摘要 推荐系统在日常的网络应用中无处不在,比如网上购物、网上买书、新闻 app、社交网络、音乐网站、电影网站等等等等,有人的地方就有推荐。根据个人的喜好,相同喜好人群的习惯等信息进行个性化的内容推荐。比如打开新闻类的 app,因为有了个性化的内容,每个人看到的新闻首页都是不一样的。协同过滤是推荐系统应用较广泛的技术,该方法搜集用户的历史记录、个人喜好等信息,计算与其他用户的相似度,利用相似用户的评价来预测目标用户对特定项目的喜好程度。优点是会给用户推荐未浏览过的项目,缺点呢,对于新用户来说,没有任何与商品的交互记录和个人喜好等信息,存在冷启动问题,导致模型无法找到相似的用户或商品。为了解决冷启动的问题,通常的做法是对于刚注册的用户,要求用户先选择自己感兴趣的话题、群组、商品、性格、喜欢的音乐类型等信息,本文尝试使用CNN、RNN 做推荐系统,发现可取得较好的效果.

#### 关键词 推荐系统 卷积神经网络 循环神经网络

## 1 引言

推荐系统是一种信息过滤系统,用于预测用户对物品的"评分"或"偏好",其近年来非常流行,应用于各行各业。推荐的对象包括:电影、音乐、新闻、书籍、学术论文、搜索查询、分众分类、以及其他产品。也有一些推荐系统专门为寻找专家、合作者、笑话、餐厅、美食、金融服务、生命保险、网路交友,以及 Twitter 页面设计。

推荐系统产生推荐列表的方式通常有两种: 协同过滤以及基于内容推荐, 或者基于个性化推荐。 协同过滤方法根据用户历史行为 (例如其购买的、选择的、评价过的物品等) 结合其他用户的相似决策建立模型。这种模型可用于预测用户对哪些物品可能感兴趣 (或用户对物品的感兴趣程度)。基于内容推荐利用一些列有关物品的离散特征,推荐出具有类似性质的相似物品。两种方法经常互相结合(参考混合推荐系统)。在当下深度学习极为流行的情况下,也出现了一些利用深度学习做推荐系统的方法。本文提出利用 CNN 及 RNN 做推荐系统的方法。

## 2 推荐系统常用方法

### 2.1 基于协同过滤的推荐系统[1]

协同过滤(英语: Collaborative Filtering),简单来说是利用某兴趣相投、拥有共同经验之群体的喜好来推荐用户感兴趣的信息,个人透过合作的机制给予信息相当程度的回应(如评分)并记录下来以达到过滤的目的进而帮助别人筛选信息,回应不一定局限于特别感兴趣的,特别不感兴趣信息的纪录也相当重要。

### 2.1.1 以用户为基础(User-based)的协同过滤

用相似统计的方法得到具有相似爱好或者兴趣的相邻用户,所以称之为以用户为基础(User-based)的协同过滤或基于邻居的协同过滤(Neighbor-based Collaborative Filtering)。 方法步骤:

- 1) 收集用户信息: 收集可以代表用户兴趣的信息。一般的网站系统使用评分的方式或是给予评价,这种方式被称为"主动评分"。另外一种是"被动评分",是根据用户的行为模式由系统代替用户完成评价,不需要用户直接打分或输入评价数据。电子商务网站在被动评分的数据获取上有其优势,用户购买的商品记录是相当有用的数据。
- 2)最近邻搜索(Nearest neighbor search, NNS):以用户为基础(User-based)的协同过滤的出发点是与用户兴趣爱好相同的另一组用户,就是计算两个用户的相似度。例如:查找 n

个和 A 有相似兴趣用户,把他们对 M 的评分作为 A 对 M 的评分预测。一般会根据数据的不同选择不同的算法,当前较多使用的相似度算法有 Pearson Correlation Coefficient、Cosine-based Similarity、Adjusted Cosine Similarity。

3)产生推荐结果:有了最近邻集合,就可以对目标用户的兴趣进行预测,产生推荐结果。依据推荐目的的不同进行不同形式的推荐,较常见的推荐结果有 Top-N 推荐和关系推荐。Top-N 推荐是针对个体用户产生,对每个人产生不一样的结果,例如:透过对 A 用户的最近邻用户进行统计,选择出现频率高且在 A 用户的评分项目中不存在的,作为推荐结果。关系推荐是对最近邻用户的记录进行关系规则(association rules)挖掘。

