Decorr: Environment Partitioning for Invariant Learning and OOD Generalization

Yufan Liao, Qi Wu, Zhaodi Wu, and Xing Yan

Abstract—Invariant learning methods, aimed at identifying a consistent predictor across multiple environments, are gaining prominence in out-of-distribution (OOD) generalization. Yet, when environments aren’t inherent in the data, practitioners must define them manually. This environment partitioning—algorithmically segmenting the training dataset into environments—crucially affects invariant learning’s efficacy but remains underdiscussed. Proper environment partitioning could broaden the applicability of invariant learning and enhance its performance. In this paper, we suggest partitioning the dataset into several environments by isolating low-correlation data subsets. Through experiments with synthetic and real data, our Decorr method demonstrates superior performance in combination with invariant learning. Decorr mitigates the issue of spurious correlations, aids in identifying stable predictors, and broadens the applicability of invariant learning methods.

Index Terms—OOD generalization, IRM, environment partitioning, decorrelation.

I. INTRODUCTION

MACHINE learning methods have made significant strides in image classification, speech recognition, machine translation, and other domains. However, these methods typically assume that the training and testing data are independently and identically distributed (i.i.d.), an assumption that may not hold in real-world applications like autopilot, healthcare, and financial prediction. The reliance on this assumption makes using these models risky in such critical applications, as the performance of the reference model [13], [14]. Another straightforward approach to partitioning is clustering. Works by Matsuura et al. [15], Sohoni et al. [10], and Thopalli et al. [16] have utilized conventional clustering techniques like k-means to divide the dataset based on feature space, while Liu et al. [17] sought to maximize the diversity of the output distribution $P(Y|\Phi(X))$ through clustering.

Although training and testing sets are not i.i.d. in the OOD setting, they should share certain common properties that aid in generalization. A widely recognized OOD assumption addressing covariate shift posits that $P_{\text{train}}(Y|X) = P_{\text{test}}(Y|X)$ [1], suggesting that the outcome distribution remains consistent across training and testing sets given $X$. Building on this premise, it follows that the environment label $e_X$, whether based on $X$ or features extracted as $\Phi(X)$, should be independent of the outcome $Y$. This foundational assumption enables us to address discrepancies between training and testing environments effectively.

However, most environment partitioning methods utilize the outcome $Y$ for segmentation. This approach is less harmful in scenarios with a high signal-to-noise ratio, such as image data, where $X$ inherently encompasses most information about $Y$. However, in the presence of noisy data, such as tabular data, these methods may mistakenly assign similar or identical
features into different environments due to variations in $Y$. For instance, two data points with the same $X$ might end up in separate environments solely because the error components (irreducible and purely stochastic) in their $Y$ values differ. This leads to disparate conditional distributions of the outcome across environments, violating the covariate shift assumption. The efficacy of these methods in high-noise contexts remains largely unexplored. While $k$-means clustering does not depend on $Y$, relying solely on the feature space, it is not supported by a clear interpretation or theoretical justification for its application in this context.

This paper explores an environment partitioning method tailored for high-noise data to enhance the OOD generalization performance of IRM. We observe that models trained on datasets with uncorrelated features generally perform well against correlation shifts. IRM specifically seeks to develop an invariant predictor that excels across various environments. Inspired by these observations, we introduce Decorr, a method designed to identify subsets of features with low correlation for environment partitioning. Decorr is computationally efficient and independent of the outcome $Y$. Through experiments with both synthetic and real data, we demonstrate that Decorr, in conjunction with IRM, consistently outperforms in OOD scenarios we established, whereas some existing partitioning methods paired with IRM yield poor, sometimes worse-than-ERM, results.

To summarize, in this paper, our contributions are:

1) We introduce Decorr, a method that manually partitions the dataset into environments to enhance OOD generalization in combination with invariant learning. Decorr identifies subsets characterized by features with low correlations, which mitigates the issue of spurious correlations and aids in identifying stable predictors.
2) We demonstrate through simulation studies that Decorrelation-based invariant learning can achieve good OOD generalization even under model misspecification.
3) The proposed Decorr method demonstrates superior performance across a diverse range of datasets, including both tabular and image types.
4) We broaden the applicability of invariant learning methods (IRM, REx, etc.) when natural environment partitions are unknown. We improve the performance of invariant learning when the natural environment partitions are suboptimal.

II. BACKGROUND

A. Invariant Risk Minimization

IRM [4] works with datasets $D_e = \{(x^e_i, y^e_i)\}$ sourced from multiple training environments $e \in \mathcal{E}_{tr}$, aiming to develop a model that excels across an extensive range of environments $\mathcal{E}_{all}$, where $\mathcal{E}_{tr} \subseteq \mathcal{E}_{all}$. The objective is to minimize the worst-case risk $R^{\text{ood}}(f) = \max_{e \in \mathcal{E}_{all}} R^{e}(f)$, with $R^{e}(f) = \mathbb{E}_e[(f(x), y)]$ representing the risk within environment $e$. Specifically, IRM seeks to identify a data representation $\Phi$ and a classifier $w$ that remains optimal across all training environments $\mathcal{E}_{tr}$ when using the representation $\Phi$. This challenge is framed as a constrained optimization problem:

$$
\min_{w, \Phi} \sum_{e \in \mathcal{E}_{tr}} R^{e}(w \circ \Phi),
\text{subject to } w \in \arg \min_{\tilde{w}} R^{e}(\tilde{w} \circ \Phi), \text{ for all } e \in \mathcal{E}_{tr}.
$$

To make the problem solvable, the practical version IRMv1 is expressed as

$$
\min_{f} \sum_{e \in \mathcal{E}_{tr}} R^{e}(f) + \lambda \|\nabla_{w_{[w=1]}R^{e}(w \cdot f)}\|^2,
$$

where $f$ indicates the entire invariant predictor, and $w = 1$ is a fixed dummy scalar. The gradient norm penalty can be interpreted as the invariance of the predictor $f$.

