Domain Generalisation via Risk Distribution Matching

Toan Nguyen, Kien Do, Bao Duong, Thin Nguyen
Applied Artificial Intelligence Institute, Deakin University, Australia
{s222165627, k.do, duongng, thin.nguyen}@deakin.edu.au

Abstract

We propose a novel approach for domain generalisation (DG) leveraging risk distributions to characterise domains, thereby achieving domain invariance. In our findings, risk distributions effectively highlight differences between training domains and reveal their inherent complexities. In testing, we may observe similar, or potentially intensifying in magnitude, divergences between risk distributions. Hence, we propose a compelling proposition: Minimising the divergences between risk distributions across training domains leads to robust invariance for DG. The key rationale behind this concept is that a model, trained on domain-invariant or stable features, may consistently produce similar risk distributions across various domains. Building upon this idea, we propose Risk Distribution Matching (RDM). Using the maximum mean discrepancy (MMD) distance, RDM aims to minimise the variance of risk distributions across training domains. However, when the number of domains increases, the direct optimisation of variance leads to linear growth in MMD computations, resulting in inefficiency. Instead, we propose an approximation that requires only one MMD computation, by aligning just two distributions: that of the worst-case domain and the aggregated distribution from all domains. Notably, this method empirically outperforms optimising distributional variance while being computationally more efficient. Unlike conventional DG matching algorithms, RDM stands out for its enhanced efficacy by concentrating on scalar risk distributions, sidestepping the pitfalls of high-dimensional challenges seen in feature or gradient matching. Our extensive experiments on standard benchmark datasets demonstrate that RDM shows superior generalisation capability over state-of-the-art DG methods.

1. Introduction

In recent years, deep learning (DL) models have witnessed remarkable achievements and demonstrated super-human performance on training distributions [27]. Nonetheless, this success is accompanied by a caveat - deep models are vulnerable to distributional shifts and exhibit catastrophic failures to unseen out-of-domain data [12, 34]. Such limitations hinder the widespread deployment of DL systems in real-world applications, where domain difference can be induced by several factors, such as spurious correlations [2] or variations in location or time [49].

In light of these challenges, domain generalisation (DG) aims to produce models capable of generalising to unseen target domains by leveraging data from diverse sets of training domains or environments [38]. An effective approach involves exploring and establishing domain invariance [32], with the expectation that these invariances will similarly apply to related, yet distinct, test domains. To this end, prevailing research focuses on characterising domains through sample representation [31, 38]. The objective is to seek for domain-invariant features by aligning the distributions of hidden representations across various domains. CORAL [53] trains a non-linear transformation that can align the second-order statistics of representations across different layers within deep networks. More, CausIIRL [11]
aims to match representation distributions that have been intervened upon the spurious factors. While these methods show promise, they can face multiple challenges with the curse of dimensionality [6, 22]. The sparsity of high-dimensional representation spaces can lead to unreliable estimates of statistical properties, which in turn affects the quality of distribution matching techniques. Also, high-dimensional representations may contain many irrelevant or redundant dimensions, which can introduce noise to the true underlying similarities or differences between distributions. As dimensionality rises, computational complexity intensifies, reducing the efficacy of these methods [39]. Such challenges similarly present in DG methods that utilise gradients for domain alignment [46, 50].

In this paper, we propose to utilise scalar risk distributions as a means to characterise domains, leading to successfully exploring and enforcing domain invariance. Our research reveals that risk distributions can be a reliable indicator of domain variation as it effectively highlights differences between training domains. In Figure 1, we present a visual evidence through histograms, contrasting the risk distributions between the “Art” and “Photo” domains on the validation set of PACS dataset [30], derived from training with Empirical Risk Minimisation (ERM) [56]. The “Photo” domain generally exhibits a larger distribution of scalar risks than that of “Art”. This suggests an inherent complexity in learning “Photo” samples, or possibly due to a more limited training dataset compared to “Art”. During the testing phase, similar divergences between risk distributions may emerge, potentially intensifying in magnitude. Hence, we propose a compelling proposition: by minimising the divergences between risk distributions across training domains, we can achieve robust invariance for DG. The underlying rationale for this concept is that a model, when learning domain-invariant and stable features, tends to produce consistent risk distributions across domains.

