Mitigating Confounding Bias in Recommendation via Information Bottleneck

Dugang Liu∗
Shenzhen University
Shenzhen, China
dugang.ldg@gmail.com

Hong Zhu
Zhenhua Dong
Xiuqiang He
Huawei Noah’s Ark Lab
Shenzhen, China

Pengxiang Cheng∗
Huawei Noah’s Ark Lab
Shenzhen, China
chengpengxiang1@huawei.com

Zhong Ming†
Shenzhen University
Shenzhen, China
panweike,mingz@szu.edu.cn

ABSTRACT
How to effectively mitigate the bias of feedback in recommender systems is an important research topic. In this paper, we first describe the generation process of the biased and unbiased feedback in recommender systems via two respective causal diagrams, where the difference between them can be regarded as the source of bias. We then define this difference as a confounding bias, which can be regarded as a collection of some specific biases that have previously been studied. For the case with biased feedback alone, we derive the conditions that need to be satisfied to obtain a debiased representation from the causal diagrams. Based on information theory, we propose a novel method called debiased information bottleneck (DIB) to optimize these conditions and then find a tractable solution for it. In particular, the proposed method constrains the model to learn a biased embedding vector with independent biased and unbiased components in the training phase, and uses only the unbiased component in the test phase to deliver more accurate recommendations. Finally, we conduct extensive experiments on a public dataset and a real product dataset to verify the effectiveness of the proposed method and discuss its properties.

CCS CONCEPTS
• Information systems → Recommender systems.

KEYWORDS
Confounding bias, Causal diagrams, Recommender systems, Information bottleneck

1 INTRODUCTION
As a feedback loop system, a recommender system is associated with various biases during the interaction between the user and the system, such as position bias [3, 38], selection bias [27, 32] and popularity bias [1, 6]. Ignoring these biases will cause a recommendation model to converge to a biased sub-optimal solution, and have harmful effects on the recommender system and the users, such as filter bubbles [16], echo chambers [11] and unfairness [10]. Therefore, how to effectively alleviate the bias of the feedback data collected in a recommender system is an important problem.

The previous works solving the bias problem in recommender systems mainly include the following four lines, i.e., heuristic-based methods [25, 43], inverse propensity score-based methods [32, 44, 45], unbiased data augmentation methods [5, 23, 39, 46], and some theoretical tools-based methods [30, 31]. The first line assumes that user feedback depends on certain specific factors and models this relationship, such as item features [12, 20] and public opinions [22, 24]. The second line uses the inverse propensity score as the sample weight to adjust the biased feedback distribution. The third line introduces a special uniform data as an unbiased target data to guide the training of the biased feedback. The last line aims to couple certain theoretical tools with the bias problem, and uses these theoretical tools to design some debiasing models, such as information bottleneck and causal inference techniques [37, 40–42]. However, most methods ignore the bias generation process, and thus may only be applicable to a certain type of bias problem.

In this paper, inspired by [13, 18], we first describe the generation process of the biased feedback and unbiased feedback in recommender systems via two respective causal diagrams, where the difference between them can be regarded as the source of bias. We define this difference as a confounding bias, which can be regarded as a collection of some specific biases that have been studied in
previous works. To simplify and match the main models in the recommendation field, we generally assume that the confounding bias will be reflected in the embedding representation of a recommendation model trained with a biased feedback data. Moreover, we propose a debiased information bottleneck (DIB) objective function to alleviate the confounding bias in the biased feedback without an unbiased data.

Specifically, the proposed method is based on our observations in the causal diagrams of the feedback generation process described above. In the training phase, we constrain the model to learn a special biased embedding vector, including a biased component responsible for the effect of the confounding bias, and an unbiased component responsible for the effect of the user’s true preference. To remove the influence of the confounding bias in the test phase, we only retain the unbiased component in the embedding vector in the process of recommending items, i.e., a debiased embedding vector. The proposed method has better interpretability because it is directly derived from the causal diagram of the bias generation process. In addition, the proposed method can be used to solve a more general bias problem because the confounding bias is essentially a fusion of some specific biases. Finally, we conduct extensive experiments on a public dataset and a real product dataset to verify the effectiveness of the proposed method, including standard unbiased tests, ablation studies, and some in-depth analysis of the proposed method.

2 RELATED WORK

2.1 Debiasing in Recommender Systems

Solving the bias problem in recommender systems is an important topic that has gradually received more attention by both the researchers and practitioners from the academia and industry. The existing works on debiasing in recommender systems can be categorized into four classes, including heuristic-based methods, inverse propensity score-based methods [32, 44, 45], unbiased data augmentation methods [5, 23, 39, 46], and some theoretical tool-based methods. A heuristic-based method links a user’s feedback with different specific factors, such as item features [12, 20], user ratings [25, 43] and public opinions [22, 24], and uses some probabilistic graphical models for modeling. An inverse propensity score-based method corrects the biased feedback distribution by introducing some sample weights. An unbiased data augmentation method guides the model training on unbiased feedback by introducing an unbiased data collected by a special uniform policy. Since the collection process of an unbiased data is very expensive in practice, some recent methods directly perform debiasing on one single biased data with some theoretical tools, such as information bottleneck [40], upper bound minimization [31], asymmetric tri-training [30], and causal inference techniques [37, 41, 42].