Another approach to invariant learning is Risk Extrapolation (REx) [18], which aims to reduce training risks while increasing the similarity of training risks across environments. Variance-REx (V-REx) adds a penalty term—the variance of training losses across all training environments—to the traditional empirical risk minimization. It has been shown that this method can perform robustly in the presence of covariate shift.

B. Environment Partitioning Methods

To our best knowledge, literature predominantly features two types of partitioning methods. Clustering methods for environment partitioning are discussed in [10], [15], [16]. The general approach involves extracting features from the data and then clustering the samples based on these features into multiple groups, with all proposed methods employing $k$-means for clustering. Conversely, EIL [11] introduces an adversarial approach that partitions data into two environments designed to maximize the IRM penalty using an ERM model. Specifically, the environment inference step seeks to optimize a probability distribution $q_i(e') := q(e'|x_i, y_i)$ to enhance the IRMv1 regularizer $C^{\text{IRM}}(\Phi, q) = \|\nabla_{w_{[w=1]}R^{e}(w \circ \Phi, q)}\|$, where $R^{e}$ represents the $q$-weighted risk. After identifying the optimal $q^*$, environments are assigned by placing data into one environment based on $q^*$, with the rest allocated to another environment.

C. Some Other Related Works

1) Feature Decorrelation: The use of correlation for feature selection is well-established in machine learning [19]–[22]. More recently, the decorrelation method has been adapted for stable learning and OOD generalization. [23] suggested decorrelating features by learning weights for training samples. [24] initially clustered variables based on the stability of their correlations, then proceeded to decorrelate pairs of variables from different clusters. [25] focused on simultaneously optimizing regression coefficients and sample weights to manage correlation. However, to our knowledge, discussions on using decorrelation for dataset partitioning to enhance invariant learning are lacking, which is the main focus of the subsequent sections in our study.
2) Covariate Shift: Covariate shift has been a significant challenge in machine learning long before the advent of OOD generalization and invariant learning. Earlier research on covariate shift focused on adaptively training a predictor using the training dataset, sometimes incorporating an unlabeled testing dataset or known test-train density ratios, but without employing multiple training sets or environment partitions. Under such conditions, Importance Weighting (IW) has proven to be an effective strategy for addressing covariate shift [26–31]. In contrast, the contexts of OOD generalization and invariant learning typically require environment partitions and do not involve any pre-knowledge of the testing set. For further insights, theories, and methodologies related to covariate shift in machine learning, please refer to [32, 33].

### III. The Proposed Method

The IRM objective outlined in Eqn. (1) seeks to minimize risk across a set of environments \( \mathcal{E}_r \), while imposing an invariant constraint on the weights \( w \). IRM operates under the assumption that the environment partition is pre-established. However, in real-world scenarios, the data can be divided into environments in numerous ways. For instance, such partitioning could be based on personal characteristics like gender, age, or education level when predicting income from personal data, or it might depend on the timing of data collection. These partitioning strategies may be subject to scrutiny. Often in practice, we are either presented with a single training dataset without a clear environment partition or handed a potentially inadequate predetermined partition. Consequently, it becomes essential to manually select an environment partition that is effective for invariant learning methods to maximize the OOD performance of the model.

In this section, we explore how to identify a subset of data \( \tilde{X} \subset X \) characterized by low correlation, making it ideal for IRM learning. Given a data matrix \( X_{n \times p} \), we denote its correlation matrix by \( R_X = (r_{ij})_{p \times p} \). The deviation of \( R_X \) from the identity matrix \( I \) is assessed using the squared Frobenius distance \( d^2(R_X, I) = \sum_{i,j=1}^{p} (r_{ij} - \delta_{ij})^2 \), which serves as a measurement of how uncorrelated \( X \) is. The formulation of our goal is as follows:

\[
\min_{X \subset \tilde{X}} d^2(R_X, I),
\]

subject to some constraints on the size of \( \tilde{X} \). Given the large feasible set and the complexity of the optimization, we approach it by minimizing a softer alternative that transforms the subset selection into an optimization of sample weights. Using a weight vector \( w_{n \times 1} \) for the observations in \( X \), the weighted correlation matrix \( R^w_X = (r^w_{ij}) \) is computed as described in [34]. The correlation minimization problem can thus be reformulated as

\[
\min_{w \in [0, 1]^n} d^2(R^w_X, I), \quad \text{with constraints on } w,
\]

which is amenable to optimization. Here, the \( i \)-th element of \( w \) represents the probability that the \( i \)-th data point is included in the new environment \( \tilde{X} \) from the entire set \( X \). Restricting \( w \) to \( \{0, 1\}^n \) causes \( \tilde{X} \) to revert to the original hard problem (3).

