

Learning Fair Representation via Distributional Contrastive Disentanglement

Changdae Oh

University of Seoul
Seoul, Republic of Korea
bnormal16@uos.ac.kr

Taero Kim

University of Seoul
Seoul, Republic of Korea
rlaxofh123@uos.ac.kr

Heeji Won

Korea University
Seoul, Republic of Korea
gmlwl1026@korea.ac.kr

Yewon Kim

University of Seoul
Seoul, Republic of Korea
yeyewon12@uos.ac.kr

Junhyuk So

POSTECH
Pohang, Republic of Korea
junhyukso@postech.ac.kr

Hosik Choi

University of Seoul
Seoul, Republic of Korea
choi.hosik@uos.ac.kr

Kyungwoo Song*

University of Seoul
Seoul, Republic of Korea
kyungwoo.song@uos.ac.kr

ABSTRACT

Learning fair representation is crucial for achieving fairness or debiasing sensitive information. Most existing works rely on adversarial representation learning to inject some invariance into representation. However, adversarial learning methods are known to suffer from relatively unstable training, and this might harm the balance between fairness and predictiveness of representation. We propose a new approach, learning *FAir Representation via distributional CONtrastive Variational AutoEncoder* (*FarconVAE*), which induces the latent space to be disentangled into sensitive and non-sensitive parts. We first construct the pair of observations with different sensitive attributes but with the same labels. Then, FarconVAE enforces each non-sensitive latent to be closer, while sensitive latents to be far from each other and also far from the non-sensitive latent by contrasting their distributions. We provide a new type of contrastive loss motivated by Gaussian and Student-t kernels for distributional contrastive learning with theoretical analysis. Besides, we adopt a new swap-reconstruction loss to boost the disentanglement further. FarconVAE shows superior performance on fairness, pretrained model debiasing, and domain generalization tasks from various modalities, including tabular, image, and text.

CCS CONCEPTS

- Computing methodologies → Neural networks; Learning latent representations;
- Social and professional topics → User characteristics.

*Corresponding author.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

KDD '22, August 14–18, 2022, Washington, DC, USA.

© 2022 Association for Computing Machinery.

ACM ISBN 978-1-4503-9385-0/22/08...\$15.00

<https://doi.org/10.1145/3534678.3539232>

KEYWORDS

Fairness; Disentanglement; Invariant Learning; Contrastive Learning; Variational Autoencoder

ACM Reference Format:

Changdae Oh, Heeji Won, Junhyuk So, Taero Kim, Yewon Kim, Hosik Choi, and Kyungwoo Song. 2022. Learning Fair Representation via Distributional Contrastive Disentanglement. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '22)*, August 14–18, 2022, Washington, DC, USA. ACM, New York, NY, USA, 11 pages. <https://doi.org/10.1145/3534678.3539232>

1 INTRODUCTION

Machine learning algorithms show the great success on many tasks, and they have been widely adopted in real-world applications. Most works of machine learning utilize a simple predictor at the test time, and the extracted features of a given dataset greatly influence the model prediction. So, the success of machine learning algorithms largely depends on the data representation that the model learned [4]. However, the input features of a given dataset might contain noise and unnecessary information for the given task, and learning a representation that covers the important characteristics of the given dataset while invariant to unwanted information is crucial.

Neural networks are known to have an advantage in representation learning. The learned representation from the neural net represents the characteristics of data with fewer dimensional vectors. Neural network based methods show a significant performance improvement on many domains including image [15], text [18], and tabular [39]. However, recent studies raise that the traditional neural networks have difficulty in achieving fairness and domain generalization [2, 32]. Neural networks provide a rich representation, but the representation also absorbs the sensitive (private) information or spurious correlation of a given dataset. Due to this unwanted information in learned representations, the model can induce unfair results in decision making system or fail to provide the correct predictions in the distribution shift scenario.

There are many directions to remove the sensitive information and spurious correlation in the model. One of them, adversarial representation learning (ARL) methods [30, 38] set two goals, (i) maximally retain salient information about a given target attribute, and (ii) minimize the information leakage about a given sensitive attribute. While these methods have shown compelling results when optimized successfully, their convergence instability hinders achieving the above goals and limits the wide use of ARL methods practically. Another promising direction is a disentangled representation learning [8, 32] that separates the non-sensitive representation and sensitive representation. Their empirical success proves the effectiveness of disentanglement-based approaches to fair expression learning. However, most of the existing methods for disentangling [8, 20] also rely on the adversarial learning technique to approximate Total Correlation [36] using the density ratio trick.

The other direction is to learn the invariant representation of a given dataset. Invariant representation denotes the shared important features invariant across domains or environments. Recently, Arovsky et al. [2] proposed Invariant Risk Minimization (IRM) that encourages invariant representation learning with bi-level optimization. The representation trained with IRM may have shared important features, but there is no guarantee that the representation does not hold any sensitive information. Besides, Group-DRO [31] is known to be effective for learning robust representation, but it is also not guaranteed about the existence of sensitive information. Although invariant learning methods [2, 7, 31] show meaningful performance improvements on domain generalization tasks, we observe that the representation learned from IRM and Group-DRO still has a spurious correlation or sensitive information largely that poses a potential risk in real-world applications.

In this paper, we propose FarconVAE (FAir Representation via distributional CONtrastive Variational AutoEncoder), a new disentangling approach with contrastive learning instead of adversarial learning. First, we construct a pair of two instances with different sensitive information and the same non-sensitive information. Then, FarconVAE 1) minimizes the distance between non-sensitive representations, 2) maximizes the dissimilarity between sensitive representations, and 3) maximizes the dissimilarity between sensitive and non-sensitive representations of each paired instance with our distributional contrastive loss. Finally, in the latent space divided into sensitive and non-sensitive representation, FarconVAE makes a fair prediction by using only non-sensitive representation.

Besides, we adopt a new feature swap based objective for FarconVAE, swap-recon, to improve the disentanglement. Swap-recon replaces the non-sensitive representation of a given data instance with that of another paired data instance while leaving the sensitive representation untouched. By reconstructing from both the swapped latent and the original latent to the same original data instance, swap-recon further boosts the disentanglement. In Appendix C, we empirically validate that swap-recon improves the representation disentanglement quality.

To the best of our knowledge, this is the first study to improve both fairness and out-of-distribution generalization performance.

FarconVAE provides a fair representation that only includes non-sensitive core information by disentangling the sensitive information. Besides, it also removes the spurious correlation in representation learned from IRM and Group-DRO, while maintaining the model accuracy.

Our contributions in this work are three-fold:

- We propose a novel framework FarconVAE that learns disentangled invariant representation with contrastive loss to achieve algorithmic fairness and domain generalization.
- We provide a new distributional contrastive loss for disentanglement motivated by the Gaussian and Student-t kernels.
- The proposed method is theoretically analyzed and empirically demonstrated on a broad range of data types (tabular, image, and text) and tasks, including fairness and domain generalization.

2 RELATED WORKS

2.1 Domain Generalization

The primary objective of domain generalization is to show stable predictive performance even though the test distributions are different from the train distribution [13]. Traditional machine learning algorithm fails domain generalization, and there have been many research works to handle the distribution shift in diverse ways, including Bayesian neural net [27], data augmentation [40], robust optimization [23, 31], and invariant learning [2, 7].

Recently, Group-Distributionally Robust Optimization (Group-DRO) [31] and Invariant Risk Minimization (IRM) [2] have been considered promising ways for domain generalization. Group-DRO optimizes the models to focus on the worst-case group with strong regularization, and IRM encourages the model to focus on the shared essential features across the group. However, there is no theoretical guarantee that the Group-DRO and IRM alleviate the spurious correlation or sensitive information removal. Recent works point out that the performance improvements of Group-DRO and IRM are limited on a shifted test distribution [13].

2.2 Learning Fair Representation

Fair representation learning aims to learn a representation that can be used for making accurate predictions without bias from sensitive information. We can divide the various fairness works depending on whether adversarial learning is used, and we introduce the related works for fair representation learning in this subsection.

2.2.1 Fair Representation with Adversarial Learning. Generative adversarial learning (GAN) [11] shows a significant improvement in density estimation, and it has been widely utilized in many tasks. For fair representation learning, density estimation of a given instance without sensitive information is necessary. Therefore, there have been many research works that adopt adversarial learning for fair representation [28, 30, 38, 42]. Controllable Invariance (CI) [38] adopts adversarial min-max game to filter out detrimental features such as sensitive information. CI introduces three types of network; encoder, discriminator, predictor, and adversarial minimax game between encoder and discriminator encourages the representation is invariant to sensitive information. Maximum Entropy Adversarial Representation Learning (MaxEnt-ARL) [30] is another kind

of adversarial method, and MaxEnt-ARL utilizes a non-zero-sum game adversarial formulation by adopting different objectives for generator and discriminator to overcome the sub-optimal problems. The order approach is Flexibly Fair Variational AutoEncoder (FFVAE) [8] based on disentangled representation learning. FFVAE learns the separated latent space for sensitive and non-sensitive information. Although the algorithm does not contain an explicit adversary, it also relies on adversarial learning to approximate the Total Correlation (TC) [36] penalty used for disentanglement.