2.2 Information Bottleneck

The information bottleneck method is a technique in information theory for finding the best trade-off between accuracy and complexity [35]. It has been regarded as a theoretical foundation of deep learning and been applied to many fields, such as robust or invariant representation learning [9, 26], disentangled representation learning [2], compressed representation learning [8], causal inference [28] and feature detection [33]. The works most relevant to ours in this line are [7, 15]. They focus on learning disentangled representation of texts through customized information bottleneck loss when the labels that only indicate the style information of texts are given. This representation includes independent style embedding and content embedding, which is similar to our expectation that the biased and unbiased components in the biased embedding vector are as independent as possible. However, these methods are not applicable to the recommender systems since the labels in the recommendation field indicate a mixture of user preferences and bias. In addition, as far as we know, there is only one work that considers the use of information bottleneck to solve the bias problem in recommender systems. That work is based on contrastive analysis of feature embedding, which proposes a counterfactual variational information bottleneck method to solve the selection bias in the recommender systems [40].

3 NOTATIONS AND PROBLEM FORMULATION

3.1 Notations

Let $X = X_1 \times \cdots \times X_d$ be a $d$-dimensional observed feature space and $Y = \{0, 1\}$ be a label space. In this paper, we focus on solving the bias problem in recommender systems. Specifically, suppose we have the following $N$ events

$$x^1, y^1, \ldots, x^N, y^N,$$

where $x^i = (x^i_1, \ldots, x^i_d) \in X$ and $y^i \in Y$ are the feature vector and the label of the $i$-th event, respectively. According to the nature of feedback in a typical recommender system, we assume that the label $y$ satisfies

$$y = \begin{cases} 1 & \text{the event was displayed and clicked,} \\ 0 & \text{the event was displayed but not clicked.} \end{cases}$$

An event represents an interaction between a user and a system. For example, a commercial system recommends a movie or displays an advertisement to a user. In particular, when no side information is available, i.e., only the user ID $u$ and the item ID $i$ are provided, an event can be simplified to $(x = (u, i), y)$.

The feedback events are used to train the recommendation model, which evaluates the users’ preference on the item set as accurately as possible by learning a decision function $\hat{y}(x) \in (-\infty, +\infty)$. In practice, the decision function is usually implemented based on a low-rank model and a neural network model, which are also included in our experiments. Both of them apply an embedding vector $z^*$ as a representation of the input $x$. Therefore, we can describe the decision function as a mapping process from the representation $z^*$ to the label $\hat{y}$, which passes through one or more hidden layers $h_j$. This process can be formalized as a Markov chain of successive representations $[40], y \rightarrow x \rightarrow z^* \rightarrow h_1 \rightarrow \cdots \rightarrow h_L \rightarrow \hat{y}$.

3.2 Confounding Bias and Problem Formulation

To better understand the source of bias and address it in a targeted manner, in Figure 1(a), we show the generation process of feedback events in recommender systems from the perspective of causal
Mitigating Confounding Bias in Recommendation via Information Bottleneck

RecSys ’21, September 27-October 1, 2021, Amsterdam, Netherlands

Liu and Cheng et al.

\[ I(z;r) = I(z;y) - H(y|r) + H(y|z,r) \]  

(7)

Figure 1: (a) A causal diagram of biased feedback, where \( x \) and \( y \) are known variables, blue arrows indicate the indirect effect and red arrows indicate the direct effect. (b) A causal diagram of unbiased feedback where the indirect effect are truncated.

inference. The input variables \( x \) (i.e., the feature vector) can be divided into three parts, including the instrumental variables \( I \), the confounder variables \( C \) and the adjustment variables \( A \). The instrumental variables \( I \) and the confounder variables \( C \) determine the treatment \( T \), and they have an indirect effect on the outcome \( y \) (i.e., the label) through the path \( \{I, C\} \rightarrow T \rightarrow y \). The confounder variables \( C \) and the adjustment variables \( A \) have a direct effect on \( y \) through the path \( \{C, A\} \rightarrow y \). Similar causal diagrams can also be found in previous works on treatment effect estimation [13, 18], and we follow their assumptions, i.e., strong ignorability [29]. The term “treatment” in recommender systems can be thought of as referring to a recommendation strategy; this is, which items the system selects, as well as how the system organizes and shows these items to some specific users.

