文章编号：2096-1472(2022)-12-50-04
DOI:10.19644/j.cnki.issn2096-1472.2022.012.010

基于对抗性训练的动态协同过滤推荐算法

黄大巧[1]，朱健军[2]，曹俊卓[2]

(1.浙江通信服务网络科技分公司，浙江 杭州 310000;
2.浙江工业大学信息学院，浙江 杭州 310000)
✉huangdaqiao@126.com; zjj@zjut.edu.cn; 2257416330@qq.com

摘　要：为了改进时间事件上的输入扰动或者攻击可能导致系统推荐性能大幅下降的问题，提出一种基于对抗性训练改进模型鲁棒性的协同过滤推荐算法。通过构建微小扰动对推荐模型进行训练，调整改进网络结构参数，从而提高系统的推荐准确度和抗干扰能力。通过在亚马逊数据集上的实验，并与几个基线模型进行不同Top-K推荐目标下的NDCG性能对比，结果表明：经过对抗训练的改进算法提升了系统鲁棒性，并且在中等扰动情况下可减少性能下降15%以上。

关键词：协同过滤推荐；鲁棒性；对抗性训练
中图分类号：TP182　**文献标识码**：A

Dynamic Collaborative Filtering Recommendation Algorithm based on Adversarial Training

HUANG Daqiao[1], ZHU Jianjun[2], CAO Junzuo[2]

(1.*Zhejiang Communication Service Network Technology Branch*, *Hangzhou* 310000, *China*;
2.*College of Information Engineering*, *Zhejiang University of Technology*, *Hangzhou* 310000, *China*)
✉huangdaqiao@126.com; zjj@zjut.edu.cn; 2257416330@qq.com

Abstract: Aiming at the problem that input disturbance or attacks on time events may lead to a significant drop in system recommendation performance, this paper proposes a collaborative filtering recommendation algorithm based on adversarial training to improve model robustness. The recommendation model is trained by constructing small disturbances, and the network structure parameters are adjusted and improved, thereby improving the recommendation accuracy and anti-interference ability of the system. Through experiments on the Amazon dataset and comparison of its NDCG (Normalized Discounted Cumulative Gain) performance with that of several baseline models under different Top-K recommendation targets, the results show that the improved algorithm after adversarial training enhances the robustness of the system and reduces the performance degradation by more than 15% under moderate disturbance.

Keywords: collaborative filtering recommendation; robustness; adversarial training

1 引言(Introduction)

因特网的广泛应用带来了爆炸式增长的信息冗余，虽然搜索引擎是当前人们获取目标信息的有效手段，但是仍然无法满足不同用户不同时间的个性化信息需求服务。推荐系统[1]可以通过分析用户的历史购买行为，基于挖掘用户、产品之间的特征相似性，向用户推荐其感兴趣的产品，刺激用户产生新的购买需求。其中，个性化推荐融合了数据处理、特征挖掘和机器学习等多种技术，成为当前数据挖掘和商业应用系统的热点研究领域之一[2]。

目前，通过神经网络进行图像分析和特征分类是推荐系统的重要环节，然而最新的研究发现，当对图像添加微小的扰动后，可能导致神经网络模型输出完全不同的分类结果，

基金项目：浙江省自然科学基金项目(LY18F010025,LY13F010011).

即微小的输入或噪声扰动都可能造成生成的推荐结果完全不同，这代表推荐系统的鲁棒性较差。

为了解决此问题，本文提出一种基于对抗性训练改进模型鲁棒性的协同过滤推荐算法。通过构建微小扰动并添加到推荐模型进行对抗性训练，从而调整网络结构参数，增强推荐模型的鲁棒性，算法通过亚马逊数据集进行了有效性验证。

2 推荐系统算法(Recommendation algorithms)

2.1 协同过滤推荐

基于用户的协同过滤[3]是根据用户的购买历史数据，根据特征嵌入将相似用户形成用户偏好组，即相似用户具有同类购买偏好，从而向其他用户预测和推荐物品。

基于用户协同过滤的推荐如图1所示，图1中的用户1和用户2都对物品A和B感兴趣，因此可以将用户1和用户2放入相似偏好的用户组；当发现用户1又喜欢物品C时，推荐算法可将物品C也推荐给用户2。