## 2.1.2 以项目为基础(Item-based)的协同过滤

以用户为基础的协同推荐算法随着用户数量的增多,计算的时间就会变长,所以在 2001 年 Sarwar 提出了基于项目的协同过滤推荐算法(Item-based Collaborative Filtering Algorithms)。以项目为基础的协同过滤方法有一个基本的假设"能够引起用户兴趣的项目,必定与其之前评分高的项目相似",透过计算项目之间的相似性来代替用户之间的相似性。方法步骤:

- 1) 收集用户信息:同以用户为基础(User-based)的协同过滤。
- 2)针对项目的最近邻搜索: 先计算已评价项目和待预测项目的相似度,并以相似度作为权重,加权各已评价项目的分数,得到待预测项目的预测值。例如: 要对项目 A 和项目 B 进行相似性计算,要先找出同时对 A 和 B 打过分的组合,对这些组合进行相似度计算,常用的算法同以用户为基础(User-based)的协同过滤。
- 3)产生推荐结果:以项目为基础的协同过滤不用考虑用户间的差别,所以精度比较差。但是却不需要用户的历史数据,或是进行用户识别。对于项目来讲,它们之间的相似性要稳定很多,因此可以离线完成工作量最大的相似性计算步骤,从而降低了在线计算量,提高推荐效率,尤其是在用户多于项目的情形下尤为显著。

#### 2.1.3 以模型为基础(Model- based)的协同过滤

以用户为基础(User-based)的协同过滤和以项目为基础(Item-based)的协同过滤系统称为以记忆为基础(Memory based)的协同过滤技术,他们共有的缺点是数据稀疏,难以处理大数据量影响即时结果,因此发展出以模型为基础的协同过滤技术。 以模型为基础的协同过滤(Model-based Collaborative Filtering)是先用历史数据得到一个模型,再用此模型进行预测。以模型为基础的协同过滤广泛使用的技术包括 Latent Semantic Indexing、Bayesian Networks...等,根据对一个样本的分析得到模型。

## 2.2 卷积神经网络[2]

基于协同过滤的推荐系统优点是会给用户推荐未浏览过的项目,缺点呢,对于新用户来说,没有任何与商品的交互记录和个人喜好等信息,存在冷启动问题,导致模型无法找到相似的用户或商品。

卷积神经网络(Convolutional Neural Network, CNN)是一种前馈神经网络,它的人工神经元可以响应一部分覆盖范围内的周围单元,对于大型图像处理有出色表现。

卷积神经网络由一个或多个卷积层和顶端的全连通层(对应经典的神经网络)组成,同时也包括关联权重和池化层(pooling layer)。这一结构使得卷积神经网络能够利用输入数

据的二维结构。与其他深度学习结构相比,卷积神经网络在图像和语音识别方面能够给出更好的结果。这一模型也可以使用反向传播算法进行训练。相比较其他深度、前馈神经网络,卷积神经网络需要考量的参数更少,使之成为一种颇具吸引力的深度学习结构,本文尝试利用卷积神经网络利用 MovieLens 数据集完成电影推荐的任务。,发现取得了不错的效果。

#### 2.2.1 卷积层

卷积层是一组平行的特征图(feature map),它通过在输入图像上滑动不同的卷积核并运行一定的运算而组成。此外,在每一个滑动的位置上,卷积核与输入图像之间会运行一个元素对应乘积并求和的运算以将感受野内的信息投影到特征图中的一个元素。这一滑动的过程可称为步幅 Z\_s,步幅 Z\_s 是控制输出特征图尺寸的一个因素。卷积核的尺寸要比输入图像小得多,且重叠或平行地作用于输入图像中,一张特征图中的所有元素都是通过一个卷积核计算得出的,也即一张特征图共享了相同的权重和偏置项。

### 2.2.2 线性整流层

线性整流层(Rectified Linear Units layer, ReLU layer)使用线性整流(Rectified Linear Units, ReLU){\displaystyle f(x)=\max(0,x)}\_\_\_作为这一层神经的激励函数(Activation function)。它可以增强判定函数和整个神经网络的非线性特性,而本身并不会改变卷积层。

