电子商务搜索算法技术白皮书

(第一版)

淘宝搜索基础算法团队出品　编著

搜索事业部

搜索基础算法团队工作室 · 杭州

内 容 简 介

各类主要的互联网服务，包括搜索、广告、推荐、等等，它们的一个典型共同特征，就是利用不断增强的计算处理能力和日益丰富的资源种类，对百万乃至上百亿量级以上的超大规模数据进行分析和挖掘，数据维度包罗万象，比如网页内容、用户行为、时间序列、等等，去充分理解消费者需求，定位供给端的品类和质量，建立一个良性的买家和卖家的公平交易平台；

淘宝搜索作为平台的一个重要联系买家和卖家的产品形态，由于其以下的特有属性，使其成为大数据智能化应用的最佳场景；

海量消费者与平台的互动行为

买家和卖家的公平交易平台

海量商家在平台进行的商业活动行为

本书将围绕淘宝搜索智能化体系的演进历程进行系统化阐述，如何依托于工程架构体系的逐步完善，逐步实现从简单人工运营加简单算法规则的时代，发展成为阿里电商平台辅助消费者与商品（卖家）的互动更加趣味化和效率化的智能中枢，不仅仅可以从海量用户行为数据中寻找行为规律，结构化行为序列，并从规律中预测结果，更重要的是给出有效的流量中心化和去中心化的投放决策，从而实现消费者，卖家，平台三者社会福利的最大化。淘宝的搜所和推荐发展到今天，正在从智能的依靠机器学习能力解决业务问题，向更高效的从不确定性中探索目标的学习 + 决策的能力进化。

目　　录

第一章　序言

学习目标与要求

1.1　算法演进之路

从 pc 互联网到移动互联网，阿里巴巴电商平台一路高歌猛进，数据规模，计算能力都发生了天翻地覆的变化；如图 1 所示，

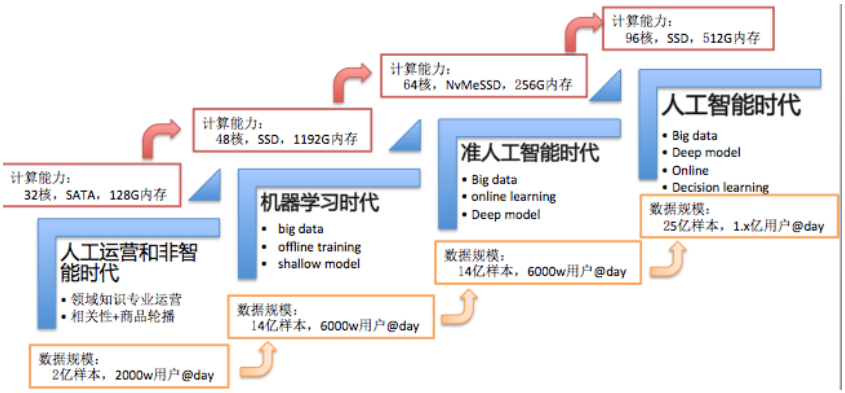


图 1.1: 搜索智能化体系演进图

1.1.1 人工 + 弱算法时代

这个时代的关键词：**规则 + 轮播**

算法及模型在搜索和推荐系统领域占据统治地位之前，具有领域知识的专业运营和产品往往充当信息展示规则的制定者，根据主观的判断和对市场的敏锐度来制定查询词背后的商品展示逻辑。“人工规则”的好处是容易理解和操控，坏处则不言而喻，随着平台规模的增大，简单规则无法精细的表达人货匹配的效率，并且容易被一些不良商家利用规则来扰乱市场秩序；实际上，早期的搜索和推荐系统也会运用一些基本的算法逻辑来保证信息匹配的正确性和人货匹配的公平性，基于传统搜索引擎技术的相关性模型，保证用户查询词语商品标题的有效匹配；基于商品成交与否的销售人气指数模型，保证有助于被消费者接受的商品得到更多的展示机会；另外还有一个就是系统为了保证让更多商家有机会得到展现，设置的按照虚拟下架周期为参考的轮播因子，即将下架的商品会得到相对较高的展示机会。

$$score(item) = 1 - \frac{ItemOffshelfTime - QueryTime}{secondsOfTwoweek} \times (\frac{docFound}{delta})$$

这个时代遗留下来几个关键问题需要解决：

1.1.2 大规模机器学习时代

这个时代的关键词：**big data，offline + shallow model**

随着平台规模的扩大，大规模商家入驻，积极的在平台上打理店铺，发布商品，相对结构化的商品组织体系，类目结构，属性信息，基于商品为 key 的销量的累积，评论的累积，这些为更好的理解商品积累了重要的原始数据资料；消费者通过搜索产品的各级页面与平台的互动越来越频繁；数据的组织形成了以人为 key 的结构体系，反馈信号也得以在闭环系统中有效的流转；所有的这些都为理解用户积累了重要的数据资料。有效数据的积累为大规模运用机器学习技术解决问题提供了必要的土壤。

这方面各大互联网公司和科研机构，学校公开发表出来的有参考价值的工作有不少，典型的有价值工作，logistic regression，gbdt；

1.1.3 准人工智能时代

这个时代关键词：**big data，online，deep model**

1.1.4 人工智能时代

这个时代的关键词：**big data，online，deep model，decision learning**

淘宝搜索算法技术演进之路可以分为四个阶段，如图所示：

1.2 评估体系

1.3 技术体系进展

recency-sensitive ranking location-sensitive ranking

参考文献

[1] Bilinear+LinUcb 的个性化主题推荐, http://www.atatech.org/articles/67847

[2] 依托搜索技术的个性化平台之路, http://www.atatech.org/articles/13748

[3] 用户意图预估之实时意图篇, http://www.atatech.org/article/detail/12636/152

[4] 知人知面需知心——论人工智能技术在推荐系统中的应用, http://geek.csdn.net/news/detail/112318

[5] Google, Ad Click PredictionL a View from the trenches. pCTR 使用 LR，通过 FTRL Proximal 算法实现在线模型更新，频率学派，写的很细致，也有工程细节

[6] Bing, Web-Scale Bayesian Click-through Rate Prediction for sponsored Search Advertising in Microsoft's Bing Search Engine。Online Bayesian Probit Regression，贝叶斯学派，涉及采样算法的模型

[7] Facebook, Practical Lessones from Predicting Clicks on Ads Clicks on Ads at facebook。DT+LR。和 GBDT 非常类似，不同之处在于用 LR 重新训练了每棵树投票的权重，人气很旺的 xgboost，在这一块也是做了优化，利用二阶导数信息得到更快收敛的步长。缺点是处理不了高纬度特征，处理连续值特征有优势。

[8] 我所经历的大数据平台发展史（三）：互联网时代 • 上篇, http://www.infoq.com/cn/articles/the-development-history-of-big-data-platform-paet02,

[9] Fast and Reliable Online Learning to Rank for Information Retrieval, https://khofm.files.wordpress.com/2013/04/thesis-katja-hofmann-online-learning.pdf

[10] Dawei Yin, etc.., Ranking Relevance in Yahoo Search, KDD'16

[11] C.J.C. Burges, FromRankNettoLambdaRanktoLambdaMART: An overview, Technical report, Microsoft Research 2010

[12] Z. Cao, T. Qin, etc.., Learningtorank: from pairwise approach to listwise approach, ICML'07

[13] A. Dong, Y. Chang, etc.., Towards recency ranking in web search. In WSDM'10.

