第3章

机器学习基础知识

3.1 模型评估与模型参数选择

如何评估一些训练好的模型并从中选择最优的模型参数？对于给定的输入 $\boldsymbol{x}$，若某个模型的输出 $\hat{\boldsymbol{y}}=\boldsymbol{f}(\boldsymbol{x})$ 偏离真实目标值 $\boldsymbol{y}$，则说明模型存在**误差**；$\hat{\boldsymbol{y}}$ 偏离 $\boldsymbol{y}$ 的程度可以用关于 $\hat{\boldsymbol{y}}$ 和 $\boldsymbol{y}$ 的某个函数 $L(\boldsymbol{y},\hat{\boldsymbol{y}})$ 来表示，作为误差的度量标准：这样的函数 $L(\boldsymbol{y},\hat{\boldsymbol{y}})$ 称为损失函数。

在某种损失函数度量下，训练集上的平均误差称为**训练误差**，测试集上的误差称为**泛化误差**。由于训练得到一个模型最终的目的是为了在未知的数据上得到尽可能准确的结果，因此泛化误差是衡量一个模型泛化能力的重要标准。

之所以不能把训练误差作为模型参数选择的标准，是因为训练集可能存在以下问题。

(1) 训练集样本太少，缺乏代表性。

(2) 训练集中本身存在错误的样本，即**噪声**。

如果片面地追求训练误差的最小化，就会导致模型参数复杂度增加，使得模型**过拟合**(overfitting)，如图 3.1 所示。

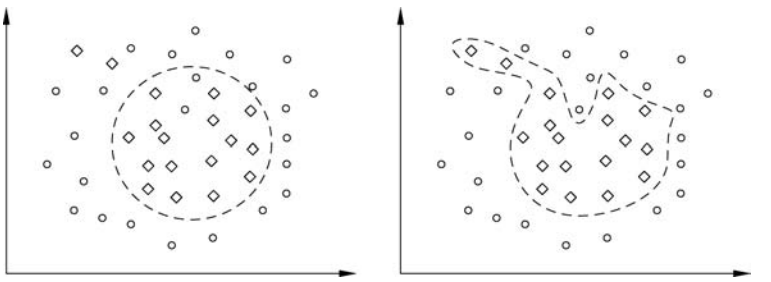

图 3.1 拟合与过拟合

为了选择效果最佳的模型，防止出现过拟合的问题，通常可以采取的方法有使用验证集调参和对损失函数进行正则化两种方法。

3.1.1 验证

模型不能过拟合于训练集，否则将不能在测试集上得到最优结果；但是否能直接以测试集上的表现来选择模型参数呢？答案是否定的。因为这样的模型参数将会是针对某个特定测试集的，那么得出来的评价标准将会失去其公平性，失去了与其他同类或不同类模型相比较的意义。

这就好比要证明某一个学生学习某门课程的能力比别人强（模型算法的有效性），那么就要让他和其他学生听一样的课、做一样的练习（相同的训练集），然后以这些学生没做过的题目来考核他们（测试集与训练集不能交叉）；但是如果直接在测试集上调参，就相当于让这个学生针对考试题目来复习，这样与其他学生的比较显然是不公平的。

因此参数的选择（即**调参**）必须在一个独立于训练集和测试集的数据集上进行，这样的用于模型调参的数据集被称为**开发集**或**验证集**。

然而很多时候能得到的数据量非常有限。这个时候可以不显式地使用验证集，而是重复使用训练集和测试集，这种方法称为**交叉验证**。常用的交叉验证方法有以下两种。

（1）简单交叉验证，即在训练集上使用不同超参数训练，使用测试集选出最佳的一组超参数设置。

（2）K-重交叉验证（K-fold cross validation），即将数据集划分成 K 等份，每次使用其中一份作为测试集，剩余的为训练集；如此进行 K 次之后，选择最佳的模型。

3.1.2 正则化

为了避免过拟合，需要选择参数复杂度最小的模型。这是因为，如果有两个效果相同的模型，而它们的参数复杂度不相同，那么冗余的复杂度一定是由于过拟合导致的。为了选择复杂度较小的模型，一种策略是在优化目标中加入**正则化项**，以惩罚冗余的复杂度：

$$\min_{\theta} L(\boldsymbol{y},\hat{\boldsymbol{y}};\boldsymbol{\theta})+\lambda \cdot J(\boldsymbol{\theta})$$

其中，$\boldsymbol{\theta}$ 为模型参数；$L(\boldsymbol{y},\hat{\boldsymbol{y}};\boldsymbol{\theta})$为原来的损失函数；$J(\boldsymbol{\theta})$是正则化项；$\lambda$ 用于调整正则化项的权重。正则化项通常为 $\boldsymbol{\theta}$ 的某阶向量范数。

