

Chapter1 Introduction

1.1 机器学习的关键组件

- data

每个数据集由一个个样本 (example, sample) 组成, 大多时候, 它们遵循独立同分布 (independently and identically distributed, i.i.d.). 样本有时也叫做数据点 (data point) 或数据实例 (data instance), 通常每个样本由一组称为特征 (features, 或协变量 (covariates)) 的属性组成。机器学习模型会根据这些属性进行预测。在监督学习问题中, 要预测的是一个特殊的属性, 它被称为标签 (label, 或目标 (target))。

- model

深度学习与经典方法的区别主要在于: 前者关注的功能强大的模型, 这些模型由神经网络错综复杂的交织在一起, 包含层层数据转换, 因此被称为深度学习 (deep learning)。

- loss function

机器学习中, 我们需要定义模型的优劣程度的度量, 这个度量在大多数情况是“可优化”的, 这被称之为目标函数 (objective function)。我们通常定义一个目标函数, 并希望优化它到最低点。因为越低越好, 所以这些函数有时被称为损失函数 (loss function, 或cost function)。

通常, 损失函数是根据模型参数定义的, 并取决于数据集。在一个数据集上, 我们可以通过最小化总损失来学习模型参数的最佳值。该数据集由一些为训练而收集的样本组成, 称为训练数据集 (training dataset, 或称为训练集 (training set))。然而, 在训练数据上表现良好的模型, 并不一定在“新数据集”上有同样的性能, 这里的“新数据集”通常称为测试数据集 (test dataset, 或称为测试集 (test set))。当一个模型在训练集上表现良好, 但不能推广到测试集时, 这个模型被称为过拟合 (overfitting) 的。

- optimization algorithm

深度学习中, 大多流行的优化算法通常基于一种基本方法--梯度下降 (gradient descent)。简而言之, 在每个步骤中, 梯度下降法都会检查每个参数, 看看如果仅对该参数进行少量变动, 训练集损失会朝哪个方向移动。然后, 它在可以减少损失的方向上优化参数。

1.2 各种机器学习问题

1. 监督学习

监督学习 (supervised learning) 擅长在“给定输入特征”的情况下预测标签。每个“特征-标签”对都称为一个样本 (example)。有时, 即使标签是未知的, 样本也可以指代输入特征。我们的目标是生成一个模型, 能够将任何输入特征映射到标签 (即预测)。

监督学习的学习过程一般可以分为三大步骤:

- i. 从已知大量数据样本中随机选取一个子集，为每个样本获取真实标签。有时，这些样本已有标签（例如，患者是否在下一年内康复？）；有时，这些样本可能需要被人工标记（例如，图像分类）。这些输入和相应的标签一起构成了训练数据集；
- ii. 选择有监督的学习算法，它将训练数据集作为输入，并输出一个“已完成学习的模型”；
- iii. 将之前没有见过的样本特征放到这个“已完成学习的模型”中，使用模型的输出作为相应标签的预测。

2. 回归

回归（regression）是最简单的监督学习任务之一。当标签取任意数值时，我们称之为回归问题，此时的目标是生成一个模型，使它的预测非常接近实际标签值。

3. 分类

区分“哪一个”的问题叫做分类（classification）问题。分类问题希望模型能够预测样本属于哪个类别（category，正式称为类（class））。例如，手写数字可能有10类，标签被设置为数字0~9。最简单的分类问题是只有两类，这被称之为二项分类（binomial classification）。回归是训练一个回归函数来输出一个数值；分类是训练一个分类器来输出预测的类别，预测类别的概率的大小传达了一种模型的不确定性。

当有两个以上的类别时，我们把这个问题称为多项分类（multiclass classification）问题。常见的例子包括手写字符识别 $\{0,1,2,\dots,9,a,b,c,\dots\}$ 。与解决回归问题不同，分类问题的常见损失函数被称为交叉熵（cross-entropy）。

4. 标注

学习预测不相互排斥的类别的问题称为多标签分类（multi-label classification）。

5. 搜索

有时我们不仅仅希望输出一个类别或一个实值，例如在信息检索领域，我们希望对一些项目进行排序。

6. 推荐

另一类与搜索和排名相关的问题是推荐系统（recommender system），它的目标是向特定用户进行“个性化”推荐。尽管推荐系统具有巨大的应用价值，但单纯用它作为预测模型仍存在一些缺陷。首先，我们的数据只包含“审查后的反馈”：用户更倾向于给他们感觉强烈的事物打分。例如，在五分制电影评分中，会有许多五星级和一星级评分，但三星级却明显很少。此外，推荐系统有可能形成反馈循环：推荐系统首先会优先推送一个购买量较大（可能被认为更好）的商品，然而目前用户的购买习惯往往是遵循推荐算法，但学习算法并不总是考虑到这一细节，进而更频繁地被推荐。

7. 序列学习

序列学习需要摄取输入序列或预测输出序列，或两者兼而有之。具体来说，输入和输出都是可变长度的序列，例如机器翻译和从语音中转录文本。

8. 无监督学习

数据中不含有“目标”的机器学习问题通常被为无监督学习（unsupervised learning）。

- i. 聚类（clustering）问题：没有标签的情况下，我们是否能给数据分类呢？
- ii. 主成分分析（principal component analysis）问题：我们能否找到少量的参数来准确地捕捉数据的线性相关属性？

- iii. 因果关系 (causality) 和概率图模型 (probabilistic graphical models) 问题：我们能否描述观察到的许多数据的根本原因？
- iv. 生成对抗性网络 (generative adversarial networks)：为我们提供一种合成数据的方法，甚至像图像和音频这样复杂的非结构化数据，潜在的统计机制是检查真实和虚假数据是否相同的测试。

9. 与环境交互(强化学习)

在强化学习问题中，智能体 (agent) 在一系列的时间步骤上与环境交互。在每个特定时间点，智能体从环境接收一些观察 (observation)，并且必须选择一个动作 (action)，然后通过某种机制 (有时称为执行器) 将其传输回环境，最后智能体从环境中获得奖励 (reward)。此后新一轮循环开始，智能体接收后续观察，并选择后续操作，依此类推。请注意，强化学习的目标是产生一个好的策略 (policy)。强化学习智能体选择的“动作”受策略控制，即一个从环境观察映射到行动的功能。

当环境可被完全观察到时，强化学习问题被称为马尔可夫决策过程 (markov decision process)。当状态不依赖于之前的操作时，我们称该问题为上下文赌博机 (contextual bandit problem)。当没有状态，只有一组最初未知回报的可用动作时，这个问题就是经典的多臂赌博机 (multi-armed bandit problem)。

1.3 参考文献

- [PyTorch documentation](#)
- [PyTorch中文文档](#)