第二章　业务问题所带来的技术挑战 @ 淘宝

学习目标与要求

2.1　业务问题的思考 @ 淘宝搜索

淘宝的搜索平台是致力于提供一个一个买家和卖家的公平交易平台；作为一个公平的市场调节员，调整供需平衡，为卖家引导潜在的兴趣用户，以提升其ROI（return on investment），为用户提供满足其需求（user intent）的商品；商业流量下的搜索自然带有其特有的技术特点：

2.1.1　动态性

网页搜索的对象的是分布于各类网站发布的网页，从索引单元上对比，数量上是绝对要远远大于商品搜索的对象集合，如果把每个商品展示页当成是淘宝网站的普通网页的化，表象上讲，商品页面的信息集合应该是网页搜索对象集合的一个子集；网页搜索中的基本对象也存在网页更新，然而淘宝搜索的商品库具有更强的动态性，宝贝的循环搁置，新卖家加入，卖家新商品的推出，价

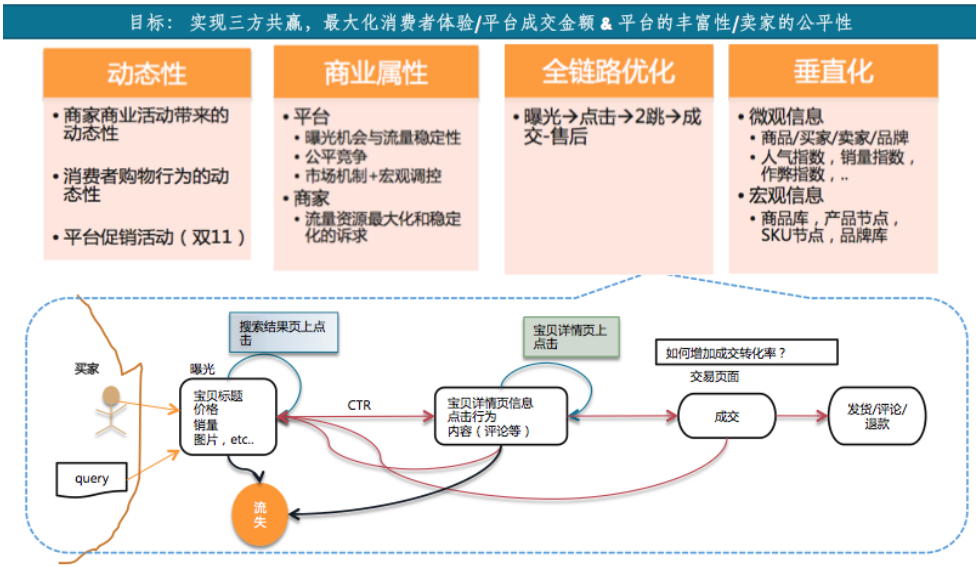


图 2.1: 电商搜索特性

格的调整，标题的更新，旧商品的下架，换季商品的促销，上下架，降价，宝贝图片的更新，销量的变化，卖家等级的提升，商品竞争程度的提升等，都需要淘宝的商品搜索引擎在第一时间捕捉到变化，并及时反映到索引结构中的相应信息单元，而最终的排序环节，这些变化也会动态的融入排序因子，带来排序的动态调整；因此对于商品搜索引擎，要求建立高效的索引更新体系，适应商品类目体系，倒排索引结构，匹配机制的召回逻辑，以及应对商品排序信息及时生效的 cache 分层机制；

2.1.2 全链路优化

众所周知，相比类似百度这样的网页搜索平台，一个明显的差异是，淘宝搜索平台拥有网购消费者从查询到完成目标商品订单，这样一条完整的行为数据闭合式链路；因此对于用户的一次查询的满意度衡量绝不能止于搜索结果页上看到一个标题相关的商品而发生了点击来判别，post-click 之后的商品详情页上的行为，甚至于进入 post-pay 之后的评论信息都应该成为度量某商品对于某次

查询（query）的满意度影响因子；因此，全链路的行为建模会是淘宝搜索体系相比于网页搜索的重要差异之处；既然谈到这点了，再多⊠嗦两句，京东也是一家做电子商务的公司，也有着不小的规模，那么如何来看淘宝搜索与京东搜索在全链路优化上的差异呢？从京东模式来看，post-pay 环节，由于销售，物流仓储的自营性，可以认为是无差异竞争的；而对于淘宝来说，售后的服务，发货速度，以及纠纷退款等环节是取决于商家与消费者之间的互动来决定的，差异性不言而喻，因此淘宝搜索有必要建立 post-pay 环节的排序度量因子；

2.1.3 商业属性

电子商务平台的搜索自然具备商业流量的根本属性，商家希望所经营商品通过得到足够的曝光而带来成交；因此，流量资源（曝光）也就成了商家必争之地。搜索排序体系的白盒化和可解释性自然是至关重要。淘宝搜索的 ranking，更接近于一个带约束的优化问题，而不是一个简单的排序，优化的目标是最大化平台的成交金额；而约束则是卖家流量分配的诉求；这个环节的涉及到的课题也是电商平台最复杂之处，我会在下面集中阐述下我的一些观点；

2.1.4 垂直化

电子商务搜索属于 vertical search 范畴，相比于网页搜索，对于平台上内容的结构化梳理，以及商业平台上积累的买家，卖家和商品关系数据的挖掘都有更高的要求；因此需要建立 micro analysis 和 macro analysis 双位一体的搜索内容加工体系，宏观分析层面指的是：除了目前已经积累并广泛运用的 5 级类目之外，完善的商品库建设，spu 节点，sku 节点，品牌库等，都是必不可少的；微观分析层面则从商品的人气指数，销量指数，作弊指数等角度给出商品自身质量的度量信息；使得搜索结果能够为消费者提供，不仅仅停留在标题相关层面的服务，可以通过合理的宏观分析带来的数据结构化，实现高效的结果查询，通过细致的微观分析，保证优质的商品优先展示给消费者；

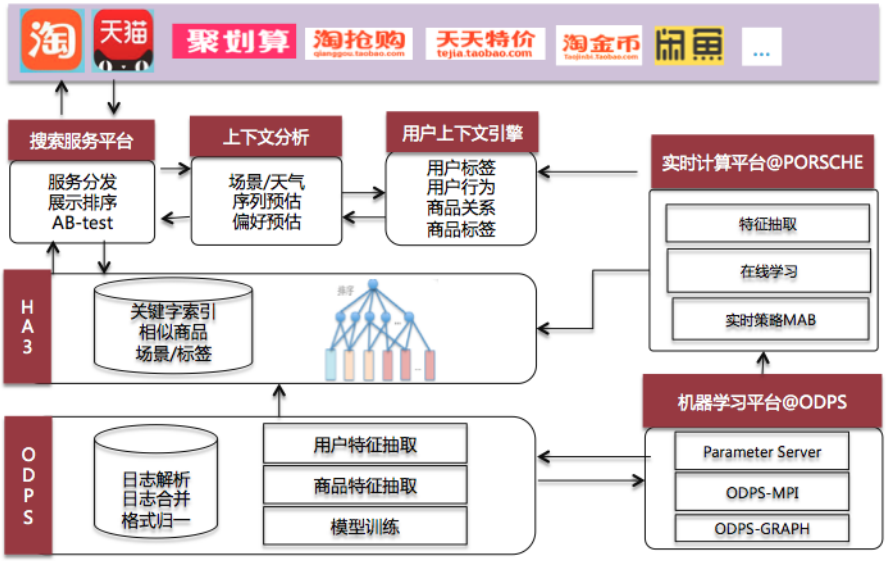


图 2.2: 智能化助力商业产品

2.2 技术挑战 @ 业务问题

2.2.1 算法模型

像众多互联网企业一样，大数据环境下，基于用户行为建模所面临的技术挑战很多，大家耳熟能详的点列举如下：

投放逻辑带来的数据 bias 对行为建模的影响

用户行为数据的稀疏性

因果关系的模糊性

用户行为的时效

行为个性化和非个性化 unified ranking

Cold start modeling

多样性与精确性的 tradeoff（过度个性化）

长短期个性化融合

2.2.2 工程技术

随着数据规模的指数级增长，完成复杂数据建模对于工程技术体系的挑战也是不言而喻：

千亿行为和关系数据存储、实时更新和查询

翻页陷阱

Cache 机制

分级实时体系 (数天/小时/秒/ms)