Building upon this idea, we propose a novel matching approach for DG, namely Risk Distribution Matching (RDM). RDM’s objective is to minimise the variance of risk distributions across all training domains. Inspired by [38], we redefine the distributional variance metric to focus specifically on risk distributions and propose to compute it via the maximum mean discrepancy (MMD) distance [19]. However, when the number of training domains increases, directly optimising the variance induces a linear growth in MMD computations, reducing efficiency. Instead, we propose an approximation that requires only one MMD computation via aligning just two distributions: that of the worst-case (or worst-performing) domain and the aggregated distribution from all domains. Empirically, this approach outperforms optimising distributional variance while significantly reducing computational complexity. Unlike prevailing matching algorithms, RDM can address the high-dimensional challenges and further improve efficacy by exclusively focusing on scalar risk distributions. Notably, our empirical studies show that RDM even exhibits enhanced generalisation while being more convenient to optimise. We summarise our contributions below:

- We propose RDM, a novel and efficient matching method for DG, based on our two hypotheses: i) risk distribution disparities offer insightful cues into domain variation; ii) reducing these divergences fosters a generalisable and invariant feature-learning predictor.

- We re-conceptualise the distributional variance metric to exclusively focus on risk distributions, with an objective to minimise it. We further provide an approximate version that aligns only the risk distribution of the worst-case domain with the aggregate from all domains, improving both performance and efficiency.

- Through extensive experiments on standard benchmark datasets, we empirically show that RDM consistently outperforms state-of-the-art DG methods, showcasing its remarkable generalisation capability.

2. Related Work

Domain Generalisation (DG)  DG aims to develop models that can generalise well on unseen target domains by leveraging knowledge from multiple source domains. Typical DG methods include domain alignment [7, 32, 38], meta learning [4, 29], data augmentation [60, 62], disentangled representation learning [44, 54], robust optimisation [8, 48] and causality-based methods [13, 25, 41]. Our proposed method RDM is related to domain alignment, striving for domain invariance to enhance OOD generalisation. Existing research focuses on characterising domains through sample representations and aligning their distributions across domains to achieve domain-invariant features [1, 38]. CORAL [53] matches mean and variance of representation distributions, while MMD-AAE [31] and FedKA [55] consider matching all moments via the maximum mean discrepancy (MMD) distance [19]. Other methods promote domain invariance by minimising contrastive loss [10] between representations sharing the same labels [35, 37]. Many studies bypass the representation focus, instead characterising domains via gradients and achieving invariance by reducing inter-domain gradient variance [46, 50, 59].

Despite their potential, aligning these high-dimensional distributions may be affected by data sparsity, diversity, and high computational demands [6, 22]. Unlike these methods, RDM offers enhanced efficacy by focusing on scalar risk distributions, overcoming the high-dimensional challenges. Further, RDM adopts a novel strategy by efficiently aligning only two distributions: that of the worst-case domain.
with the aggregate from all domains. From our experiments, RDM generally exhibits better generalisation performance while being more convenient to optimise compared to competing matching techniques. To the best of our knowledge, the incarnation of risk distributions for domain matching in RDM is novel and sensible.

**Distribution matching** Distribution matching has been an important topic with a wide range of applications in machine learning such as DG [31, 53], domain adaptation [9, 58], generative modelling [28, 33]. Early methods, like the MMD distance [19], leverage kernel-based approaches to quantify the distance between distributions, laying the foundation for many subsequent DG techniques [31, 38]. Further advancements have explored optimal transport methods, like the Wasserstein distance [3, 36], which provides a geometrically intuitive means to compare distributions. Other metrics, such as the Kullback-Leibler [26] or Jensen-Shannon [14, 16] divergences, can serve to measure the divergence between training risk distributions via an analytical measure of the divergence between distributions. Its inherent advantages characterises each domain and provides valuable insights into domain variation. Specifically, we propose to leverage the distributional variance across them to align risk distributions.

Invariance and Causality in DG Causal methods in DG assume that the causal mechanism of the target given causal input features is invariant while non-causal features may change across domains [2, 25, 45]. Based on this assumption, methods establish domain invariance to recover the causal mechanism, thereby improving generalisation. ICP [45] has shown that the causal predictor has an invariant distribution of residuals in regression models, however, is not suitable for deep learning. EQRM [13] and REx [25] leverage the invariance in the average risks over samples across domains. In contrast to above methods, we consider matching entire risk distributions over samples across domains, which, as our experiments demonstrate, is more powerful and enhances generalisation capability.