However, adversarial learning is known to have convergence instability problems, and it might hinder learning the robust representation. We empirically observe that the previous adversarial learning-based fair algorithm has difficulty separating the sensitive information. To solve the problems, we propose a contrastive learning-based disentangled representation learning method, FarconVAE, instead of adversarial learning.

2.2.2 Fair Representation without Adversarial Learning. Recently, there have been other fair representation learning research works without adversarial learning [6, 26, 32, 41]. Zemel et al. [41] propose fair clustering methods with probabilistic mapping, and Variational Fair AutoEncoder (VFAE) [26] adopts Maximum Mean Discrepancy (MMD) measure [12] to penalize the posterior. Besides, Fair Filter (FairFil) [6] removes the sensitive information that is inherent in the sentence embedding from a pretrained language model. To learn debiased embeddings, FairFil utilizes contrastive learning and mutual information estimator.

Orthogonal Disentangled Fair Representations (ODFR) [32] is a non-adversarial disentangle-based methods, and it introduces orthogonal priors to enforce an orthogonality constraint between sensitive and non-sensitive representation. $q_{\phi_s}(z_s|x)$ and $q_{\phi_x}(z_x|x)$ denote the posteriors of sensitive and non-sensitive representation parameterized by ϕ_s and ϕ_x respectively, and $p(z_x)$ and $p(z_s)$ denote the priors, where $p(z_x) = \mathcal{N}([1, 0]^T, I)$ and $p(z_s) = \mathcal{N}([0, 1]^T, I)$.

$$LOD = KL((q_{\phi_x}(z_x|x)||p(z_x)) + KL((q_{\phi_s}(z_s|x)||p(z_s))) \quad (1)$$

However, minimizing LOD in Eq. 1 does not guarantee a robust fair representation. It is known that the vanilla KL-divergence between posterior and fixed prior might cause the posterior collapse, and the representation might not contain meaningful information of given data [14]. As a result, ODFR adopts additional auxiliary components such as entropy loss. Besides, there are diverse ways to set orthogonal priors, and the performance of ODFR may largely depend on the choice of prior.

FarconVAE has a relationship with FairFil and ODFR, but there are three major differences. First, FarconVAE measures the divergence between two posteriors for disentanglement instead of the fixed prior in ODFR. Thus, FarconVAE is relatively free from posterior collapse problems and prior choice. Second, we adopt a new distributional contrastive loss motivated by Gaussian and Student-t kernel. It makes FarconVAE get highly disentangled fair representation without the need for auxiliary components such as discriminators and entropy loss. Third, in contrast to ODFR and FairFil, which have shown effectiveness in limited data types for only fair prediction tasks, our FarconVAE has validated on both fairness and domain generalization tasks across three representative data types.

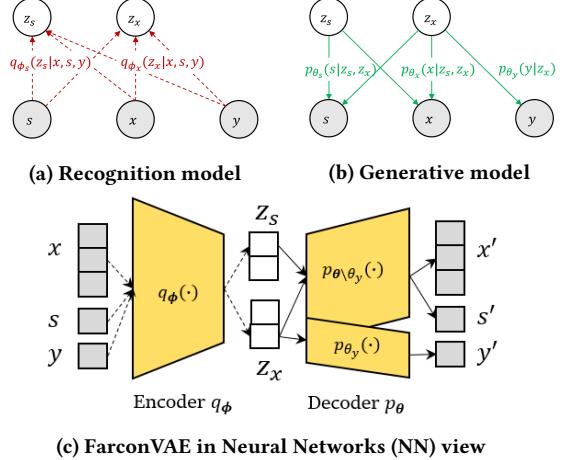


Figure 1: Graphical notations of FarconVAE (a), (b), and neural network view (c). The dashed line denotes the recognition models, neural network with parameter ϕ , and the solid line represents the generative models, neural network with parameter θ . Also, the gray color denotes the observed variables, while the white color denotes the latent variables.

2.3 Contrastive Learning

Recently, Contrastive learning has emerged as a new promising paradigm for self-supervised representation learning, showing powerful performance in a broad domain such as Vision [5], NLP [9], and Graph [24]. InfoNCE [34] is a widely used loss function for contrastive learning that effectively formulates the instance discrimination task. InfoNCE loss encourages the similarity between positive pairs and the dissimilarity between negative pairs. Representation space learned by contrastive learning has performed well in various downstream tasks such as classification, clustering, or semantic similarity evaluation. However, there is limited work [37] that handled the disentanglement with contrastive learning. This paper provides a new distributional contrastive learning method to obtain disentangled invariant representation and apply it to fairness and domain generalization tasks.

3 METHODOLOGY

In this section, we firstly introduce the basic notation and problem formulation in Section 3.1. In Sections 3.2, 3.3, we describe FarconVAE in detail, and cover the kernel motivated distributional contrastive loss that induces stable disentanglement, respectively. In Section 3.4, we provide a description for swap-recon, a new feature swap based regularization. Finally, we theoretically analyze our two specified contrastive losses in Section 3.5.

3.1 Problem Definition

Let x be an observed input feature, s be its sensitive attribute, and y be a target label. As described in [2, 32], the sensitive attribute s is highly correlated with feature x and spuriously correlated with label y on many real-world datasets, even if it is essentially irrelevant.

In this situation, We want to build a fair ML algorithm. Mathematically, fairness can be defined as $p_\theta(y|x) = p_\theta(y|x, s)$ [32]. The Fairness definition shows that the model output needs to be independent of the sensitive attribute. As a result, a fair representation debiased w.r.t sensitive information is necessary to achieve fairness. Furthermore, performance degradation for target label prediction should be minimized. However, the existing methods for building fair algorithms have difficulty in learning robust representation satisfying both predictiveness and fairness, as stated in Section 2.

In this work, we propose FarconVAE, which aims to learn a function that maps each data (x, s, y) to disentangled representation z_s and z_x on the two separated latent spaces $\mathcal{Z}_s, \mathcal{Z}_x$ that involve different semantic meanings. Specifically, \mathcal{Z}_s is a latent space to absorb and isolate the whole sensitive information from observation, and \mathcal{Z}_x maximally preserves only non-sensitive information to predict the target accurately. In other words, z_x is a fair representation used for target prediction that has high predictiveness without relying on sensitive information.

3.2 FarconVAE Structure

Figure 1 represents the FarconVAE in terms of graphical model and neural net view. FarconVAE assumes that there are three observable variables, input feature x , sensitive attribute s , and target label y . FarconVAE has one encoder $p_\phi(\cdot)$ that splits into two heads for encoding z_x and z_s , and two decoders: $p_{\theta_y}(\cdot)$ for decoding y and $p_{\theta \setminus \theta_y}(\cdot)$ that splits into two heads for decoding x and s . The goal of FarconVAE is to capture two disentangled latent z_s and z_x , where z_s and z_x denote the sensitive and non-sensitive representation, respectively. With these two latent variables, The log marginal likelihood of the x, s and y with model parameters θ is as follows:

$$\log p_\theta(x, s, y) = \log \int \int p_\theta(x, s, y, z_x, z_s) dz_x dz_s \quad (2)$$

3.2.1 Model Inference. Direct optimization of marginal likelihood, Eq. 2, is intractable, so we utilize the variational inference [17] to approximate the marginal likelihood. We introduce the variational distribution q , and we adopt encoder q_ϕ and decoder p_θ as neural networks parameterized by $\phi = \{\phi_{body}, \phi_{head_x}, \phi_{head_s}\}$ and $\theta = \{\theta_{body}, \theta_{head_x}, \theta_{head_s}, \theta_y\}$, respectively. In the following all sections, we will notate $\{\phi_{body} \cup \phi_{head_x}\}$ as ϕ_x and $\{\phi_{body} \cup \phi_{head_s}\}$ as ϕ_s , $\{\theta_{body} \cup \theta_{head_x}\}$ as θ_x , and $\{\theta_{body} \cup \theta_{head_s}\}$ as θ_s .

