

毕业设计（论文）

基于python的手写数字识别算法的实现

|  |  |
| --- | --- |
| 院 别 | 计算机与通信工程学院 |
| 专业名称 | 计算机科学与技术 |
| 班级学号 | **2133605** |
| 学生姓名 | 张浩天 |
| 指导教师 | 王翠荣 |

**2017**年**6**月**4**日

基于Hadoop的数据挖掘算法的研究与实现

摘 要

在当下信息化和网络化的大环境下，各行各业都采用计算机进行管理和运行，由此积累了大量的信息数据。在医疗行业方面，伴随着数字化进程的不断深入发展，在医学信息库当中包涵着大量的病人的信息数据。在这些数据当中既包括很多关于病人基本信息的结构化数据也包括大量的非结构化的医疗图像数据，这就为医疗图像挖掘提供了大量的资源。从海量的医学信息图像中挖掘出有效的信息，用来加速医生的诊断决策过程和提高医生诊断结果的准确度是医疗图像数据挖掘的最终目标。像Hadoop这样的分布式环境以及相关技术成为医疗图像数据挖掘的最佳选择。

关键词：数据挖掘，Hadoop，k-means,，医疗数据

Design and implementation of mining algorithm based on hadoop for data

Author:

Tutor:

Abstract

In the current information technology and network environment, businesses are managed and run by computer, which has accumulated a large amount of information and data. In the medical sector, along with the deepening of the development of digital processes

This paper introduces the HDFS and MapReduce Hadoop subprojects under the platform, and then introduced the relevant knowledge about cluster analysis and data mining. Thesis analyzes the k-means algorithm strengths and weaknesses and shortcomings for which the corresponding improvement, then subjected to a parallel realization by MapReduce programming model. Finally, medical images of this algorithm has been tested, experiments show that the improved algorithm for image segmentation is good, but after data processing becomes greater parallelism and faster.

Keywords：Hadoop, HDFS, k-means,Data Mining,Medical Data

目 录

1 绪论 6

1.1 研究背景及现状 6

1.2 研究目标及工作内容 7

1.2.1 研究目标 7

1.2.2 工作内容 7

1.3 本文组织结构 8

2 手写识别与人工神经网络概述 9

2.1 手写识别技术的意义 9

2.2 手写数字识别算法与其理论价值 9

2.3 手写识别的优劣判定 10

2.4 手写识别算法的技术难点 10

2.5 python 10

2.5.1 matplotlib 10

2.5.2 … 10

2.6 pycharm 10

2.7 MINST 10

3 基于混合神经网络的手写识别算法的实现 10

3.1 功能介绍 10

3.2 整体架构介绍 11

3.3 详细介绍 12

3.3.1 输入数据处理部分 12

3.3.2 卷积层（C1） 14

3.3.3 池化层 18

3.3.4 全连接层 20

3.3.5 输出层 26

3.3.6 权值更新 26

4 实验分析与优化 32

4.1 实验环境（jupyter） 32

4.2 实验数据 32

4.2.1 数据预处理 32

4.3 实验结果与优化分析 32

4.3.1 批的大小（batch size） 32

4.3.2 训练次数（epoch） 34

4.3.3 学习率（learning rate） 34

4.3.4 神经元数量 35

4.3.5 卷积层的作用 36

4.3.6 数据标准化 37

4.3.7 偏移量的作用 38

5 论文的总结与展望 39

致谢 39

参考文献 39

附录 39

# 绪论

## 研究背景及现状

手写识别是模式识别的一种，是由二十世纪六十年代初出现的一门学科。从二十世纪九十年代后，由于GPU等计算核心速度的极大提升，模式识别的应用从以前的单纯的数学计算提升到了对图像甚至视频的范围以至于现在的计算机视觉技术。模式识别的研究方向是用一定的算法，使计算机实现学习的能力。通过大量的学习，使其得到对人类接触到的事物具备的判断与识别的能力。获得这里能力的机器在一定程度上可以取代大量重复的人工劳动如复杂的生产线。也正因为如此，模式识别在近年来成为人工智能领域极其热门的一个领域。模式识别的主要功能是分类，即判断系统所需要处理的数据属于哪一个类别。如判定邮件是否为垃圾邮件，判断音频所对应的英文单词等。模式识别在流程上主要包括信息的输入，信息的预处理，对信息特征的提取，识别与分类等环节。

在模式识别中，手写识别是十分热门也是相对来说比较成熟的一个分支。一方面来说手写识别的应用极为广泛，如今人们在手机与电子阅读设备中的阅读时间远超于纸质产品，电子设备又具有可搜索，环保，方便携带等特点，生活中高准确率的手写识别需求极高；另一方面来说，手写识别有很多推广，许多其他方面的技术如物体识别，路牌等打印文字的识别会与手写识别有技术上的共性。

从手写识别数据的来源来分，手写识别由脱机识别和联机识别两个大类，脱机识别又可以被称作光学字符识别，简称为OCR。联机识别在技术上与OCR完全不同，因为联机识别中数字写下的比划，力度，速度都是有效的信息，这样的信息在OCR中是无法得到的，这样也使联机识别的准确率相对OCR高了很多。在OCR中，由于输入的数据往往是照片，扫描仪等，输入的数据只有图片的像素数据，而且因为环境的不稳定，不同中字符的位置，亮度，纸张噪点等影响，会使OCR相对于联机识别难度更高。

随着计算机运算性能的显著提高，计算机运算成本的不断下降，模式识别已经从模型的理论建立一步步发展到了广泛实际应用阶段。借助现代性能高效的CPU，复杂的模式识别问题如语音识别与图片中的物体识别。但对于生活中一些需要复杂的实时处理的问题时，又由于当今计算机存储容量与其高复杂度运算的矛盾而进入瓶颈，这就促使了得益于大规模并行运算的人神经网络技术应用到模式识别问题中。神经网络技术将模式识别领入了另一个时代，手写识别就是其中一个得益于神经网络的领域。

手写识别是一个古老的课题，在很长时间以来，对于字符识别这样的工作是使用传统算法解决的，而即使是最好的传统识别算法，其对手写印刷体的识别也仅仅停留在了94%到96%之间，对手写体字符的识别更是停留在了研究阶段，其识别率很低以至于无法有效利用。在二十世纪九十年代之后，神经网络通过其自我学习与大规模分布式并行处理的方式，且因为其拥有非线性与强推广能力与高容错性的特点，其集齐了广泛的研究与关注。基于神经网络的手写识别算法在准确率上得到了极大的提升，并有对噪点容错性强等特点，迅速淘汰了传统的手写识别算法。现代高度优化的神经网络算法如LeNet5等，其对处理过的手写字符的准确率达到99.9%以上，对路牌等环境复杂的字符识别准确率也达到了96%以上。

## 研究目标及工作内容

### 研究目标

设计并实现神经网络算法，通过组合不同的神经网络结构并给与优化，通过使用大量手写数据对其进行训练，使神经网络可以对手写数字进行高准确率的识的别。本文仅仅使用python最基本的工具包，从最底层对神经网络进行实现，目的是对算法的实现过程进行深入的分析，同时通过调整算法各部分的细节，更好的对各个参数与部分对神经网络训练的影响进行分析，从而对算法进行彻底的优化。

### 工作内容

1. 详细介绍本神经网络的架构与层次作用。
2. 详细介绍卷积神经网络与全连接神经网络的底层算法与基本原理。
3. 通过理论与实验的分析，分析神经网络各部分对算法性能与准确率的影响，对网络进行优化，并分析此算法的优缺点。对算法中有提升空间的部分进行分析，修改与展望。
4. 对未被识别的开源手写数字数据库部分进行识别，为手写识别研究提供有效数据。

## 本文组织结构

第一章 介绍了手写识别算法的研究背景与研究的意义，介绍了手写识别算法近年来的研究方向与进程，分析了传统手写识别算法的不足之处以及基于神经网络的手写识别算法的优势，在本章的最后，简要说明了本文的研究目标与工作内容，对本文的组织结构进行了简洁的阐述。

第二章 介绍了云计算的基本概念和特征，介绍了Hadoop平台基本框架和原理以及它的两个核心技术HDFS、MapReduce。并分别介绍了这两个技术的框架以及工作原理。

第三章 详细的介绍

第四章 对k-mean算

第五章 详细讲述

# 手写识别与人工神经网络概述

## 手写识别技术的意义

手写识别在技术上属于模式识别的中最典型的应用之一。手写识别的主要目标是利用计算机，自动的将含有手写识别字符的图片转换为计算机中的字符数据，手写识别在技术上分为光学字符识别（OCR）与联机手写识别（主要是手写输入法），其由于输入信息不同，对应的算法与优化完全不同，本文的算法主要针对光学字符的识别，联机识别算法暂不讨论。

