A PRINCIPLED APPROACH TO MODEL VALIDATION IN DOMAIN GENERALIZATION

Boyang Lyu†‡, Thuan Nguyen†¶, Matthias Scheutz†, Prakash Ishwar‡, Shuchin Aeron†

† Department of Computer Science, Tufts University, Medford, MA 02155
‡ Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155
¶Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215

ABSTRACT

Domain generalization aims to learn a model with good generalization ability, that is, the learned model should not only perform well on several seen domains but also on unseen domains with different data distributions. State-of-the-art domain generalization methods typically train a representation function followed by a classifier jointly to minimize both the classification risk and the domain discrepancy. However, when it comes to model selection, most of these methods rely on traditional validation routines that select models solely based on the lowest classification risk on the validation set. In this paper, we theoretically demonstrate a trade-off between minimizing classification risk and mitigating domain discrepancy, i.e., it is impossible to achieve the minimum of these two objectives simultaneously. Motivated by this theoretical result, we propose a novel model selection method suggesting that the validation process should account for both the classification risk and the domain discrepancy. We validate the effectiveness of the proposed method by numerical results on several domain generalization datasets.

Index Terms—Domain generalization, model selection.

1. INTRODUCTION AND RELATED WORK

The success of traditional machine learning methods relies on an important assumption that the training and the test data are independent and identically distributed (i.i.d). However, in many real-world scenarios, the distributions of data in the training set and test set are not identical due to the “distribution-shift” phenomenon. Mitigating the problem caused by the distribution shift is the primary goal of the Domain Generalization (DG) problem, where a model is trained using data from several seen domains but later will be applied to unseen (unknown but related) domains with different data distributions.

To address DG problem, a large number of methods consider training a representation function that can learn domain-invariant features1 by minimizing the domain discrepancy in the representation space [1–6]. Though the domain discrepancy has been accounted for at the training step, few works considered it for model selection at the validation step [7]. Indeed, following traditional machine learning settings, most of the state-of-the-art DG methods form a validation set using a small portion of data from all seen domains and select the model that achieves the lowest classification risk or highest classification accuracy on it. However, unlike the traditional machine learning settings where a model with lower classification risk on the validation set is likely to perform better on the test set, we theoretically show that for DG problem, where the i.i.d assumption does not hold, selecting the model with minimum classification risk may enlarge the domain discrepancy, subsequently leading to a non-optimal model on the unseen domain. We thus argue that one needs to consider both the classification risk and the domain discrepancy for selecting good models on unseen domains.

We summarize our contributions as follows:

1. We theoretically show that there is a trade-off between minimizing classification risk and domain discrepancy. This trade-off leads to the conclusion that only targeting a model with the lowest classification risk on the validation set may encourage distribution mismatch between domains (enlarging domain discrepancy), and reduce the model’s generalization ability.

2. Based on our theoretical result and considering the limited attention given to DG-specific validation processes, we propose a simple yet effective validation/model selection method that integrates both the classification risk and domain discrepancy as the validation criterion. We further demonstrate the effectiveness of this approach on various DG benchmark datasets.

The trade-off between minimizing the classification risk and domain discrepancy has been mentioned in the literature [8, 9]2. Shai et al. [8] constructed an upper bound on the risk of the target domain, composed of the risk from the source domain and the discrepancy between the target and source domains. The authors suggested that there must be a trade-off between minimizing the domain discrepancy and minimizing the seen domain’s risk but did not propose any further details on how

1These authors contributed equally to this work.

2The works in [8, 9] are for domain adaptation, not domain generalization. However, one may derive a similar conclusion by replacing the “source domain” with seen domain and the “target domain” with unseen domain.
this trade-off is determined and characterized. Zhao et al. [9] showed that the sum of the risks from source and target domains is lower bounded by the distribution discrepancy between domains. If the discrepancy between domains is large, one can not simultaneously achieve small risks on both domains. Though sharing some similarities, our theoretical result differs from [9] since Zhao et al. considered the trade-off between minimizing the risks of different domains rather than the trade-off between optimizing the classification risk and the domain discrepancy. On the other hand, most DG works adopt the model selection methods following the traditional machine learning settings, i.e., a validation set is first formed by combining small portions of data from all seen domains and the model that produces the lowest classification risk or highest classification accuracy on the validation set is then selected. To the best of our knowledge, there are only a few works that explore new model selection methods under DG settings [10–14]. The most related work of this study is [13], where the authors mentioned that they use the training loss (including both classification risk and adversarial domain discrepancy loss) on the validation set for model selection. However, it is not clear from their paper and their released code how the performance on unseen domains (Sec. 4).

