Abstract

The ability to generalize under distributional shifts is essential to reliable machine learning, while models optimized with empirical risk minimization usually fail on non-i.i.d testing data. Recently, invariant learning methods for out-of-distribution (OOD) generalization propose to find causally invariant relationships with multi-environments. However, modern datasets are frequently multi-sourced without explicit source labels, rendering many invariant learning methods inapplicable. In this paper, we propose Kernelized Heterogeneous Risk Minimization (KerHRM) algorithm, which achieves both the latent heterogeneity exploration and invariant learning in kernel space, and then gives feedback to the original neural network by appointing invariant gradient direction. We theoretically justify our algorithm and empirically validate the effectiveness of our algorithm with extensive experiments.

1 Introduction

Traditional machine learning algorithms which optimize the empirical risk often suffer from poor generalization performance under distributional shifts caused by latent heterogeneity or selection biases that widely exist in real-world data[9,20]. How to guarantee a machine learning algorithm with good generalization ability on data drawn out-of-distribution is of paramount significance, especially in high-stake applications such as financial analysis, criminal justice and medical diagnosis, etc.[13,18], which is known as the out-of-distribution(OOD) generalization problem[1].

To ensure the OOD generalization ability, invariant learning methods assume the existence of the causally invariant correlations and exploit them through given environments, which makes their performances heavily dependent on the quality of environments. Further, the requirements for the environment labels are too strict to meet with, since real-world datasets are frequently assembled by merging data from multiple sources without explicit source labels. Recently, several works[5,15] to relax such restrictions have been proposed. Creager et al.[5] directly infer the environments according to a given biased model first and then performs invariant learning. But the two stages cannot be jointly optimized and the quality of inferred environments depends heavily on the pre-provided biased model. Further, for complicated data, using invariant representation for environment inference is harmful, since the environment-specific features are gradually discarded, causing the extinction of latent heterogeneity and rendering data from different latent environments undistinguishable. Liu et al.[15] design a mechanism where two interactive modules for environment inference and invariant learning respectively can promote each other. However, it can only deal with scenarios where invariant and variant features are decomposed on raw feature level, and will break down when the decomposition can only be performed in representation space(e.g., image data).

*Equal Contributions
†Corresponding Author

This paper focuses on the integration of latent heterogeneity exploration and invariant learning on representation level. In order to incorporate representation learning with theoretical guarantees, we introduce Neural Tangent Kernel (NTK) into our algorithm. According to NTK theory, training the neural network is equivalent to linear regression using Neural Tangent Features (NTF), which converts non-linear neural networks into linear regression in NTF space and makes the integration possible. Based on this, our Kernelized Heterogeneous Risk Minimization (KerHRM) algorithm is proposed, which synchronously optimizes the latent heterogeneity exploration module $\mathcal{M}_v$ and invariance learning module $\mathcal{M}_p$ in NTF space. Specifically, we propose our novel Invariant Gradient Descent (IGD) for $\mathcal{M}_p$, which performs invariant learning in NTF space and then feeds back to neural networks with appointed invariant gradient direction. For $\mathcal{M}_v$, we construct an orthogonal heterogeneity-aware kernel to capture the environment-specific features and to further accelerate the heterogeneity exploration. Theoretically, we demonstrate our heterogeneity exploration algorithm for $\mathcal{M}_v$ with rate-distortion theory and justify the orthogonality property of the built kernel, which jointly can illustrate the mutual promotion between the two modules. Empirically, experiments on both synthetic and real-world data validate the superiority of KerHRM in terms of good out-of-distribution generalization performance.

2 Preliminaries

Following [11], we consider data $D = \{D^e\}_{e \in \text{supp}(\mathcal{E}_{tr})}$ with different sources data $D^e = \{X^e, Y^e\}$ collected from multiple training environments $\mathcal{E}_{tr}$. Here environment labels are unavailable as in most of the real applications. $\mathcal{E}_{tr}$ is a random variable on indices of training environments and $P^e$ is the distribution of data and label in environment $e$. The goal of this work is to find a predictor $f(\cdot) : \mathcal{X} \rightarrow \mathcal{Y}$ with good out-of-distribution generalization performance, which is formalized as:

$$\arg \min_f \max_{e \in \text{supp}(\mathcal{E})} \mathcal{L}(f|e) \tag{1}$$

where $\mathcal{L}(f|e) = \mathbb{E}^e[\ell(X^e, Y^e)]$ represents the risk of predictor $f$ on environment $e$, and $\ell(\cdot, \cdot) : \mathcal{Y} \times \mathcal{Y} \rightarrow \mathbb{R}^+$ the loss function. Note that $\mathcal{E}$ is the random variable on indices of all possible environments such that $\text{supp}(\mathcal{E}_{tr}) \subset \text{supp}(\mathcal{E})$. Usually, for all $e \in \text{supp}(\mathcal{E}) \setminus \text{supp}(\mathcal{E}_{tr})$, the data and label distribution $P^e(X, Y)$ can be quite different from that of training environments $\mathcal{E}_{tr}$. Therefore, the problem in equation (1) is referred to as Out-of-Distribution (OOD) Generalization problem [11]. Since it is impossible to characterize the latent environments $\mathcal{E}$ without any prior knowledge or structural assumptions, the invariance assumption is proposed for invariant learning:

**Assumption 2.1.** There exists random variable $\Psi^*_S(X)$ such that the following properties hold:

- **a. Invariance property:** for all $e, e' \in \text{supp}(\mathcal{E})$, we have $P^e(Y|\Psi^*_S(X)) = P^{e'}(Y|\Psi^*_S(X))$ holds.
- **b. Sufficiency property:** $Y = f(\Psi^*_S) + \epsilon, \epsilon \perp X$.

