

# 【概念篇】个性化推荐系统那些绕不开的经典问题

2018-03-07 刑无刀



## 【概念篇】个性化推荐系统那些绕不开的经典问题

朗读人：黄洲君 11'17" | 5.17M

推荐系统发展到了今天，已经出现了一些常见的问题，一部分已经有很好的解决方案，另外一部分却还没有通用解决方案，需要根据实际情况做一下具体的分析。

今天我来和你聊一聊这些问题。我会首先讲讲一些推荐系统中的问题模式，然后再专门说一些需要面对的具体问题。

### 推荐系统的问题模式

我们知道，推荐系统的使命是为用户和物品建立连接，建立的方式是提前找出那些隐藏的连接呈现给用户，这是一个预测问题；所以推荐系统的预测问题模式，从达成的连接目标角度区分，有两大类：

1. 评分预测；
2. 行为预测。

因为评分和行为是用户对推荐结果的两类反馈，我们给他们推荐了一个或多个物品，目的是希望他们“消费”，这种消费反应在用户行为上，比如“点击查看”，信息咨询类的还有“阅读完成”，视频音乐类的有“播放完成”，电商类的“加入购物车”等。

整个行为呈现一个漏斗形状，从曝光到最终消费完成。最后在用户完成消费后，产品方一般还希望他们告诉自己消费的体验，这时候就有评分了；所以不同推荐系统的任务也不同，有的直接去预测用户如果消费完之后会给多少评分，更多的推荐系统则会分层，致力于预测用户的行为。下面我分别详细说一下这两类问题。

## 评分预测

评分预测相关算法模型研究的兴盛，最大的助攻是 Netflix 举办的推荐算法大赛。

评分预测要干的事情是这样的：假如用户消费完一个物品之后会给出一个打分，比如通常是 1~5 分，或者有的网站用星星的颗数表示，也是一样。

我们就想能不能提前预测一个用户对每一个物品会打多少分，找出那些他可能会打高分，但是还没消费的物品，然后装作若无其事地呈现在他面前，惊不惊喜，意不意外？

说干就干，怎么干呢？正如王小波给李银河写的信那样：不能胡干。一个朴素的思想是：建立一个模型，这个模型会给用户历史上打过分的物品去预测分数。

预测分数和实际分数之间会有误差，我们根据这个误差去调整模型参数，让这个误差越来越小，最后得到的这个模型理论上就可以为我们干活了。事实上，这其实就是一个机器学习里面的回归问题。

Netflix 比赛的评判标准就是 RMSE，即均方根误差，怎么算的呢？

$$RMSE = \sqrt{\frac{\sum_{t=1}^n (\hat{y}_t - y_t)^2}{n}}$$

这个公式中的 t 表示每一个样本，n 表示总共的样本数，有帽子的  $\hat{y}_t$  就是模型预测出的分数，是我们交的作业，秃顶的  $y_t$  就是用户自己打的分数，是标准答案，然后一个样本一个样本地对答案，模型预测分数和用户自己打分相减，这就是我们预测的误差。

由于误差有正数也有负数，而我们只关心绝对值大小，所以再给误差求平方，这就是名字中的“方”的来源，再对所有样本的误差平方求平均值，这就是名字中“均”的来源，因为我们对误差都平方了，所以最后再对均值开方根，这就是名字中的“根”的来源。这个过程就是求均方根误差。

评分预测问题常见于各种点评类产品（如：书影音的点评），但评分类推荐存在以下问题：

1. 数据不易收集，我刚才说过，用户给出评分意味着他已经完成了前面所有的漏斗环节；
2. 数据质量不能保证，伪造评分数据门槛低，同时真实的评分数据又处在转化漏斗最后一环，门槛高；
3. 评分的分布不稳定，整体评分在不同时期会差别很大，个人评分在不同时期标准不同，人和人之间的标准差别很大。

