Out-of-distribution Generalization via Partial Feature Decorrelation

Xin Guo*, Zhengxu Yu*, Chao Xiang, Zhongming Jin, Jianqiang Huang, Deng Cai, Senior Member, IEEE, Xiaofei He, Senior Member, IEEE, and Xian-Sheng Hua, Fellow, IEEE

Abstract—Most deep-learning-based image classification methods assume that all samples are generated under an independent and identically distributed (IID) setting. However, out-of-distribution (OOD) generalization is more common in practice, which means an agnostic context distribution shift between training and testing environments. To address this problem, we present a novel Partial Feature Decorrelation Learning (PFDL) algorithm, which jointly optimizes a feature decomposition network and the target image classification model. The feature decomposition network decomposes feature embeddings into the independent and the correlated parts such that the correlations between features will be highlighted. Then, the correlated features help learn a stable feature representation by decorrelating the highlighted correlations while optimizing the image classification model. We verify the correlation modeling ability of the feature decomposition network on a synthetic image classification model. The experiments on real-world datasets demonstrate that our method can improve the backbone model’s accuracy on OOD datasets.

Index Terms—Stable learning, image classification, out-of-distribution generalization.

I. INTRODUCTION

CLASSIFYING unknown images based on a model trained on a training dataset is a common machine learning problem [1]–[5]. With the rise of deep learning methods, image classification accuracy has been improved tremendously on many public datasets [6]–[10]. Most deep-learning-based image classification methods follow a consistency assumption that all samples are generated under an independent and identically distributed (IID) setting [11]. Under this assumption, an approximation of the true distribution can be learned by yielding a lower loss on the training set. However, in real-world applications, we cannot guarantee the unknown test data have the same distribution as the training data due to the data generation bias [11]–[16], which is known as out-of-distribution (OOD) generalization [17]–[19]. Consequently, in such training environment, these IID-based methods will inevitably overfit the statistical correlations between features and omit the actual causality between the target object and the label [20].

A toy example of this agnostic distribution shift problem caused by data generation bias has been shown in Figure. 1 in which ‘bear in the forest’ has a higher data frequency than ‘bear in the water.’ The label of the first row is ‘bear’, and the second row is ‘cow’. A typical IID-based deep-learning model trained on such a dataset will inevitably absorb the correlation between object ‘bear’ and context ‘forest’ to yield a lower training loss. Consequently, causality between the feature of the target object ‘bear’ and the label ‘bear’ is blurred by the correlation between the feature of context ‘forest’ and the label ‘bear’. We can find a similar correlation between the context feature ‘water’ and the label ‘cow’ in Figure. 1. This dilemma can lead to an unstable performance in a testing environment where ‘cow in the forest’ has higher data frequency. Because the misspecified model partly relies on the correlation between the context features ‘water’ and the label ‘cow’.

Recently, many works have been proposed to solve this agnostic distribution shift problem [21]–[29], including domain adaption-based methods and some causality-based sample re-weighting methods [23], [25], [27]. Some domain adaption-based methods are based on a straightforward thought of taking advantage of the prior knowledge of the testing environment. However, it is impossible to obtain prior knowledge of the test data in many real-world applications, which hinders the application of these methods. As for causality-based sample re-weighting methods, most of them [24], [25], [28], [29] are based on increasing the importance of samples with lower data frequency to mitigate the impact of the agnostic distribution shift problem. Most of these methods require a large re-weighting matrix whose parameter number is proportional to the number of training samples, both computation and memory...
intensive.

To address these problems, we propose to learn a stable feature representation in an OOD generalization setting by decomposing and removing the effect of correlations on the feature embeddings. Specifically, we propose a novel Partial Feature Decorrelation Learning (PFDL) algorithm for OOD image classification tasks. In this algorithm, we jointly optimize a feature decomposition network and the target image classification model while fixing each of the network’s parameters in turn. The start point of the feature decomposition network is to learn and decompose the correlated part features from the learned feature embedding using the followed decorrelation operations. After that, we decorrelate the correlated part features while optimizing the target image classification model. We can learn a stable feature representation by decorrelating as many correlations as possible without disturbing the stable connections between features. Compared with previous sample re-weighting-based methods, our model’s parameter number is not proportional to the training sample number, which provides better scalability than previous works in applications with massive training data. The experimental results demonstrate that the model’s accuracy and stability trained by our method can outperform all the baselines and the state-of-the-art stable learning methods on several OOD datasets.

We summarize the contributions of this work as follows:

1. We study how to learn a stable feature representation under OOD generalization problems from decomposing and decorrelating the correlated part features to improve the model’s accuracy and propose a novel Partial Feature Decorrelation Learning (PFDL) algorithm.

2. We design a feature decomposition network that separates the independent features from the correlated ones. We also develop a Partial Feature Decorrelation objective function, which aims to learn a stable feature representation by decorrelating the correlations while optimizing the target image classification model.

3. We verify the correlation modeling ability of the feature decomposition network on a synthetic dataset. The experimental results demonstrate that our model can achieve state-of-the-art performance on real-world datasets.