3. Preliminaries

Domain generalisation (DG) involves training a classifier \( f \) on data composed of multiple training domains (also called environments) so that \( f \) can perform well on unseen domains at test time. Mathematically, let \( D = \{ D_1, ..., D_m \} \) denote the training set consisting of \( m \) different domains/environments, and let \( D_e := \{(x^e_i, y^e_i)\}_{i=1}^{n_e} \) denote the training data belonging to domain \( e \) (1 \( \leq e \leq m \)). Given a loss function \( \ell \), the risk of a particular domain sample \((x^e_i, y^e_i)\) is denoted by \( R_e := \ell (f(x^e_i), y^e_i) \), and the expected risk \( \overline{R}_e \) of domain \( e \) is defined as:

\[
\overline{R}_e := \mathbb{E}_{(x^e_i, y^e_i) \sim D_e} [\ell (f(x^e_i), y^e_i)] = \mathbb{E}_{D_e} [R_e] \tag{1}
\]

A common approach to train \( f \) is Empirical Risk Minimisation (ERM) [56] which minimises the expected risks across all training domains. Its loss function, denoted by \( \mathcal{L}_{\text{ERM}} \), is computed as follows:

\[
\mathcal{L}_{\text{ERM}} = \mathbb{E}_{e \sim \mathcal{E}} \mathbb{E}_{(x^e_i, y^e_i) \sim D_e} [\ell (f(x^e_i), y^e_i)] = \mathbb{E}_{e \sim \mathcal{E}} [\overline{R}_e] \tag{2}
\]

\[
\mathcal{L}_{\text{ERM}} + \lambda V_R (\{T_1, ..., T_m\}) \tag{4}
\]

where \( \mathcal{E} := \{1, ..., m\} \) denotes the set of all domains.

4. Risk Distribution Matching

A model \( f \) trained via ERM often struggles with generalisation to new test domains. This is because it tends to capture domain-specific features [2, 41], such as domain styles, to achieve low risks in training domains, rather than focusing on domain-invariant or semantic features. To overcome this issue, we present a novel training objective that bolsters generalisation through domain invariance. Our goal requires utilising a unique domain representative that both characterises each domain and provides valuable insights into domain variation. Specifically, we propose to leverage the distribution of risks over all samples within a domain (or shortly risk distribution) as this representative. Unlike other domain representatives, like latent representation or gradient distributions [31, 50], the risk distribution sidesteps high-dimensional challenges like data sparsity and high computational demands [6, 39]. In essence, a model capturing stable, domain-invariant features may consistently yield similar risk distributions across all domains. In pursuit of invariant models, we propose **Risk Distribution Matching** (RDM), a novel approach for DG that reduces the divergences between training risk distributions via minimising the distributional variance across them.

Let \( T_e \) be the probability distribution over the risks of all samples in domain \( e \) (i.e., \( \{R^e_i\}_{i=1}^{n_e} \)). We refer to \( T_e \) as the risk distribution of domain \( e \), the representative that effectively captures the core characteristics of the domain. We denote \( V_R (\{T_1, ..., T_m\}) \) the distributional variance across the risk distributions \( \{T_1, ..., T_m\} \) in the real number space. We achieve our objective by minimising the following loss function:

\[
\mathcal{L}_{\text{final}} := \mathcal{L}_{\text{ERM}} + \lambda V_R (\{ T_1, ..., T_m \}) \tag{4}
\]
where \( \lambda \geq 0 \) is a coefficient balancing between reducing the total training risks with enforcing invariance across domains. \( \lambda \) is set to 1 unless specified otherwise.