## 手写数字识别算法与其理论价值

手写数字识别是手写识别算法的一个最典型的分支，其研究的理论价值很大：

1. 阿拉伯数字是全球通用的文字，也是世界上被使用次数最多的十个字符。因为这时全球通用的字符，所以对手写数字的研究是超越国界的，其研究与文化背景无关，全球的研究成果都可以进行共享，对手写数字识别算法也研讨也十分方便与统一。
2. 手写数字识别算法的应用范围极广，在很多领域，手写数字识别的自动化可以大大提高处理的效率，降低人工成本。如邮政编码的识别，报税表单与存款单等。这些工作往往包含着大量的重复简单的人工劳动，强度大且效率低。而手写识别的出现可以大大减少人力的成本，提高工作的效率，也使无纸化办公的未来更进一步。
3. 相对于对其他种类字符的识别，手写数字算法所需要的识别的种类只有十个，远少于字符识别（200个左右）甚至汉字识别（10000个以上），其识别率相对较高，所需要的算法工程量也较低，因为这个优点，对于新的模型与理论，往往使用手写数字识别的方法来验证算法的准确性，对其分析以及做深入的研究。因为比较简单，对于基于机器学习与神经网络的手写识别算法来说，其所需要的训练数据与训练时间也相对较少，新开发的机器学习与模式识别算法都是用手写识别数据进行理论有效性检验，然后才推广到更复杂模型如路牌识别与字符识别。典型的例子有Lecun的卷积神经网络LeNet以及[Vladimir N. Vapnik](https://en.wikipedia.org/wiki/Vladimir_N._Vapnik" \o "Vladimir N. Vapnik)发明的支持向量机（SVM）。
4. 手写数字识别算法的推广很简单。比如对英文字母的识别与对路牌与车牌号的识别，其算法与手写数字识别大同小异。在现代的研究中，许多新算法就是对手写英文字符与手写数字同时进行识别的。

## 手写识别算法的技术难点

手写数字识别看似简单，只有十种类别且笔画简单，但在实际识别过程中，一些算法的实验表明，即使有几万中类别，印刷体汉字的识别准确率是高于手写数字识别的。联机手写识别的准确率也是一直高于手写数字的OCR的。其主要原因是数字与数字之间比划相差很小，数字的写法相对简单，同一个数字的写法相差很多。虽然数字是世界通用的文字，但是在数字的字体方面，是存在很强的地域性的，不同国家对一些数字的书写习惯不同，如英美数字的“7”要比亚洲人的习惯多一比等。

经过多年的探索，国内与国外针对手写数字识别的算法研究上已经几近成熟，但依然存在下面两大问题

1. 在手写数字识别的精度方面，其精度要更高。手写识别无法通过上下文等方法进行错误验证，而在有些情况，如支票等与经济，财会相关的应用中，任何错误都是不允许发生的。因此，在手写数字识别的研究中，大多都是在向提高识别准确率的方向而努力。
2. 由于数字识别往往涉及到大量的数据，一张数字表格往往就有几千个数字需要识别，所以识别的速度同样是数字识别的要求之一，然而精度与速度往往是相互矛盾的，这就使识别算法需要权衡二者。

## 人工神经网络概述

人工神经网络旨在通过模仿人脑中神经网络的基本结构，将人脑模型数学化并简化而成的数学模型。从生理学看，人脑的神经网络是由大量的，有这复杂连接的神经元组成的，人的学习过程其实是对人脑中神经元间关联强弱的自适应性调整。人脑的神经元在处理不同问题的方面是有不同结构形态的，所以人工神经网络也有这不同的形态，如递归神经网络，卷积神经网络，全连接神经网络等。神经网络的最小组成单元是神经元，虽然种类繁多，但基本结构几乎相同。

和人脑一样，人工神经网络必须经过学习才能准确的工作。通过学习来提高自身性能是神经网络的一个重要特点。一般情况下，其改善自身性能的方法是通过提高内部神经元之间的连接强度（权值）达到的，人工神经网络的学习方式，可以以接收到的信息种类来分成下面三种：

1. 监督学习（Supervised Learning）

监督学习的直观理解其实是模仿，监督学习的学习来源是样本数据，而监督学习就是通过让人工神经网络对样本数据的读取，不断调整自己内部的权值，不断的让自己在输入样本数据时，输出对应的样本结果，由于在学习的过程中，样本数据中含有样本输入与输出，所以这种方法叫做监督学习。监督学习的优点是速度快，结果容易预测。但是监督学习的缺点也有很多，由于监督学习中神经网络其实是单纯的模仿，所以在样本情况比较复杂的情况下，神经网络容易忘掉很久之前的样本信息，造成网络只对训练后期的数据比较敏感。还有在物体识别等算法中，在生活中并没有大量的数据供神经网络去学习，这时就需要大量的人工标注，其高成本也是监督学习的缺点之一。

1. 非监督学习（Unsupervised Learning）

非监督学习不存在处理好的训练样本，其训练数据是单纯的统计数据，非监督学习的程序通过寻找输入数据的规律来调节自身的参数甚至结构，与监督学习不同的是，非监督学习的目标是更好的表示统计数据内部的结构与特征，训练的过程中不断提取新的特征，在应用到模式识别中时，非监督学习通过自身对特征的理解将输入数据分成很多类，训练完成的程序可以讲未出现过的数据进行归类，这是一种完全无人参与的自学习功能。由于无需对数据的人工处理，非监督学习的成本要低于监督学习，也因此在近年来受到更高的关注。

1. 强化学习（Reinforcement Learning）

强化学习介于监督学习与非监督学习的之间，强化学习中对系统的输出结果没有正确与错误的判断，而是给出一个综合评判的奖惩信息，神经网络通过奖惩之间的权衡来改变自己内部的权值与结构，从而得到一个最佳的平衡点。

# 基于混合神经网络的手写识别算法的实现

## 功能介绍

本算法旨在通过用利用神经网络的优势，高效的对手写数字进行识别，即将手写在纸上或设备上的数字的图片信息高正确率地转换为纸上或设备上的数字。

## 整体架构介绍

为了充分发挥各个神经网络的优点，使其既有卷积神经网络高效，速度快，对噪点的容错性高的优点，又有全联接的前导神经网络准确性高的特点，本算法使用将卷积神经网络与前导神经网络抽样后全联接的方法来高效的完成对手写数字图像的识别。

>整体网络图 figure\_all

本神经网络的主体分为输入数据处理，神经网络运算和输出数据处理。

其中输入数据处理（IN\_PRO）是将原始数据处理成神经网络容易识别的且经过标准化的数据集。

神经网络(在运算上分为训练阶段与识别阶段。在训练阶段神经网络通过所给的训练数据与答案修改与更新自己的参数，从而使自己通过输入数据所计算出来的答案越来越接近真实正确的答案。识别阶段即使用通过大量数据训练过的神经网络，让测试数据通过神经网络进行运算从而得出预测的结果。

在这里神经网络部分（NN）分为输入层（IN）卷积层（C1），池化层（S1），隐藏层（H1），输出层（OUT）

输出处理则将大量的原始，为优化结果而标准化的数据处理成可以利用，统计的直观数据。在这里输出处理只有一部分（OUT\_PRO）。

## 详细介绍

下面将对本算法的各个层次的原理，设计与实现进行详尽的介绍。

### 输入数据处理部分

>输入处理图 in1

本部分旨在对原始数据的处理，其中原始数据有训练数据（32000张PNG图片，其中每个图片的分辨率为28\*28，图片为灰度图片）；训练数据的标签，即这32000张图片所显示的具体数字的答案；测试数据（10000张图片，图片格式与训练数据相同）以及测试数据的标签。

对训练与测试数据的处理：

训练数据原始为图片，先用python的Image库将整个图片加载成矩阵，由于输入的图片均为灰阶图片，所以根据Image库的算法，输出的矩阵为输入图片对应像素的灰阶值。

然后对这个矩阵进行标准化，标准化的意思是，通过线性或者非线性转换，将矩阵的最大值-最小值范围控制在0-1之间且让最大值和最小值尽量分别接近0与1。对于本文针对的灰阶矩阵，其最大值为255，最小值为0，所以我们可以通过把每个数字除以255的方式将其标准化。

用此方法，我们成功将输入矩阵进行了标准化。对于标准化的作用，本文将在后面介绍线性神经元与其梯度下降算法的部分详细介绍。

对训练与测试标签数据的处理：

训练数据与测试数据通过神经网络的计算会得到其预测的结果的特征，在这里这个特征的值就决定了本神经网络对输入图像的识别结果。区别于数字本身的连续性，对于神经网络的分类任务来说，其特征应该是互不相干的，例如：1与9之间的相关性应和1与2之间的相关性完全一样。所以需要用编码的方式排除数字本身的相关性，本算法使用的编码方式是独热编码（One-Hot Encoding）