#### Algorithm 1: The Decorr Algorithm

**Input:** training set \( X = \{x_i\}_{i=1}^n \), number of desired environments \( k \), restriction parameter \( p_0 \), learning rate \( \alpha \), number of epochs \( T \), and \( \lambda \) (suggested to be 100)

**Output:** the partitioned environments \( \bigcup_{j=1}^k X_j = X \)

**Initialization:** the residual set \( X_r = X \)

1. for \( j = 1, 2, \ldots, k - 1 \)
2. Re-denote \( X_r = \{x_i\}_{i=1}^n \) and randomly initialize \( w_i \sim \text{Uniform}([p_0, 1]), \ i = 1, 2, \ldots, |X_r| \)
3. Let \( t = 0 \)
4. while not converged and \( t < T \)
5. \[ L(w) = d^2(R^w_X, I) + \lambda \left( \frac{1}{|X_r|} \right) \left( 1 - \frac{T}{T+1} \right)^2 \]
6. \( w \leftarrow w - \alpha \frac{\partial L(w)}{\partial w} \)
7. \( t \leftarrow t + 1 \)
8. end while
9. Let \( x_i \in X_j \) with probability \( w_i \), for \( i = 1, 2, \ldots, |X_r| \)
10. \( X_r \leftarrow X_r - X_j \)
11. end for
12. \( X_k \leftarrow X_r \)

The specified target poses convergence challenges without constraints on \( w \). To address this, we propose two restrictions. First, considering \( k \) as the number of desired environments, we limit the mean of the weights with \( \frac{1}{n} \sum_{i=1}^{n} w_i = \frac{k}{k} \). This constraint prevents the predominance of excessively small values in \( w \), which could lead to a small sample size and high variance within the partitioned environments. We enforce this by incorporating a penalty term \( \lambda \left( \frac{1}{n} \sum_{i=1}^{n} w_i - \frac{k}{k} \right)^2 \) into the objective. Additionally, we constrain \( w_i \in [p_0, 1] \) where \( p_0 \) is a minimal value near zero—rather than \( w_i \in [0, 1] \). This adjustment not only facilitates the optimization’s convergence but also guarantees that all data points in the training set are eligible for inclusion in the partitioned set, allowing the model trained on this set to adapt to the entire distribution of observations rather than a confined segment. This approach also balances the trade-off between diversity shift and correlation shift [35].

To partition the training dataset into environments such that \( \bigcup_{j=1}^{k} X_j = X \), we iteratively optimize the objective specified in Eqn. (4) with respect to the residual sample set, selecting samples to establish each new environment sequentially. We detail this procedure in Algorithm 1. Once the environments are delineated, we employ IRM as the learning strategy to enhance OOD generalization.

To explore the impact of various environment partitioning strategies, we applied EIIl, \( k \)-means, and Decorr to a two-dimensional toy dataset where \( x_0 \) and \( x_1 \) exhibit positive correlation, and \( y \) is the sum of \( x_0 \) and an error term. The resulting partitions are illustrated in Fig. 1. The EIIl partition shows no clear patterns, suggesting a strong dependence on the label \( y \) and deviating from expected environmental separations. Both \( k \)-means and Decorr reveal spatial characteristics. Decorr divides the dataset into environments characterized by distinct covariate relationships: one positively correlated (triangle) and one almost uncorrelated (circle). While \( k \)-means also
bifurcates the data spatially, the divisions it creates feature similar covariate properties with only a mean shift.

A. OOD Generalization under Model Misspecification

In addition to our earlier discussions, we design an experiment to demonstrate that our method can achieve OOD generalization even when the models are misspecified. We adhere to most data-generating configurations and settings as described in [25]. We denote $S \in \mathbb{R}^{p_x \times 1}$ as the invariant features and $V \in \mathbb{R}^{p_x \times 1}$ as the spurious features, and $n$ is the sample size. The data are generated according to the model outlined below:

$$S_j \overset{i.i.d}{\sim} \mathcal{N}(0, 1), \quad j = 1, \ldots, p_s,$$

$$V_k \overset{i.i.d}{\sim} \mathcal{N}(0, 1), \quad k = 1, \ldots, p_v,$$

$$Y = S^T \beta + f(S) + \varepsilon,$$

where $\varepsilon \sim \mathcal{N}(0, 1)$ and $f(S)$ is a nonlinear term. We define $f(S) = S_1 S_2 S_3$ or $f(S) = \varepsilon S_1 S_2 S_3$, even though $p_v$ may exceed 3. The coefficient vector $\beta = [\frac{1}{3}, -\frac{2}{3}, 1, -\frac{1}{3}, \frac{2}{3}, -1, \ldots]^T$ cycles through these six values, truncated to fit $p_s$ dimensions. Here, a straightforward $p_v = p_v = 5$ is set by us.

To create training and testing sets with selection bias, we first produce original samples using the aforementioned method, then allocate each sample to the set based on the target variables $S$. A $r > 1$ results in a positive correlation between $V$ and $Y$, while $r < -1$ leads to a negative correlation. Nonetheless, the generation of $Y$ is independent of $V$, thereby introducing a spurious correlation through selection bias. In our experiment, $n_{\text{train}} = 2$ with 20,000 samples in the training set, and $n_{\text{test}} = -2$ with 10,000 samples in the testing set.