用户爸爸们给产品施舍的评分数据，我们又叫做显式反馈，意思是他们非常清晰明白地告诉了我们，他们对这个物品的态度；与之相对的还有隐式反馈，通常就是各类用户行为，也就是另一类推荐系统问题：行为预测。

## 行为预测

实际上，用户爸爸们每天要在不同的 App 或者网站之间不停批阅奏章，日理万机，非常忙，所以能够提交的像评分这种显式反馈数据很少。

但是没关系，只要用户来了，就会有各种行为数据产生，从登录刷新，到购买收藏，都是用户行为，这类数据是用户们在自觉自愿的情况下产生的，数据量比显式反馈多很多。

用户的行为通常呈现漏斗关系，我希望用户最终达成的行为可能不是那么容易得到的，比如购买，比如建立一个社交关系，比如完整消费一个长内容，通常是从登录刷新开始，逐层经历漏斗流失。

而推荐系统肩负的使命自然是达成用户行为，也就是连接越多越好。这也是这一类推荐系统问题的关注点。

推荐系统预测行为方式有很多，常见的有两种：直接预测行为本身发生的概率，和预测物品的相对排序。直接预测用户行为这一类技术，有一个更烂大街的名字，叫做 CTR 预估。这里的 C 原本是点击行为 Click，但这个解决问题的模式可以引申到任何其他用户行为，如收藏、购买。

CTR 意思就是 Click Through Rate，即“点击率”。把每一个推荐给用户的物品按照“会否点击”二分类，构建分类模型，预估其中一种分类的概率，就是 CTR 预估。

行为预测说白了，就是利用隐式反馈数据预测隐式反馈的发生概率；也因此，各家互联网产品要高度重视隐式反馈，归纳起来有以下几点原因。

1. 数据比显式反馈更加稠密。诚然，评分数据总体来说是很稀疏的，之前 Netflix 的百万美元挑战赛给出的数据稀疏度大概是 1.2%，毕竟评分数据是要消耗更多注意力的数据。
2. 隐式反馈更代表用户的真实想法，比如你不是很赞成川普的观点，但还是想经常看到他的内容（以便吐槽他），这是显式反馈无法捕捉的。而人们在 Quora 上投出一些赞成票也许只是为了鼓励一下作者，或者表达一些作者的同情，甚至只是因为政治正确而投，实际上对内容很难说真正感兴趣。

3. 隐式反馈常常和模型的目标函数关联更密切，也因此通常更容易在 AB 测试中和测试指标挂钩。这个好理解，比如 CTR 预估当然关注的是点击这个隐式反馈。

用户给出较高评分的先决条件是用户要有“评分”的行为，所以行为预测解决的是推荐系统的 80% 问题，评分预测解决的是最后那 20% 的问题，行为预测就像是我们剁手买买买后，可爱的商品要先乘坐飞机，飞跃千山万水到所在区域来，而评分预测则是快递员最终将东西递交到你手上这个过程。

## 几个常见顽疾

讨论了两大类推荐系统的问题后，我们再来看几个推荐系统的隐藏顽疾。之所以说这些是隐藏顽疾，是因为它们还没有很好的通用解决方案，并且不容易被重视，这几个顽疾分别是：

1. 冷启动问题；
2. 探索与利用问题；
3. 安全问题。

### 1 冷启动问题

推荐系统是数据贪婪型应用，所谓数据贪婪型应用，就是对数据的需求绝无足够的那一天。冷启动问题广泛存在于互联网产品中，但我们这里仅仅限于推荐系统的冷启动。

新用户或者不活跃用户，以及新物品或展示次数较少的物品，这些用户和物品，由于缺乏相关数据，很是空虚寂寞冷，因此就是冷启动问题的关注对象。

关于“如何解决冷启动”本身，有伪命题的嫌疑，因为通常的解决方式就是给它加热：想办法引入数据，想办法从已有数据中主动学习（一种半监督学习）。我们会在后面的文章中详细讨论冷启动的问题。