For a representation function $f$, the distribution discrepancy between seen and unseen domains induced by $f$ is:

$$D(f) = d(p^{(s)}(Y, Z)||p^{(u)}(Y, Z))$$ (2)

where $d(\cdot||\cdot)$ is a divergence measure between two distributions. Indeed, to deal with the “distribution-shift”, one usually looks for a mapping $f$ such that the discrepancy between distributions of seen and unseen domains $D(f)$ is small [15, 16]. A large number of DG works focus on training a model that minimizes both the classification risk $C^{(s)}(f, g)$ and the discrepancy $D(f)$ using data from seen domains [1–6]. Note that while $C^{(s)}(f, g)$ can be directly minimized, one usually need to approximately/heuristically optimize $D(f)$ by optimizing the distribution discrepancy between several seen domains. Since there are already well-established theoretical and empirical works on minimizing the classification risk and domain discrepancy, our work aims to highlight the trade-off between these two objectives (Sec 3) and argues that taking both objectives into account during model selection can improve model’s performance on unseen domains (Sec. 4).

3. TRADE-OFF BETWEEN CLASSIFICATION RISK AND DOMAIN DISCREPANCY

We first begin with a definition.

Definition 1 (Classification risk-domain discrepancy function). For any representation function $f$ and classifier $g$, define:

$$T(\Delta) = \min_{f : X \rightarrow Z} D(f) = \min_{f : X \rightarrow Z} d(p^{(s)}(Y, Z)||p^{(u)}(Y, Z))$$

s.t. $C^{(s)}(f, g) = \int_{x \in X} p^{(s)}(x)\ell(g(f(x)), y^{(s)}(x))dx \leq \Delta$ (3)

where $\Delta$ is a positive number, $\ell(\cdot, \cdot)$ is a distance measure, and $d(\cdot||\cdot)$ is a divergence measure.

$T(\Delta)$ is the minimal discrepancy between the joint distribution of the unseen domain and seen domain if the classification risk on seen domain $C^{(s)}(f, g)$ does not exceed a positive threshold $\Delta$. Next, we formally show that there is a trade-off between minimizing the distribution discrepancy $D(f)$ and minimizing the classification risk $C^{(s)}(f, g)$.

Theorem 1 (Main result). If the divergence measure $d(a||b)$ is convex (in both $a$ and $b$), for a fixed classifier $g$, $T(\Delta)$ defined in (3) is monotonically non-increasing, and convex.

Proof. The proof of this theorem is mainly based on the proposed approach in Rate-Distortion theory [17]. Particularly, consider two positive numbers $\Delta_1$ and $\Delta_2$, and assume $\Delta_1 \leq \Delta_2$. For a given classifier $g$, we use $\mathcal{F}_{\Delta_1}$ and $\mathcal{F}_{\Delta_2}$ to denote the sets of mappings $f$ such that $C^{(s)}(f, g) \leq \Delta_1$ and $C^{(s)}(f, g) \leq \Delta_2$, respectively. First, we show that $T(\Delta)$ is non-increasing. Indeed, from $\Delta_1 \leq \Delta_2$, $\mathcal{F}_{\Delta_1} \subset \mathcal{F}_{\Delta_2}$:

$$T(\Delta_1) = \min_{f \in \mathcal{F}_{\Delta_1}} d(p^{(s)}(Y, Z)||p^{(u)}(Y, Z))$$

$$\geq \min_{f \in \mathcal{F}_{\Delta_2}} d(p^{(s)}(Y, Z)||p^{(u)}(Y, Z)) = T(\Delta_2).$$
Second, to prove the convexity of $T(\Delta)$, we show that:

\[ \lambda T(\Delta_1) + (1-\lambda) T(\Delta_2) \geq T(\lambda \Delta_1 + (1-\lambda) \Delta_2), \quad \forall \lambda \in [0, 1]. \]  

(4)

To prove (4), we need some additional notations. Define:

\[ f_1 = \arg \min_{f:X \to Z} D(f) \quad \text{s.t.} \quad C(s(f, g)) \leq \Delta_1, \]  