For the disentanglement between z_x and z_s , the conditional independence between z_x and z_s given x, s, y is necessary. Under the conditional independence assumption, we construct the variational objective [17, 22], called evidence lower bound (ELBO), as follows:

$$\begin{aligned} & \log p_\theta(x, s, y) \\ & \geq \mathbb{E}_{q_\phi} [\log p_{\theta_x}(x|z_x, z_s) + \log p_{\theta_s}(s|z_x, z_s) + \log p_{\theta_y}(y|z_x)] \\ & - \text{KL}(q_{\phi_x}(z_x|x, s, y) || p(z_x)) - \text{KL}(q_{\phi_s}(z_s|x, s, y) || p(z_s)) \quad (3) \\ & = \mathcal{L}_{ELBO}(\phi, \theta; x, s, y) \quad (4) \end{aligned}$$

\mathcal{L}_{ELBO} in Eq. 4 consists of three components. First, the KL divergence in Eq. 3 can be interpreted as a regularization term to prevent the variational posteriors $q_{\phi_x}(z_x|x, s, y)$ and $q_{\phi_s}(z_s|x, s, y)$ moving too far from their priors. Second, reconstruction terms, $p_{\theta_x}(x|z_x, z_s)$ and $p_{\theta_s}(s|z_x, z_s)$ encourage the latent representation

z_x and z_s to preserve the salient information of x and s . Third, prediction term $p_{\theta_y}(y|z_x)$ gives an ability to model to predict the target value, and it injects task-specific information to representation z_x .

By maximizing the ELBO in Eq. 4, we can infer the parameters of distribution over the joint latent variables z_s and z_x that depend on x, s , and y . These two latent representations include the salient information of the given dataset. Different with z_s, z_x has capability to predict y , and its difference contributes to disentanglement between z_s and z_x . However, FarconVAE can be improved in two ways. First, \mathcal{L}_{ELBO} just assumes the conditional independence between z_x and z_s given x, s, y . Second, z_x still has sensitive information if the y is spuriously correlated with s . Therefore, we provide a new contrastive loss with FarconVAE and introduce it in Section 3.3.

3.2.2 Model in Detail. In this subsection, we provide the distributional assumption in FarconVAE. For the prior $p(z_s)$ and $p(z_x)$, we adopt standard Gaussian $\mathcal{N}(z_s; 0, I)$ and $\mathcal{N}(z_x; 0, I)$, respectively.

For encoder, we formulate the variational posterior distribution $q_\phi(\cdot|\cdot)$ as Gaussian distribution with diagonal covariance structure, parameterized by neural network. In the remaining sections, we will omit the parameter of posterior and refer to it as $q(\cdot|\cdot)$. In the formulas below, z . can be z_x or z_s .

$$\log q_\phi(z|\cdot, s, y) = \log \mathcal{N}(z; \mu_z, \sigma_z^2 I)$$

For decoder, we adopt Gaussian distribution for continuous variables and Bernoulli distribution for discrete variables. Like above, the parameters of the distribution are parameterized by θ .

$$\begin{aligned} p_{\theta_x}(x|z_x, z_s) &= \mathcal{N}(x; \mu_x, \sigma_x^2 I) \text{ or } p_{\theta_x}(x|z_x, z_s) = \text{Ber}(x; \mu_x) \\ p_{\theta_s}(s|z_x, z_s) &= \mathcal{N}(s; \mu_s, \sigma_s^2 I) \text{ or } p_{\theta_s}(s|z_x, z_s) = \text{Ber}(s; \mu_s) \\ p_{\theta_y}(y|z_x) &= \mathcal{N}(y; \mu_y, \sigma_y^2 I) \text{ or } p_{\theta_y}(y|z_x) = \text{Ber}(y; \mu_y) \end{aligned}$$

To reconstruct feature x and sensitive attribute s , FarconVAE uses both z_x and z_s , while for predicting target label y it utilizes z_x only.

3.3 Contrastive Learning for Disentanglement

For given x, s, y , we can estimate the counterfactual that has the same label y , but different sensitive attribute \tilde{s} and its corresponding \tilde{x} (similar to x). Counterfactual estimation can be replacing the given sensitive s , as opposite s' [21], or finding the similar instance that has different sensitive attribute [33]. Given original data instance and its counterfactual, we train the model with a pair of them with \mathcal{L}_{ELBO} in Eq. 4. Besides, we introduce the contrastive loss to ensure the disentanglement between z_x and z_s . For the latent representation of given dataset and its counterfactual, $z_x, z_s, z_{\tilde{x}}, z_{\tilde{s}}$, the similarity between z_x and $z_{\tilde{x}}$, the difference between z_s and $z_{\tilde{s}}$, and the difference between z_x (or $z_{\tilde{x}}$) and z_s (or $z_{\tilde{s}}$) are required.

In this perspective, we regard $(z_x, z_{\tilde{x}})$ as a positive pair and $(z_s, z_{\tilde{s}})$, (z_x, z_s) , $(z_{\tilde{x}}, z_{\tilde{s}})$ as negative pairs by analogy with problem setting in contrastive learning literature. To encourage the similarity between positive representation pair and the difference between negative representation pair, we minimize the divergence between posterior $(q(z_x|\cdot), q(z_{\tilde{x}}|\cdot))$ and minimize the similarity between posterior $(q(z_s|\cdot), q(z_{\tilde{s}}|\cdot))$, $(q(z_x|\cdot), q(z_s|\cdot))$, and $(q(z_{\tilde{x}}|\cdot), q(z_{\tilde{s}}|\cdot))$ simultaneously using Distributional Contrastive loss:

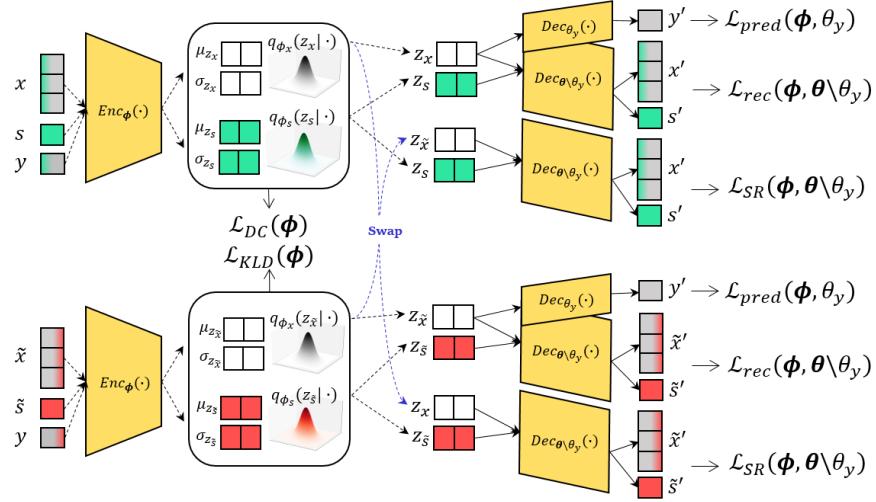


Figure 2: Overall framework. Green and Red colors denote the sensitive information, while white denotes non-sensitive residual information. When the original data (x, s, y) is given, we find or generate the data $(\tilde{x}, \tilde{s}, y)$ that has a different sensitive attribute while having the same target label for constructing pair. After that, we extract latent representation $z_x, z_s, z_{\tilde{x}}, z_{\tilde{s}}$. For given representations, we enforce 1) similarity between z_x and $z_{\tilde{x}}$, 2) dissimilarity between z_s and $z_{\tilde{s}}$ 3) dissimilarity between z_x (or $z_{\tilde{x}}$) and z_s (or $z_{\tilde{s}}$) using distribution contrastive loss for disentangling. Moreover, we adopt swap-recon (SR) that further enhances the disentanglement by performing consistent reconstruction with both swapped and original latent. As a result, FarconVAE provides the disentangled fair representation z_x . In training, we put y as input to FarconVAE for better predictive-ness, but it requires the true label in test time. We solve this by using the best classifier that predicts y from x . See Appendix B for details.

$$\mathcal{L}_{DC} = \mathcal{D}_z(q(z_x|\cdot), q(z_{\tilde{x}}|\cdot)) + \sum_{neg \in NPP} k(\mathcal{D}_z(neg)) \quad (5)$$

where \mathcal{D}_z is an arbitrary divergence between two distributions, $k(\cdot)$ is any positive definite kernel function (e.g. Gaussian RBF), and $NPP = \{(q(z_s|\cdot), q(z_{\tilde{s}}|\cdot)), (q(z_x|\cdot), q(z_{\tilde{x}}|\cdot)), (q(z_{\tilde{x}}|\cdot), q(z_{\tilde{s}}|\cdot))\}$ is a set of negative posterior pairs. Thus, $\mathcal{D}_z(neg)$ denotes a divergence between two negatively paired distributions. For convenience in implementation, we choose \mathcal{D}_z as the averaged KL divergence that simply averages two possible KL divergences between probability distributions, i.e., $\bar{KL}(p_0, p_1) = \frac{(KL(p_0||p_1) + KL(p_1||p_0))}{2}$. Note that, the divergence is both the statistical distance and the generalized squared distance between two distributions. Consequently, after being passed through the kernel function $k(\cdot)$, the distance between two distributions is converted into the similarity between two distributions.