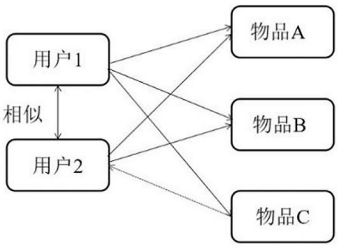

图1 基于用户协同过滤的推荐

Fig.1 Recommendation based on user collaborative filtering

研究人员采用皮尔森相似性表示用户相似度关系，其计算公式如下：

$$\ell_{u,v}=\frac{\sum_{p\in P_{u,v}}(r_{u,p}-\bar{r}_u)(r_{v,p}-\bar{r}_v)}{\sqrt{\sum_{p\in P_{u,v}}(r_{u,p}-\bar{r}_u)^2}\sqrt{\sum_{p\in P_{u,v}}(r_{v,p}-\bar{r}_v)^2}} \tag{1}$$

式(1)中，$r_{u,p}$、$r_{v,p}$分别表示用户u、v对物品集合p的评分向量。

2.2 CP分解算法

CP分解算法[4](图2)是目前数据分析领域常用的高维张量分解方法之一，可以降低参数维度，并且在计算复杂度上低于Tucker分解等方法。

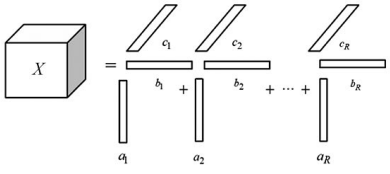

图2 CP分解算法

Fig.2 Candecomp decomposition algorithm

CP分解算法模型结构，计算如式(2)所示：

$$X\equiv\sum_{i=1}^{R}u_i\circ v_i\circ w_i \tag{2}$$

其中，$u_i\circ v_i\circ w_i$是秩为1的张量求和，R为正整数表示张量的秩，“∘”表示为外积运算，另一种表示如下：

$$X=\lambda;U,V,W \tag{3}$$

其中，$U\in R^{M\times r}$，$V\in R^{N\times r}$，$W\in R^{K\times r}$。λ是长度为r的向量，符合$0<\lambda_r\leqslant\cdots\leqslant\lambda_1$。向量$\lambda$在通常情况下往往被省略，从而得到式(4)：

$$X=U,V,W\equiv\sum_{\alpha=1}^{r}u_\alpha\circ v_\alpha\circ w_\alpha \tag{4}$$

3 推荐模型设计(Design of recommendation model)

3.1 动态协同过滤模型

商品的推荐通常与其时间属性相关，比如季节不同，人们对衣服的色调偏好会有不同。因此，时间属性作为推荐模型中一种时间序列上的感知参量，对精细化和个性化推荐有重要的意义。动态协同过滤(Dynamic Collaborative Filtering，DCF)[5]模型采用时间因子刻画时间尺度上的用户偏好，可以较好地提高推荐质量。

在模型中，r、p、q分别表示时间、用户和产品，评分S_1和S_2是用户—产品及产品—时间的相关度，比如S_1=1和S_2=1分别表示用户喜爱产品和合适的时间段即适合向用户推荐该产品。S_1和S_2可表示如下：

$$S_1=\sum_{i=1}^{K_1}U_{ip}V_{iq} \tag{5}$$

$$S_2=\sum_{j=1}^{K_2}T_{jr}W_{jq} \tag{6}$$

式(5)和式(6)中，$U\in R^{K_1\times P}$，$V\in R^{K_1\times Q}$，$T\in R^{K_2\times R}$，$W\in R^{K_2\times Q}$。因此，DCF模型可以定义式(7)：

$$\hat{A}_{pqr}=(U_{*p}^{T}V_{*q})(T_{*r}^{T}W_{*q}) \tag{7}$$

其中，$U_{*p}^{T}V_{*q}$和$T_{*r}^{T}W_{*q}$是特征因子的潜在表达，分别是用户购买偏好和产品时间特征。研究人员基于耦合矩阵张量分解(Coupled Matrix Tensor Factorization，CMTF)框架[6]对DCF模型进行张量分解，实现对模型中时间因子的动态协同过滤。