### 2 探索与利用问题

探索与利用，行话又叫做 EE 问题。假如我们已经知道了用户的喜好，一般有三种对待方式：

1. 全部给他推荐他目前肯定感兴趣的物品；
2. 无视他的兴趣，按照其他逻辑给他推荐，如编辑推荐、随机推荐、按时间先后推荐等等；
3. 大部分给他推荐感兴趣的，小部分去试探新的兴趣，如同一边收割长好的韭菜，一边播种新的韭菜。

哪一种更科学和持久呢？显然是第三种，那么如何平衡这里的“大部分”和“小部分”呢？

这就是 Exploit 和 Explore 问题的核心了。Exploit 意为“开采”，对用户身上已经探明的兴趣加以利用，Explore 意为“探索”，探明用户身上还不知道的兴趣。

我们会在后面的文章中详细讨论 EE 问题。

### 3 安全问题

凡是系统就有漏洞，凡是漏洞有利可图，就一定有人去图，推荐系统也不例外。如果你正在一款流量非常大的产品上构建推荐系统，那么一定要考虑推荐系统攻击问题。推荐系统被攻击的影响大致有以下几个：

1. 给出不靠谱的推荐结果，影响用户体验并最终影响品牌形象；
2. 收集了不靠谱的脏数据，这个影响会一直持续留存在产品中，很难完全消除；
3. 损失了产品的商业利益，这个是直接的经济损失。

所以推荐系统的安全问题：有哪些攻击手段，以及对应的防御办法，这些我们也会在后面的文章中予以讨论。

### 总结

今天，我从两个角度总结了推荐系统中的常见问题。

第一个角度是模型的角度，将推荐系统的模型分成了预测评分和预测行为，这样一来，自己有什么数据就选择什么样的模型。另一个角度是看看推荐系统中一些永恒存在但是潜在的问题，包括冷启动、EE 问题、安全问题。

好了，说到这里，你可以去观察一下你用过的推荐系统，看看它们的模型是预测评分还是预测行为，你可以在下面留言，我们一起讨论。感谢你的收听，我们下次再见。

想迅速了解并掌握推荐系统的同学，可以购买《推荐系统三十六式》专栏，作者在推荐系统方面有 8 年的经验，为推荐系统学习者架构起整体的知识脉络，并在此基础上补充实践案例与经验，力图解决系统起步阶段 80% 的问题。



版权归极客邦科技所有，未经许可不得转载

## 精选留言



上个纪元的赵天师  
不做笔记都对不起文稿，赞

凸 28

2018-03-09

## 作者回复

不回答都对不起这留言，棒

2018-03-10



愚公移山

凸 8

老师，还是有些不理解隐式反馈常常和模型的目标函数关联更密切，显示反馈，如评分，通常也与模型的目标函数关联十分密切。

2018-03-10

## 作者回复

隐式反馈往往是用户的行为，是用户正常的消费路径，最终通向商业目标，比如掏钱。但评分是个旁支，往往不必通向最终商业目标。

2018-03-14



叶晓锋

凸 4

老师你好，非常感谢您对评分预测和行为预测的划分，而且因为用户爸爸很忙，对很多场景来说不可能采集到足够的评分反馈，我们应该更多的关注行为预测，隐式反馈，解决80%的问题。老师讲到行为预测分为概率预测和相对排序预测，我特别关注相对排序预测，老师能否解答下概率预测和相对排序预测的区别？

2018-03-07

## 作者回复

不要急，后面会专门讲到。

2018-03-08



禾子先生

凸 3

刑老师，之前用mahout，采用皮尔逊算法，进行基于用户和物品的推荐，推荐效果不好，碰到一个非常严重的问题，希望老师能够指点下。我们是电商系统，给用户的行为进行评分并采集，如给点击商品行为评1分，添加购物车评2分，购买评3分，用户数据在20w左右，评分数据在150w左右，结果每次推荐巨慢，经常要1分钟才有推荐结果，而且还经常导致内存溢出，希望老师能指点下。