By adopting Gaussian or Student-t kernel for kernel function $k(\cdot)$, we specify our two *Distributional Contrastive* losses as below:

$$\mathcal{L}_{DC-t} = \bar{KL}(q(z_x|\cdot)||q(z_{\tilde{x}}|\cdot)) + \sum_{neg \in NPP} (1 + \bar{KL}(neg))^{-1} \quad (6)$$

$$\mathcal{L}_{DC-G} = \bar{KL}(q(z_x|\cdot)||q(z_{\tilde{x}}|\cdot)) + \sum_{neg \in NPP} \exp(-\bar{KL}(neg)) \quad (7)$$

In Section 3.5, we present a theoretical analysis for these losses.

3.4 Swap-Reconstruction

Besides distributional contrasting, we perform the swap-reconstruction task (referred to *swap-recon*) that improves disentanglement further. After passing the encoder, the observation pair $\{(x, s, y), (\tilde{x}, \tilde{s}, y)\}$ is encoded as $\{(z_x, z_s), (z_{\tilde{x}}, z_{\tilde{s}})\}$. As mentioned above subsection, we hope that only z_s and $z_{\tilde{s}}$ contain sensitive information and z_x and $z_{\tilde{x}}$ have non-sensitive residual information. For taking a step closer to this goal, we swap the non-sensitive representations z_x and $z_{\tilde{x}}$ each other and form new concatenated latent vector pairs $(z_{\tilde{x}}, z_s)$ and $(z_x, z_{\tilde{s}})$. To reconstruct the original observation (x, s, y) and $(\tilde{x}, \tilde{s}, y)$ from the swapped latent $(z_{\tilde{x}}, z_s)$ and $(z_x, z_{\tilde{s}})$, FarconVAE is incentivized to encode only non-sensitive information in z_x and $z_{\tilde{x}}$. In the early training stage, the swap-recon generates diverse combinations of non-sensitive and sensitive information, and we observe that it improves not only disentanglement, but also generalization performance. The loss term is defined as:

$$\mathcal{L}_{SR} = \frac{1}{2} ((\log p_{\theta_x}(x|z_{\tilde{x}}, z_s) + \log p_{\theta_s}(s|z_{\tilde{x}}, z_s)) + (\log p_{\theta_x}(\tilde{x}|z_x, z_{\tilde{s}}) + \log p_{\theta_s}(\tilde{s}|z_x, z_{\tilde{s}}))) \quad (8)$$

There were similar methods to our swap-recon, and they showed promising results in disentangling [29] or debiasing [19]. However, this is the first study that proposes swap-recon under the contrastive learning framework. We utilize \mathcal{L}_{SR} , swap-recon loss, with our main distributional contrastive loss \mathcal{L}_{DC} .

3.4.1 Overall Objective. FarconVAE is a general framework for disentangled fair representation learning. To encourage disentanglement, we use a distributional contrastive loss and swap-recon loss as shown in Figure 2. The overall objective becomes as follows:

$$\begin{aligned} \mathcal{L}_{\text{Farcon}}(\phi, \theta; x, \tilde{x}, s, \tilde{s}, y) \\ = \frac{1}{2} (\mathcal{L}_{\text{ELBO}}(\phi, \theta; x, s, y) + \mathcal{L}_{\text{ELBO}}(\phi, \theta; \tilde{x}, \tilde{s}, y)) \\ + \alpha \mathcal{L}_{\text{DC}}(\phi, \theta; x, \tilde{x}, s, \tilde{s}, y) + \gamma \mathcal{L}_{\text{SR}}(\phi, \theta; \theta_y; x, \tilde{x}, s, \tilde{s}, y) \end{aligned}$$

where α and γ are hyperparameters to weigh the distributional contrastive loss and the swap-recon loss, respectively. $\mathcal{L}_{\text{ELBO}}$ term is optimized over the given original data instance (x, s, y) , and its counterfactual instance $(\tilde{x}, \tilde{s}, y)$ individually. On the other hand, \mathcal{L}_{DC} and \mathcal{L}_{SR} terms are optimized over both original and counterfactual instances simultaneously. We demonstrate the effectiveness of proposed loss terms \mathcal{L}_{DC} and \mathcal{L}_{SR} in Appendix C.

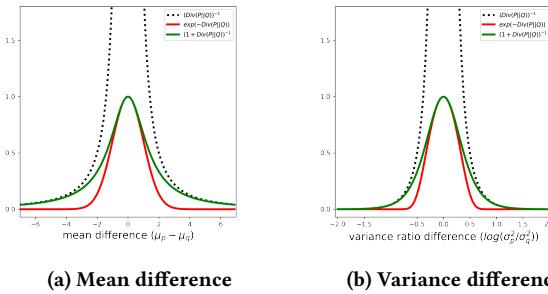


Figure 3: Comparison among similarities. In (a), we set the same variance and vary the means. In (b), we set the same mean and vary the variances.

3.5 Theoretical Analysis

This subsection presents the theoretical analysis of our distributional contrastive loss. The naive way to achieve contrastive disentangling is to use a simple reciprocal of divergence as a $k(\cdot)$ in Eq. 5. However, setting $k(\cdot)$ as a simple reciprocal might cause a numeric instability, as shown in Figure 3. To mitigate the numerical instability and to encourage disentanglement, we provide new kernel motivated contrastive learning. We formulate Gaussian Kernel motivated similarity $\exp(-\text{Div}(P||Q))$ and Student-t motivated similarity $(1 + \text{Div}(P||Q))^{-1}$ for distribution P and Q as shown in Eq. 7 and Eq. 6. If the variance of P and Q are the same, the Student-t kernel based loss returns a greater loss than the Gaussian kernel based loss, when the disentanglement is not enough, as shown in Figure 3 and Proposition 1. Therefore, Student-t kernel contrastive loss may enforce more rigorous disentanglement. In the following propositions, Div denotes the KL divergence.

PROPOSITION 1. Assume that univariate random variables z_1 and z_2 follow Gaussian distribution $N(\mu_1, \sigma^2)$, and $N(\mu_2, \sigma^2)$, respectively. Then $(1 + \text{Div}(p(z_1)||p(z_2)))^{-1} \geq \exp(-\text{Div}(p(z_1)||p(z_2)))$.

We can derive similar results when the mean of P and Q are the same, as shown in Proposition 2. These rigorous disentanglement

properties of Student-t based methods are effective in the general case, but they may overfit when the amount of data is restricted.

Besides, this phenomenon can also occur when we handle noisy datasets. A noisy dataset, which contains corrupted labels as well as some outliers, might have a relatively large variance [1]. Proposition 2 ii) denotes that the Student- t based methods enforce rigorous disentangling even though the variance of Q is large enough. Therefore, this strict enforcement of disentanglement can also lead to overfitting in a noisy dataset, too. We provide an empirical validation on noisy settings in Section 4.1.

PROPOSITION 2. Assume that univariate random variables z_1 and z_2 follow Gaussian distribution $N(\mu_1, \sigma_1^2)$, and $N(\mu_2, \sigma_2^2)$, respectively. Then, i) the global minimum of $(1 + \text{Div}(p(z_1)||p(z_2)))^{-1} - \exp(-\text{Div}(p(z_1)||p(z_2)))$ is zero if $\mu_1 = \mu_2$, and ii) $\lim_{\sigma_2 \rightarrow \infty} (1 + \text{Div}(p(z_1)||p(z_2)))^{-1} - \exp(-\text{Div}(p(z_1)||p(z_2))) > 0$.

4 EXPERIMENTS

To validate FarconVAE, we define three research questions in terms of disentangled fairness, debiasing pretrained large-scale models, and domain generalization. We answer each question in Sections 4.1, 4.2, and 4.3, respectively¹. See Appendix A for detail setup.

RQ1) Disentangled Fairness: Do latent representations z_x contain non-sensitive important information only, excluding sensitive information, while maintaining the predictive performance?

RQ2) Pretrained Models Debiasing: Can FarconVAE be utilized for debiasing a pretrained large-scale model such as BERT?

RQ3) Domain Generalization: Does FarconVAE alleviate the spurious correlation as well as unfairness?