独热编码：

独热编码直观来说就是用总状态数的比特数，其中一个比特为0其他比特为1的方法来表示状态的一种码制。

在本文的算法中，总状态数即为10。下面是编码表：

|  |  |  |
| --- | --- | --- |
| 原始数据 | 二进制 | 独热编码 |
| 0 | 0000 | 1000000000 |
| 1 | 0001 | 0100000000 |
| 2 | 0010 | 0010000000 |
| 3 | 0011 | 0001000000 |
| 4 | 0100 | 0000100000 |
| 5 | 0101 | 0000010000 |
| 6 | 0110 | 0000001000 |
| 7 | 0111 | 0000000100 |
| 8 | 1000 | 0000000010 |
| 9 | 1001 | 0000000001 |

表格 1-a

经过编码后的标签由于其向量积均为0，所以互不相关。且在总状态数较少的情况下独热编码更简单高效，另一方面又增加了状态的空间，使算法更加准确。

### 卷积层（C1）

卷积神经网络(Convolutional Neural Network, CNN)：

卷积神经网络是深度学习与计算机视觉中极其重要的网络结构之一，许多及其成功的模型都是基于CNN的，特别是基于ImageNet等的各种图像物体识别算法。卷积神经网络算法相对于传统的图像处理算法有很多优点，其中一个就是其巧妙的避免了复杂耗时的预处理工作（如人工特征的提取），原始图像数据经过CNN可以直接进入下一步的运算，不需要人工的参与。

如前文所说，在图像识别的过程中，图像往往会被看成一个或多个的二维矩阵，本文用到的MINST图像库中，图像库中每一个图片就可以看成是28 \* 28 的二维矩阵，因为它是黑白图片，只有一个颜色通道。如果是彩色图片就会有RGB三个颜色通道，就会被表示为三个二维矩阵。传统的神经网络算法使用的是全链接的方式，这种连接方式是将每一个颜色通道的每一个像素都与下一层的神经元·所连接，这样会使参数的数量指数增长，导致参数的数量巨大，使整个神经网络的训练及其耗时甚至时间数量级巨大，无法训练。而卷积神经网络通过局部链接，权值共享两个主要方法，在几乎不消耗准确率的情况下大幅减少变量数，从而避免这一困难的发生。

（图片）

直观的看，卷积层的参数可以看作是一系列的可以训练和学习的过滤器（卷积核）。在前向学习的过程中，每次我们将图片的每一个小部分通过一个过滤器，点乘后再组成新的二维数据，每个过滤器计算成的二维数据再组成三维数据。我可以理解成每个过滤器只关心一部分图片的特征，再综合图片的各个特征进行下一步的训练。

局部连接：

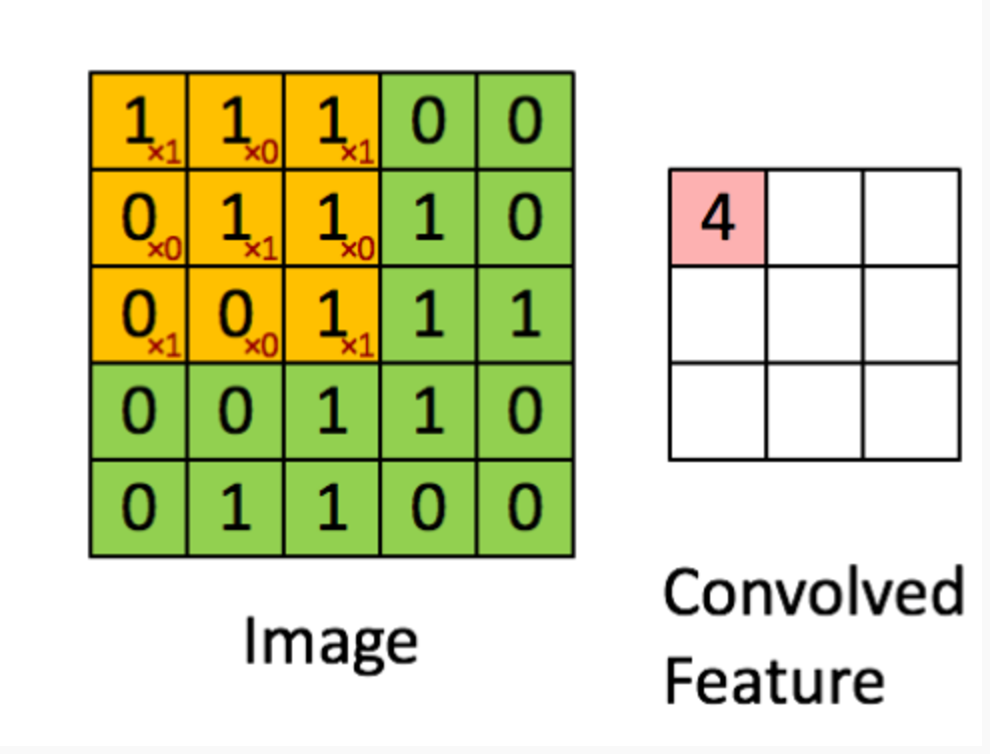
局部连接是卷积神经网络独特的原因之一，上文提到在图片中，使用全连接的神经网络在工程上是不可行的，而局部链接的意思就是卷积神经网络的神经元只会与上层的神经元的局部区域进行连接。可以把上层数据想象成一张画，画的上面有一个滑动的窗口，每次运算时只有窗口内的数据会与下层进行关联。这就引出了卷积神经网络的一个重要的变量：窗口大小，一般窗口的长与宽是相等的，窗口的长\*宽叫做感受野（receptive field），在整个运算中，这个窗口会逐格滑动，一步步近似覆盖图片的每一个小区域。

在本算法中，我们的MINST图片库输入的图片数据大小为[1\*28\*28]，我们设定感受野（窗口）大小为[5\*5]，为了提取不同的特征，我们有6个不同的卷积核。

权值共享：

权值共享是卷积神经网络中很巧妙的处理方方式，它可以使卷积神经网络的训练与识别时的计算复杂度和参数的个数下降非常非常多。在本算法中，我们共有6个卷积核，每个卷积核大小为5 \* 5，所以经过特征图（feature map）的长与宽都为（28-5+1），共有6个特征图，所以每个图片的总变量数位6\*24\*24 = 3456个神经元，每个窗口由于数据的连接，有5\*5=25个权重，所以共有25\*3456= 86400个参数，如果每张图片的计算量都是这么大的话，会变得非常非常慢，也就失去了它的意义。

因为每个卷积的神经元可以看成是一个过滤器，那么我们可以大胆的假设，这个神经元用于连接每个数据窗口的权重都是固定的，不会因为窗口的位置而改变。这意味着，对于每一个卷积神经原来说，不管其对应的数据窗口在图片的哪个位置，其权重都是同一组数。那就代表，我们的卷积层中，我们只需要神经元个数\*卷积核的维度= 6\*6\*5=180个权重。



如果每个神经元在不同位置对应的权重是固定的，那么同一个卷积神经元进行计算卷积积分的整个过程就可以看成是一组固定的权重和不同位置的数据窗口做内积的过程，在数学上刚好对应着『卷积』操作，这也是卷积神经网络名字的来源。

另外，因为每个神经元的权重都是固定的，它们都可以看做一个恒定的过滤器，比如我们的6个卷积神经元作为过滤器后可视化之后的样子如图：



需要说明的一点是，参数共享并不是一个在每个场景都适用的一种策略，在一些特定的场合中，如人脸识别中，由于一般照片中人的面部都集中在画面的中央，所以在人脸识别的过程中，我们不能把照片上的每个位置的窗口数据的作用都视作等同的。在这种情况下，我们希望数据窗口滑过中心区域的时候其权重和其他边缘区域是不同的。对于这种情况我们有一种特殊的层对应这种功能，叫做**局部连接层，**在本算法中局部连接层没有被用到，就暂不赘述。

具体实现：

本算法使用的是批梯度下降法（mini-batch learning）进行训练，即将多个输入数据同时通过神经网络进行计算，计算后将更新的数据进行叠加来更新，这样既会利用python的系统优化提高计算效率，又会避免低效重复的更新，具体将在本章后面有花的部分进行详细描述。

首先初始化经卷积后的多个特征图，由于有每次训练是由多个输入数据组成的批，每批有6个特征图，每个特征图是24（图片宽度-窗口宽度+1）\*24的矩阵，我们先初始化特征图组为批大小\*特征图数\*特征图高\*特征图宽的四维矩阵，然后用每个卷积核分别用窗口划过每张图片，每滑动一次求出相应的积并填入特征图相应的位置中。具体代码如下。

conved\_input = np.zeros((train\_data\_batch.shape[0], num\_of\_fmap, image\_size - conv\_core + 1, image\_size - conv\_core + 1), dtype = np.float)  
**for** i **in** range(0, train\_data\_batch.shape[0]):  
 **for** j **in** range(0, num\_of\_fmap):  
 **for** k **in** range(0, image\_size - conv\_core + 1):  
 **for** l **in** range(0, image\_size - conv\_core + 1):  
 conved\_input[i][j][k][l] = sum(sum(two\_d\_input[i][k:k + conv\_core, l:l + conv\_core] \* (in\_to\_conv\_weights[j]. reshape(conv\_core, conv\_core))))