Different recommendation strategies will produce different direct effects on feedback events by influencing the treatment \( T \). This will lead to the inherent variability in the feedback events, and make most recommendation models that aim to minimize the error of the observed feedback not have good generalizability. Conversely, because the direct effect does not depend on the treatment, it can be considered as a stable and true user preference. This means that if we can cut off the indirect effect, i.e., we have a special strategy that only depends on the direct effect, then the collected feedback events are relatively stable and unbiased. We show the generation process of this unbiased feedback event in Figure 1(b). By comparing Figure 1(a) and 1(b), we call the bias brought by the recommendation strategy the confounding bias. Confounding bias is essentially a collection of biases at the system level, such as the position bias and popularity bias.

**Definition 3.1 (Confounding Bias).** Suppose that the variables \( x \), the outcome \( y \), the indirect effect \( \{I, C\} \rightarrow T \rightarrow y \) and the direct effect \( \{C, A\} \rightarrow y \) from \( x \) to \( y \) are given. Confounding bias refers to the confusion of the observed feedback in recommender systems caused by the indirect effect.

On the other hand, previous works have shown that the unbiased feedback can be obtained through a uniform policy [5, 23, 39, 46], i.e., for user requests, the system randomly samples items from a candidate set, and displays them after some random arrangement. However, the uniform policy will harm the user experience and reduce the platform revenue. Hence, a more appealing scenario is that only the biased feedback is available. Therefore, in this paper, we focus on mitigating the confounding bias with the biased feedback alone.

4 THE PROPOSED METHOD

In practice, it may be difficult to directly group the variables \( x \) to obtain the instrumental variables \( I \), the confounder variables \( C \) and the adjustment variables \( A \). Instead, since the goal of most recommendation models is to learn an accurate embedding representation vector derived from the variables \( x \), we make a general assumption, which is intuitively reasonable. The representation \( z^* \), which is a good proxy for the variables \( x \), naturally suffers from the influence of the biased variables in \( x \). Since the correspondence between the biased variables and the semantics of the dimension in \( z^* \) is difficult to be obtained, \( z^* \) is also indistinguishable.

**Assumption 4.1.** The confounding bias will be reflected in the embedding representation learned by a traditional recommendation model, and the bias will usually corrupt all the dimensions, i.e., the original representation \( z^* \) is biased and indistinguishable.

Based on this assumption, we illustrate the main idea of the proposed method in Figure 2. In the training phase (i.e., Figure 2(a)), we constrain the model to obtain a special biased representation vector from the variables \( x \), which includes two independent components, i.e., a biased component \( r \) and an unbiased component \( z \). The biased component \( r \) is responsible for the indirect effect, while the unbiased component \( z \) is responsible for the direct effect. Note that this special biased embedding vector, i.e., \([r, z] \), is easier to distinguish the influence of the confounding bias than the original representation \( z^* \). In the test phase (i.e., Figure 2(b)), we discard the biased component and only use the unbiased component for more accurate recommendation.
Figure 2: (a) In the training phase, the model obtains a special biased embedding vector from the variables \( x \), which includes a biased component \( r \) and an unbiased component \( z \). (b) In the test phase, the biased component \( r \) is discarded, and the unbiased component \( z \) is used in the recommendation process.

From Figure 1(a), we can see that in order to meet our expectation on more accurate recommendation, we have to satisfy the following conditions: 1) to avoid the influence of the biased variables, the unbiased component \( z \) should not overfit the variables \( x \); 2) due to the role of the direct effect, the unbiased component \( z \) needs to predict the label \( y \) as accurately as possible; 3) the biased component \( r \) and the unbiased component \( z \) must be as independent as possible to get a better distinction, i.e., \( z \perp r \); and 4) due to the role of the indirect effect, the biased component \( r \) is also beneficial to predict the label \( y \) to a certain extent. Note that we have not constrained the relationship between the biased component \( r \) and the variables \( x \), because the degree of dependence between them is determined by the strength of the bias in the feedback data, and blindly optimizing it may lead to bad results. Inspired by information theory, we can then derive the required objective function to be minimized from the above analysis,

\[
L_{DIB} := \min \beta I(z;x) + I(z;y) + \gamma I(z;r) - \alpha I(z;y|r), \tag{3}
\]

where term (1) is a compression term that describes the mutual information between the variables \( x \) and the unbiased embedding \( z \); term (2) is an accuracy term that describes the performance of the unbiased embedding \( z \); term (3) is a de-confounder penalty term, which describes the dependency degree between the biased embedding \( r \) and the unbiased embedding \( z \); and term (4) is similar to term (2), which is used for the potential gain from the biased embedding \( r \). Note that \( \beta, \gamma \) and \( \alpha \) are the weight parameters. Since terms (1) and (2) in Eq.(3) are similar to a standard information bottleneck, we call the proposed method a debiased information bottleneck, or DIB for short. By optimizing \( L_{DIB} \), we expect to get the desired biased and unbiased components, and can then prune the confounding bias.

## 5 A TRACTABLE OPTIMIZATION FRAMEWORK

\( L_{DIB} \) is clearly an intractable optimization function, especially the key term \( I(z;r) \) used to induce the desired embedding separation. Next, we discuss the optimization of the de-confounder penalty term \( I(z;r) \) and the compression term \( I(z;x) \), and derive an upper bound of Eq.(3). Finally, we describe a tractable solution for the objective function \( L_{DIB} \) according to the upper bound.