事实上,其他的一些函数也可以用于增强网络的非线性特性,如双曲正切函数  ${\displaystyle\ f(x)=\tanh(x)}_, {\displaystyle\ f(x)=|\tanh(x)|}_, 或者 Sigmoid 函数 {\displaystyle\ f(x)=(1+e^{-x})^{-1}}_, 相比其它函数来说,ReLU 函数更受青睐,这是因为它可以将神经网络的训练速度提升数倍,而并不会对模型的泛化准确度造成显著影响。$ 

### 2.2.3 池化层

池化(Pooling)是卷积神经网络中另一个重要的概念,它实际上是一种形式的降采样。有多种不同形式的非线性池化函数,而其中"最大池化(Max pooling)"是最为常见的。它是将输入的图像划分为若干个矩形区域,对每个子区域输出最大值。直觉上,这种机制能够有效地原因在于,在发现一个特征之后,它的精确位置远不及它和其他特征的相对位置的关系重要。池化层会不断地减小数据的空间大小,因此参数的数量和计算量也会下降,这在一定程度上也控制了过拟合。通常来说,CNN的卷积层之间都会周期性地插入池化层。

池化层通常会分别作用于每个输入的特征并减小其大小。当前最常用形式的池化层是每隔 2个元素从图像划分出{\displaystyle 2\times 2}。的区块,然后对每个区块中的 4 个数取最大值。这将会减少 75%的数据量。

除了最大池化之外,池化层也可以使用其他池化函数,例如"平均池化"甚至"L2-范数池化"等。过去,平均池化的使用曾经较为广泛,但是最近由于最大池化在实践中的表现更好,平均池化已经不太常用。

由于池化层过快地减少了数据的大小,当前文献中的趋势是使用较小的池化滤镜,甚至不再使用池化层。

#### 2.2.4 损失函数层

损失函数层(loss layer)用于决定训练过程如何来"惩罚"网络的预测结果和真实结果之间的差异,它通常是网络的最后一层。各种不同的损失函数适用于不同类型的任务。例如,Softmax 交叉熵损失函数常常被用于在 K 个类别中选出一个,而 Sigmoid 交叉熵损失函数常常用于多个独立的二分类问题。欧几里德损失函数常常用于结果取值范围为任意实数的问

## 2.3 循环神经网络[3]

循环神经网络(Recurrent Neural Network, RNN)是一类以序列(sequence)数据为输入,在序列的演进方向进行递归(recursion)且所有节点(循环单元)按链式连接的递归神经网络(recursive neural network)

RNNs 的目的使用来处理序列数据。在传统的神经网络模型中,是从输入层到隐含层再到输出层,层与层之间是全连接的,每层之间的节点是无连接的。但是这种普通的神经网络对于很多问题却无能无力。例如,你要预测句子的下一个单词是什么,一般需要用到前面的单词,因为一个句子中前后单词并不是独立的。RNNs 之所以称为循环神经网路,即一个序列当前的输出与前面的输出也有关。具体的表现形式为网络会对前面的信息进行记忆并应用于当前输出的计算中,即隐藏层之间的节点不再无连接而是有连接的,并且隐藏层的输入不仅包括输入层的输出还包括上一时刻隐藏层的输出。理论上,RNNs 能够对任何长度的序列数据进行处理。但是在实践中,为了降低复杂性往往假设当前的状态只与前面的几个状态相关,下图便是一个典型的 RNNs

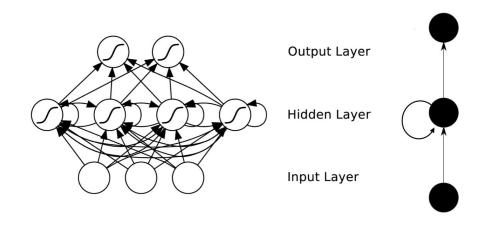


图 1 RNN 网络

RNNs 包含输入单元(Input units), 输入集标记为{x0,x1,...,xt,xt+1,...} {x0,x1,...,xt,xt+1,...}, 而输出单元(Output units)的输出集则被标记为{y0,y1,...,yt,yt+1....} {y0,y1,...,yt,yt+1....}。RNNs 还包含隐藏单元(Hidden units), 我们将其输出集标记为

{s0,s1,...,st,st+1,...}{s0,s1,...,st,st+1,...},这些隐藏单元完成了最为主要的工作。你会发现,在图中:有一条单向流动的信息流是从输入单元到达隐藏单元的,与此同时另一条单向流动的信息流从隐藏单元到达输出单元。在某些情况下,RNNs会打破后者的限制,引导信息从输出单元返回隐藏单元,这些被称为"Back Projections",并且隐藏层的输入还包括上一隐藏层的状态,即隐藏层内的节点可以自连也可以互连。