由于本程序是基于CPU，所以每个求积需要单独运算，本算法经过GPU加速后可以根据GPU的核心数（如NVIDIA GeForce GTX1050Ti有640个核心）同时运算，可大幅提高速度。

### 池化层

图？

一般来说，在卷积神经网络中，池化层是在连续的卷积层中间或者卷积到全连接层中间的层。它的作用也非常简单，就是通过抽样的方法逐步地减少和压缩数据和参数的量，在一定程度上也会减小过拟合的现象，即过度的符合训练数据而使容错性降低。池化层做的操作也非常简单，就是将原数据上的每个小区域压缩成一个值(小区域的区域最大值（MAX）或者平均值（AVERAGE）)，最常见的池化层的设定是，将原数据切成由2\*2的小块组成的格式，在每块里面取最大值作为输出，这样我们就自然而然减少了75%的数据量，抽样的方式根据分数据特点的不同而不同。

在最大值和平均值的池化方式外，我们也可以设定其他的抽样方式，如L2范数池化。

本算法中对池化层和它的操作的直观理解的示意图为：



如图为本算法中池化层的一个直观的示意，即对上一层（卷积层）处理后得出的6\*24\*24的数据（一般来说，特征图的数量被称为厚度）的每一个切片（1\*24\*24的部分）做了一个下采样。下图为次采样操作的实际操作。



具体实现：

在本算法中，通过上文我们知道，由上层卷积神经网络计算出了维度为批大小\*特征图数\*特征图高\*特征图宽的四维矩阵，我们对每个特征度进行取样单位为2\*2，的最大值取样，所以取样后的特征图的维度为批大小\*特征图数\*（特征图高／2）\*（特征图宽／2），对于每个取样后的特征图的位置，其值为对应的四个特征图的值的最大值。为了方便后面更新权制，需要把最大值所在位置的坐标也同时记录下来，具体代码如下：

conved\_input\_maxloc = np.zeros( (train\_data\_batch.shape[0], num\_of\_fmap, image\_size - conv\_core + 1, image\_size - conv\_core + 1),dtype=np.float)

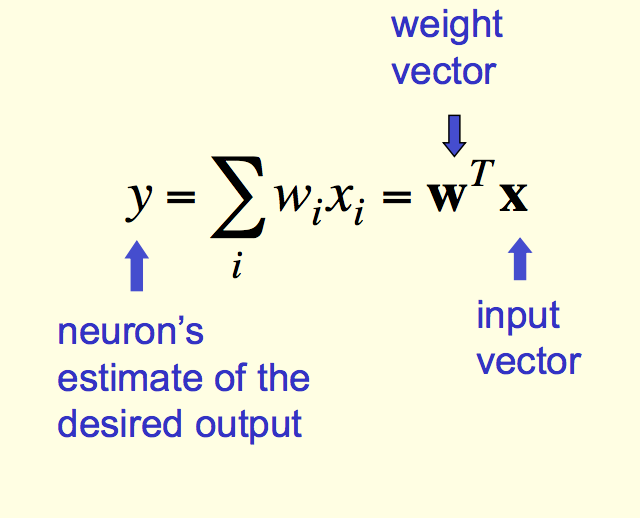
sampled\_input = np.zeros((train\_data\_batch.shape[0], num\_of\_fmap, int((image\_size - conv\_core + 1) / 2), int((image\_size - conv\_core + 1) / 2)), dtype=np.float)  
**for** i **in** range(0, train\_data\_batch.shape[0]):  
 **for** j **in** range(0, num\_of\_fmap):  
 **for** k **in** range(0, int(conved\_input.shape[2] / 2)):  
 **for** l **in** range(0, int(conved\_input.shape[3] / 2)):  
 sampled\_input[i][j][k][l] = np.amax(conved\_input[i][j][2 \* k:2 \* k + 2, 2 \* l:2 \* l + 2])  
 agmx = np.argmax(conved\_input[i][j][2 \* k:2 \* k + 2, 2 \* l:2 \* l + 2])  
 conved\_input\_maxloc[i][j][2 \* k + int(agmx / 2)][2 \* l + agmx % 2] = 1

### 全连接层

全连接神经网络是神经网络中最基本，最标准的形式。全连接的意思是，神经网络中一层的所有神经元都和上一层的所有神经元之间进行关联，相对于卷积神经网络，全连接神经网络的矩阵运算比较和直接。现代的很多卷积神经网络结构，其末层或末几层都会采用全连接去学习更多的信息。要理解全连接层的工作原理，我们必须了解组成全连接层与所有神经网络的基本单元——神经元的工作原理。



在神经网络中有很多种类的神经元，在全连接神经网络中最常见的神经元叫做现行神经元，又叫做线性过滤器，线性神经元的有一系列的输入，它的参数是这些输入的权值，输出是它输入值的加权和。



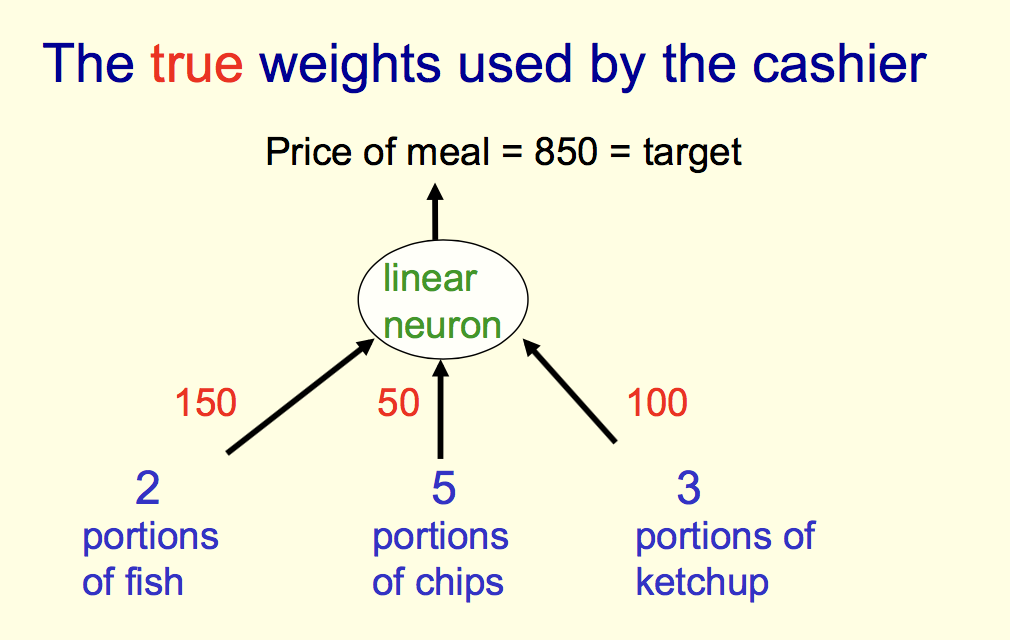
神经元的偏差方程是用来计算神经元输出值与正确值差别的方程，对于不同的情况，有不同的计算偏差的方式，在数字预测方面经常会使用方差模型，在坐标方面有欧式距离和曼哈顿距离，在文字处理方面经常使用交叉熵作为偏差方程。神经元的目标是通过更新自身的参数（对每个输入的权值）来尽量减少输出的偏差，使自身更佳准确，在这里，偏差是所有残差的平方和。

一个神经元的例子：

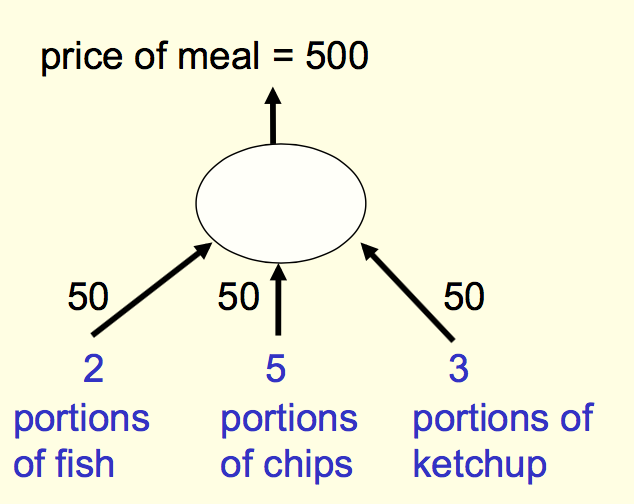
假设你每天在食堂吃午餐，每天的午餐由不同数量的鱼，菜，米饭组成，每次点完餐阿姨只会告诉你总价格，几天之后，你就可以推算出每种食物的单价了。在这里假设你就是一个线性神经元：

每个种类的价格组成了线性神经元的权值：

开始的时候我们会随机猜每种菜品的价格，然后每过一天，通过我们点的每种菜的数量和阿姨告诉我们的总价格，一点点更新我们的猜想，使其更加接近正确的值。



我们首先预测每种食物的价格都为50元（这里是初始值，可以为任何非零数，如果是零会导致更新时的变量为0，无法更新，在卷积神经网络中有时候会用到这个方法保持权值的同步）