2.2.3 效果评估

效果评估是保证体系迭代朝正向发展的关键保障。

模型正确性评估

Ab 体系下分群评估

社会化评测

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

第三章　搜索工程和算法架构体系

学习目标与要求

3.1　工程架构

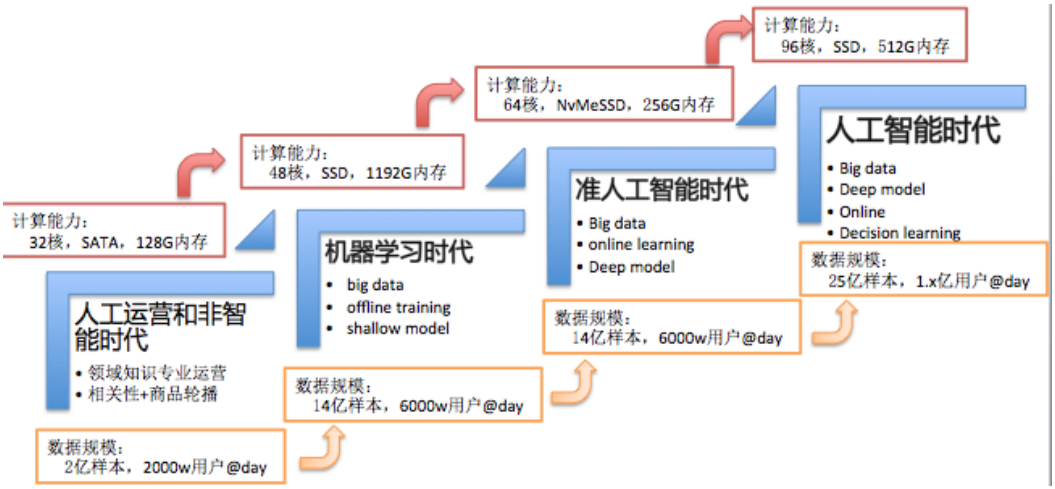


图 3.1: 工程架构图

3.2 算法架构

大规模机器学习体系如下图所示：

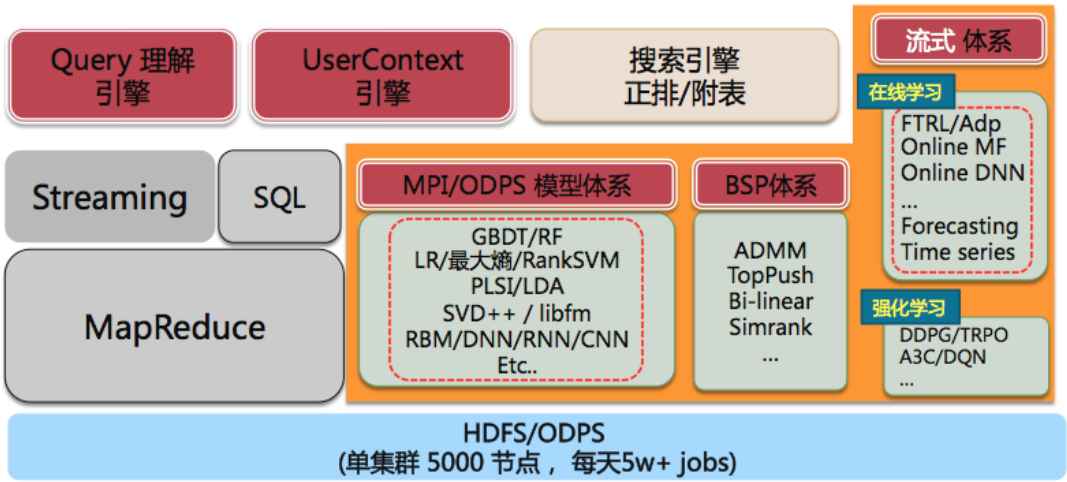


图 3.2: 大规模机器学习 @ 淘宝搜索

3.3 评估指标及 ab 系统

我们平台上所关心的指标有：

uv 转化率: $cvr = \frac{buyuv}{uv}$

uv 点击率: $ctr = \frac{ipvuv}{uv}$

客单价:

GMV:

3.4 工作流和数据流

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

第四章　搜索词背后的技术

学习目标与要求

淘宝的平台上有数十亿的商品，消费者在平台上想要快速找到自己想买的商品，只能在淘宝搜索输入查询词，也就是我们通常说的 query，来表达购物的需求。如果能够理解用户 Query 背后的购物意图，就能够帮助搜索引擎自动将符合用户意图的商品返回给用户，提升结果的准确率，从而提高用户在平台上的购物满意度和体验。

4.1　底纹推荐技术

底纹推荐技术, 实际上是实现一个从用户到 query 的映射模型：$user \rightarrow query$

4.2　查询词改写扩展技术

查询词改写扩展技术, 转换为技术语言，是一个完成从原始 query 到新 query 的映射模型：$query \rightarrow query^{*}$

4.3　查询词意图预测技术

查询词意图预测技术, 意图可以类目：$query \rightarrow category$

4.4　查询词图像化映射技术

4.5　深层语义匹配技术

4.6　AI4B 实战 @ 查询词图像化映射技术

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

第五章　商品理解算法技术

学习目标与要求

5.1　商品销量预测与人气分模型

5.2　详情页满意度模型

@ 仁重

5.3　用户浏览模型 & 用户点击满意度模型

5.4　网络效应分

5.5　商品簇模型

5.6　AI4B 实战

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

[2] 流量个性化 v.s 商业化 - 双 11 珠峰项目中控算法, http://www.atatech.org/articles/67132

[3] 确定性保证下流量分配在线全局优化策略, http://www.atatech.org/articles/55983

[4] 搜索流量确定性项目总结, http://www.atatech.org/articles/59651

[5] 网络效应分介绍, https://www.atatech.org/articles/52962

[6] Unbiased Learning-to-Rank with Biased Feedback, http://weibo.com/ttarticle/p/show?id=2309404077533346815648

第六章　用户理解算法技术

学习目标与要求

6.1　用户画像模型

物以类聚，人以群分。不同的人群，在总体上有着不同的行为特点和购物需求。我们对用户的了解，是从他/她所属的人群开始的。人群可以按不同的维度划分，如性别、年龄、购买力、地域等。例如，在服饰行业中，男性用户更喜欢买男装，女性用户更喜欢买女装。这样，在用户搜索“T 恤”时，我们可以根据他的性别展示更符合他偏好的结果。不同年龄段的用户的购物需求也会有明显的差异，例如穿衣风格或者手机款式。为了识别用户所属的人群，需要使用尽量多的数据。最基础的是用户注册的信息，不过这种信息有时并不准确。比如，用户注册时填的不准确，或者用户把账号长期给家人使用。所以还需要使用用户在网站上的行为数据来校正这些数据。这时会使用机器学习的方法，把用户肖像建模看成一个分类问题，使用各种来源的数据来预测用户所属的人群。

6.1.1 性别

性别作为用户最重要的基本属性之一，必然是个性化考虑因素。对电子商务网站来讲，性别也是搜索和推荐系统决策因素之一。淘宝主要消费群体是女性，用户数据容易被女性行为主导，人气排序下表现尤为明显。性别个性化则是根据用户的性别影响排序，在用户 query 没有明确表明性别的情况下提前与用户性别相同的商品，旨在减少翻页次数 or 换 query 次数从而提高 ctr。另外，如果用户能看到更多与其购买意图相关的商品，可能会提高成交转化率。

背景 为了利用性别影响排序，首先需要解决如何标记商品性别。商品的性别可通过类目或者属性来表现，而类目的性别表现又分为窄义性别和广义性别。窄义性别表现类目有服饰、鞋和包等，此类型只要提前相应类目或者类目下具有某些特征的商品即可；广义性别表现类目包括窄义类目和诸如手机、电脑、游戏币等隐含类别，该类型下商品的性别与类目无关，而是由商品本身的特征决定的，如颜色、风格等（与性别无明显关系），这类性别标签需要挖掘才能发现。性别个性化另外一个重要的方面是如何预测用户性别。用户注册时的性别信息和支付宝实名认证都可以作为判断性别的依据，但考虑到用户可能填错以及实名认证用户少、甚至有账号被同时多个用户使用的情况，我们不能直接应用这些信息。个性化用到的性别必须有物理性别与淘宝性别之分，所以必须建立一套合理的性别预测方案。

建模 训练: 根据一级类目成交的性别占比得到男性、女性、无性别购买类目组（一级类目的子集）。对有购买记录的用户：根据用户在性别相关类目下的 ipv 及 ipv 天数、支付宝笔数及金额、虚拟物品笔数占比及不同时间段 ipv 占比计算各维度权重，得到回归模型。对无购买记录的用户：女性类目总体 ipv 和 ipv 天数、男性类目总体 ipv 及用户注册时长作为预测维度计算权重得到回归模型。预测: 根据用户是否有成交启用不同模型，回归值大于等于 0 时为女性，否则为男性。

特征

- 分别 15 个女性、男性倾向类目的点击总数
- 分别 15 个女性、男性倾向类目的购买总数
- 强女性类目点击天数
- 强男性类目点击天数
- 总点击天数
- 强女性类目购买天数
- 强男性类目购买天数
- 总购买天数
- 女性倾向类目点击次数占比
- 男性倾向类目点击次数占比
- 点击占比熵
- 女性倾向类目购买次数占比
- 男性倾向类目购买次数占比
- 购买占比熵
- 强女性、男性类目类目点击天数差占有点击天数的比例
- 强女性、男性类目类目购买天数差占有购买天数的比例

效果 最终效果，总体召回率：86%，总体准确率：94%。

6.1.2 年龄

用户年龄的识别可以简单的使用身份证上的生日计算年龄。

表 6.1: 准确率

新版	样本数	预测男	预测女	召回率	准确率
真实男	1380636	1192135	73080	86.3%	93.4%
真实女	1353568	84840	1156177	85.4%	94.1%

6.1.3 购买力

随着中国经济和电子商务的快速发展，用户也在快速成长，对于高品质、高端商品的需求不断上升，而目前我们的搜索对于这部分用户需求的满足不是很好，高端用户在不断流失。本项目的旨在通过算法和运营配合挖掘出淘宝上的高端用户，同时展现给这些用户合适的商品，以提高这部分用户的体验和留存率。