### 5.1 The De-confounder Penalty Term

Based on the chain rule of mutual information, we have the following equation about the de-confounder penalty term \( \gamma \) in Eq.(3),

\[
I(z;r) = I(z;y) - I(z;y|r) + I(z;r|y). \tag{4}
\]

We further inspect the term \( I(z;r|y) \) in Eq.(4). Since the distribution of \( z \) depends solely on the variables \( x \), and \( x \) is affected by \( y \), we have \( H(z|y, r) = H(z|y) \), where \( H(\cdot|\cdot) \) denotes the conditional entropy [15, 26]. Combining the properties of mutual information, we have,

\[
I(z;r|y) = H(z|y) - H(z|y, r) = H(z|y) - H(z|y) = 0. \tag{5}
\]

By substituting Eq.(5) into Eq.(4), we have,

\[
I(z;r) = I(z;y) - I(z;y|r). \tag{6}
\]

Since the term \( I(z;y|r) \) in Eq.(6) is still difficult to be calculated, we use the form of conditional entropy to further simplify it,

\[
I(z;r) = I(z;y) - H(y|r) + H(y|z, r). \tag{7}
\]
Finally, combining Eq.(3) and Eq.(7), we can rewrite the objective function $L_{\text{DIB}}$ in Eq.(3) as follows,

$$L_{\text{DIB}} = \beta I(z; x) - I(z; y) + \gamma I(z; r) - \alpha I(r; y)$$

$$= \beta I(z; x) - I(z; y) + \gamma (I(z; y) - H(y) + H(y|z,r)) - \alpha I(r; y)$$

$$= \beta I(z; x) - (1 - \gamma) I(z; y) - \gamma H(y) + \gamma H(y|z,r) - \alpha I(r; y).$$

(8)

5.2 The Compression Term

We can find that only the compression term $I(z; x)$ is related to the variables $x$ in Eq.(8). To optimize it directly, we describe a simple and precise expression of this mutual information using a method similar to that in [15, 40]. First, based on the relationship between mutual information and Kullback-Leibler (KL) divergence, the compression term $I(z; x)$ can be calculated as follows,

$$I(z; x) = \mathbb{E}_x \left[ D_{\text{KL}}(p(z|x) \parallel p(z)) \right]$$

$$= \sum_x p(x) \sum_{z} p(z|x) \log p(z|x) - \sum_z p(z) \log p(z).$$

(9)

However, the marginal probability $p(z) = \sum_x p(x|z)p(x)$ is usually difficult to be calculated in practice. We use variational approximation to address this issue, i.e., we use a variational distribution $q(z)$ instead of $p(z)$. According to Gibbs’ inequality, we know that the KL divergence is non-negative. Therefore, we can derive an upper bound of Eq.(9),

$$D_{\text{KL}}(p(z) \parallel q(z)) \ge 0$$

$$\Rightarrow - \sum_z p(z) \log p(z) \le - \sum_z p(z) \log q(z)$$

$$\Rightarrow D_{\text{KL}}(p(z|x) \parallel p(z)) \le D_{\text{KL}}(p(z|x) \parallel q(z)).$$

(10)

Similar to most previous works [21], we can assume that the posterior $p(z|x) = \mathcal{N}(\mu(x), \text{diag}(\sigma^2(x)))$ is a Gaussian distribution, where $\mu(x)$ is the encoded embedding of the variables $x$ and $\text{diag}(\sigma^2(x))$ is the diagonal matrix indicating the variance. Through the reparameterization trick, the embedding $z$ can be generated according to $z = \mu(x) + \epsilon \sigma(x)$, where $\epsilon \sim \mathcal{N}(0, I)$. Obviously, if we fix $\sigma(x)$ to be an all-zero matrix, $z$ will reduce to a deterministic embedding. On the other hand, the prior $q(z)$ is assumed to be a standard Gaussian variational distribution, i.e., $q(z) = \mathcal{N}(0, I)$. Finally, we can rewrite the upper bound,

$$D_{\text{KL}}(p(z|x) \parallel q(z)) = \frac{1}{2} \| \mu(x) \|^2 + \frac{1}{2} \sum_d (\sigma^2_d - \log \sigma^2_d - 1).$$

(11)

where $\sigma^2_d$ is an element in $\text{diag}(\sigma^2(x))$, i.e., $\text{diag}(\sigma^2(x)) = (\sigma^2_d)_{d=1}^D$. This means that for a deterministic embedding $z$, we can optimize this upper bound by directly applying the $\ell_2$-norm regularization on the embedding vector $z$, which is equivalent to optimizing the compression term $I(z; x)$. Note that the compression term in previous works act on the entire biased representation $z^*$, and we only compress the unbiased component $z$ of the representation.