在这里输入值为:

线性神经元权值

残差

根据学习规则（delta-rule）权值的变化量 其中为学习率，即学习的速度。

假定学习率，则鱼，菜，饭的变化分别为

更新后的权值为 进一步接近正确值，当有新的数据，循环的次数越来越多之后，预测的价格会越来越接近于真实的价值。这个方法的优化后的标准化方法叫做梯度下降，用偏导的方法找到使误差下降最快的变化量。

梯度下降：

梯度下降又被称为最速下降法，是一种迭代的最优化算法，函数在一个位置的梯度可以表示为这个函数在这一点的时候它最“陡峭”的方向，那么如果一个点向它对应方向的梯度增加很小的数量，那么这个更新后的点的函数值一定会下降。



而梯度下降法正是利用了这样特点，把每个神经元的参数当作这个上点的“坐标”而这个函数就是神经元权值与整个神经网络的偏差的关系，那么利用梯度下降的方法，经过很多很多次的迭代，不断的更新神经元的权值，整个申请网络的偏差就会不断的下降，最终达到一个最小值。

全连接神经网络：

全连接神经网络又多层神经元组成，第n层的神经元的输入与第n-1层的神经元的输出进行相连，同时第n层神经元的输出与第n+1层神经元的输入相连接，这样一层一层传递数据，最终传递出结果，再通过输出结果一层一层的向前更新变量（back-propagation）。通过多层神经网络的数据传递与权值更新，其能通过训练找到数据与其标签的隐藏含义，而相对于单层神经元组成的网络，其能更好的识别更加复杂和隐含的模型。多层神经网络在结构上分为输入层（input layer），隐藏层（hidden layer），和输出层（output layer），其中隐藏层可以有多个。

图

在多层神经网络中，由于是全连接的结构，第n+1层与第n层之间的连接数为他们的神经元数的积，在这里表示位于第n层神经元的权值，表示从上一层第i个神经元连向下一层第j个神经元的权值。

图

在计算的过程中，第n层的第j个神经元的输出值等于第n-1层每个神经元的输出值与其对第n层第i个神经元加权总和

全连接神经网络的计算极其相似于矩阵的乘法，现假设每个批次只有一组输入数据，输入数据为一横行的数据：

设矩阵W[i][j]表示输入数据到第一层隐藏层的权值，纵坐标表示输入神经元i，横坐标表示输出神经元j，W[i][j]表示

将输入矩阵与权制矩阵点乘，通过点乘法则得到矩阵：

正好为隐藏层的输出值，这个数组可以在与下一层的权值进行点乘，如此就可以依次迭代快速得出所有层的值。

在批梯度下降法中，可以将一个批次中每行数据并成一个批次大小\*数据维度的矩阵，这样可以通过矩阵与矩阵的乘法快速高效的点乘出下一层的值：

具体实现：

在本算法中，由上层卷积神经网络经池化后的数据维度为批大小 \* 特征图数 \*（特征图高／2）\*（特征图宽／2），在这里为了更好的利用矩阵的特性进行全连接计算，将池化后的数据进行处理，将维度变化为二维，纵向为批大小，将每批的数据转换为1行，这样输入到全连接神经网络的数据就会变成批大小 \* （特征图数 \*（特征图高／2）2，综合速度与准确性的考虑，本算法中我们设定隐藏层大小为200 个线性神经元，输入数据经过与权值的矩阵点乘后，为了使训练更加高效，又将点乘后的数据加入了可训练的偏差值后得到了隐藏层。由于输出结构为之前独热编码后的0-9的数字，所以有10个输出的神经元。用同样的方法由隐藏层计算出输出层后，由于本程序的宗旨是预测数字，所以比较合适的偏差是计算机对于其认为图像为每个数字概率。在这里使用将输出层映射到sigmoid函数的方法，对于sigmoid函数的作用，将在优化的部分详尽解释。

图

具体代码：

oned\_fnn\_in = sampled\_input.reshape(sampled\_input.shape[0], sampled\_input.shape[1] \* sampled\_input.shape[2] \* sampled\_input.shape[3])

hid\_state = np.dot(train\_batch, in\_to\_hid\_weights)  
hid\_state = hid\_state + hid\_bias  
out\_state = np.dot(hid\_state, hid\_to\_out\_weights)  
out\_state = out\_state + out\_bias  
out\_state = 1 / (1 + np.exp(-out\_state))

### 输出层

输出层的作用很简单，将上层输出的神经网络求出的每个数概率中，选出最大的一项输出结果。

为了测试，也可以输出其他的结果，比如概率最高的N个数或保证一定概率的置信数组。

具体代码：

prediction = np.argmax(out\_state, axis=1)

### 权值更新

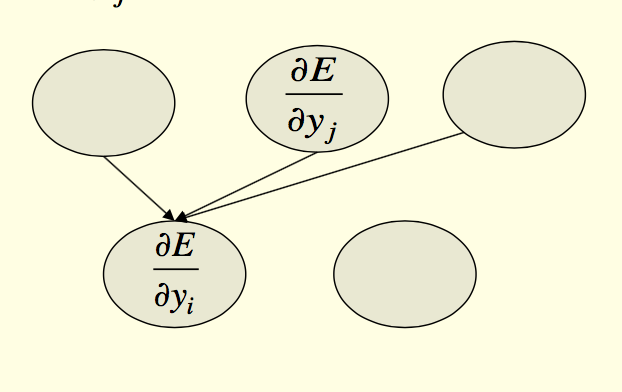
前文提到，神经元是通过梯度下降的方法来使自身变得准确的，而神经网络是通过其当中每一个神经元的梯度下降来提高整个神经网络的准确性的。相对于一个一个为神经元求其对整个神经网络残差的偏导数，利用偏导数的链式法则（）神经网络利用反向传播的方法来按层批量更新权值。

反向传播：

反向传播的基本思想是梯度下降，对于复杂的神经网络，我们无法通过解方程的方式得到每个权值的最佳值，但是我们可以通过求梯度的方式来得到每个神经元的每个权值在变化量足够小的时候其相对于最佳值的方向，对于复杂的神经网络，由于上层神经元的输出会与多个下层神经元进行连接，所以对于这样的神经元来说，其变化量其实是其所有连接的神经元对结果的影响和的加权值。相对于单独计算，反向传播大大提高了运算效率。

全连接神经网络的反向传播：

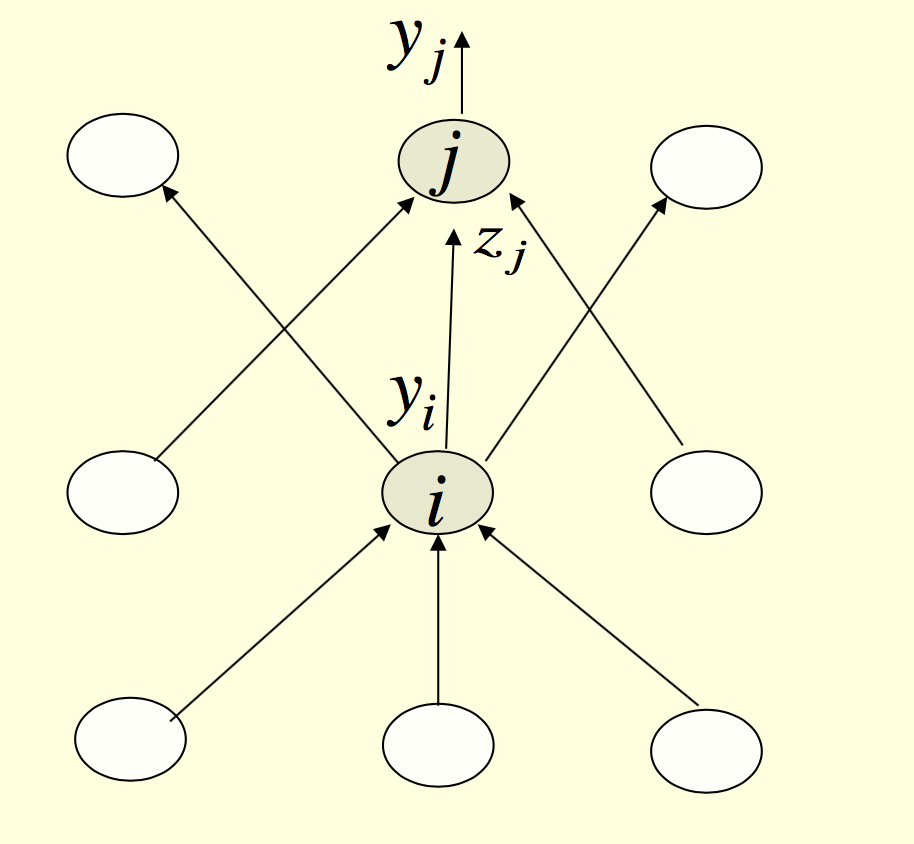
之所以叫反向传播，是因为这个方法是按照从输入到输出的顺序一层一层向前推进的，这样巧妙的利用了链式法则的优势。