To compute \( \mathbb{V}_H(\{T_1, \ldots, T_m\}) \), we require a suitable representation for the implicit risk distribution \( T_e \) of domain \( e \). Leveraging kernel mean embedding [51], we express \( T_e \) as its embedding, \( \mu_{T_e} \), within a reproducing kernel Hilbert space (RKHS) \( H \) using a feature map \( \phi : \mathbb{R} \rightarrow H \) below:

\[
\mu_{T_e} := \mathbb{E}_{R_e \sim T_e} [\phi (R_e)] \quad (5)
\]

\[
= \mathbb{E}_{R_e \sim T_e} [k (R_e, \cdot)] \quad (6)
\]

where a kernel function \( k (\cdot, \cdot) : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \) is introduced to bypass the explicit specification of \( \phi \). Assuming the condition \((\mathbb{E}_{R_e \sim T_e} (k (R_e, R_e)) < \infty)\), the mean map \( \mu_{T_e} \) remains an element of \( H \) [19, 31]. It is noteworthy that for a characteristic kernel \( k \), the representation \( \mu_{T_e} \) within \( H \) is unique [19, 38]. Consequently, two distinct risk distributions \( T_u \) and \( T_v \) for any domains \( u, v \) respectively have different kernel mean embeddings in \( H \). In this work, we use the RBF kernel, a well-known characteristic kernel defined as \( k (x, x') := \exp (-\frac{1}{2\sigma^2} \|x - x'\|^2) \), where \( \sigma > 0 \) is the bandwidth parameter.

With the unique representation of \( T_e \) established, our objective becomes computing the distributional variance between risk distributions within \( H \), represented by \( \mathbb{V}_H(\{T_1, \ldots, T_m\}) \). Inspired by [38], we redefine the variance metric to focus specifically on risk distributions across multiple domains below:

\[
\mathbb{V}_H(\{T_1, \ldots, T_m\}) := \frac{1}{m} \sum_{e=1}^{m} \|\mu_{T_e} - \mu_T\|_H^2 \quad (7)
\]

where \( \mathcal{T} = \frac{1}{m} \sum_{e=1}^{m} T_e \) denotes the probability distribution over the risks of all samples in the entire training set, or equivalently, the set of all \( m \) domains. Meanwhile, \( \mu_{T_e} \) and \( \mu_T \) represent the mean embeddings of \( T_e \) and \( \mathcal{T} \), respectively, and are computed as in Eq. 5. Incorporating \( \mathbb{V}_H(\{T_1, \ldots, T_m\}) \) into our loss function from Eq. 4, we get:

\[
\mathcal{L}_{\text{final}} := \mathcal{L}_{\text{ERM}} + \lambda \mathbb{V}_H(\{T_1, \ldots, T_m\}) \quad (8)
\]

Minimising \( \mathbb{V}_H(\{T_1, \ldots, T_m\}) \) in Eq. 8 facilitates our objective of equalising risk distributions across all domains, as proven by the theorem below.

**Theorem 1.** [38] Given the distributional variance \( \mathbb{V}_H(\{T_1, \ldots, T_m\}) \) is calculated with a characteristic kernel \( k \), \( \mathbb{V}_H(\{T_1, \ldots, T_m\}) = 0 \) if and only if \( T_1 = \ldots = T_m (= \mathcal{T}) \).

**Proof.** Please refer to our appendix for the proof. \( \square \)

In the next part, we present how to compute the distributional variance using the Maximum Mean Discrepancy (MMD) distance [19], relying only on risk samples. Then, we propose an efficient approximation of optimising the distributional variance, yielding improved empirical performance.

### 4.1. Maximum Mean Discrepancy

For domain \( e \), the squared norm, \( \|\mu_{T_e} - \mu_T\|_H^2 \), defined in Eq. 7, is identified as the squared MMD distance [18] between distributions \( T_e \) and \( \mathcal{T} \). It is expressed as follows:

\[
\text{MMD}^2 (T_e, \mathcal{T}) := \|\mu_{T_e} - \mu_T\|_H^2
\]

\[
= \|\mathbb{E}_{R_e \sim T_e} [\phi (R_e)] - \mathbb{E}_{R_f \sim \mathcal{T}} [\phi (R_f)]\|_H^2
\]

\[
= \mathbb{E}_{R_e, R_f \sim \mathcal{T}} \langle \phi (R_e), \phi (R_f) \rangle - 2 \mathbb{E}_{R_e \sim T_e, R_f \sim \mathcal{T}} \langle \phi (R_e), \phi (R_f) \rangle + \mathbb{E}_{R_f \sim \mathcal{T}} ||\phi (R_f)\|_H^2
\]

where \( \langle \cdot, \cdot \rangle \) denote the inner product operation in \( H \). Through the kernel trick, we can compute these inner products via the kernel function \( k \) without an explicit form of \( \phi \) below:

\[
\text{MMD}^2 (T_e, \mathcal{T}) = \mathbb{E}_{R_e, R_f \sim \mathcal{T}} k (R_e, R_f)
\]

\[
- 2 \mathbb{E}_{R_e \sim T_e, R_f \sim \mathcal{T}} k (R_e, R_f)
\]

\[
+ \mathbb{E}_{R_f \sim \mathcal{T}} k (R_f)
\]