可将循环神经网络进行展开成一个全神经网络。例如,对一个包含 5 个单词的语句,那么展开的网络便是一个五层的神经网络,每一层代表一个单词。对于该网络的计算过程如下:

1)xt 表示第 t,t=1,2,3...t,t=1,2,3...步(step)的输入。比如,x1x1 为第二个词的 one-hot 向量(根据上图, x0x0 为第一个词);

2)PS: 使用计算机对自然语言进行处理, 便需要将自然语言处理成为机器能够识别的符

号,加上在机器学习过程中,需要将其进行数值化。而词是自然语言理解与处理的基础,因此需要对词进行数值化,词向量(Word Representation,Word embeding)[1]便是一种可行又有效的方法。何为词向量,即使用一个指定长度的实数向量 v 来表示一个词。有一种种最简单的表示方法,就是使用 One-hot vector 表示单词,即根据单词的数量|V|生成一个|V|\*1的向量,当某一位为一的时候其他位都为零,然后这个向量就代表一个单词。缺点也很明显:

- 1)由于向量长度是根据单词个数来的,如果有新词出现,这个向量还得增加,麻烦! (Impossible to keep up to date);
  - 2) 主观性太强(subjective)
  - 3) 单词过多
- 4) 很难计算单词之间的相似性。现在有一种更加有效的词向量模式,该模式是通过神经网或者深度学习对词进行训练,输出一个指定维度的向量,该向量便是输入词的表达。如word2vec。
- 3、st 为隐藏层的第 t 步的状态,它是网络的记忆单元。 st 根据当前输入层的输出与上一步隐藏层的状态进行计算。st=f(Uxt+Wst-1)st=f(Uxt+Wst-1),其中 ff 一般是非线性的激活函数,如 tanh 或 ReLU,在计算 s0s0 时,即第一个单词的隐藏层状态,需要用到 s-1s-1,但是其并不存在,在实现中一般置为 0 向量;
  - 4、ot 是第 t 步的输出,如下个单词的向量表示,ot=softmax(Vst)ot=softmax(Vst). 需要注意的是:

可以认为隐藏层状态 st 是网络的记忆单元. st 包含了前面所有步的隐藏层状态。而输出层的输出 ot 只与当前步的 st 有关,在实践中,为了降低网络的复杂度,往往 st 只包含前面若干步而不是所有步的隐藏层状态;

在传统神经网络中,每一个网络层的参数是不共享的。而在 RNNs 中,每输入一步,每一层各自都共享参数 U,V,WU,V,W。其反应者 RNNs 中的每一步都在做相同的事,只是输入不同,因此大大地降低了网络中需要学习的参数;这里并没有说清楚,解释一下,传统神经网络的参数是不共享的,并不是表示对于每个输入有不同的参数,而是将 RNN 是进行展开,这样变成了多层的网络,如果这是一个多层的传统神经网络,那么 xt 到 st 之间的 U 矩阵与xt+1 到 st+1 之间的 UU 是不同的,而 RNNs 中的却是一样的,同理对于 s 与 s 层之间的 W、s 层与 o 层之间的 V 也是一样的。

上图中每一步都会有输出,但是每一步都要有输出并不是必须的。比如,我们需要预测一条语句所表达的情绪,我们仅仅需要关系最后一个单词输入后的输出,而不需要知道每个单词输入后的输出。同理,每步都需要输入也不是必须的。RNNs 的关键之处在于隐藏层,隐藏层能够捕捉序列的信息。

#### 2.4 word2vec

#### 2.4.1 词向量

词向量具有良好的语义特性,是表示词语特征的常用方式。词向量每一维的值代表一个具有一定的语义和语法上解释的特征。所以,可以将词向量的每一维称为一个词语特征。词向量具有多种形式,distributed representation 是其中一种。一个 distributed representation 是一个稠密、低维的实值向量。distributed representation 的每一维表示词语的一个潜在特征,

该特 征捕获了有用的句法和语义特性。可见,distributed representation 中的 distributed 一词体现了词向量这样一个特点:将词语的不同句法和语义特征分布到它的每一个维度去表示。