在这里神经元j是输出层的神经元，由图可知，上一层神经元的偏导数实际上是由下一层与其连接的神经元的偏导数叠加而成。

我们假设此网络的偏差方程为方差：

那么输出层神经元j相对于偏差E的偏导数



对于输出层，上文提到，输出层神经元经常会用到像sigmoid或softmax的函数进行优化，所以这里神经元j的输入可能并不与输出成线性相关的关系：

在这里举例使用本算法的sigmoid神经元作为输出神经元：

则下一层的神经元i，因为对于下一层神经元j，神经元相当于对其做了权值Wij的‘贡献’，因此其相对于偏差E的偏导数可以理解为为上一层所有神经元的输入值偏导数的加权和：

对于每层神经元来说，以权值的角度看，可以理解成下层神经元是输入其中的权值的“以输入值为权值的加权和”那么权值的偏导数实际上就是其指向的神经元的偏导数于其对应输入值的积：

按此方法可以依次向前推进，依次求出全连接神经网络中输入层到隐藏层权值的偏导值。如果全连接层前面有其他的神经网络层，也需要求出其输入层的偏导值以进行下一步运算。

卷积神经网络的反向传播：

卷积神经网络的反向传播思想于全连接神经网络大同小异，其宗旨都是找到神经元或权值当把它们当成下一层输入的时候的权值，再用这个权值与其连接下一层的偏导数进行加权乘积。

图：

在本算法卷积神经网络中，由于在卷积之后有最大值池化的优化，所以在求偏导数时需要将池化中筛选掉的输入值同时筛选掉。筛选掉后对于每个卷积核的权值，找到与其进行加权乘积后的输入值，再进行点乘后得出其偏微分。

实现：

在本算法中，输出层为sigmoid神经元，其维度为批大小\*10，结构为：

根据前面推导的sigmoid神经元的偏导公式，输出层的偏导矩阵为：

通过输出层神经元偏导矩阵与隐藏层输出值矩阵的转置进行点乘可以得到隐藏层到输出层权值的偏导，其维度为隐层神经元个数\*输出神经元个数，与隐层神经元到输出神经元的权值矩阵相同：

由于偏移量没有权值，所以起偏导就等于其连接的神经元的偏导和：

通过输出层偏导矩阵与隐藏层到输出层权值转置进行点乘，得到隐藏层神经元的偏导矩阵，矩阵的维度为批大小\*隐层神经元个数，与隐层神经元矩阵相同：

通过同样的方法依次求出输入层到输出层权值偏导矩阵，输入层偏导矩阵，隐藏层偏移量偏导：

再利用全连接神经网络输入层的偏导来求卷积核的权值的偏导数：

本算法中，先利用之前记录下来的最大值的坐标与卷积神经网络的输入数据，合成一个维度与输入数据相同，只保留最大值池化（将池化没有选中的设为零）的数组。再直接用卷积核上的想要求出卷积的那个参数所有“划过”的点乘上其对应的输入向量，最后加和：

再将已经求出的所有的偏微分乘上学习率，用其对应的权值去减去求出的变化量，久完成了权值的更新。

具体代码：

*# bprop:err*err = out\_state - train\_label\_batch  
CE = (err \* err / 2).sum(axis=1)  
d\_Out = out\_state \* (1 - out\_state) \* err  
d\_hid\_to\_out = np.dot(hid\_state.transpose(), d\_Out)  
d\_hid = np.dot(d\_Out, hid\_to\_out\_weights.transpose())  
d\_in\_to\_hid = np.dot(train\_batch.transpose(), d\_hid)  
d\_in = np.dot(d\_hid, in\_to\_hid\_weights.transpose())  
  
*# update weights*del\_hid\_to\_out = -1 \* alpha \* d\_hid\_to\_out / batch\_size  
del\_in\_to\_hid = -1 \* alpha \* d\_in\_to\_hid / batch\_size  
hid\_to\_out\_weights += del\_hid\_to\_out  
in\_to\_hid\_weights += del\_in\_to\_hid  
  
hid\_bias += -1 \* alpha \* d\_hid  
out\_bias += -1 \* alpha \* d\_Out

d\_in = d\_in.reshape(d\_in.shape[0], num\_of\_fmap, int((28 - conv\_core + 1) / 2),  
 int((28 - conv\_core + 1) / 2))  
expd\_d\_in = np.zeros((d\_in.shape[0], d\_in.shape[1], d\_in.shape[2] \* 2, d\_in.shape[3] \* 2), dtype=np.float)  
*# print(d\_in.shape)*kr = [[1, 1], [1, 1]]  
**for** i **in** range(0, train\_data\_batch.shape[0]):  
 **for** j **in** range(0, num\_of\_fmap):  
 expd\_d\_in[i][j] = np.kron(d\_in[i][j], kr)  
*# print(expd\_d\_in[0][0])*expd\_d\_in = expd\_d\_in \* conved\_input\_maxloc  
*# print(expd\_d\_in[0][5])  
# print(train\_data\_batch)*d\_cov\_w = np.zeros((d\_in.shape[1], conv\_core, conv\_core), dtype=np.float)  
**for** i **in** range(0, train\_data\_batch.shape[0]):  
 **for** j **in** range(0, num\_of\_fmap):  
 **for** k **in** range(0, conv\_core):  
 **for** l **in** range(0, conv\_core):  
 d\_cov\_w[j][k][l] += sum(sum(  
 expd\_d\_in[i][j] \* two\_d\_input[i][k:k + expd\_d\_in.shape[2], l:l + expd\_d\_in.shape[3]]))in\_to\_conv\_weights += -alpha \* (d\_cov\_w.reshape(d\_cov\_w.shape[0], d\_cov\_w.shape[1] \* d\_cov\_w.shape[2]))

# 实验分析与优化

## 实验环境

本算法的实验基于python的交互式笔记本Jupyter，Jupyter是一个交互式的开源编程，学习与测试平台，其最大的一个优点是对变量的保存，在神经网络算法中，有些训练后的权值数据是通过几十分钟的训练得到的，如果每次调整都要重新训练的话实验效率将很低，在jupyter的交互式测试环境下，在不损失变量的值的情况下分小段调试代码，直观高效的完成对实验数据的测试。

### 硬件环境

MacBook Pro 2016

Intel Core i7 3.3GHz (2 Cores) CPU

16 GB 2133 MHz LPDDR3 Memory

Intel Iris Graphics 550 1536 MB

### 软件环境

操作系统：macOS Sierra 10.12.6

python版本：python3.6.0

python相关库版本：

ipython 6.0.0

jupyter-console 5.1.0

numpy 1.12.1

pandas 0.20.0

matplotlib 2.0.1

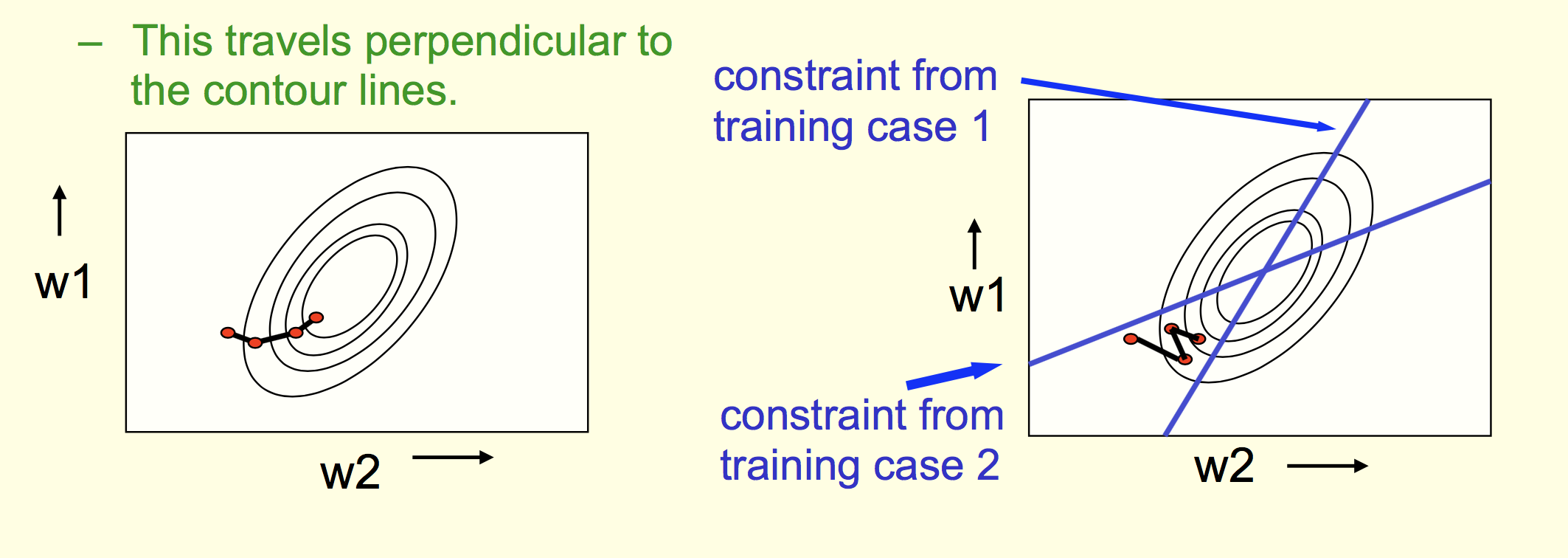
IDE: pyCharm Community Edition 2016.3.2

## 实验数据

## 实验结果与优化分析

在本算法中，对算法运算时间，准确率，效率，容错性等特性有影响的参数有很多，如卷积核大小，池化层的池化程度，学习率，有无偏移量，隐藏层的神经元数量，隐藏层的层数等。通过调整各个参数的数量，来对算法进行优化，下面通过实验与分析了解各个参数的作用与在本算法中的最佳选择：

