# 深度学习

## 深度学习基础

### 1.1机器学习和深度学习

机器学习：“计算机程序可以在给定某种类别的任务 T 和性能度量 P 下学习经验 E ，如果其在任务 T 中的性能恰好可以用 P 度量，则随着经验 E 而提高。”让我们根据前边的解释来定义我们的预测系统：我们的任务是确定可能产生飓风的气象条件。性能P是在系统所有给定的条件下有多少次正确预测飓风。经验E是我们的系统的迭代次数。

深度学习：深度学习是一种特殊的机器学习，通过学习将世界使用嵌套的概念层次来表示并实现巨大的功能和灵活性，其中每个概念都定义为与简单概念相关联，而更为抽象的表示则以较不抽象的方式来计算。

机器学习和深度学习的对比：深度学习与传统的机器学习最主要的区别在于随着数据规模的增加其性能也不断增长。当数据很少时，深度学习算法的性能并不好。这是因为深度学习算法需要大量的数据来完美地理解它。另一方面，在这种情况下，传统的机器学习算法使用制定的规则，性能会比较好。传统机器学会将问题分解为两步：物体检测和物体识别。首先，使用一个边界框检测算法扫描整张图片找到可能的是物体的区域；然后使用物体识别算法(例如 SVM 结合 HOG )对上一步检测出来的物体进行识别。相反，深度学习会直接将输入数据进行运算得到输出结果。例如可以直接将图片传给 YOLO 网络(一种深度学习算法)，YOLO 网络会给出图片中的物体和名称。

### 1.2 深度学习简介



深度学习将所需的复杂映射分解为一系列嵌套的简单映射（每个由模型的不同层描述）

来解决这一难题。输入展示在可见层 (visible layer)，这样命名的原因是因为它包含我们能观察到的变量。然后是一系列从图像中提取越来越多抽象特征的隐藏层 (hidden layer)。因为它们的值不在数据中给出，所以将这些层称为 ‘‘隐藏”; 模型必须确定哪些概念有利于解释观察数据中的关系。

一种是在深度概率模型中使用的方法，将描述概念如何彼此相关的图的深度视为模型深度。一种将计算图的深度视为模型深度。



从线性模型（线性加权重）到连接机制（当网络将大量简单计算单元连接在一起时可以实现智能行为）。连接机制其中一个概念是分布式表示，这一想法是系统每个的输入应该由许多特征表示的，并且每个特征应参与许多可能输入的表示。连接机制运动的另一个重要成就是反向传播算法的成功运用（训练具有内部表示的深度神经网络）和普及 (Rumelhart et al., 1986c; LeCun, 1987)。这个算法虽然曾黯然失色不再流行，但截至写书之时，仍是训练深度模型的主要方法。神经网络研究的第三次浪潮始于 2006 年的突破。名为深度信念网络的神经网络可以使用一种称为贪心逐层训练的策略进行有效地训练。

### 1.3 深度学习数学基础

#### 1.3.1 线性代数

##### 1.3.1.1 标量，向量，矩阵和张量

标量 (scalar)：一个标量就是一个单独的数，不同于线性代数中大多数概念会涉及到多个数。我们用斜体表示标量。标量通常赋予小写的变量名称。当我们介绍标量时，会明确它们是哪种类型的数。比如，在定义实数标量时，我们可能会说‘让 s ∈ R 表示一条线的斜率’。在定义自然数标量时，我们可能会说‘让 n ∈ N 表示元素的数目’。

向量 (vector)：一个向量是一列数。这些数是有序排列的。通过次序中的索引，我们可以确定每个单独的数。通常我们赋予向量粗体的小写变量名称，比如 x。向量中的元素可以通过带脚标的斜体表示。向量 x 的第一个元素是 x1，第二个元素是 x2，等等。有时我们需要指定向量中某个集合的元素。在这种情况下，我们定义一个包含这些索引的集合，然后将该集合写在脚标处。比如，指定 x1，x3 和 x6，我们定义集合 S = {1, 3, 6} xS。比如 x\_1 表示 x 中除 x1 外的所有元素，x\_S 表示 x 中除 x1，x3，x6 外所有元素构成的向量。