We employ linear regression of $Y$ against $(S, V)$ as the base model to fit the synthetic data. We compare Decorr against other environment partitioning strategies (pure random and $k$-means), combined with two different invariant learning algorithms (IRM and V-REx [18]). Additionally, we include ERM (Empirical Risk Minimization) and Decorr+ERM, the latter of which applies ERM to the first environment divided by Decorr, as baselines. To assess each model’s generalization capability, we use $\frac{1}{p_v} ||\hat{\beta}_v||_1$, the $L_1$ norm of the coefficient on $V$, which should ideally be zero for an optimal model, and the Mean Squared Error (MSE) in the testing set. The experimental results for two types of $f(S)$ are presented in Table I and II respectively. The results indicate that Decorr achieves superior performance on environment partitioning relative to other methods, meanwhile underscoring the importance of using invariant learning approaches, as evidenced by the baseline performance of ERM and Decorr+ERM. The $L_1$ norm of the coefficient on $V$ and the MSE for the testing set are significantly reduced when using Decorr+ERM or Decorr+REx.

### IV. Experiments

We assess four distinct environment partitioning methods: pure random, EII [11], $k$-means, and Decorr, along with the complete procedure of Heterogeneous Risk Minimization (HRM, [17]) in some experiments. Additionally, we deploy the original IRM (and V-Rex [18] exclusively in real data experiments) where environments are pre-defined, and also employ ERM for comparative analysis. We utilize either the original or widely used implementations of IRM [11], EII [11] and

---

1. https://github.com/facebookresearch/InvarianceUnitTests
2. https://github.com/creager/eiil
Decorr+IRM, underscoring both the superiority of Decorr and the importance of invariant learning.

| Method         | $\frac{1}{p^2}||\hat{\beta}_c||_1$ | Testing Set MSE |
|---------------|--------------------------|-----------------|
| ERM           | 0.77 (0.03)              | 2.64 (0.16)     |
| Decor + ERM   | 0.78 (0.08)              | 2.60 (0.24)     |
| $k$-means + IRM | 0.58 (0.16)          | 2.00 (0.15)     |
| Random + IRM  | 0.70 (0.25)              | 2.12 (0.50)     |
| Decor + IRM   | 0.39 (0.25)              | 2.12 (0.36)     |
| $k$-means + REx | 0.72 (0.10)           | 2.41 (0.20)     |
| Random + REx  | 0.83 (0.10)              | 2.58 (0.19)     |
| Decor + REx   | 0.38 (0.18)              | 1.64 (0.08)     |

HRM

Across all experiments, we set parameters $p_0 = 0.1$, $\alpha = 0.1$, $T = 5000$, and $\lambda = 100$ for Decor, adjusting $k$ according to the specific requirements of each scenario. For instance, in synthetic data experiments, $k$ corresponds to the actual number of environments in the training data, ranging from 2 to 8, though in most cases, $k$ is either 2 or 3. Similarly, in related studies employing methods like EIIL, HRM, or $k$-means, the number of training environments typically ranges between 2 and 3.

Although this paper primarily does not target high signal-to-noise ratio data, we showcase the adaptability of Decor by applying it to two image datasets, CMNIST and Waterbirds, demonstrating its effectiveness across various dataset types. Feature extraction is conducted using a neural network before proceeding with the decorrelation process. Decor is applied to these extracted low-dimensional features (k-means is applied similarly). After partitioning the dataset, we continue to employ the original raw image data for IRM training.

### A. Synthetic Data Experiments

1) A Toy Example: Following [36], we consider a toy $d$-dimensional example generated by

$$x_1 \sim \mathcal{N}(0, (\sigma^c)^2 I),$$

$$\hat{y} \sim \mathcal{N}(W_{yx}x_1, (\sigma^e)^2 I),$$

$$x_2 \sim \mathcal{N}(W_{xy}\hat{y}, I),$$

where $x_1, \hat{y}, x_2 \in \mathbb{R}^d$. The task is to predict $y = 1_4^T \hat{y}$ given $x = (x_1, x_2)$. We can write $W_{xy}\hat{y} \sim \mathcal{N}(x_2, I)$ if we ignore the causal mechanics, hence using $x_2$ to predict $y$ has a fixed noise. Therefore, if $\sigma^c$ is small, the model will rely more on $x_1$ due to the lower noise in predicting $y$ using $x_1$. Conversely, if $\sigma^c$ is large, the model will rely more on $x_2$. For simplicity, we set $W_{xy} = W_{yx} = I$ and $\sigma^c = 0.1, 1.5, 2$ for three different environments. In each environment $e$, 1,000 samples are generated. The goal is for the model to learn the true causal relationship, $y = 1_4^T x_1 + \varepsilon$, rather than the spurious correlation between $x_2$ and $y$. Therefore, we assess the effectiveness of different environment partitioning strategies by calculating the Mean Squared Error (MSE) between the linear regression coefficients and the ground-truth coefficients $\beta^* = (1_d, 0_d)$.

Data from original environments are combined, followed by the application of environment partitioning strategies to achieve the same number of environments, and then the application of IRM. We consider scenarios featuring varying numbers of original environments (2 or 3, corresponding to the first two $\sigma^e$ or all three) and different data dimensions $d = 2, 5, 10, 20$. The penalty weight in IRM is set as $\lambda = 10$. Results, derived from 10 trials to calculate the mean and the standard deviation, are displayed in Table III. In most instances, Decorr yields coefficients that are closest to $\beta^*$. Original IRM, when true environments are known (as indicated in the last row), reliably generates the true coefficients.

2) Risks of IRM: Next, we consider another example in [5], which is generated by

$$y = \begin{cases} 
1, & \text{with probability } \eta, \\
1, & \text{otherwise},
\end{cases}$$

and

$$z_c \sim \mathcal{N}(y \cdot \mu_c, \sigma_c^2 I),$$

$$z_e \sim \mathcal{N}(y \cdot \mu_e, \sigma_e^2 I),$$

$$x = f(z_c, z_e).$$

Assume data are drawn from $E$ training environments $E = \{e_1, e_2, \ldots, e_E\}$. For a given environment $e$, a data point is obtained by first randomly sampling a label $y$, then sampling invariant features $z_c \in \mathbb{R}^{d_c}$ and environmental features $z_e \in \mathbb{R}^{d_e}$. Finally, the observation $x$ is generated.