We reformulate our loss function in Eq. 8 to incorporate MMD as follows:

\[
\mathcal{L}_{\text{final}} := \mathcal{L}_{\text{ERM}} + \lambda \frac{1}{m} \sum_{e=1}^{m} \text{MMD}^2 (T_e, \mathcal{T})
\]

\[
= \mathcal{L}_{\text{ERM}} + \lambda \mathcal{L}_{\text{RDM}} \quad (13)
\]

The loss function \( \mathcal{L}_{\text{RDM}} \) involves minimising \( \text{MMD}^2 (T_e, \mathcal{T}) \) for every domain \( e \). Ideally, the distributional variance reaches its lowest value at 0 if \( \text{MMD} (T_e, \mathcal{T}) = 0 \), equivalent to \( T_e = \mathcal{T} \) [18, 19], across \( e \) domains. The objective also entails aligning each individual risk distribution, \( T_e \), with the aggregated distribution spanning all domains, \( \mathcal{T} \). With the characteristic RBF kernel, it can be viewed as matching an infinite number of moments across all risk distributions.

We emphasise our choice of MMD owing to its benefits for effective risk distribution matching: i) MMD is an
important member of the Integral Probability Metric family [40] that offers an analytical solution facilitated through RKHS, and ii) MMD enjoys the property of quantifying the dissimilarity between two implicit distributions via their finite samples in a non-parametric manner.

4.2. Further improvement of RDM

We find that effective alignment of risk distributions across $m$ domains can be achieved by matching the risk distribution of the worst-case domain, denoted as $w$, with the combined risk distribution of all domains, offering an approximation to the optimisation of risk distributional variance seen in Eq. 13. This approximate version significantly reduces the MMD distances computation in $\mathcal{L}_{\text{RDM}}$ from $O(m)$ to $O(1)$, and further improves generalisation, as we demonstrate with empirical evidence in Section 5.

Denote by $w = \arg\max_{e \in \mathcal{E}} R_e$ the worst-case domain, i.e., the domain that has the largest expected risk in $\mathcal{E}$. The approximate RDM’s loss, $\hat{\mathcal{L}}_{\text{RDM}}$, is computed as follows:

$$\hat{\mathcal{L}}_{\text{RDM}} = \text{MMD}^2(T_w, T)$$

$$\approx \mathcal{L}_{\text{RDM}}$$

In our experiments, we observed only a small gap between $\hat{\mathcal{L}}_{\text{RDM}}$ and $\mathcal{L}_{\text{RDM}}$, while optimising $\hat{\mathcal{L}}_{\text{RDM}}$ proving to be more computationally efficient. The key insight emerges from $\mathcal{R}_e$, the first moment (or mean) of $T_e$. Often, the average risk can serve as a measure of domain uniqueness or divergence [25, 46]. Specifically, a domain with notably distinct mean risk is more likely to diverge greatly from other risk distributions. Under such circumstances, $\mathcal{L}_{\text{RDM}}$ will be an upper-bound of $\mathcal{L}_{\text{RDM}}$, as shown by:

$$\mathcal{L}_{\text{RDM}} = \frac{1}{m} \sum_{e=1}^{m} \text{MMD}^2(T_e, T) \leq \frac{1}{m} \sum_{e=1}^{m} \text{MMD}^2(T_w, T) = \text{MMD}^2(T_w, T) = \hat{\mathcal{L}}_{\text{RDM}}.$$ 

By optimising $\hat{\mathcal{L}}_{\text{RDM}}$, we can also potentially decrease $\mathcal{L}_{\text{RDM}}$, thus aligning risk distributions across domains effectively. More, $\hat{\mathcal{L}}_{\text{RDM}}$ drives the model to prioritise the worst-case domain’s optimisation. This approach enhances the model’s robustness to extreme training scenarios, which further improves generalisation as proven in [25, 48]. These insights shed light on the superior performance of optimising $\hat{\mathcal{L}}_{\text{RDM}}$ over $\mathcal{L}_{\text{RDM}}$. Therefore, we opted to use $\hat{\mathcal{L}}_{\text{RDM}}$, simplifying our model’s training and further bolstering its OOD performance.