矩阵 (matrix)：矩阵是二维数组，其中的每一个元素被两个索引而非一个所确定。我们通常会赋予矩阵粗体的大写变量名称，比如 A。

[ A1,1 A1,2 ]

[ A2,1 A2,2 ]

张量 (tensor)：在某些情况下，我们会讨论不只两维坐标的数组。一般地，一组数组中的元素分布在若干维坐标的规则网格中，我们将其称之为张量。我们使用这种字体 A 来表示张量 “A’’。张量 A 中坐标为 (i, j, k) 的元素记作 Ai,j,k。

注意：

1.转置 (transpose) 是矩阵的重要操作之一。矩阵的转置是以对角线为轴的镜像，这条从左上角到右下角的对角线被称为主对角线 (main diagonal)。。我们将矩阵 A 的转置表示为 A⊤，定义如下(A⊤)i,j = Aj,i.



即可以这么理解，按照主对角线进行镜像。

2.向量可以看作是只有一列的矩阵。对应地，向量的转置可以看作是只有一行的矩阵。有时，我们将向量表示成行矩阵的转置，写在行中，然后使用转置将其变为标准的列向量，比如 x = [x1, x2, x3]⊤.

3.标量可以看作是只有一个元素的矩阵。因此，标量的转置等于它本身，a = a⊤。

4.只要矩阵的形状一样，我们可以把两个矩阵相加。两个矩阵相加是指对应位置的元素相加，比如 C = A + B，其中 Ci,j = Ai,j + Bi,j。

5.标量和矩阵相乘，或是和矩阵相加时，我们将其与矩阵的每个元素相乘或相加，比如 D = a · B + c，其中 Di,j = a · Bi,j + c。在深度学习中，我们也使用一些不那么常规的符号。我们允许矩阵和向量相加，产生另一个矩阵：C = A + b，其中 Ci,j = Ai,j + bj。换言之，向量 b 和矩阵 A 的每一行相加。这个速记方法使我们无需在加法操作前定义复制向量 b 到矩阵的每一行。这种隐式地复制向量 b 到很多位置的方式，被称为广播 (broadcasting)。

##### 1.3.1.2 矩阵和向量相乘

两个矩阵 A 和 B 的矩阵乘积 (matrixproduct) 是第三个矩阵 C。为了使乘法定义良好，矩阵 A 的列数必须和矩阵 B 的行数相等。如果矩阵 A 的形状是 m × n，矩阵 B 的形状是 n × p，那么矩阵 C 的形状是 m × p。矩阵乘积可以作用于两个或多个并在一起的矩阵，C = AB，该乘法操作定义为Ci,j =∑Ai,k Bk,j .需要注意的是，两个两个矩阵的标准乘积不是指两个矩阵中对应元素的乘积。不过，那样的矩阵操作确实是存在的，被称为元素对应乘积 或者哈达玛乘积A◎B。两个相同维数的向量 x 和 y 的点积 (dot product) 可看作是矩阵乘积 x⊤y。我们可以把矩阵乘积 C = AB 中计算 Ci,j 的步骤看作是 A 的第 i 行和 B 的第 j 列之间的点积。矩阵支持分配A（B+C）=AB+AC 结合律ABC=ACB 不支持结合律。两个向量的点积 (dot product) 满足交换律x⊤y = y⊤x（x⊤y =（x⊤y)⊤= y⊤x）。矩阵乘积的转置有着简单的形式：(AB)⊤ = B⊤A⊤。

##### 1.3.1.3 单位矩阵和逆矩阵

单位矩阵：I3

[ 1 0 0 ]

[ 0 1 0]

[ 0 0 1]