We let $E$ vary from 2 to 8, and for each case, we do training and testing 10 times to average the results. In each environment, we set $\eta = 0.5, \mu_c = Z_1 + 0.5 \text{sign}(Z_1), \mu_e = 1.5 Z_2 + Z_c, \sigma_c^2 = 2$, $\sigma_e^2 = 0.1$, where $Z_1 \in \mathbb{R}^3, Z_2 \in \mathbb{R}^6, Z_c \in \mathbb{R}^6, \forall e \in E$ are all sampled from standard normal. $Z_1$ and $Z_2$ are shared across environments and $Z_c$ is not. In each environment $e$, we sample 1,000 points. Again, data from original environments are combined, followed by the application of environment partitioning strategies (to obtain the same number of environments) and then IRM. In this experiment, we set $f$ as the identity function. After training a logistic classifier, we generate 5,000 different testing environments (each with a new $Z_c$ drawn from standard normal) to compute the worst-case prediction error rate. The penalty weight for IRM is $\lambda = 10^4$. Most hyper-parameters align with those in the study by [5]. The results, presented in Fig. 2, indicate that Decorr consistently yields a stable low error rate. This clearly demonstrates the superiority of Decorr.

### B. Real Data Experiments

1) Implementation Details: For each task, we utilize MLPs with two hidden layers featuring tanh activations and a dropout rate of $p = 0.5$ following each hidden layer. The size of each hidden layer is $2^{\text{int}(\log_2 p) + 2}$, where $p$ is the input dimension. The output layer is either linear or logistic. We employ Adam optimization [37] with default parameters (learning rate $= 0.001$, $\beta_1 = 0.9$, $\beta_2 = 0.999$, $\varepsilon = 10^{-8}$) to minimize binary cross-entropy loss for classification and MSE for regression.
TABLE III: A toy example generated by Eqn. (6). Our Decorr achieves the lowest MSE between linear regression coefficients and the ground-truth coefficients $\beta^* = (1_d, 0_d)$, in various scenarios featuring varying numbers of original/partitioned environments and different data dimensions. Standard deviations over 10 trials are included.

| Method          | Number of Environments = 2 |       | Number of Environments = 3 |       |
|-----------------|-----------------------------|-------|-----------------------------|-------|
|                 | $d = 2$                     | $d = 5$ | $d = 10$                    | $d = 20$ |
| ERM             | 0.28 (0.01)                 | 0.28 (0.02) | 0.28 (0.02)              | 0.46 (0.01) |
| Random + IRM    | 0.28 (0.06)                 | 0.27 (0.04) | 0.27 (0.02)              | 0.29 (0.02) |
| k-means + IRM   | 0.21 (0.05)                 | 0.27 (0.04) | 0.27 (0.03)              | 0.28 (0.02) |
| HRM             | 0.38 (0.17)                 | 0.43 (0.06) | 0.44 (0.04)              | 0.47 (0.02) |
| Decorr + IRM    | 0.13 (0.03)                 | 0.16 (0.09) | 0.16 (0.06)              | 0.19 (0.02) |
| IRM (Oracle)    | 0.02 (0.00)                 | 0.02 (0.01) | 0.02 (0.00)              | 0.02 (0.00) |

The training involves a maximum of 20,000 iterations and includes an $L_2$ penalty term weighted by 0.001. For IRM, the penalty weight is $\lambda = 10^4$. Except for occupancy estimation, all other experiments utilize $k = 2$ for Decorr and comparable methods, i.e., partitioning to create 2 environments. Unless otherwise specified, the original environment partitions for IRM and REx are determined based on the timestamps of the observations.

2) Financial Indicators: The task for the financial indicators dataset is to predict whether a stock’s price will increase over the following year based on the stock’s financial indicators. The dataset is divided into five annual segments from 2014 to 2018. Following the implementation details in [18], we treat each year as a baseline environment, utilizing three environments for training, one for validation through early stopping, and one for testing. This setup results in a total of 20 different tasks. Additionally, we compile another set of 20 tasks, each using a single environment for training, one for validation, and three for testing. In this configuration, the original IRM and REx are ineffective due to the presence of only one explicit training environment. Following [1], we assess all methods based on average error rate, worst-case error rate, and standard deviation across environments for each task set. The results, displayed in Table [V] indicate that Decorr achieves the best performance. The superiority of Decorr+IRM over pure IRM suggests that the original environment partitions, determined by the timestamps of observations, are suboptimal.

3) Adult: The Adult dataset is a tabular collection derived from a U.S. census, aimed at classifying whether an individual’s annual income exceeds or falls below 50,000 USD based on specific characteristics. We retain only race and sex as categorical variables, converting them into binary values $\{0, 1\}$. To introduce a distributional shift between training and testing data, we first identify either race or sex as the biased feature, denoted as $x^b$, and categorize the dataset into four groups: $\{x^b = 0, y = 0\}$, $\{x^b = 1, y = 1\}$, $\{x^b = 0, y = 1\}$, and $\{x^b = 1, y = 0\}$. For the training set, we use 90% of the data from the first two groups and only an $\alpha$ proportion from the last two groups, with the remainder allocated to the testing set. A lower $\alpha$ value increases the distributional shift, whereas an $\alpha$ of 0.9 results in no shift. We anticipate that IRM-based methods will learn the spurious correlation ($x^b = 1$ leads to $y = 1$) under small $\alpha$ values. The error rate results on the testing set are depicted in Fig. [3] and [4]. For pure IRM and REx, original environments are defined by the value of the biased feature.

