法中？

以决策树归纳为例，代价信息修改每个叶结点上的决策规则。

典型的二元分类，若误分代价相同，则将正类批派到结点t

p(+|t) > p(-|t)

=> p(+|t) > 1-p(+|t)

=> p(+|t) > 0.5

从而表明，叶结点的类标号取决于到达该结点的训练记录的多数类

若引入代价信息

C(i|t) = sum( p(j|t)\*c(j, i) ) j=类别

若两类

c(+|t) = p(+|t)\*c(+, +) + p(-|t)\*c(-, +) > c(- |t) = p(+|t)\*c(+, 1) + p(-|t)\*c(-, -)

=> p(+|t) > [c(-,-) - c(-,+)]/[c(+,+) + c(-,-) - c(-,+) - c(+,-)]

1. 基于抽样的方法

降采样：　对多的某类样本执行降采样，从而生成基分类器，多次如此，从而生成多分类器，然后**组合多分类器**

上采样：对少的某类样本执行上采样，如在少样本集中，对某个数据的k近邻，随机生成新的样本。

**上采样缺点：对于噪声数据，上采样可能导致模型过分拟合，因为一些噪声样本也可能被复制多次**。原则上，上采样没有向训练集中添加任何新的信息

## 多类问题解决方法？

分解成K个二类问题(yi, yj+ym+...)，也称为1-r方法　（容易产生不平衡类）

分解成K(k-1)/2个二类问题(yi, yj)，也称为1-1方法

　（当为类(yi, yj)构建分类器，不属于yi or yj的样本忽略）

最终通过组合所有二元分类器的预测对检验实例分类。组合预测的典型做法是使用投票表决，将检验样本指派到得票最多的类

纠错输出编码error-correcting output coding, ECOC

受信息理论中通过噪声信道发送信息的启发。其基本思想是借助于代码字向传输信息中增加一些冗余，从而使得接收方能发现接收信息中的一些错误，而且如果错误量很少，还可能恢复原始信息。

**对于多类学习，每个类yi用一个长度为n的唯一位串来表示，称为它的代码字**。然后训练n个二元分类器，预测代码字串的每个二进位。检验实例的预测类由这样的代码字给出，该代码字到二元分类器产生的代码字海明距离最近。（两个位串之间的海明距离是它们的不同的二进位的数目）

关键是：如何为不同的类设计合适的代码字集合？

对于通信任务，代码字应该最大化各行之间的海明距离，使得纠错可以进行。

对于多类学习要求，将代码字列向和行向的距离很好地分开。较大的列向距离可以确保二元分类器是相互独立的。

|  |  |
| --- | --- |
| 类 | 代码字 |
| y1 | 1 1 1 1 1 |
| y2 | 0 0 0 1 1 |
| y3 | 1 1 1 0 0 |

文献：稀有类，不平衡数据集，代价敏感学习，多类学习

## 关联分析

用来发现描述数据中**强关联特征的模式**。由于搜索空间是指数规模的，关联分析的目标是以有效的方式提取最有趣的模式。常见的应用：具体有相关功能的基因组、识别用户一起访问的web页面、理解地球气候系统不同元素之间的联系等

## 聚类

发现紧密相关的观测值结果。常见应用：对相关的顾客分组、找出显著影响地球气候的海洋区域以及压缩数据等。

**聚类分析只是解决其他问题（如数据汇总）的起点**。聚类分析 仅根据在数据中发现的描述对象及其关系的信息，将数据对象分组。其目标是，组内相似性越大，组间差别越大

人类擅长将对象划分成组（聚类），并将特定的对象指派到这些组（分类），聚类分析 是研究自动发现这些类的技术

聚类分析提供由个别数据到数据对象所指派的族的抽象。聚类技术使用**族原型（即代表簇中其他对象的数据对象）**来刻画簇特征

族原型的使用：

汇总：许多数据分析技术如回归和PCA，可以将算法用于仅包含族原型的数据集，而不是整个数据集。依赖分析类型，原型个数和原型代表数据的精度，汇总结果可以与使用所有数据得到的结果相媲美

有效地发现最近邻：找出最近邻可能需要计算所有点对点之间的距离。通常，可以更有效地发现簇和族原型。如果对象相对地靠近族的原型，则我们可以使用族原型减少发现对象最近邻所需要计算的距离的数目。为了找出一个对象的最近邻，只需要计算到邻近族中对象的距离

聚类类型：

* 划分与层次

划分聚类partitional clustering:简单地将数据对象集划分成不重叠的子集（簇），使得每个数据对象恰在一个子集中。

层次聚类hierarchical clustering

* 互斥，重叠与模糊的

模糊聚类：每个点属于每个簇的概率，点的隶属概率之和为1

* 完全的与部分的

族类型：

* 基于原型的

族是对象的集合，其中每个对象到定义刻簇的原型的距离比到其他族的原型的距离更近。对**于具有连续属性的数据，簇的原型通常是质心；**

**对于具有分类属性的数据，簇的原型通常是中心点，即簇中最有代表性的点**

通常把基于原型的簇看作基于中心的簇，这种簇趋向于呈球状

* 基于图的

若数据用图表示，其中结点是对象，而边代表对象之间的联系。则簇可以定义为连通分支，如基于邻近的簇：两个对象相连仅当它们的距离在指定的范围之内。缺点：容易受噪声干扰

* 基于密度的

优点：当族不规则或互相盘绕，并且有噪声和离群点时，常常使用密度的簇定义

* 概念簇：

把簇定义为有某种共同性质的对象的集合。

K均值算法：

随机选择K个点作为初始质心

repeat

将每个点指派到最近的质心，形成K个簇

重新计算每个簇的质心

until 质心不发生变化

指派点到最近的质心？

需要邻近性度量，通过欧氏空间中的点使用欧几里得距离，对文档用余弦相似性。

聚类目标？

通常用一个目标函数表示，该函数依赖于点到簇质心的邻近性，如最小化每个点到最近质心的距离平方和

K均值：常见的邻近度，质心和目标函数组合

|  |  |  |
| --- | --- | --- |
| 邻近度函数 | 质心 | 目标函数 |
| 曼哈顿距离 | 中位数 | 最小化对象到其簇质心的L1距离和 |
| 平方欧几里得距离 | 均值 | 最小化距离平方和 |
| 余弦 | 均值 | 最小化余弦相似度和 |
| Bregman散度 | 均值 | 最小化Bregman散度和 |

余弦相似度或平方欧几里得距离是Bregman散度的特例

使用平方误差标准时，离群点可能过度影响所发现的簇，如何识别离群点？

记录每个点对SSE （sum of the squared error)的影响，删除那些具有异乎寻常影响的点，还可能需要删除很小的簇，因为它们常常代表离群点的组。

**K均值缺陷：**

**当簇具有非球形形状，或具有不同尺寸，或具不同密度时，K均值很难检测到“自然的”的簇。因为K均值目标函数是最小化等尺寸和等密度的球形簇，或者明显分离的簇。**

凝聚层次聚类算法：

计算邻近度矩阵

repeat

合并最接近的两人个簇

更新邻近性矩阵，以反映新的簇与原来的簇之间的邻近性

until仅剩下一个簇

簇之间的邻近性：

MIN：不同的结点子集中两人个结点之间的最短边

MAX: 不同的结点子集中两人个结点之间的最长边

组平均：取自不同簇的所有点对邻近度的平均值

层次聚类的空间复杂度O(m\*m),时间复杂度O(m\*m\*log(m))

## 异常检测

识别其特征显著不同于其他数据的观测值。常见应用：检测欺诈、网络攻击、疾病的不寻常模式、生态系统扰动等。