3.2 动态协同过滤模型的对抗性扰动添加

在DCF模型的基础上，研究人员进一步添加对抗性学习机制，提出了基于对抗性扰动的动态协同过滤(Adversarial Dynamic Collaborative Filtering，ADCF)模型(图3)。

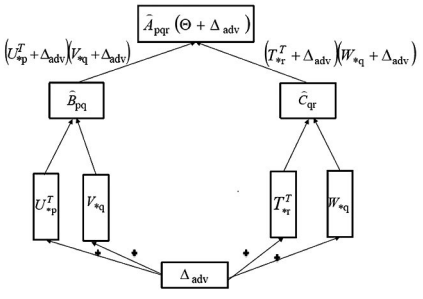

Fig.3 ADCF model framework

如图3所示，通过在DCF模型参数上添加对抗性扰动Δ_{adv}，如式(8)所示：

$$\hat{A}_{pqr}(\Theta+\Delta_{adv})=(U_{*p}^{T}+\Delta_{adv})(V_{*q}+\Delta_{adv})(T_{*r}^{T}+\Delta_{adv})(W_{*q}+\Delta_{adv}) \tag{8}$$

式(8)中，U、V、W、T分别是用户、产品、产品特征矩阵和时间因子特征，p、q、r分别是用户、物品、时间，$\Delta_{adv}\in R^{K}$是

模型参数上添加的对抗性扰动。

基于随机梯度下降法(Stochastic Gradient Descent，SGD)[7]训练模型到收敛状态，同时通过添加不同对抗性扰动，使得模型性能和稳定性降低，即该扰动目的就是最大化地降低模型性能，公式如下：

$$\Delta_{\text{adv}} = \arg \max_{\Delta,\|\Delta\|\leqslant\varepsilon} L'_{\text{BPR}}(D|\Theta) \tag{9}$$

式(9)中，$L'_{\text{BPR}}(D|\Theta)=L_{\text{BPR}}(D|\Theta+\Delta)$，$D$和$\Theta$分别是训练集和模型参数，$\varepsilon\geqslant 0$是添加扰动的幅度超参数，$\|\cdot\|$表示$L_2$范数。因此，目标函数可表示为式(10)：

$$L'_{\text{BPR}}(D|\Theta) = \sum_{(p\,q\,q'\,r)\in D_{pr}} -\ln\sigma\left(\hat{A}_{pqq'r}\right) + \lambda_1 \sum_{(p\,q\,q')\in D_q} - \ln\sigma\left(\hat{B}_{pqq'}\right) + \lambda_2 \sum_{(q\,q'\,r)\in D_r} -\ln\sigma\left(\hat{C}_{qq'r}\right) \tag{10}$$

其中，$\hat{A}_{pqq'r}$、$\hat{B}_{pqq'}$和$\hat{C}_{qq'r}$如式(11)—式(13)所示：

$$\hat{A}_{pqq'r} = \hat{A}_{pqr}(\Theta + \Delta_q) - \hat{A}_{pq'r}(\Theta + \Delta_{q'}) \tag{11}$$

$$\hat{B}_{pqq'} = \hat{B}_{pq}(\Theta + \Delta_q) - \hat{B}_{pq'}(\Theta + \Delta_{q'}) \tag{12}$$

$$\hat{C}_{qq'r} = \hat{C}_{qr}(\Theta + \Delta_q) - \hat{C}_{q'r}(\Theta + \Delta_{q'}) \tag{13}$$

通过训练减弱算法模型对微小扰动的敏感性，从而最终得到在对抗性扰动下具有较高鲁棒性的模型，模型优化目标如式(14)所示：

$$\Theta^* = \arg\min_{\Theta} L_{\text{BPR}}(D|\Theta) + \lambda L'_{\text{BPR}}(D|\Theta) \tag{14}$$

式(14)中，λ是控制被扰动模型影响程度的超参数，其值越大，则说明加入的扰动越大，当值为0时，则表示无扰动。

因此，ADCF模型所进行的对抗性训练类似于进行极大值−极小值的零和博弈，如式(15)所示：

$$\Theta^*, \Delta^* = \arg\min_{\Theta} \max_{\Delta,\|\Delta\|\leqslant\varepsilon} L_{\text{BPR}}(D|\Theta) + \lambda L'_{\text{BPR}}(D|\Theta) \tag{15}$$