2018-03-07

## 作者回复

内存溢出这个我恐怕不能直接知道原因。另外，你们人为给行为赋予权重这个做法不太合适，不如直接预测行为。

2018-03-08



13113604627

凸 2

我是推荐系统小白，目前做的是主要是一些工程性的开发，想转型学习推荐系统，看了前三章，感觉还是一些概念性的东西，请问学完这个后，自己能搭起一个简单的推荐系统吗？

2018-05-16



杨阳

凸 2

刚入门，正好看到。确认过眼神，遇上对的人。

2018-05-08



晴れよ

凸 2

评分预测是显示反馈，因为用户已经购买过商品表明了他们的态度，给其他商品打分是为了找出符合用户态度的商品然后做推荐；行为预测之所以说是隐式反馈，是因为我们仅有用户的行为数据，但是用户还没实际的买账操作，相比用户已经购买的显式态度，这是用户的隐性态度。

2018-05-03



吴文敏

凸 2

对于存在多种隐反馈行为的推荐系统，比如电商这一场景（同时有点击、浏览、收藏、加入购物车），该如何设计推荐策略。我们过去的做法是将这些行为作为不同维度的量化特征对来预测将来某一种行为会不会发生。老师有没有好的建议？

2018-03-26

### 作者回复

可以这样做，但是可能有过拟合的危险，因为多种行为可能不见得是时序先后发生的。还有一种做法是分别对每种行为建模预测，在不同场景使用不同侧重的模型。

2018-03-26



极简2018

凸 2

是不是还有个滞后性问题，怎么解决

2018-03-13

### 作者回复

推荐系统滞后是局限性，因为总是要在历史数据中有记录了才能反应出来。艾莎门就是这样的局限性导致的。

2018-03-14



山羊wayne

凸 2

均方根讲的确实形象，赞一个

2018-03-12

### 作者回复

收下了。

2018-03-14



yxj▶

凸 2

请问刑老师，如果我们用神经网络的机器学习方法来搭建推荐系统模型，我们如果把评分预测作为神经网络最末层输出，那么是否可能会在其中的隐藏层预测出用户的行为预测呢？

2018-03-07

### 作者回复

隐藏层不好解释，恐怕和行为预测还不能直接挂钩。

2018-03-08



NaNa

冚 2

评论留言是评分预测还是行为预测

2018-03-07

### 作者回复

留言是个行为。

2018-03-08



rushui

冚 2

电商广告推荐里面一般都是做pCTR和pCVR

2018-03-07

### 作者回复

主要差不多这样，也有别的。

2018-03-08



八戒

冚 1

点击行为数据获取，我们会拿到很多负样本，这样在训练模型的时候效果不好，老师有什么方案解决么，谢谢啦

2018-04-13



Edward

冚 1

数据稀疏度1.2%是什么意思

2018-03-16

### 作者回复

矩阵中只有1.2%的位置有数据。

2018-03-16



大西vince

冚 1

老师，我是一个信息流广告优化师，我们在工作中常常是靠猜用户的兴趣，人工点击率和转化率预估，所以能不能请您详细说说点击率和转化率预估算法的逻辑。

2018-03-13

### 作者回复

能。

2018-03-14



我要飞上月球

冚 0

老师好，有个问题问下，“两种：直接预测行为本身发生的概率，和预测物品的相对排序。”这两者的区别怎么理解

2018-06-07



宁静致远

冂 0

老师，想问个问题：推荐系统会采用各种不同的算法，但我在想不通算法之间预测出来的结果差异会不会很大，那这得如何去选择比较优的算法去预测结果啊

2018-05-24



懒鼠

冂 0

在对隐式反馈数据处理的时候，我们会根据行为的时间成本和交互成本去给各个行为定一个分值，然后再进行一些预测。这样就将行为预测转变为打分预测。

2018-05-08



Amoun

冂 0

评分预测相比行为预测来说，可以理解成评分预测是为了更好的行为预测吗？对用户的未消费的产品进行预测评分，到最后不还是融合各个评分、将评分进行排序，然后对用户的行为进行预测吗？

2018-05-07