This assumption indicates invariance and sufficiency for predicting the target $Y$ using $\Psi^*_S$, which is known as invariant representations with stable relationships with $Y$ across $\mathcal{E}$. To acquire such $\Psi^*_S$, a branch of works [4][11][15] proposes to find the maximal invariant predictor (MIP) of an invariance set, which are defined as follows:

**Definition 2.1.** The invariance set $\mathcal{I}_E$ with respect to $\mathcal{E}$ is defined as:

$$\mathcal{I}_E = \{\Psi_S(X) : Y \perp \!\!\!\perp \mathcal{E}|\Psi_S(X)\} = \{\Psi_S(X) : H[Y|\Psi_S(X)] = H[Y|\Psi_S(X), \mathcal{E}]\} \tag{2}$$

where $H[\cdot]$ is the Shannon entropy of a random variable. The corresponding maximal invariant predictor (MIP) of $\mathcal{I}_E$ is defined as $S = \arg \max_{\mathcal{E} \in \mathcal{E}_E} \mathbb{I}(Y; \Phi)$, where $\mathbb{I}(\cdot; \cdot)$ measures Shannon mutual information between two random variables.

Firstly, we propose that using the maximal invariant predictor $S$ of $\mathcal{I}_E$ can guarantee OOD optimality in Theorem 2.1. The formal statement is similar to [15] and can be found in Appendix A.3.

**Theorem 2.1.** (Optimality Guarantee, informal) For predictor $\Phi^*_S(X)$ satisfying Assumption 2.1, $\Psi^*_S$ is the maximal invariant predictor with respect to $\mathcal{E}$ and the solution to OOD problem in equation (1) is $\mathbb{E}_Y[Y|\Psi^*_S] = \arg \min_f \sup_{e \in \text{supp}(\mathcal{E})} \mathbb{E} \mathcal{L}(f|e)$.

However, recent works [4][11] on finding MIP solutions rely on the availability of data from multiple training environments $\mathcal{E}_{tr}$, which is hard to meet with in practice. Further, their validity is highly determined by the given $\mathcal{E}_{tr}$. Since $\mathcal{I}_E \subseteq \mathcal{I}_{E_{tr}}$, the invariance regularized by $\mathcal{E}_{tr}$ is often too large and the learned MIP may contain variant components and fails to generalize well. Based on this,
Algorithm 1 Kernelized Heterogeneous Risk Minimization (KerHRM) Algorithm

Input: Heterogeneous dataset $D = \{D^e = (X^e, Y^e)\}_{e \in E_{tr}}$

Initialization: MLP model $f_w(\cdot)$ with initial $w_0$, Neural Tangent Feature $\Phi(X) = \nabla_w f_w(X)$ (fixed in following), clustering kernel $\kappa_c^{(0)}(x_1, x_2) = \phi(x_1)^T \phi(x_2)$.

for $t = 1$ to $T$ do
1. Generate $E_{learn}^{(t)}$ with clustering kernel $\kappa_c^{(t-1)}$: $E_{learn}^{(t)} = M_c((\Phi(X), Y), \kappa^{(t-1)}_c)$
2. Learn invariant model parameters $\theta_{inv}^{(t)}$ with $E_{inv}$ in NTF space: $\theta_{inv}^{(t)} = M_p(E_{learn}^{(t)})$
3. Feedback to Neural Network $f_w(\cdot)$ with $\theta_{inv}^{(t)}$: $w_{inv}^{(t)} = \arg \min_w L(w; X, Y) + \text{Reg}(w; \theta_{inv}^{(t)})$
4. Update the clustering kernel $\kappa_c^{(t)}$ with $\theta_{inv}^{(t)}$: $\kappa_c^{(t)} \leftarrow \text{Orthogonal Transform}(\kappa_c^{(t-1)}, \theta_{inv}^{(t)})$
end for

**Problem 1. (Problem Setting)** Assume that $X = h(\Psi^{s}_S, \Psi^{s}_V) \in \mathbb{R}^d$, where $\Psi^{s}_S$ satisfies Assumption 2.1, $h(\cdot)$ is an unknown transformation function and $\Psi^{s}_V \perp \Psi^*_V$ (following functional representation lemma[2]), given heterogeneous dataset $D = \{D^e\}_{e \in E_{learn}(\text{ inv.})}$ without environment labels, the task is to generate environments $E_{learn}^{(t)}$ with minimal $|\mathcal{I}_{E_{learn}}|$ and meanwhile learn invariant models.

**3 Method**

**Remark.** Following the analysis in section 2 to generate environments $E_{learn}$ with minimal $|\mathcal{I}_{E_{learn}}|$ is equivalent to generate environments with as varying $P(Y|\Psi^*_V)$ as possible, so as to exclude variant parts $\Psi^*_V$ from the invariant set $\mathcal{I}_{E_{learn}}$.

In spite of such insight, the latent $\Psi^{s}_S, \Psi^*_V$ make it impossible to directly generate $E_{learn}$. In this work, we propose our Kernelized Heterogeneous Risk Minimization (KerHRM) algorithm with two interactive modules, the frontend $M_c$ for heterogeneity exploration and backend $M_p$ for invariant prediction. Specifically, given pooled data, the algorithm starts with the heterogeneity exploration module $M_c$ with a learned heterogeneity-aware kernel $\kappa_c$ to generate $E_{learn}$. The learned environments are used by $M_p$ to produce invariant direction $\theta_{inv}$ in Neural Tangent Feature (NTF) space that captures the invariant components $\Psi_S$, and then $\theta_{inv}$ is used to guide the gradient descent of neural networks. After that, we update the kernel $\kappa_c$ to orthogonalize with the invariant direction $\theta_{inv}$ so as to better capture the variant components $\Psi_V$ and realize the mutual promotion between $M_c$ and $M_p$ iteratively. The whole framework is jointly optimized, so that the mutual promotion between heterogeneity exploration and invariant learning can be fully leveraged. For smoothness we
begin with the invariant prediction step to illustrate our algorithm, and the flow of whole algorithm is shown in figure [1].