II. RELATED WORK

A. Causality-based Methods

Most recently proposed causality-based methods [24], [25], [28]–[30] are based on sample re-weighting, which does not directly change the biased sample features but shifts the training dataset’s distribution by varying the importance of the samples. [24] proposes a sample re-weighting method to address the collinearity among input variables caused by the agnostic distribution shift. [25] proposes a feature decorrelation-based sample re-weighting method to decorrelate all features without considering the possible causality between features. However, these sample re-weighting methods require a large re-weighting matrix whose parameter number is proportional to the training samples. Hence, these works are both computation and memory intensive. This disadvantage limits their scalability in machine learning tasks with a large number of training data. Unlike these methods, our model learns the associations between features using a neural network whose parameter number is not proportional to the sample number, which provides feasibility for tasks with an extensive training dataset.

B. Non-causality-based Methods

In addition to causality-based methods, a variety of domain adaptation [27], [31], [32], domain generalization [33], and transfer learning methods [22], [23] are proposed to address the OOD generalization problem. Some of these methods handle the distribution shift between training and testing datasets by aligning the training dataset to the target dataset or vice versa. To achieve that, these methods require prior knowledge of the target domain distribution. However, it is impossible to acquire prior knowledge in many real-world applications. Unlike them, our method is intended to partition the observed associations among features to improve the model’s performance, which requires no prior knowledge of the testing environments.

C. Feature Decorrelation

Some Lasso-based framework [34], [35] propose to decorrelate features by adding a regularizer that imposes the highly correlated features not to be selected simultaneously. [24]–[26] propose to address the problem by removing the dependencies between features via learning weights for training samples, which helps deep models get rid of spurious correlations and, in turn, concentrate more on the true connection between discriminative features and labels.

III. PARTIAL FEATURE DECORRELATION LEARNING

Our goal is to learn a predictive model for image classification with agnostic distribution shift in this paper. As we discussed above, the agnostic distribution shift can result in correlations between features.

A. Problem Definition

We first introduce a formal definition of the OOD image classification problem proposed by [11] as follows:

a) OOD Image Classification: Given the training dataset \( \mathcal{D}_{\text{train}} = \{(x_i, y_i)\}_{i=1}^{n_{\text{train}}} \) and the testing dataset \( \mathcal{D}_{\text{test}} = \{(x_i, y_i)\}_{i=1}^{n_{\text{test}}} \), where \( x_i \in \mathbb{R}^{c \times h \times w} \) represents an image sample, and \( y_i \in \mathbb{R}^p \) represents its label, the task is to learn a feature extractor \( f : \mathbb{R}^{c \times h \times w} \rightarrow \mathbb{R}^p \) with a dimension hyper-parameter \( p \) and a classifier \( z : \mathbb{R}^p \rightarrow \mathbb{R}^1 \) so that \( z \circ f \) can predict the labels of testing data precisely when data distributions \( \psi(\mathcal{D}_{\text{train}}) \neq \psi(\mathcal{D}_{\text{test}}) \), and \( \psi(\mathcal{D}_{\text{test}}) \) is unknown.

b) Notations: In this work, capital letter refers to random vector and bold capital letter refers to matrix. \( n \) refers to the sample size, and \( p \) is the dimensions of variables. For any matrix \( U \in \mathbb{R}^{n \times p} \), we let \( U_i \) and \( U_{j,:} \) represent the \( i \)-th sample and the \( j \)-th variable in \( U \), respectively. \( U(-j) \in \mathbb{R}^{n \times (p-1)} \) denotes the rest of \( U \) by removing its \( j \)-th dimension.
**B. Feature Decomposition Network**

This subsection introduces our feature decomposition network, which decomposes feature embedding into the independent and correlated parts. Let random vector $U$ denotes the feature embedding extracted by $f$. Thus $U$ represents feature embeddings of the training set $D_{train}$ extracted by $f$. We can treat $U \in \mathbb{R}^p$ as a concatenation of random vectors $S \in \mathbb{R}^{p_s}$ and $V \in \mathbb{R}^{p_v}$, where $p = p_s + p_v$ and $U = [S^T; V^T]^T$. Inspired by [36], we suppose $S$ can be decomposed into two parts $S = S_{ind} + \hat{g}(V)$. The independent part $S_{ind}$ is independent of $V$, and the correlated part $\hat{g}(V)$ is a function of $V$.