A\*A- =I3 A乘以A逆矩阵=单位矩阵 Ax=b A A-X = b A- x=b A-

确定 Ax = b 是否有解相当于确定向量 b 是否在 A 列向量的生成子空间中。这

个特殊的生成子空间被称为 A 的列空间 (column space) 或者 A 的值域 (range)。

##### 1.3.1.4 范数

在机器学习中，我们经常使用被称为范数 (norm) 的函数衡量向量大小。范数（包括 L

p 范数）是将向量映射到非负值的函数。直观上来说，向量 x 的范数是衡量从原点到点 x 的距离。

#### 1.3.2 概率和信息论

几乎所有的活动都需要能够在不确定性存在时进行推理。不确定性有三种可能的来源：1. 被建模系统内在的随机性。2. 不完全观测。3.不完全建模。

随机变量，概率分布，边缘概率，条件概率。概率分布：Multinoulli 分布和Bernoulli分布和高斯分布(正太分布)，指数分布，经验分布和混合分布。





信息论是应用数学的一个分支，主要研究的是对一个信号能够提供信息的多少进行量化。信息论的基本想法是一个不太可能的事件居然发生了，要比一个非常可能的事件发生，能提供更多的信息。消息说：‘‘今天早上太阳升起’’ 信息量是如此之少以至于没有必要发送，但一条消息说：‘‘今天早上有日食’’ 信息量就很丰富。我们想要通过这种基本想法来量化信息。特别地，

• 非常可能发生的事件信息量要比较少，并且极端情况下，确保能够发生的事件应该没有信息量。

• 更不可能发生的事件要具有更高的信息量。

• 独立事件应具有增量的信息。例如，投掷的硬币两次正面朝上传递的信息量，应该是投掷一次硬币正面朝上的信息量的两倍。

为了满足上述三个性质，我们定义一个事件 x = x 的自信息 (self-information)为

I(x) = = log P(x). (3.48)

在本书中，我们总是用 log 来表示自然对数，底数为 e。因此我们定义的 I(x) 单位是奈特 (nats)。一奈特是以 1e 的概率观测到一个事件时获得的信息量。其他的材料中使用底数为 2 的对数，单位是比特 (bit) 或者香农 (shannons)；通过比特度量的信息只是通过奈特度量信息的常数倍。

#### 1.3.3 数值计算

机器学习算法通常需要大量的数值计算。这通常是指通过迭代地更新解来解决数学问题的算法，而不是解析地提供正确解的符号表达。常见的操作包括优化（找到最小化或最大化函数值的参数）和线性方程组的求解。

条件数表明函数相对于输入的微小变化而变化的快慢程度。输入被轻微扰动而迅速改变的函数对于科学计算来说是可能是有问题的，因为输入中的舍入误差可能导致输出的巨大变化。

我们把要最小化或最大化的函数称为目标函数 (objective function) 或准则 (criterion)。当我们对其进行最小化时，我们也把它称为代价函数 (cost function)、损失函数 (loss function) 或误差函数 (error function)。

我们会探讨两种统计学的主要方法：频率估计和贝叶斯推断。大部分机器学习算法可以分成监督学习和无监督学习两类；我们将探讨不同的分类，并为每类提供一些简单的机器学习算法作为示例。大部分深度学习算法都基于随机梯度下降求解。我们将介绍如何组合不同的算法部分，例如优化算法、代价函数、模型和数据集，来建立一个机器学习算法。

### 1.4 机器学习基础

**任务，T**

通常机器学习任务定义为机器学习系统该如何处理样本 (example)。样本是指我们从某些希望机器学习系统处理的对象或事件中收集到的已经量化的特征 (feature)的集合。

机器学习可以解决很多类型的任务。一些非常常见的机器学习任务列举如下：

• 分类：在这类任务中，计算机程序需要指定某些输入属于 k 类中的哪一类。

• 输入缺失分类：当输入向量的每个度量不被保证的时候，分类问题将会更有挑战。

• 回归：这类任务中，计算机程序会给定输入预测数值。为了解决这个问题，学

习算法会

• 转录：这类任务中，机器学习系统观测一些相对非结构化表示的数据，并转录信息为离散的文本形式。

• 机器翻译：在机器翻译任务中，输入是一种语言的符号序列，计算机程序必须将其转化成另一种语言的符号序列。

• 结构化输出：结构化输出任务涉及到输出是不同元素之间重要关系的向量（或者是含多个值的其他数据结构）的任务。这是一个很大的范畴，包括上面转录任务和翻译任务在内的很多其他任务。例如语法分析——映射自然语言句子到语法结构树，并标记树的节点为动词，名词，副词等等。参考Collobert2011) 应用深度学习到语法分析。另一个例子是图像的像素级分割，将每一个像素分配到特定类别。