3.1 $\mathcal{M}_p$: Invariant Gradient Descent with $\mathcal{E}_{\text{learn}}$ (Step 1)

For our invariant learning module $\mathcal{M}_p$, we propose Invariant Gradient Descent (IGD) algorithm. Taking the learned environments $\mathcal{E}_{\text{learn}}$ as input, our IGD firstly performs invariant learning in Neural Tangent Feature (NTF) [10] space to obtain the invariant direction $\theta_{\text{inv}}$, and then guides the whole neural network $f_w(\cdot)$ with $\theta_{\text{inv}}$ to learn the invariant model (neural network)’s parameters $w_{\text{inv}}$.

Neural Tangent Feature Space The NTK theory [10] shows that training the neural network is equivalent to linear regression using non-linear NTFs $\phi(x)$, as in equation [3]. For each data point $x \in \mathbb{R}^d$, where $d$ is the feature dimension, the corresponding feature is given by $\phi(x) = \nabla_w f_w(x) \in \mathbb{R}^p$, where $p$ is the number of neural network’s parameters. Firstly, we would like to dissect the feature components within $\phi(x)$ by decomposing the invariant and variant components hidden in $\phi(x)$. Therefore, we propose to perform Singular Value Decomposition (SVD) on the NTF matrix:

$$
\Phi(X)^T \approx \underbrace{U \cdot \frac{S}{\sqrt{\beta}} \cdot V^T}_{\beta \gg n \geq k}
$$

where $p \gg n \geq k$.

Intuitively, in equation [3], each row of $V_j^T \in V^T$ represents the $j$-th feature component of $\mathbb{R}^p$ and we take $k$ such different feature components with the top $k$ largest singular values to represent the data, and the rationality of low rank decomposition is guaranteed theoretically [21,16] and empirically [2]. Since SVD ensures every feature components orthogonal, the neural tangent feature of the $i$-th data point can be decomposed into $\phi(x_i)^T \approx \sum_{j=1}^k U_{i,j} \cdot S_{i,j} \cdot V_{j}^T$, where $U_{i,j} \cdot S_{i,j}$ denotes the strength of the $j$-th feature component in the $i$-th data. However, since neural networks have millions of parameters, the high dimension prevents us from learning directly on high dimensional NTFs $\Phi(X)$. Therefore, we rewrite the initial formulation of linear regression into:

$$
f_w(X) \approx f_{w_0}(X) + \Phi(X)^T(w - w_0) \approx f_{w_0}(X) + USV^T(w - w_0)
$$

where we let $\theta = V^T(w - w_0) \in \mathbb{R}^k$ which reflects how the model parameter $w$ utilizes the $k$ feature components. Since $V^T$ is orthogonal, fitting $w - w_0$ with features $\Phi(X)$ is equivalent to fitting $\theta$ using reduced NTFs $\Psi(X)$. In this way, we convert the original high-dimensional regression problem into the low-dimensional one in equation [5], since in wide neural networks, we have $p \gg n \geq k$.

Invariant Learning with Reduced NTFs $\Psi(X)$ We could perform invariant learning on reduced NTFs $\Psi(X)$ in linear space. In this work, we adopt the invariant regularizer proposed in [11] to learn $\theta = V^T(w - w_0)$ due to its optimality guarantees, and the objective function is:

$$
\theta_{\text{inv}} = \arg \min_{\theta} \sum_{\epsilon \in \mathcal{E}_{\text{learn}}} \mathcal{L}^\epsilon(\theta; \Psi, Y) + \alpha \cdot \text{Var}_{\mathcal{E}_{\text{learn}}} (\nabla_\theta \mathcal{L}^\epsilon)
$$

Guide Neural Network with invariant direction $\theta_{\text{inv}}$ With the learned $\theta_{\text{inv}}$, it remains to feed back to the neural network’s parameters $w$. Since for neural networks with millions of parameters whose $p \approx 10^8$, it is difficult to directly obtain $w$ as $w = w_0 + V\theta_{\text{inv}}$. Therefore, we design a loss function to approximate the projection $(w - w_0)/|V\theta_{\text{inv}}|$. Note that $f_w(X) = f_{w_0}(X) + USV^T(w - w_0) = f_{w_0}(X) + US\theta_{\text{inv}}$, we have

$$
S^{-1}U^T(f_w(X) - f_{w_0}(X)) = \theta_{\text{inv}}
$$

Therefore, we can ensure the updated parameters $w$ satisfy that $S^{-1}U^T(f_w(X) - f_{w_0}(X)) \in \mathbb{R}^k$ is parallel to $\theta_{\text{inv}}$, which leads to the following loss function:

$$
w_{\text{inv}} = \arg \min_w \mathcal{L}(w; X, Y) + \lambda \left(1 - \frac{|\langle \theta_{\text{inv}}, S^{-1}U^T(f_w(X) - f_{w_0}(X)) \rangle|}{||\theta_{\text{inv}}|| \cdot ||S^{-1}U^T(f_w(X) - f_{w_0}(X))||} \right)
$$

where $\mathcal{L}(w; X, Y)$ is the empirical prediction loss over training data and the second term is to force the invariance property of the neural network.