### 批的大小（batch size）



在线上学习（每次只学习一个图像）中，由于对于复杂的神经网络，其残差函数比较负载，在梯度下降时，可能出现每次下降的方向不一样，出现zigzag的现象，

zigzag向量图：

通过批学习的方法，用同一组权值同时训练多组输入数据，将每组数据的变化量加和后更新权值，用这种方法可以通过抵消掉其他方向的重合部分，从而提高更新权值的效率。以下是在其它参数固定的情况下，批大小分别为1，10，100，1000时训练准确率与训练进度的图像和训练准确率与训练时间的图像：



由图像我们可以看出，在合理的批的大小范围内，在训练进度相同时，神经网络的准确率几乎是相同的，此时批的大小对训练精度的影响几乎可以忽略不计；但是在训练时间上可以出，在合理的批大小范围内，随着批大小的增大，训练的速度会明显提升。儿训练后的最终精度并不会受到明显的影响。但是当批的大小过大时（batch size=1000），由于每次更新的权值变化量积累过多，会造成过量更新，使权值无法接近最优点，造成训练失败，对于某些情况，可以用减少学习率的方法来解决这个问题。

### 训练次数（epoch）

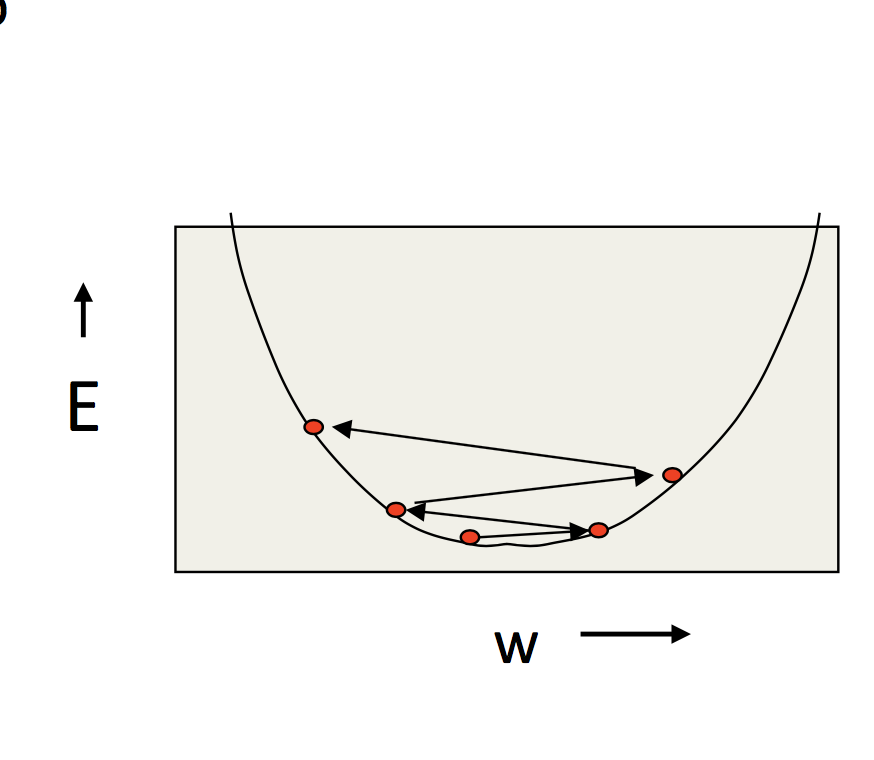
在机器学习的过程中，由于数据量有限且步长（学习率）较小，特别是当批尺寸比较大的时候，由于权值更新的次数有限，权值在一次训练过并没有达到最优解，这时候可以使用多次训练的方法使其充分学习，批尺寸越大的时候其达到较高精度所需要的训练次数就越多。在训练达到算法精度的极限后，算法的预测准确性不会再因为扩大训练次数而提高：



由图像可以看出，当批大小为1和10时，神经网络的准确率在第3次训练后不再增加，当批大小为200时，神经网络的准确率在第5次训练后不再增加。

### 学习率（learning rate）

因为每次权值的更新变化量都是其偏导与学习率的乘积，所以学习率在一定程度上直接决定着神经网络学习的速度。对于过小的学习率，神经网络对训练数据会不能有效利用，神经网络的学习速度会很慢。而对于过大的学习率，由于每次更新的权值过大，会出现“跳过”最优解的情况，而离最优解更远之后会造成其所在权值偏导增大，求出的权值变化量更大，进一步远离最优解，最后造成学习失败。

慢图

在实验中，我们分别使用学习率为0.001，0.01，0.1，0.5四个不同的学习率对神经网络进行训练，下面是学习进度与神经网络识别准确率的关系：

**

由图像可以看出，对于过小的学习率，学习速度将非常慢，算法的效率将很低，当学t率很高时，会使神经网络在接近最优解时出现“跳过”最优解的情况，使神经网络的准确率停留在一个较低的位置，当学习率很高时，神经网络的变化量过大，导致和权值随机变化的效果，造成精度无法提升，学习失败。现代算法中常使用动态学习率的方法，既保留了高学习率学习速度快的优势，又保留了低学习率最终精度高的优势，由于比较复杂，在本算法中暂不考虑。

### 神经元数量

这里的神经元数量指的是全连接层隐藏神经元的数量，隐藏层神经元的数量决定着神经网络的灵活性，隐藏层神经元数量越多，神经网络越复杂，神经网络越能学习出复杂的模型来识别输入的数据。但过多的隐藏层神经元有两个缺点：一个是由于全连接神经网络的权值是输出层和输出层神经元数量与隐藏层神经元数量的乘积，过多的隐藏层神经元会让计算量指数增加，使训练速度变慢；第二个是过多的隐藏层神经元会造成过度拟合（overfitting）即神经网络过于灵活，使其训练的结果过于贴近训练数据而没有容错，其训练的结果仅仅高度拟合训练的数据，而无法对与训练数据稍有不同的测试数据进行准确的识别：

正常与过度拟合图：

在实验中，我们分别对隐藏层神经元数量为1，10，2000的全连接神经网络隐藏层神经元数量的神经网络进行相同训练数据的训练，下面分别是学习进度与神经网络对训练数据识别准确率的关系和学习进度与神经网络对测试数据识别准确率的关系：



对于只有一个隐藏层神经元的网络，由于其灵活性太差，不能完成对10个数的分类识别，造成识别失败，对于有2000个神经元的网络，由于其神经网络隐藏层层过于庞大，造成其对训练数据的过拟合，使其对原数据的识别准确率极高而对未在原数据出现过的训练数据识别率较低。由于本数据集训练数据与测试数据较相似，所以在测试中均出现测试数据正确率与训练数据正确率“同步”上升与下降的现象。值得提到的是，拥有2000个隐藏层神经元的神经网络训练总时间为2166.36秒，为100个隐藏神经元的神经网络（159.93秒）的近20倍。综上，神经网络不能通过盲目增加隐藏神经元的方式来提高识别的精度与效率，反而会适得其反。