We propose to learn the correlation function $\hat{g} : \mathbb{R}^{p_v} \rightarrow \mathbb{R}^{p_v}$ with a network $g : \mathbb{R}^{p_v} \rightarrow \mathbb{R}^{p_v}$. Then, we can divide $\mathbb{E}||S - g(V)||^2_2$ as follows:

$$
\begin{align*}
\mathbb{E}||S - g(V)||^2_2 &= \mathbb{E}||S_{ind} + \hat{g}(V) - g(V)||^2_2 \\
&= \mathbb{E}||S_{ind} - E[S_{ind}] + (\hat{g}(V) + E[S_{ind}]) - g(V)||^2_2 \\
&= \mathbb{E}||S_{ind} - E[S_{ind}]||^2_2 + \mathbb{E}[(\hat{g}(V) + E[S_{ind}]) - g(V)||^2_2 \\
&\quad + 2 \mathbb{E}[S_{ind} - E[S_{ind}]]^T \mathbb{E}[\hat{g}(V) + E[S_{ind}]] - g(V) \\
&= \mathbb{E}||S_{ind} - E[S_{ind}]||^2_2 + \mathbb{E}[(\hat{g}(V) + E[S_{ind}]) - g(V)||^2_2
\end{align*}
$$

(1)

For simplicity but without loss of generality, we can assume that $\mathbb{E}[S_{ind}] = 0$, then (1) becomes:

$$
\mathbb{E}||S - g(V)||^2_2 = \mathbb{E}||S_{ind}||^2_2 + \mathbb{E}||\hat{g}(V) - g(V)||^2_2
$$

(2)

Since $S_{ind}$ and $V$ are independent, $\mathbb{E}||S - g(V)||^2_2$ reaches minimum if and only if $g(V) = \hat{g}(V)$. In conclusion, the solution to the optimization problem

$$
\min_{\hat{g}} \mathbb{E}||S - g(V)||^2_2
$$

(3)

is $\hat{g}$.

Thanks to the universal approximation theorem [37], we can use multi-layer perceptrons (MLPs) to model the correlations between $S$ and $V$.

In practice, a training set $D_{train} = \{(x_i, y_i)\}_{i=1}^n$, and feature embedding $U_i = f(x_i)$ is given, where $U \in \mathbb{R}^{n \times p}$ and $p$ denotes the dimension of the feature embedding. In our model, for each feature dimension, we successively consider each $U_{i,j} \in \mathbb{R}^{n \times 1}$ of the feature embedding as the random sample of random vector $S$ and the rest part $U_{i,-j} \in \mathbb{R}^{n \times (p-1)}$ as the random sample of random vector $V$. Then we have the loss function of the feature decomposition network $g$ as follows:

$$
\mathcal{L}_g = \frac{1}{n} \frac{1}{p} \sum_{j=1}^{p} \sum_{i=1}^{n} ||U_{i,j} - \hat{U}_{i,j}||^2_2
$$

(4)
where \( \tilde{U}_{i,j} = g(U^{(-j)}_{i,j}) \), and \( U^{(-j)}_{i,j} \) denotes the sample \( x_i \)'s feature embedding except the \( j \)-th dimension.

However, suppose \( D_{\text{train}} \) and \( D_{\text{test}} \) are generated under OOD generalization settings. In that case, the training set \( D_{\text{train}} \) is biased from the true distribution. The model will inevitably overfit the correlations only existing in the training set and omit some causality and connections between features. It can make the residual \( S_{\text{ind}} \) of the misspecified model deviate from the true \( S_{\text{ind}} \).

Hence, if we can adjust the feature extractor to reduce the distance between \( S_{\text{ind}} \) and \( S_{\text{ind}} \), we can learn a stable image classification model. Although the true \( S_{\text{ind}} \) is unknown, we can still lower the loss in (3) by iteratively optimizing \( g \) and the target image classification model. There is no prior knowledge about which part of the feature embedding is the effect of correlation features in real-world applications. Hence, as shown in (3) and Figure. 2 'Step 1', we successively modeling each dimension \( U_{i,j} \) of the feature embedding using a parameter-shared feature decomposition network \( g \).

C. Partial Feature Decorrelation Algorithm

In this subsection, we introduce the partial feature decorrelation learning algorithm, which uses (4) and \( g \) to help learn a stable feature representation.

Our goal is to decorrelate correlated features. Given a feature extractor \( f \), we use the well-trained and fixed feature decomposition network \( g \) to decompose the correlated part features when training feature extractor \( f \) and classifier \( z \).

In general cases, assume that \( X \in \mathbb{R}^{n \times p_x} \) and \( Y \in \mathbb{R}^{n \times p_y} \) are the random samples of random vectors \( X \in \mathbb{R}^{p_x} \) and \( Y \in \mathbb{R}^{p_y} \). If \( X \) and \( Y \) are independent, we have \( \operatorname{cov}(X,Y) = \mathbb{E}[X^T Y] - \mathbb{E}[X]^T \mathbb{E}[Y] = 0 \). Thus, \( \mathbb{E}[X^T Y] = \mathbb{E}[X]^T \mathbb{E}[Y] \). Moreover, if \( \mathbb{E}[Y] = 0 \), then \( \mathbb{E}[X^T Y] = 0 \). For simplicity but without loss of generality, we assume that \( \mathbb{E}[V] = 0 \). Hence, we propose the feature decorrelation constraint that minimize the correlation between \( g(V) \) and \( V \) to partially decorrelate features, when training the feature extractor \( f \). Formally:

\[
L_{\text{decorr}} = \frac{1}{p} \sum_{j=1}^{p} \left\| \frac{1}{n(p-1)} \sum_{i=1}^{n} \sum_{k \neq j} U_{i,j} U^{(-j)}_{i,k} \right\|_2^2
\]

(5)

where \( U_{i,j} = g(U^{(-j)}_{i,j}) \), in which the parameters of network \( g \) is fixed and optimized in advance using (4). Because \( g(V) \) is the correlated part of \( S \), our setting in fact minimize the correlation between \( S \) and \( V \).