3.2 Variant Component Decomposition with $\theta_{\text{inv}}$ (Step 2)

The core of our KerHRM is the mutual promotion of the heterogeneity exploration module $\mathcal{M}_c$ and the invariant learning module $\mathcal{M}_p$. From our insight, we should leverage the variant components $\Psi_V$
to exploit the latent heterogeneity. Therefore, with the better invariant direction $\theta_{inv}$ learned by $M_p$ that captures the invariant components in data, it remains to capture better variant components $\Psi_V$ so as to further accelerate the heterogeneity exploration procedure, for which we design a clustering kernel $\kappa_c$ on the reduce NTF space of $\mathbb{R}^K$ with the help of $\theta_{inv}$ learned in section 3.1. Recall the NTF decomposition in equation 3, the initial similarity of two data points $x_i$ and $x_j$ can be decomposed as:

$$\kappa_c^{(0)}(x_i, x_j) = \phi(x_i)^T \phi(x_j) = \langle U_i S, U_j S \rangle$$ (9)

With the invariant direction $\theta_{inv}^{(t)}$ learned by $M_p$ in iteration $t$, we can wipe out the invariant components used by $\theta_{inv}^{(t)}$ via

$$\Psi_{V}^{(t+1)}(x_i) = U_i S - \left(U_i S, \theta_{inv}^{(t)}\right) \theta_{inv}^{(t)} / \|\theta_{inv}^{(t)}\|^2$$ (10)

which gives a new heterogeneity-aware kernel that better captures the variant components $\Psi_V$ as $\kappa_c^{(t+1)}(x_i, x_j) = \Psi_{V}^{(t+1)}(x_i)^T \Psi_{V}^{(t+1)}(x_j)$.

### 3.3 $M_c$: Heterogeneity exploration with $\kappa_c$ (Step 3)

$M_c$ takes one heterogeneous dataset as input, and outputs a learned multi-environment partition $E_{learn}$ for invariant prediction module $M_p$, and we implement it as a clustering algorithm with kernel regression given the heterogeneity-aware $\kappa_c(x_i, x_j) = \Psi_V(x_i)^T \Psi_V(x_j)$ that captures the variant components in data. Following the analysis above, only the variant components $\Psi_V$ should be leveraged to identify the latent heterogeneity, and therefore we use the kernel $\kappa_c$ as well as $\Psi_V(X)$ learned in section 3.2 to capture the different relationship between $\Psi_V$ and $Y$, for which we use $P(Y|\Psi_V)$ as the clustering center. Specifically, we assume the $j$-th cluster centre $P_{\Theta_j}(Y|\Psi_V(X))$ to be a Gaussian around $f(\Theta_j; \Psi_V(X))$ as:

$$h_j(\Psi_V(X), Y) = P_{\Theta_j}(Y|\Psi_V(X)) = \frac{1}{\sqrt{2\pi\sigma}} \exp(-\frac{(Y - f(\Theta_j; \Psi_V(X)))^2}{2\sigma^2})$$ (11)

For the given $N = \sum_{i \in \text{support}(E_{latent})} |D^i|$ data points $D = \{\psi_V(x_i), y_i\}_{i=1}^N$, the empirical distribution can be modeled as $\hat{P}_N = \frac{1}{N} \sum_{i=1}^N \delta_{\psi_V(x_i), y_i}$. Under this setting, we propose one convex clustering algorithm, which aims at finding a mixture distribution in distribution set $Q$ defined as:

$$Q = \{Q = \sum_{j \in [K]} q_j h_j(\Psi_V(X), Y), q \in \Delta_K \}$$ (12)

to fit the empirical data best. Therefore, the original objective function and the simplified one are:

$$\min_{Q \in Q} D_{KL}(\hat{P}_N\|Q) \Leftrightarrow \min_{\Theta, q} \left\{ \mathcal{L}_c = -\frac{1}{N} \sum_{i \in [N]} \log \left[ \sum_{j \in [K]} q_j h_j(\psi_V(x_i), y_i) \right] \right\}$$ (13)

Note that our clustering algorithm differs from others since the cluster centres are learned models parameterized with $\Theta$. As for optimization, we use EM algorithm to optimize the centre parameters $\Theta$ and the mixture weights $q$ iteratively. Specifically, when optimizing the cluster centre model $f(\Theta_j; \cdot)$, we use kernel regression with $\kappa_c(\cdot, \cdot)$ to avoid computing $\Psi_V(X)$ and allow large $K$. For generating the learned environments $E_{learn}$, we assign $i$-th point to $j$-th cluster with probability $P_{i,j} = q_j h_j(\psi_V(x_i), y_i) / \sum_{l \in [K]} q_l h_l(\psi_V(x_i), y_i)$.

### 4 Theoretical Analysis

In this section, we provide theoretical justifications of the mutual promotion between $M_c$ and $M_p$. Since our algorithm does not violate the theoretical analysis in [11] and [10] which proves that better $E_{learn}$ from $M_c$ benefits the MIP learned by $M_p$, to finish the mutual promotion, we only need to justify that better $\theta_{inv}$ from $M_p$ benefits the learning of $E_{learn}$ in $M_c$.

1. **Using $\Psi_V$ benefits the clustering.** Firstly, we introduce Lemma 4.1 from [15] to show that using $\Psi_V$ benefits the clustering in terms of larger between-cluster distance.

**Lemma 4.1.** For $c_i, c_j \in \text{support}(E_{latent})$, assume that $X$ satisfying Assumption 2.1 then under reasonable assumption(15), we have $D_{KL}(P_{\psi_V}(Y|X)\|P_{\psi_V}(Y|X)) \leq D_{KL}(P_{\psi_V}(Y|\Psi_V)\|P_{\psi_V}(Y|\Psi_V))$.