3.2 监督学习与非监督学习

模型与最优化算法的选择，很大程度上取决于能得到什么样的数据。如果数据集中样本点只包含模型的输入 $\boldsymbol{x}$，那么就需要采用非监督学习的算法；如果这些样本点以$\langle \boldsymbol{x},\boldsymbol{y}\rangle$的输入-输出二元组的形式出现，那么就可以采用监督学习的算法。

3.2.1　监督学习

在监督学习中，根据训练集$\{\langle \boldsymbol{x}^{(i)}, \boldsymbol{y}^{(i)} \rangle\}_{i=1}^{N}$中的观测样本点来优化模型$\boldsymbol{f}(\cdot)$，使得给定测试样例$\boldsymbol{x}'$作为模型输入，其输出$\hat{\boldsymbol{y}}$尽可能接近正确输出$\boldsymbol{y}'$。

监督学习算法主要适用于两大类问题：回归和分类。这两类问题的区别在于：回归问题的输出是连续值，而分类问题的输出是离散值。

1. 回归

回归问题在生活中非常常见，其最简单的形式是一个连续函数的拟合。如果一个购物网站想要计算出其在某个时期的预期收益，研究人员会将相关因素如广告投放量、网站流量、优惠力度等纳入自变量，根据现有数据拟合函数，得到在未来某一时刻的预测值。

回归问题中通常使用均方损失函数来作为度量模型效果的指标，最简单的求解例子是最小二乘法。

2. 分类

分类问题也是生活中非常常见的一类问题，例如，需要从金融市场的交易记录中分类出正常的交易记录以及潜在的恶意交易。

度量分类问题的指标通常为**准确率**(accuracy)：对于测试集中的D个样本，有k个被正确分类，$D-k$个被错误分类，则准确率为

$$\text{accuracy}=\frac{k}{D}$$

然而在一些特殊的分类问题中，属于各类的样本并不是均一分布，甚至其出现概率相差很多个数量级，这种分类问题称为**不平衡类问题**。在不平衡类问题中，准确率并没有多大意义。例如，检测一批产品是否为次品时，若次品出现的概率为1%，那么即使某个模型完全不能识别次品，只要每次都“蒙”这件产品不是次品，仍然能够达到99%的准确率。显然我们需要一些别的指标。

通常在不平衡类问题中，使用***F*-度量**来作为评价模型的指标。以二元不平衡分类问题为例，这种分类问题往往是异常检测，模型的好坏往往取决于能否很好地检出异常，同时尽可能不误报异常。如果定义占样本少数的类为**正类**(positive class)，占样本多数的类为**负类**(negative class)，那么预测只可能出现以下4种状况。

(1) 将正类样本预测为正类(true positive，TP)。

(2) 将负类样本预测为正类(false positive，FP)。

(3) 将正类样本预测为负类(false negative，FN)。

(4) 将负类样本预测为负类(true negative，TN)。

定义**召回率**(recall)：

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

召回率度量了在所有的正类样本中，模型正确检出的比率，因此也称为**查全率**。

定义**精确率**(precision)：

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

精确率度量了在所有被模型预测为正类的样本中，正确预测的比率，因此也称为**查准率**。

F-度量则是在召回率与精确率之间去调和平均数；有时候在实际问题上，若更加看重其中某一个度量，还可以给它加上一个权值 α，称为 F_α-度量：

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

特殊地，当 $\alpha=1$ 时：

$$F_1=\frac{2RP}{R+P}$$

可以看到，如果模型“不够警觉”，没有检测出一些正类样本，那么召回率就会受损；而如果模型倾向于“滥杀无辜”，那么精确率就会下降。因此较高的 F-度量意味着模型倾向于“不冤枉一个好人，也不放过一个坏人”，是一个较为适合不平衡类问题的指标。

可用于分类问题的模型很多，例如，Logistic 回归分类器、决策树、支持向量机、感知器、神经网络，等等。

3.2.2 非监督学习

在非监督学习中，数据集 $\{\boldsymbol{x}^{(i)}\}_{i=1}^{N}$ 中只有模型的输入，而并不提供正确的输出 $\boldsymbol{y}^{(i)}$ 作为监督信号。

非监督学习通常用于这样的分类问题：给定一些样本的特征值，而不给出它们正确的分类，也不给出所有可能的类别；而是通过学习确定这些样本可以分为哪些类别、它们各自都属于哪一类。这一类问题称为**聚类**。