模型参数Θ和扰动Δ是游戏的两个玩家，总是尽量最小化己方的损失并最大化对方的损失。对所有可能要发生的情况进行遍历后就会进入平衡状态，即算法模型得到收敛。

上述的ADCF扰动模型包括两个超参数ε和λ。其中，ε是对抗性学习中加入的扰动程度，λ是由于扰动所产生的损失在总损失中的大小，即对模型的影响程度。过大或过小的超参数值都可能达不到对模型的扰动调优效果，因此在模型训练时需要进行有效调参。

4 实验设计(Experimental design)

4.1实验数据集

本文采用亚马逊购物网站的鞋子数据集进行算法验证，并与五个常用的基线算法进行性能对比。

表1是数据集的统计特性，数据集被随机分成训练集(80%)、验证集(10%)和测试集(10%)，分别用于模型参数训练、超参数验证调整和性能测试。

表1 亚马逊数据集统计特性表

Tab.1 Table of statistics characteristics of Amazon dataset

数据源	购买记录/条	用户数/个	商品数/个
亚马逊	94,560	32,538	8,231

4.2 实验环境

实验验证的硬件环境包括Inteli7−8700的CPU，RTX2080的计算显卡，32 GB的内存；软件环境操作系统为Win10，算法框架为Tensorflow。

4.3 评价指标

本文使用NDCG作为性能评估指标，如式(16)所示：

$$NDCG = \frac{DCG_p}{IDCG_p} \tag{16}$$

NDCG表示将推荐结果的Top−K列表中产品i相关度与理想列表相比的排序准确性，该值越大，则表示推荐列表中物品位置顺序越准确。

5 实验结果分析(Experimental results analysis)

研究人员对实验结果进行以下分析：(1)推荐准确度性能对比；(2)模型鲁棒性对比；(3)扰动超参数ε的影响。

5.1 推荐准确度性能对比

针对ADCF算法性能，分别在$K=5$、10和15时，对五种基线算法进行Top−K的NDCG指标对比。

表2是和基线算法的对比结果，表明个性化推荐方法可以提高推荐准确度。比如，相比非个性化的POP排序方法，MF、AMR、VBPR、DCF和ADCF等基于隐式反馈算法可以挖掘交易过程隐含的互动特征，超过了简单的产品时间流行度特征排序，从而使针对不同用户的推荐更具个性化，因此总体效果更为好。

表2 NDCG指标下的性能对比

Tab.2 Performance comparison based on NDCG index

对比算法	K=5	K=10	K=20
POP	0.00035	0.00023	0.00070
MF[8]	0.00192	0.00184	0.00176
AMR[9]	0.00235	0.00211	0.00179
VBPR[10]	0.00232	0.00204	0.00181
DCF[5]	0.00162	0.00141	0.00118
ADCF	**0.00303**	**0.00260**	**0.00206**

同时，对抗性训练过后的模型性能都有较大的提升。比如，AMR、ADCF相比MF、DCF的性能提升充分说明对抗性学习可以挖掘更全面的数据特征，从而达到了更显著的推荐效果；进一步，通过横向比较可以发现所有模型随着K的增加都呈下降趋势，但增加了对抗性扰动的ADCF模型的推荐效果更稳定。

5.2 模型鲁棒性对比

为了进行鲁棒性验证，研究人员首先对DCF模型进行迭代训练直至达到收敛状态，然后在该收敛模型参数上进行对抗性扰动，用于破坏当前模型的稳定状态，并且再次通过网络参数的迭代和更新适应不同扰动，从而实现新的收敛状态。

表3中的数据是鲁棒性实验结果对比。表3首先记录了DCF和ADCF模型在加入相同大小扰动后的性能变化幅度，也记录了加入不同大小扰动后的性能下降情况。比如，当ε=0.05时，DCF和ADCF的性能对比无扰动状态，分别下降了10.5%和4.64%，DCF性能的下降幅度远大于ADCF，即表明添加扰动训练后的ADCF模型相比DCF，对于不同程度的扰动和噪声的稳定性更强，即网络参数可以更好地适应外界的微小干扰，从而有效增强了系统的鲁棒性。