(5)

\[ f_2 = \arg \min_{f:X \to Z} D(f) \quad \text{s.t.} \quad C(s(f, g)) \leq \Delta_2. \]  

(6)

Note that for any $f, Y \to X \to Z$ forms a Markov chain, thus:

\[ p^{(u)}(Y, Z) = p^{(u)}(Y \mid X) p^{(u)}(X, Z), \]  

(7)

\[ p^{(s)}(Y, Z) = p^{(s)}(Y \mid X) p^{(s)}(X, Z), \]  

(8)

where $p^{(u)}(Y \mid X)$ and $p^{(s)}(Y \mid X)$ are independent of $f$ and only depend on the conditional distributions of label and data on seen and unseen domains.

Let $p^{(u)}_1(Y, Z), p^{(s)}_1(Y, Z)$ be the joint distributions of $Y$ and $Z$ on unseen and seen domain produced by $f_1$, and similarly $p^{(u)}_2(Y, Z), p^{(s)}_2(Y, Z)$ be the joint distributions produced by $f_2$. Define:

\[ p^{(u)}_\lambda(X, Z) = \lambda p^{(u)}_1(X, Z) + (1-\lambda) p^{(u)}_2(X, Z), \]  

(9)

\[ p^{(s)}_\lambda(X, Z) = \lambda p^{(s)}_1(X, Z) + (1-\lambda) p^{(s)}_2(X, Z). \]  

(10)

By definition, the left hand side of (4) can be rewritten by:

\[
\lambda T(\Delta_1) + (1-\lambda) T(\Delta_2) = \lambda d(p^{(u)}_1(Y, Z) || p^{(s)}_1(Y, Z)) + (1-\lambda) d(p^{(u)}_2(Y, Z) || p^{(s)}_2(Y, Z)) = \lambda d(p^{(u)}(Y \mid X) p^{(u)}_1(X, Z)||p^{(s)}(Y \mid X) p^{(s)}_1(X, Z)) + (1-\lambda) d(p^{(s)}(Y \mid X) p^{(u)}_2(X, Z)||p^{(s)}(Y \mid X) p^{(s)}_2(X, Z)) \\
\geq d(p^{(u)}(Y \mid X) p^{(u)}_\lambda(X, Z)||p^{(s)}(Y \mid X) p^{(s)}_\lambda(X, Z)) \]  

(11)

where (11) and (12) are due to (7) and (8); (13) is due to (9), (10), and the convexity of $d(\cdot || \cdot)$.

Let $f_\lambda$ be the corresponding function that induces the joint distribution $p^{(u)}_\lambda(X, Z)$ and $p^{(s)}_\lambda(X, Z)$. Define:

\[ \Delta_\lambda = \int_{x \in X} \int_{z \in Z} p^{(s)}_\lambda(x, z) \ell(g(z), y^{(s)}(x)) \, dx \, dz. \]  

(14)

By definition of $T(\Delta)$ in Definition 1, we have:

\[ d(p^{(u)}(Y \mid X) p^{(u)}_\lambda(X, Z)||p^{(s)}(Y \mid X) p^{(s)}_\lambda(X, Z)) \geq T(\Delta_\lambda). \]  

(15)

Combine (13) and (15):

\[ \lambda T(\Delta_1) + (1-\lambda) T(\Delta_2) \geq T(\Delta_\lambda). \]  

(16)

That said, the left-hand side of (4) is greater or equal to $T(\Delta_\lambda)$. Next, we show that:

\[ T(\Delta_\lambda) \geq T(\lambda \Delta_1 + (1-\lambda) \Delta_2). \]  

(17)

Since $T(\Delta)$ is non-increasing, (17) is equivalent to:

\[ \Delta_\lambda \leq \lambda \Delta_1 + (1-\lambda) \Delta_2. \]  

Indeed, we have:

\[ \Delta_\lambda = \int_{x \in X} \int_{z \in Z} p^{(s)}_\lambda(x, z) \ell(g(z), y^{(s)}(x)) \, dx \, dz \]  

(19)

\[ = \lambda \int_{x \in X} \int_{z \in Z} p^{(s)}_1(x, z) \ell(g(z), y^{(s)}(x)) \, dx \, dz + (1-\lambda) \int_{x \in X} \int_{z \in Z} p^{(s)}_2(x, z) \ell(g(z), y^{(s)}(x)) \, dx \, dz \]  