The overall loss function for training \( f \) and \( z \) is:

\[
L_f = \frac{1}{n} \sum_{i=1}^{n} L_n(z(U_{i,i})) + L_{\text{decorr}}
\]

(6)

where \( L_n \) is the original image classification loss function, e.g., a Cross-Entropy loss function.

Based on (4) and (6), we develop the Partial Feature Decorrelation Learning (PFDL) algorithm for OOD image classification, shown in Algorithm. 1. The flow chart of the proposed PFDL algorithm has been shown in Figure. 2.

As shown in Figure. 2 and Algorithm. 1 for each mini-batch, we first train the feature decomposition network in 'Step 1' with the fixed feature extractor using (4). We then train the feature extractor and classifier in 'Step 2' with the fixed feature decomposition network using (6).

a) Connections to Causal Inference: Causal effect decomposition methods \[36, 38\] shed some lights on our model. The causal effect decomposition method is intended to partition observed associations among variables into direct and indirect effects when independent relationships exist \[38\]. By doing so, one can better analyze the direct effects of treatment features on the outcome. In fact, the direct and indirect effects are connected to the independent and correlated parts in our feature decomposition network.

b) Connections to Information Theory: From \[39\], we know that two random vectors \( X \) and \( Y \) with values over the space \( X \times Y \) are independent if and only if the mutual information between \( X \) and \( Y \) is equal to 0. In fact, our motivation can also be interpreted as learning a discriminative feature representation by reducing the mutual information between the independent part features and other features.

Algorithm 1 Partial Feature Decorrelation Learning

Input: Training set \( D_{\text{train}} = \{(x_i, y_i)\}_{i=1}^{n} \), maximum epoch number \( E \), initialized feature extractor \( f^{(0)} \), classifier \( z^{(0)} \) and feature decomposition network \( g^{(0)} \)

Output: Optimized \( f, z \)

1: \( t = 0 \)
2: for \( e \) in range(0, \( E \)) do
3: repeat
4: Sample mini-batch \( \{x, y\}_t \) from \( D_{\text{train}} \)
5: Calculate \( L_g \) using (4) with \( (g^{(t)}, f^{(t)}, \{x, y\}_t) \)
6: Update \( g^{(t+1)} \) with a stochastic gradient descent optimizer by fixing \( f^{(t)} \)
7: Calculate \( L_{fz} \) using (6) with \( (g^{(t+1)}, f^{(t)}, z^{(t)}, \{x, y\}_t) \)
8: Update \( f^{(t+1)}, z^{(t+1)} \) with a stochastic gradient descent optimizer by fixing \( g^{(t+1)} \)
9: \( t = t + 1 \)
10: until \( D_{\text{train}} \) has been traversed
11: end for
12: return \( f^{(t)} \) and \( z^{(t)} \)

IV. EXPERIMENTS

We evaluate the proposed PFDL algorithm in terms of the model performance quantitatively and qualitatively. We first introduce the datasets and evaluation metrics. We verify the correlation modeling ability of the proposed Feature Decomposition Network on a synthetic OOD prediction dataset MMADS \[25\] compared with several baseline methods and a state-of-the-art stable learning method \[25\]. We then demonstrate the effectiveness of PFDL on a OOD image classification dataset NICO \[11\], comparing it with several baseline and state-of-the-art methods.

A. Datasets

a) MMADS: This synthetic dataset is to mimic the agnost distribution shift problem in which part of the causality is
omitted due to the data generation bias, resulting in a statistical correlation between features. The task on this dataset is to predict the ground-truth using the input features. Given a input feature vector $X = [S^T; V^T]^T$ (where $X \in \mathbb{R}^r$, $S \in \mathbb{R}^{p_S}$, $V \in \mathbb{R}^v$, and $p = p_s + p_v$) and the ground-truth $Y \in \mathbb{R}^1$, the stable feature $S$ has real causality with the ground-truth $Y$, and correlation feature $V$ does not. Following the setting used by the state-of-the-art stable learning method DWR [25], we mimic three kinds of relationship between $S$ and $V$, including independent (S.L.V), ‘V depends on S’ (S → V) and ‘S depends on V’ (S ← V).

S.L.V: In this setting, $S$ and $V$ are independent, but $S, V$ could be dependent with each other. Hence, we generate $X = \{S_1, \ldots, S_{p_S}, V_1, \ldots, V_{p_v}\}$ with independent Gaussian distributions with the help of auxiliary variables $Z$ as following:

$$Z_{i,1}, \ldots, Z_{i,p_s} \sim \mathcal{N}(0, 1); V_{1,1}, \ldots, V_{p_v} \sim \mathcal{N}(0, 1)$$ (7)

$$S_{i} = 0.8 * Z_{i,1} + 0.2 * Z_{i,2}, i = 1, 2, \ldots, p_s$$ (8)

where the number of stable variables $p_s = 0.5 * p$ and the number of unstable variables $p_v = 0.5 * p$. $S_j$ represents the $j$-th variable in $S$.