Then similar to [14], we use the rate-distortion theory to demonstrate why larger $D_{KL}$ between cluster centres benefits our convex clustering as well as the quality of $E_{learn}$.
Theorem 4.1. (Rate-Distortion) For the proposed convex clustering algorithm, we have:
\[
\min_{Q \in \mathcal{Q}} D_{KL}(\hat{P}_V || Q) = \min \mathbb{I}(I; J) + (1/2\sigma^2)E_{L,J}[d(\psi_V(x_i), y_i, \Theta)] + \text{Const} \tag{14}
\]
where \( r_{ij} = P(j | \psi_V(x_i), y_i) \) is a discrete random variable over the space \( \{1, 2, ..., N\} \times \{1, 2, ..., K\} \) which denotes the probability of \( i \)-th data point belonging to \( j \)-th cluster, \( I, J \) are the marginal distribution of random variable \( r_{ij} \) respectively, \( d(\psi_V(x_i), y_i, \Theta) = (\hat{f}_\Theta(\psi_V(x_i)) - y_i)^2 \) and \( \mathbb{I}(\cdot; \cdot) \) the Shannon mutual information. Note that the optimal \( r \) can be obtained by the optimal \( \Theta \) and therefore we only minimize the r.h.s with respect to \( \Theta \).

Actually \( d \) models the conditional distribution \( P(Y | \psi_V) \). If in the underlying distribution of the empirical data \( P(Y | \psi_V) \) differs a lot between different clusters, the optimizer will put more efforts in optimizing \( E_{L,J}[d(\psi_V(x_i), y_i, \Theta)] \) to avoid inducing larger error, resulting in smaller efforts put on optimization of \( \mathbb{I}(I; J) \) and a relatively larger \( \mathbb{I}(I; J) \). This means data sample points \( I \) have a larger mutual information with cluster index \( J \), thus the clustering is prone to be more accurate.

2. Orthogonality Property: Better \( \theta_{\text{inv}} \) for better \( \psi_V \). Firstly, we prove the orthogonality property between \( \theta_{\text{inv}} \) and parameters \( \Theta \) of clustering centres \( f_{\Theta_j}(\cdot) \).

Theorem 4.2. (Orthogonality Property) Denote the data matrix of \( j \)-th environment \( X^j \) and \( \psi_V(X^j) \) is the invariant feature and following functional representation lemma \([7]\) \( \psi_V \) is the invariant feature with \( \psi_V \perp \psi_S \) and its relationship with the target \( Y \) relies on the environment-specific \( \beta_e \).

Example. Assume that data points from environments \( e \in \mathcal{E} \) are generated as follows:
\[
X = Y(\Psi^e_S + \beta_e \Psi^e_V) + N(0, \Sigma) \in \mathbb{R}^d
\tag{15}
\]
where \( Y = \pm 1 \) with equal probability, the coefficient \( \beta_e \) varies across environment \( e \), \( \Psi^e_S \in \mathbb{R}^d \) is the invariant feature and following functional representation lemma \([7]\) \( \Psi^e_V \) is the variant feature with \( \Psi_V \perp \Psi_S \) and its relationship with the target \( Y \) relies on the environment-specific \( \beta_e \).

Remark. In example \([4]\) when \( \mathcal{M}_p \) achieves optimal, we have \( \theta_{\text{inv}} = \Psi^e_S \), which is the mid vertical hyperplane of the two Gaussian distribution. Then following equation \([10]\) we have \( \psi_V = X - (X^T \theta_{\text{inv}}) \theta_{\text{inv}} = Y \beta_e \Psi^e_V \), which directly shows that in the next iteration, \( \mathcal{M}_e \) uses solely variant components \( \psi_V \) in \( X \) to learn environments \( \mathcal{E}_{\text{learn}} \) with diverse \( P(Y|X) = P(Y|\psi_V) \), which by lemma \([7, 7]\) and theorem \([7, 7]\) gives the best clustering results.

5 Experiments

In this section, we validate the effectiveness of our method on synthetic data and real-world data.

Baselines. We compare our proposed KerHRM with the following methods:

- Distributionally Robust Optimization (DRO) \([8]\):
\[
\min_{\theta} \sup_{Q \in \mathcal{Q}_d} E_Q[\ell(\theta; X, Y)]
\]
- Environment Inference for Invariant Learning (EIIL) \([5]\):
\[
\min_{\Phi} \max_{u \in \mathcal{E}} \frac{1}{N_e} \sum_{i=1}^{N_e} u_i(e) \ell(w \odot \Phi(x_i), y_i) + \lambda \| \nabla_w |_{w=0} \|_2 \|
\tag{16}
\]
- Heterogeneous Risk Minimization (HRM) \([13]\)
- Invariant Risk Minimization (IRM) \([11]\) with environment \( \mathcal{E}_{\text{er}} \) labels:
\[
\min_{\Phi} \sum_{e \in \mathcal{E}_{\text{er}}} L^e + \lambda \| \nabla_w |_{w=1.0} L^e (w \odot \Phi) \|_2^2
\tag{17}
\]
We choose one typical method of DRO as DRO is another main branch of methods for OOD generalization problem of the same setting with us (no environment labels). And HRM and EIIL are another methods for inferring environments for invariant learning without environment labels. We choose IRM as another baseline for its fame in invariant learning, but note that IRM is based on multiple training environments and we provide \( \mathcal{E}_r \) labels for it, while the others do not need. Further, for ablation study, we run KerHRM for only one iteration without the feedback loop and denote it as Static KerHRM(KerHRM'). For all experiments, we use a two-layer MLP with 1024 hidden units.

**Evaluation Metrics** To evaluate the prediction performance, for task with only one testing environment, we simply use the prediction accuracy of the testing environment. While for tasks with multiple environments, we introduce Mean_Error defined as Mean_Error = \( \frac{1}{|\mathcal{E}_{test}|} \sum_{e \in \mathcal{E}_{test}} \mathcal{L}^e \), Std_Error defined as Std_Error = \( \sqrt{\frac{1}{|\mathcal{E}_{test}|-1} \sum_{e \in \mathcal{E}_{test}} (\mathcal{L}^e - \text{Mean_Error})^2} \), which are mean and standard deviation error across \( \mathcal{E}_{test} \). And we use the average mean error for \( \mathcal{L}^e \).