非监督学习得到的模型的效果应该使用何种指标来衡量呢？由于通常没有正确的输出 $\boldsymbol{y}$，可采取一些其他办法来度量其模型效果。

(1) 直观检测，这是一种非量化的方法。例如，对文本的主体进行聚类，可以在直观上判断属于同一个类的文本是否具有某个共同的主题，这样的分类是否有明显的语义上的共同点。由于这种评价非常主观，通常不采用。

(2) 基于任务的评价。如果聚类得到的模型被用于某个特定的任务，可以维持该任务中其他的设定不变，而使用不同的聚类模型，通过某种指标度量该任务的最终结果来间接判断聚类模型的优劣。

(3) 人工标注测试集。有时候采用非监督学习的原因是人工标注成本过高，导致标注数据缺乏，只能使用无标注数据来训练。在这种情况下，可以人工标注少量的数据作为测试集，用于建立量化的评价指标。

第4章

TensorFlow深度学习基础

在介绍 TensorFlow 之前，读者需要先了解 Numpy。Numpy 是一种用于科学计算的框架，它提供了一个 N 维矩阵对象 ndarray，初始化、计算 ndarray 的函数，以及变换 ndarray 形状和组合拆分 ndarray 的函数。

TensorFlow 的 Tensor 与 Numpy 的 ndarray 十分类似，但是 Tensor 具备两个而 ndarray 不具备、对于深度学习来说非常重要的功能：一是 Tensor 能用 GPU 计算。GPU 根据芯片性能的不同，在进行矩阵运算时，能比 CPU 快几十倍；二是 Tensor 在计算时能够作为节点自动加入计算图中，而计算图可以为其中的每个节点自动计算微分。下面，我们首先介绍 Tensor 对象及其运算。后文给出的代码都依赖于以下两个模块。

```
1 import tensorflow as tf
2 import numpy as np
```

4.1 Tensor 对象及其运算

Tensor 对象是一个维度任意的矩阵，但 Tensor 中所有元素的数据类型必须一致。TensorFlow 包含的数据类型与普通编程语言的数据类型类似，包含浮点型、有符号整型和无符号整型，这些类型既可以定义在 CPU 上，也可以定义在 GPU 上。在使用 Tensor 数据类型时，可通过 dtype 属性指定数据类型，通过 device 指定设备(CPU 或者 GPU)。Tensor 分为常量和变量，区别在于变量可以在计算图中重新被赋值。

```
1 # tf.Tensor
2 print('tf.Tensor 默认为:{}'.format(tf.constant(1).dtype))
```

```
 3
 4 # 可以用 list 构建
 5 a = tf.constant([[1, 2], [3, 4]], dtype = tf.float64)
 6 # 可以用 ndarray 构建
 7 b = tf.constant(np.array([[1, 2], [3, 4]]), dtype = tf.uint8)
 8 print(a)
 9 print(b)
10
11 # 通过 device 指定设备
12 with tf.device('/gpu:0'):
13     c = tf.ones((2, 2))
14     print(c, c.device)
>>> tf.Tensor 默认为:< dtype: 'int32'>
>>> tf.Tensor(
    [[1. 2.]
     [3. 4.]], shape = (2, 2), dtype = float64)
>>> tf.Tensor(
    [[1 2]
     [3 4]], shape = (2, 2), dtype = uint8)
>>> tf.Tensor(
    [[1. 1.]
     [1. 1.]], shape = (2, 2), dtype = float32) /job:localhost/replica:0/task:0/device:GPU:0
```

通过 device 指定在 GPU 上定义变量后，可在终端通过 nvidia-smi 命令查看显存占用。

对 Tensor 执行算术运算符的运算时，是两个矩阵对应元素的运算。tf. matmul()函数执行矩阵乘法计算的代码如下：

```
1 a = tf.constant([[1, 2], [3, 4]])
2 b = tf.constant([[1, 2], [3, 4]])
3 c = a * b
4 print("逐元素相乘:", c)
5 c = tf.matmul(a, b)
6 print("矩阵乘法:", c)
>>> 逐元素相乘: tf.Tensor(
    [[ 1 4]
     [ 9 16]], shape = (2, 2), dtype = int32)
>>> 矩阵乘法: tf.Tensor(
    [[ 7 10]
     [15 22]], shape = (2, 2), dtype = int32)
```