4.1 Fair Classification

Table 1 denotes the performance on Adult, German, and Extended YaleB [10] datasets. Adult and German are tabular datasets [3], and their targets are binary about income and credit risk, respectively. Gender is a sensitive attribute for both datasets. The YaleB dataset is a visual dataset, and the target task is to classify the facial identity as irrelevant to the light condition that is regarded as a sensitive attribute. FarconVAE-G and FarconVAE-t denote the FarconVAE with Gaussian and Student-t kernel contrastive loss. We report the mean and standard deviation of 10 runs. To measure s accuracy, we first train the FarconVAE and encode the entire dataset, and then train a linear classifier for s on it. The representation that has similar s accuracy with Random-Guess can be interpreted as fair.

In terms of y and s accuracy, our FarconVAEs significantly improve the performance over baselines. They show the highest y accuracy while s accuracy is the closest with the Random-Guessing. It denotes that z_x extracted by our model contains the non-sensitive core information while removing the sensitive information. Note that FarconVAE-t has poor performance on s accuracy in German dataset, which is relatively small. Thus, the Student-t kernel based contrastive learning may overfit, while its Gaussian kernel based counterpart still works well. Besides, we visualize the learned representation of FarconVAE and ODFR. Figure 4 denotes that z_x of FarconVAE has important information to classify the target label y , while successfully removing the sensitive information about s .

¹We release the code at: <https://github.com/changdaeho/FarconVAE>

Table 1: Fair classification results on the Adult, German, and YaleB datasets. Random-Guess denotes the y and s accuracy when we predict the class randomly. Therefore, the s accuracy of Random-Guess is the barometer to determine whether the representation has sensitive information or not. * denotes the reported performance in the supplementary material of [32].

Model	Adult		German		YaleB	
	y accuracy	s accuracy	y accuracy	s accuracy	y accuracy	s accuracy
Random-Guess	50.00	50.00	50.00	50.00	2.63	20.00
LFR*	82.30	<u>67.00</u>	72.30	80.50	-	-
VAE*	81.90	66.00	72.50	79.50	-	-
VFAE*	81.30	<u>67.00</u>	72.70	79.70	85.00	57.00
CI	84.49±0.15	68.62±7.19	80.05±0.16	51.70±18.16	89.79±0.33	8.67±1.83
MaxEnt-ARL	84.52±0.06	67.90±0.94	78.75±0.35	49.25±8.82	89.95±0.30	8.67±1.83
ODFR	84.43±0.11	68.93±0.15	78.05±1.34	53.60±12.86	85.09±0.86	14.84±17.91
FarconVAE-t	<u>84.67±0.02</u>	67.38±0.00	83.35±0.75	54.24±18.31	<u>90.96±0.18</u>	20.01±8.30
FarconVAE-G	84.67±0.01	67.36±0.04	<u>83.20±0.35</u>	49.80±13.38	90.99±0.04	<u>18.07±13.27</u>

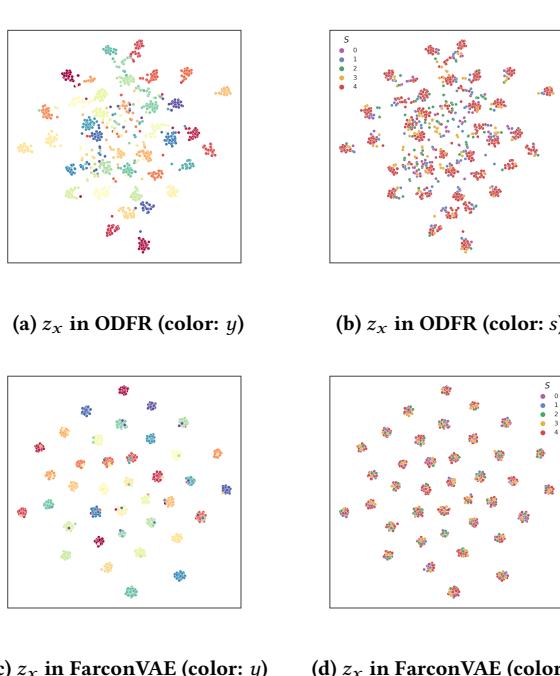


Figure 4: t-SNE visualization of representation learned from ODFR and FarconVAE on YaleB. From (a) and (c), the representation of FarconVAE is more distinctive for label y . (b) and (d) show similar patterns, but the representation of FarconVAE shows less distinctive with respect to sensitive information s , and it denotes the fair representation.

To validate the robustness of our model, we perform the evaluation on noisy data settings. We construct a training set by corrupting the original sensitive attribute s with another one proportional to rate ϵ . Figure 5 represents the performance according to the noise rate ϵ . FarconVAE-t and FarconVAE-G maintain their performance even though the ϵ increases, while other models show performance

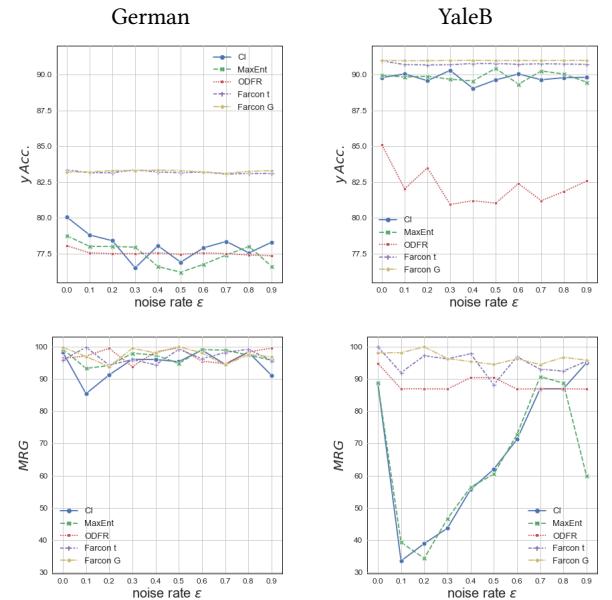


Figure 5: Performance change over noise rate ϵ . Matching with Random Guess (MRG) evaluates the similarity between Random-Guess performance and model performance on s accuracy, i.e., $100\% - |s \text{ accuracy}_{\text{Random-Guess}} - s \text{ accuracy}_{\text{Model}}|$. FarconVAE, especially FarconVAE-G shows a stable performance even though the noise rate ϵ is large.

degradation. When we compare FarconVAE-t and FarconVAE-G, FarconVAE-G shows better performance than FarconVAE-t. It corresponds with our theoretical analysis, as shown in Section 3.5.

4.2 Debiased Sentence Representation

We evaluate our model on a text dataset as well as a tabular and image dataset. It is known that the traditional word embedding or pretrained language model such as BERT [18] has a harmful bias. We validate whether our model, FarconVAE can debias the sentence

Table 2: Debiasing performance on BERT. We use Student-t kernel for FarconVAE. * denotes the reported performance in [6].

	Pretrained BERT					BERT post SST-2				
	Origin*	Sent-D*	FairF ⁻	FairF	FarconVAE	Origin*	Sent-D*	FairF ⁻	FairF	FarconVAE
Names, Career/Family	0.477	0.096	<u>0.067</u>	0.114	0.003	0.036	0.109	0.142	<u>0.042</u>	0.101
Terms, Career/Family	0.108	0.437	<u>0.052</u>	0.051	<u>0.052</u>	0.010	<u>0.057</u>	0.136	0.089	0.097
Terms, Math/Arts	0.253	0.194	0.154	<u>0.097</u>	0.047	<u>0.219</u>	0.221	0.423	0.729	0.034
Names, Math/Arts	0.254	0.194	0.015	0.084	<u>0.056</u>	1.153	0.755	0.769	<u>0.735</u>	0.323
Terms, Science/Arts	0.399	<u>0.075</u>	0.227	0.045	0.179	0.103	<u>0.081</u>	0.118	0.217	0.016
Names, Science/Arts	0.636	0.540	<u>0.424</u>	0.518	0.005	0.222	<u>0.047</u>	0.172	0.077	0.045
Avg. Abs. Effect Size	0.354	0.256	0.154	<u>0.151</u>	0.057	0.291	0.212	0.293	<u>0.163</u>	0.103
Classification Acc.	-	-	-	-	-	92.7	<u>89.1</u>	87.557	87.193	85.468

representation, pretrained from BERT or not. Following the same experiment and evaluation setting with [6], when the input sentence contains a sensitive word, we replace it with the word with the opposite semantic meaning from the pre-defined sensitive word dictionary to construct a contrastive pair. We use the absolute SEAT effect size [25] as a measure of bias. Table 2 denotes the results for our model and baseline models including original BERT, Sent-D [25], and FairFil [6]. Like FairFil, our FarconVAE acts like a small filter that takes the BERT’s sentence representation as input and outputs the debiased representation. When we adopt FarconVAE on BERT, the degree of bias reduces from 0.354 to 0.057. Another column, “BERT post SST-2”, denotes the fine-tuning performance with debiased representation. FarconVAE makes relatively poor classification, but it alleviates the bias largely from 0.291 to 0.103. The results show that FarconVAE can better remove bias in a large-scale language model than existing methods.