4) Occupancy Estimation: The Occupancy Estimation dataset comprises data from various sensors (temperature, light, sound, CO2, etc.) recorded every minute in a room.

5) Stock: The Stock dataset comprises market data and technical indicators for 10 U.S. stocks from 2005 to 2020. We attempt to predict whether the closing price of a stock will be higher tomorrow than it is today using today’s technical indicators. For each stock, we allocate the first 70% of the data as the training set, 10% as the validation set for early stopping, and the final 20% as the testing set. The modeling is conducted on a per-stock basis. We assess methods based on average error rate, worst-case error rate, and standard deviation across different stocks. Results are presented in Table [VI] where Decorr once again yields the lowest testing error. For pure IRM and REx, original environments are determined by the collection times of the samples.

C. Image Data Experiments

To demonstrate the applicability of our method across diverse data types, we implement Decorr and other baseline methods on two image datasets. With minor adjustments to Decorr tailored to the specifics of image data, our method consistently outperforms the others. Unless specified otherwise,
TABLE IV: The experiment on the Financial Indicators dataset. There are five pre-determined original environments. Task set 1 utilizes three environments for training, while task set 2 uses one environment for training. Each task set comprises 20 tasks, with the average error rate, worst-case error rate, and standard deviation across these tasks reported.

| Method            | Task Set 1 | Task Set 2 |
|-------------------|------------|------------|
|                   | Average Error | Worst Error | STD | Average Error | Worst Error | STD |
| ERM               | 45.02 (0.00) | 52.92 (0.12) | 5.20 | 46.79 (0.01) | 51.05 (0.05) | 2.44 |
| Random + IRM      | 45.95 (0.28) | 53.77 (0.58) | 4.27 | 46.57 (0.26) | 52.03 (0.79) | 2.57 |
| EIIL              | 48.95 (0.16) | 57.37 (0.65) | 4.52 | 48.97 (0.38) | 54.62 (0.70) | 2.71 |
| k-means + IRM     | 45.20 (0.34) | 53.64 (0.44) | 6.19 | 46.79 (0.28) | 54.72 (1.22) | 3.43 |
| HRM               | 44.64 (0.00) | 53.52 (0.03) | 5.71 | 46.71 (0.00) | 51.17 (0.00) | 2.48 |
| Decorr + IRM      | 43.99 (0.10) | 51.61 (0.04) | 5.33 | 43.96 (0.25) | 50.23 (1.17) | 2.81 |

Fig. 2: The example of Risks of IRM.
Fig. 3: The Adult dataset: using race as the bias feature.
Fig. 4: The Adult dataset: using sex as the bias feature.

TABLE V: The Occupancy Estimation dataset.

| Method            | Training Error | Testing Error |
|-------------------|----------------|---------------|
| ERM               | 0.026 (0.000)  | 0.773 (0.000) |
| Random + IRM      | 0.587 (0.053)  | 0.824 (0.093) |
| EIIL              | 0.191 (0.203)  | 0.690 (0.048) |
| k-means + IRM     | 0.044 (0.001)  | 0.352 (0.009) |
| HRM               | 0.166 (0.000)  | 1.154 (0.000) |
| Decorr + IRM      | 0.143 (0.009)  | **0.268 (0.011)** |
| IRM               | 0.420 (0.006)  | 0.840 (0.021) |
| V-REx             | 0.060 (0.001)  | 0.686 (0.030) |

TABLE VI: The Stock dataset.

| Method            | Average Error | Worst-Case Error | STD |
|-------------------|---------------|------------------|-----|
| ERM               | 50.33 (0.10)  | 56.65 (0.26)     | 3.86|
| Random + IRM      | 50.11 (0.35)  | 54.54 (0.81)     | 2.62|
| EIIL              | 49.70 (0.33)  | **52.29 (0.44)** | **1.65** |
| k-means + IRM     | 50.02 (0.30)  | 54.92 (0.23)     | 2.68|
| HRM               | 50.22 (0.00)  | 55.97 (0.00)     | 4.78|
| Decorr + IRM      | 49.13 (0.34)  | 53.50 (0.75)     | 3.66|

the implementation details follow those outlined in Section IV-B.

Image data have much higher dimensions than tabular data, making direct decorrelation of raw image data impractical. We first need to extract features using a trained convolutional neural network, using the output from the last fully-connected layer as the data’s features. With these extracted low-dimensional features, we can proceed with decorrelation as before (we apply k-means in this manner as well). After partitioning the dataset, we continue to use the raw image data for IRM training. For Decorr, we do not enforce uniform sample sizes across partitioned environments (i.e., λ = 0 in Algorithm 1), allowing for more diversified environments in image datasets.

1) Colored MNIST: Colored MNIST (CMNIST), introduced by [4] to assess IRM’s capability to learn nonlinear invariant predictors, is an image dataset derived from MNIST. In CMNIST, each MNIST image is colored either red or green, creating a strong but spurious correlation between the image’s color and its class label. This correlation poses a challenge for regular deep learning models, which tend to classify images based on color rather than shape.