5.1 Synthetic Data

**Classification with Spurious Correlation**

Following [19], we induce the spurious correlation between the label \( Y \in \{+1, -1\} \) and a spurious attribute \( A \in \{+1, -1\} \). Specifically, each environment is characterized by its bias rate \( r \in (0, 1) \), where the bias rate \( r \) represents that for 100 \( \ast r\% \) data, \( A = Y \), and for the other 100 \( \ast (1 - r)\% \) data, \( A = -Y \). Intuitively, \( r \) measures the strength and direction of the spurious correlation between the label \( Y \) and spurious attribute \( A \), where larger \( |r - 0.5| \) signifies higher spurious correlation between \( Y \) and \( A \), and \( \text{sign}(r - 0.5) \) represents the direction of such spurious correlation, since there is no spurious correlation when \( r = 0.5 \). We assume \( X = H[S, V]^T \in \mathbb{R}^{2d} \), where \( S \in \mathbb{R}^d \) is the invariant feature generated from label \( Y \) and \( V \) the variant feature generated from spurious attribute \( A \):

\[
S|Y \sim \mathcal{N}(Y\mathbf{1}, \sigma_Y^2 I_d), \quad V|A \sim \mathcal{N}(A\mathbf{1}, \sigma_A^2 I_d)
\]  

(18)

and \( H \in \mathbb{R}^{2d \times 2d} \) is an random orthogonal matrix to scramble the invariant and variant component, which makes it more practical. Typically, we set \( \sigma_Y^2 \geq \sigma_A^2 \) to let the model more prone to use spurious \( V \) since \( V \) is more informative.

In training, we set \( d = 5 \) and generate 2000 data points, where 50% points are from environment \( e_1 \) with \( r_1 = 0.9 \) and the other from environment \( e_2 \) with \( r_2 \). For our method, we set the cluster number \( K = 2 \). In testing, we generate 1000 data points from environment \( e_3 \) with \( r_3 = 0.1 \) to induce distributional shifts from training. In this experiments, we vary the bias rate \( r_2 \) of environment \( e_2 \) and the scrambled matrix \( H \) which can be an orthogonal or identity matrix (as done in [1]), and results after 10 runs are reported in Table [1].

From the results, we have the following observations and analysis: ERM suffers from the distributional shifts between training and testing, which yields the worst performance in testing. DRO can only provide slight resistance to distributional shifts, which we think is due to the over-pessimism problem. EIIL achieves the best training performance but also performs poorly in testing. HRM outperforms the above three baselines, but its testing accuracy is just around the random guess(0.50), which is due to the disturbance of the simple raw feature setting in [15]. IRM performs better when the heterogeneity between training environments is large(\( r_2 \) is small), which verifies our analysis in section 4 that the performance of invariant learning methods highly depends on the quality of the given \( \mathcal{E}_{tr} \). Compared to all baselines, our KerHRM performs the best with respect to highest testing accuracy and lowest (Train_Acc – Test_Acc), showing its superiority to IRM and original HRM.

Further, we also empirically analyze the sensitivity to the choice of cluster number \( K \) of our KerHRM. We set \( r_2 = 0.80 \) and test the performance with \( K = \{2, 3, 4, 5\} \) respectively. Results compared with IRM are shown in Table [2]. From the results, we can see that the cluster number of our methods does not need to be the ground truth number (ground truth is 2) and our KerHRM is not sensitive to the choice of cluster number \( K \). Intuitively, we only need the learned environments to reflect the variance of relationships between \( P(Y|\Psi^r_e) \), but do not require the environments to be ground truth. However, we notice that when \( K \) is far away from the proper one, the convergence of clustering algorithm is much slower.

**Regression with Selection Bias**

In this setting, we induce the spurious correlation between the label \( Y \) and spurious attributes \( V \) through selection bias mechanism, which is similar to that in [12]. We assume \( X = H[S, V]^T \in \mathbb{R}^{2d} \). Our method is trained as follows:

\[
\mathcal{L} = \mathbb{E}_{e \in \mathcal{E}_{test}} \mathcal{L}^e,
\]

where \( \mathcal{L}^e = \frac{1}{|\mathcal{E}_{test}|} \sum_{e \in \mathcal{E}_{test}} (Y^e_y - Y^e_s)^2 \mathcal{E}_r^e \), \( Y^e_s \) is the target label of environment \( e \) and \( Y^e_y \) is the output of our model.

\[
\mathcal{E}_r^e = \left\{ Y^e_s | Y^e_s \neq Y^e_y \right\}
\]

(19)

We also run KerHRM for only one iteration without the feedback loop and denote it as Static KerHRM(KerHRM'). For all experiments, we use a two-layer MLP with 1024 hidden units.
Table 1: Results in classification simulation experiments of different methods with varying bias rate \( r \), and scrambled matrix \( H \), and each result is averaged over ten times runs.

<table>
<thead>
<tr>
<th>Methods</th>
<th>( r = 0.70 )</th>
<th>( r = 0.75 )</th>
<th>( r = 0.80 )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Train_Acc</td>
<td>Test_Acc</td>
<td>Train_Acc</td>
</tr>
<tr>
<td>ERM</td>
<td>0.884</td>
<td>0.400</td>
<td>0.862</td>
</tr>
<tr>
<td>DRO</td>
<td>0.857</td>
<td>0.473</td>
<td>0.870</td>
</tr>
<tr>
<td>EIIL</td>
<td>0.927</td>
<td>0.523</td>
<td>0.925</td>
</tr>
<tr>
<td>HRM</td>
<td>0.836</td>
<td>0.543</td>
<td>0.832</td>
</tr>
<tr>
<td>KerHRM(^*)</td>
<td>0.764</td>
<td>0.671</td>
<td>0.782</td>
</tr>
<tr>
<td>KerHRM</td>
<td>0.759</td>
<td>0.724</td>
<td>0.760</td>
</tr>
</tbody>
</table>

Table 2: Ablation study on the cluster number \( K \). Each result is averaged over ten times runs.