商品的价格档 为了便于在业务中分析各种数据，可以将用户的购买力分成几个档次（如 1 7 档），档次越高表示用户的购买力越大。用户的购物行为中可以很方便的体现购买力。这时需要先确定商品的价格档。由于每个类目商品的价格差异很大，所以需要按类目来划分。例如：最近一个月主搜引导成交的笔单价从小到大排序，按指定分位点划分成七档，如：0,0.2,0.4,0.6,0.8,0.9,0.95,1。

用户购买力模型 我们使用了 GBDT 模型，训练用户的购买力。以未来搜索引导的成交在类目下的价格分档为目标，建立了一个多分类的模型。

特征

- 服饰类成交额、笔单价（衣）
- 食品类成交额、笔单价（食）
- 日用品开销（家居百货）
- 是否有房 + 住房档次（住）

- 装修档次（住）
- 是否有车 + 车档次（行）
- 酒店门票类开销（行）
- 购买品牌、奢侈品
- 职业
- 教育程度
- 年龄段
- 手机型号
- 资产等级
- 好友关系

6.1.4 家庭账号

但由于家庭账号，或者代买的情况。

6.1.5 用户-商品 CTR 预估

背景 “个性化”在淘宝搜索中起着至关重要的作用，即让不同的用户看到最符合自己需求的商品。为了实现这个目标，最直接的方式就是预估商品到不同人群的 ctr。当用户搜索时，使用这个分数排序，就可以把符合用户所属人群的商品优先展示。

建模

6.2 Cohort 模型

6.3 AI4B 实战

参考文献

[1]

第七章　个性化搜索背后的核心技术

学习目标与要求

进入正题之前首先谈一谈个性化方向后续需要关注的几个点，搜索个性化时至今日，已经成为互联网网站的技术标配，虽然业界取得了一些成绩，但挑战仍然存在；

首先来看看为什么要作个性化，搜索中引入个性化的目的是什么每天有近30000 个查询“连衣裙”的消费者，query + “user context”的查询逻辑能够实现不同的消费群体看到不同商品投放结果，实现平台上人-货匹配在搜索流量上的个性化细分，比如说，“肥胖”的女性查询结果里面更多的展现宽松风格的商品，而消费能力高的消费者更多的展现高品位的大牌商品，从而达到流量投放效率的最大化；总而言之，目的是两个：a). 提升流量匹配效率：具体表现在购物路径上的效果指标；b). 改善宽泛 query 下得流量集中性，提升宽泛 query 下不同人群看到的展示商品不同，而带来成交商品和点击商品的丰富性；总而言之：对于广大消费者，由于个性化能够细分搜索意图，拟合个体偏好，有助于更快捷找到需求；

弄清楚了搜索个性化的目的，下面想来澄清几个问题：

1. 个性化并不是定制化

Customization：实现的境界是 You are what you say you are？或者说，平台按照系统理解的用户 profile，并按照某种特定个性化规则去投放，即是，实现

you are what the system thinks you are. 对于针对用户的查询结果的信息展示是局限在 explicit 的“feature”层面，比方说，按照购买力匹配规则，按照品牌偏好规则等等；定制化的好处的确能够在某种程度上带来强的个性化体验，但是带来的伤害也是不言而喻；而 Personalization 是：根据用户行为所挖掘的偏好信息来进行展示商品的投放，即是，实现 you are what you click on and what you buy；对于针对用户的查询结果的商品展示是基于“内容和数据”层面；不去刻意的假设用户的行为是由于某个特定维度（人口统计类特征，偏好类特征，人群特征）造成的，消费者点击或成交行为的发生，是所有个性化信息的综合表现；为什么我在这里先提出这个问题，因为经常听到的很多关于，目前线上个性化效果不尽人意的反馈，在这里，也不去刻意回避我们自己的问题，个性化数据，模型的覆盖率，准确性和时效性等都需要进一步的优化和改进；然而，对于那些为了增强所谓的个性化体验而实行的规则式匹配逻辑，都是极其不科学的做法，对于消费者而言，他们需要的是找到一个符合他／她需求的商品，而个性化体验强弱与否并非是最终的目的，我相信的是，消费者不会因为我们预测到他的性别，购买力，偏好的品牌就做出点击或购买的决策，个性化是我们系统实现高效的【人 - 货】匹配效率的手段，并非是消费者的购物诉求；在这里也请从事个性化方面的运营，产品，甚至算法同学能时刻理解这点；

2. 不要陷入活跃/资深用户的悖论

正常的用户无论其活跃与否，都不会愿意浪费时间去填写所谓的友好的交互式表单来帮助系统去理解他们，从而得到更好的个性化体验；他们关注的是展示商品整体是否满足他们的需求，而不会去刻意的由于商品的某个维度匹配了他/她得某个偏好而做出最终的选择；这里列举一个曾经的产品设计，在搜索结果页，给出用户可以定制的个性化偏好交互界面，希望消费者能告诉我们他们的个性化 profile，出发点是好的，结局大家懂的；

3. 个性化 explore 的重要性

随着个性化元素在搜索全链路的渗透，从 query 的个性化标注，海选的个性化召回，精排中的个性化排序因子，以及个性化 rerank，个性化展示，使得最终呈现给用户的内容取决于系统底层根据用户历史行为所挖掘的个性化特征，人口统计学维度，兴趣点偏好维度，session 级别实时特征，过度的”user specific

historical behaviour driven"的个性化投放，会使得用户逐渐丧失对展示结果的新鲜感，并且视野变得越来越狭窄，进而使得底层的用户数据模型丧失自我修复和自我扩展能力；因此一个完整的个性化体系，必须考虑 explore 机制的设计环节；

4. 个性化评估的方法论

要想推动个性化效果的正向迭代，首先需要建立起合理的效果评估体系；然而这仍然是一个很大的问题，学术界流行的准确率，召回率，F1 值，AUC，RMSE，等都有很大的局限性，这一层面的评估，只能保证数据模型的正确性；而在实际工作中，这些指标上的不一定能保证线上效果的收益；因此我们需要第二层次的评估手段，来看个性化算法效果。实现个性化的投放效果，是系统层面的主动而为，而且并没有去引导消费者端在一次搜索看到展示结果后，做出选择。因此在消费者不知情情况下，消费者的行为反馈可以用来作为个性化效果评估的一个手段。对于已经上线的个性化特征，需要部署相应的统计分析模块，在 ABtest 机制下，监控各个特征的覆盖率，以及覆盖流量下的点击率，转化率等；虽然无法直接统计到这些特征对于点击和转化带来的精确影响，但是通过追踪高权重 user 的体验 - 点击率，2 跳率，转化率等，能够了解这些特征的影响趋势，及早发现问题；这里特别强调下，采用高权重 user 的行为数据来分析的原因是，高权重用户意味着是活跃用户，意味着行为丰富，而这类用户的个性化特征的表现会更有代表性；最后，我也来谈谈对于针对个性化效果的社会化评测的意见和想法，便于理解，就以用户购买力为例来讲讲，为了更好来把握该维度数据的有效性，经常利用的手段是社会化评测来给定一些查询下，看看展示结果里面展示商品的价格是否符合评测者的价格偏好，从表象上看，似乎没有问题，然而，这里面确有一个本质上的问题，我们限定了这些参与评测人得判断角度，只关注商品价格，并给出满意与否的结论，而在实际购物场景下，用户对于商品满意与否接受与否，并不是只限定在价格本身，因此这样的评测还是有一定的局限性；我个人的观点，还是去真实的模拟线上的判断环境，不去刻意要求消费者去关注某个固定的维度，只是给出 site by site 的结果，让用户判断哪边展示的商品更符合他的口味，当然，这不同 site 的展示结果的差异，背后只是某个维度的个性化带来的影响，这样去评测，才更加客观；总结一句话，

就是众包评测的关键是，希望参与者能做出客观的反馈，不应该做任何主观性的引导；

5. 个性化体系对于系统和框架的影响

在搜索场景下实现个性化的效果，就需要去建模分析【query-user-商品】三元组构成下得海量数据分析，数据是极端稀疏的，算法时间和空间的复杂性，都对于体统能很好的支持分布和并行的数据分析和建模能力提出了很高的要求；另外，用户偏好的时效性，也需要我们能够实现增量，实时计算能力，个性化的实施，使得传统引擎依赖的性能优化利器，cache 机制无法施展手脚，因此对于引擎的创新性改造也提出了更高的要求；另外，个性化数据的挖掘都是存在不确定性的，如何来设计一套能够保证误差不会累积的算法体系，也就是说需要建立一套数据自我修复的实时反馈体系，来保证由消费者端实时获取的客观反馈数据参与到个性化投放环节来保证模型的自我修复能力快于数据误差的传播速度；这样才能保证数据产生的价值形成良性的循环，构成大数据生态体系；