CMNIST is framed as a binary classification task, following the construction guidelines in [4]. Initially, images are assigned a preliminary label $\tilde{y} = 0$ for digits 0-4 and $\tilde{y} = 1$ for digits 5-9. The final label $y$ is then derived by flipping $\tilde{y}$ with a 0.1 probability, which introduces data noise. Subsequently, the color ID $z$ is sampled by flipping $y$ with a probability $p_e$, set at 0.2 for the first training environment and 0.1 for the second. In contrast, the test environment has a $p_e$ of 0.9, indicating a significant reversal in the correlation between color and label. The images are then colored according to their color ID $z$.

Figures 5 and 6 provide a visual representation of this setup.

Following [4], we employ an MLP with two hidden layers as our base model. The network architecture and all hyperparameters remain consistent. We assess the methods by
computing the error rate on the testing set. We also compute the percentage of data points exhibiting rare patterns (i.e., red images labeled 0-4 or green images labeled 5-9) within each partitioned environment. A significant discrepancy in percentages between two partitioned environments suggests greater diversity, which is potentially advantageous for invariant learning. Each model undergoes training for 5,000 epochs, with the initial 100 epochs proceeding without an IRM penalty. The outcomes, detailed in Table VII, demonstrate Decorr’s great superiority.

Table VII: The CMNIST experiment. Decorr achieves the lowest error rate on the testing set, compared to other baseline environment partitioning methods.

| Method       | Average Error | % of Rare Patterns |
|--------------|---------------|--------------------|
| ERM          | 43.33 (0.14)  | –                  |
| Random + IRM | 40.16 (0.16)  | 15.15 (0.08)       |
| k-means + IRM | 41.93 (0.52)  | 15.32 (0.21)       |
| Decorr + IRM | 34.89 (6.24)  | 40.24 (0.49)       |
| IRM          | 30.18 (0.94)  | 19.89 (0.13)       |
| V-REx        | 34.22 (0.04)  | 19.89 (0.13)       |

Fig. 5: CMNIST training set examples: most of 0-4 are green, and most of 5-9 are red.

Fig. 6: CMNIST testing set examples: most of 0-4 are red, and most of 5-9 are green.

D. Summary

In this section, we briefly summarize the characteristics of the tested methods. IRM performs exceptionally well when the environment partition aligns with the true data-generating mechanisms. However, this alignment is often not present in real datasets. We observe that the simple and natural split-by-time partition offers no significant advantage. k-means provides a straightforward approach to environment partitioning and consistently demonstrates good performance across multiple experiments. However, as illustrated in Fig. 4, k-means may not always be the optimal method for partitioning. Our Decorr algorithm consistently achieves the best performance in the experiments mentioned above. Notably, Decorr does not aim to reconstruct the original data sources; rather, it seeks to identify partitions that exceed the performance of the original or natural partitions.

Table VIII: The Waterbirds experiment. Decorr achieves the lowest error rate on the testing set, compared to other baseline environment partitioning methods.

| Method       | Average Error |
|--------------|---------------|
| ERM          | 25.76 (0.23)  |
| Random + IRM | 22.96 (0.43)  |
| k-means + IRM| 24.32 (0.65)  |
| Decorr + IRM | 22.70 (0.44)  |
| IRM          | 22.36 (0.08)  |
| V-REx        | 33.53 (7.84)  |

V. Conclusion

Invariant learning is a robust framework for Out-Of-Distribution (OOD) generalization, with environment partitioning playing a critical role in the effectiveness of IRM. Although existing partitioning methods perform well in some cases, their efficacy varies and they are not supported by a clear interpretation or justification. Inspired by the advantages of a low-correlated training set, we developed the Decorr algorithm, which partitions data into multiple environments with minimal internal correlation. We further provide explanations that uncorrelated environments enhance OOD generalization. Our partitioning approach offers distinct benefits over existing methods. Across various types of tasks, including image-based ones, we demonstrate that our method consistently and significantly enhances the performance of IRM, greatly broadening its applicability.

REFERENCES

[1] Z. Shen, J. Liu, Y. He, X. Zhang, R. Xu, H. Yu, and P. Cui, “Towards out-of-distribution generalization: A survey,” arXiv Preprint arXiv:2108.13624, 2021.

[2] K. Zhou, Z. Liu, Y. Qiao, T. Xiang, and C. C. Loy, “Domain generalization: A survey,” 2021.
[3] R. Geirhos, J.-H. Jacobsen, C. Michaelis, R. Zemel, W. Brendel, M. Bethge, and F. A. Wichmann, “Shortcut learning in deep neural networks,” *Nature Machine Intelligence*, vol. 2, no. 11, pp. 665–673, 2020.

[4] M. Arjovsky, L. Bottou, I. Gulrajani, and D. Lopez-Paz, “Invariant risk minimization,” *Stat.*, vol. 1050, p. 27, 2020.

[5] E. Rosenfeld, P. K. Ravikumar, and A. Risteski, “The risks of invariant risk minimization,” in *International Conference on Learning Representations*, 2020.

[6] F. Ahmed, Y. Bengio, H. van Seijen, and A. Courville, “Systematic generalisation with group invariant predictions,” in *International Conference on Learning Representations*, 2020.

[7] K. Ahuja, K. Shanmugam, K. Varshney, and A. Dharandar, “Invariant risk minimization games,” in *International Conference on Machine Learning*, PMLR, 2021, pp. 145–155.