$S \rightarrow V$: In this setting, the stable features $S$ are the causes of the unstable features $V$. We first generate dependent stable features $S$ with Eq. (8). Then, we generate unstable features $V$ based on $S$: $V_{j} = 0.8 * S_{j} + 0.2 * S_{j+1} + \mathcal{N}(0, 1)$, where we let $j + 1 = \text{mod}(j + 1, p_s)$. The function $\text{mod}(a, b)$ returns the modulus after division of $a$ by $b$.

$S \leftarrow V$: In this setting, unstable features $V$ are the causes of stable features $S$. We first generate the unstable features $V$ with Eq. (7). Then, we generate the stable features $S$ based on $V$: $S_{j} = 0.2 * V_{j} + 0.8 * V_{j+1} + \mathcal{N}(0, 1)$, where we let $j + 1 = \text{mod}(j + 1, p_v)$.

The relationship among $S$, $V$ and $Y$ has the form: $Y_{\text{poly}} = [S, V] \cdot [\beta_S, \beta_V]^T + S_1 S_2 S_3 + \epsilon$, where $Y_{\text{poly}}$ denotes the ground-truth generated from a polynomial nonlinear function, $\beta_S = \{\frac{1}{2}, -\frac{3}{2}, 1, -\frac{1}{2}, \frac{1}{2}, -1, \ldots\}$, $\beta_V = 0$ and $\epsilon = \mathcal{N}(0, 0.3)$.

To mimic the OOD generalization settings, we generate a set of environments, each with a distinct joint distribution $P^e(X, Y)$ while preserving $P(Y|S)$ as the same. To achieve that, we generate environments by varying $P^e(V_b|S)$ on a subset $V_b \in V$. Following the setting used by DWR [25], we vary $P^e(V_b|S)$ via biased sample selection with a bias rate $r \in [-3, -1] \cup [1, 3]$. For each sample, the probability of being selected is defined as $P^e_r = \prod_{V \in V_b} \left| P^e \right|^{-5r}$, where $D_i = |f(S) - \text{sign}(r) * V_i|$. If $r > 0$, $\text{sign}(r) = 1$, otherwise $\text{sign}(r) = -1$.

In this paper, we choose the number of sample size $n$ from $\{1000, 2000, 4000\}$, the feature dimension $p$ from $\{10, 20, 40\}$ and the bias rate from $\{1.5, 1.7, 2.0\}$. The details of the discussion and results are given in Sec. IV.C.

b) NICO: NICO [11] dataset is a OOD image classification dataset, which contains 25,000 images obtained from the Internet. NICO contains two superclasses: Animal and Vehicle, with 10 classes for Animal and 9 classes for the Vehicle. Specifically, there are 9 or 10 contexts in each class, and each image has been manually annotated in its context. The average size of classes is about 1300 images.

We evaluate our model on the NICO dataset using the Animal superclass. We used the proportional bias setting used by previous work [11], in which all contexts are used on both training and testing sets, but the percentage of each context is different on training and testing sets. Particularly, one context of each class will be randomly selected as the dominant context for both training and testing, and the rest is considered the minor contexts. The dominant ratio $r_d$ is defined as $\text{Dominant ratio} = N_{\text{dominant}} / N_{\text{minor}}$ where $N_{\text{dominant}}$ refers to the sample size of the dominant context and $N_{\text{minor}}$ refers to the average size of other contexts where we uniformly sample other contexts.

c) Colored-MNIST: This dataset is a synthetic dataset formed by coloring each image either red or green in a way that correlates strongly (but spuriously) with the class label. We followed the experiment setting of state-of-the-art work IRM [29].

B. Evaluation Metrics

a) MMADS: We use coefficient estimation error $\hat{\beta}_\text{error}$ to evaluate the correlation modeling ability of the feature decomposition network. The $\beta_\text{error}$ between the learned coefficient $\beta$ and the true coefficient $\beta$ is defined as $\beta_\text{error} = \frac{1}{p} \left| \beta - \beta \right|$, where $p$ is the feature dimension of $\beta$. We report both mean and variance of $\beta_\text{error}$ of five independent experiments. Moreover, we use RMSE, Average Error (AE) [25] and Stability Error (SE) [25] to evaluate stability of our model.

b) NICO and Colored-MNIST: Following [11], [29], we use accuracy to evaluate the classification ability in both NICO and Colored-MNIST datasets.