(20)

\[ \leq \lambda (\Delta_1) + (1-\lambda) \Delta_2 \]  

(22)

with (19) due to (14), (20) and (21) due to (9), (22) due to (5) and (6), respectively. From (18) and (22), (17) follows. Finally, from (16) and (17), (4) follows. The proof is complete. \qed

It is worth noting that the convexity of $d(\cdot || \cdot)$ is not a restricted condition, indeed, most of the divergence functions, for example, the Kullback-Leibler (KL) divergence is convex.

Theorem 1 shows that only enforcing a small distribution discrepancy between domains will increase the classification risk and vice-versa.

4. A NEW VALIDATION METHOD

Based on Theorem 1, we argue that to select a good model for unseen domains, one must account for both the classification risk and the domain discrepancy not only in the training process but also in the validation process. Note that state-of-the-art model evaluation methods for DG are mainly based on the classification risk or, equivalently, the classification accuracy [7] [18] on the validation set to select the models. Given this fact, we propose to select a model that minimizes the following objective function on the validation set:

\[ L_{\text{Validation loss}} = \beta(1-\alpha) L_{\text{Classification risk}} + \alpha L_{\text{Domain-discrepancy loss}} \]  

(23)

where $\alpha$ is the convex combination hyper-parameter and $\beta$ is the scale hyper-parameter that supports the combination of objectives with different scales.

It is pretty clear that the cross-entropy loss is a good representation of classification risk. However, it is hard to choose the measure for quantifying the domain-discrepancy loss. Indeed, there exist various definitions of domain discrepancy. Several works characterize the domain-discrepancy via the difference in the marginal distributions [5, 6], other works measure it by the mismatch in conditional distributions [1]. We believe that finding a good measure for domain discrepancy is still an open problem. Therefore, in this short paper, we decide to use the widely accepted Maximum Mean Discrepancy (MMD) loss [6] in the feature space to quantify the domain discrepancy. We also acknowledge that though MMD measure is extensively used, it may not be the optimal choice.

In practice, we found that MMD loss is at the same scale as the cross-entropy loss when the training process is stable, we thus choose $\beta$ as 1. For $\alpha$, we consider the classification performance as the more important goal and thus heuristically...
choose $\alpha$ as 0.2. From our experiments, we found that the performance of our validation method is robust to small values of $\alpha$ within the range of $[0.1, 0.3]$. One more insight from Theorem 1 is that it is advisable to avoid extreme points in $\Delta$ (classification error) to maintain a balance between the model’s generalization and prediction capabilities. This means the classification error should not be too small or too large. Thus, for each hyper-parameter configuration, we sort the validation cross-entropy loss in ascending order and only pick the models that produce 5% to 50% percentile of the validation cross-entropy loss as a subset of candidates for model selection. Our implementation is released at this link\(^3\).

5. NUMERICAL RESULTS

We compare the proposed model selection method with the Training-domain validation method described in [18] on three datasets: PACS, VLCS, and Colored-MNIST (C-MNIST) using DomainBed package and 12 different DG algorithms provided there [18]. Recall that the Training-domain validation method chooses the model that produces the highest validation accuracy, while our method selects the model that minimizes the objective function in (23). For PACS and VLCS datasets, we report the average test accuracy over 4 different tasks with each time leaving one domain out as the unseen domain. For the C-MNIST dataset, we only focus on the most difficult domain, where the correlation between the label and the color of the unseen domain is completely different from the seen domains and no algorithm can achieve more than 10.5% points accuracy [18].

The validation set is formed using 20% data from each seen domain, denoted as the training-domain validation set in [18]. We follow exactly the same settings and training routine used in DomainBed and conduct 20 trials of random search over a joint distribution of hyper-parameters for each task per algorithm. For the MMD loss implementation, we directly use the code provided in DomainBed package. We train each model for 5000 steps. The validation cross-entropy loss, MMD loss, and validation accuracy are recorded every 100 steps for VLCS dataset and every 300 steps for PACS and C-MNIST datasets.