此外，还有一些具有特定功能的函数，如 tf. clip_by_value()函数起的是分段函数的作用，可用于去掉矩阵中过小或者过大的元素；tf. round()函数可以将小数部分化整；tf. tanh()函数用来计算双曲正切函数，该函数可以将数值映射到(0,1)。其代码如下：

```
1 a = tf.constant([[1, 2], [3, 4]])
2 tf.clip_by_value(a, clip_value_min = 2, clip_value_max = 3)
```

```
3 a = tf.constant([-2.1, 0.5, 0.501, 0.99])
4 tf.round(a)
5 a = tf.constant([-3, -2, -1, -0.5, 0, 0.5, 1, 2, 3])
6 tf.tanh(a)
>>> tf.Tensor([[2 2]
    [3 3]], shape=(2, 2), dtype=int32)
>>> tf.Tensor([-2. 0. 1. 1.], shape=(4,), dtype=float32)
>>> tf.Tensor(
    [-0.9950547  -0.9640276  -0.7615942
     -0.46211717  0.          0.46211717
      0.7615942   0.9640276   0.9950547 ], shape=(9,),
dtype=float32)
```

除了直接从 ndarray 或 list 类型的数据中创建 Tensor 外，TensorFlow 还提供了一些函数可直接创建数据(这类函数往往需要提供矩阵的维度)。tf.range()函数与 Python 内置的 range()函数的使用方法基本相同，其第 3 个参数是步长。tf.linspace()函数第 3 个参数指定返回的个数，tf.ones()函数返回全 1 矩阵、tf.zeros()函数返回全 0 矩阵。其代码如下：

```
1 print(tf.range(5))
2 print(tf.range(1, 5, 2))
3 print(tf.linspace(0, 5, 10))
4 print(tf.ones((3, 3)))
5 print(tf.zeros((3, 3)))
>>> tf.Tensor([0 1 2 3 4], shape=(5,), dtype=int32)
>>> tf.Tensor([1 3], shape=(2,), dtype=int32)
>>> tf.Tensor(
    [0.          0.55555556 1.11111111 1.66666667 2.22222222 2.77777778
     3.33333333 3.88888889 4.44444444 5.         ], shape=(10,), dtype=float64)
>>> tf.Tensor(
    [[1. 1. 1.]
     [1. 1. 1.]
     [1. 1. 1.]], shape=(3, 3), dtype=float32)
>>> tf.Tensor(
    [[0. 0. 0.]
     [0. 0. 0.]
     [0. 0. 0.]], shape=(3, 3), dtype=float32)
```

tf.random.uniform()函数返回[0,1]均匀分布采样的元素所组成的矩阵，tf.random.normal()函数返回从正态分布采样的元素所组成的矩阵。tf.random.uniform()函数还可以加参数，返回指定区间均匀分布采样的随机整数所生成的矩阵。其代码如下：

```
1 tf.random.uniform((3, 3))
>>> <tf.Tensor: shape=(3, 3), dtype=float32, numpy=
    array([[0.41092885, 0.76087844, 0.75520504],
           [0.57500243, 0.7695035 , 0.11660695],
           [0.9336704 , 0.44821036, 0.8459077 ]], dtype=float32)>
1 tf.random.normal((3, 3))
>>> <tf.Tensor: shape=(3, 3), dtype=float32, numpy=
    array([[ 0.40765482, 0.63089305, -0.04709337],
```

```
            [ -0.46935162, -0.18415603, 0.18200386],
            [ 0.17893875, -1.2706778 , 0.69634026]], dtype=float32)>
1 tf.random.uniform((3, 3), 0, 9, dtype=tf.int32)
>>> <tf.Tensor: shape=(3, 3), dtype=int32, numpy=
    array([[5, 1, 7],
           [2, 2, 2],
           [1, 6, 3]])>
```

4.2 Tensor 的索引和切片

Tensor 不仅支持基本的索引和切片操作，还支持 ndarray 中的高级索引（整数索引和布尔索引）操作。其代码如下：

```
 1 a = tf.reshape(tf.range(9), (3, 3))
 2 # 基本索引
 3 print(a[2, 2])
 4
 5 # 切片
 6 print(a[1:, :-1])
 7
 8 # 带步长的切片
 9 print(a[::2])
10
11 # 布尔索引
12 index = a>4
13 print(index)
14 print(a[index])
>>> <tf.Tensor: shape=(), dtype=int32, numpy=8>
>>> <tf.Tensor: shape=(2, 2), dtype=int32, numpy=
    array([[3, 4],
           [6, 7]])>
>>> <tf.Tensor: shape=(2, 3), dtype=int32, numpy=
    array([[0, 1, 2],
           [6, 7, 8]])>
>>> tf.Tensor(
    [[False False False]
     [False False True]
     [ True True True]], shape=(3, 3), dtype=bool)
>>> tf.Tensor([5 6 7 8], shape=(4,), dtype=int32)
```