个性化是一种解决“长尾需求”的方式，“长尾理论”说的是用户需求集中度越来越低，用户和用户之间不一样，我们如何来区分这种不一样？个性化搜索就是融合推荐元素，以实现：用户个体需求主导的“pull”式搜索加平台以数据驱动的方式对用户进行“push”式相关信息推送；

综述性的东西，@ 三桐，@ 公达

7.1　匹配学习

7.1.1　一阶人货匹配模型

@ 公达 u2i，u2s，u2b

7.1.2　高阶人货匹配模型

@ 公达 u2i2i，u2s2i，u2b2i

7.1.3 深度匹配模型

7.1.4 序列匹配模型

前面三个章节我们递进的描述了用户与单个商品之间的匹配方式和模型。然而，上述方法均假设用户的购物行为之间是独立的——并不存在依赖、相关或序列关系。

举例来说，一个用户 $U_1$2 天内依次购买了以下商品：烤箱、面粉、奶油；另一个用户 U_2 半年内依次购买了孕妇衣、尿布和奶瓶。我们先考虑用户 U_1，我们可以从他购买了烤箱和面粉 2 种商品推断他很可能想要做蛋糕（而这从每个单一买的商品都是很难推断的），因此也许需要奶油；再考虑用户 U_2，我们可以从她依次购买了孕妇衣和尿布推断她很可能怀孕过并且已经生了小宝宝（从某一件来推荐会比较勉强），因此马上会需要奶瓶等婴儿用品。

从上面例子我们可以看出，用户的购物行为之间往往是存在高阶依赖关系的，即仅用户购买了一个商品集合 $\{A, B, C\}$ 后，才会购买商品 D；同时，用户的购物行为也会存在序列关系，即用户购买 C，仅会在他依次购买了商品 A 和 B 之后。在这 2 种关系下，我们前 3 节使用的模型会很难捕捉这类规律。因此我们需要一种模型，能整体的考虑用户的行为历史（而不是将其行为拆分成一个一个的单独分析），进而推断他接下来的需求。

下面我们会首先介绍几种经典的序列模型以及带有记忆功能的模型，然后会详细介绍在淘宝搜索中，我们怎样使用这类模型做到用户与商品之间的序列匹配。

在机器学习的任务环境中，我们有大量的场景都是需要做一个序列预测和带有记忆的推断的。例如在 query 自动补全的场景下，我们需要根据用户输入的文字或者词序列来预测用户下一个最可能会输入的词语；又例如有这样一个问题，需要让机器在阅读了一整篇文章后，回答若干关于这个文章的问题。这类问题和场景下都需要模型具有一定的记忆能力，能在获取新信息的同时，记住部分老的信息。

A) 最常用而有效的方式是使用一个递归神经网络模型 (RNN [4, 5])。正如

其名字描述的，递归神经网络在隐层结构上存在一个循环，即当前隐层的输入是上一个隐层的输出以及当前的输入 2 项一起。由于每个隐层的信息都能递归的输入到下一个隐层中，因此会具有一定的记忆能力。如图7.1，我们将 RNN 按时间序列“打开”，可以看到前一时刻的隐层 S_{t-1} 和当前输入 X_t 会共同影响当前的隐层 S_t。

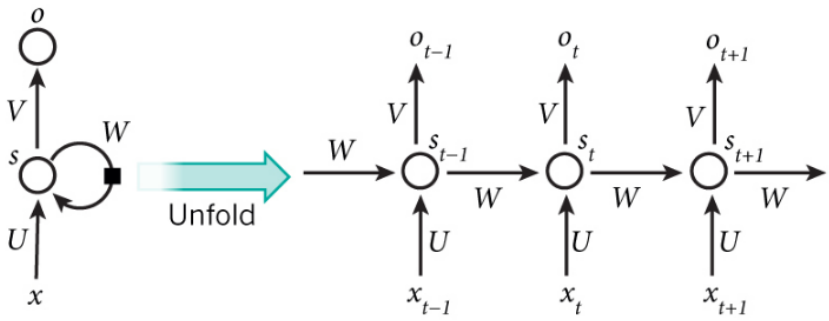


图 7.1: 递归神经网络 (RNN) 示意图

然而 RNN 存在的最大问题是“梯度消失和爆炸”问题 [6]。这是因为在神经网络进行反向传播 (backpropagation) 的时候，传播的梯度会是 $w_{l,h}(t)$(递归网络的权重) 的倍数；因此在递归层数较深的时候，梯度会消失掉 (当 $|w_{l,h} * y_l^{'}| < 1$) 或者爆炸 (当 $|w_{l,h} * y_l^{'}| > 1$)。由于 RNN 存在“梯度消失和爆炸”问题，RNN 的“记忆”只能是很短期的，并不具备长期的记忆。

B) 为了解决梯度消失和爆炸”问题,一种更为巧妙的递归网络结构 LSTM(Long Short-Term Memory)cite5 被设计了出来。在 LSTM 中，RNN 中递归的隐层单元被一个存储单元 (LSTMUnit) 所替代，每个存储单元由一个输入门 (InputGate), 一个输出门 (OutputGate) 和一个长期的内部的通过遗忘门 (ForgetGate) 更新的内部状态 (Cell) 相关联, 如图7.2。

图 7.2: LSTM(Long Short-Term Memory) 示意图

内部状态 Cell 可以可以理解为模型存储的长期记忆：每进行一次递归迭代

的时候，Cell 会通过遗忘门遗忘掉部分记忆，同时通过输入门决定当前输入有多少有效信息是需要被记住的，从而得到新的记忆。最终的输出通过当前新的记忆得到，由输出们决定新的记忆中哪些是当前需要的。在 LSTM 的反向传播过程中，不同于 RNN 中梯度是一个连乘的形式 (由于链式法则)，可以转化成一个连加的形式，因此有效的避免了梯度的消失和爆炸，从而具备一定的长期记忆的能力。在基础的 LSTM 基础上，学者们提出了多种 LSTM 的变种，比如 [10]、GRU[11] 和 Clockwork RNN[12], 他们在计算性能上会有较大的差别，然而效果基本没太大差距 [13, 14]。一个基本的 LSTM 更新公式如下：

$$i_t = \sigma(W_{hi} * h_{t-1} + W_{xi} * x_t + b_i) \tag{7.1}$$

$$f_t = \sigma(W_{hf} * h_{t-1} + W_{xf} * x_t + b_f) \tag{7.2}$$

$$o_t = \sigma(W_{ho} * h_{t-1} + W_{xo} * x_t o + b_o) \tag{7.3}$$

$$g_t = tanh(W_{hg} * h_{t-1} + W_{xg} * x_t + b_g) \tag{7.4}$$

$$c_t = (f_t . * c_{t-1}) + (i_t . * g_t) \tag{7.5}$$

$$h_t = o_t . * tanh(c_t) \tag{7.6}$$

C) 递归神经网络外主要能有效的处理“序列”相关的问题, 因此被大量的用在 NLP 的问题中。除了 RNN 外, 也有一些其他的模型有类似功能, 例如神经图灵机 (Neural Turing Machine, NTM[7]) 和记忆神经网络 (Memory Networks,MenNN[8, 9]), 他们在不同场景下会比 RNN“记住”更久远的信息,从而得到更好的效果。神经图灵机的主要思想是使用一个 $M * N$ 的矩阵取存储一份长期记忆（这与 LSTM 是类似的，只是 LSTM 维护的是一个向量），该矩阵和一个神经网络共同进行学习和预测。记忆矩阵会通过选择性的读和写来进行迭代更新, 同时由于每部分都是可微的，因此可以通过梯度下降法进行训练。NTM 的基本工作原理如下图：

图 7.3: Neural Turing Machine（NTM）示意图

记忆神经网络 [8] 主要用在长期记忆的推断，网络会从一个长文本中自动的将重要的信息编码后记录下来。最后产出的模型能回答关于长文本的任何问题

——根据问题从记忆中寻找相关内容，然后产生答案。一个经典的 MemNN 的预测过程由简单的 4 步组成：

- 将输入 x 编码成一个隐向量 $I(x)$。
- 更新记忆 m_i，$m_i = G(m_i, I(x), m)$。即通过当前的隐向量，当前记忆，整体记忆，去更新记忆中的一块内容。
- 通过当天的记忆内容和输入决定输出向量。$o = O(I(x), m)$
- 最后将输出向量解析成最终的回答。$r = R(o)$