#### 2.4.1 word2vec

Word2vec,是一群用来产生词向量的相关模型。这些模型为浅而双层的神经网络,用来训练以重新建构语言学之词文本。网络以词表现,并且需猜测相邻位置的输入词,在word2vec 中词袋模型假设下,词的顺序是不重要的。训练完成之后,word2vec 模型可用来映射每个词到一个向量,可用来表示词对词之间的关系,该向量为神经网络之隐藏层。

## 3 基于循环卷积神经网络的推荐实验结果与分析

本文采用对 userid、occupation、movieid、age、gender 做循环神经网络预测、对电影名做文本卷积神经网络预测,发现可取得好的电影推荐效果。

#### 3.1 实验数据

本文采用 公开的 MovieLens 数据集作为实验数据集

## 3.2 实验方法

### 3.2.1 数据的预处理

本文针对 MovieLens 数据集采用一下思路进行数据预处理

表 1 MovieLens 数据集操作

属性名	预处理操作
UserID	不变
Occupation	不变
MovieID	不变
Gender	将'F'和'M'转换成0和1
Age	转换成7个连续数字0~6
Genres	转成数字。首先将 Genres 中的类别转成字符 串到数字的字典,然后再将每个电影的 Genres 字段转成数字列表,因为有些电影是 多个 Genres 的组合。
Title	处理方式跟 Genres 字段一样,首先创建文本 到数字的字典,然后将 Title 中的描述转成数 字的列表。另外 Title 中的年份也需要去掉

注: Genres 和 Title 字段需要将长度统一,这样在神经网络中方便处理。空白部分用'< PAD >' 对应的数字填充

### 3.2.2 模型设计

本文利用循环神经网络提取用户特征、利用循环神经网络及文本卷积网络提取电影特征,最终利用两个特征生成预测结果。

## 模型具体设计如下:

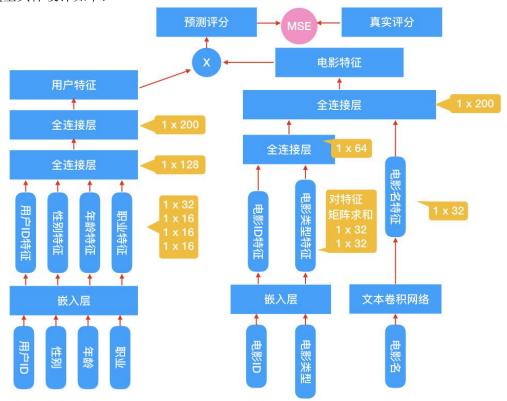


图 2 一种新的电影推荐方法模型架构

#### 1、循环神经网络设计如下:

通过研究数据集中的字段类型,本文发现有一些是类别字段,通常的处理是将这些字段转成one hot 编码,但是像 UserID、MovieID 这样的字段就会变成非常的稀疏,输入的维度急剧膨胀,这是本文不愿意见到的,所以在预处理数据时将这些字段转成了数字,本文用这个数字当做嵌入矩阵的索引,在网络的第一层使用了嵌入层,维度是(N,32)和(N,16)。 这里的思想其实和 word2vec 比较类似。本文会对用户或者电影的每个属性都指定一个特征维度空间,这就好比本文在自然语言处理中对每个单词指定特征维度空间。本文将用到的属性的特征维度设置为了 32 或者 16.

电影类型的处理要多一步,有时一个电影有多个电影类型,这样从嵌入矩阵索引出来是一个(n,32)的矩阵,因为有多个类型嘛,本文要将这个矩阵求和,变成(1,32)的向量。

电影名的处理比较特殊,没有使用循环神经网络,而是用了文本卷积网络,下文会进行说明。

从嵌入层索引出特征以后,将各特征传入全连接层,将输出再次传入全连接层,最终分别得到(1,200)的用户特征和电影特征两个特征向量。

本文的目的就是要训练出用户特征和电影特征,在实现推荐功能时使用。得到这两个特征以后,就可以选择任意的方式来拟合评分了。我使用了两种方式,一个是上图中画出的将两个特征做向量乘法,将结果与真实评分做回归,采用 MSE 优化损失。因为本质上这是一个回归问题,另一种方式是,将两个特征作为输入,再次传入全连接层,输出一个值,将输出值回归到真实评分,采用 MSE 优化损失。