<table>
<thead>
<tr>
<th></th>
<th>IRM</th>
<th>HRM</th>
<th>KerHRM ((K = 2))</th>
<th>KerHRM ((K = 3))</th>
<th>KerHRM ((K = 4))</th>
<th>KerHRM ((K = 5))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train_Acc</td>
<td>0.877</td>
<td>0.852</td>
<td>0.741</td>
<td>0.758</td>
<td>0.756</td>
<td>0.753</td>
</tr>
<tr>
<td>Test_Acc</td>
<td>0.401</td>
<td>0.488</td>
<td>0.693</td>
<td>0.687</td>
<td>0.698</td>
<td>0.668</td>
</tr>
</tbody>
</table>

\( \mathbb{R}^d \) and \( Y = f(S) + \epsilon \), where \( f(\cdot) \) is a non-linear function such that \( P(Y|S) \) remains invariant across environments while \( P(Y|V) \) changes arbitrarily. For simplicity, we select data \((x_i, y_i)\) with probability \( P(x_i, y_i) \) according to a certain variable \( V_b \in V \):

\[
P(x_i, y_i) = |r|^{-5s|y_i - \text{sign}(r) \cdot V_b|}
\]  

where \(|r| > 1\). Intuitively, \( r \) eventually controls the strengths and direction of the spurious correlation between \( V_b \) and \( Y \)(i.e. if \( r > 0 \), a data point whose \( V_b \) is close to its \( y \) is more probably to be selected.). The larger value of \(|r|\) means the stronger spurious correlation between \( V_b \) and \( Y \), and \( r > 0 \) means positive correlation and vice versa. Therefore, here we use \( r \) to define different environments.

In training, we generate 1000 points from environment \( e_1 \) with a predefined \( r \) and 100 points from \( e_2 \) with \( r = -1 \). In testing, to simulate distributional shifts, we generate data points for 6 environments with \( r \in \{-2.9, -2.7, \ldots, -1.9\} \). We compare our KerHRM with ERM, DRO, EIIL and IRM. We conduct experiments with different settings on \( r \) and the scrambled matrix \( H \).

From the results in Table 3, we have the following analysis: ERM, DRO and EIIL performs poor with respect to high average and stability error, which is similar to that in classification experiments(Table 1). The results of HRM are quite different in two scenarios, where Scenario 1 corresponds to the simple raw feature setting \((H = I)\) in [15] but Scenario 2 violates such simple setting with random orthogonal \( H \) and greatly harms HRM. Compared to all baselines, our KerHRM achieves lowest average error in 5/6 settings, and its superiority is especially obvious in our more general setting(Scenario 2).

**Colored MNIST**

To further validate our method’s capacity under general settings, we use the colored MNIST dataset, where data \( X \) are high-dimensional non-linear transformation from invariant features(digit Y) and variant features(color C). Following [11], we build a synthetic binary classification task, where each image is colored either red or green in a way that strongly and spuriously correlates with the class label \( Y \). Firstly, a binary label \( Y \) is assigned to each images according to its digits: \( Y = 0 \) for digits 0~4 and \( Y = 1 \) for digits 5~9. Secondly, we sample the color id \( C \) by flipping \( Y \) with probability \( e \) and therefore forms environments, where \( e = 0.1 \) for the first training environment, \( e = 0.2 \) for the second training environments and \( e = 0.9 \) for the testing environment. Thirdly, we induce noisy labels by randomly flipping the label \( Y \) with probability 0.2.

We randomly sample 2500 images for each environments, and the two training environments are mixed without environment label \( E_p \) for ERM, DRO, EIIL, HRM\(^*\) and IRM, while for IRM, the \( E_p \) labels are provided. For IRM, we sample 1000 data from the two training environments respectively and select the hyper-parameters which maximize the minimum accuracy of two validation environments. Note that we have no access to the testing environment while training, therefore we cannot resort to testing data to select the best one, which is more reasonable and different from that in [11]. For the others, since we have no access to \( E \) labels, we simply pool the 2000 data points for validation. The results are shown in Table 4 where Perfect Inv. Model represents the oracle.
Table 3: Results in selection bias simulation experiments of different methods with varying selection bias $r$, and scrambled matrix $H$, and each result is averaged over ten runs.

<table>
<thead>
<tr>
<th>r</th>
<th>Methods</th>
<th>$r = 1.9$</th>
<th>$r = 1.5$</th>
<th>$r = 2.3$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean_Error</td>
<td>Std_Error</td>
<td>Mean_Error</td>
<td>Std_Error</td>
</tr>
<tr>
<td>1.9</td>
<td>ERM</td>
<td>5.056</td>
<td>0.223</td>
<td>5.442</td>
</tr>
<tr>
<td>1.5</td>
<td>DRO</td>
<td>4.571</td>
<td>0.205</td>
<td>4.908</td>
</tr>
<tr>
<td>2.3</td>
<td>EHRM</td>
<td>5.006</td>
<td>0.211</td>
<td>5.252</td>
</tr>
<tr>
<td>2.3</td>
<td>IRM(ε, r)</td>
<td>3.625</td>
<td>0.057</td>
<td>3.901</td>
</tr>
<tr>
<td>1.9</td>
<td>KerHRM</td>
<td>3.873</td>
<td>0.176</td>
<td>4.356</td>
</tr>
<tr>
<td>1.9</td>
<td>KerHRM</td>
<td>4.384</td>
<td>0.191</td>
<td>3.989</td>
</tr>
<tr>
<td>1.5</td>
<td>KerHRM</td>
<td>4.112</td>
<td>0.182</td>
<td>3.659</td>
</tr>
</tbody>
</table>

Table 4: Colored MNIST results. The first row indicates whether each method needs the environment label. The Perfect Inv. Model represents the oracle results that can be achieved. The Generalization Gap is defined as $(Test \text{ Accuracy} - Train \text{ Accuracy})$.