然而 MemNN 的一个问题在于并不能 End-to-End 的去学习,同时 NTM 和 MemNN 并没有关注输入的顺序信息。

3，在个性化搜索中，最为重要的是怎么去理解和认识一个淘宝的用户。除了用户的一些基本画像信息, 我们拥有最为关键的、与其他平台不同的数据是用户在淘宝上的行为。由于用户在淘宝上的行为天然是一个长期的行为序列, 因此很自然考虑使用 RNN 等序列模型取进行处理。一个最基础的模型结构如图7.4。

图 7.4: 淘宝序列匹配模型示意图

从图中我们可以看到网络主要由 3 大部分组成，分别是：1，首先得到用户的行为序列；2，将用户的行为序列经过一个带记忆的网络编码成隐向量 H；3，将 H 通过多目标网络训练不同的目标。那么下面我们将从这三方面详细说明淘宝搜索中的序列匹配模型。

a) 首先是用户序列部分。我们使用用户有过行为的商品序列作为用户的表示, 每一个商品被 embedding 到一个 128 维的向量中, 这个向量可以从 word2vec 的方法进行无监督学习得到，也可以从一个长期 fine tune 的深度神经网络得到。在获得商品表示的算法中，一个商品 embedding 前的编码主要包括商品 ID、店铺、类目、价格信息。

商品的 embedding 部分是在训练训练网络前提前训练好的，我们并没有将其放到训练序列的网络中，主要是因为 ID 特征十分稀疏，在一个 LSTM 的网络

图 7.5: 商品 embedding

中，数据可能并不支持训练这么大规模的特征维度，从而影响模型的整体效果。然而这样的问题是，预训练得到的商品只包含了基本的商品特征，可能并不最适合当前的序列匹配网络。因此受 transfer learning 的启发，向量经过 embedding 的商品向量并不是直接作为特征输入到 LSTM 或者 MemNN 中，而是根据商品的行为类型（点击、成交、收藏、加购）和来源经过不同的卷积核生成一个新的 128 维向量，然后输入到序列网络。这样既对用户的行为进行了区分，可以学习得到不同行为的重要性；同时对预训练得到的商品向量往新的目标上调整。

b) 在得到用户的商品行为序列后，我们需要使用一个序列或者记忆模型，将序列编码成一个通用的用户状态 H。这里我们对比了 LSTM 和 End-to-end memory network[9]。LSTM 在上文中已经有过一些介绍，而一个 End-to-end memory network 与经典的 memNN 的区别在于它可以通过一个整体的网络去学习，基本的网络结构如图7.6。它首先将输入序列中的每一项同时映射成 2 个向量 m_i 和 c_i，分别表示“输入记忆”和“输出记忆”。“输入记忆”决定序列中每一项的重要性 p_i，p_i 和和 c_i 相乘求和得到输出向量 o。输出向量 o 和用户向量决定最终的答案 a。LSTM 使用一个记忆单元 $Cell$ 去记忆历史信息；而 End-to-end memory network 正着重于将原始序列压缩，并自动挖掘序列中元素的重要性。我们使用两种方法在大量数据上进行了实验对比，从 AUC 来看 LSTM 会略优于 End-to-end memory network，但是 End-to-end memory network 在计算速度上会远优于 LSTM。

$$c_i = \sigma(W_c * x_i \tag{7.7}$$

$$m_i = \sigma(W_m * x_i \tag{7.8}$$

$$p_i = Softmax(u^T m_i) \tag{7.9}$$

$$o = \sum_i p_i c_i \tag{7.10}$$

$$a = Softmax(W(o+u)) \tag{7.11}$$

c) 在得到的用户的隐向量后，进行匹配是容易的，只需要一个不用太深的

图 7.6: End-to-end memory network

DNN 网络对用户向量 H 和商品向量放到一起进行预测即可。但是为了学到更加鲁棒的网络结构，我们使用 multi-task 的相关技术 [?] 建立了多个辅助目标共同学习。因为 multi-task learning 不是本章重点，因此不再详细介绍，结果部分会有相关对比结果。

4，结果展示

7.2 排序学习

@ 元涵，@ 凌运，@ 龙楚

7.2.1

7.3 展示学习

个性化短标题：@ 苏哲，@ 仁重

7.4 模型参数优化

@ 公达

7.5 AI4B 实战

参考文献

[1] 淘宝搜索全链路有效行为量化模型 (UBM&UCM), http://www.atatech.org/articles/38550

[2] User Browsing Model 的实现与应用, http://www.atatech.org/articles/23111

[3] 搜索个性化介绍, http://www.atatech.org/articles/48548

[4] Mikolov, T., Karafi´at, M., Burget, L., Cernock‘y, J., Khudanpur, S.: Recurrent neural network based language model. J. Interspeech. 1045–1048 (2010)

[5] Hochreiter, S., Schmidhuber J.: Long short-term memory. J. Neural Computation. 9(8), 1735–1780 (1997)

[6] Learning Long-Term Dependencies with Gradient Descent is Difficult

[7] Graves, A., Wayne, G., Danihelka, I.: Neural Turing Machine. arXiv preprint:1410.5401v2 (2014)

[8] Weston, J., Chopra, S., Bordes, A.: Memory Networks. C. International Conference on Learning Representations. arXiv:1410.3916 (2015)

[9] Sukhbaatar, S., Szlam, A., Weston, J., Fergus, R.: End-To-End Memory Networks. J. Advances in Neural Information Processing Systems. 28, 2440–2448 (2015)

[10] Gers, Felix A and Schmidhuber, J: Recurrent Nets that Time and Count. J. in IJCNN 2000

[11] Cho, Kyunghyun and Van Merrienboer, Bart and Gulcehre, Caglar and Bahdanau, Dzmitry and Bougares, Fethi and Schwenk, Holger and Bengio, Yoshuai: Learning Phrase Representations using RNN Encoder–Decoder for Statistical Machine Translation. arXiv preprint arXiv:1406.1078 (2014)

[12] Koutnik, Jan and Greff, Klaus and Gomez, Faustino and Schmidhuber, Juergen: A Clockwork RNN. J. arXiv preprint arXiv:1402.3511 (2014)

[13] Zaremba, Wojciech: An Empirical Exploration of Recurrent Network Architectures. in LMLR 2015

[14] Greff, Klaus and Srivastava, Rupesh K and Koutnik, Jan and Steunebrink, Bas R and Schmidhuber, J: A search space odyssey. IEEE transactions on neural networks and learning systems (2016)

第八章　实时计算背后的核心技术

学习目标与要求

非 i.i.d 的数据分布，non-stationary 环境，很多传统的 bounding 理论是不成立的；

8.1　在线矩阵分解

@ 达卿，@ 席奈

8.2　在线 LTR

@ 凌运

8.3　在线深度学习

@ 京五

8.4　大规模 WDL 模型

8.5　LR stacking on GBDT

8.6　AI4B 实战

参考文献

[1] 搜索双链路实时计算体系 @ 双 11 实战, http://www.atatech.org/articles/44909

[2] 基于在线矩阵分解的淘宝搜索实时个性化, http://www.atatech.org/articles/38646

[3] BP 如何运行, http://www.offconvex.org/2016/12/20/backprop/

第九章　智能决策体系的建立

学习目标与要求

9.1　基于 MAB 的排序策略优化

@ 帛逸

9.2　基于 CMAB 的排序策略优化

@ 公达，凌运

9.3　基于强化学习的排序策略优化

@ 哲予，@ 达卿

9.4　级联式

9.5 AI4B 实战

参考文献

[1] 实时策略寻优，http://www.atatech.org/articles/44963

[2] 强化学习博客，http://blog.exbot.net/?s=

第十章　消费者权益智能分发核心技术

学习目标与要求

10.1　问题框架性描述

在我们的业务场景下，经常会遇到这样的问题，比方说平台希望通过流量资源吸引商家提供更多更有价值的货源；大促的时候，希望通过向消费者发放一定数额的红包或者购物券，来激发消费者的购物意愿；那么要解决好这类业务需求，我们需要解决以下几个关键问题：