5. Experiments

We evaluate and analyse RDM using a synthetic ColoredMNIST dataset [2] and multiple benchmarks from the DomainBed suite [20]. Each of our claims is backed by empirical evidence in this section. Our source code to reproduce results is available at: https://github.com/nktoan/risk-distribution-matching

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Initialisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rand.</td>
<td>72.1±0.7</td>
</tr>
<tr>
<td>ERM</td>
<td>72.4±1.0</td>
</tr>
<tr>
<td>GroupDRO</td>
<td>56.3±1.5</td>
</tr>
<tr>
<td>IGA</td>
<td>52.5±2.4</td>
</tr>
<tr>
<td>IRM</td>
<td>55.2±4.0</td>
</tr>
<tr>
<td>VREx</td>
<td>54.3±1.7</td>
</tr>
<tr>
<td>EQRM</td>
<td>55.3±2.8</td>
</tr>
<tr>
<td>CORAL</td>
<td>54.6±3.2</td>
</tr>
<tr>
<td>MMD</td>
<td>72.1±0.4</td>
</tr>
<tr>
<td>Oracle</td>
<td>72.4±1.0</td>
</tr>
<tr>
<td>Optimum</td>
<td>75.0</td>
</tr>
</tbody>
</table>

Table 1. ColoredMNIST test accuracy where the best results are marked as bold. Results of other methods are referenced from [13].

5.1. Synthetic Dataset: ColoredMNIST

We evaluate all baselines on a synthetic binary classification task, namely ColoredMNIST [2]. This dataset involves categorising digits (0-9) into two labels: “zero” for 0 to 4 range and “one” for 5 to 9 range, with each digit colored either red or green. The dataset is designed to assess the generalisation and robustness of baseline models against the influence of spurious color features. The dataset contains two training domains, where the chance of red digits being classified as “zero” is 80% and 90%, respectively, while this probability decreases to only 10% during testing. The goal is to train a predictor invariant to “digit color” features, capturing only “digit shape” features.

Following [13], we employ a two-hidden-layer MLP with 390 hidden units for all baselines. Optimised through the Adam optimiser [23] at a learning rate of 0.0001, with a dropout rate of 0.2, we train each algorithm for 600 iterations with a batch size of 25,000. We repeat the experiment ten times over different values of the penalty weight $\lambda$. We find our matching penalty quite small, yielding optimal RDM’s performance within the $\lambda$ range of [1000, 10000]. We provide more details about experimental settings in the supplementary material.

We compare RDM with ERM and three different types of algorithms: robust optimisation (GroupDRO [48], IGA [24]), causal methods learning invariance (IRM [2], VREx [25], EQRM [13]) and representation distribution matching (MMD [31], CORAL [53]). All algorithms are run using two distinct network configurations: (i) initialising the network randomly via Xavier method [17]; (ii) pre-training the network with ERM for 400 iterations prior to performing the algorithms. Table 1 shows that our pro-
posed method RDM surpasses all algorithms, irrespective of the network configuration. RDM exhibits improvements of 1.0% and 6.8% over CORAL, both without and with pre-trained ERM, respectively, underlining the effectiveness of aligning risk distributions instead of high-dimensional representations. VREx and EQR M, which pursue invariant predictors by equalising average training risks across domains, demonstrate suboptimal performance compared to our approach. This improvement arises from our consideration of the entire risk distributions and the matching of all moments across them, which inherently foster stronger invariance for DG. Notably, all methods experience enhanced performance with ERM initialisation. RDM even excels beyond oracle performance (ERM trained on grayscale digits with 50% red and 50% green) and converges towards optimality.

Figure 2 demonstrates histograms with their KDE curves [42] depicting the risk distributions of ERM and RDM across four domains. The figure confirms our hypothesis that the disparities among risk distributions could serve as a valuable signal of domain variation. ERM’s histogram shows a clear difference between environments with 90% and 80% chance of red digits labelled “zero” and those with only 50% or 10%. More, ERM tends to overfit to training domains, which negatively impacts its generalisation to test domains. Remarkably, RDM effectively minimises the divergences between risk distributions across all domains, including test domains with lower risks. This also aligns with our motivation: an invariant or stable feature-learning predictor, by displaying similar risk distributions across domains, inherently boosts generalisation.