C. Experiments on MMADS Dataset

We first use the synthetic dataset MMADS to quantitatively and qualitatively evaluate the decorrelation ability of our model since all correlations are manually controlled. To mimic the OOD generalization scenario, we use different probability $P(V_b|S)$ on a subset $V_b \in V$ for training and testing environment to create correlations between $V$ and the ground-truth $Y$ while simulating the agnostic distribution shift between training and testing. By doing so, we can use the coefficient estimation error on correlation features $V$ as a quantitative index to evaluate how our method models correlations. We also use Average Error (AE) and Stability Error (SE) to evaluate the stability improvement provided by our method.

a) Compared Methods: We use four methods as baseline methods on the MMADS dataset, including the state-of-the-art stable learning method DWR [25] and three IID-based machine learning baseline methods OLS [40], Lasso [41], and Ridge Regression [42]. We used the official implementation of DWR provided by the authors.

b) Implementation: All models are trained on the same training dataset generated using a specific bias rate $r_{\text{train}}$. We repeat this training process five times with different $r_{\text{train}}$ and report the mean and variance of $\beta_\text{error}$ on $V$, since
the $V$ is correlation features correlated with $Y$ due to data generation bias. To evaluate the prediction stability, we test all models on several test environments with various bias rates $r_{test} \in [-3, -1) \cup (1, 3]$. For each test bias rate, five different test datasets are generated. To verify the correlation modeling ability of our method, we directly use the output of the feature decomposition network as auxiliary features, feed it into the coefficient estimator (same as DWR) to fit the biased training data, and then evaluate the coefficient estimator error.

For DWR, we used the hyper-parameters provided in their official implementation. The learning rate of DWR is 0.005, and the maximum iteration is 5000. As for the hyper-parameters of PFDL, the learning rate is 0.001, and the maximum iteration is the same as DWR.

As for computing resources, all experiments on the MMADS dataset are completed with a MacBook Pro laptop without GPU acceleration. Each experiment on the MMADS dataset is completed in minutes, including the training and testing process.

c) Results: The experimental results are shown in Figure. 3 and Table. I. We visualized the results of three different correlation settings $S \perp V$, $S \leftarrow V$, $S \rightarrow V$. We can notice that our algorithm can achieve the lowest coefficient estimation error on $\beta_V$ compared with all baselines. It shows that our method can model the correlations between features accurately in all three different correlations settings. Similar evidence can be found in Table. I, where our method achieved the lowest $\beta_V$ error and SE in all experiments compared with all baselines, including state-of-the-art method DWR. Besides, we can notice that our method can significantly mitigate the model misspecification caused by correlations and improve the stability of the model across different test datasets by using...
the output of the feature decomposition network.

We can notice that the performance of our proposal is stable when the sample size changing, but the performance of the state-of-the-art method DWR is affected by the sample size when the sample size changing, but the performance of the state-of-the-art method DWR is affected by the sample size as shown in Table 1. It shows that our method is more robust when training with a small number of samples.

These observations lead to the conclusion that our proposal can achieve better stability across different test datasets than the state-of-the-art methods.

D. Experiments on NICO Dataset

We then demonstrate the effectiveness of our model on the real-world OOD image classification dataset NICO. As discussed above, we use the proportional bias setting to show the stability improvement brought by our model compared with several baseline methods.

a) Compared Methods: We compare our model with several state-of-the-art methods on NICO datasets, including CN, CN+BN, and CNBB [11]. Moreover, we reproduced the state-of-the-art stable learning method DWR on the NICO dataset. The results of CN, CN+BN, and CNBB models are reported by [11]. The backbone model CN is a typical ConvNet based neural network. The CN+BN denotes a typical CNN-based model with batch normalization. And the CNBB is the state-of-the-art method proposed by [11].

b) Implementation: We then randomly sample 60% images of each context of each class to form the training set and regard the rest as the testing set. In each class, we randomly sample a dominant context, and the rest becomes the minor contexts. For a dataset with Dominant Ratio = 1 : 5, we will sample five minor context images of each minor context while we sample one dominant context image, until either dominant or minor context image runs out. Moreover, the context information is not available to the model during the training stage.

In Table 1, all models are trained on the same training set with Dominant Ratio = 5 : 1, and tested on seven different testing sets with different Dominant Ratio.

As for hyper-parameters, the initial learning rate is 0.01 for all models and multiplied by 0.1 for every 80 epochs. All models are trained for 160 epochs.

As for computing resources, all experiments on the NICO dataset are completed with a single Tesla P100 GPU. Each experiment is completed in hours, including the training and testing process. The computing performance demonstrates that our model does not consume too much extra computing resources.

1) Results: Table 1 lists the OOD image classification performance on the NICO dataset. We can observe that PFDL deployed on a ResNet-50 [5] backbone achieves the best accuracy in all seven settings. We can notice that the accuracy of each model varies proportionally to the OOD generalization settings. Both our model and the baselines achieve the best performance in Dominant Ratio = 5 : 1, because all models are trained on the training set with Dominant Ratio = 5 : 1. Besides, we can notice that our model can significantly improve the classification accuracy in the most challenging settings. The smaller value in this table, the better. We use bold font to highlight the results of our model.