平台如何来规划用来调度的资源？这一部分，我们通常需要根据有效收集需求方的大量离线数据，分析其所能满足平台要求的效率情况来估算资源总量。

平台如何来高效的完成离线计划？这一部分，我们通常需要根据需求方在平台上在线服务的实际效率和累积收益与离线计划的差异来动态合理的调整，称之为在线分配。

大体的问题框架下涉及的符号定义和关系示意图如图所示：

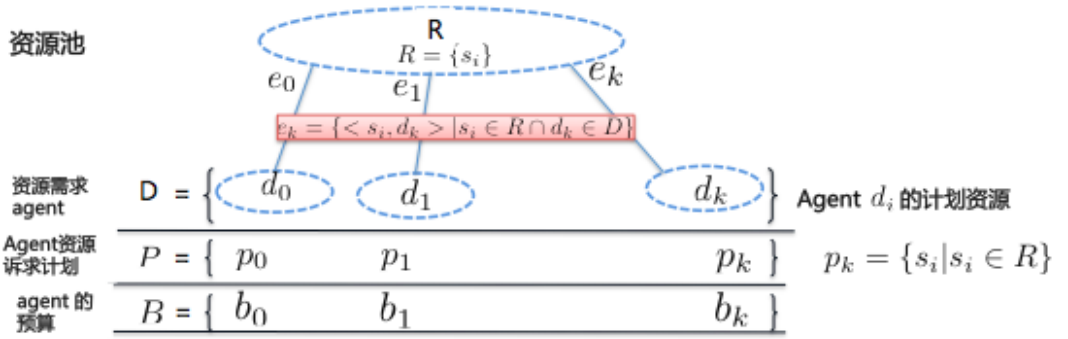


图 10.1: 资源分配图

$$max \sum_{s_i \in S, d_j \in D} X_{s_i,d_j} \times G_{s_i,d_j} \tag{10.1}$$

$$s.t. \sum_{s_i \in r_{d_j} = \{s_k | \exists < s_k, d_j >\}} X_{s_i,d_j} \times C_{s_i,d_j} \leq b_{d_j} \tag{10.2}$$

$$\sum_{s_i \in \{s_k | \exists < s_k, d_j >\}} X_{s_i,d_j} \times G_{s_i,d_j} \geq p_{d_j} \tag{10.3}$$

$$X_{s_i,d_j} \leq 1 \tag{10.4}$$

$$\sum_{d_k \in \{d_j | \exists < s_i, d_j >\}} X_{s_i,d_k} = 1 \tag{10.5}$$

10.1.1　离线计划问题建模

平台总资源池，R, 资源需求方集合，$D = d_i$, 对于资源需求方，可能涉及两个限制条件，任意一个需求方 d_i 的资源与平台签订的 minimum resource volumn, 这个是需要平台满足需求方的 bottom request，还有一个是需求方为每一个资源需要支付基本的 cost，而需求方能够支付的预算是有限的，

10.1.2　在线分配模型

10.1.3 应用实例：红包智能化发放算法

是 R；平台需求方，$D = \{d_i\}$, 能够用来向平台换取资源的预算上限表示为 $b_i \; \forall d_i \in D, B(d_i) \leq b_i$, 平台将资源 r_i 分配给需求方 d_j 的概率是 $x_{i,j}$ 且平台从此次分配中获取的收益为 $c_{i,j}$. 则整个问题可以建模为：

10.2 购物券/红包发放技术

@ 达卿，@ 云志

10.3 附录

我们先思考梯度下降（GD）这种一阶方法：这里一个问题是步长控制问题。这时牛顿法这些二阶方法出现了：将函数在局部极值点附近进行二阶 Taylor 展开近似可得：其中，为梯度向量，为 Hessian 矩阵。对上式求导并置 0，以求在二阶近似原函数的情况下快速求出函数极值点，可解得：结合两个更新公式可知，Hessian 矩阵起到了控制步长的作用。简单粗暴点的说，Hessian 矩阵的特征值控制了更新步长。详细的，我们知道对实对称矩阵而言：其中，是单位特征向量矩阵，是对应特征值对角矩阵。故：可以看出，这里控制（每个特征方向）步长的，有两个东西：原来的一阶梯度和对应的 Hessian 矩阵特征值。所以很多用 gradient descend 算法进行分析时，经常会说 Hessian 矩阵特征值这东西，极端的则表示这种，若特征值间差异巨大，则有些方向学习缓慢，有些不断波动，（二维情况就是你经常看到的那种蛇形曲线...）这些现象也侧面说明了步长这东西

10.4 结束语

What is a good example of combining machine learning with operation research to solve a major problem?

Controlling incoming and outgoing traffic in an airport is a very good Operations Research problem. This can be coupled with say, machine learning algorithm for weather prediction to make best use of the facilities available in an airport. The OR algorithm would solve the existing problem, while the ML idea would keep track of unexpected emergency landings by predicting based on suitable metrics.

Internet congestion control:

Sequencing problems are generally looked at as Operations Research areas. One of the first examples that are cited as an application of Operations Research is assembly line scheduling. If we look at internet congestion control as a similar model, we can apply an Operations Research based sequencing model coupled with ML algorithms for predicting sudden rise in traffic, virality etc.

Like I mentioned in the beginning, any problem under any domain can be modeled using Machine Learning and Operations research concepts. The efficiency of the same might be debatable.

参考文献

[1] http://www.atatech.org/articles/66486, 双 11 搜索关键词红包：商家、用户与平台的三方共赢

[2] 双 11 关键词红包：搜索链路新型互动性产品探索, http://www.atatech.org/articles/44778

[3] 淘宝外卖智能补贴算法, http://www.atatech.org/articles/72599

[4] 大数据下线性最优化问题 solver 介绍, https://www.atatech.org/articles/69242?commentId=115358comment-115358

第十一章　迁移学习

学习目标与要求

11.1　营销场景下的深度迁移学习应用

@ 一尘，@ 海凯

参考文献

[1] Gan 导读，http://weibo.com/ttarticle/p/show?id=2309404060390806926698

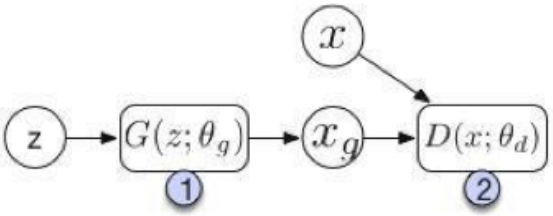
第十二章　对抗学习

学习目标与要求

12.1　GAN 的技术应用

在我们实际大数据环境中，我们需要从数据中挖掘出基本的结构化信息，从而可以帮助我们有效构造样本，解决一些传统监督学习所无法解决的问题；比方说，正样本覆盖率低，负样本缺失，模型 overfitting，鲁棒性不够等等；生成式模型的目的是找到一个函数可以最大的似然数据的真实分布；通常我们用 $f(X:\theta$ 来表示这样的一个函数，找到一个使生成的数据最像真实数据的过程就是一个 MLE 的过程。问题是：当数据的分布比较复杂时，简单的函数无法表达样本空间；现在通过深度网络结构可以表达一个更加复杂的函数，但是训练过程成为了关键。基于 sampling 的训练过程显示不是高效的；早年 graphical model 会采用变分推断方法；还有今年出现的对抗学习方法；GAN 相关技术的演变如下图所示：

最经典的 GAN 模型，由 Ian Goodfellow 提出，先从一个简单的分布中采样一个噪声信号，然后经过生成函数后映射到我们想去拟合的数据分布 x_g。生成的数据和真实数据都会输入到一个识别网络 D，识别网络通过判别输出一个标量，表示数据来自真实数据的概率。在实现上，要求 G 和 D 都是可微分函数，



$$\min_G \{\max_D V(D,G) = \mathbb{E}_{\boldsymbol{x}\sim p_{\text{data}}(\boldsymbol{x})}[\log D(\boldsymbol{x})] + \mathbb{E}_{\boldsymbol{z}\sim p_{\boldsymbol{z}}(\boldsymbol{z})}[\log(1 - D(G(\boldsymbol{z})))]\}$$

图 12.1: 标准 GAN 算法示意图

可以用多层神经网络来实现；后半部分是模型训练中的目标函数。从公式上看，类似于 CrossEntropy，注意到 D 是 P(Xdata) 的近似。对于 D 来说，要尽量使公式最大化（识别能力强), 而对于 G 又想使其最小。整个训练过程是一个迭代过程，但是在迭代中，对 D 的优化又是内循环。生成模型可以发挥价值的场所：

特征表示

强化学习中的探索

逆强化学习

迁移学习

参考文献

[1] Gan 导读，http://weibo.com/ttarticle/p/show?id=2309404060390806926698

[2] John Glover, Modeling documents with generative adversarial networks, workshop on adversarial training, NIPS 2016, Barcelona, Spain

第十三章　反作弊技术 @ 淘宝

学习目标与要求

1. 基于 GraphMining 炒信识别技术.

2. 搜索反作弊舆情系统架构.