[8] C. Lu, Y. Wu, J. M. Hernández-Lobato, and B. Schölkopf, “Nonlinear invariant risk minimization: A causal approach,” *arXiv Preprint arXiv:2102.12353*, 2021.

[9] P. Chattopadhyay, Y. Balaji, and J. Hoffman, “Learning to balance specificity and invariance for in and out of domain generalization,” in *European Conference on Computer Vision*. Springer, 2020, pp. 301–318.

[10] N. Sohoni, J. Dunnmon, G. Angus, A. Gu, and C. Ré, “No subclass left behind: Fine-grained robustness in coarse-grained classification problems,” *Advances in Neural Information Processing Systems*, vol. 33, pp. 19 339–19 352, 2020.

[11] E. Creager, J.-H. Jacobsen, and R. Zemel, “Environment inference for invariant learning,” in *International Conference on Machine Learning*, PMLR, 2021, pp. 2189–2200.

[12] E. Z. Liu, B. Haghgoo, A. S. Chen, A. Raghunathan, P. W. Koh, S. Sagawa, P. Liang, and C. Finn, “Just train twice: Improving group robustness without training group information,” in *International Conference on Machine Learning*, PMLR, 2021, pp. 6781–6792.

[13] J. Nam, H. Cha, S. Ahn, J. Lee, and J. Shin, “Learning from failure: De-biasing classifier from biased classifier,” *Advances in Neural Information Processing Systems*, vol. 33, pp. 20 673–20 684, 2020.

[14] N. Duaev, B. D. Roads, X. Lin, D. N. Barry, K. R. Patil, and B. C. Love, “A too-good-to-be-true prior to reduce shortcut reliance,” *Pattern Recognition Letters*, vol. 166, pp. 164–171, 2023.

[15] T. Matsuura and T. Harada, “Domain generalization using a mixture of multiple latent domains,” in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 07, 2020, pp. 11 749–11 756.

[16] K. Thopalli, S. Katoh, A. Spanias, P. Turaga, and J. J. Thiagarajan, “Improving multi-domain generalization through domain re-labeling,” *arXiv Preprint arXiv:2112.09802*, 2021.

[17] J. Liu, Z. Hu, P. Cui, B. Li, and Z. Shen, “Heterogeneous risk minimization,” in *International Conference on Machine Learning*. PMLR, 2021, pp. 6804–6814.

[18] D. Krueger, E. Caballero, J.-H. Jacobsen, A. Zhang, J. Binas, D. Zhang, R. Le Priol, and A. Courville, “Out-of-distribution generalization via risk extrapolation (rex),” in *International Conference on Machine Learning*, PMLR, 2021, pp. 5815–5826.

[19] M. A. Hall et al., “Correlation-based feature selection for machine learning,” 1999.

[20] L. Yu and H. Liu, “Feature selection for high-dimensional data: A fast correlation-based filter solution,” in *International Conference on Machine Learning*, 2003, pp. 856–863.

[21] M. A. Hall, “Correlation-based feature selection of discrete and numeric class machine learning,” 2000.

[22] E. C. Blesiss and E. Karthikeyan, “Signis: a feature selection algorithm using correlation based method,” *Journal of Algorithms & Computational Technology*, vol. 6, no. 3, pp. 385–394, 2012.

[23] X. Zhang, P. Cui, R. Xu, L. Zhou, Y. He, and Z. Shen, “Deep stable learning for out-of-distribution generalization,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 5372–5382.

[24] Z. Shen, P. Cui, J. Liu, T. Zhang, B. Li, and Z. Chen, “Stable learning via differentiated variate decorrelation,” in *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2020, pp. 2185–2193.

[25] S. Sickel, M. Brückner, and T. Scheffer, “Discriminating learning under covariate shift,” *Journal of Machine Learning Research*, vol. 10, no. 9, 2009.

[26] T. Fang, N. Lu, G. Niu, and M. Sugiyama, “Rethinking importance weighting for deep learning under distribution shift,” *Advances in Neural Information Processing Systems*, vol. 33, pp. 11 996–12 007, 2020.

[27] M. Sugiyama and M. Kawanabe, *Machine learning in non-stationary environments: Introduction to covariate shift adaptation*. MIT Press, 2012.

[28] J. Quiñonero-Candela, M. Sugiyama, A. Schwaighofer, and N. D. Lawrence, *Dataset shift in machine learning*. MIT Press, 2022.

[29] J. F. P. d. Costa, *Weighted Correlation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 1653–1655. [Online]. Available: https://doi.org/10.1007/978-3-642-04898-2_612

[30] S. Bickel, M. Brückner, and T. Scheffer, “Discriminative learning under model misspecification and agnostic distribution shift,” in *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2020, pp. 1485–1492.

[31] B. Aubin, A. Slowik, M. Arjovsky, L. Bottou, and D. Lopez-Paz, “Linear out-of-domain tests for invariance discovery,” *arXiv Preprint arXiv:2102.10897*, 2021.

[32] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” in *International Conference on Learning Representations*, 2015.

[33] S. Sagawa, P. W. Koh, T. B. Hashimoto, and P. Liang, “Distributionally robust neural networks,” in *International Conference on Learning Representations*, 2019.

[34] C. Wah, S. Branson, P. Welinder, P. Perona, and S. Belongie, “The caltech-ucsd birds-200-2011 dataset,” 2011.

[35] B. Zhou, A. Lapedriza, A. Khosla, A. Oliva, and A. Torralba, “Places: A 10 million image database for scene recognition,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 6, pp. 1452–1464, 2017.