### TABLE I

| Scenario: varying sample size n | Methods | OLS | Lasso | Ridge | DWR | Ours |
|---------------------------------|---------|-----|-------|-------|-----|-----|
| n=1000,p=10,r=1.7               | OLS     | 0.097 | 0.099 | 0.099 | 0.066 | 0.027 |
|                                | Lasso   | 0.097 | 0.101 | 0.101 | 0.067 | 0.025 |
|                                | Ridge   | 0.097 | 0.101 | 0.101 | 0.067 | 0.025 |
|                                | DWR     | 0.097 | 0.101 | 0.101 | 0.067 | 0.025 |
|                                | Ours    | 0.097 | 0.101 | 0.101 | 0.067 | 0.025 |
| n=2000,p=10,r=1.7               | OLS     | 0.583 | 0.583 | 0.583 | 0.509 | 0.613 |
|                                | Lasso   | 0.583 | 0.617 | 0.583 | 0.509 | 0.613 |
|                                | Ridge   | 0.583 | 0.617 | 0.583 | 0.509 | 0.613 |
|                                | DWR     | 0.587 | 0.621 | 0.587 | 0.505 | 0.569 |
|                                | Ours    | 0.587 | 0.621 | 0.587 | 0.505 | 0.569 |
| n=4000,p=10,r=1.7               | OLS     | 0.254 | 0.254 | 0.254 | 0.103 | 0.093 |
|                                | Lasso   | 0.236 | 0.267 | 0.236 | 0.110 | 0.081 |
|                                | Ridge   | 0.236 | 0.267 | 0.236 | 0.110 | 0.081 |
|                                | DWR     | 0.236 | 0.267 | 0.236 | 0.110 | 0.081 |
|                                | Ours    | 0.236 | 0.267 | 0.236 | 0.110 | 0.081 |

### TABLE II

#### Results on NICO dataset. The evaluation metric is standard classification accuracy in percentage. Models are trained on the same training set with Dominant Ratio = 5 : 1. The symbol '-' denotes that the previous work has not implemented this setting. We added these settings to show a fine-grained evaluation.

| Dominant Ratio | 1 : 5 | 1 : 3 | 1 : 1 | 2 : 1 | 3 : 1 | 4 : 1 | 5 : 1 |
|----------------|------|------|------|------|------|------|------|
| DWR [25]       | 35.66| 35.61| 37.29| 40.37| 41.81| 43.08| 43.72|
| CN [11]        | 37.17| 37.80| 41.46| 42.50| 43.23|-|
| CN+BN [11]     | 38.70| 39.60| 41.64| 42.00| 43.85|-|
| CNBB [11]      | 39.06| 39.60| 42.12| 43.33| 44.15|-|
| PFDL (Ours)    | 41.31| 41.41| 43.70| 47.46| 46.80| 49.29| 50.87|

The smaller value in this table, the better. We use bold font to highlight the results of our model.
setting 1 : 5, demonstrating our model’s effectiveness.

E. Experiments on Colored-MNIST.

We then evaluate our model in the Colored-MNIST. The Colored-MNIST is a synthetic image classification dataset formed by coloring each image of the MNIST [1] dataset either red or green in a way that correlates strongly with the class label.

a) Compared Methods: We compared our method with an MLP based model trained by using standard Empirical Risk Minimization (ERM) scheme. We also compared it with the state-of-the-art stable learning method IRM [29].

b) Implementation: We used the same implementation settings as in IRM [29]. The IRM model is also an MLP based neural network. We generate two training sets and one testing set with different correlation ratios (same as IRM [29]). The init learning rate is 0.001 for all methods.

c) Results: Table III lists the image classification accuracy of all models. As we can notice, our model deployed in the IRM learning scheme can further improve the accuracy in test environments. It also demonstrates the effectiveness of our model.

V. Conclusion

In this work, we study the OOD image classification problem. We present a novel Partial Feature Decorrelation Learning (PFDL) algorithm to improve the backbone model’s stability by partially decorrelating features during training. Experiments on both synthetic and real-world datasets demonstrate that our method can help improve the stability of the backbone models and outperforms the state-of-the-art stable learning methods. We first verify the correlation modeling ability of our method on a synthetic dataset. We then demonstrate the effectiveness of our model on a OOD image classification dataset.

Broader Impact

Our model is a data pretreatment method that causes no explicit ethical problems. As for benefits, our method can help improve the model’s stability on unknown test datasets and reduce the data annotation costs for fine-tuning the model into new scenarios. It can be applied to most deep-learning-based and linear models in many application scenarios like quantitative financial analysis, social media, and time series-based forecasting tasks. Moreover, our method helps to leverage biases in the data. Thus the likely beneficiaries are companies that have business suffering the model misspecification problem. The consequence of the failure of the model is poor classification or regression performance. Our work may affect the interests of companies whose primary business is data annotations.

Acknowledgment

This work was supported in part by The National Key Research and Development Program of China (Grant Nos: 2018AAA0101400), in part by The National Nature Science Foundation of China (Grant Nos: 62036009, U1909203, 61936006, 62133013), in part by Innovation Capability Support Program of Shaanxi (Program No. 2021TD-05).