• 异常检测：这类任务中，计算机程序在一组事件或对象中筛选，并标记不正常

或非典型的个体。

• 合成和采样：这类任务中，机器学习程序生成一些和训练数据相似的新样本。波形。这是一类结构化输出任务，但是多了每个输入并非只有一个正确输出的条件，我们明确希望输出有很大的偏差，使结果看上去更加自然和真实。

• 缺失值填补：这类任务中，机器学习算法给定一个新样本x ∈ Rn，x 中某些元

素 xi 缺失。算法必须填补这些缺失值。

• 去噪：这类任务中，机器学习算法的输入是，由未知破坏过程从干净样本x ∈ Rn得到的污染样本x˜ ∈ Rn。算法根据污染后的样本x˜ 预测干净的样本x，或者更一般地预测条件概率分布 P(x | x˜)。

• 密度估计或概率分布律函数估计：在密度估计问题中，机器学习算法学习函数pmodel : R

n → R，其中 pmodel(x) 可以解释成样本采样空间的概率密度函数（如果 x 是连续的）或者概率分布律函数（如果 x 是离散的）。

**性能度量，P**

为了评估机器学习算法的能力，我们必须设计其性能的定量度量。通常性能度量P 是特定于系统执行的任务 T 而言的。对于诸如分类，缺失输入分类和转录任务，我们通常度量模型的准确率 (accuracy)。准确率是指该模型输出正确结果的样本比例。我们也可以通过错误率 (errorrate) 得到相同的信息。错误率是指该模型输出错误结果的样本比例。

**经验，E**

根据学习过程中的不同经验，机器学习算法可以大致分类为无监督 (unsupervised) 和监督 (supervised)。本书中的大部分学习算法可以理解成在整个数据集 (dataset) 上获取经验。数据集是指很多样本组成的集合。有时我们也将样本称为数据点 (data point)。

无监督学习算法 (unsupervised learning algorithm) 训练含有很多特征的数据集，然后学习出这个数据集上有用的结构性质。在深度学习中，我们通常要学习生成数据集的整个概率分布，显式地，比如密度估计，或是隐式地，比如合成或去噪。还有一些其他类型的无监督学习任务，例如聚类，将数据集分成相似样本的集合。

监督学习算法 (supervised learning algorithm) 训练含有很多特征的数据集，不过数据集中的样本都有一个标签 (label) 或目标 (target)。例如，Iris数据集注明了每个鸢尾花卉样本属于什么品种。监督学习算法通过研究 Iris数据集，学习如何根据测量结果将样本划分到三个不同品种。

大部分机器学习算法简单地训练于一个数据集上。数据集可以用很多不同方式来表示。在所有的情况下，数据集都是样本的集合，而样本是特征的集合。表示数据集的常用方法是设计矩阵 (design matrix)。设计矩阵的每一行包含一个不同的样本。每一列对应不同的特征。

通常情况下，当我们训练机器学习模型时，我们可以访问训练集，在训练集上计算一些度量误差，被称为训练误差 (training error)，并且我们会降低训练误差。目前为止，我们讨论的是一个简单的优化问题。机器学习和优化不同的地方在于，我们也希望泛化误差 (generalization error)，也被称为测试误差 (test error)，很低。泛化误差被定义为新输入的误差期望。这里，期望取值自我们期望系统在现实中从输入分布中采样得到的不同可能值。

在这个过程中，测试误差期望会大于或等于训练误差期望。以下是决定机器学习算法效果是否好的因素：

1. 降低训练误差

2. 缩小训练误差和测试误差的差距

这两个因素对应机器学习的两个主要挑战：欠拟合 (underfitting) 和过拟合 (overfitting)。欠拟合发生于模型不能在训练集上获得足够低的误差。过拟合发生于训练误差和和测试误差之间的差距太大。

点估计也可以指输入和目标变量之间关系的估计。我们将这类点估计称为函数估计。

### 1.5 CNN RNN DNN

## 2.Tensorflow

### 2.1 基础

#### 2.1.1 简介

TensorFlow™ 是一个采用数据流图（data flow graphs），用于数值计算的开源软件库。节点（Nodes）在图中表示数学操作，图中的线（edges）则表示在节点间相互联系的多维数据数组，即张量（tensor）。它灵活的架构让你可以在多种平台上展开计算，例如台式计算机中的一个或多个CPU（或GPU），服务器，移动设备等等。TensorFlow 最初由Google大脑小组（隶属于Google机器智能研究机构）的研究员和工程师们开发出来，用于机器学习和深度神经网络方面的研究，但这个系统的通用性使其也可广泛用于其他计算领域。