5.3 Algorithm

For the mutual information $I(z; y)$ in Eq.(8), we have $I(z; y) = H(y) - H(y|z)$. Since $H(y)$ is a positive constant and can be ignored, we have the following inequality,

$$I(z; y) \ge -H(y|z).$$

(12)

This inequality also applies to the mutual information $I(r; y)$ in Eq.(8). Combining Eq.(11) and Eq.(12), we can rewrite Eq.(8) as follows,

$$L_{\text{DIB}} = \beta I(z; x) - (1 - \gamma) I(z; y) - \gamma H(y) + \gamma H(y|z) - \alpha I(r; y)$$

$$\le \beta \| \mu(x) \|^2 + (1 - \gamma) \gamma H(y) - (\gamma - \alpha) H(y) + \gamma H(y|z, r).$$

(13)

Finally, we get a tractable solution for $L_{\text{DIB}}$.

$$\hat{L}_{\text{DIB}} = (1 - \gamma) \hat{H}(y|z) - (\gamma - \alpha) \gamma H(y) + \beta \| \mu(x) \|^2.$$  

(a) \quad (b) \quad (c) \quad (d) \quad (14)

where $0 < \alpha < \gamma < 1$. Let $\hat{y}_r, \hat{y}_z$, and $\hat{y}_{z,c}$ be the predicted labels generated by the biased component $r$, the unbiased component $z$, and the biased embedding vector $[z, r]$ as shown in Figure 2(a), respectively, the final objective function also contains four terms: term (a) denotes the cross entropy between $\hat{y}_z$ and $y$; term (b) denotes the cross entropy between $\hat{y}_r$ and $y$; term (c) denotes the cross entropy between $\hat{y}_{z,c}$ and $y$; and term (d) is the regularization term to improve the robustness of the embedding representation. A complete optimization process of DIB is shown in Algorithm 1.

Algorithm 1 Debiasing Information Bottleneck (DIB)

Input: Observed feedback events $\{(x, y)\}$; hyper-parameters $\alpha, \beta, \gamma$

1. Initialize the parameters of the model $\theta$ (including the biased embedding representation $r$ and the unbiased embedding representation $z$);

2. repeat

3. Calculate term (c) in Eq.(14) by the concatenation of $z$ and $r$, i.e., $H(y|z, r)$;

4. Calculate term (a) in Eq.(14) by $z$, i.e., $H(y|z)$ (to keep the dimensions consistent, $z$ is concatenated with a zero vector with the same dimension of $r$);

5. Calculate term (b) in Eq.(14) by $r$, i.e., $H(y|r)$ (similar to the above operation);

6. Calculate term (d) in Eq.(14) by applying regularization to $z$;

7. Update the model parameters $\theta$ via stochastic gradient descent based on $L_{\text{DIB}}$ (i.e., Eq.(14));

8. until training loss stops to decrease.

6 EXPERIMENTS

In this section, we conduct comprehensive experiments with the aim of answering the following three key questions.

- RQ1: How does the proposed method perform against the baselines in an unbiased evaluation?
- RQ2: What is the role of each term in the proposed method (i.e., the ablation studies of our DIB)?
- RQ3: What are the characteristics of the proposed method in the training process?

6.1 Experiment Setup

6.1.1 Datasets. In order to evaluate the performance of the model in mitigating the confounding bias, we need a test set that includes
unbiased feedback events to simulate the ideal distribution. We consider both a public dataset and a real-world product dataset in the experiments, where the statistics are described in Table 1.

- **Yahoo! R3**: This dataset contains ratings collected from two different sources on Yahoo! Music services, containing 15,400 users and 1000 songs. The user set consists of ratings provided by users’ subjective choices and is therefore considered to be biased. The random set consists of ratings collected during an online survey, i.e., each of the first 5400 users is required to provide ratings on ten randomly displayed songs, which can be considered unbiased. We binarize each rating by checking whether it is larger than 3 and then obtain some positive feedback and negative feedback. Note that the missing entries are treated as negative feedback. For the user set, we randomly split it into two subsets from the user level: 80% of each user’s feedback for training and the remaining 20% for validation to tune the hyper-parameters. The random set is used as the test set for evaluating our method.

- **Product**: This is a large-scale dataset for CTR prediction, which includes two weeks of user click records from a real-world advertising system. This data covers 122 displayed advertisements and approximately 300,000 users. Similarly, it contains a user set and a random set. The user set is recorded when the system is using several traditional ranking-oriented recommendation policies, and the random set is recorded using a uniform policy. Next, we randomly split the user set into two subsets in the same way as that for Yahoo! R3, i.e., 80% feedback is used as the training set, and the rest is used as the validation set. The entire random set is used as the test set.