淘宝搜索为了维护公平、公正的搜索排序环境，严厉打击商家刷销量行为。下面简单介绍以下两种基于 GraphMining 的虚假交易识别。

13.1　物流网络

13.1.1　基于物流网络识别虚假交易

当前淘宝炒信卖家为了提升自己的销量，进行虚假交易行为，随着虚假交易识别的精准性，卖家和炒信买家通过盗用正常用户的运单、地址信息，模拟真实交易，影响搜索排序，商品评价体系，最终影响正常用户购物决策。如图 13.1，蓝色点为买家、红色点为商品，存在复杂交易网络，在如下交易网络中我们加入物流信息节点，进行虚假交易识别

物流网络识别算法如下:

1. 原始交易网络边：AC、BD

图 13.1: 交易网络示意图

图 13.2: 物流网络识别示意图

2. 物流运单网络边：AX、XC、BX、XD

3. 同人网络边：AB、CD、BC 在实际网路中同人网络最多出线如上几条边情况，假如 AC 出现同人边，则为卖家自炒作

4. 信息盗用炒作识别技术方案:1). 依照同人、物流、交易网络构建物流网。2). 由于一笔运单号在正常情况下只能被一对买卖家使用，将问题转化为经典图染色问题。3). 实际算法中采用 DFS 遍历网络节点，并进行染色，产出运单号中多次染色节点，如图 13.2

13.2 行为网络模型

行为网络模型基于用户交易过程中的相关日志数据结合相关交易网络关系识别异常交易。行为网络模型分为用户-商品异常行为分类与基于交易图网络关系的传播算法两部分。

在假设正常用户与异常用户在交易过程中具有不同的行为特征的前提下，用户-商品异常行为分类模型基于用户特征、商品特征与用户-商品组合特征预测用户 u 在商品 i 的交易过程中的异常概率值 w_{ui}，即 $w_{ui} = f(\vec{x}_u, \vec{x}_i, \vec{x}_{ui})$，其中 $\vec{x}_u = (x_{u,1}, ..., x_{u,n})$ 为用户维度相关属性特征，$\vec{x}_i = (x_{i,1}, ..., x_{i,m})$ 为商品维度相关属性特征，$\vec{x}_{ui} = (x_{ui,1}, ..., x_{ui,l})$ 为用户与交易过程中被购买商品的组合特征，$f(\vec{x})$ 为可以相关业务决策模型也可以是通用的 XGBoost，GBDT，DNN 等分类模型。淘宝反作弊目前会借助于相关深度学习神经网络算法代替部分人工的特征工程，从海量的日志数据中提取抽象化的识别特征挖掘异常交易行为。

异常行为分类模型基于用户与商品维度相关特征计算非正常人群的概率，在正常用户与异常用户群体具有较大区分度时具有较高的准确率，但是模型仅仅考虑用户与商品之间的关系，没有考虑用户以及商品交易网络的全局信息，基于交易图网络关系的迭代算法为模型引入了图关系维度的相关信息，其思想为将预测模型得到的异常概率值 w_{ui} 作为用户 u 对商品 i 的作用，由传播迭代得

到用户与商品在全网的异常影响分，如下所示：

$$\begin{aligned} V_I^{(t)} &= W_{UI}^T \cdot V_U^{(t-1)} \\ V_U^{(t)} &= W_{UI} \cdot V_I^{(t)} \\ V_U^{(t)} &= \frac{V_U^{(t)}}{\|V_U^{(t)}\|}, V_I^{(t)} = \frac{V_I^{(t)}}{\|V_I^{(t)}\|} \end{aligned} \tag{13.1}$$

其中，$W_{UI,ui} = w_{ui}, u \in S_u, i \in S_i$ 为用户商品行为矩阵，S_u 为用户集合，S_i 为商品集合。图传播算法得到的用户 u 的传播分 v_u 与商品 i 传播分 v_i。传播模型相关收敛性证明如下所示：

$$\begin{aligned} A &= W_{UI}^T \cdot W_{UI} \\ V_u^{(t)} &= \frac{1}{\prod_{j=0}^{t-1} \|AV_u^{(j)}\|_1} \lambda_i^t [\alpha_1 v_1 + \sum_{i=2}^{|U|} (\frac{\lambda_i}{\lambda_1})^t \alpha_i v_i] \end{aligned} \tag{13.2}$$

用户与商品的传播分数能代表用户在交易网络中的异常严重程度，基于 v_i 与 v_u 值可以直接定义用户与商品发生交易的异常分数 s_{ui}，也可以结合异常分类模型值 $f(\vec{x})$，训练高阶分类模型 $w'_{ui} = f'(f(\vec{x}), v_u, v_i)$，同时考虑到用户与商品的交易网络边权重 W_{UI} 发生变化，可不断迭代传播算法即采用如下更新公式：

$$\begin{aligned} v_u &\leftarrow GraphModel(f(\vec{x}), v_u, v_i) \\ v_i &\leftarrow GraphModel(f(\vec{x}), v_u, v_i) \end{aligned} \tag{13.3}$$

当 v_u 与 v_i 值最终收敛后获得较为稳定的用户以及商品维度的全局异常交易分数，基于稳定的异常分数定义 s_{ui} 值，算法伪代码如下所示：

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

第十四章　融入商业策略的流量优化探索

学习目标与要求

14.1　商业变现模式对比

14.2　担保式流量分发系统的算法应用

14.2.1　基于 PID 控制器的流量分配模型

为了更好的服务品牌商家、满足其日常大促的活动需求，同时也为了与其它平台竞争，淘宝推出“流量包”计划。流量包的具体产品形态是，根据卖家需求和流量预估结果，平台与卖家达成一致的流量目标并签订协议，商家给平台提供优惠政策，平台通过推荐和搜索等场景投放卖家商品履行流量合约。这个产品不仅帮助商家实现了营销计划，同时也为平台提供了更优质的货源，买家也能从中获益。

具体到搜索层面，需要在完成流量目标的前提下最大化平台收益。商家希望获取高质量流量，平台需要协调商家流量并兼顾整体收益。由于两者相互影

响，所以需要统筹处理。从商家角度讲，希望分配到高质量的流量，比如高效率query、高转化用户的流量；从平台角度讲，对每次 pv 是否进行结果干预需要考虑干预与不干预之间的收益 gap，并且希望能实现这个收益 gap 的最大化。同时由于大促的特殊性，线上情况和历史表现存在较大的差异，单纯通过离线方式很难精确达到目标，需要实时的调控系统来实现流量目标的精确控制。

搜索场景下流量调控与推荐场景下流量调控的主要差异在于，搜索是有关键词的，被调控的对象必须满足搜索相关性的约束。所以，需要先为活动商家圈定一批关键词，称为进店 query，只在这些 query 下对活动商家的商品进行流量控制。在线上投放时，还会考虑用户是否是当前店铺的潜在用户。

14.2.2 流量分配

具体说来，流量分配就是从进店 query 中选择一部分 query 进行干预，比如增大活动商家商品的展现机会，在达到流量目标的前提下最大化平台收益。

目标

平台的整体收益可以用调控流量下卖家的收益与平台损失的收益差来表示，是否调控由店铺的点击收益和平台的点击损失共同决定。

约束

问题可形式化成如下的优化问题 假设流量干预下 q 到 s 的 ctr 与正常排序下 q 到 s 的 ctr 相同，且忽略位置对 ctr 的影响。为了方便求解，假设关键词的搜索量和点击率是固定的。事实上，大促期间关键词的主动搜索也是存在增量的，而且有一些关键词推荐场景会对活动商家的进店 query 进行引导，可以将 query 搜索量的变化带来的点击收益累计到目标中来。

由于大促的特殊性，线上情况和历史表现可能存在较大的差异，所以在离线预估了每个卖家 ctr 阈值的基础上，还需要用在线的 PID 控制器进行流量控制，也就是对每个卖家的 ctr 阈值进行在线调整。

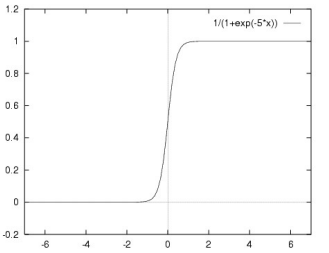


图 14.1: sigmoid

14.3 驱动供应链优化的流量分发系统设计

@ 仁重

14.4 商业流量与免费流量有效平衡的流量分发系统

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

[2] 流量个性化 v.s 商业化 - 双 11 珠峰项目中控算法, http://www.atatech.org/articles/67132

[3] 确定性保证下流量分配在线全局优化策略, http://www.atatech.org/articles/55983

[4] 搜索流量确定性项目总结, http://www.atatech.org/articles/59651

第十五章　新技术视角下的搜索智能化思考

学习目标与要求

15.1　多智能体学习

15.2　强化迁移学习

15.3　终生学习

参考文献

[1] C. Burges, T. Shaked, etc.., Learning to rank using gradient descent. In Proceedings of the 22nd international conference on machine learning, ACM

参考文献

[1] Dimitri P. Bertsekas，Dynamic Programming and Optimal Control, Vol. II, 4th Edition: Approximate Dynamic Programming