With $\alpha = 0.2$, $\beta = 1$, the performance of each algorithm under different validation methods on PACS, VLCS and Colored-MNIST datasets is shown in Table 1. We refer to the Training-domain validation method as “Traditional” and the proposed method as “Ours”. For the PACS dataset, the proposed validation method can select slightly better models for seven out of twelve DG algorithms. For the remaining five DG algorithms, our method achieves comparable performance with the “Traditional” method on CORAL [5] and VREx [24]. However, for Fish [19], CDANN [22] and RSC [25], we observe a performance deterioration. The effectiveness of the proposed method can be more easily observed on VLCS dataset, where eight out of twelve DG algorithms get an improved model selected, with the improvement varies from 0.2% to 3.2%. For the C-MNIST dataset, the proposed validation method consistently selects models with better performance compared with the “Traditional” validation method. Accuracy improves for nine out of twelve tested algorithms with the most significant improvement for VREx [24] method by 5.4%.

6. CONCLUSION

By showing the trade-off between minimizing the classification risk and domain discrepancy, we demonstrate that the traditional model selection methods may not be suitable for DG problem and propose a new model selection method that considers both objectives. While our approach outperforms traditional methods on several DG algorithms and datasets, it lacks an automatic hyper-parameter tuning strategy. Note that the domain discrepancies may vary across different datasets, one may not expect the same optimal values of $\alpha$ and $\beta$ for all datasets. Determining the “optimal” ones could be a hard problem both practically and theoretically. We thus leave it as an open problem for future work. Despite this limitation, we believe our approach provides insight and initial results for exploring new model selection methods specific for DG problem.

\(^3\)https://github.com/thuan2412/A-principled-approach-for-model-validation-for-domain-generalization

Table 1. Classification accuracy of 12 tested algorithms on PACS, VLCS, and C-MNIST datasets using the Training-domain validation method (Traditional) proposed in [18] vs. using our new validation method.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PACS (Traditional)</td>
<td>84.6</td>
<td>84.9</td>
<td>84.2</td>
<td>83.3</td>
<td>85.1</td>
<td>83.6</td>
<td>84.6</td>
<td>86.4</td>
<td>83.0</td>
<td>84.5</td>
<td>85.2</td>
<td>83.7</td>
<td></td>
</tr>
<tr>
<td>PACS (Ours)</td>
<td>82.0</td>
<td>85.3</td>
<td>84.3</td>
<td>85.3</td>
<td>84.9</td>
<td>85.0</td>
<td>84.9</td>
<td>82.0</td>
<td>84.2</td>
<td>84.2</td>
<td>81.3</td>
<td>85.1</td>
<td>7/12</td>
</tr>
<tr>
<td>VLCS (Traditional)</td>
<td>79.4</td>
<td>76.0</td>
<td>78.1</td>
<td>77.4</td>
<td>76.8</td>
<td>78.5</td>
<td>77.8</td>
<td>79.2</td>
<td>77.3</td>
<td>76.4</td>
<td>78.6</td>
<td>80.5</td>
<td></td>
</tr>
<tr>
<td>VLCS (Ours)</td>
<td>77.5</td>
<td>79.2</td>
<td>79.6</td>
<td>77.6</td>
<td>78.8</td>
<td>78.0</td>
<td>78.5</td>
<td>80.3</td>
<td>78.2</td>
<td>78.6</td>
<td>76.1</td>
<td>79.3</td>
<td>8/12</td>
</tr>
<tr>
<td>C-MNIST (Traditional)</td>
<td>10.0</td>
<td>10.0</td>
<td>10.2</td>
<td>10.4</td>
<td>9.7</td>
<td>10.4</td>
<td>10.0</td>
<td>9.9</td>
<td>10.5</td>
<td>10.2</td>
<td>10.2</td>
<td>10.4</td>
<td></td>
</tr>
<tr>
<td>C-MNIST (Ours)</td>
<td>9.7</td>
<td>10.9</td>
<td>12.6</td>
<td>10.3</td>
<td>11.2</td>
<td>9.9</td>
<td>11.1</td>
<td>10.2</td>
<td>11.5</td>
<td>15.6</td>
<td>13.8</td>
<td>10.5</td>
<td>9/12</td>
</tr>
</tbody>
</table>
7. REFERENCES


Authorized licensed use limited to: TUFTS UNIV. Downloaded on May 12,2023 at 13:48:00 UTC from IEEE Xplore. Restrictions apply.