### Table 1: Statistics of the datasets. P/N represents the ratio between the numbers of positive and negative feedback.

<table>
<thead>
<tr>
<th></th>
<th>Yahoo! R3</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#Feedback</td>
<td>P/N</td>
</tr>
<tr>
<td>training</td>
<td>254,713</td>
<td>67.02%</td>
</tr>
<tr>
<td>validation</td>
<td>56,991</td>
<td>67.00%</td>
</tr>
<tr>
<td>test</td>
<td>54,000</td>
<td>9.64%</td>
</tr>
</tbody>
</table>

**6.1.2 Evaluation Metrics.** For all experiments, we employ four evaluation metrics that are widely used in recommender systems, including the area under the ROC curve (AUC), precision (P@K), recall (R@K) and normalized discounted cumulative gain (nDCG). We set the length of the recommendation list as 50, and choose AUC as our main evaluation metric because it is one of the most important metrics in the industry and previous works on debiasing. Due to space limitation, we report the results of P@K and R@K important metrics in the industry and previous works on debiasing.

**6.1.3 Baselines.** Since most debiasing methods are integrated into some existing recommendation models, in order to evaluate the generalization of our method, we adopt two of the most common recommendation models as the backbones, i.e., matrix factorization (MF) [17] and neural collaborative filtering (NCF) [14]. In addition, among the four lines of debiasing methods summarized in Sec. 2.1, the heuristic-based methods are usually inefficient, and the unbiased data augmentation methods are not suitable for the scenario where only a biased data is available for training in this paper. Therefore, we choose the representative methods in the other two lines as the baselines. Note that based on different backbones, each of these baselines has two versions.

- **MF [17]**: This is one of the most classic recommendation models. The user-item interaction matrix is factorized to learn the representation of the users and items, and their inner products are used to predict the preferences.

- **NCF [14]**: This is one of the most classic recommendation models combined with neural networks. Compared with the linearity of matrix factorization, neural networks are used to model the nonlinear relationship between users and items to further improve the recommendation performance.

- **IPS [32]**: This is a representative method based on the inverse propensity score (IPS) in debiasing recommendation. The estimated propensity score is used as the weight of the training feedback to adjust the biased distribution of recommendation. We estimate the propensity score of item $i$ for any user via the relative item popularity,

$$P_{u,i} = \left( \frac{\sum_{u \in U} O_{u,i}}{\max_{i \in I} \sum_{u \in U} O_{u,i}} \right)^{\eta},$$

where $O_{u,i}$ indicates the observation status of user $u$ for item $i$, i.e., $O_{u,i} = 1$ means that the user $u$ observes the item $i$, while $O_{u,i} = 0$ is the opposite, and $\eta$ is a control weight used to adapt to different datasets. Similar methods have also been adopted in previous works [19, 31].

- **SNIPS [34]**: The above method based on the inverse propensity score has the problem of high variance. To solve this problem, a self-normalized inverse propensity score is proposed and can be written as,

$$\hat{L}_{SNIPS} = \frac{\sum_{(u,i) \in D} \frac{L(\hat{Y}_{u,i}, Y_{u,i})}{P_{u,i}}}{\sum_{(u,i) \in D} \frac{1}{P_{u,i}}},$$

where $P_{u,i}$ is calculated according to Eq.(15), and $L(\hat{Y}_{u,i}, Y_{u,i})$ is the cross-entropy loss of the observed feedback. $Y_{u,i}$ and $\hat{Y}_{u,i}$ are the true and predicted label of user $u$ for item $i$, respectively.

- **AT [30]**: For the selection bias in recommender systems, an upper bound of the generalization error is derived and solved by an asymmetric tri-training method. Two pre-models are used to generate a pseudo-label set, and the target model and the two pre-models are then retrained on this set. This process is repeated until the debiasing performance of the target model is improved the most.

- **Rel [31]**: Based on the idea of positive unlabeled learning, an unbiased estimation is derived for binary feedback modeling in recommender systems. The inverse propensity score is estimated and weighted differently for positive feedback and negative feedback. The objective function can be represented as follows,
Table 2: Hyper-parameters and their values tuned in the experiments.

<table>
<thead>
<tr>
<th>Name</th>
<th>Range</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>rank</td>
<td>{5, 10, \ldots, 195, 200}</td>
<td>Embedded dimension</td>
</tr>
<tr>
<td>\beta</td>
<td>{1e^{-5}, 1e^{-4}, \ldots, 1e^{-1}}</td>
<td>Regularization</td>
</tr>
<tr>
<td>bs</td>
<td>{2^7, 2^{13}, \ldots, 2^13, 2^{14}}</td>
<td>Batch size</td>
</tr>
<tr>
<td>lr</td>
<td>{1e^{-4}, 5e^{-4}, \ldots, 5e^{-2}, 1e^{-1}}</td>
<td>Learning rate</td>
</tr>
<tr>
<td>\gamma</td>
<td>[0.1, 0.2]</td>
<td>Loss weighting</td>
</tr>
<tr>
<td>\alpha</td>
<td>[0.001, 0.1]</td>
<td>Loss weighting</td>
</tr>
</tbody>
</table>

where \( \delta^{(1)}_{u,i} \) and \( \delta^{(0)}_{u,i} \) denote the positive loss and the negative loss, respectively, and \( P_{u,i} \) is calculated by Eq.(15).