什么是数据流图（Data Flow Graph）：数据流图用“结点”（nodes）和“线”(edges)的有向图来描述数学计算。“节点” 一般用来表示施加的数学操作，但也可以表示数据输入（feed in）的起点/输出（push out）的终点，或者是读取/写入持久变量（persistent variable）的终点。“线”表示“节点”之间的输入/输出关系。这些数据“线”可以输运“size可动态调整”的多维数据数组，即“张量”（tensor）。张量从图中流过的直观图像是这个工具取名为“Tensorflow”的原因。一旦输入端的所有张量准备好，节点将被分配到各种计算设备完成异步并行地执行运算。



#### 2.1.2 Tensorflow介绍

Tensorflow是一种计算图模型，即用图的形式来表示运算过程的一种模型。Tensorflow程序一般分为图的构建和图的执行两个阶段。图的构建阶段也称为图的定义阶段，该过程会在图模型中定义所需的运算，每次运算的的结果以及原始的输入数据都可称为一个节点（operation ，缩写为op）。以下程序构建过程：



“import tensorflow as tf”，是在python中导入tensorflow模块,并另起名为“tf”；接着定义了两个常量op，m1和m2，均为1\*2的矩阵；最后将m1和m2的值作为输入创建一个矩阵加法op，并输出最后的结果result。我们分析最终的输出结果可知，其并没有输出矩阵相加的结果，而是输出了一个包含三个属性的Tensor。

第二个阶段为图的执行阶段，也就是在会话（session）中执行图模型中定义好的运算。我们通过程序2-2来解释图的执行阶段：

描述了图的执行过程，首先通过“tf.session()”启动默认图模型，再调用run()方法启动、运图模型，传入上述参数result，执行矩阵的加法，并打印出相加的结果，最后在任务完成时要记得调用close()方法，关闭会话。

我们还可以利用CPU或GPU等计算资源分布式执行图的运算过程。一般我们无需显示的指定计算资源，Tensorflow可以自动地进行识别，如果检测到我们的GPU环境，会优先的利用GPU环境执行我们的程序。但如果我们的计算机中有多于一个可用的GPU，这就需要我们手动的指派GPU去执行特定的op。tf.device(“/gpu:2”)。

Tensorflow中还提供了默认会话的机制，我们通过调用函数as\_default()生成默认会话。Sseion.as\_default()。交互式环境中经常会使用的InteractiveSession()方法，其创建sess对象后，可以直接输出运算结果。Ss = tf.InteractiveSession()。

首先，图模型的最大好处是节约系统开销，提高资源的利用率，可以更加高效的进行运算。因为我们在图的执行阶段，只需要运行我们需要的op,这样就大大的提高了资源的利用率；其次，这种结构有利于我们提取中间某些节点的结果，方便以后利用中间的节点去进行其它运算；还有就是这种结构对分布式运算更加友好，运算的过程可以分配给多个CPU或是GPU同时进行，提高运算效率；最后，因为图模型把运算分解成了很多个子环节，所以这种结构也让我们的求导变得更加方便。

Tensor（张量）是Tensorflow中最重要的数据结构，用来表示Tensorflow程序中的所有数据。Tensor本是广泛应用在物理、数学领域中的一个物理量。那么在Tensorflow中该如何理解Tensor的概念呢？

实际上，我们可以把Tensor理解成N维矩阵（N维数组）。其中零维张量表示的是一个标量，也就是一个数；一维张量表示的是一个向量，也可以看作是一个一维数组；二维张量表示的是一个矩阵；同理，N维张量也就是N维矩阵。

在计算图模型中，操作间所传递的数据都可以看做是Tensor。



构建图的运算过程输出的结果是一个Tensor，且其主要由三个属性构成：Name、Shape和Type。Name代表的是张量的名字，也是张量的唯一标识符，我们可以在每个op上添加name属性来对节点进行命名，Name的值表示的是该张量来自于第几个输出结果（编号从0开始），上例中的“mul\_3:0”说明是第一个结果的输出。Shape代表的是张量的维度，上例中shape的输出结果(1,1)说明该张量result是一个二维数组，且每个维度数组的长度是1。最后一个属性表示的是张量的类型，每个张量都会有唯一的类型，常见的张量类型如图2-2所示。