5.2. DomainBed

Dataset and Protocol Following previous works [13, 20], we extensively evaluate all methods on five well-known DG benchmarks: VLCS [15], PACS [30], OfficeHome [57], TerraIncognita [5], and DomainNet [43]. For a fair comparison, we reuse the training and evaluation protocol in DomainBed [20], including the dataset splits, training iterations, and model selection criteria. Our evaluation employs the leave-one-domain-out approach: each model is trained on all domains except one and then tested on the excluded domain. The final model is chosen based on its combined accuracy across all training-domain validation sets.

Implementation Details We use ResNet-50 [21] pre-trained on ImageNet [47] as the default backbone. The model is optimised via the Adam optimiser for 5,000 iterations on every dataset. We follow [13, 25] to pre-train baselines with ERM for certain iterations before performing the algorithms. Importantly, we find that achieving accurate risk distribution matching using distribution samples requires larger batch sizes - details of which are examined in our ablation studies. For most datasets, the optimal batch size lies between [70, 100]. However, for huge datasets like TerraIncognita and DomainNet, it is between [30, 60]. Although computational resources limit us from testing larger batch sizes, these ranges consistently achieve strong performance on benchmarks. The matching coefficient \( \lambda \) in our method is set in \([0.1, 10.0]\). Additional hyper-parameters like learning rate, dropout rate, or weight decay, adhere to the preset ranges as detailed in [13]. We provide more implementation details in the supplementary material. We repeat our experiments ten times with varied seed values and hyper-parameters and report the average results.

Experimental Results In Table 2, we show the average out-of-domain (OOD) accuracies of state-of-the-art DG methods on five benchmarks. Due to space constraints, domain-specific accuracies are detailed in the supplementary material. We compare RDM with ERM and various types of algorithms: distributional robustness (GroupDRO),
causal methods learning invariance (IRM, VREx, EQRm), gradient matching (Fish [50], Fishr [46]), representation distribution matching (MMD, CORAL) and other variants (Mixup [60], MLdG [29]). To ensure fairness in our evaluations, we have used the same training data volume across all baselines, although further employing augmentations can enhance models’ performance.

On average, RDM surpasses other baselines across all benchmarks, notably achieving a 1.5% average improvement over ERM. The significant improvement of RDM on DomainNet, a large-scale dataset with 586,575 images across 6 domains, is worth mentioning. This suggests that characterising domains with risk distributions to achieve invariance effectively enhances OOD performance. Compared to distributional robustness methods, RDM notably outperforms GroupDRO with improvement of 2.8% on PACS and a substantial 10.1% on DomainNet. RDM consistently improves over causality-based methods that rely on the average risk for domain invariance. This superiority attributes to our novel adoption of risk distributions, achieving enhanced invariance for DG. Our remarkable improvement over MMD suggests that aligning risk distributions via the MMD distance is more effective, easier to optimise than aligning representation distributions. While RDM typically outperforms CORAL and Fish in OOD scenarios, it only remains competitive or sometimes underperforms on certain datasets like OfficeHome. This decrease in performance may stem from the dataset’s inherent tendency to overfit within our risk distribution alignment objective. OfficeHome has only average about 240 samples per class, significantly fewer than other datasets with at least 1,400. This reduced sample size may not provide sufficiently diverse risk distributions to capture stable class features, resulting in overfitting on the training set. Despite these limitations, our OfficeHome results still outperform several well-known baselines such as MLdG, VREx, or ERM. For a detailed discussion on this challenge, please refer to our supplementary material.