tf.where(condition, x, y)判断 condition 的条件是否满足，当某个元素满足时，就返回对应矩阵 x 相同位置的元素，否则返回矩阵 y 的元素。其代码如下：

```
1 x = tf.random.normal((3, 2))
2 y = tf.ones((3, 2))
```

```
3 print(x)
4 print(tf.where(x > 0, x, y))
>>> tf.Tensor(
    [[ - 0.28848228   - 0.80543387]
     [   0.31449378     1.434097 ]
     [ - 1.1104414      0.69934136]], shape = (3, 2), dtype = float32)
>>> tf.Tensor(
    [[1.          1.          ]
     [0.31449378  1.434097    ]
     [1.          0.69934136]], shape = (3, 2), dtype = float32)
```

4.3 Tensor 的变换、拼接和拆分

TensorFlow 提供了大量对 Tensor 进行操作的函数，这些函数内部使用指针实现对矩阵的形状变换、拼接和拆分等操作，使得大家无须关心 Tensor 在内存的物理结构或者管理指针就可以方便快速地执行这些操作。

属性 Tensor.shape()函数和 Tensor.get_shape()函数可以查看 Tensor 的维度，tf.size()函数可以查看矩阵的元素个数。Tensor.reshape()函数可以用于修改 Tensor 的维度。其代码如下：

```
1 a = tf.random.normal((1, 2, 3, 4, 5))
2 print("元素个数:", tf.size(a))
3 print("矩阵维度:", a.shape, a.get_shape())
4 b = tf.reshape(a, (2 * 3, 4 * 5))
5 print(b.shape)
>>> 元素个数: tf.Tensor(120, shape = (), dtype = int32)
>>> 矩阵维度: (1, 2, 3, 4, 5) (1, 2, 3, 4, 5)
>>> (6, 20)
```

tf.squeeze()函数和 tf.unsqueeze()函数用于给 Tensor 去掉和添加轴。tf.squeeze()函数可以去掉维度为 1 的轴，而 tf.unsqueeze()函数用于给 Tensor 的指定位置添加一个维度为 1 的轴。其代码如下：

```
1 b = tf.squeeze(a)
2 b.shape
>>> TensorShape([2, 3, 4, 5])
1 tf.expand_dims(a, 0).shape
>>> TensorShape([1, 1, 2, 3, 4, 5])
```

tf.transpose()函数用于 Tensor 的转置，perm 参数用来指定转置的维度。

```
1 a = tf.constant([[2]])
2 b = tf.constant([[2, 3]])
3 print(tf.transpose(a, [1, 0]))
4 print(tf.transpose(b, [1, 0]))
>>> tf.Tensor([[2]], shape = (1, 1), dtype = int32)
```

```
>>> tf.Tensor(
    [[2]
     [3]], shape = (2, 1), dtype = int32)
```

TesnsorFlow 提供的 tf. concat()函数和 tf. stack()函数用于拼接矩阵，区别在于：tf. concat()函数在已有的轴 axis 上拼接矩阵，给定轴的维度可以不同，而其他轴的维度必须相同。tf. stack()函数在新的轴上拼接，同时它要求被拼接矩阵的所有维度都相同。下面的代码可以很清楚地表明它们的使用方式和区别。

```
1 a = tf.random.normal((2, 3))
2 b = tf.random.normal((3, 3))
3
4 c = tf.concat((a, b), axis = 0)
5 d = tf.concat((b, b, b), axis = 1)
6
7 print(c.shape)
8 print(d.shape)
>>> (5, 3)
>>> (3, 9)
1 c = tf.stack((b, b), axis = 1)
2 d = tf.stack((b, b), axis = 0)
3 print(c.shape)
4 print(d.shape)
>>> (3, 2, 3)
>>> (2, 3, 3)
```

除了拼接矩阵外，TensorFlow 还提供了 tf. split()函数并将其用于拆分矩阵。其代码如下：

```
1 a = tf.random.normal((10,3))
2 for x in tf.split(a, [1,2,3,4],axis = 0):
3     print(x.shape)
4
5 for x in tf.split(a, 2, axis = 0):
6     print(x.shape)
>>> (1, 3)
    (2, 3)
    (3, 3)
    (4, 3)
>>> (5, 3)
    (5, 3)
```

4.4 TensorFlow 的 Reduction 操作

Reduction 运算的特点是它往往对一个 Tensor 内的元素做归约操作，如 tf. reduce_max()函数找极大值，tf. reduce_sum()函数计算累加。另外它还提供了 axis 参数来指定