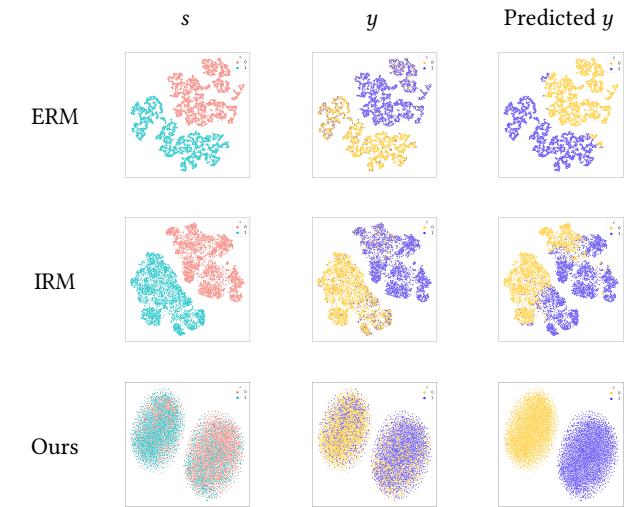
4.3 Domain Generalization

Domain Generalization requires the invariant representations [2] or robust representation [31], and it is commonly known that IRM and Group-DRO improve the domain generalization by alleviating the spurious correlation. However, there is no guarantee that the representations learned by IRM and Group-DRO are free from spurious correlation. We observe that the IRM and Group-DRO improve the predictiveness of representation for y over Empirical Risk Minimization (ERM), but the representations from IRM and Group-DRO still have sensitive information largely. Table 3 denotes the performance of y accuracy and s accuracy on cMNIST [2] and Waterbirds² [35] those are intentionally constructed to have a spurious correlation between y and s . On Waterbirds, we additionally report the worst y acc. which measures the worst accuracy among four groups distinguished by the (s, y) combinations. We applied FarconVAE on top of the feature extractor trained with IRM (for cMNIST) or Group-DRO (for Waterbirds) method. Our method successfully disentangles and removes s information from the learned representation by IRM or Group-DRO, so the FarconVAE is free from spurious correlation and significantly improves the y accuracy.

Figure 6 denotes the visualization of learned embedding from ERM, IRM, and FarconVAE on cMNIST. As shown in the first column

Table 3: Domain generalization performance on cMNIST and Waterbirds. Mean and standard deviation of five runs.

Model	cMNIST		Waterbirds		
	y acc.	s acc.	y acc.	worst y acc.	s acc.
ERM	16.91 ± 0.57	97.65 ± 0.21	78.47 ± 0.57	31.87 ± 1.20	86.07 ± 0.69
IRM	66.27 ± 1.42	100.00 ± 0.00	-	-	-
gDRO	-	-	90.21 ± 0.57	85.98 ± 1.16	86.60 ± 0.91
Ours	70.43 ± 0.61	35.10 ± 3.35	95.03 ± 0.99	91.71 ± 1.48	51.71 ± 0.38

**Figure 6: t-SNE visualization for representation of the penultimate layer from ERM, IRM, and FarconVAE. As shown in the first column, the representations by ERM and IRM have sensitive information, while that from FarconVAE has significantly less sensitive information. Because the representation from ERM and IRM has spurious correlation, they have difficulty in predicting y in test time when the correlation is reversed, while FarconVAE shows stable prediction.**

²For a consistent evaluation, we report average accuracy for y and s . It is different from the weighted average accuracy (for y) reported in [31] for Waterbirds dataset.

of Figure 6, the learned representation from ERM and IRM are easily divided by sensitive attribute s . However, the representation learned from FarconVAE is not easily divided by sensitive attributes. From the second and third columns, we can check that FarconVAE predicts y well, while ERM and IRM predict opposite y entirely or partially, respectively. To the best of our knowledge, this is the first work that provides general disentangling methods that can be utilized in both domain generalization and fairness tasks.

5 CONCLUSION

Algorithmic fairness demands fair representation learning that captures the non-sensitive core information. Domain generalization tasks also have difficulty removing spurious features for domain-invariant learning. This paper proposes FarconVAE, a new contrast-based disentangling approach that removes sensitive information or spurious correlation from representation while maintaining non-sensitive core information. We provide a kernel motivated distributional contrastive loss that stably induces disentangled invariant representation and a swap-recon loss that enforces swap-consistent reconstruction for further enhancing disentanglement.

FarconVAE improves the out-of-distribution generalization as well as the fairness. Besides, we observe that the representation learned by IRM or Group-DRO still has a strong spurious correlation between the targets and sensitive attributes, and FarconVAE mitigates this correlation significantly. We provide extensive empirical results about fairness, pretrained model debiasing, and domain generalization on tabular, image, and text datasets. Moreover, we derive a theoretical result for our new contrastive loss.

ACKNOWLEDGEMENTS

This work was partly supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2021-0-02067, Next generation AI for multi-purpose video search, 50%) and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT). (No. 2021R1F1A1060117, Research and Application of Artificial Intelligence Algorithm for Removing Spurious Bias, 50%)