2、用于电影名文本处理的的卷积神经网络,介绍如下

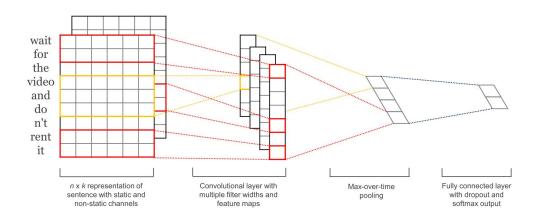


图 3 Kim Yoon 的文本卷积网络架构

本文采用了 Kim Yoon 14 年[4]的工作,用于文本的卷积神经网络实现对电影名的处理

网络的第一层是词嵌入层,由每一个单词的嵌入向量组成的嵌入矩阵。下一层使用多个不同尺寸(窗口大小)的卷积核在嵌入矩阵上做卷积,窗口大小指的是每次卷积覆盖几个单词。这里跟对图像做卷积不太一样,图像的卷积通常用 2x2、3x3、5x5 之类的尺寸,而文本卷积要覆盖整个单词的嵌入向量,所以尺寸是(单词数,向量维度),比如每次滑动 3 个,4 个或者 5 个单词。第三层网络是 max pooling 得到一个长向量,最后使用 dropout 做正则化,最终得到了电影 Title 的特征。

## 3.3 实验结果

## 3.3.1 模型训练结果

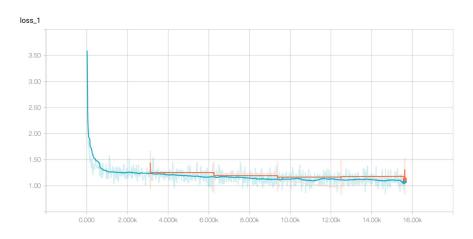


图 4 模型训练效果

## 3.3.2 模型用于推荐同类型的电影

```
n [38]: recommend_same_type_movie(1401, 20)

INFO:tensorflow:Restoring parameters from ./save
您看的电影是: [1401 'Ghosts of Mississippi (1996)' 'Drama']
以下是给您的推荐:
1123
[1139 'Everything Relative (1996)' 'Drama']
1380
[1401 'Ghosts of Mississippi (1996)' 'Drama']
426
[430 'Calendar Girl (1993)' 'Drama']
3125
[3194 'Way We Were, The (1973)' 'Drama']
795
[805 'Time to Kill, A (1996)' 'Drama']
Out[38]: {426, 795, 1123, 1380, 3125}
```

图 5 模型预测展示 1

## 3.3.3 模型用于推荐用户喜欢的电影

```
n [40]: recommend_your_favorite_movie(234, 10)

INFO:tensorflow:Restoring parameters from ./save
以下是给您的推荐:
523
[527 "Schindler's List (1993)" 'Drama|War']
1132
[1148 'Wrong Trousers, The (1993)' 'Animation|Comedy']
2836
[2905 'Sanjuro (1962)' 'Action|Adventure']
3228
[3297 'With Byrd at the South Pole (1930)' 'Documentary']
2495
[2564 'Empty Mirror, The (1999)' 'Drama']

Dut[40]: [523, 1132, 2495, 2836, 3228]
```

图 6 模型预测展示 2

## 3.3.4 模型用于推荐看过这个电影的用户还看了(喜欢)哪些电影

图 7 模型预测展示 3

## 4 结论与展望

本文提出一种新的用于电影推荐的模型架构,通过在 Movielens 数据集上进行验证,发现可取的好的电影推荐效果。

## 未来本文可尝试以下方法对本文模型进行改进

## 表 3 模型改进方法

可行操作	
1. 加上年份信息,看看是否影响推荐效果。	
2. GBDT(lightGBM,xgboost)。	
3. 电影类型不使用 sum, 使用其他方式来描述电影特征, 获得更好地效果。	
4. 尝试随机采样。	
5. 将用户的所有属性都设置为 32 特征,而不是有的是 32, 有的是 16。	
6. 将电影特征的 dropout 加到拼接好的电影特征上,而不是加到 title 的特征上。	
7. 拼接的用户矩阵没有使用 dropout, 试着将用户特征和电影特征都加上 dropout 看看最终的性能是否提升。	

# 参考文献

[1] 维基百科-推荐系统

8. 尝试使用 tensorflow 自己的 batch 方法。

- [2] 维基百科-卷积神经网络
- [3] 维基百科-循环神经网络
- [4] Kim Y. Convolutional neural networks for sentence classification[J]. arXiv preprint arXiv:1408.5882, 2014.

代码见 https://github.com/TianhaoFu/Recommendation