表3 NDCG指标下不同 ε 的鲁棒性对比

Tab.3 Robustness comparison under different ε based on NDCG index

NDCG	ε=0.05	ε=0.1	ε=0.5
DCF	10.5%	18.5%	33.7%
ADCF	**4.64%**	**2.40%**	**2.60%**

5.3 扰动超参数ε的影响

图4是超参数对模型性能影响的结果图。为了研究控制扰动幅度的超参数ε对模型的影响，研究人员先将另一个正则化超参数λ固定为1，计算了不同ε取值(即不同大小的扰动)情况下对NDCG@5推荐效果的影响。当ε在0.001—1时，模型性能呈显著下降趋势，随后性能呈小幅度变化。

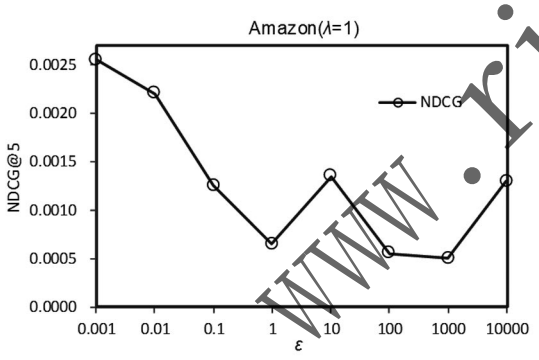

图4 ε对ADCF模型性能的影响

Fig.4 Effect of ε on the performance of ADCF model

6 结论(Conclusion)

本文针对改进推荐系统的鲁棒性问题，提出了一种基于对抗性训练的动态协同过滤算法，通过在模型上加入微小扰动并通过对抗性训练方式改进模型参数，从而增强推荐系统的鲁棒性。通过在亚马逊数据集上实验并与基线模型对比，结果表明经过对抗训练的改进算法，相比原始算法可减少推荐性能下降15%以上，即有效改进了模型的鲁棒性，同时有效提升了推荐准确度。接下来可以进一步考虑融入商品视觉和序列交互特征等提升推荐算法的准确度，还可以研究显示反馈对推荐算法的影响。

参考文献(References)

[1] BOBADILLA J, ORTEGA F, HERNANDO A, et al. Recommender systems survey[J]. KnowledgeBased Systems, 2013, 46(1):109−132.

[2] 黄川林,鲁艳霞.基于协同过滤和标签的混合音乐推荐算法研究[J].软件工程,2021,24(4):10−14.

[3] ADOMAVICIUS G, TUZHILIN A. Toward the next generation of recommender systems: A survey of the state−of−the−art and possible extensions[J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(6):734−749.

[4] LIU Y Y, SHANGF H, JIAO L C, et al. Trace norm regularized CANDECOMP/PARAFAC decomposition with missing data[J]. IEEE Transactions on Cybernetics, 2015, 45(11): 2437−2448.

[5] BURY M, SCHWIEGELSHOHN C, SORELLA M. Similarity search for dynamic data streams[J]. IEEE Transactions on Knowledge and Data Engineering, 2020, 32(11):2241−2253.

[6] IOANNIDIS V N, ZAMZAM A S, GIANNAKIS G B, et al. Coupled graphs and tensor factorization for recommender systems and community detection[J]. IEEE Transactions on Knowledge and Data Engineering, 2021, 33(3):909−920.

[7] LEI Y W, HU T, LI G Y, et al. Stochastic gradient descent for nonconvex learning without bounded gradient assumptions[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(10):4394−4400.

[8] HE X N,TANG J H, DU X Y, et al. Fast Matrix factorization with nonuniform weights on missing data[J].IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(8): 2791−2804.

[9] TANG J H, DU X Y, HE X N, et al. Adversarial training towards robust multimedia recommender system[J].IEEE Transactions on Knowledge and Data Engineering, 2020, 32(5):855−867.

[10] GAO X Y, FENG F L, HE X N, et al. Hierarchical attention network for visually−aware rood recommendation[J]. IEEE Transactions on Multimedia, 2020, 22(6):1647−1659.

作者简介：

黄大巧(1972−)，男，硕士，工程师.研究领域：推荐系统，网络分析.

朱健军(1974−)，男，博士，讲师.研究领域：推荐系统，物联网技术.

曹俊卓(1994−)，男，硕士，讲师.研究领域：推荐系统，数据挖掘.本文通信作者.