<table>
<thead>
<tr>
<th>Method</th>
<th>ERM</th>
<th>DRO</th>
<th>EHRM</th>
<th>KerHRM</th>
<th>KerHRM</th>
<th>KerHRM</th>
<th>\text{Perfect Inv. Model}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need (E_{tr}) Label?</td>
<td>\xmark</td>
<td>\xmark</td>
<td>\xmark</td>
<td>\xmark</td>
<td>\xmark</td>
<td>\xmark</td>
<td>\xmark</td>
</tr>
<tr>
<td>Train Accuracy</td>
<td>0.845</td>
<td>0.644</td>
<td>0.717</td>
<td>0.835</td>
<td>0.766</td>
<td>0.802</td>
<td>0.654</td>
</tr>
<tr>
<td>Test Accuracy</td>
<td>0.116</td>
<td>0.419</td>
<td>0.542</td>
<td>0.283</td>
<td>0.468</td>
<td>0.296</td>
<td>0.648</td>
</tr>
<tr>
<td>Generalization Gap</td>
<td>-0.739</td>
<td>-0.223</td>
<td>-0.235</td>
<td>-0.553</td>
<td>-0.298</td>
<td>-0.506</td>
<td>-0.006</td>
</tr>
</tbody>
</table>

From the results, our KerHRM generalize the HRM to much more complicated data and consistently achieves the best performances. KerHRM even outperforms IRM significantly in an unfair setting where we provide perfect environment labels for IRM, which shows the limitation of manually labeled environments. Further, to best show the mutual promotion between \(M_c\) and \(M_p\), we plot the training and testing accuracy as well as the KL-divergence \(D_{KL}\) of \(P(Y|C)\) between the learned \(\mathcal{E}_{tr}\) over iterations in figure 2. From figure 2, we firstly validate the mutual promotion between \(M_c\) and \(M_p\) since \(D_{KL}\) and testing accuracy escalate synchronously over iterations. Secondly, figure 2 corresponds to our analysis in section 2 that the performance of invariant learning method is highly correlated to the heterogeneity of \(\mathcal{E}_{tr}\), which sheds lights to the importance of how to leverage the intrinsic heterogeneity in training data for invariant learning.

5.2 Real-world Data

In this experiment, we test our method on a real-world regression dataset (Kaggle) of house sales prices from King County, USA\(^3\) where the target variable is the transaction price of the house and each sample contains 17 predictive variables, such as the built year, number of bedrooms, and square footage of home, etc. Since it is fairly reasonable to assume the relationships between predictive variables and the target vary along the time (for example, the pricing mode may change along the time), there exist distributional shifts in the price-prediction task with respect to the build year of houses. Specifically, the houses in this dataset were built between 1900 ~ 2015, and we divide the whole dataset into 6 periods, where each contains a time span of two decades. Notice that the later periods have larger distributional shifts. We train all methods on the first period where built_year $\in [1900, 1920)$ and test on the other 5 periods and report the average results over 10 runs in figure 3. For IRM, we further divide the period 1 into two decades for the \(\mathcal{E}_{tr}\) provided.

\(^3\)https://www.kaggle.com/c/house-prices-advanced-regression-techniques/data
Figure 2: Results for the Colored MNIST task. We plot the training and testing accuracy, as well as the KL-divergence between learned $\mathcal{E}_{tr}$.

Figure 3: Results for the real-world regression task. We train all methods on $e_1$ and test on the others, and report the average results over 10 runs.

Analysis The testing errors of ERM and DRO increase sharply across environments, indicating the existence of the distributional shifts between environments. IRM performs better than ERM and DRO, which shows the usefulness of environment labels for OOD generalization and the possibility of learning invariant predictor from multiple environments. The proposed KerHRM outperforms EIIL and HRM, which validates its superiority of heterogeneity exploration. KerHRM even outperforms IRM, which indicates the limitation of manually labeled environments in invariant learning and the necessity of latent heterogeneity exploration.

6 Limitations

Although the proposed KerHRM is a competitive method, it has several limitations. Firstly, since in $\mathcal{M}_e$ we take the model parameters as cluster centres, the strict convergence guarantee for our clustering algorithm $\mathcal{M}_c$ is quite hard to analyze. And empirically, we find when the pre-defined cluster number $K$ is far away from the ground-truth, the convergence of $\mathcal{M}_c$ will become quite slow. Further, such restriction also affects the analysis of the mutual promotion between $\mathcal{M}_c$ and $\mathcal{M}_p$, which we can only empirically provide some verification. Besides, although we incorporate Neural Tangent Kernel to deal with data beyond raw feature level, how to deal with more complicated data still remains unsolved. Also, how to incorporate deep learning with the mutual promotion between the two modules needs further investigation, and we left it for future work.

7 Conclusion

In this paper, we propose the KerHRM algorithm for the OOD generalization problem, which achieves both the latent heterogeneity exploration and invariant prediction. From our theoretical and empirical analysis, we find that the heterogeneity of environments plays a key role in invariant learning, which is consistent with some recent analysis[17] and opens a new line of research for OOD generalization problem. Our code is available at https://github.com/LJSthu/Kernelized-HRM.

Acknowledgements

This work was supported National Key R&D Program of China (No. 2018AAA0102004).
References