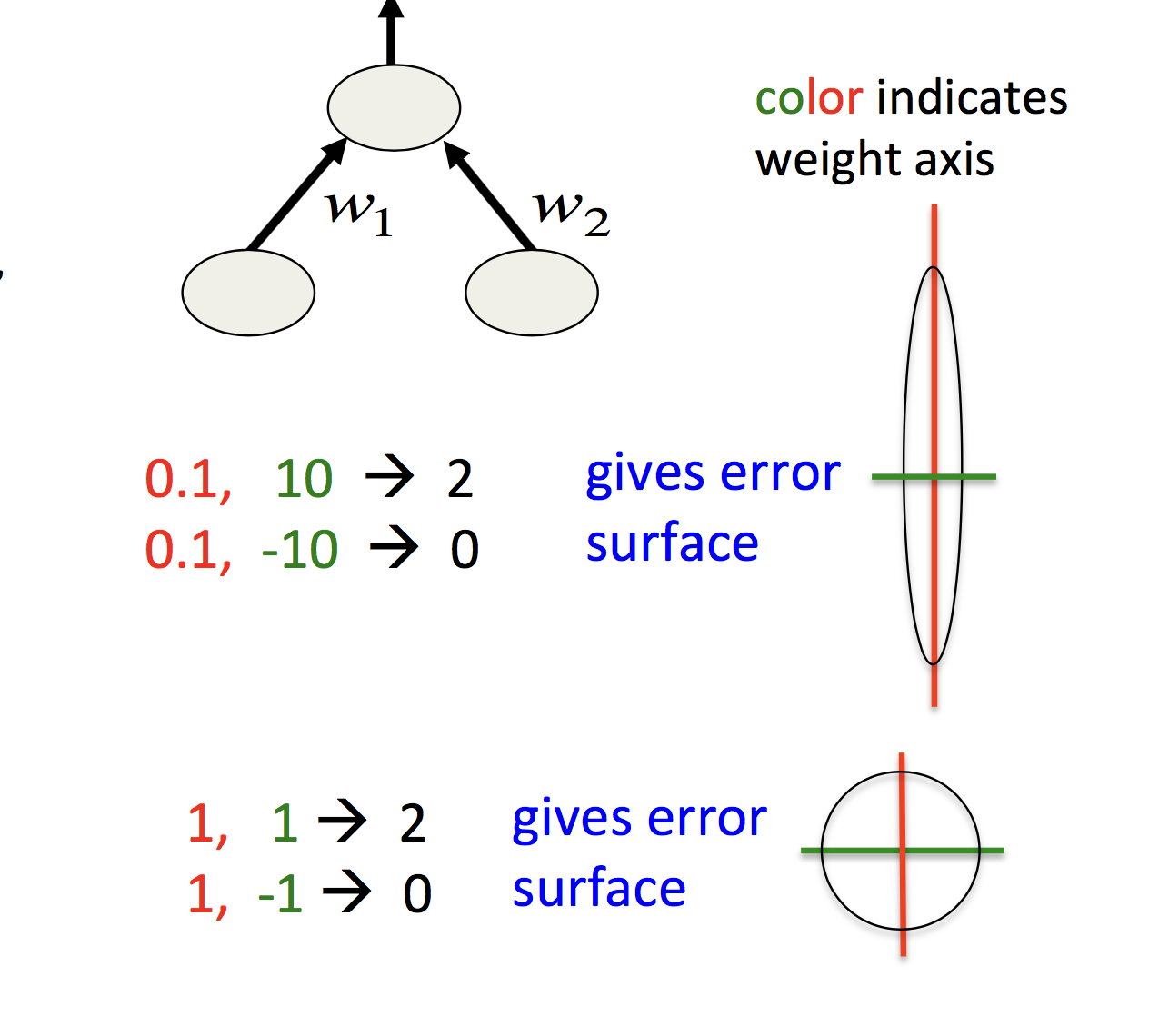
### 卷积层的作用

卷积神经网络会在大幅减少神经网络参数个数的同时，由于其对图像进行了预处理，使神经网络对图像中如数字位置，图像噪点等影响的适用性增强，同时减少神经网络的运算量，加快学习的效率。在实验中，我们别用有卷积神经网络的与无卷积神经网络的网络分别对同一组数据进行学习，得出学习进度与准确率的关系：



可以看出，通过卷积神经网络的处理，神经网络对图像的训练效率有所增加，训练达到相同准确率所需要的训练数据有所减小，因此卷积神经网络在图像数据比较匮乏时也可以发挥很大的作用。另外，由于经过卷积和池化，图像无可避免的有信息的损失，所以最终的识别准确性不如全连接神经网络。由于卷积神经网络的运算速度很依赖显卡的加速，由于运行环境的原因无法达成，所以本文暂不在运行时间方面进行二者的比较。

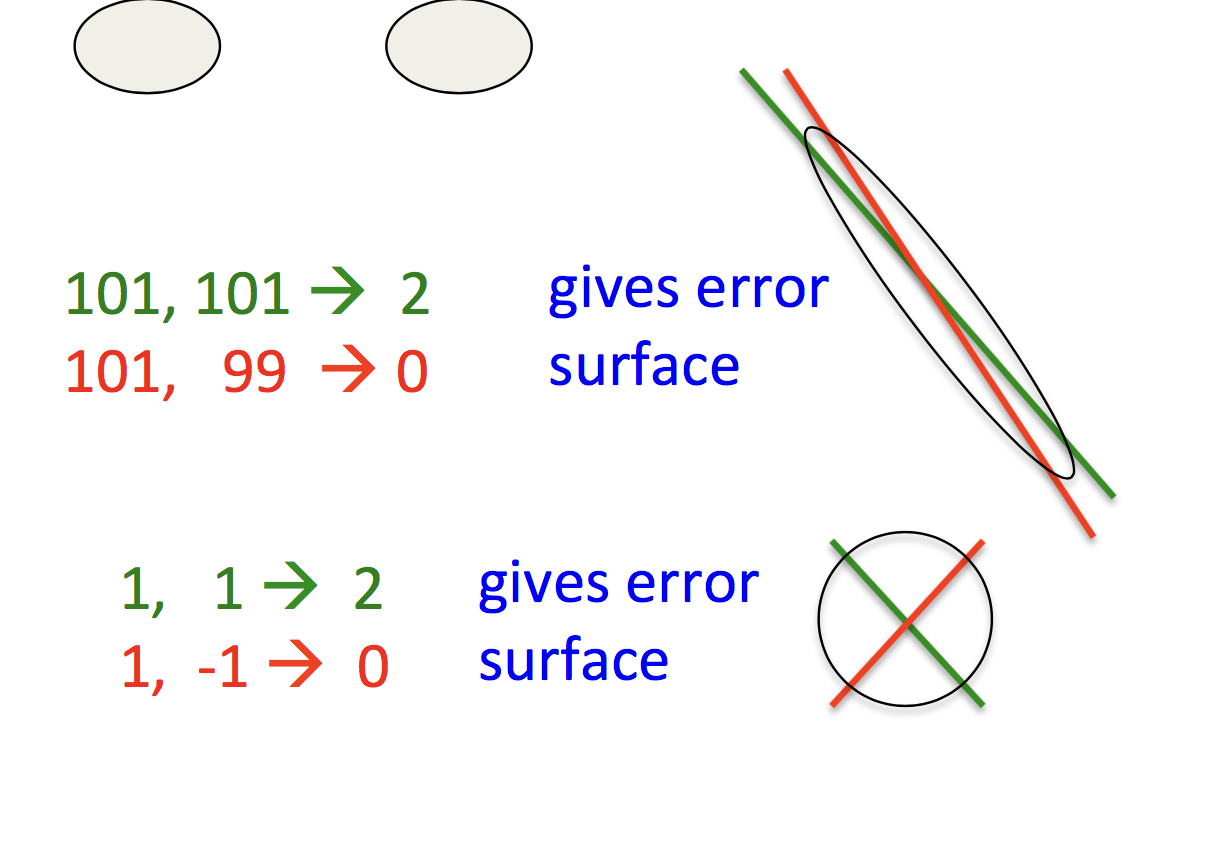
### 数据标准化

在训练过程中，由于训练数据可能有很多数据组成，比如房屋价格的预测算法，可能训练数据中同时有房屋的历史价格（百万单位）与房屋的窗户数（一到几十的单位），这时如果不加处理直接将数据放入神经网络进行训练，神经网络进行梯度下降时的残差函数会在x轴和y轴上的差别很大，假设x轴上的数量级远大于y轴上的数量级，那么每次进行梯度下降时，其x轴方向的梯度必然远小于y轴上的梯度，使梯度下降的方向十分接近y轴的方向，这样会出现在y轴方向来回摆动而在x轴方向移动很慢的现象，使学习的速度急剧下降，效率极低。

为了解决这一问题，可以训练之前，对训练数据与测试数据使用同样的方法，将数据中每种数字都等比例或使用合适的非线性方程转化为(-1,-1)范围的数量级。统一后的数量级的在残差函数上因为数量级相同，会在x与y轴上较接近，避免了沿某一坐标轴来回摆动的现象发生。在本算法中由于数据（像素灰度值）本身在同一数量级中，标准化对算法的提升效果不明显，就暂不进行试验性分析。

### 偏移量的作用

偏移量在神经网络中的作用与标准化相似，如果训练中有相关性较强的两组数据，比如房屋总面积与房屋的可用面积，或图片相邻两个像素的灰度值。当出现这种情况时，残差函数会在y=x或y=-x方向被拉的很长，与上一节遇到的情况相同，这时残差函数的梯度下降的方向会十分接近y=x或y=-x并在这个方向，使权值在这个方向来回摆动而不能接近最低点。通过使用偏移量，将相近的权值同时加上或剪掉一个常数的方法，将其符号调整为不同的，这样会使被拉长的残差函数恢复在各个方向与原点距离数量级相近的状态。



# 论文的总结与展望

# 致谢

# 参考文献

# 附录