Tensorflow中对常量的初始化，不管是对数值、向量还是对矩阵的初始化，都是通过调用constant()函数实现的。因为constant()函数在Tensorflow中的使用非常频繁，经常被用于构建图模型中常量的定义，所以接下来，我们通过程序2-9了解一下constant()的相关属性：



函数constant有五个参数，分别为value，name，dtype，shape和verify\_shape。其中value为必选参数，其它均为可选参数。Value为常量的具体值，可以是一个数字，一维向量或是多维矩阵。Name是常量的名字，用于区别其它常量。Dtype是常量的类型，具体类型可参见图2-2。Shape是指常量的维度，我们可以自行定义常量的维度。

verify\_shape是验证shape是否正确，默认值为关闭状态(False)。也就是说当该参数true状态时，就会检测我们所写的参数shape是否与value的真实shape一致，若不一致就会报TypeError错误。如：上例中的实际shape为(2,0)，若我们将参数中的shape属性改为(2,1)，程序就会报如下错误：

TypeError: Expected Tensor's shape: (2, 1), got (2,).

Tensorflow还提供了一些常见常量的初始化，如：tf.zeros、tf.ones、tf.fill、tf.linspace、tf.range等，均可以快速初始化一些常量。例如：我们想要快速初始化N维全0的矩阵，我们可以利用tf.zeros进行初始化。Tensorflow还可以生成一些随机的张量，方便快速初始化一些随机值。如：tf.random\_normal()、tf.truncated\_normal()、tf.random\_uniform()、tf.random\_shuffle()等。

除了常量constant()，变量variable()也是在Tensorflow中经常会被用到的函数。变量的作用是保存和更新参数。执行图模型时，一定要对变量进行初始化，经过初始化后的变量才能拿来使用。变量的使用包括创建、初始化、保存、加载等操作。



展示了创建变量的多种方式。我们可以把函数variable()理解为构造函数，构造函数的使用需要初始值，而这个初始值是一个任何形状、类型的Tensor。也就是说，我们既可以通过创建数字变量、一维向量、二维矩阵初始化Tensor，也可以使用常量或是随机常量初始化Tensor，来完成变量的创建。当我们完成了变量的创建，接下来，我们要对变量进行初始化。变量在使用前一定要进行初始化，且变量的初始化必须在模型的其它操作运行之前完成。初始化变量的三种方式：初始化全部变量、初始化变量的子集以及初始化单个变量。首先，global\_variables\_initializer()方法是不管全局有多少个变量，全部进行初始化，是最简单也是最常用的一种方式；variables\_initializer()是初始化变量的子集，相比于全部初始化化的方式更加节约内存；Variable()是初始化单个变量，函数的参数便是要初始化的变量内容。通过上述的三种方式，我们便可以实现变量的初始化，放心的使用变量了。



我们经常在训练模型后，希望保存训练的结果，以便下次再使用或是方便日后查看，这时就用到了Tensorflow变量的保存。变量的保存是通过tf.train.Saver()方法创建一个Saver管理器，来保存计算图模型中的所有变量。



我们要注意，我们的存储文件save.ckpt是一个二进制文件，Saver存储器提供了向该二进制文件保存变量和恢复变量的方法。保存变量的方法就是程序中的save()方法，保存的内容是从变量名到tensor值的映射关系。Saver提供了一个内置的计数器自动为checkpoint文件编号。这就支持训练模型在任意步骤多次保存。此外，还可以通过global\_step参数自行对保存文件进行编号，例如：global\_step=2，则保存变量的文件夹为model.ckpt-2。

那如何才能恢复变量呢？首先，我们要知道一定要用和保存变量相同的Saver对象来恢复变量。其次，不需要事先对变量进行初始化。

本程序示例中，我们要注意：变量的获取是通过restore()方法，该方法有两个参数，分别是session和获取变量文件的位置。我们还可以通过latest\_checkpoint()方法，获取到该目录下最近一次保存的模型。

以上就是对变量创建、初始化、保存、加载等操作的介绍。此外，还有一些与变量相关的重要函数，如：eval()等。