References

[1] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” Advances in neural information processing systems, vol. 25, pp. 1097–1105, 2012.

[3] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, “Going deeper with convolutions,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 1–9.

[4] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014.

[5] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770–778.

[6] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, “Imagenet: A large-scale hierarchical image database,” in 2009 IEEE conference on computer vision and pattern recognition. Ieee, 2009, pp. 248–255.

[7] A. Krizhevsky, G. Hinton et al., “Learning multiple layers of features from tiny images,” 2009.

[8] L. Deng, “The mnist database of handwritten digits for machine learning research [best of the web],” IEEE Signal Processing Magazine, vol. 29, no. 6, pp. 141–142, 2012.

[9] L. Fei-Fei, R. Fergus, and P. Perona, “Learning generative visual models from few training examples: An incremental bayesian approach tested on 101 object categories,” in 2004 conference on computer vision and pattern recognition workshop. Ieee, 2004, pp. 178–178.

[10] M. Everingham, S. A. Eslami, L. Van Gool, C. K. Williams, J. Winn, and A. Zisserman, “The pascal visual object classes challenge: A retrospective,” International journal of computer vision, vol. 111, no. 1, pp. 98–136, 2015.

[11] Y. He, Z. Shen, and P. Cui, “Towards non-iid image classification: A dataset and baselines,” Pattern Recognition, vol. 110, p. 107383, 2021.

[12] T. Hua, W. Wang, Z. Xue, S. Ren, Y. Wang, and H. Zhao, “On feature decorrelation in self-supervised learning,” in Proceedings of the IEEE/CVF International Conference on Computer Vision, 2021, pp. 9598–9608.

[13] X. Liu, L. Li, F. Liu, B. Hou, S. Yang, and L. Jiao, “Gafnet: Group attention fusion network for pan and ms image high-resolution classification,” IEEE Transactions on Cybernetics, 2021.

[14] X. Guo, B. Pan, D. Cai, and X. He, “Robust asymmetric bayesian adaptive matrix factorization,” in Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, 2017, pp. 1760–1766.

[15] X. Guo, Z. Jin, C. Chen, H. Nie, J. Huang, D. Cai, X. He, and X. Hua, “Discriminative-generative dual memory video anomaly detection,” arXiv preprint arXiv:2104.14430, 2021.

[16] X. Liu, L. Jiao, F. Liu, X. Hou, and D. Zhang, “Feature correlation analysis of two-branch convolutional networks for multi-source image classification,” in IGARSS 2020-2020 IEEE International Geoscience and Remote Sensing Symposium. IEEE, 2020, pp. 936–939.

[17] V. Nagarajan, A. Andressen, and B. Neyshabur, “Understanding the failure modes of out-of-distribution generalization,” arXiv preprint arXiv:2010.15773, 2020.

[18] S. M. Xie, A. Kumar, R. Jones, F. Khani, T. Ma, and P. Liang, “In-nout: Pre-training and self-training using auxiliary information for out-of-distribution robustness,” arXiv preprint arXiv:2012.04550, 2020.

[19] H. Bai, R. Sun, L. Hong, F. Zhou, N. Ye, J.-J. Ye, S.-H. G. Chan, and Z. Li, “Decaug: Out-of-distribution generalization via decomposed feature representation and semantic augmentation,” arXiv preprint arXiv:2012.09382, 2020.

[20] A. Torralba and A. A. Efros, “Unbiased look at dataset bias,” in Proceedings of the IEEE conference on computer vision and pattern recognition. IEEE, 2011, pp. 1521–1528.
Deng Cai is a professor in the State Key Lab of CAD&CG, College of Computer Science at Zhejiang University, China. He received a Ph.D. degree in computer science from the University of Illinois at Urbana Champaign in 2009. His research interests include machine learning, data mining, and information retrieval.

Xiaofei He received a B.S. degree in Computer Science from Zhejiang University, China, in 2000 and a Ph.D. degree in Computer Science from the University of Chicago, in 2005. He is a Professor in the State Key Lab of CAD&CG at Zhejiang University, China. Prior to joining Zhejiang University, he was a Research Scientist at Yahoo! Research Labs, Burbank, CA. His research interests include machine learning, information retrieval, and computer vision. He is a senior member of IEEE.

Xian-Sheng Hua (F'16) received the B.S. and Ph.D. degrees in applied mathematics from Peking University, Beijing, in 1996 and 2001, respectively. In 2001, he joined Microsoft Research Asia as a Researcher and has been a Senior Researcher of Microsoft Research Redmond since 2013. He became a Researcher and the Senior Director of the Alibaba Group in 2015. He has authored or co-authored over 250 research papers and has filed over 90 patents. His research interests include multimedia search, advertising, understanding and mining, pattern recognition, and machine learning. He was honored as one of the recipients of MIT35. He served as a Program Co-Chair for the IEEE ICME 2013, the ACM Multimedia 2012, the IEEE ICME 2012, and on the Technical Directions Board of the IEEE Signal Processing Society. He is an ACM Distinguished Scientist and IEEE Fellow.