5.3. Analysis

In this section, we provide empirical evidence backing our claims in Section 4. In Figure 3a, we highlight a small gap when aligning the risk distribution of the worst-case domain with that of all domains combined (RDM with $\mathcal{L}_{\text{RDM}}$), compared to directly optimising the distributional variance (RDM with $\mathcal{L}_{\text{RDM}}$). Notably, $\mathcal{L}_{\text{RDM}}$ consistently represents an upper bound of $\mathcal{L}_{\text{RDM}}$, which is sensible since the worst-case domain often exhibits the most distinct risk distribution. This suggests that optimising $\mathcal{L}_{\text{RDM}}$ also helps reduce the distributional variance $\mathcal{L}_{\text{RDM}}$, bringing the risk distributions across domains closer.
When the number of training domains grows, especially with large-scale datasets like DomainNet, emphasising the risk distribution of the worst-case domain not only proves to be a more efficient approach but also significantly enhances OOD performance. In our exploration of training resources for DomainNet, we study three matching methods: Fish, CORAL and two variants of our RDM method. For a fair evaluation, all experiments were conducted with identical GPU resources, settings, and hyper-parameters, such as batch size or training iterations. Results can be seen in Table 3. Full details on training resources for these methods on other datasets are available in the supplementary material due to space constraints.

Our RDM with the $L_{\text{RDM}}$ objective proves fastest in training and achieves the notably highest $43.4\%$ accuracy on DomainNet. While RDM demands more memory than Fish, due to the storage of MMD distance values, it can be trained in less time - under an hour - and still delivers a $0.7\%$ performance boost. This gain over Fish, a leading gradient matching method on DomainNet, is significant. Among two variants of RDM, the one using $L_{\text{RDM}}$ is both the fastest and most accurate, justifying our claims on the benefits of aligning the risk distribution of the worst-case domain.

More, to further highlight the efficacy of risk distribution alignment for DG, we compare the OOD performance learning curves of RDM with competing baselines using representation (CORAL) and gradient (Fish) alignments, as depicted in Figure 3b. Impressively, RDM consistently outperforms, demonstrating enhanced generalisation throughout the training process.

5.4. Ablation studies

We explore the impact of the matching coefficient $\lambda$ and training batch size on risk distribution matching, using primarily the PACS dataset for brevity. While other datasets exhibit similar trends, their detailed results are provided in the supplementary material.

Matching coefficient $\lambda$ Figure 4a illustrates the performance of RDM on the PACS dataset for varying values of the matching coefficient $\lambda$, spanning $\{0.1, 1.0, 2.5, 5.0, 7.5, 10.0\}$. Notably, as $\lambda$ increases, RDM’s accuracy consistently improves, justifying the significance of our risk distribution matching module in fostering generalisation. In particular, when $\lambda = 5.0$, RDM demonstrates a notable $1.6\%$ average accuracy boost across all domains, in contrast to when using only $\lambda = 0.1$. Across most datasets, a $\lambda$ value within $[0.1, 10.0]$ appears sufficient to produce good results.

Batch size We study the impact of batch size on RDM’s performance. Our assumption is that achieving accurate risk distribution matching through data samples would require larger batch sizes. Figure 4b validates this, revealing enhanced generalisation results on PACS with increased batch sizes. For PACS, sizes between $[70, 100]$ yield promising, potentially optimal outcomes, despite computational limitations restrict our exploration of larger sizes.

6. Conclusion

We have demonstrated that RDM, a novel matching method for domain generalisation (DG), provides enhanced generalisation capability by aligning risk distributions across domains. RDM efficiently overcomes high-dimensional challenges of conventional DG matching methods. RDM is built on our observation that risk distributions can effectively represent the differences between all domains, bypassing the need to directly compute the distributional variance. This approximate version not only offers computational efficiency but also delivers improved out-of-domain results. Our extensive experiments on several benchmarks reveal that RDM surpasses leading DG techniques. We hope our work can inspire further investigations into the benefits of risk distributions for DG.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Training (s)</th>
<th>Mem (GiB)</th>
<th>Acc (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fish</td>
<td>11,502</td>
<td>5.26</td>
<td>42.7</td>
</tr>
<tr>
<td>CORAL</td>
<td>11,504</td>
<td>17.00</td>
<td>41.5</td>
</tr>
<tr>
<td>RDM with $L_{\text{RDM}}$</td>
<td>9,854</td>
<td>16.94</td>
<td>43.1</td>
</tr>
<tr>
<td>RDM with $L_{\text{RDM}}$</td>
<td>7,749</td>
<td>16.23</td>
<td>43.4</td>
</tr>
</tbody>
</table>

Table 3. Comparison between Fish, CORAL, and two variants of our method in terms of the training time (seconds), memory usage per iteration (GiB) and accuracy (%) on DomainNet.
References