REFERENCES

- [1] Jinwon An and Sungzoon Cho. 2015. Variational autoencoder based anomaly detection using reconstruction probability. *Special Lecture on IE* 2, 1 (2015), 1–18.
- [2] Martin Arjovsky, Léon Bottou, Ishaaan Gulrajani, and David Lopez-Paz. 2019. Invariant risk minimization. *arXiv preprint arXiv:1907.02893* (2019).
- [3] Arthur Asuncion and David Newman. 2007. UCI machine learning repository.
- [4] Yoshua Bengio, Aaron Courville, and Pascal Vincent. 2013. Representation learning: A review and new perspectives. *IEEE transactions on pattern analysis and machine intelligence* 35, 8 (2013), 1798–1828.
- [5] Ting Chen, Simon Kornblith, Mohammad Norouzi, and Geoffrey Hinton. 2020. A simple framework for contrastive learning of visual representations. In *International conference on machine learning*. PMLR, 1597–1607.
- [6] Pengyu Cheng, Weituo Hao, Siyang Yuan, Shijing Si, and Lawrence Carin. 2021. FairFil: Contrastive Neural Debiasing Method for Pretrained Text Encoders. In *International Conference on Learning Representations*.
- [7] Elliot Creager, Jörn-Henrik Jacobsen, and Richard Zemel. 2021. Environment inference for invariant learning. In *International Conference on Machine Learning*. PMLR, 2189–2200.
- [8] Elliot Creager, David Madras, Jörn-Henrik Jacobsen, Marissa Weis, Kevin Swersky, Tonianne Pitassi, and Richard Zemel. 2019. Flexibly fair representation learning by disentanglement. In *International conference on machine learning*. PMLR, 1436–1445.
- [9] Tianyu Gao, Xingcheng Yao, and Danqi Chen. 2021. SimCSE: Simple Contrastive Learning of Sentence Embeddings. In *Empirical Methods in Natural Language Processing (EMNLP)*.
- [10] Athinodoros S. Georghiades, Peter N. Belhumeur, and David J. Kriegman. 2001. From few to many: Illumination cone models for face recognition under variable lighting and pose. *IEEE transactions on pattern analysis and machine intelligence* 23, 6 (2001), 643–660.
- [11] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. Generative adversarial nets. *Advances in neural information processing systems* 27 (2014).
- [12] Arthur Gretton, Karsten Borgwardt, Malte Rasch, Bernhard Schölkopf, and Alex Smola. 2006. A kernel method for the two-sample-problem. *Advances in neural information processing systems* 19 (2006).
- [13] Ishaaan Gulrajani and David Lopez-Paz. 2020. In Search of Lost Domain Generalization. In *International Conference on Learning Representations*.
- [14] Junxian He, Daniel Spokoiny, Graham Neubig, and Taylor Berg-Kirkpatrick. 2018. Lagging Inference Networks and Posterior Collapse in Variational Autoencoders. In *International Conference on Learning Representations*.
- [15] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 770–778.
- [16] Irina Higgins, Loic Matthey, Arka Pal, Christopher Burgess, Xavier Glorot, Matthew Botvinick, Shakir Mohamed, and Alexander Lerchner. 2016. beta-vae: Learning basic visual concepts with a constrained variational framework. (2016).
- [17] Michael I Jordan, Zoubin Ghahramani, Tommi S Jaakkola, and Lawrence K Saul. 1999. An introduction to variational methods for graphical models. *Machine learning* 37, 2 (1999), 183–233.
- [18] Jacob Devlin Ming-Wei Chang Kenton and Lee Kristina Toutanova. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of NAACL-HLT*. 4171–4186.
- [19] Eungyeup Kim, Jihyeon Lee, and Jaegul Choo. 2021. Biaswap: Removing dataset bias with bias-tailored swapping augmentation. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 14992–15001.
- [20] Hyunjik Kim and Andriy Mnih. 2018. Disentangling by factorising. In *International Conference on Machine Learning*. PMLR, 2649–2658.
- [21] Hyemi Kim, Seungjae Shin, JoonHo Jang, Kyungwoo Song, Weonyoung Joo, Wanmo Kang, and Il-Chul Moon. 2021. Counterfactual fairness with disentangled causal effect variational autoencoder. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 35. 8128–8136.
- [22] Diederik P. Kingma and Max Welling. 2014. Auto-Encoding Variational Bayes. In *2nd International Conference on Learning Representations, ICLR 2014, Banff, AB, Canada, April 14–16, 2014, Conference Track Proceedings*, Yoshua Bengio and Yann LeCun (Eds.).
- [23] Daniel Levy, Yair Carmon, John C Duchi, and Aaron Sidford. 2020. Large-scale methods for distributionally robust optimization. *Advances in Neural Information Processing Systems* 33 (2020), 8847–8860.
- [24] Yujia Li, Chenjie Gu, Thomas Dullien, Oriol Vinyals, and Pushmeet Kohli. 2019. Graph matching networks for learning the similarity of graph structured objects. In *International conference on machine learning*. PMLR, 3835–3845.
- [25] Paul Pu Liang, Irene Mengze Li, Emily Zheng, Yao Chong Lim, Ruslan Salakhutdinov, and Louis-Philippe Morency. 2020. Towards debiasing sentence representations. *arXiv preprint arXiv:2007.08100* (2020).
- [26] Christos Louizos, Kevin Swersky, Yujia Li, Max Welling, and Richard Zemel. 2015. The variational fair autoencoder. *arXiv preprint arXiv:1511.00830* (2015).
- [27] Wesley J Maddox, Pavel Izmailov, Timur Garipov, Dmitry P Vetrov, and Andrew Gordon Wilson. 2019. A simple baseline for bayesian uncertainty in deep learning. *Advances in Neural Information Processing Systems* 32 (2019).
- [28] David Madras, Elliot Creager, Tonianne Pitassi, and Richard Zemel. 2018. Learning adversarially fair and transferable representations. In *International Conference on Machine Learning*. PMLR, 3384–3393.
- [29] Michael F Mathieu, Junbo Jake Zhao, Junbo Zhao, Aditya Ramesh, Pablo Sprechmann, and Yann LeCun. 2016. Disentangling factors of variation in deep representation using adversarial training. *Advances in neural information processing systems* 29 (2016).
- [30] Proteek Chandan Roy and Vishnu Naresh Boddeti. 2019. Mitigating information leakage in image representations: A maximum entropy approach. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2586–2594.
- [31] Shiori Sagawa, Pang Wei Koh, Tatsunori B Hashimoto, and Percy Liang. 2020. Distributionally robust neural networks for group shifts: On the importance of regularization for worst-case generalization. *arXiv preprint arXiv:1911.08731* (2020).
- [32] Mhd Hasan Sarhan, Nassir Navab, Abouzar Eslami, and Shadi Albarqouni. 2020. Fairness by learning orthogonal disentangled representations. In *European Conference on Computer Vision*. Springer, 746–761.
- [33] Uri Shalit, Fredrik D Johansson, and David Sontag. 2017. Estimating individual treatment effect: generalization bounds and algorithms. In *International Conference on Machine Learning*. PMLR, 3076–3085.

- [34] Aaron van den Oord, Yazhe Li, and Oriol Vinyals. 2019. Representation Learning with Contrastive Predictive Coding. *arXiv:1807.03748 [cs.LG]*
- [35] Catherine Wah, Steve Branson, Peter Welinder, Pietro Perona, and Serge Belongie. 2011. The caltech-ucsd birds-200-2011 dataset. (2011).
- [36] Satosi Watanabe. 1960. Information theoretical analysis of multivariate correlation. *IBM Journal of research and development* 4, 1 (1960), 66–82.
- [37] Ethan Weinberger, Nicasia Beebe-Wang, and Su-In Lee. 2022. Moment Matching Deep Contrastive Latent Variable Models. *arXiv preprint arXiv:2202.10560* (2022).
- [38] Qizhe Xie, Zihang Dai, Yulun Du, Eduard Hovy, and Graham Neubig. 2017. Controllable invariance through adversarial feature learning. *Advances in neural information processing systems* 30 (2017).
- [39] Lei Xu, Maria Skoularidou, Alfredo Cuesta-Infante, and Kalyan Veeramachaneni. 2019. Modeling tabular data using conditional gan. *Advances in Neural Information Processing Systems* 32 (2019).
- [40] Minghao Xu, Jian Zhang, Bingbing Ni, Teng Li, Chengjie Wang, Qi Tian, and Wenjun Zhang. 2020. Adversarial domain adaptation with domain mixup. In *Proceedings of the 2018 AAAI Conference on Artificial Intelligence*, Vol. 34. 6502–6509.
- [41] Rich Zemel, Yu Wu, Kevin Swersky, Toni Pitassi, and Cynthia Dwork. 2013. Learning fair representations. In *International conference on machine learning*. PMLR, 325–333.
- [42] Brian Hu Zhang, Blake Lemoine, and Margaret Mitchell. 2018. Mitigating unwanted biases with adversarial learning. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*. 335–340.
- [43] Bolei Zhou, Agata Lapedriza, Aditya Khosla, Aude Oliva, and Antonio Torralba. 2017. Places: A 10 million image database for scene recognition. *IEEE transactions on pattern analysis and machine intelligence* 40, 6 (2017), 1452–1464.

A EXPERIMENTAL SETUP

A.1 Fair Classification

For fair classification, we consider three benchmark datasets previously used in [32]. The Adult dataset contains 45,222 instances, each with 14 attributes. The target y is a binary label of annual income more or less than \$50,000 and gender is sensitive attribute s . The German dataset has 1,000 instances, each with 20 attributes, and the target task is to classify bank account holders with good or bad credit risk. The sensitive attribute is gender again. Both of these are tabular datasets obtained from the UCI ML-repository [3]. The Extended YaleB [10] is a visual dataset that contains the face images of 38 people under five different light conditions. The target task is to identify one of the 38 people for a given data instance, while the light condition is the sensitive attribute here.

A.2 Pretrained Model Debiasing

For the pretrained model debiasing task, we validate our method on BERT [18]. Specifically, we attach the FarconVAE-t on top of BERT’s layers, takes [CLS] token embedding for each sentence as model input x and the sensitive words are regarded as s . Following the setup [6], we use the same corpora consisting of 183,060 sentences for training, and the sensitive attribute is mainly gender-related words.

A.3 Domain Generalization

For domain generalization task, we experimented with two image datasets cMNIST [2] and Waterbirds [31]. The cMNIST is a synthetic dataset for binary classification, which intentionally makes correlation between labels (digit) and sensitive attributes (color) of the train set. A model is evaluated with the test set, which has the opposite correlation to the train set. The Waterbirds dataset is constructed by combining bird photographs from the CUB dataset [35] with backgrounds from the Places dataset [43]. The target label is the bird’s breed (waterbird or landbird), and the sensitive attribute is the background (water or land). Like cMNIST, there is a spurious correlation between y and s in the train dataset.

B IMPLEMENTATION DETAILS

B.1 Conditional Information at Test Time

We put y as FarconVAE input to increase the predictiveness of the representation. But unlike the training phase, we generally do not have access to true labels in the testing phase. So we train a separate classifier predicting y from x in advance or together with FarconVAE’s training phase. It is also possible to use a well-fitted pretrained model on the given dataset. After we build the best classifier that maps x to y , we use the predicted label \hat{y} by the classifier for each test set instance as the input of FarconVAE. For Adult, German, Extended YaleB, and CMNIST, this classifier is a simple multi-layer perceptron (MLP). For Waterbirds dataset, the classifier is ResNet-50 [15]. For debiasing task on BERT, when FarconVAE is trained on the unannotated corpus (results of the left side in Table 2), the target label does not exist. In this case, we input the constant $y = 0.5$ to FarconVAE. When FarconVAE is finetuned with BERT on the labeled corpus (results of the right side in Table 2), we also input the constant $y = 0.5$ for consistent training.