- **CVIB [40]:** It is an alternative framework for debiasing learning without an unbiased feedback data, which is called the information-theoretic counterfactual variational information bottleneck. By separating the task-aware mutual information term in standard information bottleneck into a factual part and a counterfactual part, it derives a contrastive information regularizer and an additional output confidence penalty to improve the learning balance between the observed and unobserved data.

### 6.1.4 Implementation Details

We implement all the methods on TensorFlow with the Adam optimizer\(^1\). By evaluating the performance on AUC on the validation set, we use the hyper-parameter search library **Optuna** [4] to accelerate the tuning process of all the methods. The range of the values of the hyper-parameters are shown in Table 2. Note that the source codes, parameter search records and results are available at https://github.com/dgliu/RecSys21_DIB.

### 6.2 RQ1: Comparison Results of Unbiased Evaluation

The comparison results are reported in Table 3 and Table 4. For the results of using matrix factorization as the backbone model shown in Table 3, the proposed method consistently outperforms all the baselines on all the metrics across the two datasets of Yahoo! R3 and Product. In addition, we have the following main observations: 1) The debiasing method is usually better than the basic baseline, i.e., matrix factorization, except for IPS-MF on Yahoo! R3. This may be due to the inaccurate estimation of the propensity score when the data size is small. 2) By avoiding the estimation of the propensity score and providing theoretical completeness, theoretical tools-based methods (i.e., CVIB, AT, and Rel) usually achieve better and more stable performance. 3) For the baseline CVIB-MF whose objective function is also induced by information theory, its improvement over MF on Yahoo! R3 is small, while the proposed method is better and more robust on both datasets.

For the results of using neural collaborative filtering as the backbone shown in Table 4, the proposed method outperforms all the baselines in most cases. Specifically, we have the following observations: 1) when K takes a relatively small value on Product, the proposed method is slightly worse than IPS-NCF. However, when K takes a larger value, the proposed method has obvious performance advantages. This means that the proposed method still has better overall performance. 2) Even with the use of the techniques to reduce variance, the incorrect estimation of the propensity score in a small dataset will be further exacerbated. 3) AT and Rel may not be well adapted to neural network-based models due to their dependence on certain types of loss functions.

### 6.3 RQ2: Ablation Studies

To understand the respective effects of the last three terms in Eq.(14) on model training, we conduct ablation studies on Yahoo! R3 and Product. The results are shown in Table 5. In the first half of Table 5, we show the results using matrix factorization as the backbone. For the results on Yahoo! R3, we can see that removing any term will hurt the performance in most cases, and removing term (d) leads to the worst performance. This may be due to the small size of Yahoo! R3, which causes the term (d) to play a more important role in avoiding overfitting of the model to the training set. Conversely, we can find that the effect of removing the term (d) on the larger Product dataset is small.

We show the results using neural collaborative filtering as the backbone model in the second half of Table 5. We note that removing the term (d) will bring the greatest performance degradation on different data scales. One possible reason is that the neural network-based model introduces more parameters, and these parameters need to be well learned under the constraints of regularization terms. There are some unexpected cases in Table 5, i.e., when K takes a small value, the full version of the proposed method has a slight disadvantage on a few metrics. This may be due to the noise caused by only considering AUC in parameter tuning. In general, all terms in the proposed method can synergistically produce the greatest gain.

### 6.4 RQ3: Model Analysis

In this section, we conduct some more in-depth analysis of the proposed method in order to have a better understanding of the properties of the proposed method.

#### 6.4.1 Visualization of the biased component r and the unbiased component z

A key question is whether the biased component r and the unbiased component z in the proposed method have a pattern that meets the expectation, i.e., they gradually become independent in training. To answer this question, at several training time points, we use the t-SNE [36] method to visualize the biased and unbiased components. The results are shown in Figure 3. We can see that as the training progresses, there is a clear separation between the biased component in blue and the unbiased component in red. This verifies the effectiveness of the proposed method. We also note that the unbiased component is looser than the biased component, and a small part of the unbiased component is still mixed with the biased component. This may be because the unbiased component needs to learn the personalized differences between the users, among whom there are still some users who are difficult to be distinguished.

#### 6.4.2 Visualization of the loss of each term in \( L_{DIB} \)

We next analyze the trend of the loss of each term in \( L_{DIB} \). The results are
Table 3: Comparison results of unbiased evaluation using MF as the backbone model, where the best results and the second best results are marked in bold and underlined, respectively. AUC is the main evaluation metric.