B.2 Model Configuration

In this subsection, we introduce the setting of model architecture, hyperparameters, and other experimental options. To learn more informative representation, we use ELBO of β -VAE formulation [16], which can control the intensity of KLD regularization instead of the basic ELBO in Section 3.2. So, our ELBO has a parameter β .

$$\mathcal{L}_{ELBO}(\phi, \theta) = L_{rec}(\phi, \theta | \theta_y) + L_{pred}(\phi, \theta_y) - \beta L_{KLD}(\phi)$$

In the sections below, $\alpha, \beta, \gamma, LR$, and WD denote the weight of loss terms L_{DC} , L_{KLD} , L_{SR} , learning rate, and weight decay hyperparameter, respectively. See Github³ for details not listed here.

B.2.1 Fair Classification. On Adult and German datasets, we follow the setup in [30, 32] for all possible configurations. So, the encoder q_ϕ and decoder $p_{\theta|\theta_y}$ are both one hidden layer with 64 hidden units and the decoder p_{θ_y} (referred as target predictor in [30, 32]) is linear logistic regression. The latent dimension of z_x are 15 in Adult and 5 in German. For Extended YaleB dataset, we use one linear layer as encoder, decoder $p_{\theta|\theta_y}$ and decoder p_{θ_y} each contain 100 hidden units. The latent dimension is also 100.

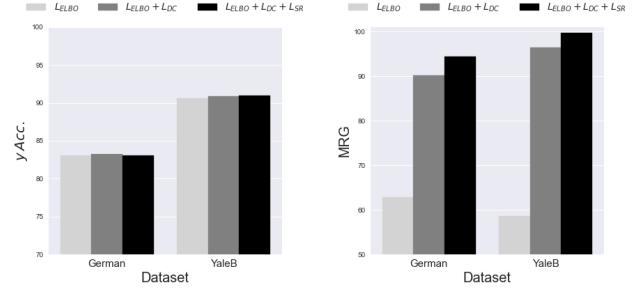
B.2.2 Pretrained Model Debiasing. We use one linear layer for all components of FarconVAE with 128 hidden units and 128 latent dim. For doing contrastive learning on unlabeled corpus, we flip the sensitive words of a given sentence to follow [6]. If a sentence does not contain any sensitive words, a constant tensor of 0.5 which has the same shape as the embedding was inputted to FarconVAE and L_{DC} and L_{SR} are not used. In the fine-tuning stage, most of the sentences do not have sensitive words, so we use the mean embedding of pre-defined sensitive words list as FarconVAE input. We use $(\alpha, \beta, \gamma, LR, WD) = (1.0, 0.2, 1.0, 5e-4, 1e-4)$ for FarconVAE contrastive-training, and $(\alpha, \beta, \gamma, LR_{BERT}, LR_{Farcon}, WD) = (1.0, 0.2, 0.0, 2e-5, 1e-4, 1e-2)$ for entire fine-tuning.

B.2.3 Domain Generalization. Like above, we attach the FarconVAE on top of IRM or Group-DRO feature extractors (fixed) and use the representation from them as FarconVAE's input feature. Again, we use one linear layer for all components of the FarconVAE latent dim set to 100 with 75 and 100 hidden units for cMNIST and Waterbirds, respectively. For cMNIST, we use $(\alpha, \beta, \gamma, LR, WD) = (1.0, 0.2, 0.0, 1e-3, 1e-4)$. For Waterbirds, we use $(\alpha, \beta, \gamma, LR, WD) = (0.5, 0.2, 0.5, 7e-4, 1e-4)$ and we anneal β from zero to 0.2 during the first 10% epochs.

C ABLATION STUDY

In this section, we provide the ablation study for our proposed methods. Figure 7 indicates that our proposed algorithm, FarconVAE with distributional contrastive loss is effective in disentangling the latent representation space, and as a result, it induces a fair representation. Moreover, the disentanglement is further enhanced when swap-recon (\mathcal{L}_{SR}) is added. MRG in the right panel of Figure 7 denotes similarity between the y accuracy of model and that of random guessing, same with Figure 5.

³<https://github.com/changdaeh/FarconVAE>



(a) Ablation study for y accuracy (b) Ablation study for MRG

Figure 7: Ablation study for \mathcal{L}_{DC} and \mathcal{L}_{SR} .

D DERIVATION OF ELBO

We assume that the z_x and z_s are conditionally independent given x, s, y^4 , i.e., $q_\phi(z_x, z_s | x, s, y) = q_{\phi_{z_x}}(z_x | x, s, y)q_{\phi_{z_s}}(z_s | x, s, y)$. Then, the evidence lower bound of the log marginal likelihood is:

$$\begin{aligned} & \log p_\theta(x, s, y) \\ &= \log \int \frac{q_\phi(z_x, z_s | x, s, y)}{q_\phi(z_x, z_s | x, s, y)} p_\theta(x, s, y | z_x, z_s) p(z_x, z_s) dz_s dz_x \\ &\geq \int q_\phi(z_x, z_s | x, s, y) \log \frac{p_\theta(x, s, y | z_x, z_s) p(z_x, z_s)}{q_\phi(z_x, z_s | x, s, y)} dz_s dz_x \\ &= \mathbb{E}_{q_\phi} [\log p_{\theta_x}(x | z_x, z_s) + \log p_{\theta_s}(s | z_x, z_s) + \log p_{\theta_y}(y | z_x)] \\ &\quad - KL(q_{\phi_x}(z_x | x, s, y) || p(z_x)) - KL(q_{\phi_s}(z_s | x, s, y) || p(z_s)) \\ &= \mathcal{L}_{ELBO}(\phi, \theta; x, s, y) \end{aligned}$$

E PROOF

Proof for Proposition 1. For simplicity, we denote t as a $\mu_1 - \mu_2$. The KL divergence between two Gaussian distributions, $\mathcal{N}(\mu_1, \sigma^2)$ and $\mathcal{N}(\mu_2, \sigma^2)$ are $\frac{t^2}{2\sigma^2}$.

Then, $(1 + Div(p(z_1) || p(z_2))) - \exp(Div(p(z_1) || p(z_2))) = \frac{t^2}{2\sigma^2} - \exp(\frac{t^2}{2\sigma^2}) + 1$.

When $\mu_1 = \mu_2$, $1 + \frac{t^2}{2\sigma^2} - \exp(\frac{t^2}{2\sigma^2}) = 0$, and $\frac{\partial(1+Div(p(z_1)||p(z_2)))-\exp(Div(p(z_1)||p(z_2)))}{\partial t} = \frac{t-t\exp(x^2/(2\sigma^2))}{\sigma^2} < 0$.

Therefore, $(1 + Div(p(z_1) || p(z_2)))^{-1} \geq \exp(-Div(p(z_1) || p(z_2)))$, and the equality holds when $t = 0$, i.e., $\mu_1 = \mu_2$.

Proof for Proposition 2. For simplicity, we denote t as a $\frac{\sigma_2}{\sigma_1}$.

i) The KL divergence between two Gaussian distributions, $\mathcal{N}(\mu, \sigma_1^2)$ and $\mathcal{N}(\mu, \sigma_2^2)$ are $\log(t) + \frac{1}{2t^2} - 0.5$.

Then, $f(t) = (1 + Div(p(z_1) || p(z_2))) - \exp(Div(p(z_1) || p(z_2))) = 0.5 + \frac{1}{2t^2} - \exp(-0.5 + \frac{1}{2t^2})t + \log(t)$.

$f(t)$ is differentiable for all $t > 0$, and the only critical point of $\frac{\partial f(t)}{\partial t} = 0$ is at $t = 1$. The domain of $f'(t)$ is $t \in R : t > 0$, and $f(t)$ is $-\infty$ when $t = 0^+$ and ∞ . Therefore, the global minimum of $(1 + Div(p(z_1) || p(z_2)))^{-1} - \exp(-Div(p(z_1) || p(z_2)))$ is zero

ii) $\lim_{\sigma_2 \rightarrow \infty} (1 + Div(p(z_1) || p(z_2)))^{-1} - \exp(Div(p(z_1) || p(z_2))) < 0$. Therefore, $(1 + Div(p(z_1) || p(z_2)))^{-1} - \exp(-Div(p(z_1) || p(z_2))) > 0$ for sufficiently large σ_2^2 .

⁴To satisfy the assumption, we adopt contrastive loss as shown in Sec. 3 of main paper