<table>
<thead>
<tr>
<th>Method</th>
<th>Yahoo! R3</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AUC</td>
<td>nDCG</td>
</tr>
<tr>
<td>MF</td>
<td>0.7081</td>
<td>0.0341</td>
</tr>
<tr>
<td>IPS-MF</td>
<td>0.7040</td>
<td>0.0259</td>
</tr>
<tr>
<td>SNIPS-MF</td>
<td>0.7124</td>
<td>0.0390</td>
</tr>
<tr>
<td>CVIB-MF</td>
<td>0.7086</td>
<td>0.0488</td>
</tr>
<tr>
<td>AT-MF</td>
<td>0.7290</td>
<td>0.0676</td>
</tr>
<tr>
<td>Rel-MF</td>
<td>0.7469</td>
<td>0.0843</td>
</tr>
</tbody>
</table>

Table 4: Comparison results of unbiased evaluation using NCF as the backbone model, where the best results and the second best results are marked in bold and underlined, respectively. AUC is the main evaluation metric.

<table>
<thead>
<tr>
<th>Method</th>
<th>Yahoo! R3</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AUC</td>
<td>nDCG</td>
</tr>
<tr>
<td>NCF</td>
<td>0.7251</td>
<td>0.0350</td>
</tr>
<tr>
<td>IPS-NCF</td>
<td>0.7221</td>
<td>0.0322</td>
</tr>
<tr>
<td>SNIPS-NCF</td>
<td>0.7230</td>
<td>0.0310</td>
</tr>
<tr>
<td>CVIB-NCF</td>
<td>0.7265</td>
<td>0.0347</td>
</tr>
<tr>
<td>AT-NCF</td>
<td>0.7139</td>
<td>0.0333</td>
</tr>
<tr>
<td>Rel-NCF</td>
<td>0.6867</td>
<td>0.0507</td>
</tr>
<tr>
<td>DIB-NCF</td>
<td>0.7553</td>
<td>0.0686</td>
</tr>
</tbody>
</table>

Table 5: Results of the ablation studies using MF and NCF as the backbone models, where the best results and the second best results are marked in bold and underlined, respectively. AUC is the main evaluation metric.

<table>
<thead>
<tr>
<th>Method</th>
<th>Yahoo! R3</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AUC</td>
<td>nDCG</td>
</tr>
<tr>
<td>DIB-MF</td>
<td>0.7602</td>
<td>0.0932</td>
</tr>
<tr>
<td>w/o term (b)</td>
<td>0.7505</td>
<td>0.0893</td>
</tr>
<tr>
<td>w/o term (c)</td>
<td>0.7545</td>
<td>0.0915</td>
</tr>
<tr>
<td>w/o term (d)</td>
<td>0.7342</td>
<td>0.0769</td>
</tr>
<tr>
<td>DIB-NCF</td>
<td>0.7553</td>
<td>0.0686</td>
</tr>
<tr>
<td>w/o term (b)</td>
<td>0.7326</td>
<td>0.0553</td>
</tr>
<tr>
<td>w/o term (c)</td>
<td>0.7373</td>
<td>0.0592</td>
</tr>
<tr>
<td>w/o term (d)</td>
<td>0.7243</td>
<td>0.0597</td>
</tr>
</tbody>
</table>

shown in Figure 4. A sufficient reduction in the loss of term (a) guarantees the basic performance of the proposed method (corresponding to the unbiased component $z$). By comparing the trends of term (b) and term (c), we can see that using the biased component $r$ alone will lead to a very poor result, but as long as it is combined with the unbiased component $z$, the best result can be achieved. This is reasonable, because the biased component itself does not reflect the user’s preferences well, but the combination with the unbiased component will lead to an over-approximation effect on the observed feedback. In addition, the trend of term (d)
Mitigating Confounding Bias in Recommendation via Information Bottleneck

Figure 3: Dynamic visualization of the unbiased component $z$ and the biased component $r$ as training progresses, in which the blue and red points are used to denote the biased component and the debiased component, respectively.

Figure 4: The trend of the loss of each term in $L_{	ext{DIB}}$ as training progresses.

7 CONCLUSIONS AND FUTURE WORK

In this paper, we describe the generation process of the biased and unbiased feedback in recommender systems via two respective causal diagrams, and then define a new bias based on the difference between them, which is called confounding bias. When only the biased feedback is available, we analyze the conditions that need to be met to alleviate the confounding bias, and propose a debiased information bottleneck (DIB) method to perform this optimization process based on the guidance of information theory. Moreover, we also derive a tractable solution for the proposed method. We verify the effectiveness of the proposed method on a public dataset and also derive a tractable solution for the proposed method. We verify the effectiveness of the proposed method on a public dataset and also derive a tractable solution for the proposed method.

For future works, we plan to extend the proposed method to scenarios where more than one biased data is available. We are also interested in further relaxing the independent assumptions of the unbiased and biased components, that is, there may be a special mixed component entangled with the biased or unbiased component in some tasks.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their expert and constructive comments and suggestions, and the support of National Natural Science Foundation of China Nos. 61836005 and 61872249.

REFERENCES


Haixin Yang, Guang Ling, Yuxin Su, Michael R Lyu, and Irwin King. 2015. Boosting response-aware score model-based collaborative filtering. IEEE Transactions on Knowledge and Data Engineering 27, 8 (2015), 2064–2077.

